A companion to the note *On the irrationality of the* 3*-adic zeta value* $\zeta_3(5)$

Produced by large language models
not reviewed by the author or by any human expert

October 2026

Contents

How to read this companion **ix**

I The idea and the tools **1**

1 How to prove that a number is irrational **2**
1.1 The one principle: a nonzero integer is at least 1 in size . . . 2
1.1.1 A first example: the number e . . . 3
1.2 Linear forms and Apéry's idea . . . 3
1.3 Counting in bits, trits and nats . . . 4
1.4 The p-adic twist: small means divisible . . . 5
1.5 The Hankel-determinant variant . . . 6
1.6 The balance sheet of the note . . . 7
1.7 Non-vanishing and the choice of K . . . 8
1.8 A map of the proof . . . 9
1.9 History and status . . . 10
Summary of the chapter . . . 10

2 p-adic numbers **12**
2.1 Valuations and absolute values on $\mathbb{Q}$ . . . 12
2.2 The product formula . . . 14
2.3 Completing $\mathbb{Q}$: the p-adic numbers . . . 15
2.3.1 Why complete, and how . . . 15
2.3.2 Digit expansions . . . 15
2.3.3 Which expansions are rational? . . . 17
2.4 Convergence of series . . . 18
2.5 Units, and the set of integration points . . . 19
2.5.1 Units . . . 19
2.5.2 The set S . . . 19
2.6 The residue field $\mathbb{F}_p$ . . . 21
2.7 The Gauss valuation of polynomials . . . 22
2.8 Legendre's formula . . . 23
2.9 What "$\zeta_3(5) = a/b$" means . . . 24
Summary of the chapter . . . 25

3 Bernoulli numbers and the 3-adic zeta value **26**
3.1 Bernoulli numbers . . . 26
3.2 Bernoulli polynomials and sums of powers . . . 27
3.3 Values of the Riemann zeta function . . . 29
3.3.1 Even positive integers: Euler's formula . . . 29
3.3.2 Negative integers . . . 29

3.3.3 Odd positive integers . . . 30
3.4 Denominators and congruences . . . 30
3.5 Dirichlet characters and the Teichmüller character . . . 31
3.6 The Kubota–Leopoldt p-adic L-function . . . 33
3.6.1 The statement . . . 33
3.6.2 Why the Euler factor at p is removed . . . 34
3.6.3 Branches, the twist, and $\zeta_p(s)$ . . . 34
3.7 Computing $\zeta_3(5)$ in two ways . . . 35
3.7.1 Route (i): a limit of Bernoulli numbers . . . 35
3.7.2 Route (ii): the series [note, (2.13)] . . . 36
3.7.3 Agreement . . . 37
3.8 What "$\zeta_3(5)$ is irrational" means . . . 37
Summary of the chapter . . . 38

4 The Volkenborn integral **39**
4.1 Why an integral? . . . 39
4.2 Riemann sums over $\mathbb{Z}_3$ . . . 40
4.2.1 A first experiment . . . 40
4.2.2 The definition . . . 40
4.3 Strict differentiability . . . 41
4.4 Binomial polynomials . . . 42
4.5 The three properties (V1)–(V3) . . . 43
4.5.1 (V2): integrals of polynomials . . . 43
4.5.2 (V1): shifting by one costs $f'(0)$ . . . 44
4.5.3 (V3): a small, flat function has a small integral . . . 45
4.6 The set S and the reflection lemma . . . 46
4.7 The value lemma: $\zeta_3(5)$ as an integral . . . 47
4.8 Harmonic sums . . . 49
4.9 The translation lemma . . . 51
Summary of the chapter . . . 52

II The machine **53**

5 The weight, the functional and purity **54**
5.1 Partial fractions and residues . . . 54
5.1.1 Principal parts . . . 54
5.1.2 The sum of the residues . . . 55
5.2 Pochhammer symbols . . . 56
5.3 The weight . . . 56
5.3.1 Definition and the four factors . . . 56
5.3.2 Antisymmetry . . . 57
5.3.3 What the zeros and the poles are for . . . 58
5.4 The functional, and why only $\zeta_3(5)$ survives . . . 58
5.4.1 The definition . . . 58
5.4.2 The heuristic: follow one pole . . . 58
5.5 Node data . . . 59
5.5.1 The leading coefficient h_k . . . 59
5.5.2 Symmetry of the node data . . . 60
5.5.3 Taylor coefficients of P at a node . . . 61
5.6 The purity lemma . . . 61
5.7 A worked example: $n = 1$, and a check by Riemann sums . . . 62

5.7.1 The local constants . . . 62
5.7.2 A check by Riemann sums . . . 63
Summary of the chapter . . . 65

6 Hankel determinants and the Hankel polynomial 66
6.1 Moments and Hankel matrices . . . 66
6.1.1 Linear functionals and their moments . . . 66
6.1.2 The Hankel matrix . . . 67
6.1.3 The Hankel matrix is a Gram matrix . . . 67
6.2 Change of basis . . . 67
6.3 Positive measures: orthogonal polynomials and Heine's formula . . . 68
6.3.1 Gram–Schmidt and orthogonal polynomials . . . 68
6.3.2 Heine's formula and the Coulomb gas . . . 69
6.3.3 Positivity . . . 70
6.4 No positivity in $\mathbb{Q}_3$ . . . 70
6.5 The Hankel polynomial . . . 71
6.5.1 Why an indeterminate . . . 71
6.5.2 The definition . . . 71
6.5.3 The degree . . . 72
6.5.4 The value at $\zeta_3(5)$, and why $K \leq 3n+1$ . . . 72
6.6 The jet form and the node matrices . . . 72
6.6.1 The Leibniz rule for Taylor coefficients . . . 72
6.6.2 The jet form . . . 73
6.6.3 A sum of matrices of rank at most four . . . 73
6.7 A worked example: $n = 1$ . . . 75
6.7.1 The moments . . . 75
6.7.2 The Hankel polynomials . . . 75
6.7.3 The rank-four decomposition . . . 76
6.7.4 The value at $\zeta_3(5)$ . . . 76
6.7.5 A triangular change of basis . . . 77
Summary of the chapter . . . 78

III The skeleton of the proof 79

7 The criterion, the four estimates and the proof of the theorem 80
7.1 The criterion . . . 80
7.1.1 What we want, and the ingredients . . . 80
7.1.2 The proof, step by step . . . 81
7.2 The criterion at $n = 1$: no contradiction, and why . . . 83
7.3 Dominance: how to know that $\Delta_K(a/b) \neq 0$ . . . 84
7.4 The four estimates . . . 85
7.4.1 The parameter κ and the intervals . . . 85
7.4.2 A picture of the leading terms . . . 86
7.4.3 Why the $n^2 \log n$ terms cancel: the product formula . . . 87
7.5 Primes in the window . . . 88
7.6 The proof of Theorem 1.1 . . . 89
7.6.1 An illustration: how large must n be? . . . 90
7.7 The logical status of the theorem . . . 91
Summary of the chapter . . . 91

IV The four estimates 93

8 Estimate 1: the 3-adic gain 94
8.1 The plan: make every entry uniformly small . . . 94
8.2 Integer-valued polynomials . . . 95
8.2.1 On $\mathbb{Z}$ and on $\mathbb{Z}_3$ . . . 95
8.2.2 On the set S . . . 96
8.3 The basis F_i . . . 97
8.3.1 Proof that F_i is integer valued on S . . . 97
8.3.2 The leading coefficients . . . 98
8.3.3 Can one do better? The optimal basis . . . 98
8.3.4 The change-of-basis inequality [note, (4.3)] . . . 99
8.4 The cost of the change of basis . . . 100
8.5 The weight on S: the factorization [note, (4.5)] . . . 101
8.5.1 The Taylor coefficients of Q_r . . . 102
8.5.2 The trit budget . . . 103
8.6 The analytic step: derivative and integral cost only logarithms . . . 103
8.6.1 Stirling numbers of the second kind . . . 104
8.6.2 The function ψ . . . 104
8.6.3 The product of two binomial polynomials . . . 105
8.6.4 The derivative of a binomial polynomial . . . 105
8.6.5 The proof of Lemma 8.15 . . . 106
8.6.6 The proof in numbers . . . 107
8.7 The proof of [note, Theorem 3.5] . . . 108
8.8 The bound against the true valuation . . . 109
Summary of the chapter . . . 111

9 The Heine expansion 112
9.1 The Vandermonde determinant . . . 112
9.2 Tensor powers of a functional . . . 113
9.3 Andreief's identity . . . 114
9.3.1 The case $s = 2$ by hand . . . 114
9.3.2 The general statement and proof . . . 114
9.4 Heine's formula . . . 115
9.5 The statement of the Heine expansion . . . 116
9.5.1 What we start from . . . 116
9.5.2 Profiles and partitions . . . 117
9.5.3 The proposition . . . 118
9.6 The proof of the Heine expansion . . . 118
9.6.1 Step 1: Heine's formula for Λ . . . 118
9.6.2 Step 2: distributing the variables over the nodes . . . 119
9.6.3 Step 3: local coordinates and the cross factor . . . 119
9.6.4 Step 4: symmetry inside a node . . . 120
9.6.5 Step 5: the tensor product factorizes over the nodes . . . 121
9.6.6 Step 6: what one node can contribute . . . 121
9.7 The expansion in numbers . . . 123
9.7.1 All of Δ_K for $n = 1$ and $n = 3$ . . . 123
9.7.2 Which profiles matter . . . 124
9.7.3 One profile taken apart . . . 125
9.8 What each part of a term carries . . . 125
Summary of the chapter . . . 126

10 Estimate 2: the size, an electrostatics problem **128**
10.1 What is being estimated . . . 128
10.2 From profiles to densities . . . 129
10.3 Logarithmic potentials and the external field . . . 130
10.4 The energy functional, its first variation and the gap . . . 131
10.5 Conditional negative definiteness . . . 132
10.6 The discrete energy bounds the size . . . 134
10.7 The modulus of continuity . . . 136
10.8 The continuum limit . . . 137
10.9 The proof of the size theorem . . . 139
10.10 The trial density and the bound for $F^\dagger$ . . . 139
10.10.1 Reduction to a linear problem [note, (E.1)] . . . 140
10.10.2 The primitives Φ and Γ [note, (E.2)] . . . 140
10.10.3 The linear problem: put the mass where the potential is highest . . . 141
10.10.4 Ball arithmetic . . . 142
Summary of the chapter . . . 143

11 Estimate 3a: denominators, the tree bound and the small primes **145**
11.1 What "the denominators of Δ_K" are . . . 145
11.2 Valuations as counts . . . 146
11.3 The tree of residue classes . . . 146
11.4 The local data of a node: η_p, e_p, f_p . . . 147
11.5 The tree bound . . . 148
11.5.1 Proof, following [note, Appendix B] . . . 148
11.6 The number D_k . . . 150
11.7 Lemma 5.16: the Taylor coefficients and the harmonic sums . . . 151
11.8 The leaf lemma . . . 152
11.9 The small primes . . . 152
11.9.1 Proof, following [note, Appendix C] . . . 153
11.9.2 A concrete test . . . 154
11.10 The middle primes . . . 155
11.11 Summing over the primes: Mertens' theorem . . . 156
11.12 What is left . . . 158
Summary of the chapter . . . 158

12 Estimate 3b: single-level primes and virtual poles **159**
12.1 Single-level primes . . . 159
12.2 The p-special points of a node . . . 160
12.3 The node data . . . 161
12.4 Virtual poles: Lemma 5.22 . . . 163
12.4.1 A generating function . . . 163
12.4.2 The lemma . . . 163
12.5 The refined local lemma . . . 164
12.5.1 Proof, following the note . . . 165
12.5.2 The cancellation in one node . . . 166
12.5.3 The refined bound against the truth . . . 166
12.6 The cancellation in action: the primes $p > 3n$ . . . 167
12.7 Why order 3 meets order 3 . . . 169
12.8 Remark 5.27: the cancellation is needed . . . 169
Summary of the chapter . . . 170

13 Estimate 3c: the circle model and the prime sum **171**
13.1 The goal . . . 171
13.2 The relaxation: Lemma 5.28 . . . 172
13.2.1 From f_p to f^+ . . . 172
13.2.2 One problem per class . . . 173
13.2.3 The price of a row: ψ_c and weak duality . . . 174
13.3 The circle model . . . 175
13.3.1 A residue class is a point on a circle . . . 175
13.3.2 The node data depend only on (x, ϱ) . . . 175
13.4 Cells: Lemma 5.31 . . . 176
13.4.1 The picture for $\varrho = 2.2$ . . . 177
13.5 Counting: Lemma 5.34 . . . 178
13.6 The prime sum: Proposition 5.36 . . . 180
13.6.1 Three facts about primes . . . 180
13.6.2 The statement . . . 181
13.6.3 Proof, following [note, Appendix C] . . . 181
13.7 The constants c_i . . . 182
13.7.1 Formula (5.39) and Proposition 5.40 . . . 182
13.7.2 How the sums are computed: Appendix E, second part . . . 183
Summary of the chapter . . . 185

14 Estimate 4: non-vanishing at an auxiliary prime **186**
14.1 The strategy . . . 186
14.2 The nodes and their local constants . . . 188
14.2.1 Partners . . . 188
14.2.2 The thresholds . . . 189
14.2.3 The types: Lemma 6.1 and Table 2 . . . 190
14.2.4 The counts and the number $K(n, p)$ . . . 191
14.2.5 The functions Φ_k: zooming in by a factor p . . . 192
14.2.6 Lemma 6.7: the scaled local constants . . . 193
14.2.7 Wilson's theorem . . . 194
14.2.8 Lemma 6.10: the partner congruence . . . 195
14.3 An adapted basis and the reduction . . . 196
14.3.1 Why $K(n, p)$, and the weights . . . 196
14.3.2 Hermite interpolation and the Chinese remainder theorem over $\mathbb{F}_p$ . . . 197
14.3.3 The Gram matrix in the new basis . . . 198
14.3.4 Taylor coefficients at the partners . . . 198
14.3.5 Weighted valuations: Lemma 6.17 . . . 199
14.3.6 The field $\mathbb{Q}_p(\sqrt{p})$ . . . 201
14.3.7 The scaled matrix and its block structure . . . 201
14.3.8 The blocks: Lemma 6.18 . . . 202
14.3.9 The block determinants . . . 203
14.3.10 Proof of Theorem 3.13 . . . 204
14.4 The worked example and further cases . . . 205
Summary of the chapter . . . 206

15 Looking back: the whole proof on two pages **208**
15.1 The proof in ten steps . . . 208
15.2 What the note takes from outside . . . 209
15.3 What the worked examples show . . . 210
15.4 What the examples cannot show . . . 210

15.5 The two proofs side by side . . . 210
15.6 Remarks on the note . . . 211
Summary of the chapter . . . 211

V The second proof **212**

16 A crash course in modular forms on $X_0(3)$ **213**
16.1 The upper half plane and the modular group . . . 213
16.1.1 Moebius maps . . . 213
16.1.2 The group $\Gamma_0(3)$ . . . 214
16.1.3 A fundamental domain for $\Gamma_0(3)$ . . . 215
16.1.4 Gluing: cusps, the elliptic point, and a sphere . . . 215
16.2 q-expansions and modular forms . . . 216
16.3 The Dedekind eta function . . . 217
16.4 The coordinate x on $X_0(3)$ . . . 218
16.4.1 Definition and q-expansion . . . 218
16.4.2 The Fricke relation and the invariance of x . . . 218
16.4.3 The sphere in the coordinate x . . . 219
16.5 The j-function and Lemma F.5(c) . . . 219
16.6 The weight-2 form B . . . 220
16.6.1 Definition and q-expansion . . . 220
16.6.2 Weight 2 and Lemma F.6 . . . 221
16.6.3 The operators D and θ, and the logarithmic derivative u . . . 221
16.7 Eisenstein series, G_5 and Eichler integrals . . . 222
16.7.1 A weight-6 form on $\Gamma_0(3)$ . . . 222
16.7.2 G_5 is an Eichler integral . . . 222
16.8 Lemma F.7: two rational functions . . . 223
16.9 The recursion (F.8) and Lemma F.9 . . . 225
16.9.1 What the recursion computes . . . 225
16.10Lemma F.10: the operator L_5 . . . 226
16.11How Chapter 17 uses these objects . . . 227
Summary of the chapter . . . 228

17 The second proof **229**
17.1 The plan in plain words . . . 229
17.1.1 One rational number, measured at every place . . . 229
17.1.2 The balance sheet, compared with the main proof . . . 230
17.1.3 What rests on what . . . 230
17.2 The determinant . . . 231
17.2.1 The germs, concretely . . . 231
17.2.2 Differential modules . . . 231
17.2.3 No rational solution: Lemma F.12 . . . 232
17.2.4 Irreducibility through monodromy: Lemma F.13 . . . 233
17.2.5 Independence of the germs: Proposition F.14 . . . 234
17.2.6 The zero estimate: Proposition F.15 . . . 234
17.2.7 Jumps, the matrix M, and $\mathcal{D}_d \neq 0$ . . . 235
17.3 The 3-adic estimate . . . 236
17.3.1 What is needed, and what it looks like . . . 236
17.3.2 Ordinary and supersingular, and Newton polygons . . . 237
17.3.3 Overconvergent modular forms: the black boxes . . . 238
17.3.4 Proposition F.24 in outline . . . 240

17.3.5 The gain: Proposition F.26 . . . 241
17.4 The primes $\ell \neq 3$ . . . 241
17.4.1 Where denominators come from . . . 241
17.4.2 The Eisenstein series $E_{\ell-1}$ and Lemma F.27 . . . 242
17.4.3 Lemma F.29: Q_ℓ is squarefree modulo ℓ . . . 242
17.4.4 The Sym^4 congruence: Proposition F.31 . . . 243
17.4.5 Smith normal form, from scratch . . . 244
17.4.6 Proposition F.36, Lemma F.38, Lemma F.39 and the layer theorem . . . 244
17.4.7 The sum over primes: Proposition F.42 . . . 245
17.5 The archimedean estimate . . . 246
17.5.1 Jensen's formula . . . 246
17.5.2 The idea, and the measure μ . . . 247
17.5.3 Leading coefficients and the Gram determinant . . . 247
17.5.4 The kernel formula: Lemma F.54 . . . 248
17.5.5 The 34 circles of Table 3 . . . 249
17.6 The final inequality . . . 249
Summary of the chapter . . . 250

A Glossary of symbols **251**

References **255**

How to read this companion

Status

This companion, like the note it explains, was produced by large language models, instances of the Claude models of Anthropic running as autonomous agents, in September and October 2026. The author of the note has not reviewed it, and no human expert has checked either the note or this companion. It is published together with the note as an explanation of its proofs. It may contain errors in its explanations, examples and remarks, in addition to any errors in the note itself.

This companion explains the note *On the irrationality of the* 3*-adic zeta value* $\zeta_3(5)$, in its version of October 2026. The note is written for specialists: in a few lines it uses p-adic integration, Bernoulli numbers, Hankel determinants, logarithmic potential theory, the prime number theorem and modular forms, and it compresses each argument. This companion tries to undo the compression for a reader who knows calculus, linear algebra and some physics: it defines the objects it uses, illustrates them with small examples, and writes out the steps of the note's proofs in more detail. Where the note takes a deep theorem from the literature (the prime number theorem, the existence of the Kubota–Leopoldt p-adic L-function, the theorems of Coleman and Buzzard on overconvergent modular forms), the companion states it and explains what it says, but does not prove it.

The proof in one paragraph

Suppose $\zeta_3(5) = a/b$ were a fraction. The note builds, for every large odd n, a polynomial $\Delta_K(X)$ with rational coefficients whose value at $X = \zeta_3(5)$ is a determinant of 3-adic integrals. Three estimates compete. The value $\Delta_K(\zeta_3(5))$ is divisible by an enormous power of 3 (the *gain*). The coefficients of Δ_K are not too large (the *size*) and have not too many primes other than 3 in their denominators (the *denominators*). If $\Delta_K(a/b)$ is not zero, clearing denominators in $\Delta_K(a/b)$ produces a nonzero integer, and the three estimates say that this integer is divisible by a power of 3 larger than the integer itself, which is impossible. The fourth estimate, *non-vanishing*, shows that $\Delta_K(a/b) \neq 0$ by looking at the polynomial modulo an auxiliary prime p of size about $2.1n$. The three quantitative estimates are of order n^2 (after the terms of order $n^2 \log n$ cancel between size and denominators), and, by the note's computed bounds, the gain wins by a margin of at least 4.58 bits per n^2 [note, Table 1].

How the companion is organised

Part I collects the tools: the logic of irrationality proofs (Chapter 1), p-adic numbers (Chapter 2), Bernoulli numbers and the definition of $\zeta_3(5)$ (Chapter 3), and the Volkenborn integral (Chapter 4). Part II builds the machine of the proof: the weight W and the functional L (Chapter 5) and the Hankel polynomial $\Delta_K(X)$ (Chapter 6). Part III gives the skeleton: the criterion and the deduction of the theorem from four estimates (Chapter 7). Part IV explains

the note's proofs of the four estimates: the 3-adic gain (Chapter 8), the size (Chapters 9 and 10), the denominators (Chapters 11 to 13) and the non-vanishing (Chapter 14), and Chapter 15 puts the whole proof on two pages and collects the remarks on the note. Part V explains the second proof of the note's Appendix F, which uses modular forms (Chapters 16 and 17). The appendix gives a glossary of the main symbols with the place where it is defined (Chapter A).

There are three ways through. The quickest is Chapter 1, then Chapter 7, then Chapter 15: this shows the architecture of the proof and what each estimate contributes, without the proofs of the estimates. The main line is Parts I to IV in order. The chapters of Part IV can be read in any order after Chapter 7, except that Chapter 9 comes before Chapter 10 and Chapter 11, Chapters 11 and 12 come before Chapter 13, and Chapter 13 comes before Chapter 14; Chapter 13 also uses the duality idea of Chapter 10. Part V needs Chapters 1 to 3, Chapter 7, and the logarithmic potentials and energies of Chapter 10.

Conventions

A reference such as [note, Lemma 2.19] points to the note's own numbering, in its version of October 2026; references without that tag point inside this companion. Each chapter opens with a blue box, *Where we are*, that places it in the proof. Yellow boxes, *Intuition*, say in plain words what an object or a step means. Green boxes, *What just happened*, sum up a long argument. Red boxes, *Remark on the note*, mark places where the note's argument is terse, where a sentence is imprecise, or where it relies on something it does not prove; they are collected in Chapter 15.

This companion was written for an earlier version of the note, and the note has since renamed several symbols to avoid clashes. The companion uses the earlier names. The main differences are the following.

earlier name (used here)	name in the note	meaning
L_k, L_k^{loc}	Λ_k, Λ_k^{loc}	local functional at the node k
$r_{k,i}$	$\mathrm{res}_{k,i}$	principal-part coefficients of PW
F_{2q}, F_{2q+1}	F_{2m}, F_{2m+1}	basis of $\mathrm{Int}(S)$
$F[\sigma]$	$\mathcal{E}[\sigma]$	energy functional
$I=(0,1)$, O	I_{in}, I_{out}	supports of the zeros and of the remaining poles
c (a residue class), S_c, V_c, ψ_c, N_c, z_c	$\mathfrak{c}$, $S_{\mathfrak{c}}$, $V_{\mathfrak{c}}$, $\psi_{\mathfrak{c}}$, $N_{\mathfrak{c}}$, $z_{\mathfrak{c}}$	residue classes of nodes
$e_p(k,s,\ell)$	$\mathsf{e}_p(k,s,\ell)$	local loss in the tree bound
λ, λ_ν (multiplier)	ξ, ξ_ν	Lagrange multiplier
$g_{[a,b]}$, $\bar{g}_\nu$	$\mathcal{G}_{[a,b]}$, $\bar{\mathcal{G}}_\nu$	cell function of the circle model
U_k	Υ_k	unit part of $\widetilde{W}_k$ in Section 6
ω (weighted valuation)	ϖ	weighted valuation in Section 6 and Appendix D
$B=[\binom{j}{a}]$	Bin	binomial matrix in Section 6
S_N, M in (V3)	Σ_N, A	Riemann sums, Lipschitz bound
$\psi(m)$, γ_m, P_c (App. A)	$\varsigma(m)$, $\hat{q}_m$, $\hat{P}_c$	proof of Lemma 4.2
γ_k, ω_x, P_j, Φ (App. B)	∇_k, ξ_x, $\mathfrak{s}_j$, $\mathcal{Q}_1$	proofs of Appendix B
Φ, Γ, ω_m (App. E)	$\mathcal{Q}_1$, $\mathcal{Q}_2$, $\bar{\sigma}_m$	the computation of $F_i^\dagger$
ω_i, Δ, c_m, e_i, $p^{(k)}$ (App. F)	ϖ_i, Wr, $\mathfrak{c}_m$, $\mathfrak{e}_i$, $\mathbf{a}^{(k)}$	second proof

The worked examples use exact rational arithmetic wherever the statement is exact; where a real-analytic constant is evaluated numerically in floating point, the text says so, since such an evaluation illustrates a bound but does not prove it.

What this companion does and does not establish

The note has not been refereed, and its proofs have not been checked by an expert. This companion explains the note's argument; it does not certify it. Writing a proof out in more detail makes it easier to check, but it does not make it checked, and the companion therefore says "the note's argument is" and not "we have proved". Where the expansion found an imprecise sentence or a step that relies on outside results, it says so in a *Remark on the note* box. The worked examples test special cases (small n, single primes, the printed constants); they can expose an error in a formula or a number, but they do not test the asymptotic estimates, which hold only for large n.

Part I

The idea and the tools

Chapter 1

How to prove that a number is irrational

Where we are. This chapter contains no part of the proof itself. It explains the idea that the whole note is built on, introduces the units in which the note keeps its accounts (bits and trits, "per n^2"), and gives a map of the proof with the note's section numbers, so that every later chapter can be placed on that map. It covers the note's introduction [note, Section 1] and previews the skeleton [note, Section 3], which is explained in full in Chapter 7. It needs nothing from other chapters. The 3-adic notions used here informally ("divisible by a high power of 3") are defined properly in Chapter 2, and the number $\zeta_3(5)$ itself is constructed in Chapter 3.

1.1 The one principle: a nonzero integer is at least 1 in size

Every irrationality proof in this companion, and most irrationality proofs in the literature, rests on one elementary fact.

Fact 1.1 (the integer gap)**.** *If $N \in \mathbb{Z}$ and $N \neq 0$, then $|N| \geq 1$.*

There is nothing to prove: the integers closest to 0 other than 0 itself are ± 1. The strength of the fact lies in how it is used. Suppose we want to show that a real number ξ is irrational. We assume the opposite, $\xi = a/b$ with integers a and $b > 0$, and from this assumption we manufacture an integer N. If we can show at the same time that

1. N is an integer (this is where the assumption $\xi = a/b$ is used, to clear denominators),
2. $N \neq 0$, and
3. $|N| < 1$,

then Fact 1.1 is contradicted, and the assumption must be false. All the work is in making the three properties hold simultaneously. Property 3 says that N is *small*; property 1 says that its denominators have been cleared, which tends to make it *large*; property 2 forbids the cheap way out, $N = 0$.

Intuition: bookkeeping. Think of $\log |N|$ as a bank balance. Producing a quantity that is very small puts money in the bank; every denominator that has to be cleared to make it an integer costs money. The proof succeeds if the balance stays negative, $\log |N| < 0$, while property 2 guarantees that the account is not simply closed. The rest of this chapter, and in a sense the rest of this companion, is about making the entries of this balance sheet precise for $\zeta_3(5)$.

1.1.1 A first example: the number e

The irrationality of e (Fourier's proof, found in most analysis textbooks) shows the bookkeeping in its simplest form. Recall $e = \sum_{j\ge 0} 1/j!$.

Proposition 1.2. *The number e is irrational.*

Proof. Suppose $e = a/b$ with integers $a, b > 0$. Fix an integer $n \ge b$ and split the series after the term $1/n!$:

$$e = S_n + T_n \ , \qquad S_n = \sum_{j=0}^{n} \frac{1}{j!} \ , \qquad T_n = \sum_{j>n} \frac{1}{j!} \ .$$

Put $N_n = n!\,T_n = n!\,(e - S_n)$. We check the three properties.

1. N_n is an integer. We have $n!\,e = n!\,a/b$, which is an integer because $b \le n$ divides $n!$. And $n!\,S_n = \sum_{j\le n} n!/j!$ is a sum of integers, since $j!$ divides $n!$ for $j \le n$. So $N_n = n!\,e - n!\,S_n$ is a difference of two integers.

2. $N_n \neq 0$. T_n is a sum of positive terms, so $N_n > 0$.

3. $N_n < 1$. For $j > n$ we have $n!/j! = 1/((n+1)(n+2)\cdots j) \le 1/(n+1)^{j-n}$, because each of the $j - n$ factors is at least $n + 1$. Summing the geometric series,

$$N_n = \sum_{j>n} \frac{n!}{j!} \le \sum_{i\ge 1} \frac{1}{(n+1)^i} = \frac{1/(n+1)}{1 - 1/(n+1)} = \frac{1}{n} \le 1 \ ,$$

and the first inequality is strict because already the term $j = n + 2$ satisfies $n!/(n+2)! < 1/(n+1)^2$. So $0 < N_n < 1$, contradicting Fact 1.1. □

Example 1.3. Evaluating $N_n = n!(e - S_n)$ numerically, for $n = 1, 2, 3, 5, 10$ one finds $N_n \approx 0.718,\ 0.437,\ 0.310,\ 0.194,\ 0.0991$, each below $1/n$, while the cleared partial sums $n!\,S_n$ are the integers $2, 5, 16, 326, 9864101$. The contradiction is visible in these numbers: if e were a/b, then for $n \ge b$ the number $n!\,e$ would be an integer, and so would N_n, which sits strictly between 0 and 1.

The balance sheet for e. The small quantity is the tail $T_n \approx 1/(n+1)!$, about $\log_2((n+1)!)$ bits below 1. The denominator that must be cleared is $n!$ (plus the fixed b), which costs $\log_2(n!)$ bits. The margin is $\log_2((n+1)!) - \log_2(n!) = \log_2(n+1) > 0$ bits, so smallness wins. For $n = 10$ the numbers are $\log_2(11!) \approx 25.250$ bits of smallness against $\log_2(10!) \approx 21.791$ bits of denominator, a margin of $\log_2 11 \approx 3.459$ bits. Non-vanishing came for free from positivity. These three entries (smallness, denominators, non-vanishing) are exactly the three entries of the note's balance sheet, in much harder form.

1.2 Linear forms and Apéry's idea

For e the approximations S_n came from the defining series for free. For a number such as $\zeta(3) = \sum_{m\ge 1} m^{-3}$ the obvious partial sums are useless: the tail $\sum_{m>n} m^{-3}$ is only of size about $1/(2n^2)$, while the denominator of $\sum_{m\le n} m^{-3}$ is about $\mathrm{lcm}(1, \ldots, n)^3$, which grows exponentially in n (see below). The cost overwhelms the gain.

The way out is to look for a sequence of *linear forms*

$$\ell_n = b_n\,\zeta(3) - a_n \ , \qquad b_n \in \mathbb{Z}, \quad a_n \in \mathbb{Q} \ ,$$

that are small compared with $1/D_n$, where D_n is a common denominator of the a_n, and with D_n under control. If $\zeta(3) = a/b$, then $D_n\,b\,\ell_n = D_n b_n a - D_n b a_n$ is an integer whenever $D_n a_n \in \mathbb{Z}$, and the three properties become: $D_n a_n \in \mathbb{Z}$, $\ell_n \neq 0$, and $D_n\,b\,|\ell_n| < 1$ for large n. Since b is fixed, the last one holds as soon as $D_n|\ell_n| \to 0$.

Fact 1.4 (Apéry's linear forms)**.** *Let*

$$b_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 , \qquad a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m-1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right) ,$$

and $d_n = \operatorname{lcm}(1, 2, \ldots, n)$*. Then* $2d_n^3 a_n \in \mathbb{Z}$*,* $\ell_n = b_n\zeta(3) - a_n$ *is nonzero, and* $|\ell_n|^{1/n} \to (\sqrt{2}-1)^4$ *as* $n \to \infty$*.*

This is Apéry's theorem [1]; the formulas above and a complete proof are in van der Poorten's exposition (A. van der Poorten, *A proof that Euler missed*, Math. Intelligencer 1 (1979), 195–203). We do not prove it; we only need the shape of the argument. The second ingredient is the growth of d_n: by the prime number theorem, $\log d_n = \sum_{p \le n} \lfloor \log_p n \rfloor \log p = n(1 + o(1))$, so $d_n^3 = e^{3n(1+o(1))}$ (this is a standard reformulation of the prime number theorem; the prime number theorem itself is stated in Chapter 7). Combining, if $\zeta(3) = a/b$ then $N_n = 2d_n^3\, b\, \ell_n$ is a nonzero integer with

$$|N_n|^{1/n} \to e^3(\sqrt{2}-1)^4 \approx 0.591 < 1 ,$$

so $|N_n| < 1$ for large n: a contradiction.

Example 1.5. Computing a_n and b_n from the double sums above in exact rational arithmetic, one finds $b_1 = 5$, $a_1 = 6$, $b_2 = 73$, $a_2 = 351/4$, $b_3 = 1445$, $a_3 = 62531/36$, $b_5 = 819005$, and $2d_n^3 a_n$ is indeed an integer for $n = 1, 2, 3, 5, 10, 20, 40$. The linear forms are $|\ell_n| \approx 1.03 \cdot 10^{-2}$, $1.12 \cdot 10^{-17}$, $1.76 \cdot 10^{-64}$ for $n = 1, 10, 40$, and the cleared quantity $2d_n^3|\ell_n|$ is about $2.1 \cdot 10^{-2}$, $3.6 \cdot 10^{-7}$, $5.4 \cdot 10^{-17}$ for the same n. The limit is $e^3/(1+\sqrt{2})^4 \approx 0.591263$; note that $(\sqrt{2}-1)^4 = 1/(1+\sqrt{2})^4$.

Intuition: where do such forms come from?. Apéry's numbers look like they fell from the sky, and historically the discovery was a surprise. Later explanations (Beukers' integrals, hypergeometric series, modular forms) show them as values of integrals or sums of rational functions, of the type $\sum_m R_n(m)$ with R_n a rational function having zeros and poles at carefully chosen places. The zeros make the sum small, the poles determine which zeta values appear and what the denominators are. The note's weight W [note, (1.2)] is a rational function of exactly this kind, with zeros of order 3 and poles of order 4; it is studied in Chapter 5.

1.3 Counting in bits, trits and nats

All the estimates in the note are statements about logarithms of sizes. The note writes log for the natural logarithm and uses $\log_2$ and $\log_3$ to "count bits and trits" [note, Section 1, Conventions]. A positive number x "has $\log_2 x$ bits": $x = 2^{\log_2 x}$, so $\log_2 x$ is how many times we can halve x before reaching 1. Likewise $\log_3 x$ counts *trits* (ternary digits), the number of factors of 3. The units convert by constant factors,

$$\log_2 x = \log_2 3 \cdot \log_3 x , \qquad \log_2 3 \approx 1.5849625 ,$$

so one trit is about 1.585 bits, and one nat ($\log x = 1$) is $1/\log 2 \approx 1.443$ bits.

Intuition: why trits. The power of 3 dividing a number is naturally counted in trits: a number divisible by 3^v "has v trits of 3-adic smallness". The size of a number and the primes $p \neq 3$ in its denominator are counted in bits by the note. To compare the two, the note multiplies the trits by $\log_2 3$, which is why $\log_2 3$ appears in the gain [note, (1.4)], [note, (3.6)]. Example: $3^{10} = 59049$ is 10 trits, and $\log_2 59049 \approx 15.8496 = 10 \log_2 3$ bits.

In the Apéry argument the natural unit of account is "bits per n": the linear form has about $-4\log_2(1+\sqrt{2}) \approx -5.086$ bits per n, and the denominator d_n^3 costs about $3\log_2 e \approx 4.328$ bits per n (at $n = 40$ the actual rates are -5.29 and 3.92, still on their way to the limits). The margin is about 0.76 bits per n. In the note the natural unit is *bits per* n^2. The reason is that the note does not work with one linear form but with a determinant of a $K \times K$ matrix with $K = \kappa n$, $\kappa \approx 3$, whose entries each carry about $10.5n$ trits of smallness. A determinant is a sum of products of K entries, so it carries about $10.5Kn = 10.5\kappa n^2$ trits (less a correction of order $\kappa^2 n^2$, Section 1.6). Correspondingly, all the main terms of the note's balance sheet are of order n^2 or $n^2 \log n$, and the margin is quoted as "4.58 bits per n^2" (Section 1.6).

1.4 The p-adic twist: small means divisible

The note does not prove that a real number is irrational. Its number $\zeta_3(5)$ lives in a different number system, the 3-adic numbers $\mathbb{Q}_3$, constructed in Chapter 2. Here is the idea in words.

There is a second, completely different way in which a rational number can be "small": it can be divisible by a high power of a prime. Write the 3-adic valuation $v_3(x)$ of a nonzero rational x for the exponent of 3 in it, so that $x = 3^{v_3(x)} \cdot (u/w)$ with integers u, w prime to 3. For example $v_3(54) = 3$ since $54 = 3^3 \cdot 2$; $v_3(2/9) = -2$; $v_3(12/45) = v_3(4/15) = -1$; $v_3(10!) = v_3(3628800) = 4$, from the factors $3, 6, 9$ of $10!$, which contribute $1 + 1 + 2$. The 3-adic absolute value is $|x|_3 = 3^{-v_3(x)}$, so that numbers divisible by many factors of 3 are 3-adically small. In $\mathbb{Q}_3$ the sequence $3, 9, 27, 81, \ldots$ tends to 0, and the series $\zeta_3(5)$ is defined by is a limit in this sense (Chapter 3).

The integer gap Fact 1.1 has a 3-adic version: a nonzero integer N divisible by 3^v satisfies $|N| \geq 3^v$, simply because $N = 3^v \cdot m$ with a nonzero integer m, and $|m| \geq 1$. So 3-adic smallness of an integer forces it to be *large* in the ordinary sense. This gives a new kind of contradiction: build from the assumption $\zeta_3(5) = a/b$ an integer $N \neq 0$ which is divisible by a huge power of 3, but whose ordinary size can be bounded above by something smaller than that power.

Example 1.6. Take $x = 3^{10}/7 = 59049/7$. It is large in absolute value, $|x| \approx 8436$, but 3-adically small, $|x|_3 = 3^{-10}$. Its 7-adic absolute value is $|x|_7 = 7^{+1} = 7$, since 7 divides the denominator once. The product of all its absolute values is

$$|x| \cdot |x|_3 \cdot |x|_7 = \frac{59049}{7} \cdot \frac{1}{59049} \cdot 7 = 1 \ ,$$

and $|x|_p = 1$ at all other primes. That this product is always 1 for a nonzero rational is the *product formula*, proved in Chapter 2. It says that a nonzero rational cannot be small at every place at once: 3-adic smallness ($|x|_3$ tiny) must be paid for by largeness in absolute value or by denominators at other primes ($|x|_p > 1$).

The note's criterion [note, Lemma 3.1, (3.2)] is exactly the product formula applied to the integer obtained by clearing the denominators of a polynomial value, written in logarithms and in bits:

$$\underbrace{v_3(\Delta_K(\zeta_3(5)))\log_2 3}_{\text{gain}} \ \leq \ \underbrace{\log_2 \|\Delta_K\|_1}_{\text{size}} + \underbrace{\sum_{p \neq 3} (-v_p(\Delta_K))^+ \log_2 p}_{\text{denominators}} + K \log_2 \max(|a|, b) \ . \qquad (1.1)$$

This is [note, (1.4)]. Here $\Delta_K(X)$ is a polynomial with rational coefficients (Section 1.5); $\|\Delta_K\|_1$ is the sum of the absolute values of its coefficients; $v_p(\Delta_K)$ is the smallest p-adic valuation of its coefficients, so $(-v_p(\Delta_K))^+ = \max(-v_p(\Delta_K), 0)$ is the exponent of the worst power of p in a denominator; and the last term accounts for the assumed fraction $\zeta_3(5) = a/b$. The

inequality holds whenever $\Delta_K(a/b) \neq 0$. Read as a balance sheet: the 3-adic smallness on the left (converted from trits to bits) cannot exceed what is spent on size and denominators on the right. The proof shows that, for large n, it does exceed it. The proof of (1.1) is given in Chapter 7.

Example 1.7 (the criterion at work on a rational number)**.** The criterion cannot be violated by a number that really is rational, and it is instructive to see how tight it is. In $\mathbb{Q}_3$ the integers $1, 4, 13, 40, 121, \ldots$, that is $c_m = 1 + 3 + \cdots + 3^{m-1} = (3^m - 1)/2$, converge to $-1/2$ (Chapter 2 explains why). Take $K = 1$ and the polynomial $F_m(X) = X - c_m$, and the true value $X = -1/2$, so $a = -1$, $b = 2$. Then $F_m(-1/2) = -3^m/2$, so the gain is $m \log_2 3$ bits; the size is $\log_2 \|F_m\|_1 = \log_2(1 + c_m)$; there are no denominators; and the last term is $K \log_2 \max(|a|, b) = 1$. Numerically:

m	gain	size	$K \log_2 \max(\lvert a\rvert, b)$	right side
1	1.585	1.000	1	2.000
3	4.755	3.807	1	4.807
6	9.510	8.512	1	9.512

The gain grows with m, but so does the size, at the same rate, and the inequality holds with a slack of about 0.002 bits at $m = 6$. A rational number can be approximated very well 3-adically, but only by polynomials with large coefficients. The note's strategy is to show that for $\zeta_3(5)$ the gain outruns size plus denominators, which by the criterion is impossible for a rational number with fixed a, b; the example only illustrates how the two sides keep pace when the number is rational.

Intuition: why the 3-adic world at all?. For a real number one needs smallness in absolute value, and the size of the numbers involved works against it. For a 3-adic number the roles are distributed differently: the 3-adic smallness (the gain) comes from the structure of the integral that defines $\zeta_3(5)$, essentially from the fact that every pole of the weight sits at 3-adic distance exactly 3 from every integration point [note, Section 4], while ordinary size enters only through the coefficients of Δ_K, which can be estimated by real analysis (an electrostatics problem, Chapter 10). The analogy with the real case stops here: there is no ordering or positivity in $\mathbb{Q}_3$, and this is why non-vanishing needs a separate argument (Section 1.7).

1.5 The Hankel-determinant variant

The note replaces Apéry's single linear form by a determinant. It defines ([note, (1.2)], [note, (1.3)]) for an odd integer n the rational function

$$W(y) = \frac{(y + \frac{n}{2})\left(y + \frac{1}{3}\right)_n^3 \left(y + \frac{2}{3}\right)_n^3}{\prod_{k=-n}^{2n} (y + k)^4}\,, \qquad (x)_n = x(x+1)\cdots(x+n-1)\,,$$

and the linear functional $L(P) = \sum_{r=1,2} \int_{\mathbb{Z}_3} (PW)'(t + \frac{r}{3})\, \mathrm{d}t$ on polynomials P, where $\int_{\mathbb{Z}_3}$ is the Volkenborn integral (Chapter 4). The weight W has poles of order 4 at the $3n + 1$ integers $-2n, \ldots, n$ and zeros of order 3 at the points $-(j + \frac{r}{3})$. Its role is that of the rational function R_n of the previous section, and the note shows [note, Lemma 2.19] that every value $L(P)$ with $\deg P \leq 6n+1$ lies in $\mathbb{Q} + \mathbb{Q}\,\zeta_3(5)$: it is a linear form $\beta(P) + \alpha(P)\zeta_3(5)$ with rational $\alpha(P), \beta(P)$ (Chapter 5).

So there are now many linear forms, one for each polynomial, and the note arranges the ones for $P = y^m$ (the *moments*) into a Hankel matrix $[L(y^{i+j})]_{0 \leq i,j < K}$. Every entry is affine

in $\zeta_3(5)$, so the determinant is the value at $X = \zeta_3(5)$ of a polynomial

$$\Delta_K(X) = \det\left[\beta(y^{i+j}) + X\,\alpha(y^{i+j})\right]_{0\le i,j<K} \in \mathbb{Q}[X]\ , \qquad \deg \Delta_K \le K\ ,$$

the *Hankel polynomial* [note, Definition 2.23], [note, (2.26)] (Chapter 6). For a physicist: if L were integration against a positive measure on $\mathbb{R}$, this determinant would be (up to $1/K!$) the partition function of K charges with logarithmic repulsion in an external potential, by Heine's formula; this picture is what controls the size estimate (Chapter 9, Chapter 10). The point of the determinant is that it multiplies the smallness of the entries: if each entry is divisible by about $3^{10.5n}$, the determinant is divisible by about $3^{10.5nK}$, a power of 3 quadratic in n.

Example 1.8. Three small computations show what a determinant does. (i) The symmetric matrix $\left(\begin{smallmatrix} 9 & 18 \\ 18 & 45 \end{smallmatrix}\right)$ has entries divisible by 3^2; its determinant is $81 = 3^4$: two rows, two trits each, four trits in total. In general a $K \times K$ determinant with all entries divisible by 3^v is divisible by 3^{Kv}, since each term of the Leibniz expansion is a product of K entries. (ii) For the positive measure $\mathrm{d}x$ on $[0,1]$ the moments are $\int_0^1 x^{i+j}\mathrm{d}x = 1/(i+j+1)$, and the Hankel determinants for $K = 1, 2, 3, 4$ are 1, 1/12, 1/2160, 1/6048000: all positive, as positivity predicts, and rapidly decreasing. (iii) If the entries are affine in an unknown X, the determinant is a polynomial in X; for instance $\det\left(\begin{smallmatrix} 1+X & \frac{1}{2}-X \\ \frac{1}{2}-X & \frac{1}{3}+2X \end{smallmatrix}\right) = X^2 + \frac{10}{3}X + \frac{1}{12}$, of degree $2 = K$. This is how $\Delta_K(X)$ arises.

The method is not new with this note. The introduction says [note, Section 1, The method] that it adapts to $p = 3$ the method that the preprint [19] applies to $\zeta_2(7)$, which in turn transfers to $\mathbb{Q}_2$ the Hankel-determinant approach of Fauzan's preprint on $\zeta(5)$ [15].

1.6 The balance sheet of the note

The note fixes $K = \kappa n$ with κ in the range $[2.8, 3]$ (why this range, see Section 1.7) and estimates the three terms of (1.1) separately. Up to terms of lower order in n, its four estimates [note, Theorems 3.5, 3.8, 3.10, 3.13] say the following.

- **Gain** [note, Theorem 3.5]: $v_3(\Delta_K(\zeta_3(5)))\log_2 3 \ge G(\kappa)n^2 - O(n\log n)$ with $G(\kappa) = (10.5\,\kappa - \frac{\kappa^2}{4})\log_2 3$. The term 10.5κ is "K rows times about $10.5n$ trits per entry": the note shows [note, (4.8)] that every relevant entry is divisible by about 3^{A_3} with $A_3 = 9n+3+3v_3(n!)$, and $A_3 = 51,\ 114,\ 1056,\ 10506$ for $n = 5, 11, 101, 1001$, so $A_3/n = 10.20,\ 10.36,\ 10.46,\ 10.50$, approaching 10.5; the term $-\kappa^2/4$ is a loss from rewriting the determinant in a basis adapted to the integration points (Chapter 8).
- **Size** [note, Theorem 3.8]: $\log_2 \|\Delta_K\|_1 \le (\kappa^2 - 6\kappa)n^2\log_2 n + F^\dagger n^2 + O(n\log n)$.
- **Denominators** [note, Theorem 3.10]: $\sum_{p\ne 3}(-v_p(\Delta_K))^+\log_2 p \le \kappa(6-\kappa)n^2\log_2 n + c\,n^2 + o(n^2)$.
- **Non-vanishing** [note, Theorem 3.13]: for suitable K in this range, $\Delta_K(a/b) \ne 0$.

The cancelling $n^2\log n$ terms. The size and the denominators have main terms of order $n^2\log_2 n$, which is much larger than the gain, of order n^2. If these terms did not cancel, the argument would be hopeless. They do cancel, exactly: $(\kappa^2 - 6\kappa) + \kappa(6-\kappa) = 0$. The note explains why [note, Section 3, after Theorem 3.5]: both estimates measure the same products, $\prod_k h_k^{s_k}\prod_{k\ne m}(k-m)^{s_k s_m}$, of leading coefficients h_k of W at the poles and of differences of poles, once with the ordinary absolute value and once with the p-adic valuations for $p \ne 3$; and by the product formula (Example 1.6) these two measurements agree up to the 3-adic part and terms of order n^2. Concretely, the coefficients of Δ_K are *tiny* (the coefficient $(\kappa^2 - 6\kappa)$ is negative for $\kappa < 6$; the note attributes the $-6\kappa n^2\log n$ to $|h_k| \approx n^{-6n}$ [note, Section 5.1, after Theorem 5.7]) but have *huge denominators*, and the two effects are mirror images of each other.

To see what is at stake, at $\kappa = 2.8$ the coefficient is $\kappa(6-\kappa) = 8.96$, and the two main terms are $\pm 8.96 \log_2 n$ bits per n^2, that is ± 89.29 bits per n^2 at $n = 10^3$ and ± 178.59 at $n = 10^6$, against a final margin of 4.58. An error of a few percent in either main term would destroy the argument; it is the exact cancellation that makes it work. What survives are the constants of order n^2: $F^\dagger$ (size) and c (denominators), both depending on κ.

The margin. After the cancellation, (1.1) becomes

$$G(\kappa)\, n^2 \le \Big(F^\dagger + c\Big)\, n^2 + o(n^2) + K \log_2 \max(|a|, b) \ ,$$

and the last term is $O(n)$ because a and b are fixed while $K \le 3n$. So everything hinges on the sign of $G(\kappa) - F^\dagger - c$. The note computes upper bounds for $F^\dagger$ and c on five intervals I_i covering $[2.8, 3]$ [note, (3.7)] and reports them in its [note, Table 1], reproduced here as Table 1.1.

I_i	$G(\kappa_{1,i})$	$F_i^\dagger$	c_i	$G(\kappa_{1,i}) - F_i^\dagger - c_i$
$[2.80, 2.84]$	43.49	8.43	30.48	4.58
$[2.84, 2.88]$	44.06	8.46	30.79	4.81
$[2.88, 2.92]$	44.64	8.52	31.10	5.02
$[2.92, 2.96]$	45.21	8.58	31.41	5.22
$[2.96, 3.00]$	45.78	8.65	31.72	5.41

Table 1.1: The note's [note, Table 1], in bits per n^2; $\kappa_{1,i}$ is the left end of I_i. The column G follows from the formula for $G(\kappa)$ and the last column from the printed values (see text); $F_i^\dagger$ and c_i are the note's computer-assisted bounds.

Evaluating $G(\kappa_{1,i}) = (10.5\kappa_{1,i} - \kappa_{1,i}^2/4) \log_2 3$ directly: for $\kappa_{1,1} = 2.80$ one gets $(29.4 - 1.96) \cdot 1.5849625\ldots = 43.491371\ldots$, and for the five intervals 43.4914, 44.0677, 44.6427, 45.2164, 45.7889, which rounded down to two decimals are the note's values. Subtracting the printed values of $F_i^\dagger$ and c_i gives the last column, 4.58, 4.81, 5.02, 5.22, 5.41, as in the note. This is only the arithmetic of the table; the bounds $F_i^\dagger$ [note, Proposition 5.11] and c_i [note, Proposition 5.40] come from the note's own computations [note, Appendix E] and are discussed in Chapter 10 and Chapter 13.

So, by the note's bounds, the gain exceeds size plus denominators by at least 4.58 bits per n^2 on the whole range of κ. Since $4.58\, n^2$ eventually beats any $o(n^2)$, the inequality fails for large n: that is the contradiction [note, (3.14)]. Note how thin the margin is in relative terms: the gain is about 43 to 46 bits per n^2, and about 90% of it is consumed by $F^\dagger + c$. The note itself notes [note, Section 1, What is new] that with a cruder local bound in place of its [note, Lemma 5.24], a numerical evaluation at $\kappa = 3$ no longer leads to a contradiction [note, Remark 5.27]. The constant c (about 30 to 32 bits) is the largest cost, and its accuracy matters most.

1.7 Non-vanishing and the choice of K

Inequality (1.1) is worthless if $\Delta_K(a/b) = 0$: then there is no nonzero integer to apply Fact 1.1 to. For the Hankel determinant of a positive measure on $\mathbb{R}$ with infinite support, non-vanishing is automatic: the Hankel matrix is a Gram matrix $[\langle y^i, y^j \rangle]$ of linearly independent vectors, hence positive definite, with positive determinant (Chapter 6). But L is a 3-adic functional; there is no positivity in $\mathbb{Q}_3$, and the note notes that no such argument is available [note, Section 1].

The note's substitute [note, Lemma 3.4] is a divisibility argument at an auxiliary prime p. Suppose that in $\Delta_K(X) = \sum_j f_j X^j$ the constant coefficient f_0 is divisible by a strictly lower

power of p than every other coefficient. Then for a/b with $p \nmid b$ every term $f_j(a/b)^j$ with $j \geq 1$ is divisible by a higher power of p than f_0, so they cannot cancel f_0, and $\Delta_K(a/b) \neq 0$. A toy example: $F(X) = 1 + 5X + 25X^2$ and $p = 5$; for $5 \nmid b$ the number $b^2F(a/b) = b^2 + 5ab + 25a^2$ is congruent to $b^2 \not\equiv 0$ modulo 5, so it is not zero. For $a/b = 1/1,\ 3/2,\ -7/3,\ 10/7$ the numbers $b^2F(a/b)$ are $31, 259, 1129, 2899$, with residues $1, 4, 4, 4$ modulo 5; for $a/b = 2/5$, where $5 \mid b$, one gets $175 \equiv 0$, and the argument says nothing (here $F(2/5) = 7 \neq 0$ anyway). Since the note does not know b, it uses that the interval $[2.1n + 2,\ 2.159n]$ contains $(0.059 + o(1))\, n/\log n$ primes by the prime number theorem [note, proof of Theorem 1.1], so for large n at least one of them does not divide b. For $n = 1001,\ 10001,\ 100001$ the window contains 9, 63, 472 primes, compared with $0.059\, n/\log n \approx 8.5,\ 64.1,\ 512.5$; the smallest primes in the windows are $p = 2111,\ 21011,\ 210011$, all $\equiv 2 \pmod 3$, and [note, (3.12)] gives $K = 10n - (10p - 14)/3 = 2978,\ 29978,\ 299978$, so $\kappa = K/n \approx 2.975,\ 2.9975,\ 2.9998$. The choice of p then fixes $K = K(n, p)$ [note, (3.12)]: the lower limit $2.1n + 2$ guarantees $K \leq 3n - 2$, and the upper limit $2.159n$ guarantees $K > 2.8n$ [note, Theorem 3.13]. This is why the balance sheet only needs to work on $\kappa \in [2.8, 3]$. Proving the dominance of f_0 is the content of [note, Section 6] and Chapter 14; it rests, among other things, on Wilson's theorem.

1.8 A map of the proof

Figure 1.1 shows the whole proof, with the chapters of this companion and the sections of the note. The arrows mean "is used by".

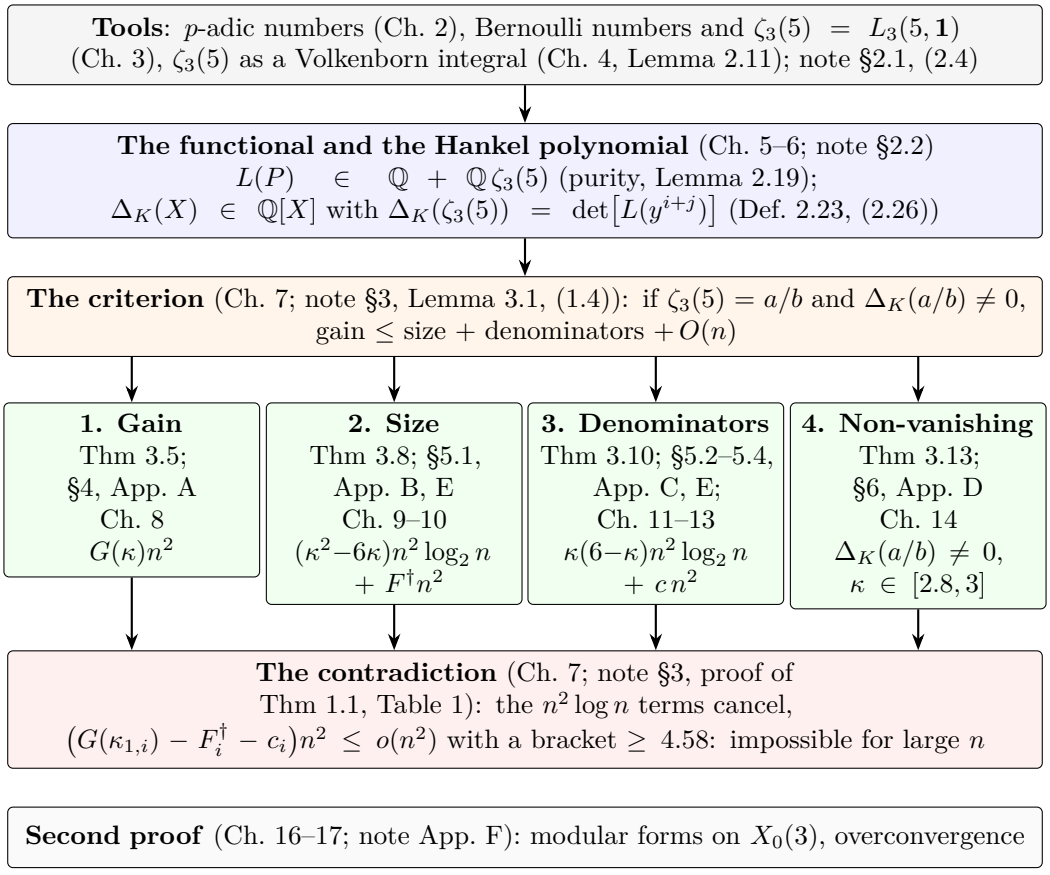


Figure 1.1: The structure of the proof of [note, Theorem 1.1]. Chapter numbers refer to this companion, section, lemma and theorem numbers to the note. The criterion supplies the inequality, the four estimates fill in its terms, and Table 1 closes the argument. The second proof shares only the statement and the normalization [note, (2.4)] with the first.

The order of these notes follows the figure from top to bottom. Part I (Chapters 1 to 4) builds the tools and writes $\zeta_3(5)$ as an integral. Part II (Chapters 5 and 6) builds the functional and the Hankel polynomial. Part III (Chapter 7) states the criterion and the four estimates and assembles the proof. Part IV explains the note's proofs of the four estimates, and Chapter 15 summarizes the whole argument. Part V explains the second proof of [note, Appendix F], which uses neither the Volkenborn functional nor any of the four estimates.

1.9 History and status

This section reports only what the note's introduction [note, Section 1] says; we have not independently surveyed the literature.

Apéry proved that $\zeta(3)$ is irrational [1], and Ball and Rivoal proved that infinitely many of the numbers $\zeta(3), \zeta(5), \zeta(7), \dots$ are irrational [3]. Both results have p-adic counterparts, for the p-adic zeta values $\zeta_p(s) = L_p(s, \omega^{1-s})$ (Chapter 3). Calegari proved that $\zeta_2(3)$ and $\zeta_3(3)$ are irrational, using overconvergent p-adic modular forms [7], and Beukers gave another proof [4]. The irrationality of $\zeta_2(5)$ was proved by Calegari, Dimitrov and Tang [9], with the arithmetic holonomy bounds of [8], and Lai, Sprang and Zudilin gave a second proof [25]. Other results concern several values at once: Lai proved that at least one of $\zeta_2(7), \zeta_2(9), \zeta_2(11), \zeta_2(13)$ is irrational [22]; Lai and Sprang proved that, for every prime p and every $\epsilon > 0$, at least $(c_p - \epsilon)\sqrt{s/\log s}$ of the values $\zeta_p(3), \zeta_p(5), \dots, \zeta_p(s)$ are irrational once the odd integer s is large enough, with an explicit constant $c_p > 0$ [24]; and Lai, Lupu and Sprang proved that for every prime $p \geq 5$ some $\zeta_p(i)$ with odd $i \in [3,\, p + p/\log p + 5]$ is irrational [23]. The note states that at $p = 3$ these results give the irrationality of $\zeta_3(3)$ and of unspecified values among $\zeta_3(3), \dots, \zeta_3(s)$ for large s.

The irrationality of $\zeta_3(5)$ was claimed before the note. Two manuscripts of Long [26, 27] (GitHub, August 2026) state the irrationality of twenty-two p-adic zeta values, among them $\zeta_3(s)$ for $s = 3, 5, 7, 9, 11$, and the note's proof uses a different method. Other preprints with claims from August and September 2026 named by the note are [19] for $\zeta_2(7)$, [21] for $\zeta_5(3)$ and [35] for $\zeta_7(3)$. Two of these are the note's sources of method: the main proof adapts [19] (which builds on Fauzan's preprint [15] on $\zeta(5)$), and the second proof adapts [35]. The note gives its own proofs of the statements it takes from [19] [note, Appendices A–C]. According to the note, three steps do not carry over from $p = 2$: the change of basis in the 3-adic estimate [note, Lemma 4.1], the refined local estimate at primes of the order of n [note, Lemma 5.24], and the non-vanishing theorem [note, Section 6], which uses Wilson's theorem [note, Lemma 6.10]. Kilani, the author of [19], also states the irrationality of $\zeta_3(5)$, in a preprint posted on 7 October 2026 [20]. The preprint applies the Hankel-determinant method of [19] to a rational function that has poles of order 4 at the integers of an interval symmetric about 0 and no zeros, and its non-vanishing argument uses an auxiliary prime just above the right end of that interval. The preprint states that its proof is formalized in Lean 4, apart from the identification of the Volkenborn integral with the Kubota–Leopoldt value.

The note's proof has not been refereed and has not been checked by an expert.

Summary of the chapter

An irrationality proof manufactures, from the assumption that the number is a/b, a quantity that must be a nonzero integer and yet is too small to be one. For e the bookkeeping is a single line; for $\zeta(3)$ Apéry's linear forms win by about 0.76 bits per n against the denominators d_n^3. The note works 3-adically: it assumes $\zeta_3(5) = a/b$, takes the Hankel polynomial $\Delta_K(X)$ built from a functional whose values are linear forms in $\zeta_3(5)$, and compares, through the criterion (1.1) [note, (1.4), Lemma 3.1], the 3-adic gain $G(\kappa)n^2$ with the size and the denominators of Δ_K.

The $n^2 \log n$ terms of the last two cancel by a product-formula mechanism, and [note, Table 1] leaves a margin of at least 4.58 bits per n^2 for $\kappa \in [2.8, 3]$, a range forced by the non-vanishing argument at an auxiliary prime.

Carried forward: the criterion (1.1) and the four estimates (made precise and proved or explained in Chapter 7 and Part IV), the units bits/trits with $\log_2 3 \approx 1.585$, the informal meaning of "3-adically small" (made precise in Chapter 2), and the map Figure 1.1.

Chapter 2

p-adic numbers

Where we are. This chapter builds the number system in which $\zeta_3(5)$ lives and collects the p-adic facts that the note uses without comment. It covers the note's [note, Section 1, Conventions] (the valuation v_p, the Gauss valuation of polynomials), the set of integration points S [note, (2.8)], the observation that opens [note, Section 4] (every node is at 3-adic distance exactly 3 from every point of S), Legendre's formula as used in [note, (4.4)] and in the proof of [note, Theorem 3.5], and the product formula behind the criterion [note, Lemma 3.1] and the second proof [note, Appendix F]. It also keeps two promises of Chapter 1: it proves the product formula (Theorem 2.8) and explains why $1, 4, 13, 40, \ldots$ tends to $-\frac{1}{2}$ (Example 2.18). It needs nothing beyond the informal remarks of Chapter 1. All numbers in the examples are computed in exact rational arithmetic.

For more than these notes contain, three textbooks are recommended: N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Ch. I (the most elementary); F. Q. Gouvêa, *p-adic Numbers: An Introduction* (very gentle, with many examples); and Robert [28] (more advanced, and the reference the note uses for the Volkenborn integral).

2.1 Valuations and absolute values on $\mathbb{Q}$

Chapter 1 used the phrase "divisible by a high power of 3" as a kind of smallness. To make limits, series and integrals out of it we need a distance function, and a distance function needs a size. The size is built from the exponent of p in a rational number.

Definition 2.1 (p-adic valuation)**.** Let p be a prime. Every nonzero rational x can be written as $x = p^v \frac{u}{w}$ with integers v, u, w, where $w > 0$ and p divides neither u nor w. The exponent v is the *p-adic valuation* $v_p(x)$. We put $v_p(0) = +\infty$.

The exponent is well defined: by unique factorization the power of p in the numerator and in the denominator of x (in lowest terms) is determined by x, and $v_p(x)$ is the first minus the second.

Definition 2.2 (p-adic absolute value)**.** $|x|_p = p^{-v_p(x)}$ for $x \neq 0$, and $|0|_p = 0$. We write $|x|$ or $|x|_\infty$ for the ordinary absolute value.

Intuition: divisible means small. $|x|_p$ is small when x contains many factors of p in the numerator, and large when it contains many in the denominator. So 3^{10} is a tiny number 3-adically, $|3^{10}|_3 = 3^{-10}$, and $\frac{1}{9}$ is a large one, $|\frac{1}{9}|_3 = 9$. Primes other than p are invisible to $|\cdot|_p$: $|2|_3 = |\frac{5}{7}|_3 = 1$. The valuation $v_p(x) = -\log_p |x|_p$ counts "how many p-adic digits of smallness" x has, the trits of Chapter 1 when $p = 3$.

Example 2.3. Here are some valuations.

x	factorization	v_2	v_3	v_5	v_7	$\lvert x\rvert_3$
54	$2 \cdot 3^3$	1	3	0	0	$1/27$
$2/9$	$2 \cdot 3^{-2}$	1	-2	0	0	9
$12/45 = 4/15$	$2^2 \cdot 3^{-1} \cdot 5^{-1}$	2	-1	-1	0	3
$10! = 3628800$	$2^8 \cdot 3^4 \cdot 5^2 \cdot 7$	8	4	2	1	$1/81$
$59049/7$	$3^{10} \cdot 7^{-1}$	0	10	0	-1	$1/59049$
$-1/2$	-2^{-1}	-1	0	0	0	1
$2/3$	$2 \cdot 3^{-1}$	1	-1	0	0	3
$-7/18$	$-7 \cdot 2^{-1} \cdot 3^{-2}$	-1	-2	0	1	9

Note that $|x|_3$ ignores the sign and every prime other than 3.

Lemma 2.4 (properties of v_p and $|\cdot|_p$)**.** *For all rationals x, y:*

1. $v_p(xy) = v_p(x) + v_p(y)$, *equivalently* $|xy|_p = |x|_p\,|y|_p$;
2. $v_p(x+y) \geq \min(v_p(x), v_p(y))$, *equivalently* $|x+y|_p \leq \max(|x|_p, |y|_p)$ *(the* ultrametric inequality*);*
3. *if* $v_p(x) \neq v_p(y)$, *then* $v_p(x+y) = \min(v_p(x), v_p(y))$, *equivalently* $|x+y|_p = \max(|x|_p, |y|_p)$.

Proof. If x or y is 0 everything is immediate (with $\infty + a = \infty$ and $\min(a, \infty) = a$), so let both be nonzero, $x = p^a \frac{u}{w}$ and $y = p^b \frac{u'}{w'}$ with $p \nmid uwu'w'$.

(1) $xy = p^{a+b} \frac{uu'}{ww'}$, and p divides neither uu' nor ww' because p is prime (if a prime divides a product, it divides a factor). So $v_p(xy) = a + b$.

(2) We may assume $a \leq b$. Then

$$x + y = p^a \, \frac{uw' + p^{b-a}u'w}{ww'} \ .$$

The numerator $uw' + p^{b-a}u'w$ is an integer (because $b - a \geq 0$) and the denominator ww' is prime to p. Pulling out any further factors of p from the numerator can only raise the exponent, so $v_p(x+y) \geq a = \min(a, b)$. (If the numerator is 0, then $x + y = 0$ and $v_p = \infty$.)

(3) If $a < b$, then $p^{b-a}u'w$ is divisible by p while uw' is not, so the numerator is not divisible by p, and $v_p(x+y) = a$ exactly. □

The ultrametric inequality is much stronger than the usual triangle inequality $|x+y| \leq |x| + |y|$: the size of a sum never exceeds the larger summand. The distance between x and y is $|x-y|_p$, and Lemma 2.4(3) has a surprising geometric consequence.

Corollary 2.5 (every triangle is isosceles)**.** *For any three rationals x, y, z, the two largest of the three distances $|x-y|_p$, $|y-z|_p$, $|x-z|_p$ are equal.*

Proof. $x - z = (x - y) + (y - z)$. If $|x-y|_p \neq |y-z|_p$, part (3) of the lemma gives $|x-z|_p = \max(|x-y|_p, |y-z|_p)$, so the two largest sides are equal. If $|x-y|_p = |y-z|_p$, these two are equal, and by part (2) the third is at most as large; so again the two largest are equal. □

Example 2.6 (an isosceles triangle)**.** Take the three integers $1, 4, 10$. Their 3-adic distances are $|1-4|_3 = |-3|_3 = \frac{1}{3}$, $|4-10|_3 = |-6|_3 = \frac{1}{3}$ and $|1-10|_3 = |-9|_3 = \frac{1}{9}$: two long sides of length $\frac{1}{3}$ and one short side of length $\frac{1}{9}$. Another triangle, with fractions: $\frac{1}{2}, \frac{5}{2}, -\frac{7}{4}$ have distances $|\frac{1}{2} - \frac{5}{2}|_3 = 1$, $|\frac{5}{2} + \frac{7}{4}|_3 = |\frac{17}{4}|_3 = 1$ and $|\frac{1}{2} + \frac{7}{4}|_3 = |\frac{9}{4}|_3 = \frac{1}{9}$.

Intuition: a hierarchical distance. In the real line, a point can be close to one of two points and far from the other in any proportion. In the 3-adic world, distances come in the discrete steps $\dots, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, \dots$, and two numbers are close when they agree in many trailing ternary digits (Section 2.3). Such a distance is organized like a family tree: two numbers are at distance 3^{-j} when their "last common ancestor" sits j generations down. A physicist has seen this geometry in the mean-field spin glass, where the overlaps between pure states are ultrametric (R. Rammal, G. Toulouse, M. A. Virasoro, *Ultrametricity for physicists*, Rev. Mod. Phys. 58 (1986) 765); the analogy is only in the geometry of the distance.

Remark 2.7. By Ostrowski's theorem, every absolute value on $\mathbb{Q}$ that is not trivial is a power of $|\cdot|_\infty$ or of one of the $|\cdot|_p$ (Koblitz, Ch. I; Gouvêa). So the p-adic absolute values are not one arbitrary choice among many: together with the ordinary one, they are all the ways of measuring the size of a rational number. The ordinary absolute value is called the *place at infinity*, the $|\cdot|_p$ the *finite places*.

2.2 The product formula

Since a nonzero rational is determined, up to sign, by its prime factorization, the sizes of x at all places cannot be independent of each other. The precise relation is the product formula, which Chapter 1 used for $x = 59049/7$ and which is the engine of the note's criterion.

Theorem 2.8 (product formula)**.** *For every nonzero rational x,*

$$|x|_\infty \prod_p |x|_p = 1 \ , \qquad \textit{equivalently} \qquad \log|x| = \sum_p v_p(x) \log p \ , \tag{2.1}$$

where p runs over all primes. Only finitely many factors differ from 1*.*

Proof. By unique factorization, $x = \pm \prod_p p^{v_p(x)}$, where $v_p(x)$ is the exponent of p (positive for primes in the numerator, negative for primes in the denominator, zero for all but finitely many primes). Taking the ordinary absolute value, $|x|_\infty = \prod_p p^{v_p(x)}$. On the other hand $|x|_p = p^{-v_p(x)}$, so $\prod_p |x|_p = \prod_p p^{-v_p(x)}$, which is exactly $1/|x|_\infty$. Taking log of $|x|_\infty = \prod_p p^{v_p(x)}$ gives the second form. □

Example 2.9. For each x below, multiplying $|x|_\infty$ with $|x|_p$ for every prime p dividing the numerator or the denominator, in exact arithmetic, gives 1:

x	$\lvert x\rvert_\infty$	the factors $\lvert x\rvert_p \neq 1$
$59049/7$	$59049/7$	$\lvert x\rvert_3 = 1/59049$, $\lvert x\rvert_7 = 7$
$-4/15$	$4/15$	$\lvert x\rvert_2 = 1/4$, $\lvert x\rvert_3 = 3$, $\lvert x\rvert_5 = 5$
$10! = 3628800$	3628800	$\lvert x\rvert_2 = 1/256$, $\lvert x\rvert_3 = 1/81$, $\lvert x\rvert_5 = 1/25$, $\lvert x\rvert_7 = 1/7$
$1000/27$	$1000/27$	$\lvert x\rvert_2 = 1/8$, $\lvert x\rvert_3 = 27$, $\lvert x\rvert_5 = 1/125$
$-7/18$	$7/18$	$\lvert x\rvert_2 = 2$, $\lvert x\rvert_3 = 9$, $\lvert x\rvert_7 = 1/7$

For 10!, for instance, $3628800 \cdot \frac{1}{256} \cdot \frac{1}{81} \cdot \frac{1}{25} \cdot \frac{1}{7} = 1$ because $256 \cdot 81 \cdot 25 \cdot 7 = 3628800$.

Intuition: a conservation law. Write (2.1) as $\log|x|_\infty + \sum_p \log|x|_p = 0$: the logarithmic sizes of x at all places add up to zero, like charges of a neutral system. A rational number cannot be small everywhere. If it is very small at 3 (many factors of 3 in the numerator), it must be correspondingly large somewhere else: in ordinary size, or through primes in its

denominator. The physics analogy stops at bookkeeping: nothing dynamical is conserved, the formula is unique factorization in disguise.

Corollary 2.10 (3-adic integer gap)**.** *If N is a nonzero integer, then $|N| \geq 3^{v_3(N)}$, that is, $v_3(N)\log_2 3 \leq \log_2 |N|$.*

Proof. By (2.1), $|N| = \prod_p p^{v_p(N)}$, and every factor is at least 1 because $v_p(N) \geq 0$ for an integer. Dropping all factors except $p = 3$ gives $|N| \geq 3^{v_3(N)}$. □

For example $|54| = 54 \geq 3^{v_3(54)} = 27$ (Example 2.3). This is the form of the integer gap $|N| \geq 1$ of Chapter 1 that the note uses: the criterion [note, Lemma 3.1] applies Corollary 2.10 to the integer obtained by clearing the denominators of $\Delta_K(a/b)$, and the terms on its right-hand side [note, (1.4)] are the factors p^{v_p} that Δ_K has at the other places. The proof of the criterion is given in Chapter 7. In the second proof [note, Appendix F, The plan] the product formula is used in the logarithmic form $\log|\mathcal{D}_d| = v_3(\mathcal{D}_d)\log 3 + \sum_{\ell\neq 3} v_\ell(\mathcal{D}_d)\log\ell$, the second form of (2.1) with the prime 3 written separately (Chapter 17).

2.3 Completing $\mathbb{Q}$: the p-adic numbers

2.3.1 Why complete, and how

In the ordinary absolute value, the rationals 1, 1.4, 1.41, 1.414, ... get closer and closer to each other without approaching any rational number; the real numbers $\mathbb{R}$ are constructed precisely so that such sequences have limits. The same happens for $|\cdot|_p$, and the p-adic numbers are the result of the same construction with the other distance.

Definition 2.11 ($\mathbb{Q}_p$)**.** A sequence (x_m) of rationals is *p-adically Cauchy* if $|x_m - x_{m'}|_p \to 0$ as $m, m' \to \infty$. Two Cauchy sequences are equivalent if their difference tends to 0. The field $\mathbb{Q}_p$ of *p-adic numbers* is the set of equivalence classes, with termwise addition and multiplication. The rational x is identified with the class of the constant sequence $x, x, x, \ldots$. The absolute value extends by $|\lim x_m|_p = \lim |x_m|_p$ (this limit exists, and is eventually constant when the limit is nonzero), and $v_p = -\log_p|\cdot|_p$.

That $\mathbb{Q}_p$ is a field, that $|\cdot|_p$ on it still satisfies Lemma 2.4 and Corollary 2.5 (by continuity), and that every Cauchy sequence in $\mathbb{Q}_p$ converges in $\mathbb{Q}_p$ (completeness) are proved in Koblitz, Ch. I, Gouvêa's book, and Robert [28]. Note that v_p still takes only integer values on $\mathbb{Q}_p^\times$: a sequence of rationals converging to a nonzero limit has eventually constant absolute value, by the isosceles property.

Definition 2.12 (p-adic integers)**.** $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \ |x|_p \leq 1\} = \{x : \ v_p(x) \geq 0\}$.

By Lemma 2.4, $\mathbb{Z}_p$ is closed under addition, subtraction and multiplication, so it is a ring. It contains $\mathbb{Z}$, and more generally every rational u/w with $p \nmid w$, since then $v_p(u/w) = v_p(u) \geq 0$. For example $\frac{1}{2}, -\frac{1}{2}, \frac{1}{4}, \frac{5}{7} \in \mathbb{Z}_3$, while $\frac{2}{3}, \frac{1}{9} \notin \mathbb{Z}_3$.

2.3.2 Digit expansions

A concrete description of $\mathbb{Q}_p$ is by digits, like decimal expansions of real numbers, except that the infinite direction is to the *left*.

Theorem 2.13 (p-adic expansion)**.** *Every $x \in \mathbb{Q}_p$, $x \neq 0$, has a unique expansion*

$$x = \sum_{k \geq v} a_k p^k \ , \qquad a_k \in \{0, 1, \ldots, p-1\} \ , \quad a_v \neq 0 \ , \tag{2.2}$$

where $v = v_p(x)$ and the series converges in $\mathbb{Q}_p$. Conversely, every such series converges and defines an element of $\mathbb{Q}_p$. We write it as $\dots a_2a_1a_0$ when $v \geq 0$, and with a "p-adic point" as in $\dots a_1a_0.a_{-1}$ when $v = -1$. In particular $\mathbb{Z}_p$ consists exactly of the expansions with no digits after the point.

The convergence part is Proposition 2.22 below; for existence and uniqueness see Koblitz, Ch. I. For rationals with denominator prime to p the digits are produced by a simple algorithm, which we prove because it is how all the digit expansions in these notes are computed.

Proposition 2.14 (digit algorithm)**.** *Let $x_0 = x = u/w$ with $p \nmid w$. Define recursively $a_i \in \{0, \dots, p-1\}$ as the residue of $u_i w^{-1}$ modulo p, where $x_i = u_i/w$, and $x_{i+1} = (x_i - a_i)/p$. Then every x_i has denominator dividing w, and for every N*

$$x = a_0 + a_1 p + \cdots + a_{N-1}p^{N-1} + p^N x_N \ , \qquad \Big| x - \sum_{i<N} a_i p^i \Big|_p \leq p^{-N} \ . \tag{2.3}$$

So $a_0, a_1, \dots$ are the p-adic digits of x.

Proof. Here w^{-1} means an integer w' with $ww' \equiv 1 \pmod p$; it exists because $p \nmid w$ (Section 2.6). With $a_i \equiv u_i w'$ we get $u_i - a_i w \equiv u_i - u_i w' w \equiv 0 \pmod p$, so $x_i - a_i = (u_i - a_i w)/w$ has numerator divisible by p, and $x_{i+1} = \frac{(u_i - a_i w)/p}{w}$ again has denominator w. The identity in (2.3) follows by induction from $x_i = a_i + p\, x_{i+1}$. Since x_N has denominator prime to p, $|x_N|_p \leq 1$, hence $|p^N x_N|_p \leq p^{-N}$. □

Intuition: close means same last digits. By (2.3), x and its truncation $\sum_{i<N} a_i p^i$ agree in the last N digits and differ by at most p^{-N}. More generally, two elements of $\mathbb{Z}_p$ are at distance at most p^{-N} exactly when they agree in their last N digits, that is, when they are congruent modulo p^N. Ordinary decimals are close when they agree in their *first* digits; p-adic numbers when they agree in their *last* ones.

Example 2.15 (the digits of $\frac{1}{4}$, step by step)**.** Take $p = 3$, $x = \frac{1}{4}$. Since $4 \equiv 1 \pmod 3$, the inverse of 4 modulo 3 is 1. The algorithm runs as follows:

i	x_i	digit a_i	$x_{i+1} = (x_i - a_i)/3$
0	$1/4$	1	$-1/4$
1	$-1/4$	2	$-3/4$
2	$-3/4$	0	$-1/4$
3	$-1/4$	2	$-3/4$
4	$-3/4$	0	$-1/4$

For instance in row 1: $-\frac{1}{4} \equiv 2 \pmod 3$ because $4 \cdot 2 = 8 \equiv -1$, and $(-\frac{1}{4} - 2)/3 = -\frac{9}{4} \cdot \frac{1}{3} = -\frac{3}{4}$. The remainders cycle between $-\frac{1}{4}$ and $-\frac{3}{4}$, so $\frac{1}{4} = \dots 20202021$ in $\mathbb{Z}_3$. A check by hand: the truncation $1 + 2 \cdot 3 = 7$ satisfies $7 - \frac{1}{4} = \frac{27}{4}$, of 3-adic absolute value 3^{-3}, better even than the promised 3^{-2} because the next digit is 0.

Example 2.16 (a table of expansions)**.** Twelve 3-adic digits, most significant on the left:

-1	$\dots 222222222222$	$\frac{1}{4}$	$\dots 202020202021$
$\frac{1}{2}$	$\dots 111111111112$	$-\frac{1}{4}$	$\dots 020202020202$
$-\frac{1}{2}$	$\dots 111111111111$	$\frac{1}{5}$	$\dots 210121012102$
10	$\dots 000000000101$	$\frac{5}{7}$	$\dots 021201021202$

Positive integers have finitely many nonzero digits, their ordinary base-3 representation ($10 = 101_3$). Negative numbers and fractions have infinitely many. And $\frac{2}{3} = 2 \cdot 3^{-1}$ has $v_3 = -1$; its expansion is $\dots 000.2$, with one digit after the point, so $\frac{2}{3} \notin \mathbb{Z}_3$ and $|\frac{2}{3}|_3 = 3$.

Example 2.17 ($-1 = \dots 2222$)**.** Add 1 to $\dots 2222$ by the school method: $2+1 = 3 = 10_3$, write 0 and carry 1; the next column is again $2+1$, and so on forever, so the result is $\dots 0000 = 0$. In terms of truncations: $2+2\cdot 3+\cdots+2\cdot 3^{N-1} = 3^N - 1$, and $|(3^N-1)-(-1)|_3 = |3^N|_3 = 3^{-N} \to 0$. For $N = 8$: $3^8 - 1 = 6560 = 22222222_3$ and $6560 + 1 = 6561 = 100000000_3$. The carry has run off to the left, into digits that a distance 3^{-8} no longer sees.

Example 2.18 ($1, 4, 13, 40, \dots \to -\frac{1}{2}$)**.** This keeps a promise of the toy example in Chapter 1. Put $c_m = 1 + 3 + \cdots + 3^{m-1} = (3^m - 1)/2$. Then

$$c_m - \left(-\tfrac{1}{2}\right) = \frac{3^m - 1}{2} + \frac{1}{2} = \frac{3^m}{2}\ , \qquad \left|c_m + \tfrac{1}{2}\right|_3 = 3^{-m}\ ,$$

since 2 is invisible to $|\cdot|_3$. So $c_m \to -\frac{1}{2}$ in $\mathbb{Q}_3$, one trit at a time:

m	1	2	3	4	5	6	7	8
c_m	1	4	13	40	121	364	1093	3280
$c_m + \frac{1}{2}$	$\frac{3}{2}$	$\frac{9}{2}$	$\frac{27}{2}$	$\frac{81}{2}$	$\frac{243}{2}$	$\frac{729}{2}$	$\frac{2187}{2}$	$\frac{6561}{2}$
$v_3(c_m + \frac{1}{2})$	1	2	3	4	5	6	7	8

In base 3, $c_m = 11\cdots1_3$ (m ones), the truncations of $-\frac{1}{2} = \dots 1111$. Correspondingly $\frac{1}{2} = -\frac{1}{2} + 1 = \dots 1112$, and indeed $2 \cdot (2 + 3 + 3^2 + \cdots + 3^7) = 2 \cdot 3281 = 6562 = 3^8 + 1$, which is $\equiv 1 \pmod{3^8}$, as it should be for an 8-digit truncation of $\frac{1}{2}$.

Check yourself 2.19. Add $\frac{1}{2} + \frac{1}{2}$ in digits, $\dots 1112 + \dots 1112$, and check that you get 1.

Answer. Last column: $2 + 2 = 4 = 11_3$, write 1, carry 1. Every further column: $1 + 1 + 1 = 3 = 10_3$, write 0, carry 1. The result is $\dots 0001 = 1$.

2.3.3 Which expansions are rational?

Proposition 2.20. *An element of $\mathbb{Q}_p$ is rational if and only if its p-adic expansion is eventually periodic.*

Proof. Multiplying by a power of p we may assume $x \in \mathbb{Z}_p$ (this shifts the digits and does not affect periodicity).

Periodic implies rational. Suppose first that the digits are purely periodic with period L, and let $A = a_0 + a_1 p + \cdots + a_{L-1}p^{L-1}$ be the integer formed by one block. Then $x = A(1 + p^L + p^{2L} + \dots) = A/(1 - p^L)$ by the geometric series (Example 2.23 below), which is rational. If the period starts only after j digits, $x = B + p^j x'$ with an integer B and a purely periodic x', again rational.

Rational implies periodic. If $x = u/w \in \mathbb{Z}_p \cap \mathbb{Q}$ with $w > 0$ and $p \nmid w$, run Proposition 2.14: $x_i = u_i/w$ with $u_{i+1} = (u_i - a_i w)/p$. Since $0 \le a_i \le p - 1$, we get $|u_{i+1}| \le (|u_i| + (p-1)w)/p$. If $|u_i| > w$ this gives $|u_{i+1}| < (|u_i| + (p-1)|u_i|)/p = |u_i|$, so the $|u_i|$ decrease strictly until they are at most w; and once $|u_i| \le w$, the same bound gives $|u_{i+1}| \le w$. So eventually all u_i lie in the finite set $\{-w, \dots, w\}$. Each x_{i+1} is determined by x_i, so as soon as a value repeats the sequence of remainders, and with it the sequence of digits, repeats periodically. □

Example 2.21. For $-\frac{1}{2} = \dots 1111$ the block is $A = 1$, $L = 1$, and $1/(1 - 3) = -\frac{1}{2}$. For $-\frac{1}{4} = \dots 0202$ the block is $a_0 = 2$, $a_1 = 0$, so $A = 2$, $L = 2$, and $2/(1 - 9) = -\frac{1}{4}$. For $\frac{1}{4}$ the remainders of Example 2.15 cycle through $-\frac{1}{4}, -\frac{3}{4}$, with $w = 4$ and numerators $|u_i| \le 4$, as in

the proof. The expansions of $\frac{1}{5}$ and $\frac{5}{7}$ in Example 2.16 become periodic from the second digit on, with periods 4 and 6. By contrast, the number

$$\xi = \sum_{k\geq 0} 3^{k^2} = 1 + 3 + 3^4 + 3^9 + 3^{16} + \cdots = \ldots 0001000000000010000000010000001000010011$$

(digits a_0 to a_{39}) has 1s at the square positions, separated by gaps $2k$ that grow; its expansion is not eventually periodic, so $\xi \in \mathbb{Z}_3$ is irrational.

2.4 Convergence of series

The Volkenborn integral [note, (2.5)] is a limit of 3-adic Riemann sums, and the note constantly expands functions in power series and integrates them term by term [note, Lemmas 2.9, 2.11]. In $\mathbb{Q}_p$, deciding whether a series converges is much easier than in $\mathbb{R}$.

Proposition 2.22 (convergence test)**.** *A series $\sum_{k\geq 0} b_k$ with $b_k \in \mathbb{Q}_p$ converges in $\mathbb{Q}_p$ if and only if $b_k \to 0$, that is, $v_p(b_k) \to \infty$.*

Proof. If the series converges, then $b_k = S_k - S_{k-1} \to 0$, where S_k are the partial sums. Conversely, for $M > N$, by the ultrametric inequality applied repeatedly,

$$|S_M - S_N|_p = \Big| \sum_{k=N+1}^{M} b_k \Big|_p \leq \max_{N<k\leq M} |b_k|_p \ ,$$

which tends to 0 as $N \to \infty$ when $b_k \to 0$. So the partial sums form a Cauchy sequence, which converges because $\mathbb{Q}_p$ is complete. □

Intuition: no harmonic-series trap. In $\mathbb{R}$ the terms $\frac{1}{k} \to 0$ but $\sum \frac{1}{k}$ diverges, because many small terms pile up. In $\mathbb{Q}_p$ they cannot pile up: a sum of terms of size at most p^{-N} has size at most p^{-N}, however many terms there are. This is the ultrametric inequality at work, and it is also the reason for the estimate (V3) of the Volkenborn integral [note, Lemma 2.6] (Chapter 4).

Example 2.23 ($3^N \to 0$ and $\sum 3^k = -\frac{1}{2}$)**.** Since $|3^N|_3 = 3^{-N}$, the powers $3, 9, 27, \ldots$ tend to 0 in $\mathbb{Q}_3$, even though they tend to infinity in $\mathbb{R}$; for instance $|3^{20}|_3 = |3486784401|_3 \approx 2.87 \cdot 10^{-10}$. More generally, for any $q \in \mathbb{Q}_p$ with $|q|_p < 1$, the geometric series converges, and since $\sum_{k<m} q^k = (1-q^m)/(1-q)$ with $q^m \to 0$,

$$\sum_{k\geq 0} q^k = \frac{1}{1-q} \qquad (|q|_p < 1) \ . \tag{2.4}$$

For $q = 3$ this is $\sum_k 3^k = \frac{1}{1-3} = -\frac{1}{2}$, whose partial sums are the c_m of Example 2.18. In $\mathbb{R}$ the same series diverges: the two worlds disagree about which series converge, and the value $-\frac{1}{2}$ is meaningful only in $\mathbb{Q}_3$. For $q = -3$, $\sum(-3)^k = \frac{1}{4}$: the partial sums are $1, -2, 7, -20, 61, -182$, at distances $3^{-1}, \ldots, 3^{-6}$ from $\frac{1}{4}$ (e.g. $7 - \frac{1}{4} = \frac{27}{4}$). The same fact in different clothes: $3^N - 1 \to -1$, which the note uses in the proof of (V2) [note, Lemma 2.6]; the digits of $3^N - 1$ are N twos (Example 2.17).

The note needs a slightly more general statement for power series.

Corollary 2.24. *If $e_m \in \mathbb{Q}_3$ satisfy $v_3(e_m) \geq m + c_0$ for a constant c_0, then $f(t) = \sum_m e_m t^m$ converges for every $t \in \mathbb{Z}_3$, and $|f(t)|_3 \leq \max_m |e_m|_3$.*

Proof. For $t \in \mathbb{Z}_3$, $v_3(e_m t^m) = v_3(e_m) + m\, v_3(t) \geq m + c_0 \to \infty$, so Proposition 2.22 applies, and the ultrametric inequality (passed to the limit) bounds the sum by the largest term, each term being at most $|e_m|_3$ since $|t^m|_3 \leq 1$. □

Example 2.25. For an integer a with $3 \nmid a$, (2.4) with $q = -3t/a$ gives

$$\frac{1}{a+3t} = \frac{1}{a} \cdot \frac{1}{1+3t/a} = \sum_{m\geq 0} \frac{(-3)^m}{a^{m+1}}\, t^m \ ,$$

with coefficients of valuation exactly m, convergent for all $t \in \mathbb{Z}_3$. With $a = 1$ and $t = 1$ this is the series $\sum(-3)^m = \frac{1}{4}$ of Example 2.23. Factors of this type, $(a+3t)^{\pm 1}$ and $a + 6t$, make up the function $Q_r(t)$ in the note's factorization of the weight [note, (4.5)], with coefficients $v_3(q_i) \geq i$; this is used in Chapter 8. The pole of $1/(a+3t)$ is at $t = -a/3$, which has $|t|_3 = 3$: it lies outside $\mathbb{Z}_3$, at exactly the distance at which the series stops converging.

One more inequality is used in the note's comment after [note, Lemma 2.6]: for $x, y \in \mathbb{Z}_3$ and $m \geq 1$,

$$|x^m - y^m|_3 \leq |x - y|_3 \ , \tag{2.5}$$

because $x^m - y^m = (x-y)(x^{m-1} + x^{m-2}y + \cdots + y^{m-1})$ and the second factor is in $\mathbb{Z}_3$, so has absolute value at most 1. For $(x, y, m) = (2, 11, 5)$ one finds $x^m - y^m = -161019$ with $v_3 = 2 = v_3(x-y)$, and for $(1, 4, 3)$, $x^m - y^m = -63$ with $v_3 = 2 > 1 = v_3(x-y)$: the inequality can be strict. So a monomial t^m on $\mathbb{Z}_3$ is 1-Lipschitz, in contrast to $\mathbb{R}$, where t^m on $[0, 2]$ has slope up to $m2^{m-1}$.

2.5 Units, and the set of integration points

2.5.1 Units

Definition 2.26 (units)**.** $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : \ |x|_p = 1\} = \{x : \ v_p(x) = 0\}$, the elements of $\mathbb{Z}_p$ whose last digit a_0 is not 0.

Lemma 2.27. *An element $x \in \mathbb{Z}_p$ has an inverse in $\mathbb{Z}_p$ if and only if $x \in \mathbb{Z}_p^\times$.*

Proof. If $xy = 1$ with $x, y \in \mathbb{Z}_p$, then $v_p(x) + v_p(y) = v_p(1) = 0$ with both terms ≥ 0, so $v_p(x) = 0$. Conversely, if $v_p(x) = 0$, then $x \neq 0$ has an inverse $1/x$ in the field $\mathbb{Q}_p$, and $v_p(1/x) = -v_p(x) = 0$, so $1/x \in \mathbb{Z}_p$. □

Example 2.28. In $\mathbb{Z}_3$ the numbers $2, 4, \frac{1}{2}, -1, \frac{5}{7}$ are units (last digits $2, 1, 2, 2, 2$), while 3 and 6 are not ($v_3 = 1$), and $\frac{1}{3} \notin \mathbb{Z}_3$ at all. The inverse of the unit 2 is $\frac{1}{2} = \ldots 1112$ (Example 2.18). The units split by their last digit into two classes, $1 + 3\mathbb{Z}_3$ (e.g. $4, \frac{1}{4}, -\frac{1}{2}$) and $2 + 3\mathbb{Z}_3$ (e.g. $2, \frac{1}{2}, -1$).

Intuition. Units are the numbers that are "of size exactly 1" at p: 3-adically, the integers prime to 3 and the fractions built from them are all of the same size. Multiplying by a unit never changes a 3-adic absolute value. This is why the note can write factors such as $3t + r + 3k$ as "a unit" and forget about them in the 3-adic bookkeeping [note, Section 4].

2.5.2 The set S

The note's functional integrates over the points $t + \frac{r}{3}$ with $t \in \mathbb{Z}_3$ and $r \in \{1, 2\}$ [note, (1.3)], and it describes this set as [note, (2.8)]

$$S = 3^{-1}\mathbb{Z}_3^\times = \{y \in \mathbb{Q}_3 : \ v_3(y) = -1\} \ . \tag{2.6}$$

Lemma 2.29. *$S = \left(\frac{1}{3} + \mathbb{Z}_3\right) \cup \left(\frac{2}{3} + \mathbb{Z}_3\right)$, and the union is disjoint.*

Proof. First, $3^{-1}\mathbb{Z}_3^\times$ and $\{v_3(y) = -1\}$ are the same set: $y = u/3$ with $v_3(u) = 0$ has $v_3(y) = -1$, and conversely $u = 3y$ has $v_3(u) = 0$. Now let $v_3(y) = -1$. Then $u = 3y$ is a unit, so its last digit r is 1 or 2, and $u = r + 3t$ with $t \in \mathbb{Z}_3$ (the remaining digits). Hence $y = \frac{r}{3} + t$. Conversely, if $y = \frac{r}{3} + t$ with $t \in \mathbb{Z}_3$, then $|t|_3 \le 1 < 3 = |\frac{r}{3}|_3$, so by Lemma 2.4(3) $|y|_3 = 3$, i.e. $v_3(y) = -1$. The two classes are disjoint because $\frac{1}{3} - \frac{2}{3} = -\frac{1}{3} \notin \mathbb{Z}_3$. □

Example 2.30. Let us classify a few rationals. $\frac{1}{3}$ and $\frac{2}{3}$ are in S with $t = 0$. $\frac{4}{3} = \frac{1}{3} + 1$ and $-\frac{1}{3} = \frac{2}{3} + (-1)$. $\frac{5}{6} = \frac{1}{3} + \frac{1}{2}$, since $\frac{1}{2} \in \mathbb{Z}_3$; $-\frac{5}{6} = \frac{2}{3} - \frac{3}{2}$; and $\frac{7}{12} = \frac{1}{3} + \frac{1}{4}$. The numbers $\frac{1}{9}$ ($v_3 = -2$) and 1 ($v_3 = 0$) are not in S. Note that the reflection $y \mapsto -y$ used in the note's [note, Lemma 2.9] exchanges the two classes: $\frac{1}{3} \mapsto -\frac{1}{3} \in \frac{2}{3} + \mathbb{Z}_3$.

The following observation, stated in the first paragraph of [note, Section 4], is the source of the whole 3-adic gain.

Proposition 2.31 (nodes are at distance exactly 3)**.** *For every $t \in \mathbb{Z}_3$, $r \in \{1, 2\}$ and $k \in \mathbb{Z}$ (more generally $k \in \mathbb{Z}_3$),*

$$\left|t + \frac{r}{3} + k\right|_3 = 3 \ , \qquad v_3\left(t + \frac{r}{3} + k\right) = -1 \ .$$

Equivalently, every point $y \in S$ is at distance exactly 3 from every integer $-k$, and $(y+k)^{-4} = 3^4 \cdot u^{-4}$ with the unit $u = 3t + r + 3k$.

Proof. $t + k \in \mathbb{Z}_3$ because $\mathbb{Z}_3$ is a ring, so $|t + k|_3 \le 1$, while $|\frac{r}{3}|_3 = 3$. The two summands of $(t + k) + \frac{r}{3}$ have different absolute values, so by Lemma 2.4(3) the sum has the larger one, 3. Finally $y + k = \frac{1}{3}(3t + r + 3k)$ and $3t + r + 3k$ has last digit $r \neq 0$, so it is a unit u, and $(y + k)^{-4} = 3^4 u^{-4}$. □

Example 2.32. The table lists $t + \frac{r}{3} + k$ for four values of $t \in \mathbb{Z}_3$ and six values of k; *every* entry has $v_3 = -1$, that is, numerator prime to 3 and exactly one factor 3 in the denominator.

t	r	$k=-6$	$k=-2$	$k=-1$	$k=0$	$k=1$	$k=3$
0	1	−17/3	−5/3	−2/3	1/3	4/3	10/3
0	2	−16/3	−4/3	−1/3	2/3	5/3	11/3
−1/2	1	−37/6	−13/6	−7/6	−1/6	5/6	17/6
−1/2	2	−35/6	−11/6	−5/6	1/6	7/6	19/6
1/4	1	−65/12	−17/12	−5/12	7/12	19/12	43/12
1/4	2	−61/12	−13/12	−1/12	11/12	23/12	47/12
5/7	1	−104/21	−20/21	1/21	22/21	43/21	85/21
5/7	2	−97/21	−13/21	8/21	29/21	50/21	92/21

As a preview of Chapter 8: for $n = 1$ the nodes are $k = -1, 0, 1, 2$ (poles at $y = -2, -1, 0, 1$), and at $y = \frac{1}{3}$ and at $y = \frac{11}{12}$ the product $\prod_k (y + k)^{-4}$ has $v_3 = 16 = 4(3n + 1)$; for $n = 3$ (10 nodes) it has $v_3 = 40 = 4(3n + 1)$. Each of the $3n + 1$ poles of order 4 contributes exactly 4 trits, wherever y sits in S.

Intuition: why this is special to the 3-adic place. On the real line the integration points $t + \frac{r}{3}$, $t \in [0, 1]$ say, are at very different distances from the poles $-k$: from 0 (the pole $y = 1$ lies among them) to about $2n$. Some poles are close, some far, and their effect on the size of the weight varies wildly. In $\mathbb{Q}_3$ all poles are equally far from all integration points, at distance exactly 3, so each pole multiplies the weight by exactly 3^4 in absolute value, uniformly on S. The real picture has no counterpart of this: it rests on the ultrametric

inequality and on the fact that the integration points carry a "$\frac{1}{3}$" that no integer shift can remove.

Check yourself 2.33. The weight also has the factor $y+\frac{n}{2}$ with n odd [note, (1.2)]. Is $|y+\frac{n}{2}|_3$ also constant on S?

Answer. Yes. Since 2 is a unit in $\mathbb{Z}_3$, $\frac{n}{2}\in\mathbb{Z}_3$, and Proposition 2.31 applies with $k=\frac{n}{2}\in\mathbb{Z}_3$: $v_3(y+\frac{n}{2})=-1$. The note writes this as $y+\frac{n}{2}=\frac{1}{6}(6t+2r+3n)$ with $6t+2r+3n$ a unit [note, Section 4]. For $n=1,3,5$ and $y=\frac{1}{3},\frac{2}{3},\frac{11}{12}$ one finds e.g. $\frac{1}{3}+\frac{1}{2}=\frac{5}{6}$, $\frac{11}{12}+\frac{3}{2}=\frac{29}{12}$, all with $v_3=-1$.

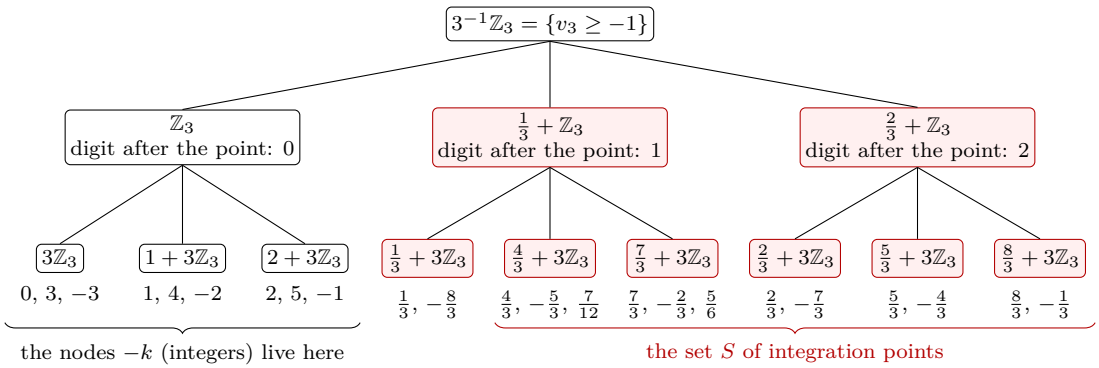


Figure 2.1: The set $3^{-1}\mathbb{Z}_3$ as a tree of digits. Each node of the tree is a ball (a set $c+3^j\mathbb{Z}_3$); going down one level fixes one more digit, starting from the rightmost one, a_{-1} (after the point), and moving left to a_0, a_1, and so on (only the first two levels are drawn, with sample elements). Two numbers are at distance 3^{-j} when a_j is the rightmost digit at which they differ: numbers in different boxes of the first level are at distance 3, numbers in different boxes of the second level below the same first-level box are at distance 1. The set S (red) is the two right branches at the top level; all integers, in particular all nodes $-k$ of the weight, are in the left branch. Hence every point of S is at distance exactly 3 from every node (Proposition 2.31).

Figure 2.1 shows the same fact as a picture. A useful consequence of the tree picture, which is just Corollary 2.5 again: inside a ball $c+3^j\mathbb{Z}_3$, *every* point is a center, and two balls are either disjoint or one contains the other.

2.6 The residue field $\mathbb{F}_p$

Several arguments of the note, the non-vanishing theorem of [note, Section 6] and Gauss's lemma below in particular, reduce a p-adic question to a question "modulo p", where the arithmetic is that of a finite field.

Definition 2.34. $\mathbb{F}_p=\{0,1,\dots,p-1\}$ with addition and multiplication modulo p.

Proposition 2.35. *$\mathbb{F}_p$ is a field: every $a\not\equiv 0 \pmod p$ has an inverse modulo p. Moreover, the map $\mathbb{Z}_p\to\mathbb{F}_p$ that sends x to its last digit a_0 is compatible with addition and multiplication (a ring homomorphism), and its kernel is $p\mathbb{Z}_p=\{v_p\geq 1\}$.*

Proof. If $p\nmid a$, then $\gcd(a,p)=1$ because p is prime, and by Bézout's identity there are integers a',c with $aa'+pc=1$, so $aa'\equiv 1 \pmod p$. For the second statement, by (2.3) with $N=1$, $x\equiv a_0$ modulo $p\mathbb{Z}_p$; sums and products of elements congruent modulo $p\mathbb{Z}_p$ are congruent modulo $p\mathbb{Z}_p$, because $p\mathbb{Z}_p$ is closed under addition and under multiplication by elements of $\mathbb{Z}_p$. The kernel consists of the x with $a_0=0$, that is $v_p(x)\geq 1$. □

Example 2.36. In $\mathbb{F}_3$ both nonzero elements are their own inverses ($2 \cdot 2 = 4 \equiv 1$). In $\mathbb{F}_{13}$, the prime that Chapter 14 uses for its worked example, the inverses of $1, \dots, 12$ are $1, 7, 9, 10, 8, 11, 2, 5, 3, 4, 6, 12$; e.g. $2 \cdot 7 = 14 \equiv 1$. Modulo 4, which is not prime, $2 \cdot 2 \equiv 0$, so $\mathbb{Z}/4$ is not a field. The reduction map sends $\frac{1}{2} \mapsto 2$, $-\frac{1}{2} \mapsto 1$, $\frac{1}{4} \mapsto 1$, $\frac{5}{7} \mapsto 2$ in $\mathbb{F}_3$, the last digits of Example 2.16.

Intuition. $\mathbb{F}_p$ is "$\mathbb{Z}_p$ seen with a blurred eye" that resolves only the last digit, just as reading off the integer part is a blurred view of a real number, except that here the blurring respects multiplication. A unit is an element whose blurred image is not 0. Because $\mathbb{F}_p$ is a field, a product of two nonzero things stays nonzero after blurring, and this is what makes Gauss's lemma work.

2.7 The Gauss valuation of polynomials

The note estimates the denominators of the polynomial $\Delta_K(X)$ prime by prime. For this it measures the "worst power of p" among the coefficients of a polynomial [note, Section 1, Conventions].

Definition 2.37 (Gauss valuation)**.** For $F = \sum_j f_j X^j \in \mathbb{Q}_p[X]$, $F \neq 0$, put $v_p(F) = \min_j v_p(f_j)$, and $v_p(0) = +\infty$.

Intuition. $v_p(F)$ is the valuation of the p-adically largest coefficient. If $v_p(F) < 0$, then $p^{-v_p(F)}$ is the largest power of p that occurs in a denominator, so $(-v_p(F))^+$ is the number of factors of p that must be cleared to make F integral at p; this is the quantity summed over p in the criterion [note, (1.4)]. If $v_p(F) \geq 0$, then $p^{v_p(F)}$ divides every coefficient.

Example 2.38. $F = \frac{3}{2}X^2 + \frac{9}{5}X + \frac{1}{3}$ has coefficient valuations $(v_3) = (1, 2, -1)$, $(v_2) = (-1, 0, 0)$, $(v_5) = (0, -1, 0)$ (from the top coefficient down), so $v_3(F) = v_2(F) = v_5(F) = -1$ and $v_7(F) = 0$.

Lemma 2.39 ([note, Section 1, Conventions])**.** *For $F, G \in \mathbb{Q}_p[X]$ and $c \in \mathbb{Q}_p$:*

1. $v_p(F + G) \geq \min(v_p(F), v_p(G))$;
2. $v_p(FG) \geq v_p(F) + v_p(G)$;
3. $v_p(cF) = v_p(c) + v_p(F)$;
4. *if $x \in \mathbb{Z}_p$, then* $v_p(F(x)) \geq v_p(F)$.

Proof. (1) The coefficient of X^j in $F + G$ is $f_j + g_j$, and by Lemma 2.4(2), $v_p(f_j + g_j) \geq \min(v_p(f_j), v_p(g_j)) \geq \min(v_p(F), v_p(G))$; take the minimum over j.

(2) The coefficient of X^j in FG is $h_j = \sum_{i=0}^{j} f_i g_{j-i}$. Each term has $v_p(f_i g_{j-i}) = v_p(f_i) + v_p(g_{j-i}) \geq v_p(F) + v_p(G)$ by Lemma 2.4(1), and the ultrametric inequality, applied to the sum of these $j + 1$ terms, gives $v_p(h_j) \geq v_p(F) + v_p(G)$.

(3) $v_p(cf_j) = v_p(c) + v_p(f_j)$ for each j; take the minimum.

(4) $F(x) = \sum_j f_j x^j$, and $v_p(f_j x^j) = v_p(f_j) + j\, v_p(x) \geq v_p(f_j) \geq v_p(F)$; apply the ultrametric inequality to the sum. □

Example 2.40. $F = X - \frac{1}{3}$ and $G = X - \frac{2}{3}$ have $v_3(F) = v_3(G) = -1$; their product $FG = X^2 - X + \frac{2}{9}$ has $v_3(FG) = -2$, and their sum $2X - 1$ has $v_3 = 0 \geq -1$. The sum of $X + \frac{1}{3}$ and $-X + \frac{2}{3}$ is the constant 1, with $v_3 = 0 > -1$: in (1) the inequality can be strict, by cancellation of the worst coefficients. Products behave differently: with $F = \frac{3}{2}X^2 + \frac{9}{5}X + \frac{1}{3}$ from Example 2.38 and $G = \frac{1}{9}X^2 + 3$ one finds $FG = \frac{1}{6}X^4 + \frac{1}{5}X^3 + \frac{245}{54}X^2 + \frac{27}{5}X + 1$ and $v_3(F), v_3(G), v_3(FG) = -1, -2, -3$: the valuations add. The next remark explains why this always happens.

Remark 2.41 (Gauss's lemma: (2) is an equality). In fact $v_p(FG) = v_p(F) + v_p(G)$ for all nonzero $F, G \in \mathbb{Q}_p[X]$; this is a form of Gauss's lemma (any algebra text that treats Gauss's lemma for $\mathbb{Z}[X]$; the version for $\mathbb{Z}_p$ is the same argument). The note states and uses only the inequality. *Proof.* By (3), $F_0 = p^{-v_p(F)}F$ and $G_0 = p^{-v_p(G)}G$ have Gauss valuation 0: their coefficients are in $\mathbb{Z}_p$ and at least one coefficient of each is a unit. Reduce all coefficients modulo p (Proposition 2.35): the reductions $\bar{F}_0, \bar{G}_0 \in \mathbb{F}_p[X]$ are nonzero polynomials. Since $\mathbb{F}_p$ is a field, the product of the leading coefficients of $\bar{F}_0$ and $\bar{G}_0$ is nonzero, so $\bar{F}_0\bar{G}_0 \neq 0$. Because reduction respects products, $\bar{F}_0\bar{G}_0$ is the reduction of F_0G_0, so F_0G_0 has a coefficient that is a unit, $v_p(F_0G_0) = 0$, and by (3) $v_p(FG) = v_p(F) + v_p(G)$. For $F = X - \frac{1}{3}$, $G = X - \frac{2}{3}$ at $p = 3$: $F_0 = 3X - 1$, $G_0 = 3X - 2$ reduce to the nonzero constants 2 and 1 in $\mathbb{F}_3$, with product $2 \neq 0$, and indeed $9FG = 9X^2 - 9X + 2$ reduces to 2.

Remark 2.42 (content and primitive part). For $F \in \mathbb{Q}[X]$, $F \neq 0$, only finitely many $v_p(F)$ are nonzero. Put $c_F = \prod_p p^{v_p(F)}$ and $Q = F/c_F$. By (3), $v_p(Q) = 0$ for every p: no coefficient of Q has any prime in its denominator, so $Q \in \mathbb{Z}[X]$, and for every prime some coefficient is not divisible by it, so the coefficients of Q have greatest common divisor 1. This is the first step of the note's proof of the criterion [note, Lemma 3.1] (Chapter 7). For $F = \frac{3}{2}X^2 + \frac{9}{5}X + \frac{1}{3}$: $c_F = 2^{-1}3^{-1}5^{-1} = \frac{1}{30}$ and $Q = 30F = 45X^2 + 54X + 10$, whose coefficients have no common factor.

Remark 2.43 (the Gauss valuation is not the size of the values). Part (4) is only an inequality, and it can be far from sharp: a polynomial can have a negative Gauss valuation and still take only p-adic integer values on $\mathbb{Z}_p$. Example: $F = \frac{1}{3}(X^3 - X)$ has $v_3(F) = -1$, but its values at $x = 0, \dots, 6$ are $0, 0, 2, 8, 20, 40, 70$, integers, because $x^3 \equiv x \pmod 3$ for every integer x (Fermat's little theorem). This is not a problem in the note, but a central theme of its [note, Section 4]: the polynomials that are integer valued on S form the class $\mathrm{Int}(S)$, and the change of basis of [note, Lemma 4.1] exploits exactly this gap between the coefficients and the values (Chapter 8). So $v_p(F)$ must not be read as "the valuation of F on $\mathbb{Z}_p$".

The note's [note, Conventions] also define $\|F\|_1 = \sum_j |f_j|$, the ordinary size counterpart of the Gauss valuation, with $\|FG\|_1 \leq \|F\|_1\|G\|_1$ (expand FG and apply the triangle inequality to each coefficient $h_j = \sum_i f_i g_{j-i}$). For the F and G of Example 2.40, $\|F\|_1 = \frac{109}{30}$, $\|G\|_1 = \frac{28}{9}$, and $\|FG\|_1 = \frac{1526}{135}$, which equals the product because all coefficients are positive and nothing cancels; for $(X + 1)(X - 1) = X^2 - 1$ one gets $2 < 2 \cdot 2$.

2.8 Legendre's formula

Factorials appear throughout the note: in the Pochhammer symbols of the weight, in the basis polynomials $F_{2q} = 3^q q!\binom{y-1/3}{q}\binom{y-2/3}{q}$ [note, (4.2)], and in $A_3 = 9n + 3 + 3v_3(n!)$ [note, (4.8)]. We need to know how many factors of p a factorial contains.

Proposition 2.44 (Legendre's formula)**.** *For a prime p and an integer $q \geq 0$, let $s_p(q)$ be the sum of the base-p digits of q. Then*

$$v_p(q!) = \sum_{i \geq 1} \left\lfloor \frac{q}{p^i} \right\rfloor = \frac{q - s_p(q)}{p - 1} \,. \tag{2.7}$$

Proof. By Lemma 2.4(1), $v_p(q!) = \sum_{m=1}^{q} v_p(m)$. Write $v_p(m) = \sum_{i \geq 1} [p^i \mid m]$, where $[\cdot]$ is 1 if the condition holds and 0 otherwise (a multiple of p^2 but not of p^3 is counted for $i = 1$ and $i = 2$, that is twice). Exchanging the two sums, $v_p(q!) = \sum_{i \geq 1} \#\{1 \leq m \leq q : \ p^i \mid m\} = \sum_{i \geq 1} \lfloor q/p^i \rfloor$, since the multiples of p^i up to q are $p^i, 2p^i, \dots, \lfloor q/p^i \rfloor p^i$. For the second form, write $q = \sum_{j \geq 0} d_j p^j$ in base p. Then $\lfloor q/p^i \rfloor = \sum_{j \geq i} d_j p^{j-i}$ (dividing by p^i shifts the digits and

drops the last i of them), and

$$\sum_{i\ge 1}\lfloor \frac{q}{p^i}\rfloor = \sum_{j\ge 1} d_j \sum_{i=1}^{j} p^{j-i} = \sum_j d_j \frac{p^j-1}{p-1} = \frac{q-s_p(q)}{p-1}\ . \qquad \square$$

Example 2.45. $q = 10 = 101_3$: $\lfloor 10/3\rfloor + \lfloor 10/9\rfloor = 3+1 = 4$, and $(10 - s_3(10))/2 = (10-2)/2 = 4$; indeed 10! contains the factors 3, 6 and 9, contributing $1+1+2$ (Example 2.3). For $p = 3$ and $q \le 30$:

q	base 3	s_3	$v_3(q!)$	q	base 3	s_3	$v_3(q!)$	q	base 3	s_3	$v_3(q!)$
0	0	0	0	11	102	3	4	21	210	3	9
1	1	1	0	12	110	2	5	22	211	4	9
2	2	2	0	13	111	3	5	23	212	5	9
3	10	1	1	14	112	4	5	24	220	4	10
4	11	2	1	15	120	3	6	25	221	5	10
5	12	3	1	16	121	4	6	26	222	6	10
6	20	2	2	17	122	5	6	27	1000	1	13
7	21	3	2	18	200	2	8	28	1001	2	13
8	22	4	2	19	201	3	8	29	1002	3	13
9	100	1	4	20	202	4	8	30	1010	2	14
10	101	2	4								

The jumps by 2 at $q = 9, 18$ and by 3 at $q = 27$ are the multiples of 9 and of 27.

Intuition. Among $1, \dots, q$, about q/p numbers are multiples of p, about q/p^2 are multiples of p^2 and contribute an extra factor, and so on: $v_p(q!) \approx q/p + q/p^2 + \cdots = q/(p-1)$. The digit sum $s_p(q)$ is the exact correction from rounding down, and it is small: a number with ℓ digits has digit sum at most $(p-1)\ell$. For $p = 3$, $v_3(q!) \approx q/2$.

The note uses (2.7) with the bound

$$s_3(q) \le 2\log_3(3q) \qquad (q \ge 1)\ , \tag{2.8}$$

which holds because q has $\lfloor \log_3 q\rfloor + 1 \le \log_3 q + 1 = \log_3(3q)$ ternary digits, each at most 2. Hence $v_3(q!) = \frac{q}{2} - O(\log q)$, which is how [note, (4.4)] and the proof of [note, Theorem 3.5] turn $2\sum_{i<K}\nu_i$ into $-K^2/4$ and $3v_3(n!)$ into $1.5n$, up to lower-order terms (Chapter 8).

Example 2.46. Formula (2.7) gives

n	$s_3(n)$	$v_3(n!)$	$v_3(n!)/n$
10	2	4	0.4
100	4	48	0.48
1000	4	498	0.498
10^4	8	4996	0.4996
10^6	14	499993	0.499993

So $v_3(n!)/n \to \frac{1}{2}$. With $v_3(5!) = 1$, $v_3(11!) = 4$, $v_3(101!) = 48$ and $v_3(1001!) = 498$ one recovers $A_3 = 9n + 3 + 3v_3(n!) = 51, 114, 1056, 10506$, the values quoted in Chapter 1.

2.9 What "$\zeta_3(5) = a/b$" means

The number $\zeta_3(5)$ is constructed in Chapter 3 as an element of $\mathbb{Q}_3$, defined by a convergent 3-adic series ([note, Theorem 2.1], [note, (2.4)]) Chapter 3 computes its first digits. The statement

to be disproved is that $\zeta_3(5) = a/b$ for some integers a, b with $b > 0$, as an equation in $\mathbb{Q}_3$, where a/b is identified with the constant sequence (Definition 2.11). Concretely, the following are equivalent: $\zeta_3(5) = a/b$; $|\zeta_3(5) - a/b|_3 = 0$; $\zeta_3(5)$ and a/b have the same 3-adic digits, all of them. By Proposition 2.20, irrationality means that the digit sequence of $\zeta_3(5)$ is not eventually periodic.

Intuition: close to a rational. A 3-adic number ξ is *close to* a rational a/b when $|\xi - a/b|_3$ is small, that is, when they share many trailing digits. No finite computation can decide irrationality this way: every finite string of digits is shared with some rational, indeed with an integer (its truncation, by (2.3)). Example: the irrational $\xi = \sum_k 3^{k^2}$ of the previous section agrees with the integer $c_5 = 1 + 3 + 3^4 + 3^9 + 3^{16} = 43066489$ to within 3^{-25}. So every 3-adic number is extremely well approximable by integers, and the quality of an approximation means something only when compared with the size of the approximating fraction, $\max(|a|, b)$: the truncation to N digits is an integer of size up to 3^N that approximates to within 3^{-N}, "for free". This is the reason why the criterion [note, (1.4)] contains, besides the gain on the left, the size of the coefficients and the height term $K \log_2 \max(|a|, b)$ on the right, and why the toy example of Chapter 1, with its approximations c_m to $-\frac{1}{2}$, sits right at the edge of that inequality. An irrationality proof must exhibit approximations that beat this free rate in a way that a fixed rational a/b could not sustain.

Check yourself 2.47. Someone computes the first 10^6 digits of $\zeta_3(5)$ and finds no period. Does this prove irrationality?

Answer. No. A rational a/b with $3 \nmid b$ has an eventually periodic expansion, the proof of Proposition 2.20 only bounds preperiod plus period by about $2b + 1$ digits (the number of possible numerators of the remainders u_i/b), and periods close to b do occur: for $\frac{5}{7}$ the period is 6 (Example 2.16). A rational with $b > 10^6$ is not excluded by the computation. Irrationality needs an argument valid for all b at once, such as the note's.

Summary of the chapter

We defined the p-adic valuation v_p and absolute value $|x|_p = p^{-v_p(x)}$ on $\mathbb{Q}$, proved that v_p is additive on products and satisfies the ultrametric inequality, with equality when the valuations differ (so every triangle is isosceles), and proved the product formula $|x|_\infty \prod_p |x|_p = 1$ and its consequence $|N| \geq 3^{v_3(N)}$ for nonzero integers. We completed $\mathbb{Q}$ to $\mathbb{Q}_p$, described its elements by digit expansions infinite to the left, computed expansions such as $-1 = \ldots 2222$, $-\frac{1}{2} = \ldots 1111$ and $\frac{1}{4} = \ldots 2021$, and showed that rationals are exactly the eventually periodic expansions. A series converges in $\mathbb{Q}_p$ as soon as its terms tend to 0, which gives $\sum 3^k = -\frac{1}{2}$ and power series with $v_3(e_m) \geq m$ on $\mathbb{Z}_3$. We introduced the units $\mathbb{Z}_p^\times$, the set of integration points $S = 3^{-1}\mathbb{Z}_3^\times = (\frac{1}{3} + \mathbb{Z}_3) \cup (\frac{2}{3} + \mathbb{Z}_3)$, and proved that $|t + \frac{r}{3} + k|_3 = 3$ for all $t \in \mathbb{Z}_3$, $r \in \{1, 2\}$, $k \in \mathbb{Z}$. We introduced $\mathbb{F}_p$, the Gauss valuation with its two inequalities and Gauss's lemma, and Legendre's formula $v_p(q!) = (q - s_p(q))/(p - 1)$ with $v_3(n!)/n \to \frac{1}{2}$.

Carried forward: the ultrametric inequality and Proposition 2.22 (used for the Volkenborn integral in Chapter 4); Proposition 2.31 and Example 2.25 (the factorization of the weight, Chapter 8); Legendre's formula and (2.8) (Chapter 8, Chapter 11); the Gauss valuation Lemma 2.39 (all of Part IV); the product formula, Corollary 2.10 and the content decomposition Remark 2.42 (the criterion, Chapter 7, and the second proof, Chapter 17); and $\mathbb{F}_p$ (Chapter 14).

Chapter 3

Bernoulli numbers and the 3-adic zeta value

Where we are. The theorem of the note is about one number, $\zeta_3(5)$. This chapter says what that number is. It covers the first half of the note's [note, Section 2.1]: the standard result [note, Theorem 2.1] on the Kubota–Leopoldt p-adic L-function, with its interpolation formula [note, (2.2)] and its series formula [note, (2.3)], the definition $\zeta_p(s) = L_p(s, \omega^{1-s})$ from [note, Section 1], and the normalization $\zeta_3(5) = L_3(5, \mathbf{1})$ [note, (2.4)]. On the way we build everything these formulas are made of: Bernoulli numbers and polynomials, Faulhaber's formula (used in the proof of (V2) [note, Lemma 2.6]), Euler's formula for $\zeta(2k)$, the values $\zeta(1-k)$, the von Staudt–Clausen theorem, the Kummer congruences, Dirichlet characters, the Teichmüller character and generalized Bernoulli numbers. At the end we compute the first 62 digits of $\zeta_3(5)$ in $\mathbb{Z}_3$-notation from the series [note, (2.13)] and confirm the first 11 of them by a second, independent route. We use from Chapter 2 the valuation v_p, the absolute value $|\cdot|_p$, digit expansions, the convergence test for series and the fact that a p-adic number is rational if and only if its digits are eventually periodic. Unless stated otherwise, the numbers in this chapter are computed in exact rational arithmetic.

The standard reference for this chapter is Washington [34], Chapters 4 and 5, which is also the note's reference. A gentler introduction to Bernoulli numbers is Ireland and Rosen, *A Classical Introduction to Modern Number Theory*, Ch. 15, and to p-adic zeta functions Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Ch. II.

3.1 Bernoulli numbers

Bernoulli numbers enter the note in two places. The Volkenborn integral of a monomial is a Bernoulli number, $\int_{\mathbb{Z}_3} t^c \, \mathrm{d}t = B_c$ (V2) [note, Lemma 2.6], explained in Chapter 4; and the formula [note, (2.3)] that defines $\zeta_3(5)$ in practice is a series in Bernoulli numbers. Historically they arose from sums of powers, $1^c + 2^c + \cdots + (M-1)^c$, and that is still the best way to think of them (Section 3.2).

Definition 3.1 (Bernoulli numbers)**.** The Bernoulli numbers $B_0, B_1, B_2, \ldots$ are the rational numbers defined by the Taylor expansion

$$\frac{t}{e^t - 1} = \sum_{n \geq 0} B_n \frac{t^n}{n!} \qquad (|t| < 2\pi) \ . \tag{3.1}$$

The function $t/(e^t - 1)$ is smooth at $t = 0$ (its value there is 1), and its nearest singularities are the zeros $t = \pm 2\pi i$ of $e^t - 1$, hence the radius of convergence 2π. Multiplying (3.1) by

$(e^t-1)/t = \sum_{j\ge 0} t^j/(j+1)!$ and comparing the coefficients of $t^m/m!$ on both sides gives $\sum_{j=0}^{m} \binom{m+1}{j} B_j = 0$ for $m \ge 1$, that is,

$$B_0 = 1\ , \qquad B_m = -\frac{1}{m+1}\sum_{j=0}^{m-1}\binom{m+1}{j}B_j \quad (m\ge 1)\ . \tag{3.2}$$

(The coefficient of t^m in the product is $\sum_j B_j/(j!\,(m-j+1)!)$; multiplied by $(m+1)!$ this is $\sum_j \binom{m+1}{j}B_j$, and it must vanish because the product is 1.)

Example 3.2 (the first Bernoulli numbers by hand)**.** With $m=1$: $B_1 = -\frac{1}{2}\binom{2}{0}B_0 = -\frac{1}{2}$. With $m=2$: $B_2 = -\frac{1}{3}(\binom{3}{0}B_0 + \binom{3}{1}B_1) = -\frac{1}{3}(1-\frac{3}{2}) = \frac{1}{6}$. With $m=3$: $B_3 = -\frac{1}{4}(1+4\cdot(-\frac{1}{2})+6\cdot\frac{1}{6}) = -\frac{1}{4}(1-2+1) = 0$.

Example 3.3 (table)**.** Computing B_n from (3.2) in exact fractions, the nonzero values up to $n=20$ are

n	0	1	2	4	6	8	10	12	14	16	18
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$	$\frac{43867}{798}$

and $B_{20} = -\frac{174611}{330}$. All odd B_n with $3 \le n \le 79$ are 0, and every B_n with even $n \ge 2$ in the table has $v_3(B_n) = -1$: its denominator contains exactly one factor 3 (the denominators are $6, 30, 42, 30, 66, 2730, 6, 510, 798, 330$). Both observations are theorems, proved or stated below.

Intuition: what the Bernoulli numbers are. $t/(e^t-1)$ is the Bose–Einstein occupation factor $1/(e^t-1)$ times t (with $t = \hbar\omega/k_BT$). The Bernoulli numbers are its Taylor coefficients: they measure how a sum $\sum_n f(n)$ differs from the integral $\int f$, which is why they appear in the Euler–Maclaurin formula and in every "sum versus integral" correction, for instance in the high-temperature expansion of a Bose gas. Their size grows quickly after the first few, $|B_{2k}| \sim 2(2k)!/(2\pi)^{2k}$ (a consequence of Euler's formula (3.7) below with $\zeta(2k) \approx 1$); for example $|B_{20}| \approx 529$.

Proposition 3.4 (odd Bernoulli numbers vanish)**.** *$B_n = 0$ for every odd $n \ge 3$.*

Proof. Put $g(t) = \frac{t}{e^t-1} + \frac{t}{2}$. Then

$$g(-t) = \frac{-t}{e^{-t}-1} - \frac{t}{2} = \frac{t\,e^t}{e^t-1} - \frac{t}{2} = \frac{t(e^t-1)+t}{e^t-1} - \frac{t}{2} = t + \frac{t}{e^t-1} - \frac{t}{2} = g(t)\ ,$$

where in the second step we multiplied numerator and denominator by $-e^t$. So g is even, its Taylor series contains only even powers, and the coefficient of t^n for odd n is 0. For $n=1$ this coefficient is $B_1 + \frac{1}{2} = 0$; for odd $n \ge 3$ it is $B_n/n!$. □

3.2 Bernoulli polynomials and sums of powers

Definition 3.5 (Bernoulli polynomials)**.** $B_k(x) = \sum_{i=0}^{k}\binom{k}{i}B_i\,x^{k-i}$. Equivalently,

$$\frac{t\,e^{xt}}{e^t-1} = \sum_{k\ge 0} B_k(x)\frac{t^k}{k!}\ . \tag{3.3}$$

The two forms agree: the left side of (3.3) is the product of $\sum_i B_i t^i/i!$ and $\sum_j x^j t^j/j!$, and the coefficient of $t^k/k!$ in the product is $\sum_i \frac{k!}{i!(k-i)!}B_i x^{k-i}$. Setting $x=0$ gives $B_k(0) = B_k$.

Example 3.6. The first Bernoulli polynomials are

$B_1(x) = x - \frac{1}{2}$, $B_2(x) = x^2 - x + \frac{1}{6}$, $B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$, $B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30}$, and $B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x$. At the points that matter for $p = 3$: $B_3(\frac{1}{3}) = \frac{1}{27}$, $B_3(\frac{2}{3}) = -\frac{1}{27}$, and $B_4(\frac{1}{3}) = B_4(\frac{2}{3}) = \frac{13}{810}$.

Proposition 3.7 (two identities)**.** *For $k \geq 1$, $B_k(x+1) - B_k(x) = k\,x^{k-1}$; and for $k \geq 0$, $B_k(1-x) = (-1)^k B_k(x)$.*

Proof. Difference: by (3.3),

$$\sum_k \big(B_k(x+1) - B_k(x)\big)\frac{t^k}{k!} = \frac{t\,e^{xt}(e^t - 1)}{e^t - 1} = t\,e^{xt} = \sum_{j\geq 0} x^j \frac{t^{j+1}}{j!}\ ,$$

and the coefficient of $t^k/k!$ on the right is $k!\,x^{k-1}/(k-1)! = kx^{k-1}$. Reflection: multiply numerator and denominator by $-e^{-t}$,

$$\frac{t\,e^{(1-x)t}}{e^t - 1} = \frac{(-t)\,e^{x(-t)}}{e^{-t} - 1} = \sum_k B_k(x)\frac{(-t)^k}{k!}\ ,$$

and compare coefficients of $t^k/k!$. □

Example 3.8. $B_4(3) - B_4(2) = 32 = 4 \cdot 2^3$. The reflection identity with $x = \frac{1}{3}$ is visible in Example 3.6: $B_3(\frac{2}{3}) = -B_3(\frac{1}{3})$ and $B_4(\frac{2}{3}) = B_4(\frac{1}{3})$.

Intuition: discrete antiderivative. The first identity says that $B_{c+1}(x)/(c+1)$ is a *discrete antiderivative* of x^c: its forward difference is x^c, just as the derivative of $x^{c+1}/(c+1)$ is x^c. The reflection identity says that the Bernoulli polynomials are symmetric (even k) or antisymmetric (odd k) about $x = \frac{1}{2}$. The note uses it in the reflection lemma [note, Lemma 2.9] (Chapter 4), and at $x = \frac{1}{3}, \frac{2}{3}$ it is the reason why the two classes $\frac{1}{3} + \mathbb{Z}_3$ and $\frac{2}{3} + \mathbb{Z}_3$ of integration points are mirror images.

Summing the difference identity over $x = 0, 1, \ldots, M-1$ makes the left side telescope:

Proposition 3.9 (Faulhaber's formula)**.** *For integers $M \geq 0$ and $c \geq 0$,*

$$\sum_{t=0}^{M-1} t^c = \frac{B_{c+1}(M) - B_{c+1}}{c+1} = \frac{1}{c+1}\sum_{i=0}^{c}\binom{c+1}{i} B_i\, M^{c+1-i}\ . \tag{3.4}$$

Proof. By Proposition 3.7 with $k = c+1$, $(c+1)t^c = B_{c+1}(t+1) - B_{c+1}(t)$. Summing over $0 \leq t \leq M-1$, all intermediate terms cancel and $(c+1)\sum_{t<M} t^c = B_{c+1}(M) - B_{c+1}(0)$, with $B_{c+1}(0) = B_{c+1}$. The second form is Definition 3.5 with the term $i = c+1$ (which is B_{c+1}) cancelled. □

Example 3.10. $\sum_{t<10} t^4 = 0 + 1 + 16 + 81 + 256 + 625 + 1296 + 2401 + 4096 + 6561 = 15333$, and $B_5(10) = 76665$, so $(B_5(10) - B_5)/5 = 76665/5 = 15333$ (here $B_5 = 0$).

Where the note uses it. In (V2) [note, Lemma 2.6] the Volkenborn integral of t^c is the limit of the Riemann sums $S_N = 3^{-N}\sum_{t<3^N} t^c$. Faulhaber with $M = 3^N$ gives $S_N = \sum_{i=0}^{c}\binom{c+1}{i}B_i\,3^{N(c-i)}/(c+1)$. The term $i = c$ is $\binom{c+1}{c}B_c/(c+1) = B_c$, and every other term contains $3^{N(c-i)}$ with $c - i \geq 1$, which tends to 0 in $\mathbb{Q}_3$. So $S_N \to B_c$ 3-adically, while in $\mathbb{R}$ the same S_N grows like $3^{Nc}/(c+1)$. For $c = 2$ one finds $S_1 = \frac{5}{3}$, $S_2 = \frac{68}{3}$, $S_3 = \frac{689}{3}$ and $v_3(S_N - \frac{1}{6}) = N$ for $N = 1, \ldots, 6$; for $c = 4$, $S_1 = \frac{17}{3}$, $S_2 = \frac{2924}{3}$ and $v_3(S_N + \frac{1}{30}) = 2N - 1$. The rates are those of the first surviving correction: for $c = 2$ it is the term $i = 1$, $3B_1\,3^N/3 = -\frac{3^N}{2}$, of valuation N; for $c = 4$ the term $i = 3$ vanishes ($B_3 = 0$) and the term $i = 2$ is $10B_2\,3^{2N}/5 = \frac{9^N}{3}$, of valuation $2N - 1$. This is the 3-adic Riemann sum, digit by digit; Chapter 4 develops it.

3.3 Values of the Riemann zeta function

The Riemann zeta function is $\zeta(s) = \sum_{n\geq 1} n^{-s}$ for real $s > 1$ (and complex s with real part > 1), and by unique factorization it is the Euler product

$$\zeta(s) = \prod_{\ell \text{ prime}} \frac{1}{1-\ell^{-s}} = \prod_{\ell} \left(1 + \ell^{-s} + \ell^{-2s} + \dots\right) . \tag{3.5}$$

Each factor $(1-\ell^{-s})^{-1}$ is the *Euler factor* at ℓ. It collects the contributions of the powers of ℓ; removing it removes from $\sum n^{-s}$ all n divisible by ℓ:

$$(1-\ell^{-s})\,\zeta(s) = \sum_{n\geq 1,\ \ell\nmid n} n^{-s} . \tag{3.6}$$

3.3.1 Even positive integers: Euler's formula

Theorem 3.11 (Euler)**.** *For $k \geq 1$,*

$$\zeta(2k) = (-1)^{k+1} \frac{B_{2k}\,(2\pi)^{2k}}{2\,(2k)!} . \tag{3.7}$$

Derivation. We use one standard fact from complex analysis, the partial-fraction expansion of the cotangent (found in any complex analysis text, e.g. Ahlfors, *Complex Analysis*): $\pi z\cot \pi z = 1 + \sum_{n\geq 1} \frac{2z^2}{z^2-n^2}$ for $z \notin \mathbb{Z}$. It says that $\pi\cot\pi z$ is the sum of the simple poles $\frac{1}{z-n}$ over all $n \in \mathbb{Z}$, paired as $\frac{1}{z-n} + \frac{1}{z+n} = \frac{2z}{z^2-n^2}$. For $|z| < 1$ expand $\frac{z^2}{z^2-n^2} = -\sum_{k\geq 1}(z/n)^{2k}$ and sum over n:

$$\pi z\cot \pi z = 1 - 2\sum_{k\geq 1} \zeta(2k)\, z^{2k} .$$

On the other hand $\cot w = i\,\frac{e^{2iw}+1}{e^{2iw}-1} = i + \frac{2i}{e^{2iw}-1}$, so with $u = 2iw$,

$$w\cot w = iw + \frac{u}{e^u - 1} = iw + \sum_{n\geq 0} B_n \frac{u^n}{n!} = 1 + \sum_{k\geq 1} B_{2k} \frac{(2iw)^{2k}}{(2k)!} ,$$

because the term $n = 1$ is $B_1 u = -iw$ and cancels iw, and the odd terms $n \geq 3$ vanish by Proposition 3.4. Put $w = \pi z$ and use $(2i)^{2k} = (-1)^k 4^k$: the coefficient of z^{2k} is $(-1)^k B_{2k}(2\pi)^{2k}/(2k)!$. Comparing it with $-2\zeta(2k)$ gives (3.7). □

Example 3.12. (3.7) gives $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{945}$, $\zeta(8) = \frac{\pi^8}{9450}$, $\zeta(10) = \frac{\pi^{10}}{93555}$, and a 30-digit floating-point evaluation of $\zeta(2k)$ agrees with these (e.g. $\zeta(4) = 1.082323233711138191 5\dots$). For $k = 1$: $(-1)^2 \cdot \frac{1}{6} \cdot 4\pi^2/(2\cdot 2) = \frac{\pi^2}{6}$. The partial sums $\sum_{n\leq M} n^{-2}$ are 1.5498, 1.6350, 1.6439 for $M = 10, 100, 1000$, against $\pi^2/6 = 1.6449$.

3.3.2 Negative integers

The series $\sum n^{-s}$ diverges for $s \leq 1$, but ζ extends to a meromorphic function on $\mathbb{C}$ with a single simple pole at $s = 1$ (Riemann), and at the negative integers its values are again Bernoulli numbers.

Theorem 3.13 (values at negative integers)**.** *For $k \geq 2$, $\zeta(1-k) = -B_k/k$ [34, Chapter 4]. In particular $\zeta(-2) = \zeta(-4) = \cdots = 0$ (the trivial zeros), by Proposition 3.4.*

Example 3.14. $\zeta(-1) = -\frac{B_2}{2} = -\frac{1}{12}$, $\zeta(-3) = -\frac{B_4}{4} = \frac{1}{120}$, $\zeta(-5) = -\frac{1}{252}$, $\zeta(-7) = \frac{1}{240}$, and $\zeta(-2) = \zeta(-4) = \zeta(-6) = \zeta(-8) = 0$; a numerical evaluation of the analytic continuation gives the same numbers ($-0.083333\dots$, $0.0083333\dots$, $-0.0039683\dots$, $0.0041667\dots$).

Intuition: rational values, and why they matter here. $\zeta(-1) = -\frac{1}{12}$ is the "$1+2+3+\cdots = -\frac{1}{12}$" that a physicist meets in the Casimir energy or in the critical dimension of the bosonic string. The sum does not converge; $-\frac{1}{12}$ is the value of the analytic continuation, exactly as in zeta-function regularization. The point for us is that the values $\zeta(1-k)$ are *rational*. A rational number is also a 3-adic number (Chapter 2), so we can ask whether these values fit together 3-adically into a continuous function. The values at positive integers cannot be used for this: $\zeta(2k)$ is a rational multiple of π^{2k}, and the real number π has no natural counterpart in $\mathbb{Q}_3$. The 3-adic zeta function is built from the negative integers alone (Section 3.6).

3.3.3 Odd positive integers

For $\zeta(3) = 1.2020569031595942854\ldots$ and $\zeta(5) = 1.0369277551433699263\ldots$ no formula like (3.7) is known. Two remarks explain why the method above cannot produce one.

First, the cotangent is built from *all* $n \in \mathbb{Z}$, and the symmetric sum $\sum_{n\neq 0} n^{-s}$ equals $2\zeta(s)$ for even s but 0 for odd s, because n and $-n$ cancel. Any expansion of a function with poles at all integers therefore sees only the even values. Second, the functional equation of ζ relates $\zeta(s)$ to $\zeta(1-s)$, and for $s = 2k+1$ the partner is $\zeta(-2k) = 0$, a trivial zero; what the functional equation gives instead is the derivative, $\zeta'(-2k) = (-1)^k(2k)!\,\zeta(2k+1)/(2(2\pi)^{2k})$ (e.g. Apostol, *Introduction to Analytic Number Theory*, Ch. 12, for the functional equation). Numerically, $\zeta'(-2) = -0.0304484570583932\cdots = -\zeta(3)/(4\pi^2)$ and $\zeta'(-4) = 0.0079838114502686\cdots = 3\zeta(5)/(4\pi^4)$. So the odd values are not rational multiples of a power of π for any reason we can see; whether they are is not known (for instance it is not known whether $\zeta(3)/\pi^3 = 0.0387681796\ldots$ is irrational). Apéry proved $\zeta(3) \notin \mathbb{Q}$ [1], and Fauzan's preprint [15] states the irrationality of $\zeta(5)$. The note's subject is the 3-adic analogue of this question.

3.4 Denominators and congruences

The 3-adic size of every term in [note, (2.13)] is controlled by the denominators of the Bernoulli numbers, and the existence of the 3-adic zeta function is foreshadowed by congruences between them.

Theorem 3.15 (von Staudt–Clausen)**.** *For even $k \geq 2$,*

$$B_k + \sum_{p \text{ prime},\ (p-1)\mid k} \frac{1}{p} \in \mathbb{Z}\,.$$

Consequently the denominator of B_k is the product of the primes p with $(p-1) \mid k$, each to the first power. (Washington [34, Chapter 5]; Ireland–Rosen, Ch. 15.)

Example 3.16. For $k = 12$ the primes with $(p-1) \mid 12$ are $2, 3, 5, 7, 13$ ($p-1 = 1, 2, 4, 6, 12$), and indeed $B_{12} = -\frac{691}{2730}$ with $2730 = 2\cdot 3\cdot 5\cdot 7\cdot 13$; and $B_{12} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13} = 1$.

Corollary 3.17 (3-adic size of Bernoulli numbers)**.** *For every prime p and every $n \geq 0$, $v_p(B_n) \geq -1$. For $p = 3$ and even $n \geq 2$, $v_3(B_n) = -1$ exactly.*

Proof. For even $n \geq 2$ the denominator is squarefree by Theorem 3.15, so $v_p(B_n) \geq -1$; and $p = 3$ always qualifies, because $p - 1 = 2$ divides every even n. For odd $n \geq 3$, $B_n = 0$ and $v_p = \infty$; $B_0 = 1$ and $B_1 = -\frac{1}{2}$ have $v_p \geq -1$ as well. □

Intuition: why $p = 3$ is special. At a prime $p \geq 5$ only every $(p-1)$-st Bernoulli number has p in its denominator; at $p = 3$ every even one does. This uniform factor $\frac{1}{3}$ is harmless

(it costs one digit everywhere), but it changes the bookkeeping: at $p = 3$ all even k lie on the branch of the 3-adic zeta function that has the pole at $s = 1$ (Section 3.6).

Theorem 3.18 (Kummer congruences)**.** *Let p be a prime, and let k, k' be positive even integers with $k \equiv k' \not\equiv 0 \pmod{p-1}$. If $k \equiv k' \pmod{(p-1)p^{m-1}}$, then*

$$(1 - p^{k-1})\frac{B_k}{k} \equiv (1 - p^{k'-1})\frac{B_{k'}}{k'} \pmod{p^m} ,$$

that is, the difference has p-adic valuation at least m ([34, Chapter 5]; both sides are p-adic integers under the hypothesis).

Example 3.19 ($p = 5$)**.** Put $x_k = -(1-5^{k-1})B_k/k$. Here $p-1 = 4$, and $k = 2, 22, 102, 502$ are all $\equiv 2 \pmod 4$, with $22-2 = 4\cdot 5$, $102-2 = 4\cdot 5^2$, $502-2 = 4\cdot 5^3$. One finds $v_5(x_{22} - x_2) = 2$, $v_5(x_{102} - x_2) = 3$, $v_5(x_{502} - x_2) = 4$, exactly the levels $m = 2, 3, 4$ that the theorem predicts. Without the factor $(1 - 5^{k-1})$ the congruence is weaker: $v_5(B_{22}/22 - B_2/2) = 1$ only. And the hypothesis $k \not\equiv 0 \pmod 4$ matters: $v_5(B_4) = -1$ (by von Staudt–Clausen, since $4 \mid 4$), so $B_4/4$ is not even a 5-adic integer.

Intuition: continuity in the exponent. The Kummer congruences say: if two exponents k, k' are close p-adically (their difference divisible by a high power of p) and lie in the same class modulo $p-1$, then the numbers $(1 - p^{k-1})B_k/k$ are close p-adically. So $k \mapsto (1 - p^{k-1})B_k/k$ is a *uniformly continuous* function of k for the p-adic distance, on each class modulo $p-1$. A uniformly continuous function on a dense set extends to its closure. This is the Kubota–Leopoldt function of Section 3.6, and the next two sections explain the two features of the statement: the class modulo $p-1$ (Section 3.5) and the factor $(1 - p^{k-1})$ (Section 3.6).

The case $p = 3$. At $p = 3$ the hypothesis $k \not\equiv 0 \pmod 2$ excludes every even k, so Theorem 3.18 says nothing; this is the pole of Section 3.6. Numerically a weaker statement survives. With $x_k = -(1 - 3^{k-1})B_k/k$ (which has $v_3(x_k) = -1$ when $3 \nmid k$), one finds $v_3(x_{k+2\cdot 3^m} - x_k) = m - 1$ for $k = 2, 4, 8, 10$ and $m = 1, \dots, 5$: one level less than at $p = 5$, which is the price of the denominator 3. When k itself becomes divisible by a high power of 3, x_k blows up: $v_3(x_{2\cdot 3^N}) = -1 - N$ for $N = 0, \dots, 6$. Both observations are explained by [note, (2.3)] below; they are stated here only for the listed cases.

3.5 Dirichlet characters and the Teichmüller character

Definition 3.20 (Dirichlet character)**.** A *Dirichlet character modulo F* is a function $\chi : \mathbb{Z} \to \mathbb{C}$ with $\chi(a + F) = \chi(a)$, $\chi(ab) = \chi(a)\chi(b)$, $\chi(1) = 1$, and $\chi(a) = 0$ exactly when $\gcd(a, F) > 1$. Its *conductor* f is the smallest modulus from which it comes (it is *primitive* if $f = F$). It is *even* if $\chi(-1) = 1$ and *odd* if $\chi(-1) = -1$. The trivial character, $\mathbf{1}(a) = 1$ for all a, has conductor 1.

Example 3.21 (the characters modulo 3)**.** Since $(\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$ has two elements, there are two characters modulo 3: the trivial one viewed modulo 3 ($1, 1, 0$ on $a \equiv 1, 2, 0$), and χ_{-3} with $\chi_{-3}(a) = +1, -1, 0$ for $a \equiv 1, 2, 0 \pmod 3$. The second is primitive of conductor 3 and odd, $\chi_{-3}(-1) = \chi_{-3}(2) = -1$; it is the Legendre symbol $\left(\frac{a}{3}\right)$.

Intuition: characters as Fourier modes. A Dirichlet character is a homomorphism from the multiplicative group $(\mathbb{Z}/F\mathbb{Z})^\times$ to the unit circle, a "plane wave" on that finite

group. Twisting a sum $\sum_n n^{-s}$ by $\chi(n)$ picks out one Fourier mode of the residue classes, as a Bloch phase picks out one momentum. For us only two characters ever appear, $\mathbf{1}$ and χ_{-3}.

The Teichmüller character is a character with values in $\mathbb{Z}_p$ rather than $\mathbb{C}$.

Definition 3.22 (Teichmüller character)**.** For a prime p and $a \in \mathbb{Z}_p$ with $p \nmid a$, $\omega(a) = \lim_{N\to\infty} a^{p^N}$ in $\mathbb{Z}_p$. It is the unique $(p-1)$-st root of unity in $\mathbb{Z}_p$ congruent to a modulo p. For $p \mid a$, $\omega(a) = 0$. We write $\langle a\rangle = a/\omega(a)$, so that $a = \omega(a)\langle a\rangle$ with $\langle a\rangle \equiv 1 \pmod p$.

That the limit exists: by Fermat $a^{p-1} = 1 + pb$ with $b \in \mathbb{Z}_p$, and raising $1 + pb$ to the power p gains one factor of p in the difference from 1 (binomial theorem), so $a^{p^{N+1}} - a^{p^N} = a^{p^N}\left((a^{p-1})^{p^N} - 1\right)$ has valuation at least $N + 1$; the sequence is Cauchy (Koblitz, Ch. I, or [34, Chapter 5]). The limit w satisfies $w^p = w$, so $w^{p-1} = 1$, and $w \equiv a \pmod p$ because $a^p \equiv a$.

Example 3.23 ($p = 3$)**.** The roots of unity of order dividing 2 in $\mathbb{Z}_3$ are ± 1, so

$$\omega(a) = \begin{cases} +1, & a \equiv 1 \pmod 3, \\ -1, & a \equiv 2 \pmod 3, \end{cases} \qquad \langle a\rangle = \pm a \in 1 + 3\mathbb{Z}_3 \ .$$

As a Dirichlet character this is χ_{-3} of Example 3.21. A table of values:

a	1	2	4	5	7	8	10	11
$\omega(a)$	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1
$\langle a\rangle$	1	-2	4	-5	7	-8	10	-11
$v_3(\langle a\rangle - 1)$	∞	1	1	1	1	2	2	1

The definition by a limit works as claimed: $v_3(2^{3^N} + 1) = N + 1$ for $N = 0, \dots, 6$ ($2 + 1 = 3$, $8 + 1 = 9$, $512 + 1 = 513 = 27 \cdot 19$, …), so $2^{3^N} \to -1 = \omega(2)$.

Example 3.24 ($p = 5$, for contrast)**.** At $p = 5$, ω takes the four values $\pm 1, \pm i$, where $i \in \mathbb{Z}_5$ is a square root of -1 (it exists in $\mathbb{Z}_5$, by Hensel's lemma, since $2^2 \equiv -1 \pmod 5$). One finds $2^{5^N} \bmod 5^8 = 2, 32, 351307, 323307, 105182, 186432, 202057, 280182$ for $N = 0, \dots, 7$; the last value $\omega(2) \equiv 280182$ has 5-adic digits $2, 1, 2, 1, 3, 4, 2, 3$, and the truncation satisfies $v_5(280182^2 + 1) = 9 > 8$ (while $\omega(2)^2 + 1 = 0$ exactly). So at $p = 5$ the Teichmüller character has order 4, at $p = 3$ order 2.

Intuition: why ω is needed. For $p \nmid a$ the factorization $a = \omega(a)\langle a\rangle$ splits a into a "phase" $\omega(a)$ (a root of unity) and a "modulus" $\langle a\rangle \in 1 + p\mathbb{Z}_p$. Then $a^k = \omega(a)^k\langle a\rangle^k$. The modulus part is continuous in the exponent: $\langle a\rangle^s = \exp(s \log\langle a\rangle)$ makes sense for $s \in \mathbb{Z}_p$ and is close to $\langle a\rangle^k$ when s is close to k. The phase part is not: $\omega(a)^k$ depends only on k modulo $p - 1$, and jumps as k moves from one class to the next. At $p = 3$ the phase is the sign $(\pm 1)^k$, and for even k it disappears: $a^k = \langle a\rangle^k$. So the even exponents k form a single family, and the function $k \mapsto a^k$ on them extends continuously to $k \in \mathbb{Z}_3$. This is the origin of the "class modulo $p - 1$" in the Kummer congruences.

Definition 3.25 (generalized Bernoulli numbers)**.** For a Dirichlet character χ of conductor f,

$$\sum_{a=1}^{f} \chi(a) \frac{t\, e^{at}}{e^{ft} - 1} = \sum_{k \ge 0} B_{k,\chi} \frac{t^k}{k!} \ , \qquad \text{equivalently} \qquad B_{k,\chi} = f^{k-1} \sum_{a=1}^{f} \chi(a)\, B_k\Big(\frac{a}{f}\Big) \ .$$

The two forms agree by (3.3) with $t \to ft$ and $x = a/f$: $\frac{te^{at}}{e^{ft}-1} = \frac{1}{f}\cdot\frac{(ft)e^{(a/f)(ft)}}{e^{ft}-1} = \frac{1}{f}\sum_k B_k(\frac{a}{f})\frac{f^k t^k}{k!}$. For $\chi = \mathbf{1}$ ($f = 1$), $B_{k,\mathbf{1}} = B_k(1)$, which equals B_k except for $B_{1,\mathbf{1}} = +\frac{1}{2}$ (by the difference identity, $B_k(1) = B_k(0) + [k = 1]$). For χ odd, $B_{k,\chi} = 0$ for even k, by the reflection identity applied to $a \mapsto f - a$.

Example 3.26 ($\chi = \omega$ at $p = 3$)**.** With $f = 3$, $B_{k,\omega} = 3^{k-1}(B_k(\frac{1}{3}) - B_k(\frac{2}{3}))$. By hand, $B_{1,\omega} = (\frac{1}{3} - \frac{1}{2}) - (\frac{2}{3} - \frac{1}{2}) = -\frac{1}{3}$ and $B_{3,\omega} = 9(\frac{1}{27} + \frac{1}{27}) = \frac{2}{3}$, using Example 3.6. Continuing, $B_{1,\omega}, \dots, B_{8,\omega} = -\frac{1}{3}, 0, \frac{2}{3}, 0, -\frac{10}{3}, 0, \frac{98}{3}, 0$.

We need these numbers only to read [note, (2.2)]; the note's computations use only $\chi = \mathbf{1}$.

3.6 The Kubota–Leopoldt p-adic L-function

3.6.1 The statement

The note takes the following theorem from Washington. We state it as the note does. Here $\mathbb{C}_p$ is the completion of an algebraic closure of $\mathbb{Q}_p$, the p-adic analogue of $\mathbb{C}$; we shall only evaluate at $s \in \mathbb{Z}_3$.

Theorem 3.27 (Kubota–Leopoldt; [note, Theorem 2.1])**.** *Let p be an odd prime, χ a Dirichlet character of conductor f, and F a common multiple of p and f. There is a p-adic meromorphic function $L_p(s,\chi)$ on $\{s \in \mathbb{C}_p : |s|_p < p^{(p-2)/(p-1)}\}$, analytic if $\chi \neq \mathbf{1}$ and with only a simple pole at $s = 1$ if $\chi = \mathbf{1}$, such that*

$$L_p(1-k,\chi) = -(1 - \chi\omega^{-k}(p)\,p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k} \qquad (k \geq 1)\ , \tag{3.8}$$

and

$$L_p(s,\chi) = \frac{1}{F}\,\frac{1}{s-1}\sum_{\substack{1\leq a\leq F\\ p\nmid a}} \chi(a)\langle a\rangle^{1-s}\sum_{j\geq 0}\binom{1-s}{j}\Big(\frac{F}{a}\Big)^j B_j\ . \tag{3.9}$$

The note cites it from [34, Section 5.2]. We do not prove it; Example 3.28 below shows that (3.8) and (3.9) are consistent with each other in the cases computed there. In (3.8), $\chi\omega^{-k}$ means the primitive character attached to the product, as in Washington; in particular for the trivial character $\mathbf{1}(p) = 1$, while a character of conductor divisible by p has value 0 at p.

Reading (3.8) at $p = 3$, $\chi = \mathbf{1}$. Since ω has order 2, $\omega^{-k} = \mathbf{1}$ for even k and $\omega^{-k} = \omega$ for odd k. So

$$L_3(1-k,\mathbf{1}) = \begin{cases} -(1-3^{k-1})\,\dfrac{B_k}{k} = (1-3^{k-1})\,\zeta(1-k), & k \text{ even},\\[2mm] -\dfrac{B_{k,\omega}}{k}, & k \text{ odd (since } \omega(3) = 0). \end{cases} \tag{3.10}$$

Example 3.28 (the two formulas agree)**.** At $s = 1 - k$ the series (3.9) is finite: $\binom{k}{j} = 0$ for $j > k$. With $p = F = 3$, $\chi = \mathbf{1}$, $a \in \{1, 2\}$, $\langle 1\rangle = 1$, $\langle 2\rangle = -2$, it reads

$$L_3(1-k,\mathbf{1}) = -\frac{1}{3k}\sum_{a=1,2}\langle a\rangle^k\sum_{j=0}^{k}\binom{k}{j}\Big(\frac{3}{a}\Big)^j B_j\ .$$

For $k = 1$: $-\frac{1}{3}[1\cdot(1-\frac{3}{2}) + (-2)(1-\frac{3}{4})] = -\frac{1}{3}[-\frac{1}{2} - \frac{1}{2}] = \frac{1}{3}$, and (3.10) gives $-B_{1,\omega} = \frac{1}{3}$. For $k = 2$, (3.10) gives $-(1-3)\frac{1/6}{2} = \frac{1}{6}$. Evaluating both formulas exactly for $k = 1, \dots, 10$, one finds them equal:

k	1	2	3	4	5	6	7	8	9	10
$L_3(1-k,\mathbf{1})$	$\frac{1}{3}$	$\frac{1}{6}$	$-\frac{2}{9}$	$-\frac{13}{60}$	$\frac{2}{3}$	$\frac{121}{126}$	$-\frac{14}{3}$	$-\frac{1093}{120}$	$\frac{1618}{27}$	$\frac{9841}{66}$

In particular, (3.9) in the form printed in the note [note, (2.3)] reproduces the interpolation values in these cases.

Intuition: what the theorem says. Take $p=3$ and even k. The rational numbers $(1-3^{k-1})\zeta(1-k)$, $k=2,4,6,\dots$, are points of $\mathbb{Q}_3$ labelled by $s=1-k$. The theorem says that they all lie on the graph of one 3-adic analytic function of s, the way the values of $\sin x$ at the integers lie on the graph of sin. Since $\{1-k : k \text{ even} \geq 2\}$ is dense in $\mathbb{Z}_3$ (every 3-adic integer is a limit of odd negative integers), the function is determined by these values, and its value at any other $s \in \mathbb{Z}_3$, for instance $s=5$, is a limit of them. The formula (3.9) is a closed form for this function that can be evaluated at any s directly, as one evaluates $\sin x$ by its Taylor series rather than by interpolating.

3.6.2 Why the Euler factor at p is removed

In (3.6), $(1-p^{-s})\zeta(s) = \sum_{p\nmid n} n^{-s}$; at $s=1-k$ this is the factor $(1-p^{k-1})$ of (3.10). The reason is that n^{k-1}, as a function of k, is p-adically continuous when $p\nmid n$ (on a class modulo $p-1$, by the intuition box above), but not when $p \mid n$.

Example 3.29. Let $k_N = 2\cdot 3^N - 4$, so that $k_N \to -4$ in $\mathbb{Z}_3$ (because $2\cdot 3^N \to 0$). For $n=2$ the powers behave continuously: $v_3(2^{k_N}-2^{-4}) = N+1$ for $N=1,\dots,6$, so $2^{k_N}\to\frac{1}{16}$. For $n=3$ they do not: $3^{k_N}\to 0$ in $\mathbb{Q}_3$, while $3^{-4}=\frac{1}{81}$ has $|3^{-4}|_3 = 81$; one finds $v_3(3^{k_N}-3^{-4}) = -4$ for every N. So any sum over n that is to be continuous in the exponent must leave out the multiples of 3, which is what removing the Euler factor does. The effect is visible in the congruences: for $k=2$ and $k' = 2+2\cdot 3^4 = 164$ one finds $v_3(x_{164}-x_2)=3$ with the factor $(1-3^{k-1})$ and $v_3(\frac{B_{164}}{164}-\frac{B_2}{2})=0$ without it.

For large k the factor is 3-adically close to 1 ($v_3(3^{k-1})=k-1$), so it does not change limits along sequences $k\to\infty$; what it changes is the values at small k, without which the points would not lie on one continuous curve.

Remark 3.30 ($\zeta_3(5)$ is not $\sum n^{-5}$). There is no 3-adic series $\sum_{3\nmid n} n^{-5}$ to define $\zeta_3(5)$ directly: its terms have $|n^{-5}|_3 = 1$ and do not tend to 0, so it diverges in $\mathbb{Q}_3$ (Chapter 2). The value $\zeta_3(5)$ exists only through the continuation from the negative integers, or equivalently through (3.9).

3.6.3 Branches, the twist, and $\zeta_p(s)$

For a general prime p, the values $(1-p^{k-1})\zeta(1-k)$ fall into $p-1$ families according to $k \bmod (p-1)$, and each family lies on a different analytic function; these are the *branches*. By (3.8) with $\chi=\omega^i$, the function $L_p(s,\omega^i)$ passes through $-(1-p^{k-1})B_k/k$ at exactly those $s=1-k$ with $k\equiv i \pmod{p-1}$ (then $\omega^i\omega^{-k}=\mathbf{1}$); at the other k it takes the twisted values $-B_{k,\omega^{i-k}}/k$. The *p-adic zeta value* at an integer s is defined by choosing the branch that matches s [note, Section 1]:

$$\zeta_p(s) = L_p(s,\omega^{1-s})\ . \tag{3.11}$$

At $s=1-k$ this gives $L_p(1-k,\omega^k) = -(1-p^{k-1})B_k/k = (1-p^{k-1})\zeta(1-k)$ for every $k\geq 2$, the Euler-factor-removed zeta value. At $p=3$ there are two branches, $L_3(s,\mathbf{1})$ (even k) and $L_3(s,\omega)$ (odd k), and for $s=5$, $\omega^{1-5}=\omega^{-4}=\mathbf{1}$, so

$$\zeta_3(5) = L_3(5,\mathbf{1}) \qquad \text{[note, (2.4)]}\ . \tag{3.12}$$

Intuition: why $s = 5$ lies on the even branch. The point $s = 5$ is a 3-adic limit of points $s = 1 - k$ with k even, for example $s_N = 1 - k_N = 5 - 2 \cdot 3^N$ with $k_N = 2 \cdot 3^N - 4$: $|s_N - 5|_3 = |2 \cdot 3^N|_3 = 3^{-N} \to 0$. At these points the function $L_3(s, \mathbf{1})$ takes the zeta values $-(1 - 3^{k_N - 1})B_{k_N}/k_N$, so $\zeta_3(5)$ is their limit. Points $1 - k$ with k odd also approach 5 (for example $k = 3^N - 4$), but at those points $L_3(s, \mathbf{1})$ takes the twisted values $-B_{k,\omega}/k$ of (3.10), not zeta values; the zeta values with odd k (all 0 for $k \geq 3$) lie on the other function $L_3(s, \omega)$. The choice of χ in $L_3(s, \chi)$ is the choice of which family of zeta values, even or odd k, the function passes through; the definition $\zeta_p(s) = L_p(s, \omega^{1-s})$ picks the family to which $1 - s$ belongs, here $1 - 5 = -4$, even.

Remark 3.31 (the even 3-adic zeta values vanish). For even s, $\zeta_3(s) = L_3(s, \omega)$. By (3.8) with $\chi = \omega$, $L_3(1 - k, \omega)$ is $-(1 - 3^{k-1})B_{k,\mathbf{1}}/k$ for odd k, which is 0 (for $k = 1$ the factor $1 - 3^0$ vanishes; for odd $k \geq 3$, $B_k = 0$), and $-B_{k,\omega}/k = 0$ for even k (Example 3.26). Evaluating (3.9) with $\chi = \omega$ at $s = 1 - k$, $k = 1, \ldots, 10$, gives 0 every time as well. An analytic function vanishing on a set with an accumulation point vanishes identically, so $L_3(s, \omega) = 0$ and $\zeta_3(2), \zeta_3(4), \ldots$ are all 0. This is the mirror image of the real case, where the even values are the explicit ones. It is also why the note's reflection [note, Lemma 2.9] "removes the even zeta values" (Chapter 4).

Intuition: the pole at $s = 1$. $L_3(s, \mathbf{1})$ has a pole at $s = 1$, i.e. at "$k = 0$". The points $k = 2 \cdot 3^N$ approach $k = 0$ 3-adically, and the values there blow up: $v_3(x_{2 \cdot 3^N}) = -1 - N$ (Section 3.4), i.e. $|x_{2 \cdot 3^N}|_3 = 3^{N+1} = 3/|k|_3$, as a simple pole $\propto 1/(s - 1)$ predicts. In (3.9) the pole is the prefactor $\frac{1}{s-1}$, and the prefactor $\frac{1}{F} = \frac{1}{3}$ explains the lost digit in the $p = 3$ congruences: a change of s by δ changes L_3 by roughly $|\delta|_3$ times $|\frac{1}{3}|_3 = 3$ (this is our reading, consistent with all cases computed, not a proved estimate).

3.7 Computing $\zeta_3(5)$ in two ways

3.7.1 Route (i): a limit of Bernoulli numbers

By (3.10) and the intuition box on $s = 5$, with $k_N = 2 \cdot 3^N - 4$,

$$\zeta_3(5) = \lim_{N \to \infty} x_{k_N} , \qquad x_k = -(1 - 3^{k-1}) \frac{B_k}{k} . \tag{3.13}$$

Two things make this legitimate: k_N is even, so these points lie on the branch $L_3(s, \mathbf{1})$; and $s_N = 1 - k_N \to 5$ in $\mathbb{Z}_3$, where $L_3(s, \mathbf{1})$ is analytic (its only pole is at $s = 1$, and 5 lies in the disc $|s|_3 < 3^{1/2}$ of Theorem 3.27), hence continuous. Each x_{k_N} is an explicit rational number, and since $3 \nmid k_N$ and $v_3(B_{k_N}) = -1$, it has $v_3(x_{k_N}) = -1$.

Example 3.32 (route (i))**.** For $N = 1$, $k_1 = 2$ and $x_2 = -(1 - 3)\frac{1/6}{2} = \frac{1}{6}$, whose 3-adic expansion is $\frac{1}{6} = 2 \cdot 3^{-1} + 1 + 3 + 3^2 + \ldots$ (because $\frac{1}{2} = \ldots 1112$, Chapter 2). We compute B_{k_N} exactly up to $N = 11$, $k_{11} = 354290$ (whose numerator has more than a million digits), reduce $3x_{k_N}$ modulo 3^{60} and compare the digits $a_{-1}, a_0, a_1, \ldots$ of $x_{k_N} = \sum_i a_i 3^i$ with those of route (ii) below. Digits are listed from a_{-1} on, left to right:

N	k_N	digits $a_{-1}a_0a_1\ldots$ of x_{k_N}	agreeing digits
1	2	211111111111111111111	1
2	14	2020202020202111111111	2
3	50	2010022211202211111020	3
4	158	2012211112010111210110	4
5	482	2012111202121002212202	5
6	1454	2012101210202111100201	6
7	4370	2012100211001211201022	7
8	13118	2012100111110002102200	8
9	39362	2012100101121202220202	9
10	118094	2012100100122000001120	10
11	354290	2012100100022112001022	11

So x_{k_N} agrees with $\zeta_3(5)$ in exactly N digits, $a_{-1},\ldots,a_{N-2}$, i.e. $v_3(x_{k_N}-\zeta_3(5))=N-1$ for $N=1,\ldots,11$, while $|s_N-5|_3=3^{-N}$. Route (i) is slow: each new digit triples the size of k.

Remark 3.33 (the odd points of the same function). The same function $L_3(s,\mathbf{1})$ can be approached through odd k. With $k=3^N-4$ (odd, and $1-k=5-3^N\to 5$), (3.10) gives the values $-B_{k,\omega}/k$. For $N=2,\ldots,7$ ($k=5,23,77,239,725,2183$) each of them has $v_3=-1$ and agrees with route (ii) below in exactly N digits ($-B_{5,\omega}/5=\frac{2}{3}$ for $N=2$, which matches the first two digits $2,0$). So both families of points, the zeta values at even k and the twisted values at odd k, lie on one function and converge to the same $\zeta_3(5)$, as Theorem 3.27 asserts.

3.7.2 Route (ii): the series [note, (2.13)]

Take $p=F=3$, $\chi=\mathbf{1}$, $s=5$ in (3.9). The sum runs over $a\in\{1,2\}$; $1-s=-4$ is even, so $\langle a\rangle^{-4}=(a/\omega(a))^{-4}=a^{-4}$ because $\omega(a)^4=1$; and $\frac{1}{F}\frac{1}{s-1}=\frac{1}{12}$. So

$$12\,\zeta_3(5)=12\,L_3(5,\mathbf{1})=\sum_{a=1,2}a^{-4}\sum_{c\ge 0}\binom{-4}{c}\Big(\frac{3}{a}\Big)^c B_c\,, \tag{3.14}$$

which is [note, (2.13)] with $m=4$. Here $\binom{-4}{c}=\frac{(-4)(-5)\cdots(-3-c)}{c!}=(-1)^c\binom{c+3}{3}$, an integer.

Lemma 3.34 (truncation). *Let $T_c=\sum_{a=1,2}a^{-4}\binom{-4}{c}(3/a)^cB_c$ be the c-th term of (3.14). Then $v_3(T_c)\ge c-1$. Consequently, truncating (3.14) after the term $c=C$ determines $12\zeta_3(5)$ modulo 3^C, i.e. $\zeta_3(5)$ modulo 3^{C-1}, i.e. its C digits $a_{-1},\ldots,a_{C-2}$.*

Proof. For each $a\in\{1,2\}$: $v_3(a^{-4})=0$; $v_3\binom{-4}{c}\ge 0$ because it is an integer; $v_3((3/a)^c)=c$; and $v_3(B_c)\ge -1$ by Corollary 3.17. Adding, each of the two summands has valuation at least $c-1$, and by the ultrametric inequality so does T_c. The tail $\sum_{c>C}T_c$ consists of terms of valuation at least C, so (passing to the limit in the ultrametric inequality, as in Chapter 2) it has valuation at least C; this is also why the series converges. Hence $12\zeta_3(5)\equiv\sum_{c\le C}T_c \pmod{3^C}$. Since $12=3\cdot 4$ with 4 a 3-adic unit, dividing by 12 lowers the valuation by 1, which gives $\zeta_3(5)$ modulo 3^{C-1}. The digits a_i with $i\le C-2$ are determined by $\zeta_3(5)$ modulo 3^{C-1}. □

Example 3.35 (the first terms, and $v_3(\zeta_3(5))=-1$). The first terms are

c	0	1	2	3	4	5	6
T_c	$\frac{17}{16}$	$\frac{99}{16}$	$\frac{975}{64}$	0	$-\frac{48573}{512}$	0	$\frac{747225}{512}$
$v_3(T_c)$	0	2	1	∞	3	∞	6
bound $c-1$	-1	0	1	2	3	4	5

By hand: $T_0 = 1+\frac{1}{16} = \frac{17}{16}$; $T_1 = \sum_a a^{-4}\cdot(-4)\cdot\frac{3}{a}\cdot(-\frac{1}{2}) = 6(1+\frac{1}{32}) = \frac{99}{16}$; $T_2 = \sum_a a^{-4}\cdot 10\cdot\frac{9}{a^2}\cdot\frac{1}{6} = 15(1+\frac{1}{64}) = \frac{975}{64}$. The bound of Lemma 3.34 holds for all $c \le 62$, and is attained for several c (e.g. $c = 2, 4, 10$); for $c = 10, \dots, 30$ the actual valuations $(9, 11, 13, 16, 17, 19, 21, 25, 27, 27, 29$ for even c) exceed it by 0 to 2.

The term $c = 0$ alone fixes the size of $\zeta_3(5)$: $v_3(T_0) = 0$ and $v_3(T_c) \ge 1$ for all $c \ge 1$, so $v_3(12\zeta_3(5)) = 0$ by Chapter 2's rule that the smallest valuation wins when it is unique, and $v_3(\zeta_3(5)) = -1$. The first two digits follow from the terms of valuation < 2: modulo 9, $3\zeta_3(5) = \frac{12\zeta_3(5)}{4} \equiv \frac{1}{4}(\frac{17}{16} + \frac{975}{64}) = \frac{1043}{256} \equiv \frac{8}{4} \equiv 2 \pmod 9$ (as $1043 \equiv 8$ and $256 \equiv 4 \pmod 9$), so $a_{-1} = 2$, $a_0 = 0$.

Example 3.36 (route (ii): 62 digits)**.** With $C = 62$, Lemma 3.34 gives the digits $a_{-1}, \dots, a_{60}$ of $\zeta_3(5) = \sum_{i \ge -1} a_i 3^i$. In groups of ten from a_{-1}, they are:

```
2012100100 0110101121 2110202000 2101020100 0110022221 0020111110 20
```

that is,

$$\zeta_3(5) = \frac{2}{3} + 0 + 1\cdot 3 + 2\cdot 3^2 + 1\cdot 3^3 + 0\cdot 3^4 + 0\cdot 3^5 + 1\cdot 3^6 + 0\cdot 3^7 + 0\cdot 3^8 + 0\cdot 3^9 + \dots$$

In the right-to-left notation of Chapter 2 (least significant digit on the right, a point before a_{-1}) the first 20 digits read $\dots 12110101100010012 10.2$.

3.7.3 Agreement

The two routes agree on every digit that route (i) determines: for each $N = 1, \dots, 11$, the first N digits of x_{k_N} coincide with those of route (ii), and the $(N+1)$-st differs (table in Example 3.32). The two computations share only the Bernoulli numbers and the statement of Theorem 3.27: route (i) uses (3.8) and the continuity of L_3, with B_k for k up to 354290; route (ii) uses (3.9) with B_c for $c \le 62$ from the recursion (3.2). The agreement is therefore a consistency check: it shows that [note, (2.2)], [note, (2.3)] and [note, (2.4)] fit together at $s = 5$, to 11 digits.

In the note, the series (3.14) reappears in the proof of the value lemma [note, Lemma 2.11], where each B_c is recognized as $\int_{\mathbb{Z}_3} t^c\,\mathrm{d}t$ and the series is summed back into the Volkenborn integral $\zeta_3(5) = \frac{1}{972}\sum_{r=1,2}\int_{\mathbb{Z}_3}(t+\frac{r}{3})^{-4}\,\mathrm{d}t$; this is the subject of Chapter 4.

Check yourself 3.37. Why does route (ii) gain one digit per term while route (i) needs k to triple for each digit?

Answer. In route (ii) the c-th term carries $(3/a)^c$, so each term is (at least) one factor of 3 smaller than the previous one. In route (i) the accuracy is $|s_N - 5|_3$ (up to the factor 3 discussed above), and $s_N = 1 - k_N$ approaches 5 only when $k_N + 4$ is divisible by a higher power of 3, which requires k_N to grow geometrically.

3.8 What "$\zeta_3(5)$ is irrational" means

$\zeta_3(5)$ is an element of $\mathbb{Q}_3$ with valuation -1, and $\mathbb{Q} \subset \mathbb{Q}_3$. [note, Theorem 1.1] asserts that $\zeta_3(5) \notin \mathbb{Q}$: there are no integers a, b with $b \ne 0$ and $b\,\zeta_3(5) = a$ in $\mathbb{Q}_3$. By the characterization of rational p-adic numbers in Chapter 2, this is equivalent to: the digit sequence $a_{-1}, a_0, a_1, \dots$ is not eventually periodic.

No finite computation can decide this. A rational number a/b with large b can have a long pre-period and a period of length up to about b, so 62 digits without visible repetition are consistent with both answers and are no evidence either way. The note's argument is of a different kind: assuming $\zeta_3(5) = a/b$, it builds nonzero integers that are divisible by a high

power of 3 but too small in absolute value to be so (Chapter 1). In that argument $\zeta_3(5)$ enters only through its representation as a Volkenborn integral [note, Lemma 2.11], which rests on [note, (2.3)] and [note, (2.4)] as explained here. The computed digits play no role in the proof; they show concretely which number the theorem is about.

Check yourself 3.38. Is $\zeta_3(5)$ the 3-adic limit of the real numbers $\sum_{n\le M} n^{-5}$, or of $\sum_{n\le M,\,3\nmid n} n^{-5}$?

Answer. Neither. The partial sums are rational, so the question makes sense, but the terms n^{-5} with $3\nmid n$ have $|n^{-5}|_3 = 1$, so the sums do not converge in $\mathbb{Q}_3$ at all. $\zeta_3(5)$ is obtained by continuing $(1-3^{k-1})\zeta(1-k)$ from $s = 1-k$ to $s = 5$, not by summing n^{-5}.

Summary of the chapter

Bernoulli numbers are the Taylor coefficients of $t/(e^t-1)$; the odd ones beyond B_1 vanish, and by von Staudt–Clausen every even one has exactly one factor 3 in its denominator, so $v_3(B_n) \ge -1$ for all n. Bernoulli polynomials are discrete antiderivatives of powers, which gives Faulhaber's formula and with it $\int_{\mathbb{Z}_3} t^c\,\mathrm{d}t = B_c$ (V2). Euler's formula expresses $\zeta(2k)$ through B_{2k} and π^{2k}, and $\zeta(1-k) = -B_k/k$ is rational; no such formula is known for $\zeta(3)$ or $\zeta(5)$. The Kummer congruences say that the Euler-factor-removed values $(1-p^{k-1})\zeta(1-k)$ depend p-adically continuously on k within a class modulo $p-1$; the Kubota–Leopoldt function $L_p(s,\chi)$ [note, Theorem 2.1] is the analytic function through these points, with the Teichmüller character ω labelling the classes. At $p=3$, $\omega(a) = \pm 1$ according to a mod 3, and $\zeta_3(5) = L_3(5,\mathbf{1})$ [note, (2.4)].

Carried forward: the series [note, (2.13)], $12\zeta_3(5) = \sum_{a=1,2} a^{-4} \sum_c \binom{-4}{c}(3/a)^c B_c$, with terms of valuation at least $c-1$ (Chapter 4 turns it into the Volkenborn integral $\zeta_3(5) = \frac{1}{972}\sum_r \int_{\mathbb{Z}_3} (t+\frac{r}{3})^{-4}\mathrm{d}t$); the facts $v_3(\zeta_3(5)) = -1$ and $v_3(B_n) \ge -1$; the reflection identity $B_k(1-x) = (-1)^k B_k(x)$ (used in [note, Lemma 2.9]); and the digits $\zeta_3(5) = \frac{2}{3} + 0 + 1\cdot 3 + 2\cdot 3^2 + \ldots$, computed to 62 digits by [note, (2.13)] and confirmed to 11 digits by the limit of $-(1-3^{k-1})B_k/k$ along $k = 2\cdot 3^N - 4$.

Chapter 4

The Volkenborn integral

Where we are. Chapter 3 produced $\zeta_3(5)$ as the value of a series of Bernoulli numbers [note, (2.13)]. This chapter rewrites that series as an integral over $\mathbb{Z}_3$ of a rational function, $\zeta_3(5) = \frac{1}{972}\sum_{r=1,2}\int_{\mathbb{Z}_3}(t+\frac{r}{3})^{-4}\,\mathrm{d}t$ [note, Lemma 2.11], and computes the whole family of basic integrals $\sum_{r=1,2}\int_{\mathbb{Z}_3}(t+\frac{r}{3}+k)^{-m}\,\mathrm{d}t$ for $k\in\mathbb{Z}$, $m\geq 1$ [note, Lemma 2.15]. These basic integrals are all that the functional L of Chapter 5 ever evaluates. We cover the second half of [note, Section 2.1]: strict differentiability, the definition [note, (2.5)], the three properties (V1)–(V3) [note, Lemma 2.6] with the Riemann-sum difference [note, (2.7)], the set S [note, (2.8)], the reflection lemma [note, Lemma 2.9], the value lemma [note, Lemma 2.11], the harmonic sums $\mathrm{HS}_3(k,M)$ [note, (2.14)] and the translation lemma [note, Lemma 2.15]. From Chapter 2 we use v_3, $|\cdot|_3$, digit expansions, the convergence test for series, the inequality $|x^m-y^m|_3\leq|x-y|_3$ on $\mathbb{Z}_3$ and the set $S=3^{-1}\mathbb{Z}_3^{\times}$; from Chapter 3 the Bernoulli numbers and polynomials, Faulhaber's formula, the identity $B_k(1-x)=(-1)^kB_k(x)$ and the series [note, (2.13)]. In the numerical examples every integral is approximated by its defining Riemann sums, computed in exact rational arithmetic or exactly modulo 3^{60}.

4.1 Why an integral?

The proof of the note is a Hankel-determinant argument (Chapter 1). One needs a linear functional L on polynomials, the matrix of its moments $L(y^{i+j})$, and its determinant. For the argument to say anything about $\zeta_3(5)$, every moment must be of the form $\beta+\alpha\,\zeta_3(5)$ with rational α,β; then the determinant is a polynomial in $\zeta_3(5)$ with rational coefficients, and if $\zeta_3(5)$ were a fraction a/b the determinant would become a rational number whose numerator can be played off against its 3-adic size.

In the real case the standard source of such functionals is an integral (or a sum) of a rational function: a rational function $R(y)$ with poles at the integers splits into partial fractions $\sum_k\sum_m c_{k,m}(y+k)^{-m}$ plus a polynomial, and the integral (or sum) of each piece is either rational or a zeta value. The note copies this structure in $\mathbb{Q}_3$. Its functional is [note, (1.3)]

$$L(P)=\sum_{r=1,2}\int_{\mathbb{Z}_3}(PW)'\Big(t+\frac{r}{3}\Big)\mathrm{d}t\ ,$$

with a rational weight W whose poles sit at the integers $-k$ (Chapter 5). After partial fractions, $L(P)$ is a rational combination of integrals of polynomials (which are rational, by (V2) below) and of the basic integrals

$$\sum_{r=1,2}\int_{\mathbb{Z}_3}\Big(t+\frac{r}{3}+k\Big)^{-m}\mathrm{d}t\qquad(k\in\mathbb{Z},\ m\geq 1)\ . \tag{4.1}$$

The goal of this chapter is to compute (4.1): it equals a rational number when m is odd, and a rational number plus $m\,3^{m+1}L_3(m+1,\mathbf{1})$ when m is even [note, Lemma 2.15]. For $m=4$ the $\zeta_3(5)$ part is $972\,\zeta_3(5)$. That is how $\zeta_3(5)$ enters the moments, and how the rational "harmonic sums" HS_3, which cause the virtual poles of Chapter 12, enter alongside it.

What we need from an "integral over $\mathbb{Z}_3$" is therefore modest: it must be linear, it must be computable on polynomials, it must make sense for the functions $(t+\frac{r}{3}+k)^{-m}$, and it must reproduce [note, (2.13)]. The Volkenborn integral does all four. It is not an integral against a measure, and it is not translation invariant; both facts are visible below with numbers.

4.2 Riemann sums over $\mathbb{Z}_3$

4.2.1 A first experiment

Average the function $f(t)=t$ over the first 3^N non-negative integers:

$$S_N = 3^{-N}\sum_{t=0}^{3^N-1} t = 3^{-N}\frac{(3^N-1)3^N}{2} = \frac{3^N-1}{2}\ .$$

In $\mathbb{R}$ this grows without bound. In $\mathbb{Q}_3$, $3^N\to 0$ (Chapter 2), so $S_N\to -\frac{1}{2}$. Written in digits, $-\frac{1}{2}=1+3+3^2+\dots$ has all digits equal to 1, and $S_N=1+3+\cdots+3^{N-1}$ is its truncation after N digits.

Example 4.1 (three Riemann sums, digit by digit)**.** Direct summation of $S_N(f)=3^{-N}\sum_{t<3^N}f(t)$ for $N=1,\dots,8$ agrees with the closed forms $S_N(t)=\frac{3^N-1}{2}$, $S_N(t^2)=\frac{(3^N-1)(2\cdot 3^N-1)}{6}$ and $S_N(\binom{t}{2})=\frac{(3^N-1)(3^N-2)}{6}$. Digits a_j of $x=\sum a_j3^j$ are listed left to right from the lowest power (here 3^0 for $f=t$, 3^{-1} for the others):

	$f=t$, limit $-\frac{1}{2}$		$f=t^2$, limit $\frac{1}{6}$		$f=\binom{t}{2}$, limit $\frac{1}{3}$	
N	S_N	digits from 3^0	S_N	digits from 3^{-1}	S_N	digits from 3^{-1}
1	1	1000000000	$\frac{5}{3}$	2100000000	$\frac{1}{3}$	1000000000
2	4	1100000000	$\frac{68}{3}$	2112000000	$\frac{28}{3}$	1001000000
3	13	1110000000	$\frac{689}{3}$	2111220000	$\frac{325}{3}$	1000110000
4	40	1111000000	$\frac{6440}{3}$	2111122200	$\frac{3160}{3}$	1000011100
5	121	1111100000	$\frac{58685}{3}$	2111112222	$\frac{29161}{3}$	1000001111
limit	$-\frac{1}{2}$	1111111111	$\frac{1}{6}$	2111111111	$\frac{1}{3}$	1000000000

In all three cases $v_3(S_N-\text{limit})=N$ for $N=1,\dots,8$ (for $\binom{t}{2}$ from $N=2$ on; $S_1=\frac{1}{3}$ is exact). So each step $N\to N+1$ fixes one more digit. For $f=t$ that is N digits, for the other two $N+1$ digits, because their limits start at 3^{-1}.

4.2.2 The definition

Definition 4.2 (Volkenborn integral; [note, (2.5)])**.** For a strictly differentiable function $f:\mathbb{Z}_3\to\mathbb{Q}_3$ (Section 4.3),

$$\int_{\mathbb{Z}_3} f(t)\,\mathrm{d}t = \lim_{N\to\infty} 3^{-N}\sum_{t=0}^{3^N-1} f(t)\ , \tag{4.2}$$

the limit taken in $\mathbb{Q}_3$. We write $S_N(f)$ for the N-th Riemann sum. The limit exists for every such f (Volkenborn [33], Robert [28] Ch. 5). The map $f\mapsto\int_{\mathbb{Z}_3}f$ is linear because each S_N is.

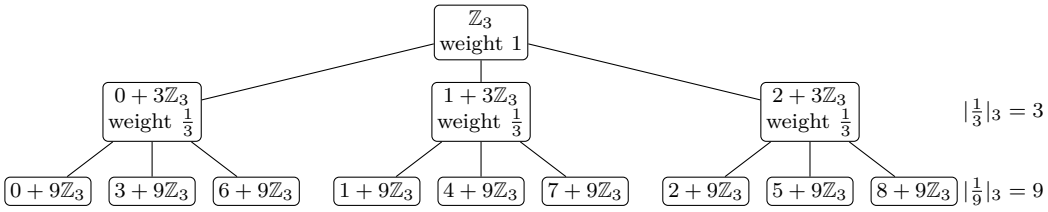


Figure 4.1: $\mathbb{Z}_3$ as a tree of balls. Level N consists of the 3^N balls $t + 3^N\mathbb{Z}_3$, $0 \le t < 3^N$, each represented by its smallest non-negative integer t. The Riemann sum S_N gives each ball the weight 3^{-N} and evaluates f at its representative. The weights add up to 1 at every level, but each individual weight is 3-adically large, $|3^{-N}|_3 = 3^N$.

Intuition: a uniform average with huge weights. $\mathbb{Z}_3$ is the disjoint union of the 3^N balls $t + 3^N\mathbb{Z}_3$, $0 \le t < 3^N$: a 3-adic integer lies in the ball labelled by its last N digits (Figure 4.1). The Riemann sum picks one point from each ball and gives it weight 3^{-N}, a "uniform distribution" on $\mathbb{Z}_3$ at resolution 3^{-N}. In $\mathbb{R}$ the analogous object, the average over a fine grid, converges to the Lebesgue integral for every continuous function, because the weights 3^{-N} are small and positive and their total is 1. Here the total is still 1, but each weight is 3-adically *large*: $|3^{-N}|_3 = 3^N \to \infty$. A change of f by ϵ at one point changes S_N by $3^{-N}\epsilon$, of absolute value $3^N|\epsilon|_3$. So the Riemann sums are extremely sensitive to the fine structure of f, and continuity of f is not enough for them to converge. What saves the day is that the points t and $t + a3^N$ that the next level adds are 3-adically *close*: if f has a derivative, $f(t + a3^N) - f(t) \approx a3^N f'(t)$, and the factor 3^N cancels the huge weight. This is why the integral is defined for (strictly) differentiable functions.

The following two examples make this concrete. Neither is in the note.

Example 4.3 (continuous, even Lipschitz, but no integral)**.** Let $f(0) = 0$ and $f(t) = 3^{v_3(t)}$ for $t \neq 0$; so $f(5) = 1$, $f(6) = 3$, $f(18) = 9$. Then $|f(t)|_3 = 3^{-v_3(t)} = |t|_3$, so f is continuous at 0, and elsewhere it is locally constant. It is even 1-Lipschitz: if $v_3(x) = v_3(y)$ then $f(x) = f(y)$, and if $v_3(x) < v_3(y)$ then $|f(x) - f(y)|_3 = |3^{v_3(x)}|_3 = |x - y|_3$ (for instance, $|f(x) - f(y)|_3 \le |x - y|_3$ for all $0 \le x < y < 729$). Its Riemann sums can be computed by counting: among $0 < t < 3^N$ exactly $2 \cdot 3^{N-1-j}$ integers have $v_3(t) = j$ (the multiples of 3^j that are not multiples of 3^{j+1}), each contributing 3^j, so

$$S_N(f) = 3^{-N} \sum_{j=0}^{N-1} 2 \cdot 3^{N-1-j} \cdot 3^j = 3^{-N} \cdot 2N\, 3^{N-1} = \frac{2N}{3}\,.$$

One finds $S_N = \frac{2}{3}, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \ldots$ for $N = 1, 2, \ldots, 9$, and $S_N - S_{N-1} = \frac{2}{3}$ always, of absolute value 3. The sequence never settles down: the integral of f does not exist. (In $\mathbb{R}$ the bounded continuous function f would have no difficulty at all.)

4.3 Strict differentiability

Definition 4.4 ([note, Section 2.1])**.** $f : \mathbb{Z}_3 \to \mathbb{Q}_3$ is *strictly differentiable* at $a \in \mathbb{Z}_3$ if the difference quotients

$$\frac{f(x) - f(y)}{x - y} \qquad (x \neq y)$$

converge to a limit, called $f'(a)$, as *both* $x \to a$ and $y \to a$ independently. It is strictly differentiable if this holds at every $a \in \mathbb{Z}_3$.

Ordinary differentiability fixes $y = a$; strict differentiability lets both points move. In $\mathbb{R}$, for a function that is continuously differentiable the two notions agree (by the mean value theorem the quotient equals $f'(\xi)$ for some ξ between x and y). In $\mathbb{Q}_3$ there is no mean value theorem, and they differ.

Example 4.5 (polynomials)**.** For $f(t) = t^2$, $\frac{x^2-y^2}{x-y} = x + y \to 2a$. In general $\frac{x^m-y^m}{x-y} = \sum_{i<m} x^i y^{m-1-i} \to m a^{m-1}$, so polynomials are strictly differentiable with the usual derivative. With numbers: $a = 1$, $x = 1 + 3^5$, $y = 1 - 3^7$ give $x + y = 2 + 3^5 - 3^7$, which differs from $f'(1) = 2$ by $3^5(1 - 9)$, of absolute value 3^{-5}.

Example 4.6 (differentiable but not strictly differentiable)**.** For $n \geq 1$ let $D_n = 3^n + 3^{2n}\mathbb{Z}_3$, the 3-adic integers whose lowest $2n$ digits $a_0, \ldots, a_{2n-1}$ agree with those of 3^n (all 0 except $a_n = 1$). These balls are disjoint (every element of D_n has $v_3 = n$). Put $f = 3^{2n}$ on D_n and $f = 0$ elsewhere. At 0: if $x \in D_n$, $|f(x) - f(0)|_3 / |x|_3 = 3^{-2n}/3^{-n} = 3^{-n}$, and otherwise $f(x) = 0$; so $f'(0) = 0$. Away from 0, f is locally constant, so $f' = 0$ there too: f is differentiable everywhere with $f' \equiv 0$. But take $x = 3^n \in D_n$ and $y = 3^n + 3^{2n-1} \notin D_n$ (its last $2n$ digits differ from those of 3^n). Then $\frac{f(x)-f(y)}{x-y} = \frac{3^{2n}}{-3^{2n-1}} = -3$ for every n, although $x, y \to 0$: the quotients do not tend to $f'(0) = 0$. The Riemann sums are $S_N = 0, 1, 4, 11, 32, 93, 276, 823, 2464, 7385$ $(N = 1, \ldots, 10)$, whose differences have v_3 alternating between 0 and 1: no convergence. So ordinary differentiability is not enough either.

Power series. The functions the note integrates are power series $f(t) = \sum_m e_m t^m$ whose coefficients satisfy $v_3(e_m) \geq m + c_0$ for a constant c_0, so that the series converges on the disc $|t|_3 < 3$, which is larger than $\mathbb{Z}_3$ (Chapter 2). The note's argument that these are strictly differentiable is: the difference quotient is

$$\frac{f(x) - f(y)}{x - y} = \sum_m e_m \sum_{i<m} x^i y^{m-1-i} \ .$$

For $x, y \in \mathbb{Z}_3$ the inner sum is in $\mathbb{Z}_3$, so the m-th term has absolute value at most $|e_m|_3 \leq 3^{-m-c_0}$, uniformly in x, y. A series of continuous functions whose terms are uniformly bounded by a sequence tending to 0 converges uniformly (the ultrametric inequality bounds every tail by its largest term), and a uniform limit of continuous functions is continuous. So the quotient extends to a continuous function on $\mathbb{Z}_3 \times \mathbb{Z}_3$, whose value on the diagonal $x = y = a$ is $\sum_m m e_m a^{m-1} = f'(a)$. Continuity at (a, a) is exactly strict differentiability at a.

Example 4.7. $f(t) = (t + \frac{1}{3})^{-4} = 81(1 + 3t)^{-4} = \sum_m 81\binom{-4}{m} 3^m t^m$ has $e_0 = 81$, $e_1 = -972$, $e_2 = 7290$, with $v_3(e_m) \geq m + 4$ (Example 4.18 below lists more). It is therefore strictly differentiable on $\mathbb{Z}_3$, with $f'(0) = e_1 = -972 = -4 \cdot 3^5$; directly, $f'(t) = -4(t + \frac{1}{3})^{-5}$ and $f'(0) = -4 \cdot 3^5$. This number 972 will reappear in Section 4.7.

4.4 Binomial polynomials

The cleanest functions to integrate are not the monomials t^c but the binomial polynomials

$$\binom{t}{c} = \frac{t(t-1)\cdots(t-c+1)}{c!} \quad (c \geq 1) \ , \qquad \binom{t}{0} = 1 \ ,$$

a polynomial of degree c in t with rational coefficients, e.g. $\binom{t}{2} = \frac{t^2-t}{2}$. They reappear in Chapter 8 as the building blocks of integer-valued polynomials.

Example 4.8 (values)**.** For $t = -3, \ldots, 6$:

t	-3	-2	-1	0	1	2	3	4	5	6
$\binom{t}{1}$	-3	-2	-1	0	1	2	3	4	5	6
$\binom{t}{2}$	6	3	1	0	0	1	3	6	10	15
$\binom{t}{3}$	-10	-4	-1	0	0	0	1	4	10	20
$\binom{t}{4}$	15	5	1	0	0	0	0	1	5	15

All values are integers although the coefficients are not, and $\binom{-1}{c} = \frac{(-1)(-2)\cdots(-c)}{c!} = (-1)^c$.

Proposition 4.9 (properties of $\binom{t}{c}$)**.** *(a)* $\binom{t}{c} \in \mathbb{Z}$ *for every* $t \in \mathbb{Z}$.
(b) $\binom{-1}{c} = (-1)^c$.
(c) $\binom{t}{c}$ *maps* $\mathbb{Z}_3$ *into* $\mathbb{Z}_3$ *and is continuous for the* 3*-adic distance.*
(d) For integers $M \geq 0$, $c \geq 0$*:* $\sum_{t=0}^{M-1} \binom{t}{c} = \binom{M}{c+1}$.

Proof. (a) For $t \geq 0$, $\binom{t}{c}$ counts the c-element subsets of a t-element set (and is 0 for $t < c$, since the product contains the factor $t - t = 0$). For $t = -s < 0$, pulling a sign out of each of the c factors gives $\binom{-s}{c} = (-1)^c \frac{s(s+1)\cdots(s+c-1)}{c!} = (-1)^c \binom{s+c-1}{c}$, again an integer. (b) Take $s = 1$: $\binom{-1}{c} = (-1)^c \binom{c}{c} = (-1)^c$. (c) A polynomial is continuous for the 3-adic distance, since sums and products of continuous functions are. The non-negative integers are dense in $\mathbb{Z}_3$ (every $x \in \mathbb{Z}_3$ is the limit of its truncations $x \bmod 3^j$), $\binom{t}{c}$ is in $\mathbb{Z}_3$ at all of them by (a), and $\mathbb{Z}_3$ is closed in $\mathbb{Q}_3$; so the continuous function $\binom{x}{c}$ maps $\mathbb{Z}_3$ into $\mathbb{Z}_3$. (d) Pascal's rule $\binom{t+1}{c+1} = \binom{t}{c+1} + \binom{t}{c}$ says that $\binom{t}{c}$ is the forward difference of $\binom{t}{c+1}$. Summing over $0 \leq t \leq M-1$, the right side telescopes: $\sum_{t<M} \binom{t}{c} = \binom{M}{c+1} - \binom{0}{c+1} = \binom{M}{c+1}$, because $\binom{0}{c+1} = 0$. □

Example 4.10. (d) with $M = 5$, $c = 2$: $0 + 0 + 1 + 3 + 6 = 10 = \binom{5}{3}$. For (c): $\frac{1}{2} \in \mathbb{Z}_3$ and $\binom{1/2}{2} = \frac{\frac{1}{2}(-\frac{1}{2})}{2} = -\frac{1}{8}$, a 3-adic unit; the integers $x_j = \frac{3^j+1}{2}$ (that is, $2, 5, 14, 41, \dots$) tend to $\frac{1}{2}$ with $v_3(x_j - \frac{1}{2}) = j$, and $v_3\big(\binom{x_j}{2} + \frac{1}{8}\big) = 2j$ for $j = 1, \dots, 6$. For $c = 3$, $\binom{1/2}{3} = \frac{1}{16}$ and $v_3\big(\binom{x_j}{3} - \frac{1}{16}\big) = j - 1$: the 3 in 3! costs one digit of accuracy, but continuity holds.

Intuition: the point $3^N - 1$. The Riemann sums of a binomial polynomial will be evaluated at $3^N - 1$, whose digits are N twos. As $N \to \infty$ these digit strings converge to $\dots 2222 = -1$ (Chapter 2). By continuity, $\binom{3^N-1}{c} \to \binom{-1}{c} = (-1)^c$. One finds $v_3\big(\binom{3^N-1}{c} - (-1)^c\big) = N$ for $c = 1$; $\infty, 3, 4, 5, 6, 7, 8$ for $c = 2$ and $N = 1, \dots, 7$ (the value ∞ meaning equality: $\binom{2}{2} = 1$); and $N - 1$ for $c = 3, 4, 5$.

4.5 The three properties (V1)–(V3)

Lemma 4.11 ([note, Lemma 2.6])**.** *(Standard facts; proofs as in the note.) Let* $f : \mathbb{Z}_3 \to \mathbb{Q}_3$ *be strictly differentiable.*
(V1) $\int_{\mathbb{Z}_3} f(t+1)\,\mathrm{d}t = \int_{\mathbb{Z}_3} f(t)\,\mathrm{d}t + f'(0)$*. Hence, for* $N \geq 1$, $\int_{\mathbb{Z}_3} f(t+N)\,\mathrm{d}t = \int_{\mathbb{Z}_3} f + \sum_{i=0}^{N-1} f'(i)$ *and* $\int_{\mathbb{Z}_3} f(t-N)\,\mathrm{d}t = \int_{\mathbb{Z}_3} f - \sum_{i=1}^{N} f'(-i)$.
(V2) $\int_{\mathbb{Z}_3} \binom{t}{c}\,\mathrm{d}t = \frac{(-1)^c}{c+1}$ *for* $c \geq 0$*, and* $\int_{\mathbb{Z}_3} t^c\,\mathrm{d}t = B_c$.
(V3) If $|f(0)|_3 \leq M$ *and* $|f(x) - f(y)|_3 \leq M|x - y|_3$ *for all* $x, y \in \mathbb{Z}_3$*, then* $|\int_{\mathbb{Z}_3} f|_3 \leq 3M$.

We take them in the order (V2), (V1), (V3).

4.5.1 (V2): integrals of polynomials

Proof of (V2). Binomials. By Proposition 4.9(d) with $M = 3^N$, the N-th Riemann sum is

$$S_N\Big(\binom{t}{c}\Big) = 3^{-N}\binom{3^N}{c+1} = 3^{-N} \cdot \frac{3^N}{c+1}\binom{3^N-1}{c} = \frac{1}{c+1}\binom{3^N-1}{c},$$

using $\binom{M}{c+1} = \frac{M}{c+1}\binom{M-1}{c}$ (pull the first factor M out of $M(M-1)\cdots(M-c)/(c+1)!$). As $N \to \infty$, $3^N - 1 \to -1$ in $\mathbb{Z}_3$, and $x \mapsto \binom{x}{c}$ is continuous (Proposition 4.9(c)), so $S_N \to \frac{1}{c+1}\binom{-1}{c} = \frac{(-1)^c}{c+1}$ by Proposition 4.9(b).

Monomials. Faulhaber's formula (Chapter 3) with $M = 3^N$ gives $S_N(t^c) = \frac{1}{c+1}\sum_{i=0}^{c}\binom{c+1}{i}B_i\, 3^{N(c-i)}$. The term $i = c$ is $\frac{c+1}{c+1}B_c = B_c$; every other term contains $3^{N(c-i)}$ with $c - i \geq 1$, which tends to 0. So $S_N(t^c) \to B_c$. □

Example 4.12. For $c = 2$: $S_N(\binom{t}{2}) = \frac{1}{3}\binom{3^N-1}{2} = \frac{(3^N-1)(3^N-2)}{6}$, the closed form of Example 4.1, with limit $\frac{1}{3}\binom{-1}{2} = \frac{1}{3}$. The integrals of $\binom{t}{c}$ for $c = 0, \ldots, 5$ are $1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, -\frac{1}{6}$, and one finds $v_3(S_N(\binom{t}{c}) - \frac{(-1)^c}{c+1}) = N$ for $c = 1, 2$ (from $N = 2$ for $c = 2$) and $N - 1$ for $c = 3, 4$, $N = 1, \ldots, 7$; these are the rates of the intuition box above. The monomial rates (N for t^2, $2N - 1$ for t^4) are worked out in Chapter 3. Note that $\int_{\mathbb{Z}_3} t\,\mathrm{d}t = B_1 = -\frac{1}{2} = \int_{\mathbb{Z}_3}\binom{t}{1}\mathrm{d}t$ and $\int_{\mathbb{Z}_3} t^2\mathrm{d}t = \frac{1}{6}$, while $\binom{t}{2} = \frac{t^2-t}{2}$ gives $\frac{1}{2}(\frac{1}{6} + \frac{1}{2}) = \frac{1}{3}$, consistently.

Intuition: the integral as a derivative at $M = 0$. Here is a way to see what (V2) computes; it is not in the note. For a polynomial f the summatory function $F(M) = \sum_{t=0}^{M-1} f(t)$ is a polynomial in M with $F(0) = 0$ (Faulhaber: for $f = t^c$, $F(M) = \frac{B_{c+1}(M) - B_{c+1}}{c+1}$; for $f = \binom{t}{c}$, $F(M) = \binom{M}{c+1}$). The Riemann sum is $S_N = F(3^N)/3^N$, a difference quotient of F at 0 with step 3^N, and as $3^N \to 0$ 3-adically it tends to

$$\int_{\mathbb{Z}_3} f(t)\,\mathrm{d}t = F'(0)\ .$$

For $f = t$: $F(M) = \frac{M(M-1)}{2}$, $F'(0) = -\frac{1}{2}$. For $f = \binom{t}{c}$: $F'(0) = \frac{\mathrm{d}}{\mathrm{d}M}\binom{M}{c+1}\big|_{M=0} = \frac{(-1)(-2)\cdots(-c)}{(c+1)!} = \frac{(-1)^c}{c+1}$. In $\mathbb{R}$ one cannot send an integer M to 0; in $\mathbb{Q}_3$ the integers 3^N do tend to 0, and the Volkenborn integral is precisely "the sum over the first M integers, divided by M, at $M = 0$".

Expanding F in its Taylor series at 0 gives the full Riemann sum, not only its limit. Since $F'(M)$ is again a sum-type expression, one finds $F^{(i+1)}(0) = \int_{\mathbb{Z}_3} f^{(i)}(t)\,\mathrm{d}t$, and

$$S_N(f) = \sum_{i\geq 0}\frac{3^{Ni}}{(i+1)!}\int_{\mathbb{Z}_3} f^{(i)}(t)\,\mathrm{d}t = \int_{\mathbb{Z}_3} f + \frac{3^N}{2}\int_{\mathbb{Z}_3} f' + \frac{3^{2N}}{6}\int_{\mathbb{Z}_3} f'' + \ldots \qquad (4.3)$$

For a polynomial f the sum is finite and (4.3) is exact; for $f = t^2$ and $N = 1$ it reads $\frac{1}{6} - \frac{3}{2} + 3 = \frac{5}{3} = S_1(t^2)$. It is the 3-adic counterpart of the Euler–Maclaurin formula, which relates sums to integrals in $\mathbb{R}$ (Graham, Knuth and Patashnik, *Concrete Mathematics*, §9.5), with the roles of sum and integral swapped. We use it only to explain convergence rates; for power series rather than polynomials, (4.3) is our extrapolation, consistent with every rate computed below but not proved here.

4.5.2 (V1): shifting by one costs $f'(0)$

Proof of (V1). The function $t \mapsto f(t+1)$ is strictly differentiable, so its integral exists. Its N-th Riemann sum minus that of f is

$$3^{-N}\Big(\sum_{t=0}^{3^N-1} f(t+1) - \sum_{t=0}^{3^N-1} f(t)\Big) = 3^{-N}\Big(\sum_{t=1}^{3^N} f(t) - \sum_{t=0}^{3^N-1} f(t)\Big) = \frac{f(3^N) - f(0)}{3^N}\ ,$$

since all terms with $1 \leq t \leq 3^N - 1$ cancel. This is the difference quotient of f at 0 with step 3^N, and $3^N \to 0$, so it tends to $f'(0)$. Taking $N \to \infty$ on both sides gives the first formula.

Shift by $N \geq 1$: apply the first formula to $f_i(t) = f(t+i)$, whose derivative at 0 is $f'(i)$: $\int_{\mathbb{Z}_3} f(t+i+1) = \int_{\mathbb{Z}_3} f(t+i) + f'(i)$. Adding these for $i = 0, \ldots, N-1$, the intermediate integrals cancel and $\int_{\mathbb{Z}_3} f(t+N) = \int_{\mathbb{Z}_3} f + \sum_{i=0}^{N-1} f'(i)$.

Shift by $-N$: apply the first formula to $g(t) = f(t-1)$, which has $g(t+1) = f(t)$ and $g'(0) = f'(-1)$: $\int_{\mathbb{Z}_3} f = \int_{\mathbb{Z}_3} g(t+1) = \int_{\mathbb{Z}_3} g + g'(0) = \int_{\mathbb{Z}_3} f(t-1) + f'(-1)$, i.e. $\int_{\mathbb{Z}_3} f(t-1) = \int_{\mathbb{Z}_3} f - f'(-1)$. Applied to $f(t-i+1)$ in place of f, this says $\int_{\mathbb{Z}_3} f(t-i) = \int_{\mathbb{Z}_3} f(t-i+1) - f'(-i)$; adding for $i = 1, \ldots, N$ gives $\int_{\mathbb{Z}_3} f(t-N) = \int_{\mathbb{Z}_3} f - \sum_{i=1}^{N} f'(-i)$. □

Intuition: why shifting costs $f'(0)$. Shifting f by 1 moves the window of summation from $\{0, \ldots, 3^N - 1\}$ to $\{1, \ldots, 3^N\}$: it drops $f(0)$ and adds $f(3^N)$. In $\mathbb{R}$ that changes an average over 3^N points by $(f(3^N) - f(0))/3^N \to 0$ for bounded f, and the Lebesgue integral is translation invariant. In $\mathbb{Q}_3$ the new point 3^N is a *neighbour* of the dropped point 0, so $f(3^N) - f(0) \approx 3^N f'(0)$, and the huge weight 3^{-N} turns this into $f'(0)$. In the language of the previous intuition box: if F is the summatory function of f, that of $f(t+1)$ is $F(M+1) - f(0) = F(M) + f(M) - f(0)$, whose derivative at $M = 0$ is $F'(0) + f'(0)$. The Volkenborn integral is *not* translation invariant, and the defect is computable. This defect is the whole content of the translation lemma (Section 4.9).

Example 4.13 (the telescoped term)**.** For $f = t$: $\frac{f(3^N)-f(0)}{3^N} = 1 = f'(0)$ exactly, and indeed $\int_{\mathbb{Z}_3}(t+1)\mathrm{d}t = -\frac{1}{2} + 1 = \frac{1}{2}$. For $f = t^2$: $\frac{3^{2N}}{3^N} = 3^N \to 0 = f'(0)$, so $\int_{\mathbb{Z}_3}(t+1)^2\mathrm{d}t = \int_{\mathbb{Z}_3} t^2\mathrm{d}t = \frac{1}{6}$ (by (V2), $\int_{\mathbb{Z}_3}(t+1)^2 = B_2 + 2B_1 + 1 = \frac{1}{6}$, consistent). For $f = (t + \frac{1}{3})^{-4}$, $f'(0) = -972$, one finds $\frac{f(3)-f(0)}{3} = -\frac{269973}{10000}$ and $v_3(\frac{f(3^N)-f(0)}{3^N} + 972) = N + 6$ for $N = 1, \ldots, 6$. For $f = \binom{t}{c}$: Pascal's rule gives $\binom{t+1}{c} = \binom{t}{c} + \binom{t}{c-1}$, so $\int_{\mathbb{Z}_3}\binom{t+1}{c}\mathrm{d}t = \frac{(-1)^c}{c+1} + \frac{(-1)^{c-1}}{c}$, while $f'(0) = \frac{\mathrm{d}}{\mathrm{d}t}\frac{t(t-1)\cdots(t-c+1)}{c!}\big|_{t=0} = \frac{(-1)(-2)\cdots(-(c-1))}{c!} = \frac{(-1)^{c-1}}{c}$, as (V1) predicts. The Riemann sums $S_N(\binom{t+1}{c}) = 3^{-N}\binom{3^N+1}{c+1}$, computed directly, converge to $\frac{1}{2}, -\frac{1}{6}, \frac{1}{12}, -\frac{1}{20}$ for $c = 1, 2, 3, 4$.

4.5.3 (V3): a small, flat function has a small integral

Proof of (V3). Step 1: the difference of consecutive Riemann sums. Every integer $0 \leq s < 3^{N+1}$ can be written uniquely as $s = t + a3^N$ with $0 \leq t < 3^N$ and $a \in \{0, 1, 2\}$ (divide s by 3^N: a is the quotient, t the remainder). So $S_{N+1} = 3^{-N-1}\sum_{t<3^N}\sum_{a=0}^{2} f(t + a3^N)$. On the other hand $S_N = 3^{-N}\sum_{t<3^N} f(t) = 3^{-N-1}\sum_{t<3^N}\sum_{a=0}^{2} f(t)$ (each term counted three times, divided by 3). Subtracting gives [note, (2.7)]:

$$S_{N+1} - S_N = 3^{-N-1}\sum_{t<3^N}\sum_{a=0}^{2}\left(f(t + a3^N) - f(t)\right). \tag{4.4}$$

Step 2: each bracket. By the Lipschitz hypothesis, $|f(t + a3^N) - f(t)|_3 \leq M|a3^N|_3 \leq M3^{-N}$. Step 3: the sum. By the ultrametric inequality, a sum of any number of terms of absolute value at most $M3^{-N}$ has absolute value at most $M3^{-N}$. Multiplying by 3^{-N-1}, of absolute value 3^{N+1}: $|S_{N+1} - S_N|_3 \leq 3^{N+1}M3^{-N} = 3M$. Step 4: induction. $S_0 = f(0)$ (one term, weight 1), so $|S_0|_3 \leq M \leq 3M$. If $|S_N|_3 \leq 3M$, then $|S_{N+1}|_3 \leq \max(|S_N|_3, |S_{N+1} - S_N|_3) \leq 3M$. So $|S_N|_3 \leq 3M$ for all N. Step 5: limit. The set $\{x : |x|_3 \leq 3M\}$ is closed, so the limit $\int_{\mathbb{Z}_3} f$ also satisfies $|\int_{\mathbb{Z}_3} f|_3 \leq 3M$. □

What just happened. In (4.4) the huge weight 3^{-N-1} meets brackets that are small because t and $t + a3^N$ are close. A Lipschitz bound makes the two effects cancel up to one factor of 3, which is the "$3M$" of (V3). A Lipschitz bound is enough to keep the Riemann sums *bounded*, not to make them *converge*: the function $3^{v_3(t)}$ of Example 4.3 has $M = 1$,

and its Riemann sums $\frac{2N}{3}$ indeed satisfy $|S_N|_3 \le 3$, without converging. Convergence needs the brackets to be $a3^N f'(t)$ up to an error $o(3^N)$, which is what strict differentiability provides; then (4.4) becomes $\sum_{t<3^N} f'(t) \cdot \frac{1}{3}\sum_a a + o(1) = 3^N S_N(f') + o(1) \to 0$. (This is the idea of the existence proof in [28], Ch. 5; we do not reproduce its details.)

Example 4.14 (the factor 3 is needed)**.** $f(t) = t^2$ has $f(0) = 0$ and, by $|x^2 - y^2|_3 \le |x - y|_3$ on $\mathbb{Z}_3$ (Chapter 2), Lipschitz constant 1; so $M = 1$. Its integral is $B_2 = \frac{1}{6}$, with $|\frac{1}{6}|_3 = 3 = 3M$. The bound of (V3) is attained. Indeed $v_3(B_c) = -1$ for all even c from 2 to 12: every $\int_{\mathbb{Z}_3} t^c$ with $c \ge 2$ even sits exactly at the bound.

How the note uses (V3). For a power series $f(t) = \sum_m e_m t^m$ with $v_3(e_m) \ge m + c_0$, the note takes $M = \max_m |e_m|_3$. Indeed $|f(0)|_3 = |e_0|_3 \le M$, and $|f(x) - f(y)|_3 = |\sum_m e_m(x^m - y^m)|_3 \le \max_m |e_m|_3 |x^m - y^m|_3 \le M|x - y|_3$, by the ultrametric inequality and $|x^m - y^m|_3 \le |x - y|_3$ for $x, y \in \mathbb{Z}_3$. So

$$\Big| \int_{\mathbb{Z}_3} \sum_m e_m t^m \, \mathrm{d}t \Big|_3 \le 3 \max_m |e_m|_3 \ . \tag{4.5}$$

This is the tool for integrating a series term by term: apply (4.5) to the tail $\sum_{m \ge I} e_m t^m$, whose coefficients have valuation at least $I + c_0$; its integral is at most $3^{1-I-c_0} \to 0$.

4.6 The set S and the reflection lemma

The note integrates at the points $t + \frac{r}{3}$, $t \in \mathbb{Z}_3$, $r \in \{1, 2\}$, which make up the set [note, (2.8)]

$$S = 3^{-1}\mathbb{Z}_3^\times = \{y \in \mathbb{Q}_3 : \ v_3(y) = -1\} = \Big(\frac{1}{3} + \mathbb{Z}_3\Big) \cup \Big(\frac{2}{3} + \mathbb{Z}_3\Big)$$

of Chapter 2. In practice, "$\int_{\mathbb{Z}_3} g(t + \frac{r}{3})\,\mathrm{d}t$ summed over $r = 1, 2$" is the integral of g over S.

The substitution $t \mapsto -1 - t$. It sends $t + \frac{r}{3}$ to $-1 - t + \frac{r}{3} = -(t + \frac{3-r}{3})$: a point of the class $\frac{r}{3} + \mathbb{Z}_3$ goes to minus a point of the other class. For example, $t = 0$, $r = 1$: $\frac{1}{3} \mapsto -\frac{2}{3}$; $t = 2$, $r = 2$: $\frac{8}{3} \mapsto -\frac{7}{3} = -(2 + \frac{1}{3})$. So on S the substitution acts as $y \mapsto -y$ and swaps the two classes. On the Riemann sums it is almost a symmetry: $t \mapsto 3^N - 1 - t$ permutes $\{0, \dots, 3^N - 1\}$, and $3^N - 1 - t$ differs from $-1 - t$ only by 3^N, which is 3-adically small.

Lemma 4.15 (reflection; [note, Lemma 2.9])**.** *Let $f(t) = \sum_{i \ge 0} e_i t^i$ with $v_3(e_i) \ge i + c_0$ for a constant c_0. Then $\int_{\mathbb{Z}_3} f(-1 - t)\,\mathrm{d}t = \int_{\mathbb{Z}_3} f(t)\,\mathrm{d}t$. Consequently, for every odd $M \ge 1$,*

$$\sum_{r=1,2} \int_{\mathbb{Z}_3} \Big(t + \frac{r}{3}\Big)^{-M} \mathrm{d}t = 0 \ . \tag{4.6}$$

Proof. Step 1: monomials. By (V2) and linearity, for any $x \in \mathbb{Q}_3$,

$$\int_{\mathbb{Z}_3} (t + x)^k \mathrm{d}t = \sum_{i=0}^{k} \binom{k}{i} x^{k-i} \int_{\mathbb{Z}_3} t^i \mathrm{d}t = \sum_{i=0}^{k} \binom{k}{i} B_i x^{k-i} = B_k(x) \ ,$$

the Bernoulli polynomial (Chapter 3). Hence $\int_{\mathbb{Z}_3}(-1-t)^k \mathrm{d}t = (-1)^k \int_{\mathbb{Z}_3}(t+1)^k \mathrm{d}t = (-1)^k B_k(1)$. The reflection identity $B_k(1 - x) = (-1)^k B_k(x)$ at $x = 0$ gives $B_k(1) = (-1)^k B_k(0)$, so $(-1)^k B_k(1) = B_k(0) = B_k = \int_{\mathbb{Z}_3} t^k \mathrm{d}t$.

Step 2: polynomials. Both sides of $\int_{\mathbb{Z}_3} f(-1 - t) = \int_{\mathbb{Z}_3} f(t)$ are linear in f, so Step 1 gives the identity for every polynomial.

Step 3: series. Fix I and split $f = f_{<I} + f_{\geq I}$, with $f_{<I} = \sum_{i<I} e_i t^i$ a polynomial. The tail $f_{\geq I}$ has coefficients of valuation $\geq I + c_0$. So does $f_{\geq I}(-1-t) = \sum_{i\geq I} e_i(-1-t)^i$: expanding $(-1-t)^i$ produces integer multiples of e_i, and integers do not lower the valuation. By (4.5) both tails have integrals of absolute value at most 3^{1-I-c_0}. Hence

$$\Big|\int_{\mathbb{Z}_3} f(-1-t) - \int_{\mathbb{Z}_3} f(t)\Big|_3 = \Big|\int_{\mathbb{Z}_3} f_{\geq I}(-1-t) - \int_{\mathbb{Z}_3} f_{\geq I}(t)\Big|_3 \leq 3^{1-I-c_0}\ ,$$

the polynomial parts cancelling by Step 2. The left side does not depend on I; letting $I \to \infty$ shows it is 0.

Step 4: the odd powers. Put $g_r(t) = (t + \frac{r}{3})^{-M} = (\frac{3}{r})^M (1 + \frac{3t}{r})^{-M}$. By the binomial series (see (4.9) below) its coefficients are $(\frac{3}{r})^M \binom{-M}{i} (\frac{3}{r})^i$, of valuation $\geq M + i$; so Step 3 applies with $c_0 = M$. By the computation above, $g_r(-1-t) = \big(-(t + \frac{3-r}{3})\big)^{-M} = (-1)^M g_{3-r}(t)$. Let $I_M = \sum_r \int_{\mathbb{Z}_3} g_r$. Then

$$I_M = \sum_{r=1,2} \int_{\mathbb{Z}_3} g_r(-1-t)\,\mathrm{d}t = (-1)^M \sum_{r=1,2} \int_{\mathbb{Z}_3} g_{3-r}(t)\,\mathrm{d}t = (-1)^M I_M\ ,$$

the first equality by Step 3, the last because $3 - r$ runs over $\{2, 1\}$ as r runs over $\{1, 2\}$. For odd M this says $I_M = -I_M$, so $I_M = 0$. □

What just happened. Polynomials reflect correctly because Bernoulli polynomials are (anti)symmetric about $\frac{1}{2}$; series reflect correctly because their tails are 3-adically negligible by (V3). The two classes $\frac{1}{3} + \mathbb{Z}_3$, $\frac{2}{3} + \mathbb{Z}_3$ are mirror images, so an odd function of y integrates to zero over S. For even M the same argument gives no information ($I_M = I_M$).

Example 4.16 (reflection in numbers)**.** Polynomials: $\int_{\mathbb{Z}_3} t\,\mathrm{d}t = -\frac{1}{2}$ and $\int_{\mathbb{Z}_3}(-1-t)\mathrm{d}t = -1 - B_1 = -\frac{1}{2}$; and $(-1)^k B_k(1) = B_k$ for $k \leq 12$. Odd powers: consider the Riemann sums of $\sum_r (t + \frac{r}{3})^{-M}$. For $M = 1$, $S_1 = \frac{621}{280}$ and $S_2 = \frac{2923475733}{2974571600}$, and $v_3(S_N) = N + 2$ for $N = 1, \ldots, 8$; for $M = 3$, $S_1 = \frac{227893419}{21952000}$ and $v_3(S_N) = N + 5$ for $N = 1, \ldots, 8$. So the Riemann sums are not zero, but they tend to 0, one digit per step, as (4.6) asserts. The rates match (4.3): the function $h = \sum_r (t + \frac{r}{3})^{-M}$ is odd under the reflection, so $\int_{\mathbb{Z}_3} h = 0$, and the first correction is $\frac{3^N}{2} \int_{\mathbb{Z}_3} h'$, with $h' = -M \sum_r (t + \frac{r}{3})^{-M-1}$, whose integral is given by Lemma 4.17 below: $v_3 = 2$ for $M = 1$ and $v_3 = 5$ for $M = 3$.

Why this matters. The reflection lemma is what "removes the even zeta values" [note, Section 2.1]: integrals of odd negative powers over S vanish, so only the even powers m, which produce $L_3(m+1, \mathbf{1})$ at the odd arguments $m + 1 = 3, 5, \ldots$, survive in the functional. With poles of order up to 4 in W and one derivative in L, the powers that occur are $m \leq 5$, and the even ones are $m = 2$, giving $L_3(3, \mathbf{1}) = \zeta_3(3)$, and $m = 4$, giving $L_3(5, \mathbf{1}) = \zeta_3(5)$. That $\zeta_3(3)$ drops out as well (its coefficient is a multiple of the sum of the residues of PW, which vanishes) is the purity lemma [note, Lemma 2.19], explained in Chapter 5.

4.7 The value lemma: $\zeta_3(5)$ as an integral

Lemma 4.17 (the value; [note, Lemma 2.11])**.** *For even $m \geq 2$,*

$$\sum_{r=1,2} \int_{\mathbb{Z}_3} \Big(t + \frac{r}{3}\Big)^{-m} \mathrm{d}t = m\, 3^{m+1} L_3(m+1, \mathbf{1})\ . \tag{4.7}$$

In particular $\zeta_3(5) = \frac{1}{972} \sum_{r=1,2} \int_{\mathbb{Z}_3} (t + \frac{r}{3})^{-4}\,\mathrm{d}t$.

The idea of the proof: both sides are the same series in Bernoulli numbers. The right side is that series by Washington's formula [note, (2.3)]; the left side becomes it when the integrand is expanded in powers of t and each t^c is integrated to B_c.

Proof. Step 1: the right side as a series. In [note, (2.3)] take $p = F = 3$, $\chi = \mathbf{1}$ and $s = m+1$. Then $\frac{1}{F}\frac{1}{s-1} = \frac{1}{3m}$, $\binom{1-s}{c} = \binom{-m}{c}$, and the sum runs over $a \in \{1,2\}$. Since $\omega(a) = \pm 1$ and m is even, $\langle a\rangle^{1-s} = (a/\omega(a))^{-m} = a^{-m}$. So [note, (2.13)]:

$$3m\, L_3(m+1,\mathbf{1}) = \sum_{a=1,2} a^{-m} \sum_{c\ge 0} \binom{-m}{c} \Big(\frac{3}{a}\Big)^c B_c \ . \tag{4.8}$$

For $m = 4$ this is the series of Chapter 3, $12\,\zeta_3(5) = \sum_a a^{-4} \sum_c \binom{-4}{c}(\frac{3}{a})^c B_c$.

Step 2: the integrand as a series. For $a \in \{1,2\}$, $t + \frac{a}{3} = \frac{a}{3}(1 + \frac{3t}{a})$, so $(t+\frac{a}{3})^{-m} = (\frac{3}{a})^m (1+x)^{-m}$ with $x = \frac{3t}{a}$. For $|x|_3 < 1$ the binomial series

$$(1+x)^{-m} = \sum_{c\ge 0} \binom{-m}{c} x^c \tag{4.9}$$

converges in $\mathbb{Q}_3$ (its coefficients $\binom{-m}{c} = (-1)^c\binom{m+c-1}{c}$ are integers and $x^c \to 0$) and equals $(1+x)^{-m}$: multiplying the partial sums by $(1+x)^m$ gives 1 up to terms of order x^c with c beyond the truncation, as for formal power series, where $(1+x)^m \sum_c \binom{-m}{c} x^c = 1$ holds identically. For $t \in \mathbb{Z}_3$, $|x|_3 = |3t/a|_3 \le \frac{1}{3}$. Hence

$$\Big(t + \frac{a}{3}\Big)^{-m} = \sum_{c\ge 0} e_{a,c}\, t^c \ , \qquad e_{a,c} = \Big(\frac{3}{a}\Big)^m \binom{-m}{c} \Big(\frac{3}{a}\Big)^c \ , \qquad v_3(e_{a,c}) \ge m + c \ . \tag{4.10}$$

Step 3: integrate term by term. Fix I. The polynomial part $\sum_{c<I} e_{a,c} t^c$ integrates to $\sum_{c<I} e_{a,c} B_c$ by (V2). The tail $\sum_{c\ge I} e_{a,c} t^c$ has coefficients of valuation $\ge m + I$, so by (4.5) its integral has absolute value at most 3^{1-m-I}. Therefore

$$\Big| \int_{\mathbb{Z}_3} \Big(t + \frac{a}{3}\Big)^{-m} \mathrm{d}t - \sum_{c<I} e_{a,c} B_c \Big|_3 \le 3^{1-m-I} \ ,$$

and letting $I \to \infty$, $\int_{\mathbb{Z}_3} (t+\frac{a}{3})^{-m} \mathrm{d}t = \sum_{c\ge 0} e_{a,c} B_c$ (the series converges because $v_3(e_{a,c}B_c) \ge m + c - 1$).

Step 4: compare. Summing over a and pulling out 3^m:

$$\begin{aligned} \sum_{a=1,2} \int_{\mathbb{Z}_3} \Big(t + \frac{a}{3}\Big)^{-m} \mathrm{d}t &= 3^m \sum_{a=1,2} a^{-m} \sum_{c\ge 0} \binom{-m}{c} \Big(\frac{3}{a}\Big)^c B_c \\ &= 3^m \cdot 3m\, L_3(m+1,\mathbf{1}) = m\, 3^{m+1} L_3(m+1,\mathbf{1}) \end{aligned}$$

by (4.8). For $m = 4$: $m\,3^{m+1} = 4 \cdot 3^5 = 4 \cdot 243 = 972$, and $L_3(5,\mathbf{1}) = \zeta_3(5)$ by [note, (2.4)]. □

Where 972 comes from. $972 = m \cdot 3^{m+1}$ at $m = 4$, and it splits as $3^4 \cdot 12$: the factor $3^4 = 81$ is $(\frac{3}{a})^4$ at $a = 1$, the size of $(t+\frac{1}{3})^{-4}$ on $\mathbb{Z}_3$ (every point of S has $|y|_3 = 3$, so $|y^{-4}|_3 = 3^{-4}$); the factor $12 = 3m$ is the normalization $\frac{1}{F}\frac{1}{s-1} = \frac{1}{3\cdot 4}$ of Washington's formula. Term-by-term integration is legitimate because the coefficients gain one factor of 3 per power of t, and (V3) turns small coefficients into a small integral.

Example 4.18 (the coefficients)**.** For $m = 4$, here are $e_{a,c}$ and their valuations, $c = 0, \dots, 6$:

c	0	1	2	3	4	5	6
$e_{1,c}$	81	-972	7290	-43740	229635	-1102248	4960116
$e_{2,c}$	$\frac{81}{16}$	$-\frac{243}{8}$	$\frac{3645}{32}$	$-\frac{10935}{32}$	$\frac{229635}{256}$	$-\frac{137781}{64}$	$\frac{1240029}{256}$
v_3	4	5	6	7	8	9	11

(The valuations are the same for $a = 1, 2$; the jump to 11 at $c = 6$ comes from $\binom{-4}{6} = 84 = 3 \cdot 28$.) The partial sums $\sum_{c \le C} \sum_a e_{a,c} B_c$ of the term-by-term integral differ from $972\,\zeta_3(5)$ by valuations $5, 5, 7, 7, 10, 10, 12, 12, 13, 13, 15, 15, 17$ for $C = 0, \dots, 12$ (odd $C \ge 3$ add nothing, since $B_c = 0$ for odd $c \ge 3$, and the term $c = 1$ has valuation 6, larger than the valuation 5 of the term $c = 2$, so it does not change the valuation of the difference).

Example 4.19 (the value lemma by Riemann sums)**.** Evaluating (4.8) with $m = 4$ (truncated at $c = 110$) gives the same 62 digits of $\zeta_3(5)$ as in Chapter 3, and $v_3(972\,\zeta_3(5)) = 4$. On the other side stand the Riemann sums S_N of $g(t) = \sum_r (t + \frac{r}{3})^{-4}$, i.e. the left side of (4.7) at finite N, which involve no Bernoulli number. For $N = 1$, by hand: the six points are $\frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{5}{3}, \frac{7}{3}, \frac{8}{3}$, and

$$S_1 = \frac{1}{3} \cdot 81 \Big(1 + \frac{1}{2^4} + \frac{1}{4^4} + \frac{1}{5^4} + \frac{1}{7^4} + \frac{1}{8^4} \Big) = \frac{177352878267}{6146560000} \, .$$

Digits from 3^4 on, left to right:

	digits $a_4 a_5 a_6 \dots$	$v_3(S_N - 972\,\zeta_3(5))$
S_1	2212111222021011	7
S_2	2210111021222112	9
$972\,\zeta_3(5)$	2210120110012111	

For $N = 1, \dots, 8$ one finds $v_3(S_N - 972\,\zeta_3(5)) = 2N + 5$, i.e. S_N agrees with $972\,\zeta_3(5)$ in its leading $3, 5, 7, 9, 11, 13, 15, 17$ digits. This is a direct numerical illustration of [note, Lemma 2.11] at $m = 4$: the definition [note, (2.5)] of the integral on one side, the series [note, (2.13)] on the other.

The rate $2N + 5$ (two digits per step, where Example 4.1 gained one) is explained by (4.3). The function g is even under the reflection, $g(-1 - t) = g(t)$, so g' is odd and $\int_{\mathbb{Z}_3} g' = 0$ by the argument of Lemma 4.15; the first nonzero correction is $\frac{3^{2N}}{6} \int_{\mathbb{Z}_3} g''$. Here $g'' = 20 \sum_r (t + \frac{r}{3})^{-6}$, whose integral is $20 \cdot 6 \cdot 3^7 L_3(7, \mathbf{1})$ by (4.7) with $m = 6$; one finds $v_3(L_3(7, \mathbf{1})) = -2$, so $v_3(\int_{\mathbb{Z}_3} g'') = 6$ and $v_3(\frac{3^{2N}}{6} \int_{\mathbb{Z}_3} g'') = 2N + 5$, exactly the observed rate.

Check yourself 4.20. Why can one not simply integrate $(t + \frac{r}{3})^{-4}$ over $\mathbb{Z}_3$ as a real integral would be computed, by an antiderivative?

Answer. (V1) shows that the Volkenborn integral is not translation invariant, so the fundamental theorem of calculus in its usual form fails: by (V1) applied to an antiderivative G of f, $\int_{\mathbb{Z}_3} G(t + 1) - \int_{\mathbb{Z}_3} G(t) = G'(0) = f(0)$, a statement about one point, not about $\int f$. The integral is computed instead from its values on polynomials (V2) and continuity (V3).

4.8 Harmonic sums

Shifting the integrand by an integer k will, by (V1), add finitely many derivative values $f'(i)$. For $f = (t + \frac{r}{3})^{-m}$ these are rational numbers of a particular shape, which the note collects into harmonic sums.

Definition 4.21 ([note, (2.14)])**.** For $k \in \mathbb{Z}$ and $M \ge 2$,

$$\mathrm{HS}_3(k, M) = \sum_{\substack{0 < u < 3k \\ 3 \nmid u}} \Big(\frac{3}{u} \Big)^M \quad (k > 0) \, , \qquad \mathrm{HS}_3(k, M) = - \sum_{\substack{3k < u < 0 \\ 3 \nmid u}} \Big(\frac{3}{u} \Big)^M \quad (k < 0) \, ,$$

and $\mathrm{HS}_3(0,M)=0$.

So $\mathrm{HS}_3(1,M)=3^M+(\frac{3}{2})^M$ (from $u=1,2$), $\mathrm{HS}_3(2,M)=3^M+(\frac{3}{2})^M+(\frac{3}{4})^M+(\frac{3}{5})^M$, and $\mathrm{HS}_3(-1,M)=-((\frac{3}{-1})^M+(\frac{3}{-2})^M)=-(-1)^M\mathrm{HS}_3(1,M)$.

Intuition. $\mathrm{HS}_3(k,M)$ is a truncated zeta sum $\sum u^{-M}$ over the integers prime to 3 up to $3|k|$, rescaled by 3^M. The rescaling makes each term small at 3: $v_3((\frac{3}{u})^M)=M$ because $3\nmid u$. At any other prime p the same term is *large* as soon as $p\mid u$: $v_p((\frac{3}{u})^M)=-M\,v_p(u)$. So a harmonic sum is harmless in the 3-adic bookkeeping of Chapter 8 but contributes denominators at the primes $p<3|k|$, $p\neq 3$. These are the "virtual poles" of Chapter 12: at a prime p, the integral behaves as though the integrand had an extra pole, coming not from W but from the translation defect.

Example 4.22 (a table)**.** A selection of the exact values of $\mathrm{HS}_3(k,M)$ for $k\in\{-2,-1,1,2,3,4\}$ and $M=2,\dots,6$, with valuations at $p=2,3,5,7$:

k	M	$\mathrm{HS}_3(k,M)$	v_2	v_3	v_5	v_7
1	3	$\frac{243}{8}$	−3	5	0	0
−1	3	$\frac{243}{8}$	−3	5	0	0
2	3	$\frac{248103}{8000}$	−6	5	−3	0
3	3	$\frac{683680257}{21952000}$	−9	7	−3	−3
1	5	$\frac{8019}{32}$	−5	6	0	0
−1	5	$\frac{8019}{32}$	−5	6	0	0
2	5	$\frac{802908207}{3200000}$	−10	6	−5	0
−2	5	$\frac{802908207}{3200000}$	−10	6	−5	0
4	5	≈ 250.93	−15	6	−5	−5
4	6	≈ 740.63	−18	6	−5	−6
1	4	$\frac{1377}{16}$	−4	4	0	0
−1	4	$-\frac{1377}{16}$	−4	4	0	0

Reading the table: $v_3\geq M$ always (sometimes more, e.g. 7 for $k=3$, $M=3$, by cancellation between terms). The prime 5 appears as soon as $u=5<3k$, i.e. $k\geq 2$, with $v_5=-M$; the prime 7 from $k\geq 3$. The prime 2 appears already at $k=\pm 1$ (from $u=\pm 2$), at $k=2$ with $v_2=-2M$ (from $u=4$), and from $k=3$ on with $v_2=-3M$ (from $u=8$). The entry $k=4$, $M=6$ has $v_5=-5$ instead of -6: the two terms with $v_5=-6$, from $u=5$ and $u=10$, sum to $(\frac{3}{5})^6(1+2^{-6})$, and $1+2^{-6}\equiv 0 \pmod 5$ because $2^6=64\equiv -1 \pmod 5$. Cancellations of this kind between terms with the same power of p are the subject of Chapter 12. (For $M=5$, $2^5\equiv 2 \pmod 5$ and nothing cancels.) The symmetry $\mathrm{HS}_3(-k,M)=(-1)^{M+1}\mathrm{HS}_3(k,M)$, visible in the table, follows from the definition by $u\mapsto -u$.

Remark on the note: "the terms with $p\mid u$ have p-adic valuation $-M$". After [note, (2.14)] the note says that at a prime $p\neq 3$ the terms with $p\mid u$ have p-adic valuation $-M$. The exact valuation is $-M\,v_p(u)$, which is $-M$ only when $p^2\nmid u$. For $p=2$ this already matters at $k=2$ ($u=4$, valuation $-2M$, see the table), and for $p=5$ from $3|k|>25$. The sentence in the note is a remark, not used as a lemma at this point; whether the later bounds (Chapters 11 and 12) need the exact valuation $-Mv_p(u)$ or only the case $p\,\|\,u$ is a question for those chapters.

4.9 The translation lemma

Lemma 4.23 (translation; [note, Lemma 2.15])**.** *For every $k \in \mathbb{Z}$ and $m \geq 1$,*

$$\sum_{r=1,2} \int_{\mathbb{Z}_3} \Big(t + \frac{r}{3} + k\Big)^{-m} \mathrm{d}t = \begin{cases} m\,3^{m+1} L_3(m+1, \mathbf{1}) - m\,\mathrm{HS}_3(k, m+1)\ , & m \text{ even}\ , \\ -m\,\mathrm{HS}_3(k, m+1)\ , & m \text{ odd}\ . \end{cases} \tag{4.11}$$

Proof. Let $f_r(t) = (t + \frac{r}{3})^{-m}$, a power series of the type of Lemma 4.15, hence strictly differentiable. Its derivative at an integer i is

$$f_r'(i) = -m\Big(i + \frac{r}{3}\Big)^{-m-1} = -m\Big(\frac{3i+r}{3}\Big)^{-m-1} = -m\,3^{m+1}(3i+r)^{-m-1} = -m\Big(\frac{3}{3i+r}\Big)^{m+1}\ .$$

The integrand on the left of (4.11) is $f_r(t+k)$.

Case $k = 0$. The left side is $\sum_r \int_{\mathbb{Z}_3} f_r$: by Lemma 4.17 it is $m\,3^{m+1}L_3(m+1,\mathbf{1})$ for even m, and by Lemma 4.15 with $M = m$ it is 0 for odd m. This is the right side, since $\mathrm{HS}_3(0, M) = 0$.

Case $k > 0$. By (V1), $\int_{\mathbb{Z}_3} f_r(t+k) = \int_{\mathbb{Z}_3} f_r + \sum_{i=0}^{k-1} f_r'(i)$. Summing over r,

$$\sum_r \int_{\mathbb{Z}_3} f_r(t+k) = \sum_r \int_{\mathbb{Z}_3} f_r - m \sum_{r=1,2} \sum_{i=0}^{k-1} \Big(\frac{3}{3i+r}\Big)^{m+1}\ .$$

As i runs over $0, \dots, k-1$ and r over $\{1,2\}$, $u = 3i + r$ runs over $1, 2, 4, 5, \dots, 3k-2, 3k-1$: each integer $0 < u < 3k$ with $3 \nmid u$ exactly once (divide u by 3: i is the quotient, $r \in \{1,2\}$ the remainder). So the double sum is $\mathrm{HS}_3(k, m+1)$ and the correction is $-m\,\mathrm{HS}_3(k, m+1)$.

Case $k < 0$. Write $k = -K$ with $K \geq 1$. By (V1), $\int_{\mathbb{Z}_3} f_r(t-K) = \int_{\mathbb{Z}_3} f_r - \sum_{i=1}^{K} f_r'(-i)$, and $f_r'(-i) = -m(\frac{3}{r-3i})^{m+1}$. So

$$\sum_r \int_{\mathbb{Z}_3} f_r(t-K) = \sum_r \int_{\mathbb{Z}_3} f_r + m \sum_{r=1,2} \sum_{i=1}^{K} \Big(\frac{3}{r-3i}\Big)^{m+1}\ .$$

As i runs over $1, \dots, K$ and r over $\{1,2\}$, $u = r - 3i$ runs over $-2, -1, -5, -4, \dots, -3K+1$: each integer $-3K < u < 0$, i.e. $3k < u < 0$, with $3 \nmid u$ exactly once. So the correction is $+m \sum_{3k<u<0,\, 3\nmid u} (\frac{3}{u})^{m+1}$, which is $-m\,\mathrm{HS}_3(k, m+1)$ with the minus sign built into the definition [note, (2.14)] for $k < 0$. □

sign conventions. Moving the integrand to the left ($k > 0$, poles at $-\frac{r}{3} - k$ further from the window $\{0, \dots, 3^N - 1\}$) subtracts $m\,\mathrm{HS}_3(k, m+1)$, a sum of positive-index terms $u = 1, 2, 4, \dots, 3k-1$. Moving it to the right ($k < 0$) adds the same kind of sum over $u = -1, -2, -4, \dots, 3k+1$; the note absorbs this sign into the definition of $\mathrm{HS}_3(k, M)$ for negative k, so that one formula (4.11) covers all k. Every correction term is a derivative value $f_r'(i) = -m(\frac{3}{u})^{m+1}$ at the integer $i = \lfloor u/3 \rfloor$, which is the 3-adic shadow of "$f'(0)$ per unit shift".

Example 4.24 ($k = 1$, $m = 4$ by hand)**.** The integrand $(t + \frac{r}{3} + 1)^{-4}$ moves the window by one. The correction is $f_1'(0) + f_2'(0) = -4 \cdot 3^5(1^{-5} + 2^{-5}) = -972(1 + \frac{1}{32})$, and indeed $4\,\mathrm{HS}_3(1,5) = 4(3^5 + \frac{3^5}{32}) = \frac{8019}{8} = 972 \cdot \frac{33}{32}$. So $\sum_r \int_{\mathbb{Z}_3} (t + \frac{r}{3} + 1)^{-4} \mathrm{d}t = 972\,\zeta_3(5) - \frac{8019}{8}$.

Example 4.25 (the translation lemma by Riemann sums)**.** For $k \in \{1, 2, -1\}$ and $m \in \{2, 3, 4\}$ we compute the Riemann sums S_N of $\sum_r (t + \frac{r}{3} + k)^{-m}$ exactly modulo 3^{60} and compare them with the right side of (4.11), using $L_3(3, \mathbf{1})$ and $L_3(5, \mathbf{1})$ from (4.8):

k	m	v_3(right side)	$v_3(S_N - \text{right side})$, $N = 1, \dots, 8$
1	2	2	$6, 7, 8, 9, 10, 11, 12, 13$
1	3	5	$6, 7, 8, 9, 10, 11, 12, 13$
1	4	4	$7, 8, 9, 10, 11, 12, 13, 14$
2	2	2	$8, 7, 8, 9, 10, 11, 12, 13$
2	3	5	$6, 7, 8, 9, 10, 11, 12, 13$
2	4	4	$8, 8, 9, 10, 11, 12, 13, 14$
-1	2	2	$7, 7, 8, 9, 10, 11, 12, 13$
-1	3	5	$6, 7, 8, 9, 10, 11, 12, 13$
-1	4	4	$9, 8, 9, 10, 11, 12, 13, 14$

In all nine cases the difference tends to 0, one digit per step from $N = 2$ on. (One digit per step rather than two as in Example 4.19: the shifted integrand is no longer symmetric under $t \mapsto -1 - t$, so the term $\frac{3^N}{2} \int_{\mathbb{Z}_3} f'$ of (4.3) no longer vanishes.) The sign of the HS_3 term matters: with it flipped for $k = -1$, $m = 3$, the difference at $N = 8$ has valuation 5, not 13, so the sign convention for $k < 0$ is the right one.

Check yourself 4.26. Without computing, what is $\sum_r \int_{\mathbb{Z}_3} (t + \frac{r}{3} - 1)^{-3}\, \mathrm{d}t$ in terms of a finite sum?

Answer. $m = 3$ is odd, so the value is $-3\,\mathrm{HS}_3(-1, 4) = 3((\frac{3}{-1})^4 + (\frac{3}{-2})^4) = 3(81 + \frac{81}{16}) = \frac{4131}{16}$, a rational number with $v_3 = 5$ ($4131 = 3^5 \cdot 17$) and denominator 2^4: no ζ_3 value appears, and the only primes in the denominator are those dividing some u with $-3 < u < 0$.

Summary of the chapter

The Volkenborn integral $\int_{\mathbb{Z}_3} f = \lim_N 3^{-N} \sum_{t<3^N} f(t)$ is a uniform average over $\mathbb{Z}_3$ whose weights 3^{-N} are 3-adically large. It exists for strictly differentiable f, in particular for power series with coefficients $v_3(e_m) \geq m + c_0$, and can fail to exist for continuous, Lipschitz or even everywhere-differentiable functions (Examples 4.3 and 4.6). It can be read as the derivative at $M = 0$ of the summatory function $M \mapsto \sum_{t<M} f(t)$. Its three working properties are: shifting by one adds $f'(0)$ (V1); $\int_{\mathbb{Z}_3} \binom{t}{c} = \frac{(-1)^c}{c+1}$ and $\int_{\mathbb{Z}_3} t^c = B_c$ (V2); and a function with values and Lipschitz constant at most M has integral at most $3M$ (V3), which justifies term-by-term integration of power series. The substitution $t \mapsto -1 - t$ acts on S as $y \mapsto -y$; it leaves integrals unchanged ([note, Lemma 2.9]), so odd powers integrate to zero over S. Expanding $(t + \frac{a}{3})^{-m}$ in powers of t and integrating each t^c to B_c reproduces Washington's series [note, (2.13)], which gives $\zeta_3(5) = \frac{1}{972} \sum_r \int_{\mathbb{Z}_3} (t + \frac{r}{3})^{-4} \mathrm{d}t$ with $972 = 4 \cdot 3^5$ ([note, Lemma 2.11]); the Riemann sums agree with this to $2N + 1$ digits at level N, for $N \leq 8$.

Carried forward: the table of basic integrals [note, Lemma 2.15], $\sum_r \int_{\mathbb{Z}_3} (t + \frac{r}{3} + k)^{-m} \mathrm{d}t = m\, 3^{m+1} L_3(m+1, \mathbf{1})[m \text{ even}] - m\, \mathrm{HS}_3(k, m+1)$, used in Chapter 5 to show that the functional L takes values in $\mathbb{Q} + \mathbb{Q}\,\zeta_3(5)$; the estimate (V3) in the form (4.5), used for the 3-adic gain in Chapter 8; and the harmonic sums $\mathrm{HS}_3(k, M)$, 3-adically of valuation at least M but with denominators $p^{M\, v_p(u)}$ at the primes $p \mid u$, $u < 3|k|$, which become the virtual poles of Chapter 12.

Part II

The machine

Chapter 5

The weight, the functional and purity

Where we are. Chapter 4 computed the basic integrals $\sum_{r=1,2}\int_{\mathbb{Z}_3}(t+\frac{r}{3}+k)^{-m}\mathrm{d}t$: a harmonic sum $-m\,\mathrm{HS}_3(k,m+1)$, plus $m\,3^{m+1}L_3(m+1,\mathbf{1})$ when m is even [note, Lemma 2.15]. This chapter builds the object to which they are applied: the weight W [note, (1.2)], a rational function with zeros of order 3 and poles of order 4, and the functional $L(P)=\sum_r\int_{\mathbb{Z}_3}(PW)'(t+\frac{r}{3})\mathrm{d}t$ [note, (1.3)]. Its main result is the purity lemma [note, Lemma 2.19]: for every polynomial P with $\deg(PW)\le -2$, $L(P)=\beta(P)+\zeta_3(5)\,\alpha(P)$ with explicit rational $\beta(P),\alpha(P)$, built from finitely many "local constants" at the poles of W. We cover the first half of [note, Section 2.2], up to and including the paragraph after [note, Lemma 2.19]: the explanation of why only $\zeta_3(5)$ survives, the properties of W, the node data $\widetilde{W}_k$, $H_k[b]$, h_k [note, (2.17)–(2.18)], and the proof of purity with the formulas [note, (2.20)–(2.22)]. The Hankel polynomial [note, Definition 2.23] is Chapter 6. From earlier chapters we use the set $S=3^{-1}\mathbb{Z}_3^\times$ and the fact that every integer is at 3-adic distance exactly 3 from every point of S (Chapter 2), the value $\zeta_3(5)=L_3(5,\mathbf{1})$ and its series [note, (2.13)] (Chapter 3), and the Volkenborn integral, the harmonic sums $\mathrm{HS}_3(k,M)$ [note, (2.14)] and the translation lemma (Chapter 4). The last section tests the purity lemma against a computation that does not use it: Riemann sums of the defining integral.

5.1 Partial fractions and residues

The functional L integrates a rational function. Chapter 4 can integrate only the simplest rational functions, the powers $(y+k)^{-m}$. So the first step is to write a rational function as a sum of such powers. This is partial fractions, familiar from calculus; we redo it in the form in which the note uses it.

5.1.1 Principal parts

Let $R(y)=A(y)/B(y)$ be a rational function with rational coefficients, A and B coprime polynomials. Its *degree* is $\deg R=\deg A-\deg B$; so $R(y)$ behaves like a constant times $y^{\deg R}$ as $y\to\infty$. A *pole of order* M at a point c is a root of B of multiplicity M. Near such a pole $g(z)=z^M R(c+z)$ is a rational function of z with no pole at $z=0$, so it has a Taylor expansion $g(z)=g_0+g_1z+g_2z^2+\cdots$ with $g_0\neq 0$, and

$$R(c+z)=\frac{g_0}{z^M}+\frac{g_1}{z^{M-1}}+\cdots+\frac{g_{M-1}}{z}+\left(g_M+g_{M+1}z+\cdots\right).$$

The *principal part* of R at c is the singular piece $\sum_{i=1}^{M} g_{M-i}(y-c)^{-i}$, and the coefficient of $(y-c)^{-1}$, namely g_{M-1}, is the *residue* of R at c. So the coefficient of $(y-c)^{-i}$ in the principal part is

$$[z^{M-i}]\left(z^M R(c+z)\right) , \tag{5.1}$$

where $[z^b]F$ denotes the coefficient of z^b in the Taylor series of F. This formula, "multiply by z^M, expand, read off the coefficients", is exactly how the note computes the principal parts of its weight [note, (2.17), (2.22)].

Fact 5.1 (partial fractions)**.** *If* $\deg R < 0$*, then* R *is the sum of its principal parts at all its poles. (Any algebra text, e.g. Lang,* Undergraduate Algebra*, Ch. IV.)*

Proof. Let $D(y)$ be $R(y)$ minus the sum of all its principal parts. At each pole c the singular piece cancels, so D has no poles: it is a polynomial. Each principal part tends to 0 as $y \to \infty$, and so does R because $\deg R < 0$. So the polynomial D tends to 0 at infinity, and is therefore 0. □

Example 5.2 (partial fractions by Taylor coefficients)**.** Take $R(y) = \frac{2y+3}{y^2(y+1)^2}$, of degree -3, with poles of order 2 at $y = 0$ and $y = -1$. At $c = 0$: $z^2R(z) = \frac{3+2z}{(1+z)^2} = (3+2z)(1-2z+3z^2-\cdots) = 3-4z+\cdots$, so the principal part is $\frac{3}{y^2} - \frac{4}{y}$. At $c = -1$: $z^2R(-1+z) = \frac{1+2z}{(1-z)^2} = (1+2z)(1+2z+\cdots) = 1+4z+\cdots$, so the principal part is $\frac{1}{(y+1)^2} + \frac{4}{y+1}$. Hence

$$\frac{2y+3}{y^2(y+1)^2} = \frac{3}{y^2} - \frac{4}{y} + \frac{1}{(y+1)^2} + \frac{4}{y+1} ,$$

as one confirms by putting the right side over a common denominator. The residues are -4 and 4, and they sum to 0.

5.1.2 The sum of the residues

That the residues in Example 5.2 cancel is not an accident. It is the one fact about partial fractions on which the whole design of the functional rests.

Lemma 5.3 (sum of residues)**.** *Let* $\deg R \le -1$*, and let* ρ_c *be the residue of* R *at the pole* c*. Then* $\sum_c \rho_c = \lim_{y\to\infty} y\,R(y)$*. In particular, if* $\deg R \le -2$*, then* $\sum_c \rho_c = 0$*.*

Proof. By Fact 5.1, $R(y) = \sum_c \sum_{i\ge 1} \rho_{c,i}(y-c)^{-i}$ with $\rho_{c,1} = \rho_c$. Multiply by y. A term with $i = 1$ becomes $\rho_c \frac{y}{y-c}$, which tends to ρ_c as $y \to \infty$. A term with $i \ge 2$ becomes $\rho_{c,i} \frac{y}{(y-c)^i}$, which tends to 0. So $yR(y) \to \sum_c \rho_c$. If $\deg R \le -2$, then $yR(y)$ has degree ≤ -1 and tends to 0. □

Intuition: total charge. Over $\mathbb{C}$, $\rho/(y-c)$ is (up to conjugation and a constant) the electric field of a point charge ρ at c in two dimensions, and $\rho_{c,i}(y-c)^{-i}$ with $i \ge 2$ are dipole, quadrupole, ... fields, which fall off faster. Seen from far away, only the monopoles survive, and the field is $(\sum_c \rho_c)/y$. A function that decays like y^{-2} has no $1/y$ term, so the total charge is zero. (The analogy is only for the algebra; nothing below is electrostatic.)

Example 5.4. $\frac{1}{y(y+1)} = \frac{1}{y} - \frac{1}{y+1}$ has degree -2 and residues $1, -1$, sum 0. In contrast $\frac{y}{(y+1)(y+2)} = \frac{2}{y+2} - \frac{1}{y+1}$ has degree -1 and residues $2, -1$, sum $1 = \lim_{y\to\infty} \frac{y^2}{(y+1)(y+2)}$. And $\frac{1}{y^2(y+1)} = \frac{1}{y^2} - \frac{1}{y} + \frac{1}{y+1}$ (degree -3) has residues $-1, 1$, sum 0.

5.2 Pochhammer symbols

The zeros of the weight are arranged in arithmetic progressions, and the note writes them with the *Pochhammer symbol* (rising factorial)

$$(x)_n = x(x+1)(x+2)\cdots(x+n-1) \qquad (n \geq 1)\ , \qquad (x)_0 = 1\ .$$

For $x = 1$ it is $n!$, and in general $(x)_n = \Gamma(x+n)/\Gamma(x)$. As a polynomial in y, $(y+x)_n$ has degree n and simple zeros at $y = -x, -x-1, \ldots, -x-n+1$.

Example 5.5. $(1)_4 = 24 = 4!$; $(\frac{1}{3})_3 = \frac{1}{3}\cdot\frac{4}{3}\cdot\frac{7}{3} = \frac{28}{27}$; $(\frac{2}{3})_3 = \frac{2}{3}\cdot\frac{5}{3}\cdot\frac{8}{3} = \frac{80}{27}$; $(y+\frac{1}{3})_2 = (y+\frac{1}{3})(y+\frac{4}{3}) = y^2 + \frac{5}{3}y + \frac{4}{9}$, with zeros at $-\frac{1}{3}$ and $-\frac{4}{3}$.

Intuition. $(y+\frac{1}{3})_n$ is a "comb" of n zeros with spacing 1, starting at $-\frac{1}{3}$ and running to the left; $(y+\frac{2}{3})_n$ is the same comb shifted by $-\frac{1}{3}$. Together, $(y+\frac{1}{3})_n(y+\frac{2}{3})_n = \prod_{j=0}^{n-1}(y+j+\frac{1}{3})(y+j+\frac{2}{3})$ vanishes at every point of $(-n, 0)$ with denominator 3, i.e. at all points $-(j+\frac{r}{3})$, $0 \leq j < n$, $r \in \{1,2\}$. These are rational numbers with $v_3 = -1$, so they lie in the set S of integration points (Chapter 2): the weight is made to vanish on finitely many integration points. Why this helps the estimates is the subject of Chapters 8 and 12; see Section 5.3.3.

5.3 The weight

5.3.1 Definition and the four factors

Throughout, n is an odd positive integer (the proof takes $n \to \infty$). The weight is [note, (1.2)]

$$W(y) = \frac{(y+\frac{n}{2})\left(y+\frac{1}{3}\right)_n^3\left(y+\frac{2}{3}\right)_n^3}{\prod_{k=-n}^{2n}(y+k)^4}\ . \tag{5.2}$$

It is a product of four factors:

- $y+\frac{n}{2}$: a simple zero at $y = -\frac{n}{2}$, the midpoint of the poles (below);
- $(y+\frac{1}{3})_n^3$: zeros of order 3 at $y = -\frac{1}{3}, -\frac{4}{3}, \ldots, -(n-1)-\frac{1}{3}$;
- $(y+\frac{2}{3})_n^3$: zeros of order 3 at $y = -\frac{2}{3}, -\frac{5}{3}, \ldots, -(n-1)-\frac{2}{3}$;
- $\prod_{k=-n}^{2n}(y+k)^{-4}$: poles of order 4 at the $3n+1$ integers $y = -k$, $k = -n, \ldots, 2n$.

The integers $k \in \mathcal{N} := \{-n, -n+1, \ldots, 2n\}$ are the *nodes*. *Note the sign*: the node k sits at $y = -k$. So the nodes $-n, \ldots, 2n$ sit at the points $y = n, n-1, \ldots, -2n$ of the line; the node $k = 2n$ is the leftmost pole and the node $k = -n$ the rightmost. This convention matches the translation lemma: near the node k the weight contains $(y+k)^{-4}$, and with $y = t + \frac{r}{3}$ this is $(t+\frac{r}{3}+k)^{-4}$, the integrand of [note, Lemma 2.15] with the same k.

Example 5.6 ($n = 1$)**.** The nodes are $k \in \{-1, 0, 1, 2\}$, at $y = 1, 0, -1, -2$, and

$$W(y) = \frac{\left(y+\frac{1}{2}\right)\left(y+\frac{1}{3}\right)^3\left(y+\frac{2}{3}\right)^3}{(y-1)^4\, y^4\, (y+1)^4\, (y+2)^4}\ .$$

The numerator has degree 7, the denominator degree 16, so $\deg W = -9$. The zeros, with their orders, are $\{-\frac{2}{3} : 3,\ -\frac{1}{2} : 1,\ -\frac{1}{3} : 3\}$, and the poles are $\{-2, -1, 0, 1\}$, each of order 4. At the integration point $y = \frac{1}{3} \in S$,

$$W\left(\tfrac{1}{3}\right) = \frac{\frac{5}{6}\cdot\left(\frac{2}{3}\right)^3\cdot 1^3}{\left(\frac{2}{3}\right)^4\left(\frac{1}{3}\right)^4\left(\frac{4}{3}\right)^4\left(\frac{7}{3}\right)^4} = \frac{5\cdot 3^{12}}{2^{10}\cdot 7^4} \approx 1.08\ ,$$

an ordinary-sized real number but 3-adically tiny: $v_3(W(\frac{1}{3})) = 12$. The valuation is the bookkeeping $4 \cdot 4$ (four poles, each $(y+k)^{-4}$ with $v_3(y+k) = -1$) -1 (from $y + \frac{1}{2}$, $v_3 = -1$) -3 (from $(y + \frac{1}{3})^3 = (\frac{2}{3})^3$) $+0$ (from $(y + \frac{2}{3})^3 = 1$).

Example 5.7 ($n = 3$)**.** The nodes are $k = -3, \dots, 6$, at $y = 3, 2, \dots, -6$; the zeros of order 3 are $-\frac{1}{3}, -\frac{2}{3}, -\frac{4}{3}, -\frac{5}{3}, -\frac{7}{3}, -\frac{8}{3}$, and the simple zero is $-\frac{3}{2}$. Here $\deg W = -21$. Figure 5.1 shows the picture.

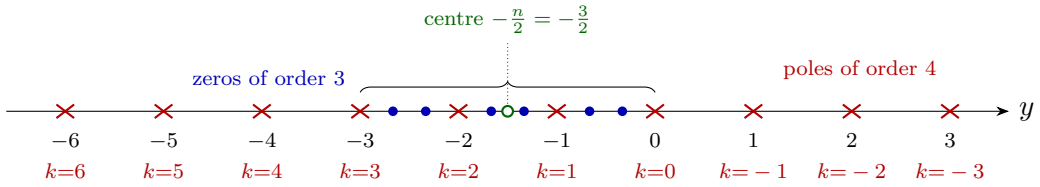


Figure 5.1: The weight W for $n = 3$ on the real line. Crosses: the poles of order 4 at the integers $y = -k$, labelled by their node $k \in \{-3, \dots, 6\}$ (note the sign). Filled dots: the zeros $-(j + \frac{r}{3})$ of order 3, $j = 0, 1, 2$, $r = 1, 2$, all in the interval $(-3, 0)$. Open circle: the simple zero at $y = -\frac{3}{2}$, the centre of the ten poles, which is not a node because n is odd. The antisymmetry $W(-n - y) = -W(y)$ is the reflection of this picture about $-\frac{3}{2}$.

Proposition 5.8 (zeros, poles and degree; [note, Section 2.2])**.** *The weight has a pole of order exactly* 4 *at each* $y = -k$, $k \in \mathcal{N}$*; a zero of order exactly* 3 *at each* $y = -(j + \frac{r}{3})$, $0 \le j < n$, $r \in \{1, 2\}$*; a simple zero at* $y = -\frac{n}{2}$*, which is not a node; and no other zeros or poles. Its degree is* $1 + 6n - 4(3n + 1) = -6n - 3$.

Proof. The numerator is a product of linear factors with roots $-\frac{n}{2}$ (once) and $-(j + \frac{r}{3})$ (three times each, from the cube of the Pochhammer symbols; the $2n$ points $j + \frac{r}{3}$ are distinct). The denominator has the integer roots $-k$, four times each. No root of the numerator is an integer: $j + \frac{r}{3}$ has denominator 3, and $\frac{n}{2}$ has denominator 2 because n is odd. So nothing cancels, and the orders are as stated. The numerator has degree $1 + 3n + 3n$, the denominator $4(3n + 1)$, since $|\mathcal{N}| = 3n + 1$. □

For $n = 1, 3, 5$ the degree is $-9, -21, -33$. For even n the factor $y + \frac{n}{2}$ would cancel against the pole at $y = -\frac{n}{2}$. This is one consequence of the note's convention that n is odd; oddness is used again later, e.g. in [note, Sections 5 and 6], where $2k - n$ is odd and $(n \pm p)/2$ are integers.

5.3.2 Antisymmetry

The poles sit at $y = n, n - 1, \dots, -2n$, symmetric about their midpoint $\frac{n+(-2n)}{2} = -\frac{n}{2}$; the zeros of order 3 fill $(-n, 0)$, also symmetric about $-\frac{n}{2}$. The reflection about $-\frac{n}{2}$ is $y \mapsto -n - y$.

Lemma 5.9 (antisymmetry; [note, Section 2.2])**.** $W(-n - y) = -W(y)$.

Proof. Substitute $y \mapsto -n - y$ in each factor.

- $(-n - y) + \frac{n}{2} = -(y + \frac{n}{2})$: one sign.
- $(-n - y + \frac{1}{3})_n = \prod_{j=0}^{n-1}(-n - y + \frac{1}{3} + j) = (-1)^n \prod_{j=0}^{n-1}(y + n - j - \frac{1}{3})$. With $j' = n - 1 - j$, which also runs over $0, \dots, n-1$, the factor is $y + j' + 1 - \frac{1}{3} = y + j' + \frac{2}{3}$, so $(-n - y + \frac{1}{3})_n = (-1)^n (y + \frac{2}{3})_n$. In the same way $(-n - y + \frac{2}{3})_n = (-1)^n (y + \frac{1}{3})_n$. The two Pochhammer symbols are exchanged, and the cubes carry the sign $(-1)^{3n}(-1)^{3n} = 1$.
- $\prod_{k=-n}^{2n}(-n - y + k)^4 = \prod_k (y + n - k)^4$, and $k' = n - k$ runs over $\{-n, \dots, 2n\}$ when k does. So the denominator is unchanged.

Altogether $W(-n - y) = -W(y)$. □

The note remarks that its argument *does not use* this symmetry; the factor $y + \frac{n}{2}$ is kept from [19]. We shall see it in the node data (Section 5.5): it relates the node k to the node $n - k$.

5.3.3 What the zeros and the poles are for

Intuition: poles give smallness, zeros control size. In $\mathbb{Q}_3$ every integration point $y \in S$ is at distance exactly 3 from every pole $-k$ (Chapter 2), so each factor $(y+k)^{-4}$ has $v_3 = +4$, uniformly on S: the $3n+1$ poles make W 3-adically small on all of S by about $4(3n+1)$ digits. Example 5.6 shows this for $n = 1$: $v_3(W(\frac{1}{3})) = 12$. This uniform smallness is the source of the 3-adic gain (Chapter 8). The zeros work the other way: they are where the real size and the denominators are controlled. On the real line the triple zeros pull W down in the middle of the nodes, which keeps the real size of the Hankel determinant in check (Chapter 10); and at primes $p \neq 3$ they cancel the denominators that the harmonic sums produce (the virtual poles, Chapters 11 and 12). One visible effect, for $n = 3$: the leading coefficient h_k of W at the node k (Section 5.5) is about 10^{-17} at the two nodes $k = 1, 2$, which sit among the zeros, against 10^{-9} to 10^{-10} at the three outermost nodes on each side (Example 5.14).

The orders are chosen so that the counting works: poles of order 4 make the principal parts reach $(y+k)^{-4}$, whose derivative $(y+k)^{-5}$ produces $\zeta_3(5)$ (Section 5.4); the zeros of order 3 on both classes $\frac{1}{3} + \mathbb{Z}$ and $\frac{2}{3} + \mathbb{Z}$ are the note's adaptation of the zeros on $\frac{1}{2} + \mathbb{Z}$ in [19] to the prime 3 [note, Section 2.2].

5.4 The functional, and why only $\zeta_3(5)$ survives

5.4.1 The definition

For a polynomial $P \in \mathbb{Q}[y]$ the note defines [note, (1.3)]

$$L(P) = \sum_{r=1,2} \int_{\mathbb{Z}_3} (PW)'\Big(t + \frac{r}{3}\Big)\mathrm{d}t \ , \tag{5.3}$$

where $(PW)'$ is the derivative of the rational function PW with respect to y, evaluated at $y = t + \frac{r}{3}$, and $\int_{\mathbb{Z}_3}$ is the Volkenborn integral (Chapter 4). In words: average the derivative of PW over the integration set $S = (\frac{1}{3} + \mathbb{Z}_3) \cup (\frac{2}{3} + \mathbb{Z}_3)$.

Well defined. The function $t \mapsto (PW)(t + \frac{r}{3})$ has its poles at $t = -k - \frac{r}{3}$, all with $|t|_3 = 3$. A rational function without poles in the disc $|t|_3 < 3$ has a Taylor series at $t = 0$ that converges there (expand each factor $(t + \frac{r}{3} + k)^{-1} = \frac{3}{r+3k}(1 + \frac{3t}{r+3k})^{-1}$ geometrically, as in Chapter 2). The same holds for its derivative. A power series converging on a disc of radius larger than 1 is strictly differentiable on $\mathbb{Z}_3$, so the Volkenborn integral exists (Chapter 4).

5.4.2 The heuristic: follow one pole

Here is the note's explanation [note, Section 2.2, first paragraph], step by step. Assume $\deg(PW) \leq -2$. Then:

1. By Fact 5.1, PW is the sum of its principal parts: terms $r_{k,i}(y+k)^{-i}$, one for each node k and each $i = 1, 2, 3, 4$ (the poles have order at most 4; P adds no poles).
2. Differentiating, $\frac{\mathrm{d}}{\mathrm{d}y}(y+k)^{-i} = -i\,(y+k)^{-(i+1)}$: a pole of order i becomes a pole of order $i+1 \in \{2, 3, 4, 5\}$.

3. By the translation lemma [note, Lemma 2.15] with $m = i+1$, the integral $\sum_r \int_{\mathbb{Z}_3}(t+\frac{r}{3}+k)^{-(i+1)}\mathrm{d}t$ is $-(i+1)\mathrm{HS}_3(k, i+2)$, a rational number, plus $(i+1)3^{i+2}L_3(i+2, \mathbf{1})$ *if* $i+1$ *is even*, i.e. if i is odd.
4. So only $i = 1$ and $i = 3$ bring a transcendental-looking number: $L_3(3, \mathbf{1}) = \zeta_3(3)$ from the simple poles, and $L_3(5, \mathbf{1}) = \zeta_3(5)$ from the poles of order 3. The orders $i = 2, 4$ give odd $m = 3, 5$, for which the reflection lemma [note, Lemma 2.9] made the L-value part vanish (Chapter 4).
5. The coefficient of $\zeta_3(3)$ turns out to be a multiple of $\sum_k r_{k,1}$, the sum of all residues of PW, which is 0 by Lemma 5.3.

So the derivative in (5.3) is what kills $\zeta_3(3)$.

Intuition: why the derivative. Without the derivative a pole of order i would give $m = i$, and the even orders $i = 2, 4$ would bring $L_3(3, \mathbf{1})$ and $L_3(5, \mathbf{1})$. The coefficient of $\zeta_3(3)$ would then be a multiple of $\sum_k r_{k,2}$, the sum of the *second* coefficients of the principal parts, and nothing forces that to vanish. The derivative shifts every order up by one, so that $\zeta_3(3)$ is paired with the residues, the one combination of partial-fraction coefficients that a decay condition forces to be zero. For $n = 1$ one finds $\sum_k r_{k,2} = 0$ for $P = 1$ (an accident of the antisymmetry, see (5.4): $r_{k,2} = H_k[2]$ and $H_{1-k}[2] = -H_k[2]$), but $\sum_k r_{k,2} = \frac{134245}{944784}$ for $P = y$. So the undifferentiated functional $\sum_r \int_{\mathbb{Z}_3}(yW)(t+\frac{r}{3})\mathrm{d}t$ would contain $54 \cdot \frac{134245}{944784}\,\zeta_3(3)$ (by [note, Lemma 2.15] with $m = 2$).

The zeros of W play no role in this argument; they are chosen for the estimates (Section 5.3.3).

5.5 Node data

To write the principal part of W at a node we use (5.1) with $c = -k$ and $M = 4$.

Definition 5.10 ([note, (2.17)])**.** For a node $k \in \mathcal{N}$,

$$\widetilde{W}_k(z) = z^4\, W(-k+z)\ , \qquad H_k[b] = [z^b]\,\widetilde{W}_k(z) \quad (b \geq 0)\ , \qquad h_k = H_k[0] = \widetilde{W}_k(0)\ .$$

So $\widetilde{W}_k$ is W seen from the node k with the pole removed; it is holomorphic at $z = 0$, and $W(-k+z) = z^{-4}(H_k[0] + H_k[1]z + H_k[2]z^2 + H_k[3]z^3 + \cdots)$. The principal part of W at $y = -k$ is $\sum_{i=1}^{4} H_k[4-i]\,(y+k)^{-i}$, and $h_k \neq 0$ is the leading coefficient, the "strength" of the pole.

Intuition. $H_k[0], \ldots, H_k[3]$ are the four numbers that describe how W blows up at the node k: h_k is the coefficient of $(y+k)^{-4}$, and $H_k[1], H_k[2], H_k[3]$ the corrections of order $(y+k)^{-3}, (y+k)^{-2}, (y+k)^{-1}$. In the charge picture of Lemma 5.3, $H_k[3]$ is the charge of the node and h_k its highest multipole. Every quantity of the proof is eventually a combination of these numbers at the $3n+1$ nodes.

5.5.1 The leading coefficient h_k

Setting $z = 0$ in $\widetilde{W}_k(z) = z^4 W(-k+z)$ cancels the factor $(y+k)^4 = z^4$ and evaluates all other factors at $y = -k$:

$$h_k = \frac{(-k+\frac{n}{2})\prod_{j=0}^{n-1}\left(-k+j+\frac{1}{3}\right)^3\left(-k+j+\frac{2}{3}\right)^3}{\prod_{m\in\mathcal{N}\setminus\{k\}}(-k+m)^4}\ .$$

This is the first formula of [note, (2.18)]. Its denominator is a product of consecutive integers:

Lemma 5.11 ([note, (2.18)]). *For $k \in \mathcal{N}$, $\prod_{m\in\mathcal{N}\setminus\{k\}}(m-k) = (-1)^{k+n}(k+n)!\,(2n-k)!$.*

Proof. Split the product at $m = k$. For $m = -n, \dots, k-1$ the factors $m-k$ are $-(k+n), \dots, -2, -1$: there are $k+n$ of them, and their product is $(-1)^{k+n}(k+n)!$. For $m = k+1, \dots, 2n$ the factors are $1, 2, \dots, 2n-k$, with product $(2n-k)!$. □

For example, for $n = 3$, $k = 1$: $(-4)(-3)(-2)(-1)\cdot 1\cdot 2\cdot 3\cdot 4\cdot 5 = 2880 = 4!\cdot 5!$. For $n = 1$ and $n = 3$, at every node, h_k from [note, (2.18)] agrees with the constant Taylor coefficient of $\widetilde{W}_k$ computed by series expansion.

Example 5.12 (h_0 for $n = 1$ by hand). For $n = 1$, $k = 0$: $\frac{n}{2} - k = \frac{1}{2}$; the only j is 0, giving $(\frac{1}{3})^3(\frac{2}{3})^3 = \frac{8}{729}$; and $\prod_{m\neq 0}(m-0) = (-1)\cdot 1\cdot 2 = -2 = (-1)^1 1!\,2!$. So $h_0 = \frac{\frac{1}{2}\cdot\frac{8}{729}}{(-2)^4} = \frac{1}{2916}$. (That $2916 = 4\cdot 3^6$ is also the constant of [note, (2.21)] is a coincidence of $n = 1$.) For $k = -1$, at $y = 1$: $h_{-1} = \frac{\frac{3}{2}(\frac{4}{3})^3(\frac{5}{3})^3}{6^4} = \frac{250}{19683} = \frac{250}{3^9}$.

5.5.2 Symmetry of the node data

Put $y = -k + z$ in $W(-n-y) = -W(y)$: since $-n-(-k+z) = -(n-k)-z$, we get $W(-(n-k)-z) = -W(-k+z)$. Multiply by $z^4 = (-z)^4$: $\widetilde{W}_{n-k}(-z) = -\widetilde{W}_k(z)$. Comparing coefficients of z^b,

$$H_{n-k}[b] = -(-1)^b\, H_k[b]\ , \qquad \text{in particular} \quad h_{n-k} = -h_k\ . \tag{5.4}$$

The node $n-k$ is the mirror image of the node k about $-\frac{n}{2}$ (it sits at $y = k-n$). It is visible in the tables below. This relation is not stated in the note and is not used anywhere.

Example 5.13 (node data for $n = 1$). Expanding $\widetilde{W}_k(z)$ to order z^3 at the four nodes gives:

k ($y = -k$)	$H_k[0] = h_k$	$H_k[1]$	$H_k[2]$	$H_k[3]$
-1 ($y = 1$)	$\frac{250}{19683}$	$-\frac{3925}{118098}$	$\frac{81715}{1417176}$	$-\frac{1991}{23328}$
0 ($y = 0$)	$\frac{1}{2916}$	$\frac{1}{216}$	$\frac{307}{11664}$	$\frac{1991}{23328}$
1 ($y = -1$)	$-\frac{1}{2916}$	$\frac{1}{216}$	$-\frac{307}{11664}$	$\frac{1991}{23328}$
2 ($y = -2$)	$-\frac{250}{19683}$	$-\frac{3925}{118098}$	$-\frac{81715}{1417176}$	$-\frac{1991}{23328}$
v_3	$-9, -6, -6, -9$	$-10, -3, -3, -10$	$-11, -6, -6, -11$	-6 (all)

The pairs $(k, n-k) = (-1, 2)$ and $(0, 1)$ show (5.4). The last column holds the residues of W; they sum to 0, as Lemma 5.3 demands for $\deg W = -9 \le -2$.

Example 5.14 (the leading coefficients for $n = 3$).

k	-3	-2	-1	0	1
h_k	$\frac{14366628991}{132824487136899962880}$	$\frac{1003003001}{208229648656711680}$	$\frac{166375}{142344486386424}$	$\frac{343}{2745215094595320}$	$\frac{1}{104114824328355840}$
$v_3(h_k)$	-32	-26	-26	-29	-26
$\lvert h_k\rvert$	$1.1\cdot 10^{-10}$	$4.8\cdot 10^{-9}$	$1.2\cdot 10^{-9}$	$1.2\cdot 10^{-13}$	$9.6\cdot 10^{-18}$

and $h_{3-k} = -h_k$ for the remaining nodes $k = 2, \dots, 6$. The 3-adic valuations of h_k are large and negative. By [note, (2.18)], $v_3(h_k) = v_3(\frac{n}{2} - k) - 18 - 4\,v_3((k+n)!\,(2n-k)!)$, since each of the six factors $(j + \frac{r}{3} - k)^3$ has $v_3 = -3$. For $k = -3$: $v_3(\frac{9}{2}) = 2$ and $v_3(0!\,9!) = 4$, so $2 - 18 - 16 = -32$; for $k = 1$: $0 - 18 - 4\cdot 2 = -26$, as in the table.

5.5.3 Taylor coefficients of P at a node

The polynomial P also has to be expanded at each node. The note writes $P_a(k) = [z^a]P(-k+z)$, the a-th Taylor coefficient of P at $y = -k$, i.e. $P_a(k) = P^{(a)}(-k)/a!$.

Example 5.15. For $P = y^2$ at $k = 2$: $P(-2+z) = 4 - 4z + z^2$, so $P_0(2) = 4$, $P_1(2) = -4$, $P_2(2) = 1$, and $P_a(2) = 0$ for $a \geq 3$. For $P = y^3$ at $k = -1$: $(1+z)^3$ gives $P_a(-1) = 1, 3, 3, 1$.

5.6 The purity lemma

Lemma 5.16 (purity; [note, Lemma 2.19])**.** *Let $P \in \mathbb{Q}[y]$ with $\deg(PW) \leq -2$. Then*

$$L(P) = \sum_{k \in \mathcal{N}} \sum_{a=0}^{3} c_{k,a}\, P_a(k) \ , \qquad c_{k,a} = \beta_{k,a} + \zeta_3(5)\, \alpha_{k,a} \ , \tag{5.5}$$

with the rational local constants

$$\beta_{k,a} = \sum_{i=1}^{4-a} i(i+1)\, \mathrm{HS}_3(k, i+2)\, H_k[4-i-a] \ , \qquad \alpha_{k,a} = \begin{cases} -2916\, H_k[1-a] & (a \leq 1) \ , \\ 0 & (a \geq 2) \ . \end{cases} \tag{5.6}$$

In particular, $L(y^m) \in \mathbb{Q} + \mathbb{Q}\,\zeta_3(5)$ for every $m \leq 6n+1$.

The local constants depend only on n and the node k, not on P; P enters only through its first four Taylor coefficients at each node. The name "purity": $L(P)$ is a pure combination of 1 and $\zeta_3(5)$, with no $\zeta_3(3)$.

Proof. The note's argument, split into its steps.

Step 1: partial fractions [note, (2.22)]. The poles of PW are among the nodes, of order at most 4, and $\deg(PW) < 0$, so by Fact 5.1

$$P(y)W(y) = \sum_{k \in \mathcal{N}} \sum_{i=1}^{4} \frac{r_{k,i}}{(y+k)^i} \ .$$

(If P vanishes at a node, the pole there has lower order and some $r_{k,i}$ are 0; the formula still holds.) To find $r_{k,i}$, use (5.1) with $c = -k$, $M = 4$: $r_{k,i}$ is the coefficient of z^{4-i} in $z^4 P(-k+z)W(-k+z) = P(-k+z)\,\widetilde{W}_k(z)$. The product of the two series $\sum_b P_b(k) z^b$ and $\sum_c H_k[c] z^c$ has coefficient of z^{4-i} equal to $\sum_{b+c=4-i} P_b(k) H_k[c]$, so

$$r_{k,i} = \sum_{b=0}^{4-i} P_b(k)\, H_k[4-i-b] \ . \tag{5.7}$$

For example $r_{k,4} = P_0(k)h_k = P(-k)h_k$ and $r_{k,1} = P_0 H_k[3] + P_1 H_k[2] + P_2 H_k[1] + P_3 H_k[0]$ (all at k).

Step 2: differentiate. $(PW)'(y) = \sum_{k,i} r_{k,i} \cdot (-i)(y+k)^{-(i+1)}$.

Step 3: integrate term by term. Put $y = t + \frac{r}{3}$, integrate over $\mathbb{Z}_3$ and sum over r. The sum over (k,i) is finite and the Volkenborn integral is linear (its Riemann sums are), so

$$L(P) = \sum_{k,i} (-i)\, r_{k,i} \sum_{r=1,2} \int_{\mathbb{Z}_3} \left(t + \frac{r}{3} + k \right)^{-(i+1)} \mathrm{d}t \ .$$

Step 4: the translation lemma. By [note, Lemma 2.15] with $m = i+1$, the inner integral is $-(i+1)\mathrm{HS}_3(k, i+2)$, plus $(i+1)3^{i+2} L_3(i+2, \mathbf{1})$ when $i+1$ is even. Multiplying by $-i\, r_{k,i}$, the term (k,i) contributes

$$i(i+1)\, \mathrm{HS}_3(k, i+2)\, r_{k,i} \qquad \text{and, for odd } i, \text{ also} \qquad -\, i(i+1)\, 3^{i+2} L_3(i+2, \mathbf{1})\, r_{k,i} \ .$$

Step 5: $i = 1$, the $\zeta_3(3)$ term vanishes. For $i = 1$: $-1 \cdot 2 \cdot 3^3 = -54$, and $L_3(3, \mathbf{1}) = \zeta_3(3)$ (at $p = 3$, $\omega^{-2} = \mathbf{1}$, as for $\zeta_3(5)$ in Chapter 3). Summed over the nodes, the contribution is $-54\,\zeta_3(3)\sum_k r_{k,1}$. The numbers $r_{k,1}$ are the residues of PW at all its poles, and $\deg(PW) \le -2$, so $\sum_k r_{k,1} = 0$ by Lemma 5.3.

Step 6: $i = 3$, the $\zeta_3(5)$ term. For $i = 3$: $-3 \cdot 4 \cdot 3^5 = -2916$, and $L_3(5, \mathbf{1}) = \zeta_3(5)$ [note, (2.4)]. The contribution of the node k is $-2916\,\zeta_3(5)\,r_{k,3}$, with $r_{k,3} = P_0(k)H_k[1] + P_1(k)H_k[0]$ by (5.7). The number $2916 = 3 \cdot 4 \cdot 3^5$ is 3 times the $972 = 4 \cdot 3^5$ of the value lemma [note, Lemma 2.11]: the factor $i = 3$ comes from differentiating $(y + k)^{-3}$, and 972 from integrating $(y + k)^{-4}$.

Step 7: collect. What remains is

$$L(P) = \sum_k \Big[\sum_{i=1}^{4} i(i+1)\mathrm{HS}_3(k, i+2)\, r_{k,i} \;-\; 2916\,\zeta_3(5)\big(P_0(k)H_k[1] + P_1(k)H_k[0]\big) \Big] .$$

Insert (5.7) into the first sum and collect the coefficient of $P_a(k)$: the pairs (i, b) with $b = a$ and $b \le 4-i$, i.e. $1 \le i \le 4-a$, give $\sum_{i=1}^{4-a} i(i+1)\mathrm{HS}_3(k, i+2)H_k[4-i-a] = \beta_{k,a}$. In the second term $P_0(k)$ has coefficient $-2916H_k[1]$ and $P_1(k)$ has $-2916H_k[0]$; that is $\alpha_{k,a} = -2916H_k[1-a]$ for $a \le 1$, and $\alpha_{k,a} = 0$ for $a \ge 2$. Only $a \le 3$ occurs, because $b \le 4 - i \le 3$. This is (5.5) with (5.6).

Step 8: monomials. $\deg(y^m W) = m + \deg W = m - 6n - 3$, which is ≤ -2 exactly when $m \le 6n + 1$. □

What just happened. The functional reads off the principal parts of PW at the $3n + 1$ nodes, at most four coefficients $r_{k,1}, \dots, r_{k,4}$ each, and turns each into a number using the table of basic integrals of Chapter 4. The harmonic sums give the rational part β, the poles of order 3 give $\zeta_3(5)$ with the constant -2916, and the simple poles would give $\zeta_3(3)$ with -54, but their total coefficient is the sum of residues, which vanishes as soon as PW decays like y^{-2}. Everything is linear in the Taylor coefficients $P_0(k), \dots, P_3(k)$, and the coefficients $c_{k,a}$ are built from HS_3 and the node data $H_k[b]$ alone.

Two features of (5.6) are worth seeing at once. First, $\mathrm{HS}_3(0, M) = 0$, so $\beta_{0,a} = 0$: the node $k = 0$ sits at $y = 0$, the integration needs no translation, and the node contributes only through $\zeta_3(5)$. Second, the note notes after the lemma that $L(P) = \beta(P) + \zeta_3(5)\alpha(P)$, $\beta(P) = \sum_{k,a} \beta_{k,a}P_a(k)$, $\alpha(P) = \sum_{k,a} \alpha_{k,a}P_a(k)$, but that if $\zeta_3(5)$ were rational the single number $L(P)$ would not determine the pair $(\beta(P), \alpha(P))$. The Hankel polynomial is therefore built from the local constants with an indeterminate X in place of $\zeta_3(5)$: $c_{k,a}(X) = \beta_{k,a} + X\alpha_{k,a}$ [note, Definition 2.23], Chapter 6.

Example 5.17 (local constants by hand)**.** For $n = 1$, $k = 1$, $a = 3$, only $i = 1$ occurs: $\beta_{1,3} = 1 \cdot 2 \cdot \mathrm{HS}_3(1, 3)\, H_1[0] = 2 \cdot \frac{243}{8} \cdot \left(-\frac{1}{2916}\right) = -\frac{1}{48}$, using $\mathrm{HS}_3(1, 3) = 3^3 + (\frac{3}{2})^3 = \frac{243}{8}$ (Chapter 4). For $a = 2$, $i = 1, 2$: $\beta_{1,2} = 2 \cdot \frac{243}{8} \cdot \frac{1}{216} + 6 \cdot \frac{1377}{16} \cdot \left(-\frac{1}{2916}\right) = \frac{9}{32} - \frac{17}{96} = \frac{5}{48}$. And $\alpha_{0,1} = -2916\, h_0 = -1$.

5.7 A worked example: $n = 1$, and a check by Riemann sums

5.7.1 The local constants

Example 5.18 (all local constants for $n = 1$)**.** From the node data of Example 5.13, the harmonic sums $\mathrm{HS}_3(k, M)$, $k \in \{-1, 1, 2\}$, $M = 3, \dots, 6$, and (5.6), one finds:

k	$\beta_{k,0}$	$\beta_{k,1}$	$\beta_{k,2}$	$\beta_{k,3}$	$\alpha_{k,0}$	$\alpha_{k,1}$
-1	$-\frac{30137923}{93312}$	$\frac{1373065}{23328}$	$-\frac{16675}{1944}$	$\frac{125}{162}$	$\frac{7850}{81}$	$-\frac{1000}{27}$
0	0	0	0	0	$-\frac{27}{2}$	-1
1	$\frac{7}{16}$	$-\frac{23}{96}$	$\frac{5}{48}$	$-\frac{1}{48}$	$-\frac{27}{2}$	1
2	$-\frac{30179531}{93312}$	$-\frac{172247}{2916}$	$-\frac{33647}{3888}$	$-\frac{1021}{1296}$	$\frac{7850}{81}$	$\frac{1000}{27}$

with $\alpha_{k,2} = \alpha_{k,3} = 0$. So, for instance, $c_{-1,0} = -\frac{30137923}{93312} + \frac{7850}{81}X$ and $c_{0,1} = -X$. The valuations of the nonzero $\beta_{k,a}$ range from -6 to 0, those of $\alpha_{k,a}$ from -4 to 3. (There is no symmetry between $\beta_{k,a}$ and $\beta_{n-k,a}$, because the harmonic sums $\mathrm{HS}_3(k,\cdot)$ and $\mathrm{HS}_3(n-k,\cdot)$ are unrelated.)

Step 1 of the proof can be seen in the same numbers: for $P = 1$, y and y^7, the sum $\sum_{k,i} r_{k,i}(y+k)^{-i}$ with $r_{k,i}$ from (5.7) equals PW identically. For $P = y^m$, $m = 0,\dots,7$, $\sum_k r_{k,1} = 0$, and for $m = 8$ (where $\deg(y^8W) = -1$) $\sum_k r_{k,1} = 1$, the leading coefficient of $y \cdot y^8W(y)$ at infinity, as Lemma 5.3 predicts.

For $P = 1$ the only Taylor coefficient is $P_0(k) = 1$, so $L(1) = \sum_k c_{k,0}$:

$$\beta(1) = \sum_k \beta_{k,0} = -\frac{10046105}{15552}\,, \qquad \alpha(1) = \sum_k \alpha_{k,0} = 2\cdot\frac{7850}{81} - \frac{27}{2}\cdot 2 = \frac{13513}{81}\,,$$

and the purity lemma predicts $L(1) = -\frac{10046105}{15552} + \frac{13513}{81}\,\zeta_3(5)$. With $\zeta_3(5)$ computed from [note, (2.13)] as in Chapter 3, here to about 120 digits instead of 62, this is a 3-adic number with $v_3(L(1)) = 12$, although $v_3(\beta(1)) = -5$ and $v_3(\alpha(1)) = -4$: the rational part and the $\zeta_3(5)$ part cancel in their first 17 digits. This cancellation is the 3-adic gain at work (Chapter 8); for $n = 1$ it is just a number, and the theorem that makes it grow with n is [note, Theorem 3.5].

5.7.2 A check by Riemann sums

The purity lemma is a chain of earlier results (partial fractions, the translation lemma, the value lemma, the reflection lemma, the series [note, (2.13)]). A check that avoids all of them is to compute $L(P)$ directly from the definition (5.3) and the definition of the Volkenborn integral [note, (2.5)]: the Riemann sums

$$S_N(P) = 3^{-N} \sum_{t=0}^{3^N-1} \sum_{r=1,2} (PW)'\Big(t + \frac{r}{3}\Big)\,.$$

We write $(PW)'$ as one rational function with integer coefficients and evaluate it exactly at the $2\cdot 3^N$ points $y = \frac{3t+r}{3}$, writing each value as $3^v \cdot u$ with u a 3-adic unit known modulo 3^{160}. This uses neither H_k, HS_3, partial fractions nor the translation lemma. For $N = 1$, in exact rationals, $S_1(1) = \frac{254898894442171336396983}{514565125122560512000000}$, with $v_3 = 12$.

Example 5.19 (purity confirmed by Riemann sums, $n = 1$)**.** For $P = y^m$, $m = 0,\dots,7$ (all monomials allowed by the lemma) and $N = 1,\dots,10$, one finds the following values of $v_3(S_N(y^m) - \beta(y^m) - \zeta_3(5)\,\alpha(y^m))$:

P	$v_3(L(P))$	$v_3\big(S_N - (\beta + \zeta_3(5)\alpha)\big)$, $N = 1,\dots,10$
1	12	15, 15, 16, 17, 18, 19, 20, 21, 22, 23
y	12	13, 14, 15, 16, 17, 18, 19, 20, 21, 22
y^2	10	15, 13, 14, 15, 16, 17, 18, 19, 20, 21
y^3	11	12, 13, 14, 15, 16, 17, 18, 19, 20, 21
y^4	8	11, 11, 12, 13, 14, 15, 16, 17, 18, 19
y^5	8	9, 10, 11, 12, 13, 14, 15, 16, 17, 18
y^6	6	9, 9, 10, 11, 12, 13, 14, 15, 16, 17
y^7	6	7, 8, 9, 10, 11, 12, 13, 14, 15, 16

In every case the difference gains exactly one 3-adic digit per level from $N = 2$ on, the same rate as the shifted integrals of Chapter 4. At $N = 10$ the Riemann sum agrees with the prediction of the purity lemma in $v_3(\text{difference}) - v_3(L(P)) = 11, 10, 11, 10, 11, 10, 11, 10$ leading digits. Digit by digit for $P = 1$, starting at 3^{12}:

$\beta(1) + \zeta_3(5)\alpha(1)$	2221221012021100
$S_1(1)$	2220021100101000
$S_2(1)$	2220002111022202
$S_5(1)$	2221220022002112
$S_{10}(1)$	2221221012011202

(read left to right as the coefficients of $3^{12}, 3^{13}, \ldots$; S_{10} matches the first 11).

Example 5.20 (the check can fail: $\deg(PW) = -1$)**.** For $P = y^8$, $\deg(PW) = -1$ and the lemma does not apply. One finds $v_3(S_N - (\beta + \zeta_3(5)\alpha)) = 2$ for all $N = 1, \ldots, 10$: the Riemann sums converge, but not to the purity prediction. Step 5 of the proof says what is missing: the term $-54\,\zeta_3(3)\sum_k r_{k,1} = -54\,\zeta_3(3)$, since $\sum_k r_{k,1} = 1$ here, and $v_3(54\,\zeta_3(3)) = 2$ (with $\zeta_3(3) = L_3(3, \mathbf{1})$ from [note, (2.13)] with $m = 2$). With this term added, the differences become $9, 7, 8, 9, \ldots, 15$ for $N = 1, \ldots, 10$, converging again at one digit per level. So the residue mechanism of Step 5 is seen at work: when the residues do not cancel, exactly $-54\,\zeta_3(3)$ times their sum appears.

Example 5.21 ($n = 3$)**.** The same check for $n = 3$ (ten nodes, $\deg W = -21$), with $N = 1, \ldots, 9$: for $P = 1$, $v_3(L(1)) = 32$ and the differences are $32, 35, 35, 36, 37, 38, 39, 40, 41$; for $P = y^{19}$ (the largest power allowed, $m = 6n + 1$), $v_3(L) = 15$ and the differences are $15, 16, \ldots, 23$. For $P = y^{20}$ ($\deg(PW) = -1$) the purity prediction misses by a constant of valuation 2, and adding $-54\,\zeta_3(3)$ gives $12, 15, 15, 16, \ldots, 21$.

what the check shows, and what it does not. For $n = 1$ and $n = 3$ and the monomials tested, the value of $L(P)$ computed from its definition agrees with the purity formula [note, (2.20)–(2.21)] to as many 3-adic digits as the Riemann sums resolve (8 to 11 leading digits at the largest N), and the agreement improves by one digit per level, as expected from Chapter 4. The $P = y^{6n+2}$ test shows that the check is sensitive: it detects a missing $\zeta_3(3)$ term of valuation 2, and confirms the constant -54. This is numerical evidence for the lemma in these cases, including the constants -54 and -2916 and the sign conventions of HS_3 and of the nodes; it is not a proof for general n. The two sides share only the definition of W and the series [note, (2.13)] for $\zeta_3(5)$ and $\zeta_3(3)$.

Check yourself 5.22. Why are the four constants $\beta_{0,a}$ zero for every n, while $\alpha_{0,0}, \alpha_{0,1}$ are not?

Answer. The node $k = 0$ sits at $y = 0$, and its terms $(t + \frac{r}{3})^{-m}$ need no translation, so their integrals have no harmonic-sum part: $\mathrm{HS}_3(0, M) = 0$ in (5.6). Their $\zeta_3(5)$ part, from $m = 4$, is the value lemma itself, $972\,\zeta_3(5)$, and survives: $\alpha_{0,a} = -2916 H_0[1 - a]$. For $n = 1$, $\alpha_{0,0} = -\frac{27}{2}$ and $\alpha_{0,1} = -1$.

Check yourself 5.23. Why is it $\deg(PW) \le -2$ and not $\deg(PW) \le -1$ in the lemma?

Answer. For $\deg(PW) = -1$ partial fractions still hold, but the residues sum to $\lim yP(y)W(y) \neq 0$, so Step 5 leaves $-54\,\zeta_3(3)\sum_k r_{k,1}$, and $L(P)$ is no longer in $\mathbb{Q} + \mathbb{Q}\,\zeta_3(5)$ (unless $\zeta_3(3)$ happened to be in that space). Example 5.20 shows the extra term numerically for $n = 1$, $P = y^8$.

Summary of the chapter

The weight W [note, (1.2)] has poles of order 4 at the $3n+1$ nodes $k \in \{-n, \dots, 2n\}$, the node k sitting at $y = -k$; zeros of order 3 at the $2n$ points $-(j + \frac{r}{3})$ in $(-n, 0)$; a simple zero at the centre $-\frac{n}{2}$, which is not a node because n is odd; degree $-6n-3$; and it is antisymmetric about its centre, $W(-n-y) = -W(y)$. The poles make W uniformly 3-adically small on S; the zeros are there for the real size and for the denominators. The functional $L(P) = \sum_r \int_{\mathbb{Z}_3} (PW)'(t + \frac{r}{3}) \mathrm{d}t$ [note, (1.3)] reduces, by partial fractions, to the basic integrals of Chapter 4: a pole of order i of PW produces a harmonic sum, and for odd i also $L_3(i+2, \mathbf{1})$. The derivative ties $\zeta_3(3)$ to the sum of the residues of PW, which is zero when $\deg(PW) \le -2$, so only $\zeta_3(5)$ survives, with the constant $-2916 = -3 \cdot 4 \cdot 3^5$ from the poles of order 3. This is the purity lemma [note, Lemma 2.19]. For $n = 1$ and $n = 3$ it agrees with Riemann sums of the defining integral to 8–11 digits, and we saw that the predicted $\zeta_3(3)$ term appears exactly when the hypothesis $\deg(PW) \le -2$ fails.

Carried forward: the node data $\widetilde{W}_k$, $H_k[b]$, h_k [note, (2.17)–(2.18)] with $\prod_{m \ne k}(m-k) = (-1)^{k+n}(k+n)!(2n-k)!$, used for the gain (Chapter 8), the Heine expansion and the size (Chapters 9 and 10) and the denominators (Chapters 11 and 12); the Taylor coefficients $P_a(k)$ and the local constants $\beta_{k,a}, \alpha_{k,a}$ [note, (2.21)] and $c_{k,a}(X) = \beta_{k,a} + X\alpha_{k,a}$ [note, Definition 2.23], from which Chapter 6 builds the functional Λ and the Hankel polynomial $\Delta_K(X)$ [note, Definition 2.23]; and the fact that the moments $L(y^m)$, $m \le 6n+1$, lie in $\mathbb{Q} + \mathbb{Q}\,\zeta_3(5)$, which allows Hankel determinants of size $K \le 3n+1$.

Chapter 6

Hankel determinants and the Hankel polynomial

Where we are. Chapter 5 built the functional $L(P) = \sum_{r=1,2} \int_{\mathbb{Z}_3} (PW)'(t + \frac{r}{3}) \mathrm{d}t$ and proved, following the note, that $L(P) = \beta(P) + \zeta_3(5)\,\alpha(P)$ with rational $\beta(P), \alpha(P)$ whenever $\deg(PW) \le -2$ (purity, [note, Lemma 2.19]); the two numbers are sums of local constants $c_{k,a} = \beta_{k,a} + \zeta_3(5)\alpha_{k,a}$ times the Taylor coefficients $P_a(k)$ of P at the nodes. This chapter builds the object to which all four estimates of the proof are applied: the Hankel polynomial $\Delta_K(X)$ [note, Definition 2.23]. We cover [note, Section 2.2] from [note, Definition 2.23] to the end: the definition, the degree bound, the identity [note, (2.26)] $\Delta_K(\zeta_3(5)) = \det[L(y^{i+j})]$ for $K \le 3n+1$, and the jet form [note, (2.27)], which writes the Hankel matrix as a sum of one small matrix per node. Before that we explain from scratch what Hankel determinants are: moments, Gram matrices, the effect of a change of basis (used again in Chapters 8 and 14), orthogonal polynomials, Heine's formula (proved in Chapter 9), and why a positive measure has positive Hankel determinants while nothing of the kind is available in $\mathbb{Q}_3$ (the reason for Chapter 14). From earlier chapters we need the valuation v_3 and digit expansions (Chapter 2), the Bernoulli numbers and $\zeta_3(5)$ (Chapter 3), the Volkenborn integral (Chapter 4), and the node data and local constants for $n = 1$ (Chapter 5).

6.1 Moments and Hankel matrices

6.1.1 Linear functionals and their moments

A *linear functional* on polynomials is a map L from polynomials (with coefficients in a field such as $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{Q}_3$) to numbers in that field with $L(aP + bQ) = aL(P) + bL(Q)$. Since every polynomial is a combination of monomials, L is determined by the numbers

$$m_j = L(y^j) \qquad (j = 0, 1, 2, \dots)\ ,$$

its *moments*. The name comes from probability: for $L(P) = \int P\,\mathrm{d}\mu$ with a measure μ, m_j is the j-th moment of μ. In this chapter there are three kinds of functionals: integration against a positive measure on $\mathbb{R}$ (the classical case), the Volkenborn integral on $\mathbb{Z}_3$ (Chapter 4), and the note's L and its formal version Λ.

Example 6.1 (three sets of moments)**.** (a) For $\mathrm{d}x$ on $[0,1]$: $m_j = \int_0^1 x^j \mathrm{d}x = \frac{1}{j+1}$, i.e. $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$. (b) For the Volkenborn integral, $m_j = \int_{\mathbb{Z}_3} t^j \mathrm{d}t = B_j$, the Bernoulli numbers with $B_1 = -\frac{1}{2}$ (Chapters 3 and 4): $1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42}, 0, -\frac{1}{30}$ for $j = 0, \dots, 8$. (c) For the

note's functional with $n = 1$, the moments $L(y^j)$, $j \le 6$, are numbers $\beta + \zeta_3(5)\alpha$ listed in Example 6.22 below; for instance $L(1) = -\frac{10046105}{15552} + \frac{13513}{81}\zeta_3(5)$ (Chapter 5).

6.1.2 The Hankel matrix

Definition 6.2 (Hankel matrix and determinant)**.** The $K \times K$ *Hankel matrix* of L is $H_K = [L(y^{i+j})]_{0 \le i,j < K} = [m_{i+j}]$, and its *Hankel determinant* is $\det H_K$. Rows and columns are numbered from 0.

The entry in row i, column j depends only on $i + j$, so H_K is constant along every anti-diagonal (the lines $i + j = \text{const}$, running from bottom left to top right):

$$H_4 = \begin{pmatrix} m_0 & m_1 & m_2 & m_3 \\ m_1 & m_2 & m_3 & m_4 \\ m_2 & m_3 & m_4 & m_5 \\ m_3 & m_4 & m_5 & m_6 \end{pmatrix}.$$

A $K \times K$ Hankel matrix uses the $2K - 1$ moments $m_0, \dots, m_{2K-2}$. This count returns in Section 6.5: it is the reason for the bound $K \le 3n + 1$.

Example 6.3. For $\mathrm{d}x$ on $[0, 1]$, $\det H_K = 1,\ \frac{1}{12},\ \frac{1}{2160},\ \frac{1}{6048000}$ for $K = 1, 2, 3, 4$ (also Chapter 1). By hand for $K = 2$: $\det\left(\begin{smallmatrix} 1 & 1/2 \\ 1/2 & 1/3 \end{smallmatrix}\right) = \frac{1}{3} - \frac{1}{4} = \frac{1}{12}$.

6.1.3 The Hankel matrix is a Gram matrix

The reason Hankel matrices are natural is that a functional L defines a bilinear form on polynomials,

$$\langle P, Q \rangle_L = L(PQ)\ ,$$

symmetric because $PQ = QP$. For $L(P) = \int P \,\mathrm{d}\mu$ this is the familiar L^2 inner product $\int PQ \,\mathrm{d}\mu$. The *Gram matrix* of a list of vectors $b_0, \dots, b_{K-1}$ for a bilinear form is $[\langle b_i, b_j \rangle]_{i,j}$. In the monomial basis $b_i = y^i$ the entries are $\langle y^i, y^j \rangle_L = L(y^i y^j) = L(y^{i+j})$, so:

Fact 6.4. *H_K is the Gram matrix of $1, y, \dots, y^{K-1}$ for the bilinear form $(P, Q) \mapsto L(PQ)$.*

> **Intuition: why anti-diagonals are constant.** The Hankel pattern is the multiplication rule $y^i \cdot y^j = y^{i+j}$ seen through L: the form $L(PQ)$ only ever sees the product, and the product of two monomials only remembers the sum of the exponents. In a basis other than the monomials the Gram matrix is still the Gram matrix of the same form, but it is in general no longer Hankel (Example 6.25 below).

6.2 Change of basis

The note changes the basis of the space of polynomials of degree $< K$ twice: in Chapter 8 to a triangular basis of integer-valued polynomials [note, Lemma 4.1], and in Chapter 14 to a basis adapted to an auxiliary prime [note, Lemma 6.12] and the paragraph after it. In both places only one fact about determinants is used.

Lemma 6.5 (change of basis)**.** *Let $b_i = \sum_{j<K} T_{ij}\, y^j$ $(0 \le i < K)$ for a $K \times K$ matrix T with entries in the same field (or ring) as the values of L. Then*

$$[L(b_i b_{i'})]_{i,i'<K} = T\, H_K\, T^{\mathsf{T}} \qquad \text{and} \qquad \det[L(b_i b_{i'})] = (\det T)^2 \det H_K\ .$$

Proof. Expand both factors and use linearity of L twice:

$$L(b_i b_{i'}) = L\Big(\sum_j T_{ij} y^j \sum_{j'} T_{i'j'} y^{j'}\Big) = \sum_{j,j'} T_{ij}\, L(y^{j+j'})\, T_{i'j'} = \sum_{j,j'} T_{ij}\, (H_K)_{jj'}\, (T^{\mathsf{T}})_{j'i'} \ ,$$

which is the (i,i') entry of $T H_K T^{\mathsf{T}}$. The determinant is multiplicative and $\det T^{\mathsf{T}} = \det T$, so $\det\Big(T H_K T^{\mathsf{T}}\Big) = \det T \cdot \det H_K \cdot \det T$. □

Nothing in the proof uses an order, square roots or a metric; it is valid when the values of L lie in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_3$, or in the polynomial ring $\mathbb{Q}[X]$, which is how the note uses it.

Example 6.6 (a 2×2 change of basis)**.** For $\mathrm{d}x$ on $[0,1]$ replace $\{1, y\}$ by $\{1,\, 2y-1\}$, so $T = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 2 \end{smallmatrix}\right)$ (row i holds the coefficients of b_i), $\det T = 2$. Then

$$T H_2 T^{\mathsf{T}} = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{3} \end{pmatrix},$$

which is also what direct integration gives: $\int_0^1 (2y-1)\mathrm{d}y = 0$, $\int_0^1 (2y-1)^2 \mathrm{d}y = \frac{1}{3}$. And $\det = \frac{1}{3} = 2^2 \cdot \frac{1}{12}$.

Intuition: what the factor $(\det T)^2$ means. $\det H_K$ is the squared "volume" spanned by $1, \dots, y^{K-1}$ measured with the form $L(PQ)$ (for a positive measure this is literally the squared volume of a parallelepiped in $L^2(\mu)$). Changing the spanning vectors by T changes the volume by $\det T$, and the squared volume by $(\det T)^2$. The two uses in the note are the two cases in which this factor is under control. If T is *triangular*, $\det T$ is the product of its diagonal entries, i.e. of the leading coefficients of the b_i; so one knows exactly how many powers of 3 the change of basis costs or gains (Chapter 8, [note, (4.3)]). If T has entries in $\mathbb{Z}_p$ and $\det T$ is a p-adic unit (*unimodular* over $\mathbb{Z}_p$), then $v_p((\det T)^2) = 0$ and the p-adic valuations of the determinant, and of each coefficient of $\Delta_K(X)$, do not change (Chapter 14, the paragraph after [note, Lemma 6.12]).

6.3 Positive measures: orthogonal polynomials and Heine's formula

This section is the classical theory, in the case where everything is real and positive. It is not used in the proof, but it is what the note's method is modelled on, and it shows exactly which piece breaks in $\mathbb{Q}_3$.

6.3.1 Gram–Schmidt and orthogonal polynomials

Let μ be a positive measure on $\mathbb{R}$ with finite moments, and apply Gram–Schmidt to $1, y, y^2, \dots$ with the inner product $\langle P, Q\rangle = \int PQ\, \mathrm{d}\mu$, without normalizing: $\pi_0 = 1$ and

$$\pi_i = y^i - \sum_{j<i} \frac{\langle y^i, \pi_j\rangle}{\langle \pi_j, \pi_j\rangle}\, \pi_j \ .$$

Then π_i is *monic* (leading coefficient 1) of degree i and orthogonal to all polynomials of lower degree. These are the *monic orthogonal polynomials* of μ.

Example 6.7 (shifted Legendre polynomials)**.** For $\mathrm{d}x$ on $[0,1]$ Gram–Schmidt gives

i	$\pi_i(y)$	$\|\pi_i\|^2 = \int_0^1 \pi_i^2 \mathrm{d}y$
0	1	1
1	$y - \frac{1}{2}$	$\frac{1}{12}$
2	$y^2 - y + \frac{1}{6}$	$\frac{1}{180}$
3	$y^3 - \frac{3}{2}y^2 + \frac{3}{5}y - \frac{1}{20}$	$\frac{1}{2800}$

with $\int_0^1 \pi_i \pi_j \mathrm{d}y = 0$ for all six pairs $i < j$. For $i = 1$ by hand: $\pi_1 = y - \frac{\langle y,1\rangle}{\langle 1,1\rangle} = y - \frac{1}{2}$, and $\int_0^1 (y - \frac{1}{2})^2 \mathrm{d}y = \frac{1}{12}$. These are the shifted Legendre polynomials: $\pi_i(y) = P_i(2y-1)/\binom{2i}{i}$, where P_i is the Legendre polynomial and $\binom{2i}{i}$ the leading coefficient of $P_i(2y-1)$.

Proposition 6.8 (Hankel determinant as a product of norms)**.** *If $\pi_0, \dots, \pi_{K-1}$ are monic and pairwise orthogonal for $L(PQ)$, then $\det H_K = \prod_{i<K} L(\pi_i^2)$. (See e.g. Szegő [32].)*

Proof. Write $\pi_i = \sum_j T_{ij} y^j$. Since π_i is monic of degree i, T is lower triangular with 1 on the diagonal, so $\det T = 1$. In the basis π_i the Gram matrix is diagonal with entries $L(\pi_i^2)$, because $L(\pi_i \pi_{i'}) = 0$ for $i \neq i'$. By Lemma 6.5, $\det H_K = (\det T)^{-2} \prod_i L(\pi_i^2) = \prod_i L(\pi_i^2)$. □

For $\mathrm{d}x$ on $[0,1]$: $1,\ 1 \cdot \frac{1}{12} = \frac{1}{12},\ \frac{1}{12} \cdot \frac{1}{180} = \frac{1}{2160},\ \frac{1}{2160} \cdot \frac{1}{2800} = \frac{1}{6048000}$, the determinants of Example 6.3. Equivalently $\|\pi_K\|^2 = \det H_{K+1} / \det H_K$: each new orthogonal polynomial multiplies the determinant by its squared norm.

6.3.2 Heine's formula and the Coulomb gas

Theorem 6.9 (Heine's formula)**.** *For a measure μ on $\mathbb{R}$ with finite moments,*

$$\det \Big[\int y^{i+j} \mathrm{d}\mu \Big]_{0 \le i,j < K} = \frac{1}{K!} \int \cdots \int \prod_{1 \le i < j \le K} (x_i - x_j)^2 \, \mathrm{d}\mu(x_1) \cdots \mathrm{d}\mu(x_K) \ .$$

(See e.g. Szegő [32]. The algebraic proof, through the Vandermonde determinant and Andreief's identity, is in Chapter 9, where the note's version [note, Proposition 5.1] is proved.)

Example 6.10. For $\mathrm{d}x$ on $[0,1]$ and $K = 2$: $\frac{1}{2} \int_0^1 \int_0^1 (x_1 - x_2)^2 \mathrm{d}x_1 \mathrm{d}x_2 = \frac{1}{2}(\frac{1}{3} - 2 \cdot \frac{1}{4} + \frac{1}{3}) = \frac{1}{12}$. The $K = 3$ case, integrated symbolically, gives $\frac{1}{2160}$, as in Example 6.3.

Intuition: the Coulomb-gas reading. Write $\mathrm{d}\mu = e^{-V(x)} \mathrm{d}x$. Then the integrand of Heine's formula is $\exp(-E)$ with

$$E(x_1, \dots, x_K) = \sum_i V(x_i) - 2 \sum_{i<j} \log |x_i - x_j| \ ,$$

the energy of K unit charges on a line, each in the external potential V, repelling each other with the two-dimensional (logarithmic) Coulomb interaction, at inverse temperature $\beta = 2$. So $K! \det H_K$ is a partition function: the same as that of the eigenvalues of a $K \times K$ Hermitian random matrix with potential V. For large K the integral is dominated by the minimum-energy configuration, an equilibrium density of charges, and $\log \det H_K \approx -E_{\min}$; this is how the note estimates the real size of the coefficients of Δ_K (Chapter 10). For $\mathrm{d}x$ on $[0,1]$ the charges are confined to $[0,1]$ and push each other towards the end points, and the factor $(x_1 - x_2)^2$ is 1 at $(0,1)$ and 0 at $(\frac{1}{2}, \frac{1}{2})$. *Where the analogy stops:* the note's functional is not integration against any measure on $\mathbb{R}$. The note's Heine expansion (Chapter 9) is the same algebra applied to the node functionals L_k of Section 6.5, which are finite sums of Taylor coefficients; the "charges" then sit on the nodes and their "Boltzmann weights" are rational numbers of either sign.

6.3.3 Positivity

Proposition 6.11 (positive measures give positive Hankel determinants)**.** *If $\mu \geq 0$ on $\mathbb{R}$ has finite moments and its support contains at least K points, then* $\det H_K > 0$.

Proof. For a nonzero coefficient vector $u = (u_0, \dots, u_{K-1})$ let $P = \sum_i u_i y^i \neq 0$. Then

$$u^{\mathsf{T}} H_K u = \sum_{i,j} u_i u_j \int y^{i+j} \mathrm{d}\mu = \int P(y)^2 \mathrm{d}\mu(y) \ .$$

The integrand is ≥ 0. It is > 0 except at the at most $K-1$ roots of P, and the support of μ has a point outside them, near which P^2 is bounded below by a positive constant on a set of positive measure; so the integral is > 0. Hence the symmetric matrix H_K is positive definite, all its eigenvalues are positive, and its determinant, their product, is positive. □

The hypothesis on the support is needed: for the point mass $\mu = \delta_3$ (so $L(P) = P(3)$), $H_2 = \left(\begin{smallmatrix} 1 & 3 \\ 3 & 9 \end{smallmatrix}\right)$ has determinant 0, because $L\big((y-3)^2\big) = 0$.

What just happened. For a positive measure on $\mathbb{R}$, the inequality $L(P^2) > 0$ for $P \neq 0$ makes the Hankel matrix positive definite, so every Hankel determinant is positive, equal to the product of the squared norms of the monic orthogonal polynomials, and equal to a Coulomb-gas partition function (Heine). The first fact is exactly what an irrationality proof needs and cannot take for granted: that the determinant is not zero.

6.4 No positivity in $\mathbb{Q}_3$

The proof of Proposition 6.11 starts from "$P^2 \geq 0$". In $\mathbb{Q}_3$ there is no such inequality: $\mathbb{Q}_3$ has no ordering compatible with its arithmetic (-2 is a square in $\mathbb{Q}_3$, see below, so "squares are ≥ 0" would make $-2 \geq 0$), and the size $|\cdot|_3$ does not see signs. The Volkenborn integral already shows the consequences.

Example 6.12 (the Volkenborn integral has negative "variance")**.** With $m_j = B_j$: $\det H_2 = B_0 B_2 - B_1^2 = \frac{1}{6} - \frac{1}{4} = -\frac{1}{12}$. In the language of probability, $\int_{\mathbb{Z}_3} t^2 \mathrm{d}t - \big(\int_{\mathbb{Z}_3} t \, \mathrm{d}t\big)^2 = -\frac{1}{12}$ would be the variance of a random variable uniformly distributed on $\mathbb{Z}_3$, and it is negative. One finds $\det H_K = 1, \ -\frac{1}{12}, \ -\frac{1}{540}, \ \frac{1}{42000}$ for $K = 1, \dots, 4$: nonzero here, but with no sign pattern that a positivity argument could predict.

The Hankel determinant can also vanish. Here is an example built by hand. Fix $c \in \mathbb{Q}_3$ and put

$$L_c(P) = \int_{\mathbb{Z}_3} P(t)\,(t^2 + c)\,\mathrm{d}t \ , \qquad m_j = B_{j+2} + c\,B_j \ ,$$

the Volkenborn integral with the polynomial weight $t^2 + c$ (linear in P, since the Volkenborn integral is). Then $m_0 = \frac{1}{6} + c$, $m_1 = -\frac{c}{2}$ (as $B_3 = 0$), $m_2 = -\frac{1}{30} + \frac{c}{6}$, and

$$\det H_2 = \Big(\frac{1}{6} + c\Big)\Big(-\frac{1}{30} + \frac{c}{6}\Big) - \frac{c^2}{4} = -\frac{15c^2 + c + 1}{180} \ .$$

Over $\mathbb{R}$ the quadratic $15c^2 + c + 1$ has discriminant $1 - 60 = -59 < 0$ and is always positive, so $\det H_2 < 0$ for every real (in particular every rational) c. Over $\mathbb{Q}_3$ it has two roots $c = \frac{-1 \pm \sqrt{-59}}{30}$, because -59 is a square in $\mathbb{Z}_3$:

Fact 6.13 (Hensel's lemma, simplest case)**.** *If $f \in \mathbb{Z}_p[s]$, $f(s_0) \equiv 0 \pmod p$ and $f'(s_0) \not\equiv 0 \pmod p$, then there is a unique $s \in \mathbb{Z}_p$ with $f(s) = 0$ and $s \equiv s_0 \pmod p$. (Koblitz,* p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Ch. I.) The idea is Newton's method: $s_{j+1} = s_j - f(s_j)/f'(s_j)$ doubles the number of correct digits at each step, and the division by $f'(s_j)$ is harmless because $f'(s_j)$ is a unit.*

For $f(s) = s^2 + 59$ and $s_0 = 1$: $f(1) = 60 \equiv 0$ and $f'(1) = 2 \not\equiv 0 \pmod 3$. The same argument with $f(s) = s^2 + 2$ and $s_0 = 1$ shows that -2 is a square in $\mathbb{Z}_3$, as used above.

Example 6.14 (a 3-adic functional with vanishing Hankel determinant)**.** Eight Newton steps modulo 3^{30} give $s = \sqrt{-59}$ with ternary digits (from 3^0) 12010221110001000212…, and $s^2 + 59 \equiv 0 \pmod{3^{30}}$. Take $c = \frac{s-1}{30}$. Since $s \equiv 1 \pmod 3$, $s - 1$ is divisible by 3 and $c \in \mathbb{Z}_3$; its digits are 202222112101022…. Then $60(15c^2 + c + 1) = (30c)^2 + 2(30c) + 60 = s^2 + 59 = 0$, so $\det H_2 = 0$ for L_c. In words: there is a nonzero polynomial $P = u_0 + u_1 t$ with $L_c(PQ) = 0$ for every Q of degree ≤ 1, $Q = P$ included, a "vector of length zero", which a positive measure cannot have.

Intuition: what this means for the proof. The note's moments $L(y^m)$ are 3-adic numbers, and the note's functional is an integral over $\mathbb{Z}_3$ against a rational weight. Example 6.14 shows that a functional of this general type can have a vanishing Hankel determinant, and that whether it does can depend on 3-adic irrational parameters; there is no inequality that rules it out. Even more to the point, the polynomial $\Delta_K(X)$ of the next section has rational coefficients and may have rational roots: for $n = 1$, $\Delta_1(X)$ is linear with the root $x_0 = \frac{10046105}{2594496}$ (Section 6.7). If $\zeta_3(5)$ were equal to such a root, the determinant would be 0 and the whole argument would collapse. This is why the note needs a separate theorem, the non-vanishing of $\Delta_K(a/b)$ for the hypothetical value a/b [note, Theorem 3.13], proved by divisibility at an auxiliary prime (Chapters 7 and 14). The note says so in [note, Section 1].

6.5 The Hankel polynomial

6.5.1 Why an indeterminate

Recall from Chapter 5 that $L(P) = \beta(P) + \zeta_3(5)\,\alpha(P)$ with $\beta(P) = \sum_{k,a} \beta_{k,a} P_a(k)$ and $\alpha(P) = \sum_{k,a} \alpha_{k,a} P_a(k)$, where $P_a(k) = [z^a]P(-k + z)$ is the a-th Taylor coefficient of P at the node $y = -k$ and the local constants $\beta_{k,a}, \alpha_{k,a}$ are the rational numbers of [note, (2.21)]. The irrationality proof assumes $\zeta_3(5) = a/b$ and derives a contradiction. Under that assumption the single number $L(P)$ would not determine the pair $(\beta(P), \alpha(P))$, so a polynomial "read off from the values of L" would be ill defined. The note avoids this by building everything from the local constants, with a symbol X in the place of $\zeta_3(5)$ (Chapter 5, end of the section on purity).

6.5.2 The definition

Definition 6.15 (the Hankel polynomial; [note, Definition 2.23])**.** For a node $k \in \mathcal{N} = \{-n, \dots, 2n\}$ put $c_{k,a}(X) = \beta_{k,a} + X\alpha_{k,a} \in \mathbb{Q}[X]$ for $0 \leq a \leq 3$ and $c_{k,a} = 0$ for $a \geq 4$. Define $\mathbb{Q}[X]$-linear maps on $\mathbb{Q}[X][y]$ by [note, (2.24)]

$$L_k(P) = \sum_{a=0}^{3} c_{k,a}(X)\, P_a(k)\ , \qquad \Lambda = \sum_{k \in \mathcal{N}} L_k\ , \qquad \Lambda(P) = \beta(P) + X\,\alpha(P)\ .$$

For $K \geq 1$ the *Hankel polynomial* is [note, (2.25)]

$$\Delta_K(X) = \det\left[\Lambda(y^{i+j})\right]_{0 \leq i,j < K} = \det\left[\beta(y^{i+j}) + X\,\alpha(y^{i+j})\right]_{0 \leq i,j < K} \in \mathbb{Q}[X]\ .$$

Intuition. L_k is "the share of the node k" in the functional: it looks at P only through its first four Taylor coefficients at $y = -k$ and weighs them with the four local constants of that node. Λ is the purity formula of Chapter 5, read as a definition, with X for $\zeta_3(5)$. It is defined on all polynomials, but it agrees with L (at $X = \zeta_3(5)$) only where the purity

lemma applies, $\deg(PW) \le -2$. $\Delta_K(X)$ is the Hankel determinant of Λ: a polynomial in X with rational coefficients, which does not depend on what $\zeta_3(5)$ is.

Example 6.16 ($n = 1$, $K = 1$)**.** $\Delta_1(X) = \Lambda(1) = \sum_k c_{k,0} = -\frac{10046105}{15552} + \frac{13513}{81}X$, from the column $a = 0$ of the table of local constants in Chapter 5. All four values $\Delta_K(X)$, $K \le 4$, are in Section 6.7.

6.5.3 The degree

Lemma 6.17 ([note, Section 2.2], after Definition 2.23)**.** $\deg \Delta_K \le K$. *More precisely, the coefficient of* X^0 *is* $\det[\beta(y^{i+j})]$ *and the coefficient of* X^K *is* $\det[\alpha(y^{i+j})]$.

Proof. By the Leibniz formula, $\Delta_K = \sum_\sigma \operatorname{sgn}(\sigma) \prod_{i<K} \Lambda(y^{i+\sigma(i)})$, a sum over the permutations σ of $\{0, \dots, K-1\}$. Every factor is affine in X, of degree ≤ 1, so every product of K factors has degree $\le K$. Setting $X = 0$ in every entry gives the coefficient of X^0, which is therefore the same Leibniz sum with β in place of Λ. The coefficient of X^K in a product of K affine factors $\beta_i + X\alpha_i$ is $\prod \alpha_i$, so the coefficient of X^K in Δ_K is the Leibniz sum of $\det[\alpha(y^{i+j})]$. □

For $n = 1$ and $K \le 4$ the degree is exactly K, and both coefficient identities hold (Section 6.7).

6.5.4 The value at $\zeta_3(5)$, and why $K \le 3n + 1$

Proposition 6.18 ([note, (2.26)])**.** *If* $K \le 3n + 1$, *then* $\Delta_K(\zeta_3(5)) = \det\left[L(y^{i+j})\right]_{0 \le i,j < K}$.

Proof. The entries of the Hankel matrix involve the monomials y^m with $m = i+j \le 2(K-1) = 2K-2$. If $K \le 3n+1$, then $2K-2 \le 6n \le 6n+1$. The purity lemma [note, Lemma 2.19] applies to y^m exactly when $\deg(y^m W) = m - 6n - 3 \le -2$, i.e. $m \le 6n+1$ (Chapter 5), and then $L(y^m) = \beta(y^m) + \zeta_3(5)\alpha(y^m) = \Lambda(y^m)|_{X=\zeta_3(5)}$. So every entry of $[\Lambda(y^{i+j})]$ evaluated at $X = \zeta_3(5)$ equals the corresponding entry of $[L(y^{i+j})]$. Substituting $X = \zeta_3(5)$ commutes with taking the determinant (the determinant is a polynomial in the entries), so the two determinants agree. □

The bound is sharp for this argument: $K = 3n+2$ would need $m = 2K-2 = 6n+2$, where $\deg(y^m W) = -1$ and the purity lemma fails. For $n = 1$, the largest admissible size is $K = 4$, which uses $y^0, \dots, y^6$; purity holds up to y^7, and the next size $K = 5$ would need y^8. Chapter 5 showed numerically that for y^8 the true $L(y^8)$ differs from $\beta(y^8) + \zeta_3(5)\alpha(y^8)$ by the missing term $-54\,\zeta_3(3)$. So $\Delta_5(\zeta_3(5))$ is the determinant of a matrix whose bottom-right entry is not $L(y^8)$. The proof takes $K \le 3n-2$ [note, Theorem 3.13], well inside the range. The remark at the end of the note's paragraph is the division of labour: the 3-adic estimate (Chapter 8) is about the right side of Proposition 6.18, a determinant of 3-adic numbers; the size, denominator and non-vanishing estimates (Chapters 10 to 14) are about the rational coefficients of $\Delta_K(X)$.

6.6 The jet form and the node matrices

6.6.1 The Leibniz rule for Taylor coefficients

The Taylor coefficients at a point multiply like the coefficients of power series. If $P(-k+z) = \sum_a P_a(k) z^a$ and $Q(-k+z) = \sum_b Q_b(k) z^b$, then the coefficient of z^m in the product is

$$(PQ)_m(k) = \sum_{a+b=m} P_a(k)\, Q_b(k)\ . \tag{6.1}$$

This is the Leibniz rule $(PQ)^{(m)} = \sum \binom{m}{a} P^{(a)} Q^{(m-a)}$ divided by $m!$. For a monomial the Taylor coefficients come from the binomial theorem: $(-k+z)^i = \sum_a \binom{i}{a}(-k)^{i-a} z^a$, so

$$(y^i)_a(k) = \binom{i}{a}(-k)^{i-a} \qquad \text{(zero for } a > i\text{)} \; . \tag{6.2}$$

Example 6.19. At $k = 1$ ($y = -1$): $(-1+z)^2 = 1-2z+z^2$ and $(-1+z)^3 = -1+3z-3z^2+z^3$. So $(y^3)_a(1) = -1, 3, -3, 1$ for $a = 0, 1, 2, 3$, which is $\binom{3}{a}(-1)^{3-a}$. And (6.1) with $P = Q = y$: $(y^2)_1(1) = (y)_0(y)_1 + (y)_1(y)_0 = (-1)(1) + (1)(-1) = -2$.

6.6.2 The jet form

Proposition 6.20 (the jet form; [note, (2.27)])**.**

$$\Lambda(y^{i+j}) = \sum_{k \in \mathcal{N}} \sum_{a+b \le 3} c_{k,a+b}\, (y^i)_a(k)\, (y^j)_b(k) \; .$$

Proof. By definition $\Lambda(y^{i+j}) = \sum_k \sum_{m=0}^{3} c_{k,m} (y^{i+j})_m(k)$. By (6.1) with $P = y^i$, $Q = y^j$, $(y^{i+j})_m(k) = \sum_{a+b=m} (y^i)_a(k)(y^j)_b(k)$. Insert this and replace the double sum over $m \le 3$ and $a + b = m$ by a single sum over the pairs (a, b) with $a + b \le 3$, in which $c_{k,m} = c_{k,a+b}$. □

6.6.3 A sum of matrices of rank at most four

Write the jet form in matrix language. For a node k let J_k be the $4 \times K$ matrix with entries $(J_k)_{a,i} = (y^i)_a(k)$, $0 \le a \le 3$, $0 \le i < K$: its column i holds the first four Taylor coefficients of y^i at the node. Let

$$C_k = \left[c_{k,a+b}\right]_{0 \le a,b \le 3} = \begin{pmatrix} c_{k,0} & c_{k,1} & c_{k,2} & c_{k,3} \\ c_{k,1} & c_{k,2} & c_{k,3} & 0 \\ c_{k,2} & c_{k,3} & 0 & 0 \\ c_{k,3} & 0 & 0 & 0 \end{pmatrix},$$

a 4×4 Hankel matrix that vanishes below the anti-diagonal (because $c_{k,a} = 0$ for $a \ge 4$). Then Proposition 6.20 says $\Lambda(y^{i+j}) = \sum_k (J_k^{\mathsf{T}} C_k J_k)_{ij}$, that is,

$$H_K = \left[\Lambda(y^{i+j})\right]_{i,j<K} = \sum_{k \in \mathcal{N}} J_k^{\mathsf{T}}\, C_k\, J_k \; . \tag{6.3}$$

Figure 6.1 shows the shapes. Each term is a product through a 4×4 matrix, so its rank is at most 4, however large K is. The term $J_k^{\mathsf{T}} C_k J_k$ is itself a Hankel matrix: by the same computation it is $[L_k(y^{i+j})]$, the Hankel matrix of the node functional L_k.

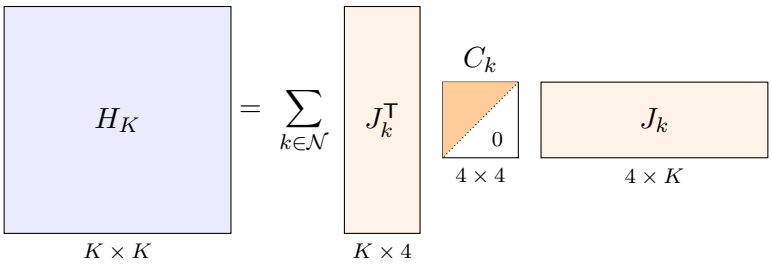


Figure 6.1: The jet form (6.3): the $K \times K$ Hankel matrix is a sum of $3n + 1$ terms, one per node, each passing through the 4×4 matrix C_k of local constants, which is zero below its anti-diagonal (shaded: the entries $c_{k,a+b}$ with $a + b \le 3$). Each term has rank at most 4.

Intuition: a node can absorb at most four rows. The node k sees a polynomial only through its first four Taylor coefficients at $y = -k$, i.e. through P modulo $(y+k)^4$: a polynomial divisible by $(y+k)^4$ is invisible to L_k. So the node functional "lives" on a 4-dimensional space, and its Hankel matrix has rank ≤ 4. Now expand $\Delta_K = \det\left(\sum_k M_k\right)$, $M_k = J_k^{\mathsf{T}} C_k J_k$, by multilinearity in the rows: Δ_K is the sum, over all ways φ of assigning to each row i a node $\varphi(i)$, of the determinant of the matrix whose row i is row i of $M_{\varphi(i)}$. If five or more rows are assigned to the same node k, they are rows of M_k, all lying in the at most 4-dimensional row space of M_k, hence linearly dependent, and that determinant is 0. So only assignments with at most four rows per node survive. This is the discrete skeleton of the note's Heine expansion [note, Proposition 5.1]: there the K "charges" are distributed over the nodes, at most four per node (Chapter 9). In the language of physics, a node behaves like an orbital that holds at most four particles; the analogy is only about counting, since nothing here is fermionic.

The note's paragraph after [note, (2.27)] names the three places where this structure is used. The Heine expansion (Chapter 9) expands Δ_K over the ways of distributing the K rows among the nodes. The denominator estimates (Chapters 11 to 13) bound the denominators contributed by each node separately, since a node enters only through its matrix C_k. The non-vanishing theorem (Chapter 14) chooses, by Lemma 6.5 with a unimodular T, a basis of polynomials in which the contributions of different nodes decouple modulo the auxiliary prime: in the note's [note, (6.13)], $\Lambda(E_x E_{x'})$ is written in exactly the form of Proposition 6.20, with the Taylor coefficients of the new basis polynomials E_x in place of those of y^i.

Example 6.21 (node matrices for $n = 1$)**.** From the local constants of Chapter 5, for the node $k = 1$:

$$C_1 = \begin{pmatrix} \frac{7}{16} - \frac{27}{2}X & X - \frac{23}{96} & \frac{5}{48} & -\frac{1}{48} \\ X - \frac{23}{96} & \frac{5}{48} & -\frac{1}{48} & 0 \\ \frac{5}{48} & -\frac{1}{48} & 0 & 0 \\ -\frac{1}{48} & 0 & 0 & 0 \end{pmatrix}, \qquad J_1 = \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -2 & 3 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (K = 4).$$

The node $k = 0$ is special: $\beta_{0,a} = 0$ for all a (Chapter 5) and $\alpha_{0,a} = 0$ for $a \ge 2$, so

$$C_0 = \begin{pmatrix} -\frac{27}{2}X & -X & 0 & 0 \\ -X & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

has rank 2; this holds for every n, since $\mathrm{HS}_3(0, \cdot) = 0$. The ranks are $4, 2, 4, 4$ for $k = -1, 0, 1, 2$. For $K = 4$ the matrix J_k is upper triangular with 1 on the diagonal ($(y^i)_i(k) = 1$), so $\det J_k = 1$, and C_k has determinant $c_{k,3}^4$ (the anti-diagonal product; reversing four indices is an even permutation). At $X = 0$ the node-1 term is

$$J_1^{\mathsf{T}} C_1 J_1 = \begin{pmatrix} \frac{7}{16} & -\frac{65}{96} & \frac{49}{48} & -\frac{143}{96} \\ -\frac{65}{96} & \frac{49}{48} & -\frac{143}{96} & \frac{101}{48} \\ \frac{49}{48} & -\frac{143}{96} & \frac{101}{48} & -\frac{277}{96} \\ -\frac{143}{96} & \frac{101}{48} & -\frac{277}{96} & \frac{185}{48} \end{pmatrix}, \qquad \det = \left(\frac{1}{48}\right)^4 = \frac{1}{5308416},$$

visibly a Hankel matrix, as it must be. For $K = 5$ each of the four node terms $J_k^{\mathsf{T}} C_k J_k$ has rank 4 (rank 2 for $k = 0$) and determinant 0, as the rank bound predicts, while their sum is the full Hankel matrix.

6.7 A worked example: $n = 1$

All computations in this section are in exact rational arithmetic in $\mathbb{Q}[X]$, starting from the local constants of Chapter 5.

6.7.1 The moments

Example 6.22 (the moments $\Lambda(y^m)$, $n = 1$)**.** Computing $\Lambda(y^m) = \sum_k \sum_a c_{k,a}(y^m)_a(k)$ with Taylor coefficients from series expansion gives:

m	$\beta(y^m)$	$\alpha(y^m)$	$v_3\big(L(y^m)\big)$
0	$-\frac{10046105}{15552}$	$\frac{13513}{81}$	12
1	$\frac{10046105}{31104}$	$-\frac{13513}{162}$	12
2	$-\frac{39778861}{31104}$	$\frac{39989}{162}$	10
3	$\frac{54645239}{31104}$	$-\frac{53227}{162}$	11
4	$-\frac{112590361}{31104}$	$\frac{48065}{162}$	8
5	$\frac{192074855}{31104}$	$-\frac{33703}{162}$	8
6	$-\frac{354213313}{31104}$	$-\frac{170659}{162}$	6

These agree with the values of Chapter 5, where they were also confirmed against Riemann sums of the defining integral. Every $\beta(y^m)$ has $v_3 = -5$ and every $\alpha(y^m)$ has $v_3 = -4$, while $L(y^m) = \beta + \zeta_3(5)\alpha$ has v_3 between 6 and 12: the two parts cancel in their first 11 to 17 ternary digits.

6.7.2 The Hankel polynomials

Example 6.23 ($\Delta_K(X)$ for $n = 1$)**.** With the denominators and numerators factored into primes (the large factors are prime, including the unfactored 19-digit numerator):

$$
\begin{aligned}
\Delta_1(X) &= -\frac{5\cdot 103\cdot 19507}{2^6\cdot 3^5} + \frac{13513}{3^4}X\ ,\\
\Delta_2(X) &= \frac{5\cdot 7\cdot 59\cdot 103\cdot 18701\cdot 19507}{2^{14}\cdot 3^8} - \frac{7\cdot 257\cdot 49627103}{2^7\cdot 3^7}X\\
&\quad + \frac{5\cdot 7\cdot 211\cdot 13513}{2^2\cdot 3^6}X^2\ ,\\
\Delta_3(X) &= \frac{7\cdot 59\cdot 163\cdot 317\cdot 18701\cdot 138053}{2^{17}\cdot 3^9} - \frac{7\cdot 13\cdot 61\cdot 137\cdot 373\cdot 5585213}{2^{12}\cdot 3^7}X\\
&\quad + \frac{7\cdot 13597\cdot 10143071}{2^4\cdot 3^6}X^2 - \frac{5\cdot 7^3\cdot 211\cdot 18869}{3^6}X^3\ ,\\
\Delta_4(X) &= \frac{131\cdot 163\cdot 317\cdot 138053\cdot 92599879}{2^{22}\cdot 3^9} - \frac{8321596318969878949}{2^{16}\cdot 3^8}X\\
&\quad + \frac{7\cdot 23\cdot 1763417967849389}{2^{12}\cdot 3^6}X^2 - \frac{7\cdot 13\cdot 16178672776103}{2^5\cdot 3^6}X^3 + \frac{7^3\cdot 18869\cdot 411529}{3^5}X^4\ .
\end{aligned}
$$

In each case $\deg \Delta_K = K$, the constant term equals $\det\big[\beta(y^{i+j})\big]$ and the top coefficient equals $\det\big[\alpha(y^{i+j})\big]$ (Lemma 6.17). The denominators contain only the primes 2 and 3, with $3^5, \dots, 3^9$; the real sizes of the coefficients grow from about 10^2 to about 10^{11}. For $n = 1$ no prime $p \geq 5$ occurs in the denominators, although the harmonic sums $\mathrm{HS}_3(2, M) = \sum_{u\in\{1,2,4,5\}}(3/u)^M$ entering $\beta_{2,a}$ contain powers of 5 in their denominators; how the denominators at primes $p \neq 3$ are controlled in general is the subject of Chapters 11 to 13.

The shared prime factors are not an accident. One finds that $\Lambda\big((y + \frac{1}{2})^m\big) = 0$ for $m = 1, 3, 5, 7$, both in its β and in its α part; $-\frac{n}{2} = -\frac{1}{2}$ is the centre of the antisymmetry

$W(-n-y) = -W(y)$ of the weight (Chapter 5). In the basis $(y+\frac{1}{2})^i$, which arises from the monomials by a lower triangular T with 1 on the diagonal, the Gram matrix $[\Lambda((y+\frac{1}{2})^{i+j})]$ therefore has zeros in a checkerboard pattern, and by Lemma 6.5 (with $\det T = 1$) Δ_K factors as the determinant of the block of even indices times that of the odd indices. For $K \le 4$ one finds indeed $\Delta_K = \det(\text{even}) \cdot \det(\text{odd})$; for example

$$\Delta_2(X) = \frac{2594496X - 10046105}{15552} \cdot \frac{7\,(202560X - 1103359)}{6912} \,,$$

which is why Δ_1 divides Δ_2. For $n = 3$ one finds likewise $\Lambda((y+\frac{3}{2})^m) = 0$ for all odd $m \le 19$. Whether this holds for all n is not proved here; the note neither states nor uses it, and it plays no role below; it is an illustration of Lemma 6.5.

6.7.3 The rank-four decomposition

For $n = 1$ and $K = 1, \dots, 5$, the four node terms $J_k^{\mathsf{T}} C_k J_k$, with J_k from the closed form (6.2) and C_k from the local constants, add up to $[\Lambda(y^{i+j})]$ entry by entry, as polynomials in X. This illustrates Proposition 6.20 for $n = 1$: the left side uses Taylor coefficients of y^{i+j} from series expansion, the right side products of binomial expressions.

6.7.4 The value at $\zeta_3(5)$

Precision. We approximate $\zeta_3(5)$ by a rational number from the series [note, (2.13)] truncated after $C = 125$ terms, as in Chapter 5. The truncations after 125 and 145 terms agree to $v_3 = 124$. So write $\zeta_3(5) = Z + \delta$ with the rational approximation Z and $v_3(\delta) \ge 124$ (and the truncation lemma of Chapter 3 bounds the truncation error rigorously). If $\Delta_K = \sum_j f_j X^j$, then

$$\Delta_K(Z+\delta) - \Delta_K(Z) = \sum_{j \ge 1} f_j \sum_{i=1}^{j} \binom{j}{i} Z^{j-i} \delta^i \,,$$

and since $v_3(\delta) > v_3(Z) = -1$ the terms with $i = 1$ have the smallest valuation, so the difference has $v_3 \ge v_3(\delta) + \min_{j \ge 1} v_3(f_j Z^{j-1})$. This bound is ≥ 116 for $K \le 4$, far above the valuations below; so the computed digits of $\Delta_K(\zeta_3(5))$ are exact.

Example 6.24 ($v_3(\Delta_K(\zeta_3(5)))$ for $n = 1$).

K	$v_3(f_j\,\zeta_3(5)^j)$, $j = 0..K$	$v_3\big(\Delta_K(\zeta_3(5))\big)$	cancelled digits	first digits of $\Delta_K(\zeta_3(5))$
1	$-5, -5$	12	17	3^{12}: 222122101202
2	$-8, -8, -8$	22	30	3^{22}: 110001021002
3	$-9, -8, -8, -9$	31	40	3^{31}: 122002022102
4	$-9, -9, -8, -9, -9$	38	47	3^{38}: 120102002120

The second column gives the valuation of each term $f_j \zeta_3(5)^j$ (recall $v_3(\zeta_3(5)) = -1$). All terms have v_3 between -9 and -5, yet their sum has $v_3 = 12, 22, 31, 38$: the terms cancel in their leading 17 to 47 ternary digits. The case $K = 1$ is $v_3(L(1)) = 12$ of Chapter 5. By Proposition 6.18, these are the valuations of $\det\big[L(y^{i+j})\big]_{i,j<K}$, a determinant of 3-adic numbers.

Intuition: gain against coefficient size, in a toy form. The number $v_3(\Delta_K(\zeta_3(5)))$ grows with K roughly like K times the valuation of a typical entry (6 to 12), as a determinant of small entries should (Chapter 1): a product of K entries each divisible by 3^v is divisible by 3^{Kv}. The irrationality criterion (Chapter 7) weighs this 3-adic smallness against the real size of the coefficients and against their denominators at primes other than 3. For $n = 1$ one finds, in trits ($\log_3$): $\log_3 \sum_j |f_j| = 6.10,\ 12.64,\ 17.74,\ 23.64$ and $\log_3$ of the 3-free part

of the common denominator $= 3.79,\ 8.83,\ 10.73,\ 13.88$ for $K = 1, \dots, 4$, against 3-adic cancellations of $17, 30, 40, 47$ trits. These numbers say nothing about irrationality: the criterion needs $n \to \infty$, and it must also absorb the unknown height of the hypothetical a/b. The theorems that make the three quantities grow like n^2 at definite rates are [note, Theorem 3.5] (gain), [note, Theorem 3.8] (size) and [note, Theorem 3.10] (denominators), compared in Chapter 7.

6.7.5 A triangular change of basis

Example 6.25 (the basis of [note, Lemma 4.1] for $K = 4$)**.** Chapter 8 replaces the monomials by the polynomials $F_0 = 1$, $F_1 = 3y$, $F_2 = 3(y-\frac{1}{3})(y-\frac{2}{3}) = 3y^2-3y+\frac{2}{3}$, $F_3 = 3yF_2 = 9y^3-9y^2+2y$ [note, (4.2)], which take values in $\mathbb{Z}_3$ on the integration set S (why, and why these, is explained there). The coefficient matrix and its determinant are

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ \frac{2}{3} & -3 & 3 & 0 \\ 0 & 2 & -9 & 9 \end{pmatrix}, \qquad \det T = 1 \cdot 3 \cdot 3 \cdot 9 = 81 = 3^4 \ ,$$

the product of the leading coefficients. Indeed TH_4T^{T} equals $[\Lambda(F_iF_{i'})]$ computed directly, and $\det[\Lambda(F_iF_{i'})] = 81^2\,\Delta_4(X)$ as polynomials in X (Lemma 6.5). The new Gram matrix is no longer Hankel. Its effect shows at $X = \zeta_3(5)$: the valuations of the entries are

$$[v_3\,L(y^{i+j})] = \begin{pmatrix} 12 & 12 & 10 & 11 \\ 12 & 10 & 11 & 8 \\ 10 & 11 & 8 & 8 \\ 11 & 8 & 8 & 6 \end{pmatrix}, \qquad [v_3\,L(F_iF_{i'})] = \begin{pmatrix} 12 & 13 & 12 & 12 \\ 13 & 12 & 12 & 12 \\ 12 & 12 & 11 & 12 \\ 12 & 12 & 12 & 11 \end{pmatrix}.$$

In the monomial basis the entries get less divisible as the degree grows (down to 6); in the basis F_i they stay at 11 or more. With $\nu_i = 0, -1, -1, -2$ (the negatives of the valuations of the leading coefficients), the bound [note, (4.3)] reads $v_3(\Delta_4(\zeta_3(5))) \geq 2\sum_i \nu_i + 4\cdot 11 = -8+44 = 36$; the actual value is 38. This is the mechanism of Chapter 8 in miniature: the change of basis costs $2 \cdot 4 = 8$ digits, and makes every entry uniformly small.

Example 6.26 (the rational root of Δ_1)**.** $\Delta_1(X) = \alpha(1)(X - x_0)$ with $x_0 = \frac{10046105}{2594496}$, a rational number with $v_3(x_0) = -1$. Its ternary digits from 3^{-1} are 20121001000110101211, those of $\zeta_3(5)$ are 20121001000110101121: they agree in 17 digits, $v_3(\zeta_3(5) - x_0) = 16$, which is $v_3(\Delta_1(\zeta_3(5))) - v_3(\alpha(1)) = 12 + 4$. So x_0 is a good rational approximation of $\zeta_3(5)$, and it is exactly the kind of number that the non-vanishing theorem has to keep away from: if $\zeta_3(5)$ were equal to x_0, then $\Delta_1(\zeta_3(5))$ would be 0. The proof does not exclude this by computation, but by [note, Theorem 3.13] for large n and K (Chapter 14).

Check yourself 6.27. Why does the change of basis $\{1, y\} \to \{1, 2y - 1\}$ in Example 6.6 multiply the determinant by 4, and what would $\{1,\ y - \frac{1}{2}\}$ do?

Answer. $\det T = 2$ (the leading coefficient of $2y - 1$), and the determinant changes by $(\det T)^2 = 4$. For $\{1, y - \frac{1}{2}\}$, $T = \left(\begin{smallmatrix} 1 & 0 \\ -1/2 & 1 \end{smallmatrix}\right)$ has $\det T = 1$, so the determinant stays $\frac{1}{12}$; the Gram matrix becomes $\mathrm{diag}(1, \frac{1}{12})$, the case $K = 2$ of Proposition 6.8.

Check yourself 6.28. Why can the node $k = 0$ never absorb more than two rows in the expansion of Δ_K?

Answer. Its matrix C_0 has only the entries $c_{0,0} = \alpha_{0,0}X$ and $c_{0,1} = \alpha_{0,1}X$, because $\beta_{0,a} = 0$ ($\mathrm{HS}_3(0, \cdot) = 0$) and $\alpha_{0,a} = 0$ for $a \geq 2$. So C_0 has rank at most 2, and so has $J_0^{\mathsf{T}}C_0J_0$; three rows taken from it are linearly dependent. (Each of its terms carries a factor X.)

Summary of the chapter

The Hankel matrix $[L(y^{i+j})]$ of a linear functional is the Gram matrix of the monomials for the bilinear form $L(PQ)$; a change of basis by a matrix T multiplies its determinant by $(\det T)^2$ (Lemma 6.5), which the note uses with a triangular T in Chapter 8 and a unimodular T in Chapter 14. For a positive measure on $\mathbb{R}$ the Hankel determinant is the product of the squared norms of the monic orthogonal polynomials (shifted Legendre polynomials for $\mathrm{d}x$ on $[0,1]$), a Coulomb-gas partition function by Heine's formula, and positive. In $\mathbb{Q}_3$ there is no positivity: the Volkenborn integral has "variance" $-\frac{1}{12}$, and the weighted Volkenborn integral with weight t^2+c, $c=\frac{-1+\sqrt{-59}}{30}\in\mathbb{Z}_3$, has a vanishing 2×2 Hankel determinant. Hence the separate non-vanishing theorem. The note replaces $\zeta_3(5)$ by an indeterminate X and defines the Hankel polynomial $\Delta_K(X)=\det\bigl[\Lambda(y^{i+j})\bigr]\in\mathbb{Q}[X]$ [note, Definition 2.23], of degree $\le K$, with $\Delta_K(\zeta_3(5))=\det\bigl[L(y^{i+j})\bigr]$ for $K\le 3n+1$ [note, (2.26)], because the entries use y^m with $m\le 2K-2\le 6n$ and purity holds for $m\le 6n+1$. By the Leibniz rule for Taylor coefficients, the Hankel matrix is the sum $\sum_k J_k^{\mathsf{T}} C_k J_k$ of one matrix of rank at most 4 per node [note, (2.27)], so in a row expansion of Δ_K each node takes at most four rows. For $n=1$ computing $\Delta_1,\dots,\Delta_4$ exactly shows that they satisfy the jet form and that $v_3(\Delta_K(\zeta_3(5)))=12,22,31,38$ although every coefficient has $v_3\ge -9$.

Carried forward: Lemma 6.5 (Chapters 8 and 14); the definition of Λ, L_k, $\Delta_K(X)$ and the identity [note, (2.26)] (Chapter 7); the jet form [note, (2.27)] with the node matrices C_k and the rule "at most four rows per node" (Chapters 9 to 13); and the absence of positivity, which makes Chapter 14 necessary.

Part III

The skeleton of the proof

Chapter 7

The criterion, the four estimates and the proof of the theorem

Where we are. This chapter is the note's [note, Section 3], the hinge of the whole argument. It proves the irrationality criterion [note, Lemma 3.1] in full, evaluates it term by term on the actual Hankel polynomials $\Delta_1, \dots, \Delta_4$ for $n = 1$, proves the dominance lemma [note, Lemma 3.4], states the four estimates [note, Theorems 3.5, 3.8, 3.10, 3.13] with pictures of their leading terms, and then follows the note's deduction of the main theorem [note, Theorem 1.1] from them, including the prime number theorem input. It needs from earlier chapters: the Gauss valuation $v_p(F)$, the content of a polynomial and the gap $|N| \geq 3^{v_3(N)}$ (Chapter 2); the balance-sheet picture and [note, Table 1] (Chapter 1); and the Hankel polynomial $\Delta_K(X)$ with its value $\Delta_K(\zeta_3(5)) = \det[L(y^{i+j})]$ for $K \leq 3n+1$, and the $n = 1$ examples (Chapter 6). The four estimates are only stated here; their proofs fill Chapters 8 to 14.

7.1 The criterion

7.1.1 What we want, and the ingredients

We assume, aiming at a contradiction, that $\zeta_3(5) = a/b$ with coprime integers a and $b > 0$. Then the 3-adic number $\Delta_K(\zeta_3(5))$, which the gain estimate shows to be divisible by a huge power of 3, equals the rational number $\Delta_K(a/b)$. The criterion turns this into an integer and compares its 3-adic valuation with its ordinary size, exactly as in the toy version of Chapter 1. Recall the notation of the note's [note, Conventions]: for $F = \sum_j f_j X^j \in \mathbb{Q}[X]$,

- $v_p(F) = \min_j v_p(f_j)$ is the Gauss valuation (Chapter 2): if it is negative, $p^{-v_p(F)}$ is the worst power of p in a denominator of a coefficient;
- $\|F\|_1 = \sum_j |f_j|$ is the ordinary size of F, with $\|FG\|_1 \leq \|F\|_1 \|G\|_1$;
- $x^+ = \max(x, 0)$, so $(-v_p(F))^+$ is the number of factors p to be cleared from the denominators, and 0 if there are none.

We write $\mathrm{ht}(a/b) = \max(|a|, b)$ and call it the *height* of the fraction; this is our name, not the note's.

Lemma 7.1 (criterion; [note, Lemma 3.1])**.** *Let $F \in \mathbb{Q}[X]$ be nonzero with $\deg F \leq K$, and let $a, b \in \mathbb{Z}$ be coprime with $b > 0$ and $F(a/b) \neq 0$. Then*

$$v_3(F(a/b)) \log_2 3 \leq \log_2 \|F\|_1 + \sum_{p \neq 3} (-v_p(F))^+ \log_2 p + K \log_2 \max(|a|, b) \ , \tag{7.1}$$

where the sum runs over all primes $p \neq 3$, including $p = 2$.

Intuition: a balance sheet in bits. Read (7.1) as an accounting identity turned into an inequality. The left side is how many bits of 3-adic smallness $F(a/b)$ has. The right side is what one has to pay to turn $F(a/b)$ into an integer and to bound that integer: the size of the coefficients, the denominators at all other primes, and the height of the fraction raised to the K-th power. A nonzero integer cannot be more divisible by 3 than it is large (Chapter 2, $|N| \geq 3^{v_3(N)}$), and the inequality is that statement after the bookkeeping. The product formula is the conservation law behind it: what is small at 3 must be large somewhere else.

7.1.2 The proof, step by step

The note's proof is four lines [note, (3.3)]. We split it into seven steps and run each on a real example. The example is $F = \Delta_4$ for $n = 1$ (written out in Chapter 6),

$$\begin{aligned}\Delta_4(X) = {} & \frac{131 \cdot 163 \cdot 317 \cdot 138053 \cdot 92599879}{2^{22} \cdot 3^9} - \frac{8321596318969878949}{2^{16} \cdot 3^8} X \\ & + \frac{7 \cdot 23 \cdot 1763417967849389}{2^{12} \cdot 3^6} X^2 - \frac{7 \cdot 13 \cdot 16178672776103}{2^5 \cdot 3^6} X^3 \\ & + \frac{7^3 \cdot 18869 \cdot 411529}{3^5} X^4 \,,\end{aligned}$$

with the fraction $a/b = x_0 = 10046105/2594496$ that Chapter 6 found as the root of Δ_1; it agrees with $\zeta_3(5)$ in 17 ternary digits ($v_3(\zeta_3(5) - x_0) = 16$), and $b = 2594496 = 2^6 \cdot 3 \cdot 13513$. $\Delta_4(x_0) \neq 0$, so the lemma applies (we come back to $\Delta_1(x_0) = \Delta_2(x_0) = 0$ in Section 7.2).

Step 1: the content. Only finitely many $v_p(F)$ are nonzero: a prime that divides no numerator and no denominator of a coefficient has $v_p(F) = 0$. So $c_F = \prod_p p^{v_p(F)}$ is a finite product, a positive rational number. *Example*: the primes in the coefficients of Δ_4 are $2, 3$ and thirteen others; $v_2(\Delta_4) = -22$, $v_3(\Delta_4) = -9$, and $v_p(\Delta_4) = 0$ for the other thirteen (each of them misses at least one coefficient). So $c_F = 2^{-22}3^{-9}$.

Step 2: the primitive part has integer coefficients. Put $Q = F/c_F$. Dividing by c_F shifts every Gauss valuation by $v_p(c_F) = v_p(F)$ (Chapter 2, $v_p(cF) = v_p(c) + v_p(F)$), so $v_p(Q) = 0$ for every prime p. Since $v_p(Q) \geq 0$ means that no coefficient of Q has p in its denominator, and this holds for every p, the coefficients of Q are integers: $Q \in \mathbb{Z}[X]$. (Since also $v_p(Q) \leq 0$ for every p, their greatest common divisor is 1; the proof does not need this.) *Example*: $Q = 2^{22}3^9\Delta_4$ has the coefficients

$$\begin{gathered}q_0 = 86531539440609939887 \,, \quad q_1 = -1597746493242216758208 \,, \\ q_2 = 7849551775991085038592 \,, \quad q_3 = -5210242942354728026112 \,, \\ q_4 = 90487454804978450432 \,,\end{gathered}$$

with greatest common divisor 1.

Step 3: clearing the denominator of a/b. Write $Q = \sum_{j \leq K} q_j X^j$ with $q_j \in \mathbb{Z}$ (some q_j may be 0 if $\deg F < K$). Then

$$N := b^K Q(a/b) = \sum_{j=0}^{K} q_j \, a^j \, b^{K-j}$$

is an integer, because every exponent $K - j$ is ≥ 0; this is where $\deg F \leq K$ is used. It is nonzero, because $b \neq 0$, $c_F \neq 0$ and $F(a/b) = c_F \, Q(a/b) \neq 0$. *Example*: for Δ_4 and x_0 the integer N has 101 ternary digits ($\log_3 |N| = 100.087$) and $v_3(N) = 50$.

Step 4: the first inequality, $v_3(Q(a/b)) \le v_3(N)$. From $N = b^K\, Q(a/b)$ we get $v_3(N) = K\, v_3(b) + v_3(Q(a/b))$, and $v_3(b) \ge 0$ because b is an integer. Equality holds if $3 \nmid b$. *Example*: $v_3(b) = 1$ for x_0, so $v_3(N) = 4 \cdot 1 + 46 = 50$, with $v_3(Q(x_0)) = 46$. (If $\zeta_3(5) = a/b$ were true, then $3 \mid b$ exactly once, since $v_3(\zeta_3(5)) = -1$ (Chapter 3); so for the real application the inequality is strict by K trits, a loss that the proof can afford.)

Step 5: the integer gap, $v_3(N) \le \log_3 |N|$. This is Chapter 2: $N = 3^{v_3(N)} m$ with a nonzero integer m, so $|N| \ge 3^{v_3(N)}$. It is the only place where it matters that N is a nonzero *integer*. *Example*: $50 \le 100.087$.

Step 6: the size of N, $\log_3 |N| \le \log_3 \|Q\|_1 + K \log_3 \max(|a|, b)$. By the triangle inequality,

$$|N| \le \sum_{j=0}^{K} |q_j|\, |a|^j\, b^{K-j} \le \sum_{j=0}^{K} |q_j|\, \max(|a|,b)^j \max(|a|,b)^{K-j} = \|Q\|_1 \max(|a|,b)^K \ ,$$

because $|a| \le \max(|a|, b)$ and $b \le \max(|a|, b)$. Take $\log_3$. *Example*: $\log_3 \|Q\|_1 = 46.517$ and $4 \log_3 10046105 = 58.702$, so the bound is $105.220 \ge 100.087$.

Step 7: back to F, and the cancellation of $v_3(F)$. Since $F(a/b) = c_F Q(a/b)$ and $v_3(c_F) = v_3(F)$, the left end of the chain is $v_3(Q(a/b)) = v_3(F(a/b)) - v_3(F)$. At the right end, $\|Q\|_1 = \|F\|_1 / c_F$, and $\log_3 c_F = \sum_p v_p(F) \log_3 p$, so

$$\log_3 \|Q\|_1 = \log_3 \|F\|_1 - v_3(F) - \sum_{p \ne 3} v_p(F) \log_3 p \ ,$$

where we have written the term $p = 3$ separately ($\log_3 3 = 1$). Steps 4 to 6 together give the chain [note, (3.3)],

$$\begin{aligned} v_3(F(a/b)) - v_3(F) \le v_3(N) &\le \log_3 |N| \\ &\le \log_3 \|F\|_1 - v_3(F) - \sum_{p \ne 3} v_p(F) \log_3 p + K \log_3 \max(|a|, b) \ . \end{aligned} \tag{7.2}$$

The term $-v_3(F)$ appears on both ends and cancels. This is the reason why the denominators at $p = 3$ do not appear in the criterion: a power of 3 in the denominators of F lowers the 3-adic valuation of $F(a/b)$ and enlarges the integer N in exactly compensating ways. Next, $-v_p(F) \le (-v_p(F))^+$, which replaces the sum over $p \ne 3$ by a sum of non-negative terms; it drops the primes with $v_p(F) > 0$ (a common factor of all coefficients), which would only have helped. Finally, multiply by $\log_2 3$ and use $\log_3 x \cdot \log_2 3 = \log_2 x$ and $\log_3 p \cdot \log_2 3 = \log_2 p$. This gives (7.1). □

Example 7.2 (the chain (7.2) in numbers)**.** Here are the seven steps for three cases, computed with exact integers. The second fraction is $T_{60} = A/3$ with $A = 704951613194098197388022 2064$, the truncation of $\zeta_3(5)$ after 60 ternary digits (starting from the digit of 3^{-1}), so $v_3(\zeta_3(5) - T_{60}) = 59$.

case	$v_3(F(\frac{a}{b}))$	$v_3(F)$	$v_3(Q(\frac{a}{b}))$	$v_3(N)$	$\log_3 \lvert N\rvert$	$\log_3 \|Q\|_1 + K \log_3 \mathrm{ht}$
Δ_4, x_0	37	−9	46	50	100.087	$46.517 + 58.702 = 105.220$
Δ_4, T_{60}	38	−9	47	51	277.391	$46.517 + 233.468 = 279.986$
Δ_3, x_0	30	−9	39	42	74.062	$35.692 + 44.027 = 79.719$

In every row the chain holds, and $\log_3 \|F\|_1 - \sum_p v_p(F) \log_3 p$ equals $\log_3 \|Q\|_1$. Note $v_3(\Delta_4(T_{60})) = 38 = v_3(\Delta_4(\zeta_3(5)))$ (Chapter 6): T_{60} is so close to $\zeta_3(5)$ that Δ_4 cannot tell them apart in its first 38 digits, whereas x_0, with only 17 common digits, gives 37. For Δ_3 the content is $c_F = 7 \cdot 2^{-17} 3^{-9}$: here $v_7(\Delta_3) = +1$, and the step $-v_7 \le (-v_7)^+ = 0$ throws away $\log_2 7 \approx 2.8$ bits, a small loss on the safe side. In bits, (7.1) for Δ_4 and x_0 reads

$$\underbrace{58.644}_{37 \log_2 3} \le \underbrace{37.464}_{\log_2 \|\Delta_4\|_1} + \underbrace{22.000}_{22 \log_2 2} + \underbrace{93.041}_{4 \log_2 10046105} = 152.504 \ .$$

The only prime $p \neq 3$ in the denominators of Δ_4 is 2, with exponent 22.

What just happened. Divide F by its content to get an integer polynomial Q, clear the denominator of a/b to get a nonzero integer $N = b^K Q(a/b)$, and compare $v_3(N)$ with $\log_3 |N|$. The content contributes its 3-part to both sides, where it cancels, and its other prime parts only to the size side, where they become the denominators term. Nothing else enters, and every inequality is elementary: $v_3(b) \ge 0$, $|N| \ge 3^{v_3(N)}$, the triangle inequality, and $-v_p \le (-v_p)^+$.

7.2 The criterion at $n = 1$: no contradiction, and why

Example 7.2 uses fractions that are *not* $\zeta_3(5)$. For the proof the relevant reading is different: under the hypothesis $\zeta_3(5) = a/b$, the left side of (7.1) with $F = \Delta_K$ is the valuation $v_3(\Delta_K(\zeta_3(5)))$, a number that we can compute without knowing a/b, because $\Delta_K(\zeta_3(5))$ is a 3-adic number determined by the digits of $\zeta_3(5)$ (Chapter 6). The other terms, except the height, are properties of the polynomial alone.

The hypothesis $F(a/b) \neq 0$ is not a formality. $\Delta_1(x_0) = \Delta_2(x_0) = 0$ (for $n = 1$, Δ_1 divides Δ_2, Chapter 6). If $\zeta_3(5)$ were equal to x_0, the criterion would say nothing for $K = 1, 2$, because there is no nonzero integer N. This is why the non-vanishing theorem is one of the four pillars of the proof.

Example 7.3 (the balance sheet at $n = 1$)**.** Under the hypothesis $\zeta_3(5) = a/b$, the terms of (7.1) for the $n = 1$ Hankel polynomials are, in bits:

K	$v_3(\Delta_K(\zeta_3(5)))$	gain	size	denominators	gain − size − den.	$2^{(\text{gain}-\text{size}-\text{den.})/K}$
1	12	19.020	9.667	6	3.353	10.22
2	22	34.869	20.036	14	0.833	1.33
3	31	49.134	28.113	17	4.021	2.53
4	38	60.229	37.464	22	0.765	1.14

The denominators term is in every case the power of 2 alone ($2^6, 2^{14}, 2^{17}, 2^{22}$): for $n = 1$ no prime $p \ge 5$ occurs in a denominator (Chapter 6). The inequality (7.1) holds if and only if $K \log_2 \mathrm{ht}(a/b) \ge \text{gain} - \text{size} - \text{den.}$, that is, $\mathrm{ht}(a/b) \ge 2^{(\text{gain}-\text{size}-\text{den.})/K}$, the last column.

So for $n = 1$ the gain already beats size plus denominators, by 0.8 to 4 bits, but the criterion is still satisfied by every fraction of height at least 11. Read the other way round, $n = 1$ and $K = 1$ prove a tiny theorem: $\zeta_3(5)$ *is not a fraction* a/b *with* $\max(|a|, b) \le 10$. Indeed, such an a/b is not the root x_0 of Δ_1, so $\Delta_1(a/b) \neq 0$, and the criterion would need $\log_2 \mathrm{ht}(a/b) \ge 3.353$, i.e. $\mathrm{ht} \ge 10.22$. As a direct confirmation, among all coprime a/b with $b > 0$ and $\max(|a|, b) \le 10$ the largest $v_3(\Delta_1(a/b))$ is -2 (at $-5/6$), far below 12, and the largest $v_3(\zeta_3(5) - a/b)$ is 2: none of them shares more than three ternary digits with $\zeta_3(5)$. The criterion has turned the digits of $\zeta_3(5)$ into a lower bound on the height of any rational equal to it. To exclude *all* heights at once, this lower bound has to go to infinity.

Intuition: why only large n can give a contradiction. For a fixed hypothetical a/b, the height term $K \log_2 \mathrm{ht}(a/b)$ grows only linearly in n, since $K \le 3n$. The other three terms are of order n^2 (and the size and denominators even of order $n^2 \log n$, before they cancel, Section 7.4). So the question is whether gain − size − denominators grows like a positive constant times n^2. If it does, with margin δn^2, then the criterion at n forces $\log_2 \mathrm{ht}(a/b) \ge \delta n^2/K \ge \delta n/3$, and a fixed a/b fails this for n large. At $n = 1$ the margins are 0.8 to 4 bits, which excludes only heights up to 10; the note's estimates say that the margin is at least about $4.58\,n^2$ bits up to lower-order terms, which excludes heights up to roughly $2^{1.5n}$, eventually any given height. No finite computation at fixed n can do this, because some huge fraction always fits the numbers (Chapter 2: every finite string of digits is shared by some rational).

7.3 Dominance: how to know that $\Delta_K(a/b) \neq 0$

We need $\Delta_K(a/b) \neq 0$ without knowing a/b. For a positive measure positivity would do this, but there is no positivity in $\mathbb{Q}_3$ (Chapter 6). Following [19], the note uses a divisibility argument at an auxiliary prime. The note remarks that the same idea, a coefficient that is strictly dominant at auxiliary primes, replaces the non-vanishing hypothesis in the irrationality criterion of Lai and Sprang [24], and that [19] uses it in the form of the following lemma.

Lemma 7.4 (dominance; [note, Lemma 3.4]). *Let $F = \sum_j f_j X^j \in \mathbb{Q}[X]$, and let p be a prime with $v_p(f_0) < v_p(f_j)$ for every $j \ge 1$. Then $F(a/b) \neq 0$ for every $a/b \in \mathbb{Q}$ with $p \nmid b$.*

Proof. The hypothesis includes $v_p(f_0) < \infty$, that is $f_0 \neq 0$ (a coefficient $f_j = 0$ has $v_p = +\infty$, which is fine). Let $p \nmid b$. Then $v_p(b) = 0$ and $v_p(a) \ge 0$, so $v_p(a/b) \ge 0$. For $j \ge 1$ the term $f_j(a/b)^j$ has $v_p(f_j(a/b)^j) = v_p(f_j) + j\,v_p(a/b) \ge v_p(f_j) > v_p(f_0)$. The sum $F(a/b) - f_0 = \sum_{j\ge1} f_j(a/b)^j$ therefore has $v_p > v_p(f_0)$ by the ultrametric inequality, and adding the term f_0, whose valuation is strictly smaller, gives $v_p(F(a/b)) = v_p(f_0)$ (ultrametric inequality with unequal valuations, Chapter 2). A number with finite valuation is not zero. □

Intuition. Think of the p-adic digits. Every term $f_j(a/b)^j$ with $j \ge 1$ is divisible by a strictly higher power of p than f_0; so the lowest nonzero p-adic digit of f_0 survives in the sum, untouched. A sum whose lowest digit is nonzero is not zero. The condition $p \nmid b$ is needed because a p in the denominator of a/b would make $(a/b)^j$ p-adically large and could lift the higher terms down to the level of f_0.

Example 7.5 (dominance on the real Δ_1 and Δ_K, $n = 1$). (i) $\Delta_1(X) = -\frac{5\cdot103\cdot19507}{2^6\cdot3^5} + \frac{13513}{3^4}X$, and 13513 is prime. At $p = 13513$ the valuations of the two coefficients are 0 and 1: the constant coefficient is dominant. So $\Delta_1(a/b) \neq 0$ whenever $13513 \nmid b$. The lemma is sharp here: the only root of Δ_1 is $x_0 = 10046105/2594496$, and its denominator $2594496 = 2^6 \cdot 3 \cdot 13513$ is divisible by 13513, as it must be. (ii) The constant coefficient is also dominant at $p = 2$ and at $p = 3$, for each of $\Delta_1, \dots, \Delta_4$: the 2-adic valuations of the coefficients $f_0, \dots, f_K$ are $(-6, 0)$, $(-14, -7, -2)$, $(-17, -12, -4, 0)$, $(-22, -16, -12, -5, 0)$. Hence $\Delta_K(a/b) \neq 0$ for $K \le 4$ and every a/b with odd b; indeed the rational roots of $\Delta_1, \dots, \Delta_4$ are only x_0 and $1103359/202560$, both with even denominators ($202560 = 2^6 \cdot 3 \cdot 5 \cdot 211$). For the four test fractions $\frac{1}{3}, \frac{7}{5}, -\frac{2}{9}, \frac{4}{7}$ one finds $v_2(\Delta_K(a/b)) = v_2(f_0)$ for all $K \le 4$, as the proof predicts. That the dominant prime is 2 at $n = 1$ is our observation for this small case; the note uses dominance at a prime p of size about $2.1n$ to $2.16n$, and for $n = 1$ that window contains no prime.

The prime can be chosen after b. In the proof by contradiction the order of choices is: first the hypothetical a/b is given, hence b is fixed; then we choose n; then we choose a prime p in the window $[2.1n+2,\ 2.159n]$ with $p \nmid b$; then $K = K(n,p)$. The non-vanishing theorem (Section 7.4) proves dominance at *every* prime of the window, so we may pick whichever one avoids b. This works as soon as the window contains more primes than b has prime factors in it. Since every prime of the window is at least $2.1n+2$, and the product of the distinct window primes dividing b divides b, at most $\log b/\log(2.1n+2)$ of them can divide b. *Example*: if b were the denominator 2594496 of x_0, then for $n = 6301$ the window $[13235, 13603]$ contains the prime factor 13513 of b, but also 34 other primes, any of which will do.

7.4 The four estimates

7.4.1 The parameter κ and the intervals

The note writes $\kappa = K/n$, the number of rows of the Hankel determinant per unit of n. All four estimates are statements for large n with κ in a bounded range, and the main terms are functions of κ times n^2 or $n^2 \log_2 n$. The range that matters is $\kappa \in [2.8, 3]$ (we derive both ends below), cut into the five intervals [note, (3.7)]

$$I_i = [\kappa_{1,i}, \kappa_{2,i}] = [2.80 + 0.04(i-1),\ 2.84 + 0.04(i-1)]\ , \qquad i = 1, \dots, 5\ . \tag{7.3}$$

Why intervals at all: the constants $F^\dagger$ and c below depend on κ and are obtained by computer from expressions that are evaluated on a whole interval at once (Chapters 10 and 13); five intervals of width 0.04 were enough to get a positive margin on each.

Theorem 7.6 (3-adic gain; [note, Theorem 3.5])**.** *For $K \le 3n+1$,*

$$v_3(\Delta_K(\zeta_3(5)))\log_2 3 \ge G(\kappa)\, n^2 - O(n\log n)\ , \qquad G(\kappa) = \left(10.5\,\kappa - \frac{\kappa^2}{4}\right)\log_2 3\ .$$

What it measures: how many bits of 3-adic smallness the determinant has. Roughly, each of the K rows contributes about $10.5n$ trits (the entries are divisible by about $3^{10.5n}$), minus a loss of $K^2/4$ trits for a change of basis; Chapter 8 proves it. *Numbers*: $G(2.8) = 43.4914$, $G(3) = 46.3602$ bits per n^2; for $n = 1$ and $K = 4$ the actual gain was 60.2 bits (Example 7.3), but the theorem is only asymptotic.

Theorem 7.7 (size; [note, Theorem 3.8])**.** *There are constants $F_i^\dagger$ ([note, (5.10)], bounded in [note, Table 1]) such that for $K/n \in I_i$*

$$\log_2 \|\Delta_K\|_1 \le (\kappa^2 - 6\kappa)\, n^2 \log_2 n + F_i^\dagger\, n^2 + O(n\log n)\ ,$$

uniformly for $K/n \in I_i$, with an implied constant that does not depend on i.

What it measures: the ordinary size of the coefficients of Δ_K. The main term is negative ($\kappa^2 - 6\kappa = -8.96$ at $\kappa = 2.8$, -9 at $\kappa = 3$): the coefficients are tiny, the bound being about $2^{-9n^2\log_2 n}$ near $\kappa = 3$. Chapters 9 and 10 prove it with a Coulomb-gas (electrostatics) analysis.

Theorem 7.8 (denominators; [note, Theorem 3.10])**.** *There are constants c_i ([note, (5.39)], bounded in [note, Table 1]) such that*

$$\sum_{p \ne 3} (-v_p(\Delta_K))^+ \log_2 p \le \kappa(6-\kappa)\, n^2 \log_2 n + c_i\, n^2 + o(n^2)\ ,$$

uniformly for $K/n \in I_i$.

What it measures: how many bits of denominators at primes $p \neq 3$ the coefficients have; the main term is positive and is the mirror image of the size's. Chapters 11 to 13 prove it, prime range by prime range.

Theorem 7.9 (non-vanishing; [note, Theorem 3.13])**.** *Let p be a prime with $2.1n + 2 \le p < 3n$, and let $K = K(n, p)$, where [note, (3.12)]*

$$K(n,p) = \begin{cases} 10n - \dfrac{10(p-1)}{3}\ , & p \equiv 1 \pmod 3\ , \\ 10n - \dfrac{10p-14}{3}\ , & p \equiv 2 \pmod 3\ . \end{cases} \tag{7.4}$$

Then $K \le 3n - 2$, and $\Delta_K(a/b) \neq 0$ for every $a/b \in \mathbb{Q}$ with $p \nmid b$. If moreover $p \le 2.159n$, then $K > 2.8n$.

What it measures: nothing; it is a yes/no statement, proved by showing that the constant coefficient of Δ_K is strictly p-adically dominant and applying Lemma 7.4. $K(n,p)$ is the number of Taylor conditions that the argument imposes at the nodes; why it has this form is explained in Chapter 14. Here we only check its two bounds, which are pure arithmetic. Since $p > 3$, $p \equiv 1$ or $2 \pmod 3$, and then $p - 1$ or $10p - 14 = 10(p-2) + 6$ is divisible by 3, so K is an integer. If $p \equiv 2$ and $p \ge 2.1n + 2$, then $K \le 10n - (21n + 20 - 14)/3 = 3n - 2$; if $p \equiv 1$, then $K \le 10n - 10(2.1n + 1)/3 = 3n - \frac{10}{3}$. If $p \le 2.159n$, then for $p \equiv 1$, $K \ge 10n - 10(2.159n - 1)/3 = 2.80\overline{3}\,n + \frac{10}{3}$, and for $p \equiv 2$, $K \ge 10n - (21.59n - 14)/3 = 2.80\overline{3}\,n + \frac{14}{3}$; both exceed $2.8n$. A direct enumeration confirms this: for all 1252821 pairs (n,p) with $n < 30000$ odd and p a prime in the window, $K(n,p)$ is an integer with $2.8n < K \le 3n - 2$; the extreme values of κ are 2.80345 and 2.99990.

Example 7.10 (the window for $n = 1001$)**.** The window $[2.1n + 2,\ 2.159n]$ is [2104.1, 2161.2], and it contains 9 primes. Each gives its own K and κ:

p	2111	2113	2129	2131	2137	2141	2143	2153	2161
$p \bmod 3$	2	1	2	1	1	2	1	2	1
K	2978	2970	2918	2910	2890	2878	2870	2838	2810
κ	2.9750	2.9670	2.9151	2.9071	2.8871	2.8751	2.8671	2.8352	2.8072
I_i	5	5	3	3	3	2	2	1	1

Larger p means smaller K: roughly $\kappa \approx 10 - \frac{10}{3}\,\frac{p}{n}$. Which p the proof uses depends on b, so κ can land in any of the five intervals.

Why $\kappa \in [2.8, 3]$. The upper end comes from the gain: $\Delta_K(\zeta_3(5)) = \det[L(y^{i+j})]$ only for $K \le 3n + 1$ (Chapter 6), because purity covers moments up to y^{6n+1}; the lower limit $2.1n + 2$ of the window gives $K \le 3n - 2$, inside this range. The lower end 2.8 comes from the upper limit $2.159n$ of the window, and the window must have positive width $(2.159 - 2.1 = 0.059)$ so that it contains many primes. The margin $G - F^\dagger - c$ in [note, Table 1] decreases from 5.41 to 4.58 as κ goes down from $[2.96, 3]$ to $[2.80, 2.84]$; the note does not compute it below 2.8, so the window cannot be widened without new computations.

7.4.2 A picture of the leading terms

Figure 7.1 shows the two facts that the proof needs from the estimates. On the right, the main terms of size and denominators cancel exactly: $(\kappa^2 - 6\kappa) + \kappa(6 - \kappa) = 0$. On the left, after the cancellation, the gain $G(\kappa)$ stays above the remaining constants $F_i^\dagger + c_i$ on all five intervals. Because $G'(\kappa) = (10.5 - \kappa/2)\log_2 3 > 0$ for $\kappa < 21$, G is increasing on $[2.8, 3]$ and $G(\kappa) \ge G(\kappa_{1,i})$ on I_i; this is why [note, Table 1] uses the left end. The increase of G across one

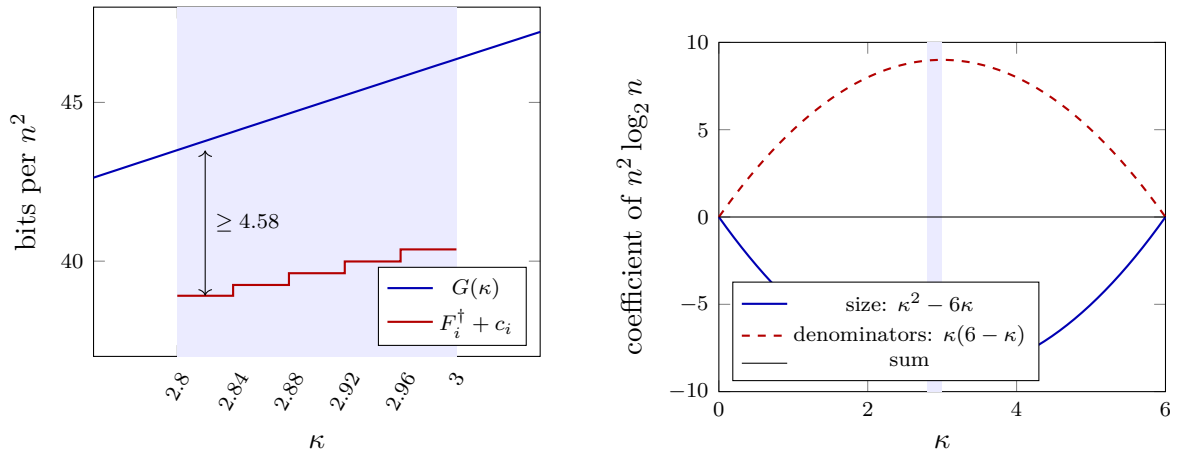


Figure 7.1: Left: the gain coefficient $G(\kappa)$ (bits per n^2) on the range $[2.8, 3]$ (shaded), against the note's upper bounds for $F_i^\dagger + c_i$ on the five intervals (sums of the entries of [note, Table 1]: 38.91, 39.25, 39.62, 39.99, 40.37). The gap between the curve and the steps is the margin; it is smallest at the left end of I_1, where it is $43.49 - 38.91 = 4.58$. Right: the two main terms of order $n^2 \log_2 n$. They are exact negatives of each other for every κ, so their sum is identically 0. Each is about $9\,n^2 \log_2 n$ bits on the shaded range, about $90\,n^2$ bits for $n = 1000$ (Chapter 1), many times the final margin of $4.58\,n^2$.

interval is about 0.57 bits per n^2. The values of $G(\kappa_{1,i})$ and the margins of [note, Table 1] are worked out in Chapter 1 (Table 1.1); the bounds $F_i^\dagger$ and c_i come from the note's computations and are discussed in Chapters 10 and 13.

7.4.3 Why the $n^2 \log n$ terms cancel: the product formula

The note explains the cancellation heuristically [note, Section 3, after Theorem 3.5]: both estimates measure the same products $\prod_k h_k^{s_k} \prod_{k \neq m} (k-m)^{s_k s_m}$ that come from the Heine expansion (Chapter 9), once with the absolute value and once with the p-adic valuations for $p \neq 3$, and by the product formula the two agree up to the 3-adic part. Here h_k is the leading coefficient of W at the node k [note, (2.18)] (Chapter 5), and $s_k \in \{0, \dots, 4\}$ is the number of rows of the determinant that the node k absorbs, with $\sum_k s_k = K$.

Intuition. For a nonzero rational $x = \pm \prod_p p^{v_p(x)}$, taking $\log_2$ gives exactly

$$\log_2 |x| = v_3(x) \log_2 3 + \sum_{p \neq 3} v_p(x) \log_2 p \ .$$

The left side is what the size estimate sees. The sum on the right, with a minus sign, is what the denominators estimate sees when the v_p are negative. So whatever the size of x is, the denominators are its mirror image, up to the 3-part. If x is tiny because it has huge denominators, the two large numbers cancel, and only $v_3(x) \log_2 3$ is left. This is a heuristic: the note's coefficients are sums of many such products, the size bound uses the triangle inequality, the denominators bound uses the ultrametric inequality, and the two error terms $F^\dagger$ and c are where the heuristic stops.

Example 7.11 (one Heine term)**.** Take every node once, $s_k = 1$ for all $3n + 1$ nodes (so $K = 3n + 1$, $\kappa \approx 3$), and $x = \prod_k h_k \prod_{k \neq m} (k - m)$. We build x from the factorized formula [note, (2.18)] for h_k by counting, for every integer $m \leq 6n + 2$, how often it occurs in numerators and denominators, and get in bits:

n	$\log_2\lvert x\rvert \,/\, (n^2\log_2 n)$	$\sum_{p\neq 3} v_p(x)\log_2 p \,/\, (n^2\log_2 n)$	$v_3(x)\log_2 3 \,/\, n^2$	$\kappa^2-6\kappa$
101	-9.018	-1.603	-49.37	-9.000
1001	-8.943	-3.942	-49.84	-9.000
10001	-8.950	-5.193	-49.91	-9.000

The identity $\log_2\lvert x\rvert = v_3(x)\log_2 3 + \sum_{p\neq 3} v_p(x)\log_2 p$ holds to rounding error ($\lvert$difference$\rvert < 2\cdot 10^{-6}$). The size of x is already close to $(\kappa^2-6\kappa)n^2\log_2 n$. The denominators side is *not* yet close to its limit -9 per $n^2\log_2 n$: the 3-part is about $-50\,n^2$ bits, of order n^2 but with a large constant, and divided by $n^2\log_2 n$ it fades only like $50/\log_2 n$ (at $n=10001$, $50/13.3\approx 3.8$). This shows on one term what "the two agree up to the 3-adic part and terms of order n^2" means, and also that what is left over is not small: here the 3-part is about $50\,n^2$ bits, ten times the final margin of $4.58\,n^2$. Its sign is such that it makes x smaller, so for this one term size plus denominators, $\log_2\lvert x\rvert - \sum_{p\neq 3} v_p(x)\log_2 p = v_3(x)\log_2 3$, is negative. How the 3-parts are accounted for in the actual estimates is the business of Chapters 8 and 10; on the side of the criterion, Step 7 of its proof shows that the 3-adic content of Δ_K cancels.

7.5 Primes in the window

Theorem 7.12 (prime number theorem; Hadamard and de la Vallée Poussin [16, 13])**.** *Let $\pi(x)$ be the number of primes $\le x$. Then $\pi(x)\log x/x \to 1$ as $x\to\infty$; in other words $\pi(x) = (1+\varepsilon(x))\,x/\log x$ with $\varepsilon(x)\to 0$.*

Intuition. Near a large number t, about one integer in $\log t$ is prime: the "density of primes" at t is $1/\log t$. Summing the density, $\pi(x)\approx\int_2^x \mathrm{d}t/\log t$ (the logarithmic integral, a better approximation than $x/\log x$ but with the same leading behaviour). We use only the statement, not its proof, which needs complex analysis of the Riemann zeta function; see for instance Apostol, *Introduction to Analytic Number Theory*, Ch. 13.

Proposition 7.13 (the window; [note, proof of Theorem 1.1])**.** *The number of primes in $[2.1n+2,\ 2.159n]$ is $(0.059+o(1))\,n/\log n$ as $n\to\infty$.*

Proof. Put $u = 2.1n+2$ and $w = 2.159n$. The number of primes in $[u,w]$ is $\pi(w)-\pi(u)$, plus 1 if u itself is prime (for n odd, $2.1n+2$ is not an integer, so this correction does not even occur; in any case it is $O(1)$). By Theorem 7.12,

$$\pi(w)-\pi(u) = \frac{w}{\log w} - \frac{u}{\log u} + \varepsilon(w)\frac{w}{\log w} - \varepsilon(u)\frac{u}{\log u}\ .$$

Each of the last two terms is at most $\max(\lvert\varepsilon(w)\rvert,\lvert\varepsilon(u)\rvert)\cdot 2.2\,n/\log n$ for large n, so together they are $o(n/\log n)$ because $\varepsilon\to 0$. For the main terms, $\log w = \log n + \log 2.159$ and $\log u = \log n + \log(2.1+2/n)$, so

$$\frac{w}{\log w} = \frac{2.159\,n}{\log n}\cdot\frac{1}{1+\log 2.159/\log n} = \frac{2.159\,n}{\log n} + O\!\left(\frac{n}{\log^2 n}\right), \qquad \frac{u}{\log u} = \frac{2.1\,n}{\log n} + O\!\left(\frac{n}{\log^2 n}\right),$$

using $1/(1+t) = 1+O(t)$ for small t and $2/n = o(1)$. The difference is $(2.159-2.1)\,n/\log n + O(n/\log^2 n) = (0.059+o(1))\,n/\log n$. □

The same answer comes from the density picture: the window has length $0.059n-2$, and over it the density $1/\log t$ is between $1/\log(2.159n)$ and $1/\log(2.1n)$, both $= (1+o(1))/\log n$. By the mean value theorem for integrals, $\int_u^w \mathrm{d}t/\log t = (w-u)/\log\xi$ for some $\xi\in[u,w]$, which is again $(0.059+o(1))n/\log n$. The subtraction step in the proof works only because the window has length proportional to n: the errors $\varepsilon(w)w/\log w$ and $\varepsilon(u)u/\log u$ are of order

$\varepsilon\, n/\log n$, and they are negligible against the main term $0.059\, n/\log n$ because both are of order $n/\log n$ and $\varepsilon \to 0$. For a window of length $\sqrt{n}$ the prime number theorem in this form would say nothing.

Example 7.14 (counting the primes)**.** Counting the primes in the window with a sieve, and comparing with the prediction:

n	primes in window	$0.059\, n/\log n$	$\int_u^w \mathrm{d}t/\log t$	ratio count/$(0.059n/\log n)$
1001	9	8.5	7.4	1.053
10001	63	64.1	59.0	0.983
100001	472	512.5	480.7	0.921
999999	4088	4270.6	4048.9	0.957

For $n \geq 10^5$ the integral is the better predictor (at $n = 1001$ and 10001 the leading form happens to be closer); the leading form $0.059n/\log n$ is off by a few percent, because $\log(2.13n)$ and $\log n$ differ by $\log 2.13 \approx 0.76$, a relative error of order $1/\log n$ that goes to 0 slowly. Among the odd $n \leq 10^6$, exactly 48 have a window that contains no prime: the 17 values $n \leq 33$, for which $2.1n + 2 > 2.159n$ and the window is empty as an interval, and 31 values from 35 to 249, for which the interval is nonempty but contains no prime (for $n = 35, 37, 41, 43$ it contains no integer at all). The largest such n is 249, and the first n whose window contains a prime is 45.

Why one of the primes avoids b. The note says that b has only finitely many prime factors, while the number of window primes tends to infinity. A quantitative form: as computed in Section 7.3, at most $\log b/\log(2.1n + 2)$ window primes divide b, a number that even decreases with n. Once the window contains more primes than that, some window prime does not divide b. (A cruder version: once $2.1n + 2 > b$, no window prime divides b at all, and a nonempty window suffices.)

7.6 The proof of Theorem 1.1

Theorem 7.15 ([note, Theorem 1.1])**.** *The number $\zeta_3(5)$ is irrational.*

The note's proof, step by step. Step 1 (hypothesis). Suppose $\zeta_3(5) = a/b$ with coprime integers a and $b > 0$. From now on a and b are fixed.

Step 2 (choice of n and p). By Proposition 7.13 the window $[2.1n + 2,\ 2.159n]$ contains $(0.059 + o(1))n/\log n$ primes, which tends to infinity, while at most $\log b/\log(2.1n + 2)$ of them divide b. So there is n_1 such that for every odd $n \geq n_1$ there is a prime p in the window with $p \nmid b$. Take such n and p, and $K = K(n, p)$ from (7.4).

Step 3 (non-vanishing and the range of κ). Since $2.1n + 2 \leq p \leq 2.159n < 3n$, Theorem 7.9 gives $2.8n < K \leq 3n - 2$ and $\Delta_K(a/b) \neq 0$. So $\kappa = K/n \in (2.8, 3)$, and κ lies in (at least) one of the intervals I_i; fix such an i.

Step 4 (the criterion). Δ_K is a nonzero polynomial (it does not vanish at a/b) of degree at most K (Chapter 6), so Lemma 7.1 applies with $F = \Delta_K$. Because $K \leq 3n + 1$, the value $\Delta_K(a/b) = \Delta_K(\zeta_3(5))$ is the Hankel determinant of [note, (2.26)], so its left side is the gain.

Step 5 (inserting the estimates). By Theorems 7.6 to 7.8,

$$G(\kappa)n^2 - O(n\log n) \leq \Big[(\kappa^2 - 6\kappa) + \kappa(6 - \kappa)\Big] n^2 \log_2 n + (F_i^{\dagger} + c_i)n^2 + o(n^2) + K\log_2 \max(|a|, b)\,. \tag{7.5}$$

The note writes this step in words, in Step 3 of its proof. The bracket is 0. The last term is at most $3n\log_2 \max(|a|, b)$, which is $O(n)$ with a constant depending on the fixed a, b.

Step 6 (the margin). Since G is increasing, $G(\kappa) \geq G(\kappa_{1,i})$. Moving everything except the n^2 terms to the right,

$$\Big(G(\kappa_{1,i}) - F_i^{\dagger} - c_i\Big)\, n^2 \leq E(n)\ , \qquad E(n) = O(n \log n) + o(n^2) + O(n) = o(n^2)\ . \tag{7.6}$$

This is [note, (3.14)], where the note writes $E = E_1 + E_2 + E_3 + 3n \log_2 \max(|a|, b)$ for the three error terms and the last term. The function E can be taken the same for all five i (see below).

Step 7 (contradiction). By [note, Table 1], the bracket is at least 4.58 for every i. So $4.58 \leq E(n)/n^2$ for every odd $n \geq n_1$, while $E(n)/n^2 \to 0$. This is false for large n. Hence the hypothesis of Step 1 is false. □

What "uniformly" and $o(n^2)$ buy. In Step 2 the prime p, and therefore K and $\kappa = K/n$, depend on n and on b; as n grows, κ wanders around in $(2.8, 3)$ in a way we do not control (Example 7.10). If the error terms of Theorems 7.7 and 7.8 were only known to be small for each *fixed* κ, with a rate depending on κ, then along a sequence of varying κ_n they might never become small. "Uniformly for $K/n \in I_i$" means that for each i there is one error function $e_i(n) = o(n^2)$ that works for all K with $K/n \in I_i$. With five intervals, $E(n) = \max_i e_i(n) + O(n \log n) + 3n \log_2 \max(|a|, b)$ is still $o(n^2)$, because the maximum of five functions that are each $o(n^2)$ is $o(n^2)$; this is "uniform in i, there being only five intervals". A statement $o(n^2)$ means: for every $\delta > 0$ there is n_δ with $E(n) \leq \delta n^2$ for $n \geq n_\delta$. With any $\delta < 4.58$ (say $\delta = 1$) this gives the contradiction; note that the proof does not say how large n_δ is, because the O and o terms have unspecified constants.

What just happened. The proof assumes $\zeta_3(5) = a/b$, picks a large odd n and a prime $p \nmid b$ in a window of length $0.059n$ (prime number theorem), sets $K = K(n, p)$ so that $\kappa = K/n \in (2.8, 3)$, gets $\Delta_K(a/b) \neq 0$ from dominance at p, applies the criterion, and inserts the three estimates. The $n^2 \log n$ terms cancel exactly, the height term is $O(n)$, and the surviving n^2 terms have a positive coefficient ≥ 4.58 by [note, Table 1]. A positive multiple of n^2 cannot be $o(n^2)$.

7.6.1 An illustration: how large must n be?

The proof gives no explicit n, because the error terms have unspecified constants. To get a feeling for the scales, here is an *illustration that ignores all error terms*, i.e. pretends that (7.6) held with $E(n)$ consisting of the height term alone. Suppose the hypothetical fraction had $\max(|a|, b) < 10^{1000}$, i.e. at most 1000 digits.

- *Margin against height.* $\log_2 10^{1000} = 3321.93$, and $4.58\, n^2 > 3n \cdot 3321.93$ holds if and only if $n > 2175.9$. At $n = 2177$: $4.58n^2 = 21706127$ against $3n \log_2 10^{1000} = 21695512$.
- *A prime avoiding b.* At $n = 2177$ the window contains 15 primes, but a 1000-digit b could be divisible by up to 273 primes of that size. The bound $\log b / \log(2.1n + 2)$ is first beaten (and stays beaten for all odd n up to $2 \cdot 10^5$) at $n = 41243$, where the window contains 203 primes against at most 202.5 that can divide b.

So, in this idealized bookkeeping, $n \approx 4 \cdot 10^4$ would exclude every fraction with at most 1000 digits, and the binding constraint would be the worst-case b that is divisible by many window primes, not the margin. These numbers depend on the unknown constants hidden in $O(n \log n)$ and $o(n^2)$, and on how fast those error terms become small, so they must not be read as a statement about the actual proof; in particular $o(n^2)$ in [note, Theorem 3.10] comes with no rate at all.

7.7 The logical status of the theorem

The deduction of this chapter is short and elementary; everything difficult is in its inputs. [note, Theorem 1.1] follows from:

- Lemmas 7.1 and 7.4 ([note, Lemmas 3.1, 3.4]): elementary, proved in full above;
- [note, (2.26)]: $\Delta_K(\zeta_3(5)) = \det[L(y^{i+j})]$ for $K \le 3n+1$, from purity [note, Lemma 2.19] (Chapters 5 and 6);
- the four estimates [note, Theorems 3.5, 3.8, 3.10, 3.13], proved in the note's [note, Sections 4–6] and [note, Appendices A–D] (Chapters 8 to 14);
- the numerical bounds $F_i^\dagger$ [note, Proposition 5.11] and c_i [note, Proposition 5.40], obtained by computer: $F_i^\dagger$ in ball arithmetic, c_i in exact rational arithmetic up to a final evaluation of Euler's constant and three logarithms [note, Appendix E]; the note's lemmas state that the computed expressions are upper bounds;
- the prime number theorem (Theorem 7.12), a textbook theorem.

The arithmetic of [note, Table 1] is worked out in Chapter 1; the computer-assisted bounds themselves are taken from the note. What this chapter adds is that the step from the inputs to the theorem is a short and transparent deduction, which is short and elementary; the weight of the proof rests on the estimates and on the computed constants.

Check yourself 7.16. Where exactly would the proof break if [note, Table 1] had one negative entry in its last column, say on I_3?

Answer. In Step 7: for those n for which the chosen prime gives $\kappa \in I_3$, inequality (7.6) has a non-positive left side and is no contradiction. Since p (hence κ) depends on b, which is unknown, we could not avoid I_3; one would have to exclude the primes whose $K(n,p)$ lands in I_3. As far as we can see this would leave two windows of smaller but still positive relative width, whose prime count still grows like a constant times $n/\log n$, so the argument would survive with a smaller constant in place of 0.059.

Check yourself 7.17. In Example 7.3 the criterion for $K=1$ excludes heights up to 10, but for $K=4$ only height 1. Why does the larger determinant do worse here?

Answer. The exclusion bound is $2^{\text{margin}/K}$: the margin is spread over K factors of the height. At $n=1$ the margin does not grow with K (3.35 bits for $K=1$, 0.77 for $K=4$), so dividing by K hurts. The method gains only when the margin grows like n^2 while K grows like n.

Summary of the chapter

We proved the criterion [note, Lemma 3.1]: for $F \in \mathbb{Q}[X]$ of degree $\le K$ with $F(a/b) \neq 0$, the 3-adic valuation of $F(a/b)$ in bits is at most $\log_2 \|F\|_1$ plus the denominators at $p \neq 3$ plus $K \log_2 \max(|a|, b)$. The proof divides by the content, clears the denominator of a/b, and compares $v_3(N)$ with $\log_3 |N|$ for the nonzero integer $N = b^K Q(a/b)$; the 3-adic content cancels. On the real $n=1$ Hankel polynomials the criterion holds with room to spare, and under the hypothesis $\zeta_3(5) = a/b$ it shows only that $\max(|a|, b) \ge 11$; a contradiction needs a margin growing like n^2. We proved the dominance lemma [note, Lemma 3.4] and saw it at work on Δ_1 ($p = 13513$) and on $\Delta_1, \dots, \Delta_4$ ($p = 2$). We stated the four estimates, drew their leading terms (the $n^2 \log n$ coefficients $\kappa^2 - 6\kappa$ and $\kappa(6-\kappa)$ cancel; $G(\kappa)$ exceeds $F_i^\dagger + c_i$ by at least 4.58 bits per n^2), illustrated the product-formula reason for the cancellation on one Heine term, derived the count $(0.059 + o(1))n/\log n$ of primes in the window from the prime number theorem, checked that $K(n,p)$ lands in $(2.8n, 3n-2]$, and proved [note, Theorem 1.1] from the four estimates and the computed constants.

Carried forward: the meaning of each term of (7.1) and the target forms of Theorem 7.6 (Chapter 8), Theorem 7.7 (Chapters 9 and 10), Theorem 7.8 (Chapters 11 to 13) and Theorem 7.9 with $K(n,p)$ (Chapter 14); the intervals I_i and the requirement of uniformity in κ, which every later estimate must respect; and the product-formula heuristic, which Chapters 10 and 13 make precise.

Part IV

The four estimates

Chapter 8

Estimate 1: the 3-adic gain

Where we are. Chapter 7 reduced the theorem to four estimates. This chapter explains the note's proof of the first one, the 3-adic gain [note, Theorem 3.5]: for $K \le 3n+1$,

$$v_3(\Delta_K(\zeta_3(5)))\log_2 3 \;\ge\; G(\kappa)\,n^2 - O(n\log n)\;, \qquad G(\kappa) = \left(10.5\,\kappa - \frac{\kappa^2}{4}\right)\log_2 3\;,$$

with $\kappa = K/n$. It is the only estimate that is about 3-adic *smallness*; the other three bound costs. We cover all of [note, Section 4] and [note, Appendix A]: integer-valued polynomials and the class $\mathrm{Int}(S)$, the basis F_i [note, Lemma 4.1] with the change-of-basis inequality [note, (4.3)] and its cost [note, (4.4)], the factorization of the weight on S [note, (4.5)], the analytic step [note, Lemma 4.6] with its proof (Mahler expansion, Stirling numbers, the function ψ), and the proof of [note, Theorem 3.5]. We use from earlier chapters: the valuation v_3, the ultrametric inequality, the set $S = 3^{-1}\mathbb{Z}_3^\times$, the fact that every integer is at 3-adic distance exactly 3 from every point of S, the unit series $1/(a+3t)$, Legendre's formula and the digit-sum bound $s_3(q) \le 2\log_3(3q)$ (all Chapter 2); the binomial polynomials $\binom{t}{c}$ and the properties (V1)–(V3) of the Volkenborn integral (Chapter 4); the weight W and the functional L (Chapter 5); the identity $\Delta_K(\zeta_3(5)) = \det\big[L(y^{i+j})\big]_{i,j<K}$ for $K \le 3n+1$ [note, (2.26)] and the change-of-basis rule $\det \to (\det T)^2 \det$ (Chapter 6).

8.1 The plan: make every entry uniformly small

Recall what we want. By [note, (2.26)], for $K \le 3n+1$ the number $\Delta_K(\zeta_3(5))$ is the determinant of the $K \times K$ Hankel matrix $[L(y^{i+j})]_{i,j<K}$, where

$$L(P) = \sum_{r=1,2} \int_{\mathbb{Z}_3} (PW)'\Big(t + \frac{r}{3}\Big)\,\mathrm{d}t$$

integrates over the points $y = t + \frac{r}{3}$, $t \in \mathbb{Z}_3$, which make up the set $S = 3^{-1}\mathbb{Z}_3^\times = \{y \in \mathbb{Q}_3 : v_3(y) = -1\}$ [note, (2.8)]. A determinant is a sum of products of K entries, one from each row (Leibniz formula). So if every entry is divisible by 3^A, the determinant is divisible by 3^{KA}: by the ultrametric inequality the valuation of a sum is at least the smallest valuation of its terms, and the valuation of a product of K entries is the sum of their valuations. This is the whole mechanism of the gain, and the question is what A is.

Where the divisibility comes from. On S the weight W is 3-adically tiny. Each of its $3n+1$ poles is a factor $(y+k)^{-4}$, and $|y+k|_3 = 3$ for every $y \in S$ and every integer k (Chapter 2), so each pole contributes exactly 3^4, uniformly on S. For $n = 1$, Chapter 5 found $v_3(W(\frac{1}{3})) = 12$, and the entries of the Hankel matrix inherit this.

Why the monomials are a bad basis. The polynomial y^m is *large* on S: $|y^m|_3 = 3^m$. So the factor y^{i+j} in the entry $L(y^{i+j})$ eats $i+j$ of the trits that the weight provides, and the entries far from the top left corner are less divisible. Chapter 6 showed this for $n=1$, $K=4$: the valuations of $L(y^{i+j})$ drop from 12 in the corner to 6 at $i=j=3$, so the naive bound $K \cdot \min$ would give only $4 \cdot 6 = 24$.

The remedy. Replace the monomials $1, y, \dots, y^{K-1}$ by polynomials $F_0, \dots, F_{K-1}$ of the same degrees that are *not* large on S: polynomials that take values in $\mathbb{Z}_3$ at every point of S. Then every product F_iF_j also takes values in $\mathbb{Z}_3$ on S, and we shall prove that L of such a polynomial is divisible by about $3^{10.5n}$, independently of its degree (up to a logarithmic loss). The price is the change of basis: by Chapter 6, $\det[L(F_iF_j)] = (\det T)^2 \det[L(y^{i+j})]$, where T is the coefficient matrix, and for a triangular T the factor $\det T$ is the product of the leading coefficients. So the plan, in which the note follows [19], has two halves:

1. an *algebraic* half: find polynomials F_i integral on S whose leading coefficients are as 3-adically large as possible (Sections 8.2 to 8.4);
2. an *analytic* half: show that $L(B)$ is divisible by about $3^{10.5n}$ for every B integral on S (Sections 8.5 and 8.6).

Intuition: a physicist's version. Think of the Hankel determinant as the squared volume of the parallelepiped spanned by the basis vectors, measured with the "metric" $L(PQ)$ (Chapter 6). The metric is tiny (3-adically) on vectors that are of unit size on S. The monomials are not of unit size on S, they grow like 3^m; so first rescale them to vectors of unit size, measure the volume there, where every entry is uniformly small, and then pay the Jacobian of the rescaling. The best rescaling is the one with the smallest Jacobian, and finding it is a question about integer-valued polynomials.

8.2 Integer-valued polynomials

8.2.1 On $\mathbb{Z}$ and on $\mathbb{Z}_3$

A polynomial with rational coefficients can take integer values at every integer without having integer coefficients. Chapter 4 met the binomial polynomials $\binom{t}{c} = t(t-1)\cdots(t-c+1)/c!$, and Chapter 2 the polynomial $\frac{1}{3}(t^3 - t)$, which has Gauss valuation -1 but is integer valued because $t^3 \equiv t \pmod 3$.

Definition 8.1 (integer-valued polynomials)**.** For a set $X \subseteq \mathbb{Q}_3$ let $\mathrm{Int}(X) = \{B \in \mathbb{Q}_3[y] : B(x) \in \mathbb{Z}_3 \text{ for all } x \in X\}$. The note uses $X = S$ [note, Section 4]; we also use $X = \mathbb{Z}_3$, and $\mathrm{Int}(\mathbb{Z})$ for the polynomials with $B(\mathbb{Z}) \subseteq \mathbb{Z}$.

$\mathrm{Int}(X)$ is closed under addition and multiplication (if two polynomials have values in $\mathbb{Z}_3$ on X, so do their sum and product) and under multiplication by elements of $\mathbb{Z}_3$; it is a ring and a $\mathbb{Z}_3$-module. The products F_iF_j in the plan above stay in $\mathrm{Int}(S)$ for this reason.

To describe $\mathrm{Int}(\mathbb{Z}_3)$ we use the *difference operator* $(\Delta f)(t) = f(t+1) - f(t)$, the discrete derivative. Pascal's rule $\binom{t+1}{c} = \binom{t}{c} + \binom{t}{c-1}$ says

$$\Delta\binom{t}{c} = \binom{t}{c-1} \qquad (c \geq 1)\ , \qquad \Delta\binom{t}{0} = 0\ , \tag{8.1}$$

so Δ acts on the binomial polynomials as $\frac{\mathrm{d}}{\mathrm{d}t}$ acts on $t^c/c!$. The binomial polynomials are the "Taylor monomials" of the discrete calculus, and the next statement is the discrete Taylor formula.

Proposition 8.2 (Mahler expansion of a polynomial; [note, (A.1)])**.** *Every polynomial $P \in \mathbb{Q}_3[t]$ of degree at most d can be written uniquely as $P = \sum_{c=0}^{d} P_c \binom{t}{c}$, with*

$$P_c = (\Delta^c P)(0) = \sum_{i=0}^{c} (-1)^{c-i} \binom{c}{i} P(i) \ . \tag{8.2}$$

Consequently $P(\mathbb{Z}_3) \subseteq \mathbb{Z}_3$ if and only if all $P_c \in \mathbb{Z}_3$, and $P(\mathbb{Z}) \subseteq \mathbb{Z}$ if and only if all $P_c \in \mathbb{Z}$. If $P(\mathbb{Z}_3) \subseteq \mathbb{Z}_3$, the monomial coefficients of P have valuation at least $-v_3(d!)$.

This is the polynomial case of Mahler's theorem on continuous functions on $\mathbb{Z}_p$ (Robert [28, Ch. 4]).

Proof. Existence and uniqueness. $\binom{t}{c}$ has degree exactly c, so $\binom{t}{0}, \dots, \binom{t}{d}$ are a basis of the polynomials of degree $\le d$ (a triangular change of basis from $1, t, \dots, t^d$). *The coefficients.* Apply Δ^c to $P = \sum_{c'} P_{c'} \binom{t}{c'}$. By (8.1), $\Delta^c \binom{t}{c'} = \binom{t}{c'-c}$ (zero if $c' < c$), and at $t = 0$ this is $\binom{0}{c'-c}$, which is 1 for $c' = c$ and 0 otherwise. So $(\Delta^c P)(0) = P_c$. Writing $\Delta = E - 1$ with the shift $(Ef)(t) = f(t+1)$, the binomial theorem for the commuting operators E and 1 gives $\Delta^c = \sum_i \binom{c}{i} (-1)^{c-i} E^i$, and $(E^i P)(0) = P(i)$. *Integrality.* If $P(\mathbb{Z}_3) \subseteq \mathbb{Z}_3$, then $P(0), \dots, P(c) \in \mathbb{Z}_3$ and (8.2) is an integer combination of them. Conversely, each $\binom{t}{c}$ maps $\mathbb{Z}_3$ to $\mathbb{Z}_3$ (Chapter 4), so an integral combination does too. The same argument works over $\mathbb{Z}$. *The coefficients in powers of t.* $\binom{t}{c} = t(t-1)\cdots(t-c+1)/c!$ has integer coefficients divided by $c!$, and $v_3(c!) \le v_3(d!)$ for $c \le d$; multiply by $P_c \in \mathbb{Z}_3$ and add. □

Example 8.3 (two Mahler expansions by difference tables)**.** For $P(t) = \frac{1}{3}(t^3 - t)$ the values at $t = 0, 1, 2, 3$ are $0, 0, 2, 8$. Taking differences repeatedly,

$$\begin{array}{cccc} 0 & 0 & 2 & 8 \\ & 0 & 2 & 6 \\ & & 2 & 4 \\ & & & 2 \end{array} \qquad \Longrightarrow \qquad P_0 = 0,\ P_1 = 0,\ P_2 = 2,\ P_3 = 2 \ ,$$

the first entries of the rows. So $\frac{1}{3}(t^3 - t) = 2\binom{t}{2} + 2\binom{t}{3}$, integer coefficients in the binomial basis although the monomial coefficients are $\pm\frac{1}{3}$. (Check at $t = 3$: $2 \cdot 3 + 2 \cdot 1 = 8$.) For $P(t) = (t+1)^3$, values $1, 8, 27, 64$, the rows begin with $1, 7, 12, 6$, so $(t+1)^3 = 1 + 7\binom{t}{1} + 12\binom{t}{2} + 6\binom{t}{3}$. Both expansions hold as polynomial identities. For $\binom{t+3}{3}^3$, a factor that will appear for $n = 3$, the Mahler coefficients are $1, 63, 873, 5191, 16620, 31560, 36750, 25830, 10080, 1680$, all integers, and the monomial coefficients have Gauss valuation -3, consistent with the bound $-v_3(9!) = -4$.

Intuition. For a function on the integers (or on $\mathbb{Z}_3$), the right notion of "small" is about values, not coefficients. The binomial basis converts values into coefficients without division, so it is the basis in which integrality is visible. Monomials hide it: $\frac{1}{3}(t^3 - t)$ looks like it has a 3 in the denominator, but it never produces one.

8.2.2 On the set S

The integration points form $S = (\frac{1}{3} + \mathbb{Z}_3) \cup (\frac{2}{3} + \mathbb{Z}_3)$. Here the situation is the opposite of $\mathbb{Z}_3$: every nonconstant monomial is large. For example $y \notin \mathrm{Int}(S)$, since $v_3(\frac{1}{3}) = -1$, but $3y \in \mathrm{Int}(S)$, and in fact $3y$ is a unit at every point of S. Hence $(3y)^i \in \mathrm{Int}(S)$, with leading coefficient 3^i. If this were the best one can do in degree i, the change of basis would cost $\sum_{i<K} 2i \approx K^2$ trits. It is not the best: the next section shows that, for example,

$$F_2(y) = 3\left(y - \frac{1}{3}\right)\left(y - \frac{2}{3}\right) = 3y^2 - 3y + \frac{2}{3}$$

lies in $\mathrm{Int}(S)$, with leading coefficient 3 instead of 9. The reason is the same as for $\frac{1}{3}(t^3-t)$ on $\mathbb{Z}$: on each of the two classes, one of the two factors $y-\frac{1}{3}$, $y-\frac{2}{3}$ is in $\mathbb{Z}_3$ (it vanishes at the base point of its class) and the other has valuation exactly -1, so the product has valuation ≥ -1 and the factor 3 makes it integral.

8.3 The basis F_i

Lemma 8.4 ([note, Lemma 4.1])**.** *For $q \geq 0$ put*

$$F_{2q}(y) = 3^q\, q! \binom{y-\frac{1}{3}}{q}\binom{y-\frac{2}{3}}{q}, \qquad F_{2q+1}(y) = 3y\, F_{2q}(y)\ . \tag{8.3}$$

Then $F_i \in \mathrm{Int}(S)$, $\deg F_i = i$, and the leading coefficient of F_i has 3-adic valuation $-\nu_i$, where

$$\nu_i = v_3(q!) - q - e \qquad \text{for } i = 2q+e,\ e \in \{0,1\}\ . \tag{8.4}$$

Consequently, for every $\mathbb{Q}_3$-linear functional Λ' on $\mathbb{Q}_3[y]$,

$$v_3 \det\left[\Lambda'(y^{i+j})\right]_{i,j<K} \ \geq\ 2\sum_{i<K}\nu_i + K \min_{i,j<K} v_3\,\Lambda'(F_iF_j)\ . \tag{8.5}$$

Here $\binom{y-\frac{1}{3}}{q}$ means the binomial polynomial $\binom{x}{q}$ evaluated at $x = y-\frac{1}{3}$, a polynomial of degree q in y.

Example 8.5 (the first basis polynomials)**.** Expanding (8.3) gives

$$F_0 = 1\ , \qquad F_1 = 3y\ , \qquad F_2 = 3y^2 - 3y + \tfrac{2}{3}\ ,$$
$$F_3 = 9y^3 - 9y^2 + 2y\ , \quad F_4 = \tfrac{9}{2}y^4 - 18y^3 + \tfrac{49}{2}y^2 - 13y + \tfrac{20}{9}\ , \quad F_5 = 3y\,F_4\ .$$

The coefficients are not in $\mathbb{Z}_3$ (there are $\frac{2}{3}$ and $\frac{20}{9}$), but the values on S are: for $y = t + \frac{r}{3}$ and $t = 0,\dots,5$,

	$t=0$	1	2	3	4	5
$F_2(t+\frac{1}{3})$	0	2	10	24	44	70
$F_2(t+\frac{2}{3})$	0	4	14	30	52	80
$F_4(t+\frac{1}{3})$	0	0	10	120	528	1540
$F_4(t+\frac{2}{3})$	0	0	28	210	780	2080

all integers. The proof below explains the pattern: $F_2(t+\frac{1}{3}) = \binom{t}{1}(3t-1)$, e.g. $2\cdot 5 = 10$ at $t=2$.

8.3.1 Proof that F_i is integer valued on S

We treat the two classes of S separately.

The class $\frac{1}{3}+\mathbb{Z}_3$. Let $y = \frac{1}{3}+s$ with $s \in \mathbb{Z}_3$.

- The first binomial factor is $\binom{y-1/3}{q} = \binom{s}{q}$, which lies in $\mathbb{Z}_3$ because $\binom{x}{q}$ maps $\mathbb{Z}_3$ into $\mathbb{Z}_3$ (Chapter 4).
- For the second factor we absorb the 3^q and the $q!$. By definition $q!\binom{x}{q} = \prod_{i<q}(x-i)$, so

$$3^q\, q!\binom{y-\frac{2}{3}}{q} = 3^q \prod_{i<q}\left(y-\frac{2}{3}-i\right) = \prod_{i<q}(3y-2-3i) = \prod_{i<q}(3s+1-2-3i) = \prod_{i<q}(3s-1-3i)\ ,$$

using $3y = 1+3s$. Every factor $3s-1-3i$ is $\equiv -1 \pmod 3$, a 3-adic unit; the product of units is a unit.

Hence $F_{2q}(\frac{1}{3}+s) = \binom{s}{q} \cdot \prod_{i<q}(3s-1-3i) \in \mathbb{Z}_3$, and its valuation equals $v_3\binom{s}{q}$.

The class $\frac{2}{3}+\mathbb{Z}_3$. Let $y = \frac{2}{3}+s$. Now the roles are exchanged: $\binom{y-2/3}{q} = \binom{s}{q} \in \mathbb{Z}_3$, and $3^q q!\binom{y-1/3}{q} = \prod_{i<q}(3y-1-3i) = \prod_{i<q}(3s+1-3i)$, a product of numbers $\equiv 1 \pmod 3$, again a unit.

Odd indices. On S, $v_3(y) = -1$, so $3y$ is a unit and $F_{2q+1} = 3y\,F_{2q}$ has the same valuation as F_{2q}, in particular $F_{2q+1}(S) \subseteq \mathbb{Z}_3$.

Degrees and leading coefficients. $\binom{x}{q}$ has degree q and leading coefficient $\frac{1}{q!}$. So F_{2q} has degree $2q$ and leading coefficient $3^q\,q! \cdot \frac{1}{q!} \cdot \frac{1}{q!} = \frac{3^q}{q!}$, of valuation $q - v_3(q!) = -\nu_{2q}$. And F_{2q+1} has degree $2q+1$ and leading coefficient $\frac{3^{q+1}}{q!}$, of valuation $q+1-v_3(q!) = -\nu_{2q+1}$. □

Intuition: why both classes are needed. On the class $\frac{1}{3}+\mathbb{Z}_3$ the first factor $\binom{y-1/3}{q}$ sees the integers ($y - \frac{1}{3} \in \mathbb{Z}_3$) and is integral, while the second factor sees points at 3-adic distance 3 from $\mathbb{Z}_3$ (offset $\frac{1}{3}$) and would have valuation $-q - v_3(q!)$; the prefactor $3^q q!$ exactly repairs it. On the other class the two factors swap jobs. One binomial factor for each class: the product works on both. The odd members $3yF_{2q}$ fill in the odd degrees at the cost of one extra factor 3.

Example 8.6 (numerical check of integrality)**.** Evaluate $F_0, \dots, F_9$ exactly at 266 points of S: $y = t + \frac{r}{3}$ for all integers $t \in [-60, 60]$ and $r = 1, 2$, and 24 further points with non-integral $t \in \mathbb{Z}_3$ ($t = \frac{1}{2}, -\frac{1}{2}, \frac{1}{4}, \frac{2}{5}, -\frac{7}{10}, \frac{13}{8}, \frac{1}{7}, \frac{22}{7}, -\frac{5}{11}, \frac{100}{13}, \frac{1}{1024}, -\frac{3}{2}$, each with $r = 1, 2$). For every $i \le 9$ the minimum of $v_3(F_i(y))$ over the points is exactly 0: all values are in $\mathbb{Z}_3$, and some are units. The number of points with a unit value is 266 for F_0, F_1; 182 for F_2, F_3; 88 for F_4, F_5; 184 for F_6, F_7; 126 for F_8, F_9 (by the proof above, $F_{2q}(\frac{r}{3}+s)$ is a unit exactly when $\binom{s}{q}$ is). So the F_i are not "wastefully" divisible by 3: no constant multiple $3^{-1}F_i$ would still be integral on S. Off S they fail: at $y = 0, 1, -2$ (points of $\mathbb{Z}_3$, not of S) one finds $v_3(F_2) = -1$ and $v_3(F_4) = -2$, and at $y = \frac{1}{9}, \frac{4}{9}$ (valuation -2) one finds $v_3(F_1) = -1$, $v_3(F_2) = -3$, $v_3(F_4) = -6$. $\mathrm{Int}(S)$ depends on S.

8.3.2 The leading coefficients

Example 8.7 (the numbers ν_i)**.** From (8.4) with $v_3(q!)$ from Legendre's formula (Chapter 2); reading off the leading coefficients from the expanded polynomials confirms $v_3(\text{lead}) = -\nu_i$ for $i \le 12$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
(q,e)	0,0	0,1	1,0	1,1	2,0	2,1	3,0	3,1	4,0	4,1	5,0	5,1	6,0
lead. coeff. of F_i	1	3	3	9	$\frac{9}{2}$	$\frac{27}{2}$	$\frac{9}{2}$	$\frac{27}{2}$	$\frac{27}{8}$	$\frac{81}{8}$	$\frac{81}{40}$	$\frac{243}{40}$	$\frac{81}{80}$
ν_i	0	−1	−1	−2	−2	−3	−2	−3	−3	−4	−4	−5	−4
$-i$ (basis $(3y)^i$)	0	−1	−2	−3	−4	−5	−6	−7	−8	−9	−10	−11	−12

The ν_i are negative and decrease roughly like $-i/4$ (from $q - v_3(q!) \approx q/2$ with $q \approx i/2$), whereas the naive basis $(3y)^i$ has $-i$. At $i = 6$ the factorial 3! in the denominator of $\frac{3^3}{3!} = \frac{9}{2}$ gives back one factor 3, so $\nu_6 = -2 > \nu_5$.

8.3.3 Can one do better? The optimal basis

The note only needs that the F_i lie in $\mathrm{Int}(S)$ and have the stated leading coefficients. It is natural to ask whether another choice of polynomials in $\mathrm{Int}(S)$ would have leading coefficients of smaller valuation and therefore a smaller cost. The answer is no, and there is a general theory behind it, due to Bhargava [5], to which the note refers.

Fact 8.8 (p-orderings; Bhargava [5])**.** *Let $X \subseteq \mathbb{Z}_3$ be infinite. Choose $a_0 \in X$ arbitrarily and, inductively, $a_i \in X$ minimizing $v_3 \prod_{j<i}(a_i - a_j)$ (a "3-ordering"). The numbers $\phi_X(i) = v_3 \prod_{j<i}(a_i - a_j)$ do not depend on the choices, and the polynomials $\prod_{j<i}(x - a_j)/(a_i - a_j)$, $i \geq 0$, form a $\mathbb{Z}_3$-basis of $\mathrm{Int}(X)$. In particular every element of $\mathrm{Int}(X)$ of degree i has a leading coefficient of valuation at least $-\phi_X(i)$, and this value is attained.*

(Bhargava calls $3^{\phi_X(i)}$ the 3-part of the generalized factorial $i!_X$; for $X = \mathbb{Z}_3$ the greedy choice $a_i = i$ gives $\phi(i) = v_3(i!)$ and the basis $\binom{x}{i}$; indeed $\prod_{j<m}(x-j) = m!\binom{x}{m}$ with $\binom{x}{m} \in \mathbb{Z}_3$ for $x \in \mathbb{Z}_3$, so the minimum over x of $v_3 \prod_{j<m}(x-j)$ is at least $v_3(m!)$, with equality at $x = m$.) The substitution $x = 3y$ maps S onto $X = \mathbb{Z}_3^\times$, and $B(y) \in \mathrm{Int}(S)$ if and only if $B(x/3) \in \mathrm{Int}(\mathbb{Z}_3^\times)$; a leading coefficient ℓ in x becomes $3^i\ell$ in y. So the smallest possible valuation of the leading coefficient of a degree-i element of $\mathrm{Int}(S)$ is $i - \phi_{\mathbb{Z}_3^\times}(i)$.

Example 8.9 (the 3-ordering of $\mathbb{Z}_3^\times$)**.** Run the greedy choice on the $2 \cdot 3^{M-1}$ residues prime to 3 modulo 3^M, for $M = 6$ and $M = 7$ (the results for $M = 6$ and $M = 7$ coincide, and the largest valuation $v_3(a_i - a_j)$ that occurs is $3 < M$, which indicates that the truncation does not affect the minima). The ordering begins $1, 2, 4, 5, 7, 8, 10, 11, 13, 14$, the units in increasing order, and for $i = 0, \ldots, 30$

$$\begin{aligned}\phi_{\mathbb{Z}_3^\times}(i) = {} & 0, 0, 1, 1, 2, 2, 4, 4, 5, 5, 6, 6, 8, 8, 9, 9, \\ & 10, 10, 13, 13, 14, 14, 15, 15, 17, 17, 18, 18, 19, 19, 21\ ,\end{aligned}$$

identical for $M = 6, 7$. For every $i \leq 30$ this equals $\psi(\lfloor i/2 \rfloor) = \lfloor i/2 \rfloor + v_3(\lfloor i/2 \rfloor!)$ (the function ψ of Section 8.6) and equals $i + \nu_i$. So the minimal possible leading valuation $i - \phi(i)$ equals $-\nu_i$, the valuation of the leading coefficient of F_i, for all $i \leq 30$.

The equality $\phi_{\mathbb{Z}_3^\times}(i) = \psi(\lfloor i/2 \rfloor)$ holds for all i, not only for $i \leq 30$. Indeed, $\mathbb{Z}_3^\times$ is the disjoint union of the classes $1 + 3\mathbb{Z}_3$ and $2 + 3\mathbb{Z}_3$; a difference of elements from different classes is a unit, so $v_3 \prod_{j<i}(a_i - a_j)$ only counts the earlier points in the class of a_i. Within each class the greedy choice is therefore a 3-ordering of that class, and a class $a + 3\mathbb{Z}_3$ is a translate of $3\mathbb{Z}_3$, and $v_3 \prod_{j<m}(3b - 3b_j) = m + v_3 \prod_{j<m}(b - b_j)$. By the independence of the numbers $\phi_X(i)$ from the choices (Fact 8.8), applied to the class, after m earlier points in the class the minimum is therefore the 3-sequence $v_3(m!)$ of $\mathbb{Z}_3$ plus one trit for each of the m factors, that is $\psi(m)$. Since ψ is strictly increasing (Lemma 8.21), the greedy choice always takes its next point in the class that has so far received fewer points, so after i steps the two classes hold $\lfloor i/2 \rfloor$ and $\lceil i/2 \rceil$ points, and $\phi_{\mathbb{Z}_3^\times}(i) = \psi(\lfloor i/2 \rfloor) = i + \nu_i$.

So, granting Fact 8.8, the F_i are optimal in every degree, and then $F_0, \ldots, F_d$ are a $\mathbb{Z}_3$-basis of the elements of $\mathrm{Int}(S)$ of degree $\leq d$, for every d: given $B \in \mathrm{Int}(S)$ of degree i, the ratio of its leading coefficient to that of F_i is in $\mathbb{Z}_3$ by optimality, subtracting that multiple of F_i lowers the degree and stays in $\mathrm{Int}(S)$, and one continues downwards. Consequently no basis of integer-valued polynomials makes the cost (8.5) smaller: any other basis $G_0, \ldots, G_{K-1}$ of elements of $\mathrm{Int}(S)$ is $G = UF$ with a matrix U over $\mathbb{Z}_3$, so the valuation of its change-of-basis determinant is that of the F_i plus $v_3 \det U \geq 0$. This optimality is not used in the proof; it explains why the change of basis at $p = 3$ costs about $K^2/4$ trits and cannot be made to gain.

8.3.4 The change-of-basis inequality [note, (4.3)]

Proof of (8.5). Write $F_i = \sum_{j \leq i} f_{ij} y^j$ and let $T = [f_{ij}]_{i,j<K}$, row i holding the coefficients of F_i. Since $\deg F_i = i$, T is lower triangular with diagonal entries f_{ii}, the leading coefficients. By the change-of-basis rule (Chapter 6), $[\Lambda'(F_iF_j)] = T\,[\Lambda'(y^{i+j})]\,T^{\mathsf{T}}$, so

$$\det[\Lambda'(F_iF_j)] = (\det T)^2 \det\left[\Lambda'(y^{i+j})\right], \qquad \det T = \prod_{i<K} f_{ii}\ .$$

Taking valuations, $v_3 \det[\Lambda'(y^{i+j})] = v_3 \det[\Lambda'(F_iF_j)] - 2\sum_{i<K} v_3(f_{ii}) = v_3 \det[\Lambda'(F_iF_j)] + 2\sum_{i<K} \nu_i$. Finally, by the Leibniz formula $\det[\Lambda'(F_iF_j)] = \sum_\sigma \operatorname{sgn}(\sigma) \prod_i \Lambda'(F_iF_{\sigma(i)})$; each product has valuation $\geq K \min_{i,j} v_3\Lambda'(F_iF_j)$, and so has the sum, by the ultrametric inequality. (If the determinant is 0, its valuation is $+\infty$ and there is nothing to prove.) □

For $n = 1$, $K = 4$, Chapter 6 found $\det T = 81$, entries $v_3 L(F_iF_j) \in \{11, 12, 13\}$ (see also Section 8.8), and the bound $2(0 - 1 - 1 - 2) + 4 \cdot 11 = 36$ against the actual 38.

8.4 The cost of the change of basis

The first term of (8.5) is negative. The note computes it as [note, (4.4)]

$$2\sum_{i<K} \nu_i = -\frac{K^2}{4} + O(K \log K) \ . \tag{8.6}$$

Derivation, step by step. Take $K = 2Q$ even first. Group the indices in pairs $i = 2q$, $2q + 1$ for $q < Q$. By (8.4) and Legendre's formula $v_3(q!) = \frac{q - s_3(q)}{2}$ (Chapter 2), with $s_3(q)$ the sum of the ternary digits of q,

$$\nu_{2q} + \nu_{2q+1} = 2(v_3(q!) - q) - 1 = (q - s_3(q)) - 2q - 1 = -q - s_3(q) - 1 \ .$$

Summing over $q < Q$ and using $\sum_{q<Q} q = \frac{Q(Q-1)}{2}$,

$$2\sum_{i<K} \nu_i = -Q(Q-1) - 2Q - 2\sum_{q<Q} s_3(q) = -Q^2 - Q - 2\sum_{q<Q} s_3(q) \ ,$$

that is, with $Q = K/2$,

$$2\sum_{i<K} \nu_i = -\frac{K^2}{4} - \frac{K}{2} - 2\sum_{q<K/2} s_3(q) \qquad (K \text{ even}) \ . \tag{8.7}$$

This is exact. For the error term, $0 \leq s_3(q) \leq 2\log_3(3q) \leq 2\log_3(\frac{3K}{2})$ for $1 \leq q < \frac{K}{2}$ (Chapter 2), so $0 \leq 2\sum_{q<K/2} s_3(q) \leq 2K \log_3(\frac{3K}{2})$, and

$$-\frac{K^2}{4} - \frac{K}{2} - 2K \log_3 \frac{3K}{2} \ \leq \ 2\sum_{i<K} \nu_i \ \leq \ -\frac{K^2}{4} \ .$$

For odd K, add the single term $2\nu_{K-1} = 2(v_3(q!) - q)$ with $q = \frac{K-1}{2}$, which is $-q - s_3(q) = O(K)$, and $-\frac{(K-1)^2}{4}$ differs from $-\frac{K^2}{4}$ by $O(K)$. This proves (8.6). The note's intermediate form $-2\sum_{q<K/2} q$ is the main term $-Q(Q-1)$ of the second display. □

Example 8.10 (the cost in numbers)**.** Summing ν_i directly gives the following; for each even K below the sum agrees with the exact formula (8.7).

K	$2\sum_{i<K} \nu_i$	$-\frac{K^2}{4}$	diff.	$\frac{\text{diff.}}{K \log_3 K}$	$(3y)^i$: $-K(K-1)$	$p = 2$: $2\sum_{i<K} v_2(i!)$	K^2
4	−8	−4	−4	−0.79	−12	4	16
10	−42	−25	−17	−0.81	−90	60	100
100	−2880	−2500	−380	−0.91	−9900	9268	10^4
1000	−255960	−250000	−5960	−0.95	−999000	989136	10^6
10^4	−25080196	−25000000	−80196	−0.96	−99990000	99860784	10^8

The relative error (difference)/$(K^2/4)$ is 68% at $K = 10$, 15% at $K = 100$ and 0.3% at $K = 10^4$: the asymptotics (8.6) becomes accurate only for large K. The difference is close to $-K \log_3 K$, because the average ternary digit is about 1, so $2\sum_{q<K/2} s_3(q) \approx K \log_3 \frac{K}{2}$.

Comparison with $p = 2$ (the note's remark after [note, (4.4)]). In [19], where $\zeta_2(7)$ is treated, the integration set is a translate of $\mathbb{Z}_2$, and the integer-valued basis there is the binomial basis in the translated variable, $\binom{y-y_0}{i}$, with leading coefficient $\frac{1}{i!}$, of 2-adic valuation $-v_2(i!)$. The same computation gives $2\sum_{i<K} v_2(i!)$ in place of $2\sum \nu_i$: a *positive* contribution, about K^2 bits since $v_2(i!) \approx i$. The last two columns of the table show the ratio approaching 1 (0.93 at $K = 100$, 0.999 at $K = 10^4$). At $p = 2$ the change of basis *gains*, because binomial polynomials on $\mathbb{Z}_p$ have large denominators; at $p = 3$ on S it *costs*, because S consists of large points ($|y|_3 = 3$) and integer-valued polynomials on S must have 3-adically small coefficients. So at $p = 3$, as the note says, the whole gain must come from the weight.

Intuition: how much the choice of basis matters. With the naive basis $(3y)^i$ the cost would be $-K(K-1)$ instead of about $-K^2/4$, and the gain constant would become $(10.5\kappa - \kappa^2)\log_2 3$ instead of $G(\kappa)$. At $\kappa = 2.8$ this is 34.17 bits per n^2 instead of 43.49, and the note's bound on size plus denominators on the first interval is $F_1^\dagger + c_1 = 8.43 + 30.48 = 38.91$ ([note, Table 1]): the margin would be -4.74 instead of $+4.58$, and the proof would not close (with the note's other estimates unchanged). The optimal basis is not a refinement; it is needed.

8.5 The weight on S: the factorization [note, (4.5)]

Now the analytic half. Recall the weight [note, (1.2)]

$$W(y) = \frac{(y+\frac{n}{2})\left(y+\frac{1}{3}\right)_n^3\left(y+\frac{2}{3}\right)_n^3}{\prod_{k=-n}^{2n}(y+k)^4}\ , \qquad (x)_n = x(x+1)\cdots(x+n-1)\ ,$$

with n odd (Chapter 5). Fix $r \in \{1,2\}$ and put $y = t + \frac{r}{3}$, $t \in \mathbb{Z}_3$. We go through the four factors and extract from each its exact power of 3.

- *The integral Pochhammer symbol.* Of the two shifts $\frac{1}{3}, \frac{2}{3}$, one equals $\frac{3-r}{3}$, and $y + \frac{3-r}{3} = t+1$. So
$$\left(y+\tfrac{3-r}{3}\right)_n = (t+1)(t+2)\cdots(t+n) = n!\binom{t+n}{n}\ ,$$
since $\binom{t+n}{n} = \frac{(t+n)(t+n-1)\cdots(t+1)}{n!}$. The polynomial $\binom{t+n}{n}$ maps $\mathbb{Z}_3$ into $\mathbb{Z}_3$ (Chapter 4). Its cube contributes $(n!)^3\binom{t+n}{n}^3$.
- *The other Pochhammer symbol.* The remaining shift is $\frac{r}{3}$, and $y + \frac{r}{3} + i = t + \frac{2r}{3} + i = \frac{1}{3}(3t + 2r + 3i)$, so
$$\left(y+\tfrac{r}{3}\right)_n = \prod_{i<n}\left(t+\tfrac{2r}{3}+i\right) = 3^{-n}\prod_{i<n}(3t+2r+3i)\ .$$
Each $3t + 2r + 3i \equiv 2r \pmod 3$ with $2r \in \{2,4\}$, so it is a unit. The cube contributes 3^{-3n} times a unit.
- *The linear factor.* $y + \frac{n}{2} = t + \frac{r}{3} + \frac{n}{2} = \frac{1}{6}(6t + 2r + 3n)$, and $6t + 2r + 3n \equiv 2r \not\equiv 0 \pmod 3$. Since $\frac{1}{6} = \frac{1}{2}\cdot\frac{1}{3}$ and $\frac{1}{2}$ is a unit, this contributes 3^{-1} times a unit.
- *The poles.* $(y+k)^{-4} = \left(\frac{3t+r+3k}{3}\right)^{-4} = 3^4(3t+r+3k)^{-4}$, and $3t + r + 3k \equiv r \pmod 3$ is a unit. With $3n+1$ nodes this contributes $3^{4(3n+1)}$ times a unit.

The powers of 3 add up to $-3n - 1 + 4(3n+1) = 9n + 3$. Collecting,

$$W\left(t+\frac{r}{3}\right) = 3^{9n+3}(n!)^3\binom{t+n}{n}^3 Q_r(t)\ , \qquad Q_r(t) = \frac{6t+2r+3n}{2}\cdot\frac{\prod_{i<n}(3t+2r+3i)^3}{\prod_{k=-n}^{2n}(3t+r+3k)^4}\ . \tag{8.8}$$

This is [note, (4.5)], with Q_r written out: a unit constant $(\frac{1}{2})$ times factors $a+6t$ and $(a+3t)^{\pm 1}$ with integers a prime to 3.

Example 8.11 ($n=1$)**.** For $n=1$, $r=1$: the nodes are $k=-1,0,1,2$, so

$$W\left(t+\tfrac{1}{3}\right) = 3^{12}\,(t+1)^3\,Q_1(t)\ , \qquad Q_1(t) = \frac{(6t+5)\,(3t+2)^3}{2\,(3t-2)^4(3t+1)^4(3t+4)^4(3t+7)^4}\ .$$

At $t=0$: $W(\frac{1}{3}) = 3^{12}\cdot\frac{5\cdot 8}{2\cdot 16\cdot 1\cdot 256\cdot 2401} = 3^{12}\cdot\frac{5}{2458624}$, and since $2458624 = 2^{10}\cdot 7^4$ this is the value $W(\frac{1}{3}) = \frac{5\cdot 3^{12}}{2^{10}\cdot 7^4}$ found in Chapter 5. More generally $v_3(W(\frac{1}{3}+t)) = 12+3v_3(t+1)$; direct evaluation gives $12, 12, 15, 12, 12, 15$ for $t=0,\dots,5$, as predicted.

Example 8.12 (numerical check of (8.8))**.** For $n=1$ and $n=3$, $r=1,2$, we compute $W(t+\frac{r}{3})/\big(3^{9n+3}(n!)^3\binom{t+n}{n}^3\big)$ exactly at all integers $t\in[-40,40]$ (except the n points $t=-1,\dots,-n$, where both sides vanish) and at $t=\frac{1}{2},-\frac{1}{2},\frac{5}{4},\frac{2}{7},-\frac{9}{10},\frac{31}{16}$: 86 points for $n=1$ and 84 for $n=3$. In every case the quotient equals the product formula for $Q_r(t)$ in (8.8), and its valuation is 0: $Q_r(t)$ is a 3-adic unit at every tested point. So the whole 3-adic size of the weight on S is $3^{9n+3}(n!)^3\binom{t+n}{n}^3$.

8.5.1 The Taylor coefficients of Q_r

For the analytic step we need Q_r as a power series in t, and the note's claim is $Q_r(t)=\sum_i q_i t^i$ with $v_3(q_i)\ge i$.

Why $v_3(q_i)\ge i$. Call a power series *good* if its coefficient of t^i has valuation $\ge i$ for every i. Each factor of Q_r is good:

- $a+3t$ and $a+6t$ have coefficients a (valuation 0) and 3 or 6 (valuation 1);
- $(a+3t)^{-1} = \sum_{m\ge 0}\frac{(-3)^m}{a^{m+1}}t^m$ for $3\nmid a$ has coefficients of valuation exactly m (Chapter 2, the unit series);
- the constant $\frac{1}{2}$ is a unit.

The product of two good series is good: the coefficient of t^i in $(\sum c_j t^j)(\sum d_m t^m)$ is $\sum_{j+m=i} c_j d_m$, each term has valuation $\ge j+m=i$, and so has the sum (ultrametric inequality). Q_r is a finite product of good series (with repetitions for the powers 3 and 4), hence good. □

A good series converges for $|t|_3<3$, because $|q_i t^i|_3 \le (|t|_3/3)^i \to 0$. This is consistent with the poles of Q_r at $t=-\frac{a}{3}$, which have $|t|_3=3$.

Example 8.13 (the first coefficients)**.** For $n=1$, $r=1$, the first coefficients of Q_1 are

$$q_0=\frac{5}{2458624}\ ,\quad q_1=-\frac{351}{34420736}\ ,\quad q_2=\frac{63639}{963780608}\ ,\quad q_3=-\frac{1022139}{3373232128}\ ,$$

with $351=3^3\cdot 13$. The valuations of $q_0,\dots,q_8$, computed in exact rational arithmetic, are:

i	0	1	2	3	4	5	6	7	8
$n=1$, $r=1$	0	3	3	4	5	7	6	9	10
$n=1$, $r=2$	0	6	3	4	5	7	6	9	10
$n=3$, $r=1$	0	2	3	3	5	6	6	12	10
$n=3$, $r=2$	0	2	3	3	5	6	6	10	10

Every entry is $\ge i$, sometimes with equality ($i=0,6$ for $n=1$; $i=0,3,6$ for $n=3$), so the bound cannot be improved in general. As a check on the series itself, $Q_1(3^{40})-q_0-q_1 3^{40}$ has $v_3=83$, as it must ($v_3(q_2 3^{80})=83$).

8.5.2 The trit budget

Read (8.8) as a budget per entry of the Hankel matrix: the poles give $4(3n+1)$ trits, the non-integral Pochhammer symbol and the linear factor cost $3n+1$ trits, and the integral Pochhammer symbol contributes $(n!)^3$, which is $3v_3(n!) \approx 1.5n$ trits by Legendre's formula. The note names the total

$$A_3 = 9n + 3 + 3v_3(n!) \ .$$

Example 8.14 (the budget for several n)**.**

n	poles $4(3n+1)$	Pochhammer + linear $-(3n+1)$	$3v_3(n!)$	A_3	A_3/n
1	16	−4	0	12	12.000
3	40	−10	3	33	11.000
5	64	−16	3	51	10.200
11	136	−34	12	114	10.364
101	1216	−304	144	1056	10.455
1001	12016	−3004	1494	10506	10.496
10001	120016	−30004	14988	105000	10.499
100001	1200016	−300004	149985	1049997	10.4999

$A_3/n \to 9 + 1.5 = 10.5$, the coefficient 10.5 in $G(\kappa)$. For $n = 1$, $A_3 = 12$ is the $v_3(W(\frac{1}{3})) = 12$ of Chapter 5.

Intuition: why the zeros sit on S-shifted classes. The zeros of W cost trits on S: a zero at a point of $\pm\frac{1}{3} + \mathbb{Z}$ is at distance ≤ 1 from half of S but at distance exactly 3 from the other half (the class of the other residue), where it contributes a factor of size 3. That is the $-3n$. In exchange, on the half where the zeros are close, they form $(t+1)_n = n!\binom{t+n}{n}$, and the $n!$ gives back about $1.5n$ trits. The zeros are needed for other reasons (they cancel the virtual poles at the primes $p \neq 3$, Chapter 12); the 3-adic estimate only has to survive them.

8.6 The analytic step: derivative and integral cost only logarithms

We now know that on S the integrand of $L(B)$, before the derivative, is 3^{A_3} times $P(t)Q_r(t)$ with $P(t) = B(t+\frac{r}{3})\binom{t+n}{n}^3$ integral on $\mathbb{Z}_3$ and Q_r good. It remains to see how much divisibility the derivative and the Volkenborn integral destroy.

Lemma 8.15 ([note, Lemma 4.6], after [19, Lemmas 4.2, 4.3])**.** *Let $d \geq 1$, let P be a polynomial of degree at most d with $P(\mathbb{Z}_3) \subseteq \mathbb{Z}_3$, and let $Q(t) = \sum_i q_i t^i$ with $v_3(q_i) \geq i$. Then PQ is strictly differentiable on $\mathbb{Z}_3$, and*

$$v_3 \int_{\mathbb{Z}_3} (PQ)'(t)\,\mathrm{d}t \ \geq \ -\log_3 d - \log_3(d+1) \ . \tag{8.9}$$

Intuition: where the two logarithms come from. Over $\mathbb{R}$, differentiating t^c multiplies by c, harmless. In $\mathbb{Z}_3$ the dangerous operations are *divisions* by integers divisible by 3. In the binomial basis, which is where integrality is visible (Proposition 8.2), the derivative of $\binom{t}{c}$ is $\sum_{i=1}^{c} \frac{(-1)^{i-1}}{i}\binom{t}{c-i}$: division by $i \leq c$, which loses at most $v_3(i) \leq \log_3 c$ trits. The Volkenborn integral of $\binom{t}{c}$ is $\frac{(-1)^c}{c+1}$ by (V2): division by $c+1$, at most $\log_3(c+1)$ trits. For $c \leq d$ this gives the two terms of (8.9). The binomial components of PQ of degree $c > d$ come from Q, and they are divisible by about 3^{c-d} (their source is q_i with $v_3(q_i) \geq i$), which more than pays for the larger divisors i and $c+1$. The proof makes this precise with a single bookkeeping function ψ.

The proof ([note, Appendix A]) needs four tools, which we introduce first: the Mahler expansion (Proposition 8.2), Stirling numbers, the function ψ, and a product formula for binomial polynomials.

8.6.1 Stirling numbers of the second kind

Definition 8.16 (Stirling numbers of the second kind)**.** For integers $i, m \geq 0$, $\left\{ {i \atop m} \right\}$ is the number of ways to partition a set of i elements into m nonempty blocks (unordered). Equivalently, by the recursion $\left\{ {i \atop m} \right\} = m\left\{ {i-1 \atop m} \right\} + \left\{ {i-1 \atop m-1} \right\}$, $\left\{ {0 \atop 0} \right\} = 1$, $\left\{ {i \atop 0} \right\} = 0$ for $i \geq 1$: the i-th element either joins one of the m blocks of a partition of the first $i-1$ elements, or forms a new block.

Example 8.17 (a small table)**.**

$i\backslash m$	0	1	2	3	4	5	6	7
0	1							
1	0	1						
2	0	1	1					
3	0	1	3	1				
4	0	1	7	6	1			
5	0	1	15	25	10	1		
6	0	1	31	90	65	15	1	
7	0	1	63	301	350	140	21	1

E.g. $\left\{ {3 \atop 2} \right\} = 3$: $\{1,2,3\}$ splits into two blocks as $\{1\}\{2,3\}$, $\{2\}\{1,3\}$, $\{3\}\{1,2\}$.

Proposition 8.18 (monomials in the binomial basis)**.** *For every integer $i \geq 0$, as polynomials in t,*

$$t^i = \sum_{m=0}^{i} \left\{ {i \atop m} \right\} m! \binom{t}{m} . \tag{8.10}$$

Proof. Both sides are polynomials of degree i, so it suffices to check them at all integers $t \geq 0$. The left side counts the maps from an i-element set A to a t-element set Y. Sort the maps by their image, of size m: the fibres of the map partition A into m nonempty blocks ($\left\{ {i \atop m} \right\}$ ways), and the map is then an injection of the m blocks into Y ($t(t-1)\cdots(t-m+1) = m!\binom{t}{m}$ ways). □

E.g. $t^3 = \binom{t}{1} + 3 \cdot 2\binom{t}{2} + 1 \cdot 6\binom{t}{3} = t + 3t(t-1) + t(t-1)(t-2)$; expanding both sides confirms (8.10) for $i \leq 15$. The point of (8.10) for us: the m-th binomial coefficient of t^i is $\left\{ {i \atop m} \right\} m!$, an integer divisible by $m!$.

8.6.2 The function ψ

Definition 8.19 ([note, Appendix A])**.** $\psi(m) = m + v_3(m!)$ for integers $m \geq 0$.

Example 8.20. $\psi(0), \ldots, \psi(15) = 0, 1, 2, 4, 5, 6, 8, 9, 10, 13, 14, 15, 17, 18, 19, 21$. The jumps by 2 at $m = 3, 6, 12, 15$ and by 3 at $m = 9$ come from the multiples of 3 and of 9. By Legendre's formula $\psi(m) = \frac{3}{2}m - \frac{1}{2}s_3(m) \approx 1.5m$.

Intuition. $\psi(m)$ is the guaranteed valuation of the m-th binomial coefficient of a good series: the coefficient q_i of t^i has $v_3 \geq i \geq m$, and converting t^i to the binomial basis multiplies by $m!$ (8.10), which adds $v_3(m!)$.

Lemma 8.21 (properties of ψ; [note, Appendix A])**.** *ψ is strictly increasing, and superadditive: $\psi(a+b) \geq \psi(a) + \psi(b)$ for all $a, b \geq 0$.*

Proof. Increasing: $\psi(m+1)-\psi(m) = 1+v_3(m+1) \geq 1$. Superadditive:

$$\psi(a+b)-\psi(a)-\psi(b) = v_3((a+b)!)-v_3(a!)-v_3(b!) = v_3\binom{a+b}{a} \geq 0 ,$$

because $\binom{a+b}{a} = \frac{(a+b)!}{a!\,b!}$ is an integer (it counts the a-element subsets of an $(a+b)$-element set). □

Example 8.22. $\psi(1+2) = 4 \geq \psi(1)+\psi(2) = 3$, with defect $v_3\binom{3}{1} = 1$; $\psi(9) = 13 \geq \psi(4)+\psi(5) = 11$, defect $v_3\binom{9}{4} = v_3(126) = 2$. A direct computation confirms $\psi(a+b)-\psi(a)-\psi(b) = v_3\binom{a+b}{a} \geq 0$ for all $a, b \leq 300$, and that ψ increases for $m < 2000$.

8.6.3 The product of two binomial polynomials

Lemma 8.23 ([note, (A.2)])**.** *For integers $a, b \geq 0$,*

$$\binom{t}{a}\binom{t}{b} = \sum_{c=\max(a,b)}^{a+b} \binom{c}{a}\binom{a}{c-b}\binom{t}{c} . \tag{8.11}$$

Proof. Both sides are polynomials in t, so it suffices to check integers $t \geq 0$. The left side counts pairs (A, B) of subsets of a t-element set with $|A| = a$, $|B| = b$. Sort them by the union $C = A \cup B$, of size c between $\max(a,b)$ and $a+b$. Choose C: $\binom{t}{c}$ ways. Choose $A \subseteq C$: $\binom{c}{a}$ ways. Then B must contain the $c-a$ elements of $C \setminus A$, and the remaining $b-(c-a)$ elements of B are chosen inside A: $\binom{a}{b-c+a} = \binom{a}{c-b}$ ways. □

Example 8.24. $a = b = 2$: $\binom{t}{2}^2 = \binom{t}{2} + 6\binom{t}{3} + 6\binom{t}{4}$ (coefficients $\binom{2}{2}\binom{2}{0} = 1$, $\binom{3}{2}\binom{2}{1} = 6$, $\binom{4}{2}\binom{2}{2} = 6$). At $t = 4$: $36 = 6 + 24 + 6$. For $t = 5$, $a = 2$, $b = 3$ there are $\binom{5}{2}\binom{5}{3} = 100$ pairs, and $\sum_c \binom{5}{c}\binom{c}{2}\binom{2}{c-3} = 100$. Expanding both sides confirms (8.11) for all $a, b \leq 8$.

The coefficients in (8.11) are integers. So a product of two polynomials with integral Mahler coefficients has integral Mahler coefficients, and the degree of the binomial terms is at least the larger of the two degrees.

8.6.4 The derivative of a binomial polynomial

Lemma 8.25 ([note, Appendix A])**.** *For $c \geq 1$,*

$$\frac{\mathrm{d}}{\mathrm{d}t}\binom{t}{c} = \sum_{i=1}^{c} \frac{(-1)^{i-1}}{i}\binom{t}{c-i} . \tag{8.12}$$

Proof. By the Vandermonde identity $\binom{t+x}{c} = \sum_{i=0}^{c}\binom{x}{i}\binom{t}{c-i}$ (a polynomial identity in t and x: for integers $t, x \geq 0$ count c-element subsets of a disjoint union of an x-set and a t-set by how many elements come from the x-set). Differentiate in x at $x = 0$; the left side gives $\frac{\mathrm{d}}{\mathrm{d}t}\binom{t}{c}$. On the right, $\binom{x}{0} = 1$ has derivative 0, and for $i \geq 1$,

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}\binom{x}{i}\Big|_{x=0} &= \frac{1}{i!}\frac{\mathrm{d}}{\mathrm{d}x}\Big[x(x-1)\cdots(x-i+1)\Big]_{x=0} \\ &= \frac{1}{i!}(-1)(-2)\cdots(-(i-1)) = \frac{(-1)^{i-1}(i-1)!}{i!} = \frac{(-1)^{i-1}}{i} ,\end{aligned}$$

since only the term in which the factor x is differentiated survives at $x = 0$. □

Example 8.26. $c = 2$: $\frac{\mathrm{d}}{\mathrm{d}t}\frac{t^2-t}{2} = t - \frac{1}{2} = \binom{t}{1} - \frac{1}{2}\binom{t}{0}$. $c = 3$: $\frac{\mathrm{d}}{\mathrm{d}t}\binom{t}{3} = \binom{t}{2} - \frac{1}{2}\binom{t}{1} + \frac{1}{3}$; at $t = 5$ both sides are $10 - \frac{5}{2} + \frac{1}{3} = \frac{47}{6}$. Expanding both sides confirms (8.12) for $c \leq 12$. Note the $\frac{1}{3}$: the derivative of an integer-valued polynomial need not be integer valued; this is the first of the two losses.

8.6.5 The proof of Lemma 8.15

We follow [note, Appendix A], which expands only the polynomial part of PQ in the binomial basis and estimates the rest directly, so that no infinite series is differentiated term by term.

Setting up. By Proposition 8.2, $P = \sum_{c\le d} P_c \binom{t}{c}$ with $P_c \in \mathbb{Z}_3$, and the monomial coefficients of P have $v_3 \ge -v_3(d!)$. The series Q is good, so it converges on $|t|_3 < 3$, a disc of radius larger than 1; so do PQ and its derivative, and a power series converging on such a disc is strictly differentiable on $\mathbb{Z}_3$ (Chapter 4). Fix an integer $M > d$ and split $Q = Q_{<M} + R_M$ with $Q_{<M} = \sum_{i<M} q_i t^i$ and $R_M = \sum_{i\ge M} q_i t^i$.

Step 1: the Mahler coefficients of $Q_{<M}$. By (8.10),

$$Q_{<M} = \sum_{i<M} q_i \sum_{m\le i} \left\{ {i \atop m} \right\} m! \binom{t}{m} = \sum_m \gamma_m \binom{t}{m}, \qquad \gamma_m = m! \sum_{m\le i<M} \left\{ {i \atop m} \right\} q_i .$$

Each term of γ_m has valuation $\ge v_3(m!) + 0 + i \ge v_3(m!) + m$, so $v_3(\gamma_m) \ge \psi(m)$, for every M.

Step 2: the Mahler coefficients of $f = PQ_{<M}$. Multiply out, $f = \sum_{a\le d} \sum_b P_a \gamma_b \binom{t}{a}\binom{t}{b}$, and expand each product by (8.11): $f = \sum_c f_c \binom{t}{c}$ with

$$f_c = \sum_{a\le d,\ b} P_a\, \gamma_b \binom{c}{a}\binom{a}{c-b} \qquad (\text{over } a, b \text{ with } \max(a,b) \le c \le a+b) .$$

In each term $b \ge c - a \ge c - d$, and $b \ge 0$, so $b \ge (c-d)^+ := \max(c-d, 0)$. Since $P_a \in \mathbb{Z}_3$, the binomial coefficients are integers, and ψ is increasing, every term has valuation $\ge \psi(b) \ge \psi((c-d)^+)$. Hence

$$v_3(f_c) \ge \psi((c-d)^+) . \tag{8.13}$$

In words: the first $d+1$ Mahler coefficients are just integral, and beyond degree d they become divisible by $3^{\psi(c-d)} \approx 3^{1.5(c-d)}$.

Step 3: one derivative. By (8.12), $f' = \sum_{c'} f'_{c'} \binom{t}{c'}$ with

$$f'_{c'} = \sum_{i\ge 1} \frac{(-1)^{i-1}}{i} f_{c'+i} .$$

The note claims [note, (A.3)]

$$v_3(f'_{c'}) \ge \psi((c'-d)^+) - \log_3 d . \tag{8.14}$$

By (8.13), the term i has valuation $\ge \psi((c'+i-d)^+) - v_3(i)$. We show that this is $\ge \psi((c'-d)^+) - \log_3 d$ in each of three cases.

- *Case 1: $c' \ge d$.* Then $(c'+i-d)^+ = (c'-d)+i$ and, by superadditivity, $\psi(c'-d+i) - v_3(i) \ge \psi(c'-d) + \psi(i) - v_3(i) \ge \psi(c'-d)$, because $\psi(i) \ge i \ge v_3(i)$ (a number $i \ge 1$ is divisible by at most $3^{\log_3 i} \le 3^i$). Since $\log_3 d \ge 0$, the claim follows.
- *Case 2: $c' + i \le d$.* Then $(c'+i-d)^+ = 0 = (c'-d)^+$ and the term has valuation $\ge -v_3(i) \ge -\log_3 i \ge -\log_3 d$, because $3^{v_3(i)}$ divides i, so $3^{v_3(i)} \le i \le d$.
- *Case 3: $c' < d < c'+i$.* Put $e = c'+i-d \ge 1$; again $(c'-d)^+ = 0$. Since $i = d+e-c' \le d+e$,

$$v_3(i) \le \log_3(d+e) \le \log_3\big(d(1+e)\big) = \log_3 d + \log_3(1+e) \le \log_3 d + \psi(e) ,$$

using $d + e \le d + de$ (as $d \ge 1$) and $\log_3(1+e) \le e \le \psi(e)$. So $\psi(e) - v_3(i) \ge -\log_3 d$.

The ultrametric inequality turns the bound on every term into (8.14).

Step 4: the integral. f' is a polynomial, so by (V2), $\int_{\mathbb{Z}_3} \binom{t}{c} \mathrm{d}t = \frac{(-1)^c}{c+1}$ (Chapter 4), and linearity,

$$\int_{\mathbb{Z}_3} f'(t)\, \mathrm{d}t = \sum_{c'} f'_{c'} \frac{(-1)^{c'}}{c'+1} ,$$

a finite sum. We claim $v_3(c'+1) \le \log_3(d+1)+\psi((c'-d)^+)$. For $c' \le d$: $v_3(c'+1) \le \log_3(c'+1) \le \log_3(d+1)$. For $c' = d+e$, $e \ge 1$: $v_3(c'+1) \le \log_3(d+1+e) \le \log_3(d+1)+\log_3(1+e) \le \log_3(d+1)+\psi(e)$, by the same inequalities as in Case 3. With (8.14), the term c' has valuation $\ge \psi((c'-d)^+) - \log_3 d - \log_3(d+1) - \psi((c'-d)^+) = -\log_3 d - \log_3(d+1)$, and so has the sum:

$$v_3 \int_{\mathbb{Z}_3} (PQ_{<M})' \mathrm{d}t \;\ge\; -\log_3 d - \log_3(d+1) \qquad \text{for every } M > d\ .$$

Step 5: the remainder. $(PR_M)' = P'R_M + PR'_M = \sum_m e_m t^m$. The monomial coefficients of P have $v_3 \ge -v_3(d!)$, and so have those of P' (multiplying by integers does not lower valuations). The coefficient of t^m in R_M is q_m (zero for $m < M$), of valuation $\ge m$ and $\ge M$; in R'_M it is $(m+1)q_{m+1}$ (zero for $m < M-1$), of valuation $\ge m+1 \ge M$. So both have coefficient valuations $\ge \max(M,m)$ at t^m. In a product with P or P' (degree $\le d$), the coefficient of t^m is a sum of products of a coefficient of $P^{(\prime)}$ at t^a, $a \le d$, and one of $R_M^{(\prime)}$ at t^{m-a}, so

$$v_3(e_m) \ge -v_3(d!) + \max(M, m-d)\ .$$

This series converges on $|t|_3 < 3$, its value at 0 and its Lipschitz constant on $\mathbb{Z}_3$ are at most $\max_m |e_m|_3$ (since $|x^m - y^m|_3 \le |x-y|_3$ on $\mathbb{Z}_3$, Chapter 2), and (V3) gives

$$v_3 \int_{\mathbb{Z}_3} (PR_M)' \mathrm{d}t \;\ge\; M - v_3(d!) - 1\ .$$

Step 6: the limit. By linearity $\int_{\mathbb{Z}_3}(PQ)' = \int_{\mathbb{Z}_3}(PQ_{<M})' + \int_{\mathbb{Z}_3}(PR_M)'$. The left side does not depend on M; the first term on the right has $v_3 \ge -\log_3 d - \log_3(d+1)$ for every M, and the second has $v_3 \ge M - v_3(d!) - 1 \to \infty$. Choosing M with $M - v_3(d!) - 1 > -\log_3 d - \log_3(d+1)$, the ultrametric inequality gives (8.9). □

What just happened. Write the integrand in the binomial basis, where integrality is visible. The polynomial P gives integral coefficients up to degree d; the good series Q gives coefficients that grow in divisibility like $\psi(c-d) \approx 1.5(c-d)$ beyond degree d (Steps 1–2, using Stirling numbers and the product identity). The derivative divides by i, the integral by $c+1$; up to degree d these divisions cost at most $\log_3 d$ and $\log_3(d+1)$, and beyond degree d they are paid for by the extra divisibility, through $\log_3(1+e) \le \psi(e)$ (Steps 3–4). The tail of Q is handled by (V3) and vanishes in the limit (Steps 5–6).

8.6.6 The proof in numbers

Example 8.27 (anatomy of Lemma 8.15)**.** Take $n = 1$, $r = 1$, $B = F_3^2$, so $P(t) = F_3(t+\frac{1}{3})^2(t+1)^3$, of degree $d = 9$, with Mahler coefficients $P_0, \dots, P_9 = 0, 512, 131276, 3291036, 26944152, 102003960, 204275520, 224033040, 127370880, 29393280$, all integers as Proposition 8.2 requires. Take $Q = Q_1$ of Example 8.11, truncated at $M = 60$ terms, with its coefficients kept as 3-adic integers modulo 3^{90}; so the coefficients of $f = PQ_{<60}$ are exact to $v_3 \ge 90$, and the truncation changes the integral by $v_3 \ge M - v_3(9!) - 1 = 55$. For the γ_m of Step 1, $v_3(\gamma_m) - \psi(m)$ for $m = 0, \dots, 20$ is $0, 2, 1, 1, 1, 2, 0, 2, 2, 0, 2, 1, 1, 1, 3, 0, 3, 3, 1, 4, 2$: never negative, and 0 at $m = 0, 6, 9, 15$. The Mahler coefficients of f and f':

c	$v_3(f_c)$	$\psi((c-d)^+)$	$v_3(f_c')$	$\psi((c-d)^+)-\log_3 d$	$v_3\big(f_c'\frac{(-1)^c}{c+1}\big)$
0	∞	0	∞	-2	∞
1	0	0	0	-2	0
2	0	0	0	-2	-1
3	1	0	2	-2	2
4	1	0	1	-2	1
5	1	0	4	-2	3
6	5	0	4	-2	4
8	6	0	8	-2	6
10	12	1	10	-1	10
11	10	2	13	0	12
12	13	4	13	2	13
15	16	8	17	6	17
20	23	15	26	13	25
25	31	22	35	20	35

(selected rows from $c \le 25$). Over all c, $v_3(f_c) - \psi((c-d)^+) \ge 0$ (the bound (8.13) is attained) and $v_3(f_c') - [\psi((c-d)^+) - \log_3 d] \ge 2$. The integral has $v_3 = -1$, from the term $c = 2$ (division by 3), against the bound $-\log_3 9 - \log_3 10 = -4.10$. Computing the integral in two ways, by the Mahler route above and by expanding f' in monomials and integrating with $\int_{\mathbb{Z}_3} t^m \mathrm{d}t = B_m$ (V2), gives identical results.

Example 8.28 (Lemma 8.15 on all Hankel entries, and a cross-check of (8.8))**.** For $n = 1$ with all pairs $i \le j < 4$, and $n = 3$ with all pairs $i \le j < 10$, and $r = 1, 2$, form $P_r(t) = F_iF_j(t + \frac{r}{3})\binom{t+n}{n}^3$ (degree $d = i + j + 3n$) and compute $I_r = \int_{\mathbb{Z}_3}(P_rQ_{r,<60})'\mathrm{d}t$ by the Mahler route. The smallest value of $v_3(I_r) + \log_3 d + \log_3(d+1)$ is 2.26 for $n = 1$ (at $i = j = 0$, $r = 1$: $d = 3$, $v_3(I_1) = 0$) and 2.74 for $n = 3$ (at $i = 0$, $j = 4$, $r = 1$: $d = 13$, $v_3(I_1) = -2$). So (8.9) holds in all tested cases with a margin of at least 2.2 trits. Then compare $3^{9n+3}(n!)^3(I_1 + I_2)$ with $L(F_iF_j)$ computed by the purity lemma (local constants and $\zeta_3(5)$, Chapter 5). The two agree to at least 59 ($n = 1$) and 53 ($n = 3$) 3-adic digits beyond the valuation of $L(F_iF_j)$ itself (the agreement is limited by the truncation of Q_r). The second computation never uses $\zeta_3(5)$, harmonic sums or partial fractions; it uses only (8.8), the Mahler expansion and (V2). So the two routes confirm each other, and with them the factorization and the purity lemma at these n.

8.7 The proof of [note, Theorem 3.5]

Theorem 8.29 (3-adic gain; [note, Theorem 3.5])**.** *For $K \le 3n + 1$, with $\kappa = K/n$,*

$$v_3(\Delta_K(\zeta_3(5)))\log_2 3 \;\ge\; G(\kappa)\,n^2 - O(n\log n)\;, \qquad G(\kappa) = \left(10.5\,\kappa - \frac{\kappa^2}{4}\right)\log_2 3\;.$$

The note's proof, step by step. Put $A_3 = 9n + 3 + 3v_3(n!)$ and $d_K = 2K - 2 + 3n$.

Step 1: reduce to one entry. By [note, (2.26)], $\Delta_K(\zeta_3(5)) = \det\big[L(y^{i+j})\big]_{i,j<K}$ (here $K \le 3n + 1$ is used). Apply Lemma 8.4 with $\Lambda' = L$. It suffices to show [note, (4.8)]

$$v_3L(B) \;\ge\; A_3 - \log_3 d_K - \log_3(d_K + 1) \tag{8.15}$$

for every $B \in \mathrm{Int}(S)$ of degree at most $2K - 2$: each F_iF_j with $i, j < K$ is such a B (a product of two elements of $\mathrm{Int}(S)$, of degree $i + j \le 2K - 2$).

Step 2: one class at a time. Fix r. By (8.8),

$$(BW)(t + \tfrac{r}{3}) = 3^{9n+3}(n!)^3P(t)\,Q_r(t)\;, \qquad P(t) = B(t + \tfrac{r}{3})\binom{t+n}{n}^3\;.$$

P maps $\mathbb{Z}_3$ into $\mathbb{Z}_3$: $t+\frac{r}{3} \in S$ for $t \in \mathbb{Z}_3$ and $B \in \mathrm{Int}(S)$, and $\binom{t+n}{n} \in \mathbb{Z}_3$. Its degree is $\le 2K-2+3n = d_K$, and $d_K \ge 3$. Q_r is good. The derivative in L is the derivative of BW at the point $t+\frac{r}{3}$, which is the t-derivative of $(BW)(t+\frac{r}{3})$ (chain rule, the inner derivative being 1). So

$$\int_{\mathbb{Z}_3} (BW)'(t+\tfrac{r}{3})\mathrm{d}t = 3^{9n+3}(n!)^3 \int_{\mathbb{Z}_3} (PQ_r)'(t)\,\mathrm{d}t\ ,$$

and Lemma 8.15 with $d = d_K$ (it allows $\deg P \le d$) bounds its valuation below by $9n+3+3v_3(n!) - \log_3 d_K - \log_3(d_K+1)$.

Step 3: sum over r. $L(B)$ is the sum of the two terms $r = 1, 2$, and by the ultrametric inequality its valuation is at least the smaller of the two bounds, which are equal. This proves (8.15), and with (8.5), [note, (4.9)]

$$v_3\Delta_K(\zeta_3(5)) \ \ge\ 2\sum_{i<K}\nu_i + K(A_3 - \log_3 d_K - \log_3(d_K+1))\ . \tag{8.16}$$

Step 4: asymptotics. Each of the three terms, with $K = \kappa n \le 3n+1$:

- By Legendre's formula $3v_3(n!) = \frac{3}{2}(n - s_3(n)) = 1.5n - O(\log n)$, so $A_3 = 10.5n + 3 - \frac{3}{2}s_3(n)$ and $KA_3 = 10.5\kappa n^2 - O(n\log n)$ (as $K \le 3n+1$ and $s_3(n) \le 2\log_3(3n)$).
- By (8.6), $2\sum_{i<K}\nu_i = -\frac{K^2}{4} - O(K\log K) = -\frac{\kappa^2}{4}n^2 - O(n\log n)$.
- $d_K = 2K - 2 + 3n \le 9n$, so $K\log_3\left(d_K(d_K+1)\right) \le (3n+1)\cdot 2\log_3(9n+1) = O(n\log n)$.

Together, $v_3\Delta_K(\zeta_3(5)) \ge (10.5\kappa - \frac{\kappa^2}{4})n^2 - O(n\log n)$, in trits; multiplying by $\log_2 3$ converts trits to bits (Chapter 1) and gives the theorem. All implied constants are absolute, uniformly in $K \le 3n+1$. □

What just happened. The gain is K rows times $A_3 \approx 10.5n$ trits per entry, minus the cost $K^2/4$ of the change to an integer-valued basis, minus $O(\log n)$ per row for the derivative and the integral. The $10.5n$ is $4(3n+1)$ from the poles at distance 3 from S, minus $3n+1$ for the Pochhammer symbol and the linear factor that are large on S, plus $1.5n$ from $(n!)^3$.

The arithmetic of $G(\kappa)$. In trits per n^2 the main term is $10.5\kappa - \frac{\kappa^2}{4}$: 27.44 at $\kappa = 2.8$ and 29.25 at $\kappa = 3$. In bits, $G(2.8) = 27.44\log_2 3 = 43.4914$ and $G(3) = 46.3602$, the values used in [note, Table 1] (rounded down there to 43.49 for I_1; on $I_5 = [2.96, 3]$ the note uses $G(2.96) = 45.7889$, printed as 45.78). G is increasing on $[2.8, 3]$, since its derivative $(10.5 - \frac{\kappa}{2})\log_2 3$ is positive for $\kappa < 21$; this is why the note may evaluate it at the left end of each interval. Of the 43.49 bits at $\kappa = 2.8$, the change of basis takes $\frac{2.8^2}{4}\log_2 3 = 3.11$ bits (from 46.60). The optimal basis matters more than this small number suggests, see the intuition box in Section 8.4.

8.8 The bound against the true valuation

The theorem is asymptotic. To see what its explicit form (8.16) says at small n, we compute the actual $v_3\Delta_K(\zeta_3(5))$ for $n = 1$ ($K \le 4 = 3n+1$) and $n = 3$ ($K \le 10 = 3n+1$). We compute the matrix $[L(F_iF_j)]$ by purity with $\zeta_3(5)$ to 124 digits, take its determinant exactly, and use $v_3\Delta_K = v_3\det[L(F_iF_j)] + 2\sum_{i<K}\nu_i$. This precision is sufficient: lengthening the truncation of the series from 125 to 200 terms changes $\det[L(F_iF_j)]$, for every K in the table, by a term whose valuation exceeds that of the determinant by at least 55 (the margin is smallest for $n = 3$, $K = 9, 10$; for $K = 10$ the determinant has valuation 311 and the change 366). For $n = 1$ this reproduces $12, 22, 31, 38$ of Chapter 6.

Example 8.30 (bound and truth)**.** Columns: $\min v_3 L(F_i F_j)$ over $i, j < K$; the cost $2\sum \nu_i$; the bound (8.5) with the actual minimum; d_K; the explicit bound (8.16); the main term $(10.5\kappa - \frac{\kappa^2}{4})n^2$ of the theorem (in trits, without the $O(n \log n)$); the actual valuation.

n	K	$\min v_3 L(F_i F_j)$	$2\sum \nu_i$	(8.5)	d_K	(8.16)	main term	actual
1	1	12	0	12	3	9.74	10.25	12
1	2	12	−2	22	5	15.81	20.00	22
1	3	11	−4	29	7	21.01	29.25	31
1	4	11	−8	36	9	23.62	38.00	38
3	1	32	0	32	9	28.90	31.25	32
3	2	32	−2	62	11	55.11	62.00	62
3	3	31	−4	89	13	80.79	92.25	91
3	4	31	−8	116	15	104.05	122.00	118
3	5	31	−12	143	17	126.95	151.25	144
3	6	31	−18	168	19	147.56	180.00	168
3	7	31	−22	195	21	169.91	208.25	196
3	8	31	−28	220	23	190.03	236.00	222
3	9	30	−34	236	25	209.94	263.25	247
3	10	30	−42	258	27	227.67	290.00	269

For $n = 3$ the per-entry budget is $A_3 = 33$, and the entries $v_3 L(F_i F_j)$, $i, j < 10$, range from 30 to 37; the analytic step allows a loss of $\log_3 d_K + \log_3(d_K + 1) \le 6.03$, and the actual loss is at most 3.

What the table shows, in the tested cases only:

- The explicit bound (8.16) holds, as it must if the note's argument is right, and it is not weak: it is positive and between 62% ($n = 1$, $K = 4$) and 90% ($n = 3$, $K = 1$) of the true valuation. (One might expect a lower bound of this kind to be negative at small n; it is not, because the per-entry budget A_3 is already large at $n = 1$ and the cost $2\sum \nu_i$ is small for small K.)
- Most of the gap comes from the analytic step: the true entries lose 0 to 3 trits relative to A_3, while the bound allows $\log_3 d_K + \log_3(d_K + 1)$, which is 2.26 to 6.03 here. The step (8.5) with the true minimum is tight to within 2 for $n = 1$ and within 11 for $n = 3$.
- The main term $(10.5\kappa - \frac{\kappa^2}{4})n^2$ alone is *not* a lower bound: for $n = 3$ and $K \ge 3$ it exceeds the actual valuation (e.g. $263.25 > 247$ at $K = 9$, i.e. $\kappa = 3$). That the two agree at $n = 1$, $K = 4$ ($38 = 38$) is a coincidence of small numbers. The $-O(n \log n)$ in the theorem is a real correction at small n, and it is what the $\log_3$ terms and the digit sums in (8.7) produce.

None of this bears on irrationality: the criterion compares n^2 coefficients and needs $n \to \infty$ (Chapter 7).

Check yourself 8.31. Why may the note use $\min_{i,j} v_3 L(F_i F_j)$ for *all* entries, even though the entries of high degree have a larger d in Lemma 8.15?

Answer. It applies Lemma 8.15 with the single value $d = d_K = 2K - 2 + 3n$, the largest degree that occurs, which the lemma allows since it only asks $\deg P \le d$; the bound $-\log_3 d - \log_3(d+1)$ decreases in d, so this is a common lower bound for all entries.

Check yourself 8.32. Show that $F_2(y) = 3y^2 - 3y + \frac{2}{3}$ is the best possible in degree 2 in the following sense: no polynomial $B \in \mathrm{Int}(S)$ of degree 2 has a leading coefficient of valuation ≤ 0.

Answer. Interpolate $B = \ell y^2 + \dots$ at the three points $a_0 = \frac{1}{3}$, $a_1 = \frac{2}{3}$, $a_2 = \frac{4}{3}$ of S (Lagrange): the leading coefficient of the interpolating quadratic is $\ell = \sum_j B(a_j)/\prod_{l\neq j}(a_j - a_l)$. The denominators are $(-\frac{1}{3})(-1) = \frac{1}{3}$, $(\frac{1}{3})(-\frac{2}{3}) = -\frac{2}{9}$ and $(1)(\frac{2}{3}) = \frac{2}{3}$, so $\ell = 3B(a_0) - \frac{9}{2}B(a_1) + \frac{3}{2}B(a_2)$. All three values are in $\mathbb{Z}_3$, so every term is divisible by 3 and $v_3(\ell) \geq 1$. F_2 attains this: $F_2(a_0) = F_2(a_1) = 0$, $F_2(a_2) = 2$, $\ell = \frac{3}{2}\cdot 2 = 3$. (This is the computation behind $\phi_{\mathbb{Z}_3^\times}(2) = 1$ in Example 8.9, in the variable $x = 3y$: the points $1, 2, 4$ are the start of the 3-ordering.)

Summary of the chapter

The 3-adic gain [note, Theorem 3.5] is proved in the note in two halves. Algebraically, the Hankel determinant is rewritten in the basis $F_{2q} = 3^q q!\binom{y-1/3}{q}\binom{y-2/3}{q}$, $F_{2q+1} = 3yF_{2q}$ [note, Lemma 4.1], whose elements take values in $\mathbb{Z}_3$ on both classes $\frac{1}{3} + \mathbb{Z}_3$ and $\frac{2}{3} + \mathbb{Z}_3$ of the integration set S (one binomial factor is integral on each class, and $3^q q!$ turns the other into a product of units). The triangular change of basis multiplies the determinant by $(\det T)^2$, which gives [note, (4.3)]: $v_3\Delta_K \geq 2\sum \nu_i + K \min v_3 L(F_iF_j)$, with $\nu_i = v_3(q!) - q - e$ and the exact cost $2\sum_{i<K}\nu_i = -\frac{K^2}{4} - \frac{K}{2} - 2\sum_{q<K/2} s_3(q)$ for even K, that is $-\frac{K^2}{4} + O(K\log K)$ [note, (4.4)]; at $p = 2$ the analogous term is a gain of about K^2 bits. By a theorem of Bhargava [5] and the argument of Fact 8.8 and the paragraph after Example 8.9 (with the example for $i \leq 30$), no basis of $\mathrm{Int}(S)$ has a smaller cost, and the naive basis $(3y)^i$ would cost so much more that the note's margins would become negative. Analytically, on S the weight factors as $W(t + \frac{r}{3}) = 3^{9n+3}(n!)^3\binom{t+n}{n}^3 Q_r(t)$ [note, (4.5)] with a unit-valued series Q_r whose t^i-coefficient has $v_3 \geq i$; the derivative and the Volkenborn integral then cost only $\log_3 d + \log_3(d+1)$ [note, Lemma 4.6], proved by the Mahler expansion, Stirling numbers, the superadditive function $\psi(m) = m + v_3(m!)$, the product identity [note, (A.2)] and the three-case bound [note, (A.3)]. So each entry has $v_3 \geq A_3 - O(\log n)$ with $A_3 = 9n+3+3v_3(n!) \approx 10.5n$, and $v_3\Delta_K(\zeta_3(5)) \geq (10.5\kappa - \frac{\kappa^2}{4})n^2 - O(n\log n)$ trits. Numerically (for $n = 1, 3$) the factorization, the bound $v_3(q_i) \geq i$, [note, Lemma 4.6] on every Hankel entry and the explicit bound [note, (4.9)] all hold, and $L(F_iF_j)$ computed through [note, (4.5)] agrees with the purity lemma to more than 50 digits.

Carried forward: the value $G(\kappa) = (10.5\kappa - \frac{\kappa^2}{4})\log_2 3$, with $G(2.8) = 43.49$ and $G(3) = 46.36$ bits per n^2, enters the final comparison of Chapter 7 and the review in Chapter 15; the binomial-basis techniques (Mahler coefficients, ψ) are not used again in the main proof.

Chapter 9

The Heine expansion

Where we are. Three of the four estimates of the proof are about the rational coefficients of the Hankel polynomial $\Delta_K(X) = \det\big[\Lambda(y^{i+j})\big]_{i,j<K}$ of Chapter 6: their real size (Chapter 10), their denominators (Chapters 11 to 13) and, indirectly, their non-vanishing (Chapter 14). A determinant of a $K \times K$ matrix whose entries are themselves sums over $3n+1$ nodes is hard to estimate as it stands. This chapter rewrites it as a sum of products, the *Heine expansion* [note, Proposition 5.1]: one term for each way of distributing K "particles" over the nodes with at most four per node, each term a product of an integer that depends only on the distances between the nodes and of one small determinant per node built from that node's local constants. We cover [note, Section 5.1] up to the paragraph after [note, Proposition 5.1], and [note, Appendix B] from its start through the proof of [note, Proposition 5.1]: Andreief's identity [note, Lemma B.1] and Steps 1–6 of the proof. From Chapter 5 we need the nodes $k \in \mathcal{N} = \{-n, \dots, 2n\}$, the leading coefficients h_k and the local constants $c_{k,a}$; from Chapter 6 the node functionals L_k, the functional $\Lambda = \sum_k L_k$, the node matrices C_k, Heine's formula with its Coulomb-gas reading, and the rule "at most four rows per node".

9.1 The Vandermonde determinant

Heine's formula for a Hankel determinant contains the product $\prod_{i<i'}(y_{i'} - y_i)^2$. Its square root is a determinant, and this is what makes the formula provable by pure algebra.

Definition 9.1 (Vandermonde)**.** For variables $w_1, \dots, w_s$ put

$$V(w) = V(w_1, \dots, w_s) = \prod_{1 \le i < i' \le s} (w_{i'} - w_i)\ , \qquad V() = V(w_1) = 1\ .$$

Proposition 9.2 (Vandermonde's determinant)**.** $V(w) = \det\big[w_i^b\big]_{1 \le i \le s,\ 0 \le b < s}$, *the determinant of the matrix whose row i is* $(1, w_i, w_i^2, \dots, w_i^{s-1})$.

Proof. Call the determinant $D(w)$. It is a polynomial in $w_1, \dots, w_s$. If $w_i = w_{i'}$ for some $i \neq i'$, two rows coincide and $D = 0$; so, as a polynomial in $w_{i'}$, D has the root w_i and is divisible by $w_{i'} - w_i$. These $\binom{s}{2}$ linear factors are pairwise coprime, so their product V divides D. Every term $\pm\prod_i w_i^{\sigma(i)}$ of the Leibniz expansion of D has total degree $0 + 1 + \cdots + (s-1) = \binom{s}{2}$, the degree of V; hence $D = c\,V$ for a constant c. The monomial $w_2 w_3^2 \cdots w_s^{s-1}$ (the diagonal of the matrix) has coefficient 1 in D, and in V it arises only by choosing $w_{i'}$ from every factor $(w_{i'} - w_i)$, again with coefficient 1. So $c = 1$. □

Example 9.3. For $s = 3$ and $w = (1, 2, 4)$:

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 16 \end{pmatrix} = 6 = (2-1)(4-1)(4-2) \ .$$

Expanding the symbolic 3×3 determinant and factoring gives $-(w_1 - w_2)(w_1 - w_3)(w_2 - w_3) = (w_2 - w_1)(w_3 - w_1)(w_3 - w_2)$.

Intuition. V vanishes exactly when two of the points collide, and $|V|$ grows with the spread of the points: it is the volume spanned by the vectors $(1, w_i, \dots, w_i^{s-1})$. Exchanging two variables exchanges two rows, so V is *antisymmetric*: it changes sign under every transposition of the variables. Its square $V^2 = \prod_{i<i'}(w_{i'} - w_i)^2$ is *symmetric*: it does not change under any permutation. In the Coulomb-gas language of Chapter 6, $V^2 = \exp\left(2\sum_{i<i'} \log|w_{i'} - w_i|\right)$ is the Boltzmann factor of the mutual repulsion of s unit charges.

9.2 Tensor powers of a functional

Heine's formula integrates V^2 against $\mu \otimes \cdots \otimes \mu$. The note's functionals are not integrals against measures on $\mathbb{R}$, so it needs an algebraic replacement for the product measure. It works over the ring $\mathbb{Q}[X]$ (polynomials in the symbol X that stands for $\zeta_3(5)$, Chapter 6); for the examples one may read $\mathbb{Q}$ instead.

Definition 9.4 (tensor power; [note, Appendix B], first paragraph)**.** Let $\Lambda' : \mathbb{Q}[X][w] \to \mathbb{Q}[X]$ be a $\mathbb{Q}[X]$-linear map (a "functional" on polynomials in one variable w), and $s \geq 1$. Its *s-th tensor power* is the $\mathbb{Q}[X]$-linear map $\Lambda'^{\otimes s} : \mathbb{Q}[X][w_1, \dots, w_s] \to \mathbb{Q}[X]$ defined on monomials by

$$\Lambda'^{\otimes s}\left(w_1^{e_1} w_2^{e_2} \cdots w_s^{e_s}\right) = \Lambda'(w^{e_1})\,\Lambda'(w^{e_2}) \cdots \Lambda'(w^{e_s})$$

and extended to all polynomials by linearity.

A functional is determined by its moments $m_j = \Lambda'(w^j)$, and then $\Lambda'^{\otimes s}$ replaces each w_i^e by m_e, separately in each variable. Two consequences, both immediate from the definition on monomials and linearity, are used below. First, if $F_1, \dots, F_s$ are polynomials in one variable, then

$$\Lambda'^{\otimes s}\left(F_1(w_1) F_2(w_2) \cdots F_s(w_s)\right) = \Lambda'(F_1) \cdots \Lambda'(F_s) \ , \tag{9.1}$$

because expanding each F_i into monomials and multiplying out gives a sum of monomials $\prod_i w_i^{e_i}$, on each of which the map is the product. Second, the same argument with groups of variables in place of single variables: if the variables are split into disjoint groups and $G_1, G_2, \dots$ are polynomials each in the variables of one group, then a "mixed" tensor product $\Lambda_1 \otimes \Lambda_2 \otimes \cdots$ (a possibly different functional for each variable, defined on monomials in the same way) maps $G_1 G_2 \cdots$ to the product of its values on the G_j. Both say: *on functions of separate variables the tensor power factorizes.*

Example 9.5 (a product measure)**.** Let $\Lambda'(F) = \int_0^1 F(w)\mathrm{d}w$, with moments $m_j = \frac{1}{j+1}$. Then

$$\Lambda'^{\otimes 2}\left(w_1^2 w_2 + 3 w_1 w_2^3\right) = m_2 m_1 + 3 m_1 m_3 = \frac{1}{3}\cdot\frac{1}{2} + 3\cdot\frac{1}{2}\cdot\frac{1}{4} = \frac{13}{24} \ ,$$

and indeed $\int_0^1\int_0^1 (w_1^2 w_2 + 3 w_1 w_2^3)\mathrm{d}w_1\mathrm{d}w_2 = \frac{13}{24}$. For an integral the tensor power is the multiple integral against the product measure (Fubini), which is the reason for the definition.

Intuition. $\Lambda'^{\otimes s}$ treats the s variables as *independent* copies, each "averaged" with Λ', as for independent random variables; but nothing requires Λ' to be positive or to be an integral. For the Volkenborn integral (moments B_j, Chapters 4 and 6) or for the node functional "take a combination of the first four Taylor coefficients at a point" the definition works in the same way. This is the generality the note needs.

9.3 Andreief's identity

9.3.1 The case $s = 2$ by hand

Take two pairs of polynomials f_0, f_1 and g_0, g_1 in one variable, and form the two 2×2 determinants in the variables w_1, w_2:

$$\det \begin{pmatrix} f_0(w_1) & f_1(w_1) \\ f_0(w_2) & f_1(w_2) \end{pmatrix} = f_0(w_1)f_1(w_2) - f_1(w_1)f_0(w_2) \ ,$$

and the same with g. Their product has four terms:

$$\begin{aligned} &f_0(w_1)g_0(w_1)\, f_1(w_2)g_1(w_2) - f_0(w_1)g_1(w_1)\, f_1(w_2)g_0(w_2) \\ &- f_1(w_1)g_0(w_1)\, f_0(w_2)g_1(w_2) + f_1(w_1)g_1(w_1)\, f_0(w_2)g_0(w_2) \ . \end{aligned}$$

Each term is a function of w_1 times a function of w_2, so by (9.1) $\Lambda'^{\otimes 2}$ maps it to the product of the two values of Λ'. Writing $A_{bb'} = \Lambda'(f_b g_{b'})$:

$$\Lambda'^{\otimes 2}(\cdots) = A_{00}A_{11} - A_{01}A_{10} - A_{10}A_{01} + A_{11}A_{00} = 2\,(A_{00}A_{11} - A_{01}A_{10}) = 2\det \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} .$$

The first and the last term give the same product, and so do the two middle ones: the two ways of assigning the roles "row 0" and "row 1" to the variables w_1, w_2 contribute equally. This is the factor $s! = 2$.

Example 9.6 (the Volkenborn integral)**.** Let Λ' have the moments $m_j = B_j$ (the Volkenborn integral, $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$). With $f = (1, w)$ and $g = (1, w^2)$ the left side is $\Lambda'^{\otimes 2}((w_2 - w_1)(w_2^2 - w_1^2)) = B_0B_3 - B_2B_1 - B_1B_2 + B_3B_0 = \frac{1}{6}$, and the right side is $2\det\left(\begin{smallmatrix} B_0 & B_2 \\ B_1 & B_3 \end{smallmatrix}\right) = 2\cdot\frac{1}{12} = \frac{1}{6}$. With $f = g = (1, w)$: $\Lambda'^{\otimes 2}((w_2 - w_1)^2) = 2(B_0B_2 - B_1^2) = -\frac{1}{6}$, which is $2\det H_2$ for the Hankel determinant $\det H_2 = -\frac{1}{12}$ of Chapter 6 (the negative "variance"). Nothing in the identity cares about signs.

9.3.2 The general statement and proof

Lemma 9.7 (Andreief; [note, Lemma B.1])**.** *Let $\Lambda' : \mathbb{Q}[X][w] \to \mathbb{Q}[X]$ be $\mathbb{Q}[X]$-linear and $f_0, \dots, f_{s-1}, g_0, \dots, g_{s-1} \in \mathbb{Q}[X][w]$. Then [note, (B.2)]*

$$\Lambda'^{\otimes s}\Big(\det\left[f_b(w_i)\right]_{i,b} \, \det\left[g_{b'}(w_i)\right]_{i,b'} \Big) = s! \, \det\left[\Lambda'(f_b g_{b'})\right]_{0 \le b,b' < s} \ , \tag{9.2}$$

where i runs over $1, \dots, s$ (rows) and b, b' over $0, \dots, s-1$ (columns).

The identity is classical: it goes back to C. Andréief in the 1880s (a historical account is P. J. Forrester, *Meet Andréief, Bordeaux 1886, and Andreev, Kharkov 1882–83*), usually stated for integrals; the note states it for arbitrary linear functionals, where the same proof works.

Proof. We follow the note's three sentences and spell out the bookkeeping. Index the rows by $i \in \{1, \dots, s\}$ and the columns by $b \in \{0, \dots, s-1\}$. A term of the Leibniz expansion of $\det[f_b(w_i)]$ chooses in every row i one column $\sigma(i)$, with different columns for different rows; so σ is a bijection $\{1, \dots, s\} \to \{0, \dots, s-1\}$, and its sign $\operatorname{sgn}(\sigma)$ is the sign of the permutation $i \mapsto \sigma(i) + 1$ of $\{1, \dots, s\}$. Thus

$$\det[f_b(w_i)] = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{i=1}^{s} f_{\sigma(i)}(w_i) \ , \qquad \det[g_{b'}(w_i)] = \sum_{\tau} \operatorname{sgn}(\tau) \prod_{i=1}^{s} g_{\tau(i)}(w_i) \ .$$

Step (i): multiply. The product of the two determinants is the double sum

$$\sum_{\sigma,\tau} \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau) \prod_{i=1}^{s} \Big(f_{\sigma(i)}(w_i)\, g_{\tau(i)}(w_i) \Big) \ ,$$

in which every summand is a product of s factors, the i-th depending on w_i only.

Step (ii): apply $\Lambda'^{\otimes s}$. By linearity and (9.1) the summand (σ, τ) is mapped to $\operatorname{sgn}(\sigma) \operatorname{sgn}(\tau) \prod_{i=1}^{s} \Lambda'(f_{\sigma(i)} g_{\tau(i)})$.

Step (iii): relabel the product by columns. As i runs over $1, \dots, s$, $b = \sigma(i)$ runs over $0, \dots, s-1$, each value once, and $i = \sigma^{-1}(b)$. So

$$\prod_{i=1}^{s} \Lambda'(f_{\sigma(i)} g_{\tau(i)}) = \prod_{b=0}^{s-1} \Lambda'(f_b g_{\tau(\sigma^{-1}(b))}) = \prod_{b=0}^{s-1} A_{b,\pi(b)} \ , \qquad A_{bb'} = \Lambda'(f_b g_{b'}) \ , \quad \pi = \tau\sigma^{-1} \ .$$

Here $\pi = \tau \circ \sigma^{-1}$ maps $\{0, \dots, s-1\}$ to itself bijectively (first σ^{-1} to a row, then τ to a column of the second matrix): it is a permutation. Signs multiply under composition, so $\operatorname{sgn}(\tau) = \operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi) \operatorname{sgn}(\sigma)$, and the coefficient is $\operatorname{sgn}(\sigma) \operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma)^2 \operatorname{sgn}(\pi) = \operatorname{sgn}(\pi)$.

Step (iv): sum over τ for fixed σ. For fixed σ, the map $\tau \mapsto \pi = \tau\sigma^{-1}$ is a bijection from the bijections τ onto the permutations π (its inverse is $\pi \mapsto \pi\sigma$). Hence

$$\sum_{\tau} \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau) \prod_{b} A_{b,\tau\sigma^{-1}(b)} = \sum_{\pi} \operatorname{sgn}(\pi) \prod_{b} A_{b,\pi(b)} = \det A \ ,$$

the Leibniz formula for $\det A$.

Step (v): sum over σ. The result of Step (iv) does not depend on σ, and there are $s!$ bijections σ. So the total is $s! \det A$. □

What just happened. Multiply the two Leibniz expansions; every term is a product of one-variable factors, so the tensor power turns it into a product of numbers $\Lambda'(f_b g_{b'})$; the pairs (σ, τ) with the same "relative permutation" $\tau\sigma^{-1}$ give the same product with the same sign; summing over that relative permutation gives one determinant, and the $s!$ choices of σ (which variable plays which row) give the factor $s!$.

An example with $s = 3$: let Λ' be the Volkenborn integral (moments B_j, so $B_4 = -\frac{1}{30}$, $B_5 = 0$), $f = (1, w, w^2)$ and $g = (1 + w,\ w^2,\ w^3 - w)$. Then $\det[f_b(w_i)] = V(w)$ and $\det[g_{b'}(w_i)] = V(w)\,(1 + e_2 + e_3)$ with $e_2 = w_1w_2 + w_1w_3 + w_2w_3$, $e_3 = w_1w_2w_3$, and in exact arithmetic both sides of (9.2) equal $-\frac{1}{50}$.

9.4 Heine's formula

Take $f_b = g_b = w^b$ in Lemma 9.7. Then both determinants are $\det\left[w_i^b\right] = V(w)$ (Proposition 9.2), and $\Lambda'(f_b g_{b'}) = \Lambda'(w^{b+b'})$ is the Hankel matrix of Λ'. So:

Corollary 9.8 (Heine's formula for any functional; [note, Lemma B.1], last sentence)**.** $\det\left[\Lambda'(w^{b+b'})\right]_{0\le b,b'<s} = \frac{1}{s!}\,\Lambda'^{\otimes s}(V(w)^2)$.

For $\Lambda' = \int\cdot\,\mathrm{d}\mu$ this is Chapter 6's Heine formula (Szegő [32], Ch. II): the tensor power is the s-fold integral. The examples there ($\mathrm{d}x$ on $[0,1]$, $s=2,3$) are instances. Example 9.6 is the instance $s=2$ for the Volkenborn integral, $-\frac{1}{12} = \frac{1}{2}\cdot(-\frac{1}{6})$. A degenerate instance shows how the corollary "knows" about collisions: for the point evaluation $\Lambda'(F) = F(a)$, $\Lambda'^{\otimes s}(G) = G(a,\dots,a)$ on every polynomial G (by (9.1) on monomials), and $V(a,\dots,a)=0$ for $s\ge 2$; so the Hankel determinant of a point mass vanishes for $s\ge 2$, as found for δ_3 in Chapter 6.

Intuition: the log-gas reading, and what is new. Chapter 6 read Heine's formula as the partition function of s charges with logarithmic repulsion in an external potential, and noted where this stops for the note's functional. Three points are new here. First, Corollary 9.8 is pure algebra: no integral, no positivity, no limit, so it can be applied to $\Lambda = \sum_k L_k$, a sum of $3n+1$ functionals that each look at four Taylor coefficients at one point. Second, for such a Λ the "gas" lives on a lattice: by linearity in each variable, each charge must be placed at one of the nodes, so the configuration space is the set of *occupation numbers* s_k (how many charges sit at the node k). A single node behaves like the point mass above, but smeared out to order 3: charges at the same node do not collide completely, because L_k sees $(y+k)^0,\dots,(y+k)^3$, and the computation of Step 6 below shows that a node can hold at most four of them, the counting version of the rank bound of Chapter 6. Third, the Boltzmann factor splits into an interaction between different nodes, $\prod(k-m)^{2s_ks_m}$ to leading order, and an on-site factor built from the local constants. The analogy stops at positivity: the on-site factors are rational numbers (or polynomials in X) of either sign, the terms can cancel, and the expansion only gives *upper* bounds (Chapter 10) and *lower* bounds for valuations (Chapter 11); it cannot by itself show that $\Delta_K \neq 0$.

9.5 The statement of the Heine expansion

9.5.1 What we start from

Recall from Chapters 5 and 6: the nodes are $k\in\mathcal{N}=\{-n,\dots,2n\}$, the node k sits at $y=-k$, and for each node there are four local constants $c_{k,a}(X)=\beta_{k,a}+X\alpha_{k,a}$, $a=0,\dots,3$, with $c_{k,a}=0$ for $a\ge 4$. The node functional and the full functional are [note, (2.24)]

$$L_k(P)=\sum_{a=0}^{3} c_{k,a}\,P_a(k)\;,\qquad P_a(k)=[z^a]\,P(-k+z)\;,\qquad \Lambda=\sum_{k\in\mathcal{N}}L_k\;,$$

and $\Delta_K(X)=\det\left[\Lambda(y^{i+j})\right]_{0\le i,j<K}$. The node matrix is the 4×4 Hankel matrix $C_k=[c_{k,a+b}]_{0\le a,b\le 3}$, zero below the anti-diagonal.

Definition 9.9 (minors $C_k[R]$; [note, Section 5.1], before Proposition 5.1)**.** For a subset $R=\{R_0<R_1<\dots<R_{|R|-1}\}\subseteq\{0,1,2,3\}$ let $C_k[R]=[c_{k,R_b+b'}]_{0\le b,b'<|R|}$: the square submatrix of C_k with row set R and the *first* $|R|$ columns.

Writing c_a for $c_{k,a}$, the fifteen minors are, symbolically in $c_0,\dots,c_3$:

$\lvert R\rvert$	R	$\det C_k[R]$
1	$\{0\},\{1\},\{2\},\{3\}$	$c_0,\ c_1,\ c_2,\ c_3$
2	$\{0,1\},\{0,2\},\{0,3\}$	$c_0c_2-c_1^2,\ \ c_0c_3-c_1c_2,\ \ -c_1c_3$
	$\{1,2\},\{1,3\},\{2,3\}$	$c_1c_3-c_2^2,\ \ -c_2c_3,\ \ -c_3^2$
3	$\{0,1,2\},\{0,1,3\}$	$-c_0c_3^2+2c_1c_2c_3-c_2^3,\ \ c_3(c_1c_3-c_2^2)$
	$\{0,2,3\},\{1,2,3\}$	$-c_2c_3^2,\ \ -c_3^3$
4	$\{0,1,2,3\}$	c_3^4

For example $C_k[\{0,3\}] = \left(\begin{smallmatrix} c_0 & c_1 \\ c_3 & 0 \end{smallmatrix}\right)$ (rows 0 and 3 of C_k, columns $0,1$; the entry $c_{3+1}=c_4$ is 0). For $n=1$ and the node $k=1$ at $X=0$ ($c_{1,a} = \frac{7}{16}, -\frac{23}{96}, \frac{5}{48}, -\frac{1}{48}$, Chapter 5): $\det C_1[\{0,1\}] = \frac{7}{16}\cdot\frac{5}{48} - \frac{529}{9216} = -\frac{109}{9216}$.

9.5.2 Profiles and partitions

Definition 9.10 (profile)**.** A *profile* for K is a vector $s=(s_k)_{k\in\mathcal{N}}$ of integers $s_k\ge 0$ with $\sum_k s_k = K$. For a profile fix a map $\iota : \{1,\dots,K\}\to\mathcal{N}$ with $|\iota^{-1}(k)| = s_k$ for every k (we always take the non-decreasing one: the first s_{-n} variables go to the node $-n$, the next s_{-n+1} to $-n+1$, and so on).

For $n=1$ we write profiles as $s=(s_{-1},s_0,s_1,s_2)$. The profile $(1,0,2,1)$ for $K=4$ has $\iota=(-1,1,1,2)$: one particle at the node -1 (at $y=1$), two at the node 1 (at $y=-1$), one at the node 2 (at $y=-2$); see Figure 9.1.

Definition 9.11 (partition, monomial symmetric polynomial)**.** A *partition* μ is a finite non-increasing sequence of positive integers $\mu_1\ge\mu_2\ge\cdots\ge\mu_\ell>0$, its *parts*; ℓ is the number of parts and $|\mu|=\sum\mu_j$ its size; the empty partition $\emptyset$ has no parts and size 0. For $s\ge\ell$ variables, the *monomial symmetric polynomial* $m_\mu(w_1,\dots,w_s)$ is the sum of all *distinct* monomials $w_1^{e_1}\cdots w_s^{e_s}$ whose exponent vector $(e_1,\dots,e_s)$ is a rearrangement of $(\mu_1,\dots,\mu_\ell,0,\dots,0)$; and $m_\emptyset=1$.

Example 9.12. In two variables: $m_{(1)}=w_1+w_2$, $m_{(2)}=w_1^2+w_2^2$, $m_{(1,1)}=w_1w_2$, $m_{(2,1)}=w_1^2w_2+w_1w_2^2$, $m_{(2,2)}=w_1^2w_2^2$. In three variables: $m_{(1,1)}=w_1w_2+w_1w_3+w_2w_3$, $m_{(2)}=w_1^2+w_2^2+w_3^2$, $m_{(2,1)}$ has the six terms $w_i^2w_j$, $i\ne j$. In one variable $m_{(j)}=w^j$. Each m_μ is symmetric, and every symmetric polynomial is a combination of them, with the coefficient of m_μ equal to the coefficient of any one of its monomials: a symmetric polynomial has the same coefficient at all rearrangements of an exponent vector.

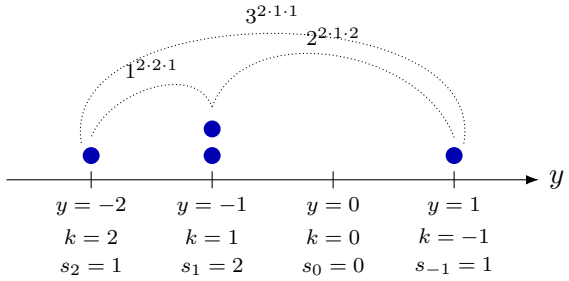


Figure 9.1: The profile $s=(1,0,2,1)$ for $n=1$, $K=4$: the four "particles" $y_1,\dots,y_4$ placed at the nodes. The leading part of the cross factor is $\prod_{k<m}|k-m|^{2s_ks_m} = 2^4\cdot1^4\cdot3^2 = 144$; each node with $s_k\ge1$ contributes a local factor built from its own local constants.

9.5.3 The proposition

Proposition 9.13 (Heine expansion; [note, Proposition 5.1])**.** *Let $K \geq 1$. Then [note, (5.2)]*

$$\Delta_K(X) = \sum_{s} \sum_{\lambda} \operatorname{coef}_\lambda(s) \prod_{k \in \mathcal{N}} M_{k,\lambda_k}(X) \ , \tag{9.3}$$

where:

(a) s runs over the profiles with $0 \leq s_k \leq 4$ and $\sum_k s_k = K$, and $\lambda = (\lambda_k)_{k \in \mathcal{N}}$ over the tuples of partitions such that λ_k has at most s_k parts and $|\lambda_k| \leq s_k(4 - s_k)$;

(b) with ι fixed for s as above, the cross factor *is [note, (5.3)]*

$$Q_s(w) = \prod_{\substack{i<i' \\ \iota(i) \neq \iota(i')}} \left(\iota(i') - \iota(i) + w_i - w_{i'}\right)^2 \in \mathbb{Z}[w_1, \ldots, w_K] \ , \tag{9.4}$$

and $\operatorname{coef}_\lambda(s) \in \mathbb{Z}$ is the coefficient in Q_s of any monomial whose exponents at the variables w_i with $\iota(i) = k$ are, for every k, a rearrangement of the parts of λ_k padded with zeros;

(c) $M_{k,\emptyset} = 1$ if $s_k = 0$, and for $s_k \geq 1$, M_{k,λ_k} is an integer combination of the minors $\det C_k[R]$ with $|R| = s_k$ and $\sum R - \binom{s_k}{2} = |\lambda_k|$, with coefficients that depend only on s_k, λ_k and R.

The note credits the proposition to [19] ("after [K26, Proposition 5.1]"). In the proof below, M_{k,λ_k} is given by the formula $M_{k,\lambda_k} = (s_k!)^{-1}(L_k^{\mathrm{loc}})^{\otimes s_k}(V^2 m_{\lambda_k})$, see (9.13).

Intuition. Read (9.3) as a partition function of a lattice gas. Distribute K particles over the nodes, at most four per node (the profile s). The weight of a configuration is the product of a pair interaction between particles at different nodes, the integer polynomial Q_s, whose constant term is $\prod_{k<m}(k-m)^{2s_k s_m}$ (Section 9.8), and of one on-site factor per occupied node, a small determinant of that node's local constants. The particles at a node are not points but carry a "polarization" w (a displacement of order at most 3 in the Taylor expansion), and the partitions λ_k record how the interaction couples to these polarizations: $\lambda = \emptyset$ is the pure point-charge interaction, the other λ are multipole corrections.

9.6 The proof of the Heine expansion

We follow the note's six steps. The running example is $n = 1$; its node data and local constants are in Chapter 5.

9.6.1 Step 1: Heine's formula for Λ

By Corollary 9.8 with $\Lambda' = \Lambda$, $s = K$, and the variables called $y_1, \ldots, y_K$:

$$\Delta_K = \frac{1}{K!}\, \Lambda^{\otimes K}\left(V(y_1, \ldots, y_K)^2\right) \ . \tag{9.5}$$

For $n = 1$ and $K = 1, \ldots, 5$ this can be carried out explicitly: expand $V(y)^2$ (it has $1, 3, 19, 201, 2961$ monomials for $K = 1, \ldots, 5$), replace every monomial $\prod_i y_i^{e_i}$ by $\prod_i \Lambda(y^{e_i})$ and divide by $K!$; the result is exactly the Hankel determinant $\Delta_K(X)$, as a polynomial in X (comparing the values at $X = 0, \ldots, K$ suffices, since both sides have degree $\leq K$). For instance $K = 2$: $V^2 = y_1^2 - 2y_1y_2 + y_2^2$ gives $\frac{1}{2}(2\Lambda(y^2)\Lambda(1) - 2\Lambda(y)^2) = \Lambda(1)\Lambda(y^2) - \Lambda(y)^2$, the 2×2 Hankel determinant.

9.6.2 Step 2: distributing the variables over the nodes

Since $\Lambda = \sum_k L_k$, every factor in the definition of $\Lambda^{\otimes K}$ on monomials splits: $\prod_i \Lambda(y^{e_i}) = \prod_i \sum_k L_k(y^{e_i})$. Multiplying out the K sums means choosing for each variable i a node $\iota(i)$:

$$\prod_{i=1}^{K} \sum_{k\in\mathcal{N}} L_k(y^{e_i}) = \sum_{\iota:\{1,\dots,K\}\to\mathcal{N}} \prod_{i=1}^{K} L_{\iota(i)}(y^{e_i}) \ .$$

By linearity this holds for every polynomial in place of the monomial:

$$\Lambda^{\otimes K} = \sum_{\iota} \bigotimes_{i=1}^{K} L_{\iota(i)} \ , \tag{9.6}$$

where $\bigotimes_i L_{\iota(i)}$ is the mixed tensor product (on monomials: $\prod_i y_i^{e_i} \mapsto \prod_i L_{\iota(i)}(y^{e_i})$). There are $|\mathcal{N}|^K = (3n+1)^K$ maps ι.

Only the occupancy matters. Let π be a permutation of $\{1,\dots,K\}$ and $\iota' = \iota\circ\pi$. Renaming the variables, $y_i \mapsto y_{\pi(i)}$, turns the functional $\bigotimes_i L_{\iota(i)}$ into $\bigotimes_i L_{\iota'(i)}$ (the variable y_i is now treated by $L_{\iota(\pi(i))}$), and leaves V^2 unchanged because V^2 is symmetric. So $\bigotimes_i L_{\iota(i)}(V^2) = \bigotimes_i L_{\iota'(i)}(V^2)$. Two maps ι, ι' differ by such a renaming exactly when they have the same *occupancy* $s_k = |\iota^{-1}(k)|$ for all k. Hence the value depends only on the profile s.

Counting. The maps with occupancy s are the ways of splitting $\{1,\dots,K\}$ into labelled groups of sizes s_k: the multinomial coefficient $K!/\prod_k s_k!$. Therefore, from (9.5),

$$\Delta_K = \frac{1}{K!}\sum_s \frac{K!}{\prod_k s_k!} \bigotimes_i L_{\iota(i)}(V^2) = \sum_s \Big(\prod_k s_k!\Big)^{-1} \bigotimes_i L_{\iota(i)}(V^2) \ , \tag{9.7}$$

with one fixed ι per profile, the sum over *all* profiles (any $s_k \geq 0$). The note anticipates that profiles with some $s_k \geq 5$ give 0; this is proved in Step 6.

Example 9.14 ($n = 1$, $K = 3$)**.** There are $4^3 = 64$ maps ι and $\binom{3+3}{3} = 20$ profiles. Evaluating $\bigotimes_i L_{\iota(i)}(V^2)$ at $X = 0$ for all 64 maps literally (expanding $V(y)^2$ and replacing $\prod_i y_i^{e_i}$ by $\prod_i L_{\iota(i)}(y^{e_i})$), one finds: the value is constant on each occupancy class; the class sizes are $3!/\prod s_k!$ (for example 3 maps, $(-1,1,1)$, $(1,-1,1)$, $(1,1,-1)$, have the occupancy $(1,0,2,0)$, and 6 have $(1,1,1,0)$); and the sum over all 64 maps equals $\Lambda^{\otimes 3}(V^2)$.

9.6.3 Step 3: local coordinates and the cross factor

The node functional L_k looks at Taylor coefficients at $y = -k$. To make this visible, introduce the *local functional*

$$L_k^{\mathrm{loc}} : \mathbb{Q}[X][w] \to \mathbb{Q}[X] \ , \qquad L_k^{\mathrm{loc}}(w^j) = c_{k,j} \quad (\text{so } = 0 \text{ for } j \geq 4) \ .$$

Then $L_k(F) = L_k^{\mathrm{loc}}\big(F(-k+w)\big)$ for every polynomial F: writing $F(-k+w) = \sum_a F_a(k) w^a$, the right side is $\sum_a c_{k,a} F_a(k) = L_k(F)$. In words, L_k^{loc} is L_k written in the coordinate $w = y + k$ centred at the node.

Fix a profile and its ι, and substitute $y_i = -\iota(i) + w_i$ in $V(y)^2$: each variable is measured from the node it was sent to. Then $\bigotimes_i L_{\iota(i)}(V(y)^2) = \bigotimes_i L_{\iota(i)}^{\mathrm{loc}}\big(V(y)^2|_{y_i=-\iota(i)+w_i}\big)$, by the identity just proved, applied variable by variable on monomials. Now look at the factors of $V(y)^2 = \prod_{i<i'}(y_{i'} - y_i)^2$:

- if $\iota(i) = \iota(i')$ (both at the same node), $y_{i'} - y_i = w_{i'} - w_i$;
- if $\iota(i) \neq \iota(i')$ (a *cross pair*), $y_{i'} - y_i = \iota(i) - \iota(i') + w_{i'} - w_i = -\big(\iota(i') - \iota(i) + w_i - w_{i'}\big)$, whose square is the factor of (9.4).

Collecting the factors of the first kind node by node, and writing $w^{(k)}$ for the group of variables w_i with $\iota(i) = k$:

$$V(y)^2\big|_{y_i=-\iota(i)+w_i} = \prod_{k\in\mathcal{N}} V\big(w^{(k)}\big)^2 \cdot Q_s(w) \ , \tag{9.8}$$

with V of an empty or one-element group equal to 1. Q_s has integer coefficients since the $\iota(i)$ are integers.

Example 9.15 ($K = 3$: two variables at one node, one at another)**.** Take $n = 1$ and the profile $(1, 0, 2, 0)$, so $\iota = (-1, 1, 1)$: $y_1 = 1 + w_1$ at the node -1, and $y_2 = -1 + w_2$, $y_3 = -1 + w_3$ at the node 1. The three factors of $V(y)^2$ become

$$(y_2 - y_1)^2 = (-2 + w_2 - w_1)^2, \qquad (y_3 - y_1)^2 = (-2 + w_3 - w_1)^2, \qquad (y_3 - y_2)^2 = (w_3 - w_2)^2 \ .$$

The last one is the intra-node factor $V(w_2, w_3)^2$; the first two are the cross factor

$$\begin{aligned} Q_s &= (2 + w_1 - w_2)^2(2 + w_1 - w_3)^2 \\ &= 16 + 32w_1 - 16w_2 - 16w_3 + 24w_1^2 + 4w_2^2 + 4w_3^2 - 24w_1w_2 - 24w_1w_3 + 16w_2w_3 + \dots \end{aligned}$$

(27 monomials in all; the full expansion confirms (9.8) for this profile and for $(1, 0, 2, 1)$). Its constant term is $16 = 2^{2\cdot1\cdot2}$: the squared distance 2 between the two nodes, once for each of the $1 \cdot 2$ cross pairs.

9.6.4 Step 4: symmetry inside a node

Write $Q_s = \sum_e q_e w_1^{e_1} \cdots w_K^{e_K}$ with $q_e \in \mathbb{Z}$. Let π permute the variables *inside* one node ($\iota(\pi(i)) = \iota(i)$ for all i). Then $y_i = -\iota(i) + w_i \mapsto -\iota(i) + w_{\pi(i)} = y_{\pi(i)}$, so π permutes the y's, maps cross pairs to cross pairs, and permutes the factors $(y_{i'} - y_i)^2$ of Q_s among themselves (the squares make the order inside a pair irrelevant). So Q_s is unchanged, and $q_e = q_{e\circ\pi}$: the coefficients are constant on the orbits of the group $\prod_k \mathrm{Sym}(w^{(k)})$ of permutations inside the nodes.

An orbit is described by listing, for every node k, the exponents at the variables of $w^{(k)}$ without regard to order: a multiset, which we write as a partition λ_k by sorting its nonzero entries. It has at most s_k parts. The tuple $\lambda = (\lambda_k)_k$ labels the orbit, and the sum of the monomials in the orbit is $\prod_k m_{\lambda_k}(w^{(k)})$. Hence

$$Q_s = \sum_{\lambda} \mathrm{coef}_\lambda(s) \prod_{k\in\mathcal{N}} m_{\lambda_k}\big(w^{(k)}\big) \ , \tag{9.9}$$

with $\mathrm{coef}_\lambda(s)$ the common coefficient of the monomials in the orbit λ, as in Proposition 9.13(b).

Example 9.16 (continuing Example 9.15)**.** Here $w^{(-1)} = \{w_1\}$ and $w^{(1)} = \{w_2, w_3\}$, and $\lambda = (\lambda_{-1}, \lambda_1)$ (the empty nodes $0, 2$ carry $\emptyset$). Grouping the terms above:

$$\begin{aligned} Q_s = 16 &+ 32\, m_{(1)}(w_1) - 16\, m_{(1)}(w_2, w_3) + 24\, m_{(2)}(w_1) + 4\, m_{(2)}(w_2, w_3) \\ &- 24\, m_{(1)}(w_1)\, m_{(1)}(w_2, w_3) + 16\, m_{(1,1)}(w_2, w_3) + \dots \end{aligned}$$

so $\mathrm{coef}_{(\emptyset,\emptyset)} = 16$, $\mathrm{coef}_{((1),\emptyset)} = 32$, $\mathrm{coef}_{(\emptyset,(1))} = -16$, $\mathrm{coef}_{(\emptyset,(1,1))} = 16$, $\mathrm{coef}_{((1),(1))} = -24$. The coefficients of w_2 and w_3 are equal (-16), as are those of w_1w_2 and w_1w_3 (-24): the symmetry in action. There are 18 orbits λ, and the coefficient is constant on each (as it is on each of the 384 orbits for the profile $(1, 0, 2, 1)$).

9.6.5 Step 5: the tensor product factorizes over the nodes

Insert (9.8) and (9.9) into the profile term:

$$\bigotimes_i L^{\mathrm{loc}}_{\iota(i)}\Big(\prod_k V(w^{(k)})^2\cdot Q_s\Big)=\sum_\lambda \mathrm{coef}_\lambda(s)\bigotimes_i L^{\mathrm{loc}}_{\iota(i)}\Big(\prod_k\big[V(w^{(k)})^2\, m_{\lambda_k}(w^{(k)})\big]\Big)\ .$$

Inside the bracket, the factor for the node k is a polynomial in the variables $w^{(k)}$ only, and the groups $w^{(k)}$ are disjoint. On those variables the mixed tensor product acts as $(L^{\mathrm{loc}}_k)^{\otimes s_k}$. By the factorization property of Section 9.2 (for groups of variables) the value is the product over the nodes:

$$\bigotimes_i L^{\mathrm{loc}}_{\iota(i)}(V(y)^2)=\sum_\lambda \mathrm{coef}_\lambda(s)\prod_{k:\,s_k\geq 1}(L^{\mathrm{loc}}_k)^{\otimes s_k}\Big(V(w^{(k)})^2\, m_{\lambda_k}(w^{(k)})\Big)\ . \tag{9.10}$$

For a node with $s_k=0$ there are no variables, and only $\lambda_k=\emptyset$ occurs.

9.6.6 Step 6: what one node can contribute

It remains to compute the *local quantity* $(L^{\mathrm{loc}}_k)^{\otimes s}(V(w)^2 m_\mu(w))$ for $s\geq 1$ variables $w=(w_1,\dots,w_s)$ and a partition μ with at most s parts. The idea: write $V^2 m_\mu = V\cdot(Vm_\mu)$, a product of two antisymmetric polynomials, expand the second one into determinants, and apply Andreief's identity once more, now to the local functional.

Antisymmetric polynomials and alternants. A polynomial $F(w_1,\dots,w_s)$ is *antisymmetric* if exchanging two variables multiplies it by -1. For a strictly decreasing sequence $\nu=(\nu_0>\nu_1>\dots>\nu_{s-1}\geq 0)$ the *alternant* is

$$a_\nu(w)=\det\big[w_i^{\nu_b}\big]_{1\leq i\leq s,\ 0\leq b<s}=\sum_\sigma \mathrm{sgn}(\sigma)\prod_i w_i^{\nu_{\sigma(i)}}\ .$$

It is antisymmetric (exchanging two variables exchanges two rows), and its monomials are the rearrangements of $w^\nu=w_1^{\nu_0}\cdots w_s^{\nu_{s-1}}$, each with coefficient ±1; the coefficient of w^ν itself (the diagonal, $\sigma(i)=i-1$) is $+1$.

Lemma 9.17 ([note, Appendix B], Step 6)**.** *Every antisymmetric $F\in\mathbb{Z}[w_1,\dots,w_s]$ equals $\sum_\nu q_\nu\, a_\nu$, the sum over strictly decreasing ν, where $q_\nu\in\mathbb{Z}$ is the coefficient of w^ν in F.*

Proof. Let q_e be the coefficient of w^e in F, and let t be the transposition of two variables $w_i, w_{i'}$. Antisymmetry says $q_{e\circ t}=-q_e$. (i) If $e_i=e_{i'}$, then $e\circ t=e$ and $q_e=-q_e$, so $q_e=0$: monomials with a repeated exponent do not occur. (ii) Every permutation is a product of transpositions, so $q_{e\circ\pi}=\mathrm{sgn}(\pi)\,q_e$. Every exponent vector with distinct entries is a rearrangement $\nu\circ\pi$ of exactly one strictly decreasing ν, so F is determined by the numbers q_ν. The polynomial $G=F-\sum_\nu q_\nu a_\nu$ is antisymmetric and has coefficient 0 at every w^ν (only a_ν contains w^ν, with coefficient 1); by (i) and (ii) it is 0. □

Now V is antisymmetric, m_μ is symmetric, so Vm_μ is antisymmetric, with integer coefficients and homogeneous of degree $\binom{s}{2}+|\mu|$. By Lemma 9.17

$$V(w)\,m_\mu(w)=\sum_\nu n_{\mu,\nu}\,a_\nu(w)\ ,\qquad n_{\mu,\nu}\in\mathbb{Z}\ ,\qquad \sum_b \nu_b=\tbinom{s}{2}+|\mu|\ , \tag{9.11}$$

the last condition because all monomials of Vm_μ have that degree.

Example 9.18 ($s = 2$ and $s = 3$)**.** For $s = 2$, $a_{(\nu_0,\nu_1)} = w_1^{\nu_0} w_2^{\nu_1} - w_1^{\nu_1} w_2^{\nu_0}$ and $V = w_2 - w_1 = -a_{(1,0)}$. Then

$$Vm_{(1)} = (w_2 - w_1)(w_1 + w_2) = -a_{(2,0)} \ , \qquad Vm_{(2)} = (w_2 - w_1)(w_1^2 + w_2^2) = -a_{(3,0)} + a_{(2,1)} \ ,$$

the second because $a_{(2,1)} = w_1^2 w_2 - w_1 w_2^2$ and $a_{(3,0)} = w_1^3 - w_2^3$. For $s = 3$: $V = -a_{(2,1,0)}$ (reversing the three columns of $\det\left[w_i^b\right]$ is one transposition), $Vm_{(1)} = -a_{(3,1,0)}$, $Vm_{(2)} = -a_{(4,1,0)} + a_{(3,2,0)}$, and $Vm_{(2,1)} = -a_{(4,2,0)} + 2a_{(3,2,1)}$. In general the $n_{\mu,\nu}$ are read off as the coefficients of Vm_μ at the strictly decreasing monomials. (These integers are known in the theory of symmetric functions: Vs_λ is an alternant for a Schur polynomial s_λ, so the $n_{\mu,\nu}$ are, up to sign, entries of the inverse Kostka matrix; Macdonald, *Symmetric Functions and Hall Polynomials*, Ch. I. The proof does not need this.)

The local Andreief identity. Apply Lemma 9.7 with $\Lambda' = L_k^{\mathrm{loc}}$, $f_b = w^b$ (so $\det[f_b(w_i)] = V$) and $g_{b'} = w^{\nu_{b'}}$ (so $\det[g_{b'}(w_i)] = a_\nu$). Since $L_k^{\mathrm{loc}}(w^{b+\nu_{b'}}) = c_{k,b+\nu_{b'}}$, summing over ν with the weights $n_{\mu,\nu}$ gives [note, (B.3)]

$$\left(L_k^{\mathrm{loc}}\right)^{\otimes s}(V^2 m_\mu) = s! \sum_\nu n_{\mu,\nu} \det\left[c_{k,b+\nu_{b'}}\right]_{0\le b,b'<s} \ . \tag{9.12}$$

Worked case $s = 2$, $\mu = (1)$: $Vm_{(1)} = -a_{(2,0)}$, so the right side is $2 \cdot (-1) \cdot \det\left(\begin{smallmatrix} c_2 & c_0 \\ c_3 & c_1 \end{smallmatrix}\right) = 2(c_0c_3 - c_1c_2)$. Directly: $V^2 m_{(1)} = (w_1^2 - 2w_1w_2 + w_2^2)(w_1 + w_2) = w_1^3 + w_2^3 - w_1^2 w_2 - w_1 w_2^2$, and $(L^{\mathrm{loc}})^{\otimes 2}$ gives $c_3c_0 + c_0c_3 - c_2c_1 - c_1c_2 = 2(c_0c_3 - c_1c_2)$.

A column of zeros. In the matrix $[c_{k,b+\nu_{b'}}]_{b,b'}$ the column b' consists of $c_{k,\nu_{b'}}, c_{k,\nu_{b'}+1}, \dots$; if $\nu_{b'} \ge 4$, all its indices are ≥ 4 and the column is zero (recall $c_{k,m} = 0$ for $m \ge 4$), so the determinant vanishes. Hence only ν with all $\nu_b \le 3$ contribute: ν is a set of s distinct elements of $\{0,1,2,3\}$. Two consequences.

- *At most four variables per node.* For $s \ge 5$ there are no s distinct elements in $\{0,1,2,3\}$, every term of (9.12) vanishes, and so does every profile term with some $s_k \ge 5$ (by (9.10) it contains the factor of that node for every λ). This proves that the sum (9.7) may be restricted to $s_k \le 4$, as in Proposition 9.13(a).
- *The bound on $|\lambda_k|$.* The largest possible $\sum_b \nu_b$ is obtained with the s largest elements $3, 2, \dots, 4-s$ of $\{0,1,2,3\}$: $\sum_{j=0}^{s-1}(3-j) = 3s - \binom{s}{2}$. With (9.11), a nonzero contribution needs $\binom{s}{2} + |\mu| \le 3s - \binom{s}{2}$, that is

$$|\mu| \le 3s - 2\tbinom{s}{2} = 3s - s(s-1) = s(4-s) \ .$$

  So $|\mu| \le 3, 4, 3, 0$ for $s = 1, 2, 3, 4$. In particular a node with four variables contributes only with $\mu = \emptyset$, and then $\nu = (3,2,1,0)$.

The minors. A surviving ν is a subset $R = \{\nu_{s-1} < \cdots < \nu_0\}$ of $\{0,1,2,3\}$ of size s. The matrix $[c_{k,b+\nu_{b'}}]_{b,b'}$, transposed, is $[c_{k,\nu_b+b'}]_{b,b'}$: rows indexed by the elements of R (in decreasing order), columns $0, \dots, s-1$. Reordering the rows increasingly gives $C_k[R]$ of Definition 9.9, at the cost of the sign $(-1)^{\binom{s}{2}}$ of reversing s rows; transposition does not change a determinant. The condition $\sum \nu = \binom{s}{2} + |\mu|$ becomes $\sum R - \binom{s}{2} = |\mu|$. Dividing (9.12) by $s!$ we define

$$M_{k,\mu} = \frac{1}{s!}\left(L_k^{\mathrm{loc}}\right)^{\otimes s}(V^2 m_\mu) = (-1)^{\binom{s}{2}} \sum_{\substack{R\subseteq\{0,1,2,3\},\ |R|=s \\ \sum R - \binom{s}{2} = |\mu|}} n_{\mu,R} \det C_k[R] \ , \tag{9.13}$$

where $n_{\mu,R} = n_{\mu,\nu}$ for ν the decreasing listing of R. This is an integer combination of minors, with coefficients depending on s, μ, R only: Proposition 9.13(c).

Assembling. Put (9.10) into (9.7). The profile s carries the factor $(\prod_k s_k!)^{-1}$, and each node with $s_k \geq 1$ contributes $(L_k^{\mathrm{loc}})^{\otimes s_k}(V^2 m_{\lambda_k}) = s_k!\, M_{k,\lambda_k}$; the factorials cancel, and

$$\Delta_K = \sum_{s:\, s_k \leq 4} \sum_{\lambda} \mathrm{coef}_\lambda(s) \prod_k M_{k,\lambda_k} \ ,$$

where the terms with $|\lambda_k| > s_k(4-s_k)$ vanish and may be dropped. This is (9.3). The note says "the signs are absorbed in the integers $n_{\mu,\nu}$", i.e. the sign $(-1)^{\binom{s}{2}}$ of (9.13) is part of the integer coefficients in (c).

Example 9.19 (the local factors for $s = 1, 2, 3, 4$)**.** Computing $M_{k,\mu}$ symbolically in $c_0, \ldots, c_3$, both from the definition and from the alternant expansion (9.12), gives the same result for every μ with $|\mu| \leq s(4-s)+2$ (and $|\mu| \leq 1$ for $s = 5$), and all $M_{k,\mu}$ with $|\mu| > s(4-s)$ are 0, as are both values for $s = 5$. Writing $c_a = c_{k,a}$:

- $s = 1$: $M_{k,(j)} = c_j$ for $j = 0, \ldots, 3$: a lone particle at a node just picks one local constant.
- $s = 2$: $M_\emptyset = c_0c_2 - c_1^2 = \det C_k[\{0,1\}]$, $M_{(1)} = c_0c_3 - c_1c_2 = \det C_k[\{0,2\}]$, $M_{(1,1)} = c_1c_3 - c_2^2 = \det C_k[\{1,2\}]$, $M_{(2)} = c_2^2 - 2c_1c_3 = \det C_k[\{0,3\}] - \det C_k[\{1,2\}]$, $M_{(2,1)} = -c_2c_3$, $M_{(3)} = c_2c_3$, $M_{(2,2)} = -c_3^2$, $M_{(3,1)} = c_3^2$, $M_{(4)} = 0$.
- $s = 3$: $M_\emptyset = \det C_k[\{0,1,2\}] = -c_0c_3^2 + 2c_1c_2c_3 - c_2^3$, $M_{(1)} = c_3(c_1c_3 - c_2^2)$, $M_{(2)} = -M_{(1,1)} = c_2c_3^2$, $M_{(3)} = M_{(1,1,1)} = -c_3^3$, $M_{(2,1)} = 2c_3^3$.
- $s = 4$: $M_\emptyset = \det C_k = c_3^4$, and $M_\mu = 0$ for $\mu \neq \emptyset$.

Numbers, $n = 1$, node $k = 1$: a profile with only this node occupied has $Q_s = 1$, so its term is $M_{1,\emptyset}$ alone. The profile terms are $(0,0,2,0)$: $-\frac{109}{9216} - \frac{89}{96}X - X^2$, which is $c_{1,0}c_{1,2} - c_{1,1}^2$ with $c_{1,0} = \frac{7}{16} - \frac{27}{2}X$, $c_{1,1} = X - \frac{23}{96}$, $c_{1,2} = \frac{5}{48}$; and $(0,0,3,0)$: $-\frac{31}{110592} + \frac{7}{4608}X = \det C_1[\{0,1,2\}]$. The node 0, with $c_{0,0} = -\frac{27}{2}X$, $c_{0,1} = -X$, $c_{0,2} = c_{0,3} = 0$, gives $(0,2,0,0)$: $M_{0,\emptyset} = 0 - X^2 = -X^2$, and every $M_{0,\mu}$ with $s = 3, 4$ vanishes, because each contains $c_{0,3}$ or $c_{0,2}$ in every term (see the list). So the node 0 holds at most two particles, in accordance with the rank-2 matrix C_0 of Chapter 6.

The proof in one paragraph. Heine's formula (Andreief with $f = g =$ monomials) writes Δ_K as $\frac{1}{K!}\Lambda^{\otimes K}(V^2)$. Splitting $\Lambda = \sum_k L_k$ in each of the K slots gives a sum over the maps ι from variables to nodes; by symmetry only the occupancy s matters, and the $K!/\prod s_k!$ maps per occupancy cancel the $\frac{1}{K!}$ up to $1/\prod s_k!$. In local coordinates $w_i = y_i + \iota(i)$, V^2 splits into intra-node Vandermondes and the integer cross factor Q_s; grouping Q_s by symmetry inside the nodes gives the integers $\mathrm{coef}_\lambda(s)$ and monomial symmetric polynomials; the tensor product factorizes over the nodes; and at each node a second use of Andreief turns $V^2 m_\mu$ into $s_k!$ times an integer combination of minors of C_k, which vanish unless the column exponents fit into $\{0,1,2,3\}$: hence $s_k \leq 4$ and $|\lambda_k| \leq s_k(4-s_k)$.

9.7 The expansion in numbers

9.7.1 All of Δ_K for $n = 1$ and $n = 3$

Every profile term $(\prod_k s_k!)^{-1} \bigotimes_i L_{\iota(i)}(V^2)$ can be computed in two ways: *literally* as in Step 2 (expand $V(y)^2$, replace $\prod_i y_i^{e_i}$ by $\prod_i L_{\iota(i)}(y^{e_i})$, with $L_k(y^e) = \sum_{a \leq 3} c_{k,a}\binom{e}{a}(-k)^{e-a}$), and through the substitution of Step 3 (expand V^2 in the local variables, drop monomials with an exponent ≥ 4, which L^{loc} kills, and replace w_i^e by $c_{\iota(i),e}$). The table sums over *all* profiles, including those with $s_k \geq 5$, and compares with the Hankel determinant computed directly from the moments $\Lambda(y^m)$.

	$n=1$ (nodes $-1,0,1,2$)				$n=3$ (nodes $-3,\dots,6$)			
K	prof.	nonzero	$\log_{10}\|\Delta_K\|$	$\log_{10}\sum_s\|T_s\|$	prof.	nonzero	$\log_{10}\|\Delta_K\|$	$\log_{10}\sum_s\|T_s\|$
1	4	4	2.91	2.94	10	10	−3.63	−3.53
2	10	10	6.03	6.07	55	55	−6.21	−6.06
3	20	19	8.46	8.47	220	219	−9.01	−8.70
4	35	31	11.28	11.29	715	705	−10.77	−10.26
5	56	43	13.68	13.68	2002	1938	−12.05	−11.57

Here T_s is the profile term (a polynomial in X) and $\|f\| = \sum_j |f_j|$ is the sum of the absolute values of the coefficients of a polynomial $f = \sum_j f_j X^j$. In every case the sum of the profile terms equals $\Delta_K(X)$ exactly; for $n = 1$ the literal and the substituted computation agree profile by profile, and for $n = 1$, $K \le 5$, Step 1 holds as well. The zero terms are exactly the ones predicted: for $K = 5$, the four (for $n = 1$) and ten (for $n = 3$) profiles with five particles at one node give 0; and every profile with $s_0 \ge 3$ gives 0 ($1, 4, 9$ of them for $n = 1$, $K = 3, 4, 5$; $1, 10, 54$ for $n = 3$). No other profile term vanished. The last column of each half measures how much the profile terms cancel: for $n = 1$ almost not at all, for $n = 3$, $K = 5$, by a factor of about 3 ($10^{0.48}$). (For $n = 3$ the table stops at $K = 5$; $K = 6$ would involve 5005 profiles (4905 with all $s_k \le 4$), with four times more monomials each.)

9.7.2 Which profiles matter

Example 9.20 ($n = 1$, $K = 3$: all twenty profiles)**.** Profiles $s = (s_{-1}, s_0, s_1, s_2)$, the number of maps $3!/\prod s_k!$, and $\log_{10}\|T_s\|$:

s	maps	$\log_{10}\|T_s\|$	s	maps	$\log_{10}\|T_s\|$	s	maps	$\log_{10}\|T_s\|$
$(2,0,0,1)$	3	8.10	$(1,1,1,0)$	6	5.25	$(0,0,0,3)$	1	2.69
$(1,0,0,2)$	3	8.10	$(0,1,1,1)$	6	5.21	$(3,0,0,0)$	1	2.68
$(1,1,0,1)$	6	7.32	$(0,0,1,2)$	3	4.64	$(0,0,2,1)$	3	2.48
$(1,0,1,1)$	6	7.32	$(2,1,0,0)$	3	4.64	$(1,2,0,0)$	3	2.27
$(2,0,1,0)$	3	6.13	$(1,0,2,0)$	3	3.87	$(0,1,2,0)$	3	1.62
$(0,1,0,2)$	3	6.10	$(0,2,0,1)$	3	3.59	$(0,2,1,0)$	3	1.29
						$(0,0,3,0)$	1	−2.74

and $(0,3,0,0)$ gives 0. Compare $\log_{10}\|\Delta_3\| = 8.46$: the two profiles that put two particles at one outer node and one at the other, $(2,0,0,1)$ and $(1,0,0,2)$, carry most of it. For instance

$$T_{(2,0,0,1)} = \tfrac{1118330620943482675}{104485552128} - \tfrac{18998082857505625}{272097792}X + \tfrac{266218750000}{6561}X^2 - \tfrac{3850000000}{729}X^3 .$$

For $K = 4$ the leader is $(2,0,0,2)$ (6 maps, $\log_{10}\|T_s\| = 11.21$ against 11.28 for Δ_4), followed by $(1,1,0,2)$ and $(2,0,1,1)$ (10.08, 10.07). For $K = 5$ the leaders are $(2,1,0,2)$ and $(2,0,1,2)$ (13.36, 13.35, against 13.68); putting the fifth particle at an outer node, $(3,0,0,2)$ or $(2,0,0,3)$, gives only 11.98 and 12.00.

Intuition. The pattern is that of a repelling gas in a box: the particles spread to the outermost nodes -1 and 2 ($y = 1$ and $y = -2$), as far apart as possible, like the charges of $\mathrm{d}x$ on $[0,1]$ in Chapter 6; but a node does not like to be crowded (an on-site factor is a determinant of local constants, and the pair interaction between particles at the same node has no distance to gain from), so the fifth particle goes inside rather than to a third place at an end. For $n = 3$ (nodes $-3,\dots,6$) the leading profiles for $K = 5$ are $(1,1,0,0,0,0,0,1,1,1)$ and its mirror $(1,1,1,0,0,0,0,0,1,1)$ (both $\log_{10}\|T_s\| = -12.33$, against -12.05 for Δ_5), and each of the six largest profiles puts at most one particle on the six middle nodes $-1,\dots,4$, and then at -1 or 4. The middle nodes lie among or next to the

triple zeros of W and have tiny leading coefficients ($|h_1| = |h_2| \approx 10^{-17}$, Chapter 5); their on-site factors are correspondingly small. This is the discrete version of the equilibrium problem of Chapter 10, where the occupancies become a density $0 \le \sigma \le 4$.

9.7.3 One profile taken apart

Example 9.21 (the decomposition (9.3) for one profile)**.** Return to $n = 1$, $K = 3$, $s = (1, 0, 2, 0)$ of Examples 9.15 and 9.16. Here $\lambda = (\lambda_{-1}, \lambda_1)$ with $\lambda_{-1} \in \{\emptyset, (1), (2), (3)\}$ (at most one part, $|\lambda_{-1}| \le 3$) and λ_1 with at most two parts and $|\lambda_1| \le 4$. The local factors are $M_{-1,(j)} = c_{-1,j}$ and the $s = 2$ list of Example 9.19 for the node 1. The leading term is

$$\operatorname{coef}_{(\emptyset,\emptyset)} M_{-1,\emptyset}\, M_{1,\emptyset} = 16 \cdot c_{-1,0} \cdot (c_{1,0}c_{1,2} - c_{1,1}^2) \ ,$$

at $X = 0$ equal to $16 \cdot (-\frac{30137923}{93312}) \cdot (-\frac{109}{9216}) = \frac{3285033607}{53747712} \approx 61.1$. There are 18 orbits λ, of which 17 give nonzero terms (the orbit $((4), \emptyset)$ from the monomial w_1^4 of Q_s is killed by $M_{-1,(4)} = c_{-1,4} = 0$); their sum is the profile term

$$T_{(1,0,2,0)} = \tfrac{9246396089}{71663616} + \tfrac{734590747}{186624}X + \tfrac{17600603}{5832}X^2 - \tfrac{29600}{81}X^3$$

(≈ 129.0 at $X = 0$), equal to $(1!\,2!)^{-1} \bigotimes_i L_{\iota(i)}(V^2)$ computed directly. For $K = 4$ and $s = (1, 0, 2, 1)$ (Figure 9.1) there are 384 orbits and 128 nonzero terms, the leading coefficient is $\operatorname{coef}_{(\emptyset,\emptyset,\emptyset)} = 144$, and again the sum agrees exactly with the directly computed profile term.

9.8 What each part of a term carries

The note's sentence after [note, Proposition 5.1]: "the local factors M_{k,λ_k} carry the local constants, hence the numbers $h_k^{s_k}$, and the cross factor $\operatorname{coef}_\lambda(s)$ carries the node differences $(k-m)^{2s_k s_m}$, up to the corrections that come from the variables w." Both halves can be made precise.

The local factors. By [note, (2.21)] (Chapter 5) each local constant is linear in the four numbers $H_k[0], \dots, H_k[3]$ that describe the pole of W at the node: $\beta_{k,a} = \sum_i i(i+1)\mathrm{HS}_3(k, i+2)H_k[4-i-a]$ and $\alpha_{k,a} = -2916H_k[1-a]$ (zero for $a \ge 2$). A minor of size s_k is a homogeneous polynomial of degree s_k in the $c_{k,a}$, so M_{k,λ_k} is homogeneous of degree s_k in $H_k[0], \dots, H_k[3]$, and

$$M_{k,\lambda_k} = h_k^{s_k} \cdot (\text{the same expression in } H_k[b]/h_k) \ , \qquad h_k = H_k[0] \ .$$

The cleanest instance is a full node: $M_{k,\emptyset} = c_{k,3}^4$ for $s_k = 4$, and $c_{k,3} = \beta_{k,3} = 2\mathrm{HS}_3(k,3)\, h_k$ (only $i = 1$ contributes). For $n = 1$: $c_{k,3} = \frac{125}{162}, 0, -\frac{1}{48}, -\frac{1021}{1296}$ for $k = -1, 0, 1, 2$, and $2\mathrm{HS}_3(k,3) = \frac{243}{4}, 0, \frac{243}{4}, \frac{248103}{4000}$; e.g. $\frac{243}{4} \cdot \frac{250}{19683} = \frac{125}{162}$ with $h_{-1} = \frac{250}{19683}$.

The cross factor. The constant term of Q_s is obtained by setting all $w_i = 0$: $\prod_{\text{cross pairs}} (\iota(i') - \iota(i))^2 = \prod_{k<m} (m-k)^{2s_k s_m}$, since there are $s_k s_m$ cross pairs between the nodes k and m. So $\operatorname{coef}_\emptyset(s) = \prod_{k<m}(k-m)^{2s_k s_m}$: 16 and 144 in the examples above. The other coefficients are the "corrections from the variables w": each factor $(d + w_i - w_{i'})^2$ with $d = \iota(i') - \iota(i)$ expands as $d^2 + 2d(w_i - w_{i'}) + (w_i - w_{i'})^2$, so a monomial of total degree r in $\operatorname{coef}_\lambda(s)$, $r = \sum_k |\lambda_k|$, costs roughly r powers of the distances less than the constant term, with combinatorial factors.

Remark 9.22 (how large the corrections are for $n = 1$). For $n = 1$ the distances are $1, 2, 3$, comparable with the exponents of the w's, and the corrections are not small. In Example 9.21 the leading λ-term is ≈ 61.1 at $X = 0$ against ≈ 129.0 for the whole profile term. For $s = (1, 0, 2, 1)$ the leading λ-term has the coefficient $-\frac{985960000}{729} \approx -1.35 \cdot 10^6$ at X^4, while the whole profile term has $+\frac{17240000}{729} \approx 2.4 \cdot 10^4$: the 127 correction terms cancel the leading one almost completely and change its sign. So at $n = 1$ "carries" is a description of where the factors come from, not a statement that the term $\lambda = \emptyset$ dominates. How the note bounds the whole sum over λ for large n is the subject of Chapter 10.

How the next chapters use the expansion. Both apply an inequality to the right side of (9.3) term by term, after the expansion has turned one determinant into a sum of products whose factors are each simple.

- The *size* (Chapter 10) uses the triangle inequality: every coefficient of $\Delta_K(X)$ is at most $\sum_s \sum_\lambda |\mathrm{coef}_\lambda(s)| \prod_k \|M_{k,\lambda_k}\|$ in absolute value (with a suitable norm on polynomials in X). The number of profiles and partitions grows only exponentially in K, while the products behave like $\prod_k |h_k|^{s_k} \prod_{k<m} |k-m|^{2s_k s_m}$, the Boltzmann weight of the lattice gas; on the scale $x = k/n$ a profile becomes a density $0 \le \sigma \le 4$ on $[-1,2]$ of total mass $\kappa = K/n$, and the largest term is governed by an energy-minimization problem with the constraint $\sigma \le 4$, the "cap" that came from Step 6 ([note, Section 5.1], after [note, (5.3)]).
- The *denominators* (Chapter 11) use the ultrametric inequality: for every prime p, $v_p(\Delta_K) \ge \min_{s,\lambda} \left[v_p(\mathrm{coef}_\lambda(s)) + \sum_k v_p(M_{k,\lambda_k}) \right]$ [note, (B.4)]. Since $\mathrm{coef}_\lambda(s) \in \mathbb{Z}$, $v_p(\mathrm{coef}_\lambda(s)) \ge 0$: the cross factors never create denominators, and every denominator of Δ_K comes from the local factors, node by node, i.e. from the minors $\det C_k[R]$. This is why the denominator estimates are local statements about the minors at a single node.

The expansion cannot show that $\Delta_K \neq 0$: a sum of nonzero terms can vanish, and in $\mathbb{Q}_3$ there is no positivity to prevent it (Chapter 6). That is the job of Chapter 14.

Check yourself 9.23. Compute $M_{k,(1,1)}$ for $s = 2$ directly from the definition $\frac{1}{2}(L_k^{\mathrm{loc}})^{\otimes 2}(V^2 m_{(1,1)})$ and identify the minor.

Answer. $V^2 m_{(1,1)} = (w_1^2 - 2w_1w_2 + w_2^2)\, w_1 w_2 = w_1^3 w_2 - 2w_1^2 w_2^2 + w_1 w_2^3$, so $(L^{\mathrm{loc}})^{\otimes 2}$ gives $c_3 c_1 - 2c_2^2 + c_1 c_3 = 2(c_1 c_3 - c_2^2)$ and $M_{k,(1,1)} = c_1 c_3 - c_2^2 = \det C_k[\{1,2\}]$; indeed $\sum R - \binom{2}{2} = 3 - 1 = 2 = |(1,1)|$.

Check yourself 9.24. Why can a node holding three particles contribute only with $|\lambda_k| \le 3$, and which minor appears for $|\lambda_k| = 3$?

Answer. The column exponents ν must be three distinct elements of $\{0,1,2,3\}$, with $\sum \nu = \binom{3}{2} + |\lambda_k| = 3 + |\lambda_k| \le 3 + 2 + 1 = 6$. For $|\lambda_k| = 3$ the only choice is $R = \{1,2,3\}$, so M_{k,λ_k} is a multiple of $\det C_k[\{1,2,3\}] = -c_{k,3}^3$; the multiples are $1, -2, 1$ for $\lambda_k = (3), (2,1), (1,1,1)$ (Example 9.19).

Summary of the chapter

Andreief's identity [note, Lemma B.1] turns the integral of a product of two $s \times s$ determinants of functions into $s!$ times one determinant of numbers; it is pure algebra, valid for any linear functional, via the tensor power $\Lambda'^{\otimes s}$ (product of the functional's values variable by variable). With monomials it gives Heine's formula $\det\left[\Lambda'(w^{b+b'})\right] = \frac{1}{s!}\Lambda'^{\otimes s}(V^2)$, V the Vandermonde. Applied to $\Lambda = \sum_k L_k$ and expanded in each slot, it writes $\Delta_K(X)$ as a sum over profiles s (occupation numbers of the nodes) of $(\prod s_k!)^{-1} \bigotimes_i L_{\iota(i)}(V^2)$; in local coordinates V^2 factors into intra-node Vandermondes and an integer cross factor Q_s; symmetry inside the nodes groups Q_s into integers $\mathrm{coef}_\lambda(s)$ times monomial symmetric polynomials; the tensor product factorizes over nodes; and a second, local use of Andreief makes each node's factor M_{k,λ_k} an integer combination of the minors $\det C_k[R]$, which vanish unless $s_k \le 4$ and $|\lambda_k| \le s_k(4 - s_k)$. This is [note, Proposition 5.1]. For $n = 1$ and $n = 3$ ($K \le 5$) the expansion reproduces Δ_K exactly; the profiles with five particles at a node and those with three or more at the node 0 vanish, and the leading profiles put the particles at the outer nodes.

Carried forward: the expansion (9.3) with its three ingredients, the profiles with the cap $s_k \le 4$ (Chapter 10: density $0 \le \sigma \le 4$), the integer cross factors $\mathrm{coef}_\lambda(s)$ with constant term $\prod_{k<m}(k-m)^{2s_k s_m}$ (Chapter 10), and the local factors M_{k,λ_k}, homogeneous of degree s_k in the node data and integer combinations of the minors $\det C_k[R]$ (Chapters 10 to 13); and the

ultrametric consequence that all denominators of Δ_K come from the minors, node by node (Chapter 11).

Chapter 10

Estimate 2: the size, an electrostatics problem

Where we are. The criterion of Chapter 7 compares the 3-adic gain with the cost of the size and of the denominators of the Hankel polynomial $\Delta_K(X)$. This chapter explains the note's proof of the size estimate, [note, Theorem 3.8]: $\log_2 \|\Delta_K\|_1 \le (\kappa^2 - 6\kappa)n^2 \log_2 n + F_i^\dagger n^2 + O(n \log n)$ with $F_i^\dagger \le 8.425, \dots, 8.648$. We cover [note, Section 5.1] from "For the size, in the rescaled variable" to the proof of [note, Theorem 3.8], [note, Appendix B] from "For Theorem 5.7 we need four lemmas" to its end ([note, Lemmas B.8, B.10, B.14, B.16] and the proof of [note, Theorem 5.7]), and the first part of [note, Appendix E], "The bound for $F_i^\dagger$". From Chapter 5 we need the nodes $k \in \mathcal{N} = \{-n, \dots, 2n\}$, the leading coefficients h_k [note, (2.18)], the Taylor coefficients $H_k[b]$ and the local constants $c_{k,a}$ [note, (2.21)]; from Chapter 9 the Heine expansion [note, Proposition 5.1], its profiles s (occupation numbers $0 \le s_k \le 4$ of the nodes with $\sum_k s_k = K$), the integer cross factors $\mathrm{coef}_\lambda(s)$ and the local factors M_{k,λ_k}. The numerical values for the potentials and for $F_i^\dagger$ in this chapter are floating-point evaluations, which are *not* a proof; the note's [note, Proposition 5.11] uses ball arithmetic.

10.1 What is being estimated

Recall that $\Delta_K(X) = \sum_j f_j X^j \in \mathbb{Q}[X]$ has degree at most K, and that $\|\Delta_K\|_1 = \sum_j |f_j|$ is the sum of the absolute values of its coefficients. In the criterion [note, (1.4)] (Chapters 1 and 7) the term $\log_2 \|\Delta_K\|_1$ appears because after clearing the denominators of $\Delta_K(a/b)$ we get an integer N, and its absolute value is at most the common denominator times $\|\Delta_K\|_1 \max(|a|, b)^K$. So $\log_2 \|\Delta_K\|_1$ is the number of bits that the real *size* of the coefficients contributes to the size of that integer. It is negative when the coefficients are small, and then it helps.

Intuition: why the logarithm. Every quantity in the balance sheet of Chapter 1 grows like n^2 or $n^2 \log n$ on the logarithmic scale. In $\|\Delta_K\|_1$ we have a sum of very many terms (the Heine expansion), each a product of very many factors. The logarithm turns the products into sums, and the sum over terms costs only the logarithm of the number of terms, which is $O(n)$. This is the same reason why a physicist computes a free energy, $-\log Z$, and not the partition function Z itself.

Theorem 10.1 (size; [note, Theorem 3.8]). *For* $K/n = \kappa \in I_i = [2.80 + 0.04(i-1),\ 2.84 + 0.04(i-1)]$, $i = 1, \dots, 5$,

$$\log_2 \|\Delta_K\|_1 \le (\kappa^2 - 6\kappa)\, n^2 \log_2 n + F_i^\dagger\, n^2 + O(n \log n)\ , \tag{10.1}$$

with $F_1^\dagger, \dots, F_5^\dagger$ *at most* 8.425174, 8.458313, 8.510836, 8.576728, 8.647895 *[note, Proposition 5.11].*

The main term $(\kappa^2 - 6\kappa)n^2 \log_2 n$ is negative for $0 < \kappa < 6$ and cancels exactly against the main term $\kappa(6-\kappa)n^2 \log_2 n$ of the denominators (Chapter 7). What is left of the size is the constant $F_i^\dagger$ in front of n^2, and the proof's margin of about 4.6 to 5.4 bits per n^2 ([note, Table 1], Chapter 1) depends on how well $F_i^\dagger$ is bounded.

Example 10.2 (the size for $n = 1, 3, 5, 7$)**.** Computing $\Delta_K(X)$ exactly from [note, Definition 2.23], as the Hankel determinant of the moments $\Lambda(y^m)$, gives the following values, in bits:

n	K (κ)	$\log_2 \lVert\Delta_K\rVert_1$	$(\kappa^2 - 6\kappa)n^2 \log_2 n$	difference/n^2
1	1, 2, 3, 4	9.67, 20.04, 28.11, 37.46	0	$9.67, \dots, 37.46$
3	3 (1)	−29.95	−71.32	4.598
3	6 (2)	−40.61	−114.12	8.167
3	9 (3)	−30.52	−128.38	10.873
5	14 (2.8)	−311.96	−520.11	8.326
5	15 (3)	−307.29	−522.43	8.606
7	20 (2.857)	−850.13	−1235.24	7.859
7	21 (3)	−846.82	−1238.04	7.984

For $n \geq 3$ the size first decreases with K (each new row adds factors h_k, which are tiny) and then increases again (the Vandermonde factors $|k-m|^{2s_k s_m}$ grow quadratically in K). At $\kappa = 3$ the excess over the main term, per n^2, is 28.1, 10.9, 8.6, 8.0 bits for $n = 1, 3, 5, 7$. Theorem 10.1 predicts at most $F_5^\dagger \approx 8.65$ plus an error $O(\log n/n)$ per n^2 whose constant is not known. So these values do not test the theorem (at $n = 7$ the error term can be anything), but they are of the predicted order of magnitude and decrease in the cases computed.

10.2 From profiles to densities

By the Heine expansion (Chapter 9), Δ_K is a sum over profiles s of products whose absolute values behave like

$$\prod_k |h_k|^{s_k} \prod_{k \neq m} |k-m|^{s_k s_m} \,, \tag{10.2}$$

up to factors that we shall show to be $e^{O(n \log n)}$. The product over $k \neq m$ runs over ordered pairs, so each unordered pair appears twice and the exponent $s_k s_m$ appears as $2s_k s_m$ in Chapter 9's notation. The logarithm of (10.2) is a quadratic function of the occupation numbers. For large n we pass to a continuum.

The rescaled variable. The node k sits at $y = -k$. Put $x = k/n$. The nodes $-n, \dots, 2n$ then sit at $x = -1, -1 + \frac{1}{n}, \dots, 2$, with spacing $\frac{1}{n}$, and a profile s becomes a step function $x \mapsto s_k$ on $[\frac{k}{n}, \frac{k+1}{n})$. Its integral is $\sum_k s_k \cdot \frac{1}{n} = K/n = \kappa$. In the limit $n \to \infty$ we get a *density* σ on $[-1, 2]$ with

$$0 \leq \sigma \leq 4 \,, \qquad \int_{-1}^{2} \sigma = \kappa \,.$$

The cap $\sigma \leq 4$ is the rule "at most four variables per node" of Chapter 9, and $\kappa \leq 3 + \frac{1}{n}$ because the note only uses $K \leq 3n + 1$ (so that [note, (2.26)] holds).

The zeros and the poles in the same variable. The zeros of W at $y = -(j + \frac{r}{3})$, $0 \leq j < n$, $r \in \{1, 2\}$, sit at $x = (j + \frac{r}{3})/n \in (0, 1)$: there are $2n$ of them in an interval of length 1, each of order 3. Counted with multiplicity and divided by n (the same normalization as for σ), this is a density $\frac{3 \cdot 2n}{n \cdot 1} = 6$ on $I = (0, 1)$. The poles are the $3n + 1$ nodes, each of order 4, on an interval of length 3: density $\frac{4 \cdot 3n}{n \cdot 3} = 4$ on $[-1, 2]$. The single zero $y = -\frac{n}{2}$ has density 0 in the limit.

Example 10.3 (the best profile for $n = 3$, $K = 9$)**.** For $n = 3$ the nodes are $-3, \dots, 6$, at $x = -1, -\frac{2}{3}, \dots, 2$. Among all 41470 profiles with $K = 9$ and $s_k \le 4$, the discrete energy $E_B(s)$ of (10.6) below (the logarithm of (10.2), slightly modified) is largest for $s = (0, 4, 0, 0, 0, 0, 0, 1, 3, 1)$: four particles at $k = -2$ ($x = -\frac{2}{3}$), and one, three, one at $k = 4, 5, 6$ ($x = \frac{4}{3}, \frac{5}{3}, 2$). Nothing sits on the nodes $-1, \dots, 3$, i.e. on $x \in [-\frac{1}{3}, 1]$, an interval that contains the zeros $(0, 1)$. As a step function this is $\sigma = 4$ on $[-\frac{2}{3}, -\frac{1}{3})$, and $1, 3$ on $[\frac{4}{3}, \frac{5}{3})$, $[\frac{5}{3}, 2)$, plus the last node: a very coarse picture of a density that avoids $(0, 1)$ and lives on the two outer intervals, as the trial density σ_0 of Section 10.10 will do.

10.3 Logarithmic potentials and the external field

Definition 10.4 ([note, (5.4)])**.** For an integrable function f on $[-1, 2]$ and $x \in \mathbb{R}$ put

$$\mathcal{L}f(x) = \int_{-1}^{2} \log|x - y|\, f(y)\, \mathrm{d}y\ , \qquad \langle f, g\rangle = \int_{-1}^{2} f(x)g(x)\, \mathrm{d}x\ .$$

Intuition: a two-dimensional Coulomb potential. In the plane, the electrostatic potential of a point charge is proportional to log of the distance (not $1/r$). So $\mathcal{L}f(x)$ is, up to sign, the potential at x of a charge distribution f on the segment, felt by a charge that also lives on the line: the "two-dimensional Coulomb gas" of random matrix theory, restricted to a line. Its logarithm comes straight from the Vandermonde factors $|k - m|$: $\sum_m s_m \log|k - m|$ is the potential at the node k of the particles at the other nodes. The integral converges at $y = x$ because log is integrable at 0.

Closed forms. Put $\Phi(w) = w \log|w| - w$ (with $\Phi(0) = 0$). Then $\Phi'(w) = \log|w| + 1 - 1 = \log|w|$ for $w \neq 0$, and Φ is continuous at 0, so Φ is a primitive of $\log|\cdot|$ on all of $\mathbb{R}$. Hence, for an interval $[\alpha, \beta]$, with the substitution $w = y - x$,

$$\mathcal{L}\mathbf{1}_{[\alpha,\beta]}(x) = \int_{\alpha}^{\beta} \log|y - x|\, \mathrm{d}y = \Phi(\beta - x) - \Phi(\alpha - x)\ . \tag{10.3}$$

For example $\mathcal{L}\mathbf{1}_I(\frac{1}{2}) = \Phi(\frac{1}{2}) - \Phi(-\frac{1}{2}) = 2(\frac{1}{2}\log\frac{1}{2} - \frac{1}{2}) = -\log 2 - 1 \approx -1.6931$, and $\mathcal{L}\mathbf{1}_{[-1,2]}(-1) = \Phi(3) - \Phi(0) = 3\log 3 - 3 \approx 0.2958$. A step function f has a potential that is a finite sum of such terms.

The external field. The note puts [note, (5.5)]

$$\mathcal{V} = 6\,\mathcal{L}\mathbf{1}_I - 4\,\mathcal{L}\mathbf{1}_{[-1,2]} = 2\,\mathcal{L}\mathbf{1}_I - 4\,\mathcal{L}\mathbf{1}_O\ , \qquad O = [-1, 0] \cup [1, 2]\ . \tag{10.4}$$

The first form is "potential of the zeros (density 6 on I) minus potential of the poles (density 4 on $[-1, 2]$)". The second form follows because $\mathbf{1}_{[-1,2]} = \mathbf{1}_I + \mathbf{1}_O$ except at the two points $0, 1$, which do not change an integral, and $\mathcal{L}$ is linear: $6\mathcal{L}\mathbf{1}_I - 4\mathcal{L}\mathbf{1}_I - 4\mathcal{L}\mathbf{1}_O = 2\mathcal{L}\mathbf{1}_I - 4\mathcal{L}\mathbf{1}_O$. So on I zeros and poles partly cancel and leave a net density $6 - 4 = 2$, and on O only the poles are present, with density 4 and the opposite sign.

Example 10.5 (the field in numbers)**.** From (10.3) (the field is symmetric about $x = \frac{1}{2}$):

x	-1	-0.5	0	0.25	0.5
$6\,\mathcal{L}\mathbf{1}_I(x)$	2.3178	−0.2714	−6.0000	−9.3740	−10.1589
$-4\,\mathcal{L}\mathbf{1}_{[-1,2]}(x)$	−1.1833	4.2234	6.4548	6.9670	7.1344
$\mathcal{V}(x)$	1.1344	3.9520	0.4548	−2.4070	−3.0245

The maximum of $\mathcal{V}$ is about 3.95, near $x = -0.5$ and $x = 1.5$, and its minimum -3.02 is at $x = \frac{1}{2}$; see Figure 10.1.

Intuition: which sign means what. The bound we are after is an *upper* bound for a logarithm, so we *maximize* the exponent: a configuration counts the more, the larger $\sum_k s_k \log|h_k| + \sum_{k\neq m} s_k s_m \log|k-m|$ is. Read the terms with this in mind, remembering that $\log|x-y|$ is large when x and y are far apart and tends to $-\infty$ when they meet.

- The self-energy $\langle\sigma, \mathcal{L}\sigma\rangle = \iint \log|x-y|\sigma(x)\sigma(y)\,\mathrm{d}x\,\mathrm{d}y$ is larger when the mass is spread out. So the particles *repel* each other: this is the Vandermonde.
- The zeros enter $\log|h_k|$ with a plus sign, $+3\log|k-\text{zero}|$: a particle gains by being *far from the zeros*. The zeros repel the particles, as charges of the same sign.
- The poles enter with a minus sign, $-4\log|k-m|$: a particle gains by being *close to the poles*. The poles attract the particles, as charges of the opposite sign.

In the second form of (10.4): a net repelling charge of density 2 on I, and a net attracting charge of density 4 on O. The particles therefore leave I and settle on O, but they cannot pile up arbitrarily (cap 4, self-repulsion). In the physicist's convention ($E = -\log(\text{weight})$, minimize E) all signs flip; the note keeps the "log of the weight" and maximizes. Where the analogy stops: the true terms of the Heine expansion have signs and can cancel; we only use the absolute values, so the electrostatic problem gives an upper bound and says nothing about cancellations.

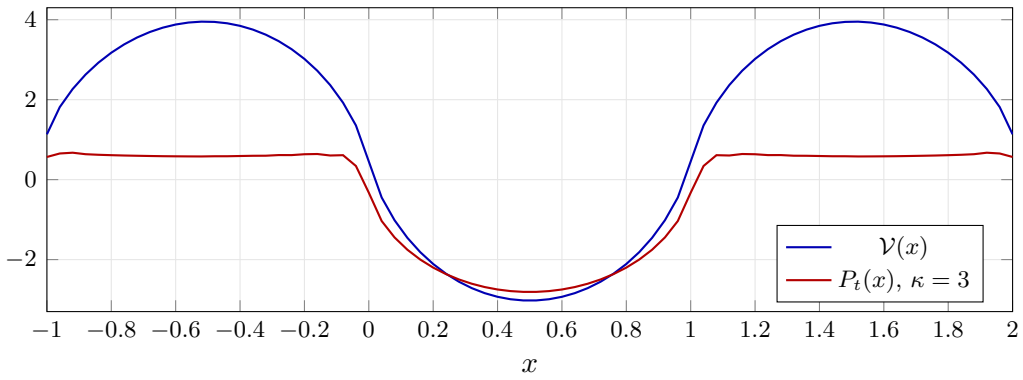


Figure 10.1: The external field $\mathcal{V}$ (10.4) and the first variation $P_t = \mathcal{V} + 2t\mathcal{L}\sigma_0$ of F at the trial density $\sigma_\kappa = t\sigma_0$, $\kappa = 3$, $t = 3/m_0 \approx 1.0367$ (Section 10.10); sampled every 0.04. Adding the particles' own repulsion $2t\mathcal{L}\sigma_0$ flattens the field on most of $O = [-1,0]\cup[1,2]$ to values between 0.57 and 0.68; it drops only near $x = 0$ and $x = 1$, where σ_0 is small.

10.4 The energy functional, its first variation and the gap

Definition 10.6 ([note, (5.6)], after [19])**.** A measurable σ on $[-1,2]$ is *feasible for* κ if $0 \le \sigma \le 4$ and $\int \sigma = \kappa$. Put

$$F[\sigma] = \langle\sigma, \mathcal{V}\rangle + \langle\sigma, \mathcal{L}\sigma\rangle\,, \qquad P_\sigma = \mathcal{V} + 2\mathcal{L}\sigma\,, \qquad \operatorname{gap}(\sigma) = \sup_{\sigma' \text{ feasible}} \langle P_\sigma, \sigma' - \sigma\rangle\,.$$

$F[\sigma]$ is the continuum version of $\frac{1}{n^2}$ times the logarithm of (10.2), without the $\log n$ terms: the energy of the particles in the field $\mathcal{V}$ plus their mutual (logarithmic) energy. Lemma 10.17 below makes this precise.

P_σ is the first variation. The kernel $\log|x-y|$ is symmetric, so $\langle f, \mathcal{L}g\rangle = \iint \log|x-y| f(x)g(y) = \langle g, \mathcal{L}f\rangle$. Hence, for any bounded η and real ϵ,

$$F[\sigma+\epsilon\eta] = F[\sigma] + \epsilon\big(\langle\eta, \mathcal{V}\rangle + \langle\eta, \mathcal{L}\sigma\rangle + \langle\sigma, \mathcal{L}\eta\rangle\big) + \epsilon^2\langle\eta, \mathcal{L}\eta\rangle = F[\sigma] + \epsilon\langle P_\sigma, \eta\rangle + \epsilon^2\langle\eta, \mathcal{L}\eta\rangle\,. \quad (10.5)$$

So $\langle P_\sigma, \eta\rangle$ is the derivative of F at σ in the direction η, and $P_\sigma(x)$ is the gain per unit of mass added at x. The factor 2 comes from the two places where σ appears in the quadratic term.

The gap is nonnegative and measures non-optimality. Taking $\sigma' = \sigma$ gives 0, so $\mathrm{gap}(\sigma) \geq 0$. The gap is the largest first-order gain obtainable by moving from σ to another feasible density. If σ were the maximizer, moving could not gain to first order, and the gap would be 0. These are the conditions of an *obstacle problem* (constrained equilibrium problem) of potential theory: at a maximizer σ^* there is a constant c with $P_{\sigma^*} = c$ where $0 < \sigma^* < 4$, $P_{\sigma^*} \leq c$ where $\sigma^* = 0$, and $P_{\sigma^*} \geq c$ where $\sigma^* = 4$ (Lagrange multiplier c for the mass, and the two obstacles 0 and 4). For constrained energy problems of this kind see e.g. Dragnev and Saff, *Constrained energy problems with applications to orthogonal polynomials of a discrete variable* (J. Anal. Math., 1997), and [30] for logarithmic potentials. The note never solves this problem: it only needs an upper bound for $\sup F$.

Proposition 10.7 (the tangent-plane bound)**.** *Suppose that $\langle \eta, \mathcal{L}\eta\rangle \leq 0$ for every bounded η with $\int \eta = 0$. Then for every κ and every σ feasible for κ,*

$$\sup_{\sigma' \text{ feasible for } \kappa} F[\sigma'] \leq F[\sigma] + \mathrm{gap}(\sigma) \ .$$

Proof. Let σ' be feasible for κ and $\eta = \sigma' - \sigma$. Then η is bounded and $\int \eta = \kappa - \kappa = 0$. By (10.5) with $\epsilon = 1$, $F[\sigma'] = F[\sigma] + \langle P_\sigma, \sigma' - \sigma\rangle + \langle \eta, \mathcal{L}\eta\rangle$. The last term is ≤ 0 by hypothesis, and the middle term is $\leq \mathrm{gap}(\sigma)$ by the definition of the gap as a supremum. Take the supremum over σ'. □

Intuition. This is the elementary fact that a concave function lies below each of its tangent planes, $f(y) \leq f(x) + \nabla f(x) \cdot (y - x)$, followed by maximizing the right side, which is linear in y, over the feasible set. A quadratic function is concave exactly when its quadratic part is ≤ 0, and the hypothesis says this on the directions that keep the mass fixed, the only ones we move in. The bound turns a hard nonlinear problem (find $\sup F$) into an easy linear one (maximize $\langle P_\sigma, \sigma'\rangle$), at the price of guessing a good σ. Moreover $F[\sigma] \leq \sup F \leq F[\sigma] + \mathrm{gap}(\sigma)$, so the gap is an upper bound for the error of the guess.

Example 10.8 (the bound at $\kappa = 3$)**.** For the trial density σ_3 of Section 10.10, a floating-point evaluation gives $F[\sigma_3]/\log 2 = 8.478236$ and $\mathrm{gap}(\sigma_3)/\log 2 = 0.120033$ bits, so $\sup F/\log 2 \in [8.478, 8.599]$ at $\kappa = 3$. At $\kappa = 2.8$: $F = 8.277362$, gap $= 0.078236$. The gap is small because P_t is almost constant where σ_κ has its mass (Figure 10.1), as it would be exactly for the maximizer.

The hypothesis of Proposition 10.7 for the kernel $\log|x-y|$ is a known fact of potential theory (a signed measure of total mass 0 has nonnegative logarithmic energy $-\iint \log|x-y|\,\mathrm{d}\mu\,\mathrm{d}\mu$; [30], Ch. I). The note does not use it in this form. It proves the discrete statement that the proof of [note, Theorem 5.7] needs, [note, Lemma B.10], to which we turn.

10.5 Conditional negative definiteness

On the lattice, $\log|k-m|$ is undefined for $k = m$. The note replaces it by

$$B(d) = \tfrac{1}{2}\log\!\left(1 + d^2\right), \qquad B(0) = 0\,, \qquad 0 \leq B(d) - \log|d| = \tfrac{1}{2}\log\left(1 + d^{-2}\right) \leq \frac{1}{2d^2} \quad (d \neq 0)\,,$$

the last step by $\log(1+u) \leq u$. For example $B(1) = \frac{1}{2}\log 2 = 0.3466$ against $\log 1 = 0$, and $B(10) = 2.3076$ against $\log 10 = 2.3026$.

Lemma 10.9 (conditional negative definiteness; [note, Lemma B.10]). *For real $x_1,\dots,x_N$ and real $\tau_1,\dots,\tau_N$ with $\sum_i \tau_i = 0$,*

$$\sum_{i,j} \tau_i \tau_j B(x_i - x_j) \le 0 \ .$$

Consequently, for real vectors $s, \tilde{s}$ indexed by the nodes with $\sum_k s_k = \sum_k \tilde{s}_k$, the discrete energy *[note, (B.7)]*

$$E_B(s) = \sum_k s_k \log|h_k| + \sum_{k,m} s_k s_m B(k-m) \tag{10.6}$$

satisfies [note, (B.11)]

$$E_B(s) \le E_B(\tilde{s}) + \langle \gamma, s - \tilde{s}\rangle \ , \qquad \gamma_k = \log|h_k| + 2\sum_m \tilde{s}_m B(k-m) \ . \tag{10.7}$$

The condition $\sum \tau_i = 0$ matters: with $\tau = (1,1)$ at two points at distance 10 the form is $2B(10) = 4.6151 > 0$. It is the discrete counterpart of "$\int \eta = 0$" in Proposition 10.7.

Proof. Step 1: a Cayley-type map. For real x put $\omega_x = \frac{\frac12 - ix}{\frac32 + ix}$. Then $|\omega_x|^2 = \frac{\frac14 + x^2}{\frac94 + x^2} < 1$. (The map $x \mapsto \omega_x$ sends the real line into the open unit disc, as a Cayley transform sends a half-plane to the disc.)

Step 2: the key identity. Multiply out:

$$(\tfrac32 + ix)(\tfrac32 - iy) = \tfrac94 - \tfrac32 iy + \tfrac32 ix + xy \ , \qquad (\tfrac12 - ix)(\tfrac12 + iy) = \tfrac14 + \tfrac12 iy - \tfrac12 ix + xy \ ,$$

and the difference is $2 - 2iy + 2ix = 2(1 + i(x-y))$. Since $\bar{\omega}_y = \frac{\frac12 + iy}{\frac32 - iy}$,

$$1 - \omega_x \bar{\omega}_y = \frac{(\frac32 + ix)(\frac32 - iy) - (\frac12 - ix)(\frac12 + iy)}{(\frac32 + ix)(\frac32 - iy)} = \frac{2(1 + i(x-y))}{(\frac32 + ix)(\frac32 - iy)} \ .$$

Take absolute values and square: $|1 - \omega_x\bar{\omega}_y|^2 = \frac{4(1+(x-y)^2)}{|\frac32 + ix|^2 |\frac32 + iy|^2}$, which is $1 + (x-y)^2 = \frac14 |1 - \omega_x\bar{\omega}_y|^2 |\frac32 + ix|^2 |\frac32 + iy|^2$. Taking $\frac12$ log:

$$B(x-y) = \log|1 - \omega_x\bar{\omega}_y| + a(x) + a(y) - \log 2 \ , \qquad a(x) = \log|\tfrac32 + ix| \ . \tag{10.8}$$

This is [note, (B.12)]. Numerically, at $(x,y) = (1,-2)$ both sides of (10.8) equal 1.151292546497 ($|\omega_1| = 0.6202$); at $(5,7)$ both equal 0.804718956217 ($|\omega_5| = 0.9626$).

Step 3: the terms that drop out. Insert (10.8) into the quadratic form. The term $a(x_i)$ contributes $\sum_{i,j} \tau_i\tau_j a(x_i) = \big(\sum_i \tau_i a(x_i)\big)\big(\sum_j \tau_j\big) = 0$, likewise $a(x_j)$, and the constant contributes $-\log 2\,(\sum_i \tau_i)^2 = 0$. Only $\sum_{i,j} \tau_i\tau_j \log|1 - \omega_{x_i}\bar{\omega}_{x_j}|$ is left.

Step 4: the series. For a complex ζ with $|\zeta| < 1$, $\log(1-\zeta) = -\sum_{m\ge1} \zeta^m/m$ (principal branch), and $\log|1-\zeta| = \mathrm{Re}\log(1-\zeta) = -\mathrm{Re}\sum_m \zeta^m/m$. With $\zeta = \omega_{x_i}\bar{\omega}_{x_j}$ (modulus < 1), and exchanging the finite sum over i,j with the absolutely convergent series,

$$\sum_{i,j} \tau_i\tau_j \log|1 - \omega_{x_i}\bar{\omega}_{x_j}| = -\mathrm{Re}\sum_{m\ge1} \frac1m \sum_{i,j} \tau_i \omega_{x_i}^m \, \tau_j \bar{\omega}_{x_j}^m = -\sum_{m\ge1} \frac1m \Big|\sum_i \tau_i \omega_{x_i}^m\Big|^2 \le 0 \ ,$$

because $\sum_{i,j} u_i\bar{u}_j = |\sum_i u_i|^2$ for $u_i = \tau_i \omega_{x_i}^m$ (τ_i real). This is [note, (B.13)], and the first claim is proved.

Step 5: the consequence. E_B is a quadratic polynomial in s with the symmetric matrix $B(k-m)$. With $\tau = s - \tilde{s}$:

$$E_B(\tilde{s} + \tau) = E_B(\tilde{s}) + \sum_k \tau_k \Big(\log|h_k| + 2\sum_m \tilde{s}_m B(k-m)\Big) + \sum_{k,m} \tau_k \tau_m B(k-m) \ ,$$

by the same computation as (10.5). The middle term is $\langle \gamma, \tau\rangle$, and the last is ≤ 0 by the first claim, since $\sum_k \tau_k = 0$. □

Example 10.10 (numbers)**.** For

$$x = (-1, 0.3, 0.7, 2, 5) \quad \text{and} \quad \tau = (1, -2, 0.5, 1.5, -1)$$

the quadratic form equals -3.5984388139, and the series $-\sum_{m<400} \frac{1}{m} |\sum_i \tau_i \omega_{x_i}^m|^2$ gives the same ten digits. For (10.7) take $n = 3$, $K = 9$, the profile $s = (0, 4, 0, 0, 0, 0, 0, 1, 3, 1)$ of Example 10.3 and $\tilde{s} = (1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$ (on the nodes $-3, \dots, 6$): then $E_B(s) = -93.72$ and $E_B(\tilde{s}) + \langle \gamma, s - \tilde{s} \rangle = -69.68$ nats, a slack of 24.03 nats, which is $-\sum_{k,m} \tau_k \tau_m B(k-m)$ for $\tau = s - \tilde{s}$.

Intuition: why the $\log n$ does not hurt. In the rescaled variable $B(k-m) \approx \log n + \log|x-y|$ for $|k-m|$ large. A constant added to the kernel changes $\sum \tau_i \tau_j B$ by the constant times $(\sum \tau_i)^2 = 0$. So the lattice form and the continuum form $\langle \eta, \mathcal{L}\eta \rangle$ with $\int \eta = 0$ are related without any $\log n$ term, which is why the comparison of a profile s with a smooth guess $\tilde{s}$ of the same mass works at the scale n^2.

10.6 The discrete energy bounds the size

Lemma 10.11 (discrete energy; [note, Lemma B.8])**.** $\log \|\Delta_K\|_1 \le \max_s E_B(s) + O(n \log n)$, *the maximum over the profiles s of [note, Proposition 5.1], uniformly in $K \le 3n + 1$.*

The note applies the triangle inequality $\|f + g\|_1 \le \|f\|_1 + \|g\|_1$ and the multiplicativity $\|fg\|_1 \le \|f\|_1 \|g\|_1$ (for polynomials in X) to the Heine expansion $\Delta_K = \sum_s \sum_\lambda \operatorname{coef}_\lambda(s) \prod_k M_{k,\lambda_k}$, and bounds the three ingredients: the number of terms, the cross factor, the local factors. We need one standard tool.

Fact 10.12 (Cauchy's estimate on a polydisc)**.** *Let $Q(w_1, \dots, w_K) = \sum_e q_e w^e$ be a polynomial with complex coefficients, $r > 0$, and $M_r = \max\{|Q(w)| : |w_1| = \cdots = |w_K| = r\}$. Then $|q_e| \le M_r \, r^{-|e|}$ for every exponent vector e, $|e| = e_1 + \cdots + e_K$.*

Proof. Put $w_i = re^{2\pi i \theta_i}$. Then $Q = \sum_{e'} q_{e'} r^{|e'|} e^{2\pi i e' \cdot \theta}$, and since $\int_{[0,1]^K} e^{2\pi i (e'-e)\cdot\theta} \mathrm{d}\theta$ is 1 for $e' = e$ and 0 otherwise, $q_e r^{|e|} = \int_{[0,1]^K} Q(re^{2\pi i\theta}) e^{-2\pi i e\cdot\theta} \mathrm{d}\theta$. The integrand has absolute value at most M_r, and the domain has volume 1. (This is the multi-variable form of the Cauchy inequalities of complex analysis.) □

Intuition. A coefficient is a Fourier coefficient of Q on the torus, so it cannot exceed the maximum of $|Q|$ there. The estimate does not care whether the coefficients come from many terms that partly cancel or from one big term; it only sees the maximum of $|Q|$.

The note's proof of Lemma 10.11, step by step. (1) The number of terms. A profile has $0 \le s_k \le 4$ at each of the $3n+1$ nodes, so there are at most 5^{3n+1} profiles. For each node, λ_k is a partition with $|\lambda_k| \le s_k(4 - s_k) \le 4$; there are $1 + 1 + 2 + 3 + 5 = 12$ partitions of size $0, \dots, 4$. So there are at most $5^{3n+1} 12^{3n+1} = e^{O(n)}$ pairs (s, λ), and $\|\Delta_K\|_1$ is at most $e^{O(n)}$ times the largest $\|\cdot\|_1$ of a single term.

(2) The cross factor via Cauchy's estimate. Recall [note, (5.3)]: $\operatorname{coef}_\lambda(s)$ is a coefficient of $Q_s(w) = \prod (\iota(i') - \iota(i) + w_i - w_{i'})^2$, the product over the pairs $i < i'$ of variables placed at different nodes, at a monomial of total degree $\sum_k |\lambda_k| \le \sum_k s_k(4 - s_k) \le 4(3n+1)$. On the polydisc $|w_i| = \frac{1}{10}$, each factor satisfies $|d + w_i - w_{i'}| \le |d| + \frac{1}{5}$, where $d = \iota(i') - \iota(i)$. There are $s_k s_m$ pairs between the nodes $k < m$, each with the factor squared; so, writing the square as one factor for (k, m) and one for (m, k), Fact 10.12 with $r = \frac{1}{10}$ gives [note, (B.9)]:

$$|\operatorname{coef}_\lambda(s)| \le 10^{4(3n+1)} \prod_{k \ne m} \left(|k - m| + \tfrac{1}{5}\right)^{s_k s_m} . \tag{10.9}$$

(3) The ratios $H_k[b]/h_k$. Recall from Chapter 5 that $\widetilde{W}_k(z) = z^4 W(-k+z)$, with Taylor coefficients $H_k[b]$ and $h_k = H_k[0]$. Its zeros and poles d (with multiplicity e_d, positive for zeros, negative for poles) are: $d = k-j-\frac{r}{3}$ (zeros of order 3), $d = k-\frac{n}{2}$ (a simple zero), and $d = k-m$, $m \neq k$ (poles of order 4). So $\widetilde{W}_k(z) = h_k \prod_d (1-z/d)^{e_d}$, and with $\log(1-u) = -\sum_j u^j/j$,

$$\frac{\widetilde{W}_k(z)}{h_k} = \exp\Big(-\sum_{j\geq 1} \frac{P_j}{j} z^j\Big)\,, \qquad P_j = \sum_d e_d d^{-j}\,.$$

All $|d| \geq \frac{1}{3}$: the zeros $k-j-\frac{r}{3}$ lie in $\frac{1}{3}\mathbb{Z}\setminus\mathbb{Z}$; $|k-\frac{n}{2}| \geq \frac{1}{2}$ since n is odd; $|k-m| \geq 1$. Then $|P_1| \leq \sum_d |e_d|/|d|$, a sum of $O(n)$ terms like $3/|k-j-\frac{r}{3}|$ and $4/|k-m|$, whose sizes are those of a harmonic series: $O(\log n)$. For $j \geq 2$: the numbers $3d$ for the zeros of order 3 are distinct nonzero integers, so $\sum 3|d|^{-j} = 3\cdot 3^j \sum |3d|^{-j} \leq 3\cdot 3^j \cdot 2\zeta(2)$; the poles give at most $4\cdot 2\zeta(2)$ and the simple zero at most 2^j; so $|P_j| \leq C3^j$. Finally, the coefficient of z^b in $\exp\Big(\sum_j a_j z^j\Big)$ is a polynomial in $a_1,\dots,a_b$ with nonnegative coefficients (expand the exponential), so its absolute value is at most the same polynomial in $|a_j| = |P_j|/j$; for $b \leq 3$ this is $O(\log n)^b$. Hence $|H_k[b]| \leq |h_k| \cdot O(\log n)^b$.

(4) The local factors. By [note, (2.21)], $c_{k,a} = \beta_{k,a} + X\alpha_{k,a}$ with $\beta_{k,a} = \sum_i i(i+1)\mathrm{HS}_3(k, i+2)H_k[4-i-a]$ and $\alpha_{k,a} = -2916 H_k[1-a]$. Here $|\mathrm{HS}_3(k,M)| = |\sum_u (3/u)^M| \leq 3^M \sum_{u\geq 1} u^{-M} \leq 3^M\zeta(2) \leq 2\cdot 3^M$ for $M \geq 2$. So $\|c_{k,a}\|_1 = |\beta_{k,a}| + |\alpha_{k,a}| \leq C_1 \max_{b\leq 3} |H_k[b]|$ with an absolute constant C_1. By [note, Proposition 5.1](c), M_{k,λ_k} is a combination of at most $\binom{4}{s_k} \leq 6$ minors $\det C_k[R]$ with bounded integer coefficients, and each minor is a sum of $s_k! \leq 24$ products of s_k local constants. With (3):

$$\log \|M_{k,\lambda_k}\|_1 \leq s_k \log|h_k| + O(s_k \log\log n) + O(1)\,.$$

(5) From $\log\Big(|d|+\frac{1}{5}\Big)$ to $B(d)$. For an integer $|d| \geq 1$, $\log\Big(|d|+\frac{1}{5}\Big) - \log|d| = \log\Big(1+\frac{1}{5|d|}\Big) \leq \frac{1}{5|d|}$ and $0 \leq B(d) - \log|d| \leq \frac{1}{2d^2}$, so $\epsilon(d) = \log\Big(|d|+\frac{1}{5}\Big) - B(d)$ satisfies $|\epsilon(d)| \leq \frac{1}{5|d|} + \frac{1}{2d^2} \leq \frac{1}{|d|}$. Since $s_m \leq 4$,

$$\sum_{k\neq m} s_k s_m \epsilon(k-m) \leq \sum_k 4 s_k \sum_{m\neq k} \frac{1}{|k-m|} \leq 4K\cdot 2\Big(1+\frac{1}{2}+\cdots+\frac{1}{3n}\Big) = O(K\log n)\,.$$

Collecting. For one term: $\log|\mathrm{coef}_\lambda(s)| \leq 4(3n+1)\log 10 + \sum_{k\neq m} s_k s_m B(k-m) + O(K\log n)$ by (2) and (5); $\sum_k \log\|M_{k,\lambda_k}\|_1 \leq \sum_k s_k \log|h_k| + O(K\log\log n) + O(n)$ by (4). Since $B(0) = 0$, $\sum_{k\neq m} = \sum_{k,m}$, and the sum is $E_B(s) + O(n\log n)$ (with $K \leq 3n+1$). With (1), $\log\|\Delta_K\|_1 \leq O(n) + \max_s E_B(s) + O(n\log n)$. □

How the large corrections of Chapter 9 are absorbed. In the Remark "how large the corrections are for $n=1$" of Chapter 9 we saw that the terms $\lambda \neq \emptyset$ of the cross factor are not small at $n=1$: for $s=(1,0,2,1)$ the 127 correction terms nearly cancel the leading one and change its sign. Step (2) does not need any of the corrections to be small. It bounds *every* coefficient of Q_s, leading or not, by the maximum of $|Q_s|$ on a small torus, divided by $r^{|e|}$. The maximum is at most $\prod(|d|+\frac{1}{5})^2$, which differs from the leading coefficient $\prod d^2$ only by the factor $\prod(1+\frac{1}{5|d|})^2 = e^{O(K\log n)}$, and $r^{-|e|} \leq 10^{4(3n+1)} = e^{O(n)}$. Both are invisible at the scale n^2. How many terms there are and how they cancel no longer matters, because the triangle inequality has already given up on cancellations.

Example 10.13 (Cauchy's estimate at $n=1$)**.** For $n=1$, $s=(1,0,2,1)$, $\iota=(-1,1,1,2)$, the cross pairs have $|d| = 2,2,3,1,1$, so $\prod(|d|+\frac{1}{5})^2 = 497.411$, against the constant term $\prod d^2 = 144$. Expanding Q_s and keeping the monomials with exponents ≤ 3, which are the ones that L^{loc} does not kill, one finds:

degree $r = \lvert e\rvert$	largest $\lvert$coefficient$\rvert$	bound $10^r \cdot 497.411$	ratio
0	144	497.4	3.5
1	672	4974.1	7.4
2	1760	49741.1	28.3
4	3400	$4.97 \cdot 10^6$	1463
10	20	$4.97 \cdot 10^{12}$	$2.5 \cdot 10^{11}$

The coefficients of degree 4 reach about 24 times the constant term, but all are below the bound. The bound is wasteful by large factors at $n = 1$; what matters is that the waste is at most $10^{4(3n+1)}$, i.e. $4(3n+1)\log 10$ nats: 92 nats at $n = 3$, 2800 nats at $n = 101$, against $n^2 \log n \approx 47079$ nats at $n = 101$.

Example 10.14 (step (3) and the whole lemma at small n)**.** $\max_k |H_k[b]/h_k|$ for $b = 1, 2, 3$ is 13.5, 76.75, 248.9 ($n = 1$), 18.2, 151.6, 788.6 ($n = 3$), 20.8, 203.8, 1263 ($n = 5$), 22.7, 244.0, 1677 ($n = 7$): slowly growing, with large constants (the two zeros at distance $\frac{1}{3}$ from the node, of order 3, contribute terms of size $3 \cdot 3^j$ to P_j). For $n = 3$, maximizing E_B over all profiles gives $\max_s E_B(s)/\log 2 = -71.60, -114.98, -135.21, -134.16$ bits for $K = 3, 6, 9, 10$, against $\log_2 \|\Delta_K\|_1 = -29.95, -40.61, -30.52, -21.15$. So at $n = 3$ the term $O(n \log n)$ of Lemma 10.11 is about 40 to 113 bits: the lemma is an asymptotic statement, and at $n = 3$ the "lower order" factors (the local constants with their 2916 and HS_3, the counting) dominate. This is consistent with the lemma, which says nothing about the size of its constant.

10.7 The modulus of continuity

The next lemma controls how much a logarithmic potential changes when the point moves by δ. It is used twice: to replace sums over nodes by integrals (Lemma 10.17), and to bound P_t on a whole cell from its value at the midpoint (Section 10.10).

Lemma 10.15 (modulus of continuity; [note, Lemma B.14])**.** *For $x < x'$ in $[-1, 2]$ and $\delta = x' - x$,*

$$\int_{-1}^{2} \big|\log|x-y| - \log|x'-y|\big|\,\mathrm{d}y \le w(\delta) := 2\delta\Big(1 + \log\frac{6+\delta}{\delta}\Big)\,.$$

Hence $|\mathcal{L}f(x) - \mathcal{L}f(x')| \le \|f\|_\infty\, w(|x - x'|)$.

Proof. Let $g(y) = \log|x-y| - \log|x'-y| = \log\frac{|x-y|}{|x'-y|}$ and $\bar{x} = \frac{x+x'}{2}$.

Sign. For $y < \bar{x}$, y is closer to x than to x', so $g(y) < 0$; for $y > \bar{x}$, $g(y) > 0$.

Symmetry. Under $y \mapsto 2\bar{x} - y$ we have $x - (2\bar{x} - y) = y - x'$ and $x' - (2\bar{x} - y) = y - x$, so $g(2\bar{x} - y) = -g(y)$ and $|g|$ is symmetric about $\bar{x}$.

Enlarging the domain. Since $x, x' \in [-1, 2]$, $\bar{x} \in [-1, 2]$ and $[-1, 2] \subseteq [\bar{x} - 3, \bar{x} + 3]$. As $|g| \ge 0$, the integral over $[-1, 2]$ is at most the integral over $[\bar{x} - 3, \bar{x} + 3]$, which by symmetry is $2G$ with $G = \int_{\bar{x}-3}^{\bar{x}} |g|$.

Computing G. Substitute $u = y - \bar{x} \in [-3, 0]$; then $|x - y| = |u + \frac{\delta}{2}|$, $|x' - y| = |u - \frac{\delta}{2}|$, and $|g| = -g$ there, so $G = \int_{-3}^{0} \big(\log|u - \frac{\delta}{2}| - \log|u + \frac{\delta}{2}|\big)\mathrm{d}u$. With $\Phi' = \log|\cdot|$:

$$G = \big[\Phi(-\tfrac{\delta}{2}) - \Phi(-3 - \tfrac{\delta}{2})\big] - \big[\Phi(\tfrac{\delta}{2}) - \Phi(-3 + \tfrac{\delta}{2})\big] = -2\Phi(\tfrac{\delta}{2}) + \Phi(3 + \tfrac{\delta}{2}) - \Phi(3 - \tfrac{\delta}{2})\,,$$

using that Φ is odd. Now $-2\Phi(\frac{\delta}{2}) = -\delta\log\frac{\delta}{2} + \delta = \delta(1 + \log\frac{2}{\delta})$, and $\Phi(3 + \frac{\delta}{2}) - \Phi(3 - \frac{\delta}{2}) = \int_{3-\delta/2}^{3+\delta/2} \log y\,\mathrm{d}y \le \delta\log\Big(3 + \frac{\delta}{2}\Big)$, since log is increasing. So $2G \le 2\delta\big(1 + \log\frac{2}{\delta} + \log\Big(3 + \frac{\delta}{2}\Big)\big) = 2\delta\big(1 + \log\frac{6+\delta}{\delta}\big)$.

The consequence. $|\mathcal{L}f(x) - \mathcal{L}f(x')| = |\int g(y)f(y)\,\mathrm{d}y| \le \|f\|_\infty \int |g| \le \|f\|_\infty w(\delta)$. □

Intuition. Moving the point by δ changes $\log|x-y|$ a lot only for y within a distance comparable to δ (where it changes by $O(1)$), and by about $\delta/|x-y|$ elsewhere. Integrating $\delta/|u|$ over $\delta \le |u| \le 3$ gives $2\delta\log\frac{3}{\delta}$. So $w(\delta) \approx 2\delta\log\frac{1}{\delta}$: almost Lipschitz, with a logarithmic loss. In particular $w(\frac{1}{n}) = \frac{2}{n}(1+\log(6n+1)) = O(\frac{\log n}{n})$, and summed over $O(n)$ nodes this is $O(\log n)$. Note also that w is increasing in δ (its derivative is $2\log\frac{6+\delta}{\delta} + \frac{2\delta}{6+\delta} > 0$), which the cell bound of Section 10.10 uses tacitly.

Example 10.16. By numerical quadrature, the integral of the lemma equals 0.5771 ($x=-1$, $\delta=0.1$), 0.8801 ($x=0.5$, $\delta=0.1$), 0.0104 ($x=-1$, $\delta=10^{-3}$), 0.0180 ($x=0.5$, $\delta=10^{-3}$), against $w(0.1)=1.0222$ and $w(10^{-3})=0.0194$. In the middle of the interval the bound exceeds the truth by only about 8% for small δ.

10.8 The continuum limit

Lemma 10.17 (continuum limit; [note, Lemma B.16])**.** *Let $1 \le \kappa \le 3+\frac{1}{n}$, let σ be feasible for κ and piecewise constant with at most J pieces, and let $\tilde{s}_k = c_n\sigma(k/n)$ with c_n chosen so that $\sum_k \tilde{s}_k = K = \kappa n$; then $c_n = 1 + O_J(1/n)$. Uniformly in $k \in \mathcal{N}$:*
(a) $\log|h_k| = -6n\log n + n\,\mathcal{V}(k/n) + O(\log n)$;
(b) $2\sum_m \tilde{s}_m B(k-m) = 2\kappa n\log n + 2n\,\mathcal{L}\sigma(k/n) + O_J(\log n)$;
(c) $E_B(\tilde{s}) = (\kappa^2-6\kappa)n^2\log n + n^2 F[\sigma] + O_J(n\log n)$.

The elementary estimate [note, (B.17)]. For $\theta \in [\frac{1}{3},1]$ and integers $0 \le M_1 \le M_2$, $\sum_{M_1\le i<M_2}\log(i+\theta) = \int_{M_1}^{M_2}\log y\,\mathrm{d}y + O(\log(M_2+2))$. Reason: log is increasing, so for $i \ge 1$, $\int_{i-1+\theta}^{i+\theta}\log \le \log(i+\theta) \le \int_{i+\theta}^{i+1+\theta}\log$; summing gives the sum between two integrals whose limits differ from M_1, M_2 by at most 2; the term $i=0$ is $\log\theta = O(1)$; moving a limit by at most 2 changes the integral by at most $2\log(M_2+2)$ near the top and by a bounded amount near 0, where log is integrable. For example, for $n=101$: $\sum_{i<101}\log(i+\theta) - \int_0^{101}\log = -0.84$, 1.38, 3.23 for $\theta = \frac{1}{3},\frac{2}{3},1$, against $\log 103 = 4.63$. Consequently, splitting at a: for real a with $|a| \le 3n$ at distance $\ge \frac{1}{3}$ from $\mathbb{Z}$ (or $a \in \mathbb{Z}$ with the term $j=a$ omitted) and integers $|A_1|, |A_2| \le 3n$, $\sum_{A_1\le j<A_2}\log|a-j| = \int_{A_1}^{A_2}\log|a-y|\,\mathrm{d}y + O(\log n)$.

The note's proof. (a) By [note, (2.18)],

$$\log|h_k| = \log|\tfrac{n}{2}-k| + 3\sum_{r=1,2}\sum_{0\le j<n}\log|k-\tfrac{r}{3}-j| - 4\sum_{m\in\mathcal{N},\,m\ne k}\log|m-k|\ .$$

The first term is between $\log\frac{1}{2}$ and $\log(3n)$: $O(\log n)$. In the second, the elementary estimate with $a = k-\frac{r}{3}$ gives $\int_0^n\log|k-\frac{r}{3}-y|\,\mathrm{d}y + O(\log n)$. The shift by $\frac{r}{3}$: substituting $y = ny'$, the difference of the two integrals is $n\int_0^1(\log|\frac{k}{n}-\frac{r}{3n}-y'| - \log|\frac{k}{n}-y'|)\mathrm{d}y'$ (the $\log n$ parts cancel), at most $n\,w(\frac{r}{3n}) = O(\log n)$ by Lemma 10.15 with $f = \mathbf{1}_I$. Rescaling,

$$\int_0^n \log|k-y|\,\mathrm{d}y = \int_0^1 (\log n + \log|x-y'|)n\,\mathrm{d}y' = n\log n + n\,\mathcal{L}\mathbf{1}_I(x)\ , \qquad x = \tfrac{k}{n}\ .$$

Likewise $\sum_{m\ne k}\log|m-k| = \int_{-n}^{2n}\log|k-y|\,\mathrm{d}y + O(\log n) = 3n\log n + n\,\mathcal{L}\mathbf{1}_{[-1,2]}(x) + O(\log n)$. Collect: the $n\log n$ terms have the coefficient $3\cdot2\cdot1 - 4\cdot3 = -6$ (two classes of zeros of order 3 on an interval of length 1, poles of order 4 on an interval of length 3), and the rest is $n(6\mathcal{L}\mathbf{1}_I - 4\mathcal{L}\mathbf{1}_{[-1,2]})(x) = n\mathcal{V}(x)$.

(b) First, $\sum_{m\ne k}|B(k-m) - \log|k-m|| \le \sum_{m\ne k}\frac{1}{2(k-m)^2} \le \zeta(2) = \frac{\pi^2}{6}$, and $\tilde{s}_m \le 4c_n$, so B may be replaced by $\log|\cdot|$ at a cost $O(1)$. On a piece $[\alpha,\beta)$ of σ, the elementary estimate and the rescaling above give $\sum_{m\in[\alpha n,\beta n),m\ne k}\log|k-m| = n(\beta-\alpha)\log n + n\int_\alpha^\beta\log|x-y|\,\mathrm{d}y + O(\log n)$.

Multiply by c_n times the value of σ on the piece ($\le 4c_n$), sum over the at most J pieces: $\sum_m \tilde{s}_m \log|k-m| = c_n(\kappa n \log n + n\mathcal{L}\sigma(x)) + O_J(\log n)$, since $\sum_{\text{pieces}} \sigma_{\text{piece}}(\beta-\alpha) = \int \sigma = \kappa$. Finally $c_n = 1 + O(1/n)$ turns $c_n(\dots)$ into $(\dots) + O(\log n)$. Multiply by 2.

Why $c_n = 1 + O_J(1/n)$: a piece $[\alpha,\beta)$ contains $n(\beta-\alpha)+O(1)$ nodes, so $\sum_k \sigma(k/n) = n\kappa + O(J)$ and $c_n = \kappa n/(\kappa n + O(J))$.

(c) By Lemma 10.15, $\mathcal{V}$ and $\mathcal{L}\sigma$ change by $O(w(\delta))$ when x moves by δ (they are the potentials of the densities $2\cdot\mathbf{1}_I - 4\cdot\mathbf{1}_O$ and σ, both bounded by 4 in absolute value). For $\phi \in \{\mathcal{V}, \mathcal{L}\sigma\}$, compare $\sum_k \sigma(k/n)\phi(k/n)$ with $n\langle\sigma,\phi\rangle = \sum_k n\int_{k/n}^{(k+1)/n}\sigma\phi$: on the $O(n)$ cells $[\frac{k}{n},\frac{k+1}{n})$ on which σ is constant the two differ by $O(w(\frac{1}{n})) = O(\frac{\log n}{n})$ each, on the at most J other cells by $O(1)$ each, and the last node $k=2n$ adds $O(1)$: in total $O_J(\log n)$. Now

$$E_B(\tilde{s}) = \sum_k \tilde{s}_k\Big(\log|h_k| + \sum_m \tilde{s}_m B(k-m)\Big) = \sum_k \tilde{s}_k\Big((\kappa-6)n\log n + n(\mathcal{V}+\mathcal{L}\sigma)(\tfrac{k}{n}) + O_J(\log n)\Big)$$

by (a) and half of (b). With $\sum_k \tilde{s}_k = \kappa n$ the first part is $(\kappa^2-6\kappa)n^2\log n$, the second is $n\cdot n\langle\sigma,\mathcal{V}+\mathcal{L}\sigma\rangle + O_J(n\log n) = n^2F[\sigma] + O_J(n\log n)$, and the third is $O_J(n\log n)$. □

Intuition: where the two $\log n$ terms come from. $|h_k|$ is a ratio of $6n$ factors (the zeros, with multiplicity) of typical size n to $12n$ factors (the poles) of typical size n: about $n^{6n}/n^{12n} = n^{-6n}$, so $\sum_k s_k \log|h_k| \approx -6n\log n\cdot\kappa n$. The Vandermonde has $(\kappa n)^2$ factors $|k-m|$ of typical size n: $\kappa^2 n^2\log n$. The "typical size" is made precise by writing $|k-m| = n|x-y|$: the factor n gives the $\log n$ terms, and $|x-y|$ gives the potentials. Everything that the densities do not see (the zero at $-\frac{n}{2}$, the offset $\frac{1}{3}$ of the zeros from the nodes, the harmonic sums and the constants $i(i+1)$, 2916 in [note, (2.21)]) is in the error terms.

Example 10.18 ($\log|h_k|$ against $-6n\log n + n\mathcal{V}(k/n)$)**.** Evaluating $\log|h_k|$ from [note, (2.18)] as a sum of logarithms (for $n=51$, $k=7$ this agrees to ten digits with the logarithm of the exact rational h_7), and $\mathcal{V}$ from (10.3):

n	k (x)	$\log\lvert h_k\rvert$	$-6n\log n + n\mathcal{V}(x)$	difference	difference/$\log n$
51	−51 (−1)	−1154.68	−1145.28	−9.40	−2.39
51	−26 (−0.51)	−1021.12	−1001.55	−19.56	−4.98
51	0 (0)	−1199.53	−1179.94	−19.59	−4.98
51	25 (0.49)	−1379.46	−1357.34	−22.12	−5.63
101	−101 (−1)	−2692.27	−2682.19	−10.08	−2.19
101	−51 (−0.505)	−2419.18	−2397.55	−21.63	−4.69
101	0 (0)	−2772.46	−2750.83	−21.64	−4.69
101	50 (0.495)	−3127.05	−3102.21	−24.84	−5.38

Here $-6n\log n = -1203.1$ ($n=51$) and -2796.8 ($n=101$): $|h_k|$ is indeed about n^{-6n}, and $n\mathcal{V}$ gives the variation along the line, from -305.5 to $+399.2$ at $n=101$ ($\mathcal{V}$ ranges over $[-3.02, 3.95]$). The difference grows like a bounded multiple of $\log n$ (between $-2.2\log n$ and $-5.6\log n$ in the cases computed), as (a) says. For (b) and (c) take $\sigma = \sigma_\kappa$ of Section 10.10 with $\kappa = K/n \approx 2.9$: then $c_n = 0.999175,\ 0.999583,\ 0.999791$ for $n = 51, 101, 201$; the largest error in (b) over all k is 12.3, 12.5, 12.8 (against $\log n = 3.9,\ 4.6,\ 5.3$); and in (c) $E_B(\tilde{s}) - (\kappa^2-6\kappa)n^2\log n - n^2F[\sigma] = -10.2,\ -9.9,\ -9.75$ times $n\log n$. So the error in (c) is genuinely of order $n\log n$, with a constant near -10, while the two main terms are, at $n=101$, -423248 and $+59291$ nats.

10.9 The proof of the size theorem

Theorem 10.19 ([note, Theorem 5.7], after [19]). *Let $J \geq 1$. For $n \leq K \leq 3n+1$ and every feasible σ that is piecewise constant with at most J pieces,*

$$\log \|\Delta_K\|_1 \leq (\kappa^2 - 6\kappa)\, n^2 \log n + n^2 (F[\sigma] + \mathrm{gap}(\sigma)) + O_J(n \log n) \ .$$

The note's proof, step by step. Step 1: reduce to a linear problem. Let $\tilde{s}$ be as in Lemma 10.17. By Lemma 10.11 and then (10.7) (both s and $\tilde{s}$ sum to K),

$$\log \|\Delta_K\|_1 \leq \max_s \left(E_B(\tilde{s}) + \langle \gamma, s - \tilde{s} \rangle \right) + O(n \log n) \ .$$

This is the discrete tangent-plane bound: the quadratic problem over profiles is replaced by a linear one.

Step 2: the slope. By Lemma 10.17(a),(b), $\gamma_k = (2\kappa - 6) n \log n + n(\mathcal{V} + 2\mathcal{L}\sigma)(\frac{k}{n}) + \delta_k = \mathrm{const}_n + n P_\sigma(\frac{k}{n}) + \delta_k$ with $\max_k |\delta_k| = O_J(\log n)$. The constant contributes $\mathrm{const}_n \sum_k (s_k - \tilde{s}_k) = 0$, and $|\langle \delta, s - \tilde{s} \rangle| \leq \max |\delta_k| \sum_k (s_k + \tilde{s}_k) = 2K \max |\delta_k| = O_J(n \log n)$. So it remains to bound $n \sum_k P_\sigma(\frac{k}{n})(s_k - \tilde{s}_k)$.

Step 3: a profile as a feasible density. For a profile s let $\tau(x) = s_k$ on $[\frac{k}{n}, \frac{k+1}{n})$ for $-n \leq k < 2n$. The last node $k = 2n$ has no cell, so put its mass on the set $E = \{\tau \leq 3\}$: $\sigma' = \tau + \frac{s_{2n}}{n|E|} \mathbf{1}_E$. Then $\int \sigma' = \frac{1}{n} \sum_{k<2n} s_k + \frac{s_{2n}}{n} = \kappa$. Where $\tau > 3$ we have $\tau = 4$ (it is an integer ≤ 4), so $4|\{\tau > 3\}| \leq \int \tau \leq \kappa \leq 3 + \frac{1}{n}$ and $|\{\tau > 3\}| < 1$; hence $|E| > 2$, and on E, $\sigma' \leq 3 + \frac{4}{2n} \leq 4$ for $n \geq 2$. So σ' is feasible for κ.

Step 4: sums become integrals. By Lemma 10.15 (applied to P_σ, the potential of the density $6 \cdot \mathbf{1}_I - 4 \cdot \mathbf{1}_{[-1,2]} + 2\sigma$, which lies in $[2, 10]$ on I and in $[-4, 4]$ on O), $\sum_k s_k P_\sigma(\frac{k}{n}) = n\langle P_\sigma, \sigma' \rangle + O(\log n)$: each of the K particles moves by at most $\frac{1}{n}$, costing $O(w(\frac{1}{n})) = O(\frac{\log n}{n})$, and the redistributed mass of the last node costs $O(1)$. By the Riemann-sum estimate in the proof of Lemma 10.17(c), $\sum_k \tilde{s}_k P_\sigma(\frac{k}{n}) = n\langle P_\sigma, \sigma \rangle + O_J(\log n)$. Hence [note, (B.18)]:

$$n \sum_k P_\sigma(\tfrac{k}{n})(s_k - \tilde{s}_k) \leq n^2 \langle P_\sigma, \sigma' - \sigma \rangle + O_J(n \log n) \leq n^2\, \mathrm{gap}(\sigma) + O_J(n \log n) \ ,$$

the last step by the definition of the gap, since σ' is feasible.

Step 5. Insert Lemma 10.17(c) for $E_B(\tilde{s})$. All constants depend only on $\|\sigma\|_\infty \leq 4$ and J. □

What just happened. Three inequalities and one approximation. (i) Triangle inequality on the Heine expansion: size $\leq$ best Boltzmann weight $E_B(s)$, up to $e^{O(n \log n)}$ (Lemma 10.11; Cauchy's estimate absorbs the cross-factor corrections). (ii) Concavity: $E_B(s) \leq E_B(\tilde{s}) + \langle \gamma, s - \tilde{s} \rangle$ for a smooth guess $\tilde{s}$ (Lemma 10.9, via the Cayley map). (iii) The linear problem over profiles is at most the linear problem over feasible densities: the gap. The approximation: sums over nodes are n times integrals plus $O(\log n)$ (Lemmas 10.15 and 10.17), which produces $-6\kappa n^2 \log n$ from the h_k, $\kappa^2 n^2 \log n$ from the Vandermonde, and $n^2(F + \mathrm{gap})$ from the potentials.

10.10 The trial density and the bound for $F^\dagger$

To apply Theorem 10.19 we need one explicit σ for each $\kappa \in [2.8, 3]$, with $F[\sigma] + \mathrm{gap}(\sigma)$ as small as possible. The note takes the trial density of [19] (Table 2 there) [note, (5.9)]: σ_0 is the step function on the 30 intervals $[\frac{j}{10}, \frac{j+1}{10})$, $-10 \leq j \leq 19$, with

$$64\,\sigma_0 = 95,\ 112,\ 113,\ 113,\ 112,\ 109,\ 104,\ 95,\ 70,\ 3 \quad \text{on} \quad [-1, -0.9),\ \ldots,\ [-0.1, 0) \ ,$$

$\sigma_0 = 0$ on $[0, 1)$, and $\sigma_0(x) = \sigma_0(1 - x)$ on $[1, 2]$. For $\kappa \in [2.8, 3]$, $\sigma_\kappa = t\,\sigma_0$ with $t = \kappa / m_0$.

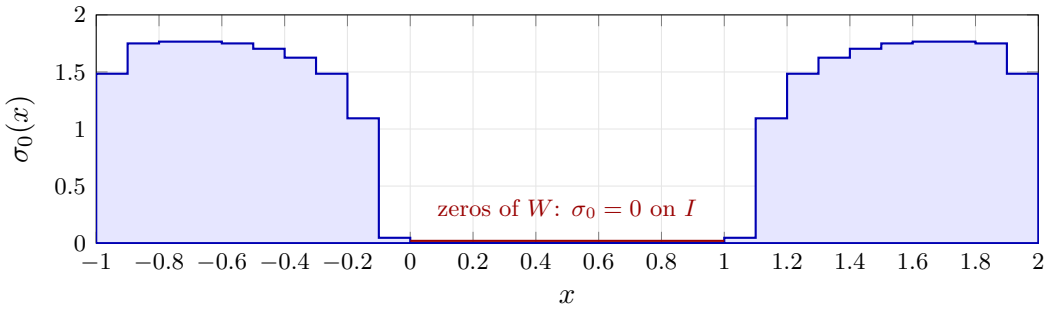


Figure 10.2: The trial density σ_0 [note, (5.9)], symmetric about $x = \frac{1}{2}$. Its mass is $m_0 = \frac{463}{160}$ and its maximum $\frac{113}{64} \approx 1.77$, far below the cap 4.

Example 10.20 (mass and feasibility)**.**

$$m_0 = 2{\cdot}\frac{1}{10}{\cdot}\frac{95+112+113+113+112+109+104+95+70+3}{64} = \frac{2\cdot 926}{640} = \frac{463}{160} = 2.89375$$

So $\int \sigma_\kappa = t\, m_0 = \kappa$. The maximum is $t \cdot \frac{113}{64}$, which is $\frac{791}{463} = 1.7084$ at $\kappa = 2.8$ and $\frac{1695}{926} = 1.8305$ at $\kappa = 3$; so $\max \sigma_\kappa < 1.84 \le 4$ and σ_κ is feasible for κ, with $J = 30$ pieces.

Why σ_0 vanishes on $(0,1)$. The field $\mathcal{V}$ is negative on most of I (Example 10.5: $\mathcal{V}(0.25) = -2.41$, $\mathcal{V}(0.5) = -3.02$), because there the net charge 2 repels the particles, while on O the attracting net charge 4 makes $\mathcal{V}$ as large as 3.95. A particle on I would lose up to about 3.4 units of P compared with one on O (Figure 10.1: $P_t(0.5) = -2.81$ against $P_t \approx 0.6$ on most of O). The self-repulsion spreads the mass over O and pushes it slightly towards the far ends -1 and 2; the drop near $x = 0$ and $x = 1$ is the zeros' repulsion again. In the language of Section 10.4: on I the obstacle $\sigma \ge 0$ is active.

10.10.1 Reduction to a linear problem [note, (E.1)]

Put $A_0 = \langle \sigma_0, \mathcal{V} \rangle$ and $B_0 = \langle \sigma_0, \mathcal{L}\sigma_0 \rangle$. Since F is quadratic and $\mathcal{L}$ linear,

$$F[\sigma_\kappa] = tA_0 + t^2 B_0 \,, \qquad P_{\sigma_\kappa} = \mathcal{V} + 2t\mathcal{L}\sigma_0 =: P_t \,, \qquad \langle P_t, \sigma_\kappa \rangle = tA_0 + 2t^2 B_0 \,.$$

Write $\mathrm{gap}(\sigma_\kappa) = M_\kappa(P_t) - \langle P_t, \sigma_\kappa \rangle$ with $M_\kappa(P) = \sup\{\langle P, \sigma' \rangle : \sigma' \text{ feasible for } \kappa\}$. Then

$$F[\sigma_\kappa] + \mathrm{gap}(\sigma_\kappa) = tA_0 + t^2 B_0 + M_\kappa(P_t) - tA_0 - 2t^2 B_0 = M_\kappa(P_t) - t^2 B_0 \,, \tag{10.10}$$

which is [note, (E.1)]. Everything is reduced to two numbers A_0, B_0 (in fact only B_0 survives) and the linear problem M_κ.

10.10.2 The primitives Φ and Γ [note, (E.2)]

With $\Phi(w) = w\log|w| - w$ as before and $\Gamma(w) = \frac{w^2}{2}\log|w| - \frac{3}{4}w^2$ (and $\Gamma(0) = 0$): $\Gamma'(w) = w\log|w| + \frac{w}{2} - \frac{3}{2}w = w\log|w| - w = \Phi(w)$. So, by (10.3) and then integrating in x with the substitution $u = b_2 - x$ (resp. $a_2 - x$), which reverses orientation,

$$\int_{a_1}^{b_1}\!\!\int_{a_2}^{b_2} \log|x-y|\,\mathrm{d}y\,\mathrm{d}x = \int_{a_1}^{b_1} \big(\Phi(b_2-x) - \Phi(a_2-x)\big)\mathrm{d}x = \big[-\Gamma(b_2-x) + \Gamma(a_2-x)\big]_{x=a_1}^{x=b_1} \,,$$

which is [note, (E.2)]: $\Gamma(b_2-a_1) - \Gamma(b_2-b_1) - \Gamma(a_2-a_1) + \Gamma(a_2-b_1)$. Since σ_0 and the density $2\mathbf{1}_I - 4\mathbf{1}_O$ of $\mathcal{V}$ are step functions, A_0 is a sum of 20×3 such double integrals and B_0 of 20×20 (the 10 zero pieces drop out).

Example 10.21 (A_0, B_0 and F)**.** For one square on the diagonal, $[0,h]^2$, (E.2) gives $\Gamma(h) - 0 - 0 + \Gamma(-h) = 2\Gamma(h) = h^2(\log h - \frac{3}{2})$, finite although the integrand is $-\infty$ on the diagonal; for $h = 0.1$ this is -0.0380258509, and for $[-1,-0.9]\times[1,1.1]$ the closed form agrees with a two-dimensional quadrature (0.0069293874). Summing the closed forms gives

$$A_0 = 9.58350572151844\ , \qquad B_0 = -3.77631679410126\ ,$$

and the same values result from integrating σ_0 times the closed-form potentials numerically; in ball arithmetic at 96 bits, $A_0 \in [9.58350572151844268410092 1 \pm 4.05\cdot 10^{-25}]$ and $B_0 \in [-3.77631679410126379296320 2 \pm 7.78\cdot 10^{-25}]$, in agreement with the note's "about -3.78". $F[\sigma_\kappa]/\log 2 = 8.277362,\ 8.384305,\ 8.478236$ bits at $\kappa = 2.8, 2.9, 3$.

Since $B_0 < 0$, $-t^2 B_0$ is increasing in t. (That $B_0 < 0$ is no contradiction with "self-repulsion": $\log|x-y| < 0$ for $|x-y| < 1$, and most pairs of points of σ_0 on the same side are closer than 1.)

10.10.3 The linear problem: put the mass where the potential is highest

$M_\kappa(P)$ asks: distribute mass κ on $[-1,2]$ with density between 0 and 4 so as to maximize $\int P\sigma'$. The answer is the *bathtub principle* (Lieb and Loss, *Analysis*, Section 1.14): fill with density 4 the set where P is largest, $\{P > c\}$, with c chosen so that $4|\{P > c\}| = \kappa$. Water poured into a bathtub settles at the lowest points; here the mass settles at the highest values of P. The note does not need the exact answer, only an upper bound that a finite computation can evaluate with rigorous error control, and uses weak linear-programming duality.

Discretization. Cut $[-1,2]$ into N_{cell} cells Q_m of length $\delta = 3/N_{\text{cell}}$, and let $\pi_m \geq \sup\{P_t(x) : x \in Q_m,\ t \in [t_a, t_b]\}$, where $t_{a,b} = \kappa_{a,b}/m_0$ for a subinterval $[\kappa_a, \kappa_b]$ of I_i. For feasible σ' let $\omega_m = \int_{Q_m}\sigma' \in [0, 4\delta]$, so $\sum_m \omega_m = \kappa$. For every real c_* [note, (E.3)]:

$$\langle P_t, \sigma'\rangle \leq \sum_m \pi_m\omega_m = c_*\kappa + \sum_m(\pi_m - c_*)\omega_m \leq c_*\kappa + 4\delta\sum_m(\pi_m - c_*)^+\ . \tag{10.11}$$

The first step uses $\sigma' \geq 0$ and $P_t \leq \pi_m$ on Q_m; the equality uses $\sum\omega_m = \kappa$; the last step bounds each term $(\pi_m - c_*)\omega_m$ by 0 if $\pi_m \leq c_*$ (since $\omega_m \geq 0$) and by $(\pi_m - c_*)4\delta$ otherwise (since $\omega_m \leq 4\delta$). The right side no longer depends on σ', so it bounds $M_\kappa(P_t)$.

> **Intuition: what c_* is.** c_* is a "price" for the mass (the Lagrange multiplier of $\int\sigma' = \kappa$). Every unit of mass earns at least c_* by the first term; a cell earns more only if $\pi_m > c_*$, and at most 4δ mass fits in it. Any c_* gives a valid bound; the best one is the threshold of the bathtub filling, for which the bound equals the bathtub value of the discrete problem. The note takes c_* = the value π_m such that the cells with larger values have total length about $\kappa_b/4$.

Uniformity in κ. For $\kappa \in [\kappa_a, \kappa_b]$, $c_*\kappa \leq c_*\kappa_b$ if $c_* \geq 0$, and $c_*\kappa \leq c_*\kappa_b + (\kappa_b - \kappa_a)(-c_*)$ if $c_* < 0$. If $c_* \geq \min_m \pi_m$, then $-c_* \leq -\min_m \pi_m$, and in both cases

$$M_\kappa(P_t) \leq M^+ := c_*\kappa_b + (\kappa_b - \kappa_a)\max(0, -\min_m \pi_m) + 4\delta\sum_m(\pi_m - c_*)^+\ .$$

With (10.10) and $-t^2B_0 \leq -t_b^2 B_0$: $F[\sigma_\kappa] + \text{gap}(\sigma_\kappa) \leq M^+ - t_b^2 B_0$ for all $\kappa \in [\kappa_a, \kappa_b]$.

The cell bounds π_m. $P_t(x)$ is affine in t, so for $t \in [t_a, t_b]$ it is at most $\max(P_{t_a}(x), P_{t_b}(x))$. It is the potential of the density $f_t = 2\mathbf{1}_I - 4\mathbf{1}_O + 2t\sigma_0$, with $\|f_t\|_\infty \leq b_\infty := 4 + 2t_b\max\sigma_0$ (a crude triangle-inequality bound). By Lemma 10.15, for $x \in Q_m$ with midpoint x_m, $|x - x_m| \leq \frac{\delta}{2}$ and $P_t(x) \leq P_t(x_m) + b_\infty w(\frac{\delta}{2})$ (w is increasing). So

$$\pi_m = \max\left(P_{t_a}(x_m), P_{t_b}(x_m)\right) + b_\infty\, w(\tfrac{\delta}{2})$$

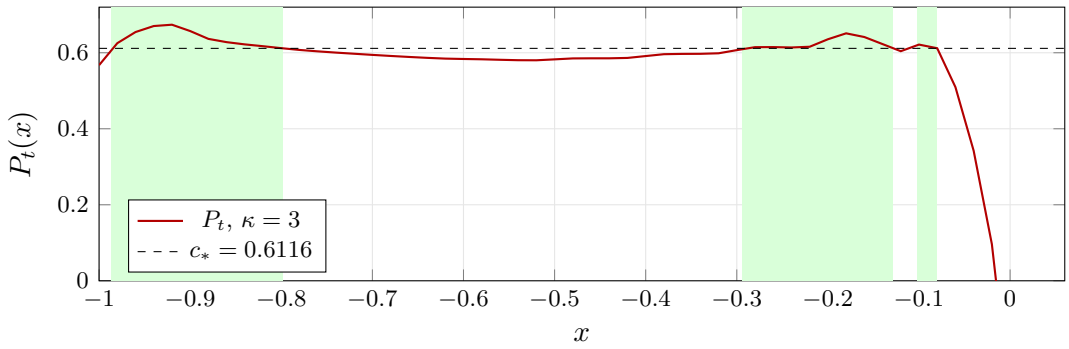


Figure 10.3: P_t on $[-1, 0.06]$ for $\kappa = 3$ (the picture on $[0.94, 2]$ is the mirror image). Shaded: the set $\{P_t > c_*\}$ on which the bathtub puts density 4, of total length $\frac{3}{4}$ on both sides together (fine grid, floating point, no modulus term). The kinks at multiples of 0.1 come from the jumps of σ_0. Sampled every 0.02.

is a valid choice, and it needs only the values of P_t at the midpoints: finite sums of values of Φ by (10.3).

Example 10.22 (the bathtub at $\kappa = 3$)**.** On a grid of 300000 cells, without the modulus term, the threshold is $c_* = 0.611552$ and $\{P_t > c_*\}$ is $[-0.9865, -0.7982] \cup [-0.2936, -0.1289] \cup [-0.1018, -0.0799]$ and its mirror image, of total length $0.75000 = \kappa/4$ (Figure 10.3). The best response to the linearized problem is thus quite different from σ_3 itself (density 4 on three short intervals per side, instead of at most 1.83 spread over O), but because P_t varies only between 0.57 and 0.68 on most of O, its value exceeds $\langle P_t, \sigma_3 \rangle$ by only $\mathrm{gap}(\sigma_3) = 0.120033$ bits.

10.10.4 Ball arithmetic

A floating-point number is a single approximation, and after millions of operations the accumulated rounding error is not tracked, or in which direction, the result is off. For example $0.1 + 0.2 - 0.3$ is $5.55 \cdot 10^{-17}$ in double precision, not 0. *Ball arithmetic* [17] represents every real number by a midpoint and a radius, $[m \pm r]$, meaning "the true value lies in this interval", and every operation (sum, product, log, ...) returns a ball guaranteed to contain the exact result for all inputs in the input balls; the library rounds the midpoint and enlarges the radius to account for the rounding. For instance, at 96 bits, $\frac{1}{3}$ becomes $[0.33333333333333333333333333 \pm 3.55 \cdot 10^{-29}]$ and $3 \cdot \frac{1}{3} - 1$ becomes $[0 \pm 3.16 \cdot 10^{-29}]$, a ball that contains the true 0; and $\Phi(\frac{1}{10}) \in [-0.33025850929940456840179914 55 \pm 5.55 \cdot 10^{-29}]$. If every step of the computation of $(M^+ - t_b^2 B_0)/\log 2$ is done in balls, and the upper end of the final ball is reported, the reported number is an upper bound, provided the ball-arithmetic library and the code of the computation are correct; that code has not been independently reviewed. The note's choices [note, Appendix E]: $N_{\mathrm{cell}} = 36000$, 20 subintervals per I_i, 96 bits; $F_i^\dagger$ is bounded by the largest upper end over the 20 subintervals.

Example 10.23 ([note, Proposition 5.11] in floating point)**.** Following (10.10)–(10.11) with the note's rule for c_* and its π_m, in double precision (not ball arithmetic) and with 20 subintervals per I_i, one obtains these bounds for $F_i^\dagger$ in bits:

I_i	$N_{\mathrm{cell}} = 3000$	$N_{\mathrm{cell}} = 36000$	note	$(F + \mathrm{gap})/\log 2$ at $\kappa_{2,i}$
$[2.80, 2.84]$	8.710048	8.425174	8.425174	8.375754
$[2.84, 2.88]$	8.749092	8.458313	8.458313	8.409151
$[2.88, 2.92]$	8.807569	8.510835	8.510836	8.461981
$[2.92, 2.96]$	8.879471	8.576727	8.576728	8.527634
$[2.96, 3.00]$	8.956701	8.647895	8.647895	8.598270

With the note's grid the double-precision values agree with all five printed bounds to the six printed decimals, the last digit being at most 10^{-6} lower in two cases, which is consistent with the note rounding the upper end of a ball upwards. The coarse grid $N_{\mathrm{cell}} = 3000$ gives bounds about 0.29 to 0.31 bits higher. This is explained by the modulus term: $b_\infty w(\frac{\delta}{2})$ at $\kappa = 3$ is 0.0796 nats for $N_{\mathrm{cell}} = 3000$ and 0.0082 for 36000, and it enters M^+ about $\kappa \approx 3$ times, i.e. $3 \cdot 0.0714/\log 2 \approx 0.31$ bits of difference. The last column is a plain estimate of $\sup_{I_i}(F + \mathrm{gap})$, taken at the right end $\kappa_{2,i}$ (bathtub on 300000 cells, no modulus term): the note's bounds exceed it by about 0.05 bits, the cost of the rigorous cell bounds and of the subintervals.

Proof of Theorem 10.1 [note, Theorem 3.8]. For $K/n = \kappa \in I_i$ apply Theorem 10.19 with $\sigma = \sigma_\kappa$ and $J = 30$, and divide by $\log 2$; $\frac{\log n}{\log 2} = \log_2 n$. By the definition [note, (5.10)], $F_i^\dagger = \frac{1}{\log 2}\sup_{\kappa \in I_i}(F[\sigma_\kappa] + \mathrm{gap}(\sigma_\kappa))$, so $F[\sigma_\kappa] + \mathrm{gap}(\sigma_\kappa) \le F_i^\dagger \log 2$, and [note, Proposition 5.11] bounds $F_i^\dagger$. The implied constant depends only on $J = 30$, not on i or κ. □

Check yourself 10.24. Why may the note use any $c_* \ge \min_m \pi_m$ in M^+, and why does it still need the condition $c_* \ge \min_m \pi_m$ at all?

Answer. (10.11) holds for every real c_*; the choice affects only the quality. The condition is used only for the uniformity in κ: when $c_* < 0$, the term $c_*\kappa$ is largest at $\kappa = \kappa_a$, and $c_*\kappa_a = c_*\kappa_b + (\kappa_b - \kappa_a)(-c_*)$; to replace $-c_*$ by the computable $\max(0, -\min_m \pi_m)$ one needs $-c_* \le -\min_m \pi_m$.

Check yourself 10.25. At a true maximizer σ^* of F, what is $\mathrm{gap}(\sigma^*)$, and what does the bathtub filling of P_{σ^*} look like?

Answer. $\mathrm{gap}(\sigma^*) = 0$: by Proposition 10.7 with $\sigma = \sigma^*$ nothing is lost, and conversely if $\mathrm{gap}(\sigma^*) > 0$, moving a little towards the maximizing σ' would increase F to first order (the quadratic term is of second order). By the obstacle conditions P_{σ^*} equals a constant c on $\{0 < \sigma^* < 4\}$, so the bathtub filling at level c is not unique there, and σ^* itself is one of the optimal fillings.

Summary of the chapter

The size $\log \|\Delta_K\|_1$ is bounded by applying the triangle inequality to the Heine expansion: up to $e^{O(n \log n)}$ it is the largest Boltzmann weight $E_B(s) = \sum_k s_k \log|h_k| + \sum_{k,m} s_k s_m B(k-m)$ of a profile [note, Lemma B.8], where Cauchy's estimate on the polydisc $|w_i| = \frac{1}{10}$ bounds every cross-factor coefficient at once and thereby absorbs the large corrections seen at $n = 1$ in Chapter 9. The kernel $B(d) = \frac{1}{2}\log(1 + d^2)$ is conditionally negative definite by the Cayley-type identity [note, (B.12)] and the series [note, (B.13)] [note, Lemma B.10], so E_B is concave on profiles of fixed mass and lies below its tangent plane at a smooth guess $\tilde{s}$. In the rescaled variable $x = k/n$, with the modulus of continuity $w(\delta)$ [note, Lemma B.14], sums over the nodes become integrals [note, Lemma B.16]: $|h_k| \approx n^{-6n} e^{n\mathcal{V}(k/n)}$ gives $-6\kappa n^2 \log n$, the Vandermonde gives $\kappa^2 n^2 \log n$, and the order-n^2 remainder is the electrostatic energy $F[\sigma] = \langle \sigma, \mathcal{V}\rangle + \langle \sigma, \mathcal{L}\sigma\rangle$ of a density $0 \le \sigma \le 4$ of mass κ in the field $\mathcal{V} = 2\mathcal{L}\mathbf{1}_I - 4\mathcal{L}\mathbf{1}_O$ (zeros repel, poles attract, particles repel each other). [note, Theorem 5.7] bounds the size by $(\kappa^2 - 6\kappa)n^2 \log n + n^2(F[\sigma] + \mathrm{gap}(\sigma))$ for any trial density, and with the trial density σ_0 of [note, (5.9)] (zero on $(0,1)$, mass $\frac{463}{160}$) the bound reduces to $M_\kappa(P_t) - t^2 B_0$ [note, (E.1)], with $B_0 = -3.7763$ from the closed forms [note, (E.2)] and the linear problem M_κ bounded by weak duality [note, (E.3)] ("put density 4 where P_t is highest") in ball arithmetic. A floating-point evaluation with the note's grid reproduces the five bounds of [note, Proposition 5.11] to six decimals.

Carried forward: [note, Theorem 3.8] with $F_i^\dagger \le 8.425174, \ldots, 8.647895$ for the final balance of Chapter 7; the main term $(\kappa^2 - 6\kappa)n^2 \log_2 n$, which cancels against the denominators'

$\kappa(6-\kappa)n^2 \log_2 n$ (Chapter 11); the same weak-duality idea, which returns in the prime sum of Chapter 13.

Chapter 11

Estimate 3a: denominators, the tree bound and the small primes

Where we are. The criterion of Chapter 7 charges, besides the size of the coefficients of $\Delta_K(X)$, their denominators at all primes $p \neq 3$. The third estimate, [note, Theorem 3.10], says that these cost at most

$$\sum_{p\neq 3} \big(-v_p(\Delta_K)\big)^+ \log_2 p \;\le\; \kappa(6-\kappa)\, n^2 \log_2 n + c_i\, n^2 + o(n^2) \qquad (K/n \in I_i)\ , \tag{11.1}$$

where $x^+ = \max(x, 0)$. This chapter covers the first half of its proof, [note, Section 5.2] with the tree part of [note, Appendix B] and the first three proofs of [note, Appendix C]: the bound for a single prime (the *tree bound*, [note, Theorem 5.13]), the number D_k [note, (5.15)], [note, Lemma 5.16], the leaf, small-primes and middle-primes lemmas [note, Lemmas 5.17–5.19], and the way the sum over the primes $p \le \epsilon n$, $\epsilon = \frac{1}{20}$, produces the main term $\kappa(6-\kappa)n^2 \log n$ through Mertens' theorem. The primes $p > \epsilon n$ are the business of Chapters 12 and 13. We use the valuation v_p, the ultrametric inequality and the Gauss valuation of polynomials (Chapter 2); the harmonic sums $\mathrm{HS}_3(k, M)$ [note, (2.14)] (Chapter 4); the weight W, the leading coefficients h_k, the Taylor coefficients $H_k[b]$ and the local constants $c_{k,a}$ (Chapter 5); the minors $\det C_k[R]$ and the Heine expansion [note, Proposition 5.1] (Chapter 9).

11.1 What "the denominators of Δ_K" are

Recall (Chapter 6) that $\Delta_K(X) = \sum_{i\le K} d_i X^i$ is a polynomial with rational coefficients d_i. To apply the criterion one clears its denominators: one multiplies by the least common multiple $\mathcal{D}$ of the denominators of $d_0, \dots, d_K$. A prime p enters $\mathcal{D}$ with the exponent $\max_i(-v_p(d_i))$ if this is positive. In the language of Chapter 2 this is $-v_p(\Delta_K)$, where v_p on polynomials is the *Gauss valuation*, the minimum of the valuations of the coefficients. So

$$\log_2 \mathcal{D} = \sum_p \big(-v_p(\Delta_K)\big)^+ \log_2 p\ ,$$

and (11.1) is this sum without the prime 3, whose contribution is part of the 3-adic bookkeeping of Chapters 7 and 8.

Example 11.1 (the actual denominators)**.** Compute $\Delta_K(X)$ exactly from [note, Definition 2.23] for $n = 3, 5, 7$ and $K = 3n$ (so $\kappa = 3$, in the last interval $I_5 = [2.96, 3]$), and form the lcm of the coefficient denominators. After all primes $\le 6n$ are divided out, the cofactor is 1 in all three cases: no prime above $6n$ divides a denominator.

n	lcm of the denominators of $\Delta_{3n}(X)$	bits at $p \neq 3$	$9n^2 \log_2 n$	$9n^2 \log_2 n + c_5 n^2$
3	$2^{183}\,3^{189}\,5^{45}\,7^{35}$	385.7	128.4	413.8
5	$2^{381}\,3^{639}\,5^{96}\,7^{97}\,11^{65}\,13^{36}$	1234.3	522.4	1315.3
7	$2^{740}\,3^{1301}\,5^{166}\,7^{131}\,11^{111}\,13^{98}\,17^{68}\,19^{36}$	2670.7	1238.0	2792.0

Here $\kappa(6-\kappa) = 9$, and the last column uses the note's bound $c_5 \leq 31.713600$ [note, Proposition 5.40]. Three things are visible. First, the exponents decrease with p, but at these small n much more slowly than the leading term $K(6n+4-K)/(p-1)$ of [note, Lemma 5.18] below: for $n = 7$ that term is $525/(p-1)$, i.e. 525 at $p = 2$ and 52.5 at $p = 11$, against the true 740 and 111; at small n the lower-order terms are as large as the main term. Second, no prime $p > 3n$ occurs at all, although the integers $3k - 3j - r$ in the local constants go up to $6n$: these primes "cost nothing", which the note asserts for large n in [note, Lemma 5.31] (Chapter 13) using the cancellation of Chapter 12. Third, the bits are close to the asymptotic right side of (11.1). At $n \leq 7$ this closeness should not be read as a confirmation: the $o(n^2)$ term is not small here (Section 11.11).

The 3-part is large too (3^{1301} for $n = 7$), but it is not part of (11.1).

11.2 Valuations as counts

Everything in this chapter rests on one identity. For a nonzero integer x and a prime p,

$$v_p(x) = \#\{j \geq 1 :\ p^j \mid x\}\ , \tag{11.2}$$

because $p^j \mid x$ holds exactly for $j = 1, \ldots, v_p(x)$. For example, for $x = 40 = 2^3 \cdot 5$: $2 \mid 40$, $4 \mid 40$, $8 \mid 40$, $16 \nmid 40$, so the count is $3 = v_2(40)$; likewise $v_5(250) = 3$.

Intuition. Apply (11.2) to a difference $x = k - m$. The statement "$p^j \mid k - m$" says that k and m are in the same residue class modulo p^j. So $v_p(k-m)$ counts the moduli $p, p^2, p^3, \ldots$ for which k and m are still together. A sum $\sum v_p(k-m)$ over many pairs becomes a sum over the levels j of the number of pairs that are together at level j. This turns products of differences, which appear in the Heine expansion, into a counting problem on a tree.

11.3 The tree of residue classes

Fix $p \neq 3$ (in this chapter $p = 2$ is allowed). For $j \geq 0$ group the nodes $k \in \mathcal{N} = \{-n, \ldots, 2n\}$ by their residue modulo p^j; for $j = 0$ there is one group, all nodes. Each class modulo p^{j+1} lies inside one class modulo p^j, so the classes form a tree: the root is $\mathcal{N}$, the children of a class c modulo p^j are the nonempty classes modulo p^{j+1} inside it. Since the nodes are $3n+1$ consecutive integers, two different nodes differ by at most $3n$, so once $p^j > 3n$ every class is a single node, a *leaf*. For a class c and a profile s (the occupation numbers of Chapter 9, $0 \leq s_k \leq 4$, $\sum_k s_k = K$) we write $S_c = \sum_{k \in c} s_k$.

By (11.2), $v_p(k-m)$ is the number of levels $j \geq 1$ at which k and m share a class, the depth of their lowest common ancestor. For $n = 3$ and $p = 2$ (Figure 11.1) the deepest level with a class of two or more nodes is $j = 3$ ($2^3 = 8 \leq 9 < 16$; the classes $\{-2, 6\}$ and $\{-3, 5\}$ modulo 8), and for $p = 5$ and $n = 5$ (Figure 11.2) it is $j = 1$. The *single-level* primes of Chapter 12 ($p \geq 5$, $p^2 > 6n$) have a one-level tree; the converse fails when $3n < p^2 \leq 6n$ (e.g. $n = 5$, $p = 5$), because the integers $3k - 3j - r$ of the local constants reach $6n$.

Check yourself 11.2. For $n = 7$ ($\mathcal{N} = \{-7, \ldots, 14\}$) and $p = 2$, how many levels $j \geq 1$ have a class with two or more nodes, and what is $\eta_2(0)$?

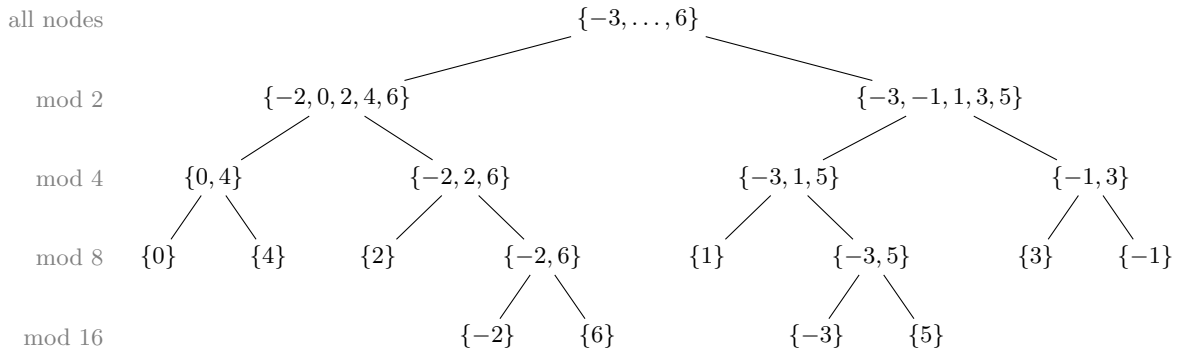


Figure 11.1: The tree of residue classes of the nodes $\mathcal{N} = \{-3, \dots, 6\}$ ($n = 3$) for $p = 2$. A node becomes a leaf at the first level where its class has one element. For two nodes $k \neq m$, $v_2(k-m)$ is the level of their lowest common class: -2 and 6 separate at level 4 and $v_2(8) = 3$; 0 and 4 separate at level 3 and $v_2(4) = 2$; 0 and 1 separate at level 1 and $v_2(1) = 0$.

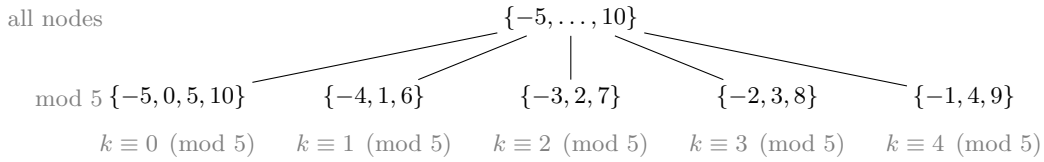


Figure 11.2: The same for $n = 5$ ($\mathcal{N} = \{-5, \dots, 10\}$) and $p = 5$. Since $25 > 3n = 15$, every class modulo 25 is a single node: the tree has one level below the root, and $v_5(k-m) \in \{0, 1\}$ for all pairs of nodes.

Answer. Two nodes can share a class modulo 2^j only if $2^j \leq 21$, so the levels are $j = 1, 2, 3, 4$ ($16 \leq 21 < 32$); the four level sums $184 + 78 + 26 + 12$ in Example 11.7 below are exactly these. For the node 0 the partners at distance 8 ($m = 8$) exist and those at distance 16 do not ($16 \notin \mathcal{N}$, $-16 \notin \mathcal{N}$), so $\eta_2(0) = 3$.

11.4 The local data of a node: η_p, e_p, f_p

Recall from Chapter 9 the shape of a term of the Heine expansion [note, (5.2)]: it is $\operatorname{coef}_\lambda(s) \prod_k M_{k,\lambda_k}$, where $\operatorname{coef}_\lambda(s) \in \mathbb{Z}$ is a coefficient of the cross factor Q_s [note, (5.3)] and the local factor M_{k,λ_k} is an integer combination of the minors $\det C_k[R]$, $|R| = s_k$, with $\sum R - \binom{s_k}{2} = |\lambda_k|$. Here $C_k[R] = [c_{k,R_b+b'}]_{b,b'<|R|}$ is the submatrix of the 4×4 node matrix $C_k = [c_{k,a+b}]$ with row set $R \subseteq \{0, 1, 2, 3\}$ and the first $|R|$ columns, and the local constants $c_{k,a}(X) = \beta_{k,a} + X\alpha_{k,a}$ are the polynomials of [note, (2.21)] (Chapter 5). We need three numbers per node, defined in [note, Section 5.2].

Definition 11.3 ([note, Section 5.2, (5.12)])**.** For a node k let $\eta_p(k) = \max_{m \in \mathcal{N} \setminus \{k\}} v_p(k-m)$, the last level at which k still shares its class with another node (it becomes a leaf at level $\eta_p(k) + 1$). For $0 \leq s \leq 4$ and $\ell \geq 0$ let

$$e_p(k, s, \ell) = \max \Big\{ -v_p\big(\det C_k[R]\big) : \; R \subseteq \{0, 1, 2, 3\}, \; |R| = s, \; \sum R - \tbinom{s}{2} = \ell \Big\}$$

($-\infty$ if there is no such R or all these minors vanish), with v_p the Gauss valuation in X. Let $f_p(k, 0) = 0$ and, for $s \geq 1$, $f_p(k, s) = \max_{0 \leq \ell \leq s(4-s)} \big(e_p(k, s, \ell) + \ell\, \eta_p(k)\big)$.

Intuition. $e_p(k, s, \ell)$ is the worst denominator (as a power of p) that a minor of the node can produce when the node holds s variables and receives ℓ "units of degree" from the

cross factor. The index $\ell = |\lambda_k|$ counts how many powers of the variables w_i of this node the cross factor supplies; we will see in the proof of the tree bound that each such unit is paid for by losing one factor of a node difference $d = k - m$, which can cost up to $\eta_p(k)$ powers of p. So $f_p(k, s)$ is the worst local loss of the node k holding s variables, with the price of the units already included.

Example 11.4 ($n = 5$, $p = 2$, the node $k = 1$)**.** The nodes are $-5, \dots, 10$. Every node has a partner at distance 8 inside $\mathcal{N}$ and none at distance 16, so $\eta_2(k) = 3$ for all k. The 15 minors $\det C_1[R]$, computed exactly as polynomials in X, have the values $-v_2$

R	0	1	2	3	01	02	03	12	13	23	012	013	023	123	0123
ℓ	0	1	2	3	0	1	2	2	3	4	0	1	2	3	0
$-v_2(\det C_1[R])$	32	29	26	23	56	54	52	51	49	46	70	74	72	69	92

So $e_2(1, 2, 2) = \max(52, 51) = 52$, and $e_2(1, 3, 1) = 74$ exceeds $e_2(1, 3, 0) = 70$. Then $f_2(1, 1) = \max(32, 29 + 3, 26 + 6, 23 + 9) = 32$, and in all $f_2(1, s) = 0, 32, 58, 78, 92$ for $s = 0, \dots, 4$ (e.g. $f_2(1, 2) = \max(56, 54 + 3, 52 + 6, 49 + 9, 46 + 12) = 58$). At the end node $k = 10$: $f_2(10, s) = 0, 35, 64, 87, 104$.

11.5 The tree bound

Theorem 11.5 (tree bound; [note, Theorem 5.13], after [19])**.** *For every prime p,*

$$-v_p(\Delta_K) \le T_p := \max_s \Big[\sum_{k \in \mathcal{N}} f_p(k, s_k) - \sum_{j \ge 1} \sum_{c \bmod p^j} \Big(S_c^2 - \sum_{k \in c} s_k^2 \Big) \Big] , \tag{11.3}$$

the maximum over the profiles s (with $s_k \le 4$, $\sum s_k = K$), c running over the classes of nodes modulo p^j.

Intuition. Think of K particles placed on the leaves of the tree. Each occupied node charges its local loss $f_p(k, s_k)$, and every class with several particles in it gives a refund of $S_c^2 - \sum_{k \in c} s_k^2$, twice the number of pairs of particles that sit in the class at *different* nodes. The refund is paid at every level the pair shares: particles at nodes p^j apart are refunded j times. So the bound is a "free energy" on the tree: local losses push for spreading, but spreading into nodes that are p-adically close earns refunds. The maximizing profile is the worst case.

11.5.1 Proof, following [note, Appendix B]

Step 1 (B.4): the ultrametric inequality. By the Heine expansion [note, (5.2)], Δ_K is a sum of terms $\mathrm{coef}_\lambda(s) \prod_k M_{k,\lambda_k}$. The Gauss valuation satisfies $v_p(F + G) \ge \min(v_p(F), v_p(G))$ and $v_p(FG) \ge v_p(F) + v_p(G)$ (Chapter 2), so

$$v_p(\Delta_K) \ge \min_{s,\lambda} \Big[v_p\big(\mathrm{coef}_\lambda(s)\big) + \sum_k v_p\big(M_{k,\lambda_k}\big) \Big] . \tag{11.4}$$

It suffices to bound each bracket from below.

Step 2: the local factors. If $s_k = 0$, then $M_{k,\emptyset} = 1$ has valuation $0 = -f_p(k, 0)$. If $s_k \ge 1$, M_{k,λ_k} is an integer combination of minors $\det C_k[R]$ with $|R| = s_k$ and $\sum R - \binom{s_k}{2} = |\lambda_k|$; integers have $v_p \ge 0$, so by the ultrametric inequality

$$v_p(M_{k,\lambda_k}) \ge \min_R v_p(\det C_k[R]) \ge -e_p(k, s_k, |\lambda_k|) .$$

Step 3: the cross factor, with the units of degree. Recall [note, (5.3)]: $Q_s(w) = \prod (d + w_i - w_{i'})^2$ over the *cross pairs* $i < i'$ with $\iota(i) \neq \iota(i')$, where $d = \iota(i') - \iota(i) \neq 0$ is the difference of the two nodes. Expand each factor in two stages:

$$(d + w_i - w_{i'})^2 = \sum_{e=0}^{2} \binom{2}{e} d^{2-e} (w_i - w_{i'})^e , \qquad (w_i - w_{i'})^e = \sum_{\alpha=0}^{e} \binom{e}{\alpha} (-1)^{e-\alpha} w_i^{\alpha} w_{i'}^{e-\alpha} .$$

For one pair with $d = 4$ this is $16 + 8w_1 - 8w_2 + w_1^2 - 2w_1w_2 + w_2^2$: the monomial w_1w_2 has $e = 2$, $\alpha = 1$, and its coefficient -2 has lost both factors 4 of the constant term 16. In general, multiplying out the product over all cross pairs, each monomial of Q_s is a sum of contributions, one for each choice of (e, α) at every pair, and each contribution is an integer times $\prod_{\text{pairs}} d^{2-e}$. Its valuation is at least

$$\sum_{\text{pairs}} (2 - e)\, v_p(d) = 2 \sum_{\text{pairs}} v_p(d) - \sum_{\text{pairs}} e\, v_p(d) .$$

Now the bookkeeping. Call the exponent e at a pair the number of *units of degree* that the pair hands out; α of them go to the variable w_i and $e - \alpha$ to $w_{i'}$. Each unit costs $v_p(d)$ in the sum $\sum e\, v_p(d)$. A unit that goes to a variable of the node k comes from a pair whose d is a difference $k - m$ with another node m, so it costs $v_p(d) \leq \eta_p(k)$. The node k receives in total the degree of the monomial in its own variables, which for a monomial in the orbit λ is $|\lambda_k|$. Hence $\sum_{\text{pairs}} e\, v_p(d) \leq \sum_k |\lambda_k|\, \eta_p(k)$. Finally, between the nodes $k < m$ there are $s_k s_m$ cross pairs, all with $|d| = m - k$. Since $\operatorname{coef}_\lambda(s)$ is a sum of such contributions, the ultrametric inequality gives [note, (B.5)]

$$v_p(\operatorname{coef}_\lambda(s)) \geq 2 \sum_{k<m} s_k s_m\, v_p(k - m) - \sum_k |\lambda_k|\, \eta_p(k) . \tag{11.5}$$

Example 11.6 ((B.5) on one cross factor)**.** Take $n = 7$, $p = 2$ and the profile with $s_0 = 1$, $s_4 = 2$, $s_8 = 1$ ($K = 4$, $\iota = (0, 4, 4, 8)$). There are five cross pairs, with $d = 4, 4, 8, 4, 4$, so the constant term of Q_s is $4^8 \cdot 8^2 = 2^{22}$, and $2 \sum s_k s_m v_2(k - m) = 2(2 \cdot 2 + 1 \cdot 3 + 2 \cdot 2) = 22$. All three nodes have $\eta_2 = 3$, so (11.5) reads $v_2(\text{coef}) \geq 22 - 3\deg$. Expanding Q_s (580 monomials), one finds the bound satisfied by every monomial, with equality for 3 of them. Examples: w_1 (one unit to the node 0): coefficient $5242880 = 2^{20} \cdot 5$, $v_2 = 20 \geq 19$; w_1^2: 2686976, $v_2 = 16 = 16$ (equality); w_4^3: -720896, $v_2 = 16 \geq 13$; $w_1w_2w_3w_4$: $131072 = 2^{17}$, $v_2 = 17 \geq 10$. The coefficient of w_2 alone is 0: the two cross pairs that contain w_2, with the nodes 0 and 8, contribute $-\frac{2}{4}$ and $+\frac{2}{4}$ times the constant term.

Step 4: combination. Put $\ell_k = |\lambda_k|$; by [note, Proposition 5.1](a), $\ell_k \leq s_k(4 - s_k)$. Adding Step 2 and (11.5), every bracket of (11.4) is at least

$$-\sum_k \big(e_p(k, s_k, \ell_k) + \ell_k\, \eta_p(k)\big) + 2 \sum_{k<m} s_k s_m\, v_p(k - m) \;\geq\; -\sum_k f_p(k, s_k) + 2 \sum_{k<m} s_k s_m\, v_p(k - m) ,$$

since $f_p(k, s_k)$ is the maximum of $e_p + \ell\eta_p$ over the allowed ℓ. Taking the minimum over s and λ and changing sign,

$$-v_p(\Delta_K) \leq \max_s \Big[\sum_k f_p(k, s_k) - 2 \sum_{k<m} s_k s_m\, v_p(k - m) \Big] .$$

Step 5: the identity (B.6). It remains to rewrite the cross term on the tree. Using (11.2) and exchanging the sums,

$$\begin{aligned} 2 \sum_{k<m} s_k s_m\, v_p(k - m) &= \sum_{k \neq m} s_k s_m \sum_{j \geq 1} [p^j \mid k - m] = \sum_{j \geq 1} \sum_{c \bmod p^j} \sum_{\substack{k,m \in c \\ k \neq m}} s_k s_m \\ &= \sum_{j \geq 1} \sum_{c \bmod p^j} \Big(S_c^2 - \sum_{k \in c} s_k^2 \Big) . \end{aligned} \tag{11.6}$$

The first equality counts each unordered pair twice; the second groups the pairs (k,m) with $p^j \mid k-m$ by their common class c modulo p^j; the third is $S_c^2 = \sum_{k,m\in c} s_k s_m$ minus the diagonal $k=m$. The sum over j is finite, because the inner sum vanishes once $p^j > 3n$. Inserting (11.6) gives (11.3). The note adds that nothing in the argument uses that p is odd. □

Example 11.7 ((B.6) on one profile)**.** For $n=7$, $p=2$ and the profile $s = (0,1,1,1,1,2,1,0,0,1,0,0,0,0,4,1,2,2,1,1,2,0)$ on the nodes $-7,\dots,14$ ($K=21$), the left side of (11.6) is 300, and the right side, level by level, is $184+78+26+12=300$ (levels $j=1,\dots,4$; $2^5=32>21$). For the same profile at $p=5$ and $p=7$ the tree has one level ($25>21$), and both sides are 62 and 26, respectively.

The tree bound in one paragraph. The ultrametric inequality reduces $v_p(\Delta_K)$ to the worst term of the Heine expansion. In a term, the local factors lose at most $e_p(k,s_k,|\lambda_k|)$ each, and the integer cross factor is divisible by the product of the squared node differences, except that each unit of degree it hands to a node k removes one difference, at a cost of at most $\eta_p(k)$. Absorbing this cost into f_p leaves $\sum_k f_p(k,s_k)$ minus the p-adic size of $\prod_{k<m}(k-m)^{2s_k s_m}$, and (11.2) rewrites the latter as a sum over the levels of the tree of the number of pairs of particles that share a class.

Evaluating T_p exactly. The maximum in (11.3) runs over a huge set of profiles, but it has a tree structure that makes it cheap. Let J be the deepest level with $p^J \le 3n$. On a level $j>J$ all classes are single nodes and contribute 0, so the objective is $\sum_k \big(f_p(k,s_k)+Js_k^2\big) - \sum_{j=1}^{J}\sum_c S_c^2$. For each class c one computes, for every total S, the best value $V_c(S)$ of its subtree, from those of its children by a max-plus convolution and the subtraction of S^2. This recursion over the tree is not part of the note. For $n=3$, $K=9$ a direct enumeration of all 41470 profiles (with the left side of (11.6) as the cross term) gives the same maxima: $T_2=185$, $T_5=51$, $T_7=35$. For $p=2$ the maximizer is $s_4=1$, $s_5=s_6=4$: local losses $f_2(4,1)+f_2(5,4)+f_2(6,4) = 17+88+88 = 193$, refund $2\cdot(1\cdot 4\cdot v_2(2)) = 8$. The true value is $-v_2(\Delta_9) = 183 \le 185$.

11.6 The number D_k

The local losses $f_p(k,s)$ come from the local constants, and these are built from the Taylor coefficients $H_k[b] = [z^b]\widetilde{W}_k(z)$ of $\widetilde{W}_k(z) = z^4 W(-k+z)$ and from harmonic sums. Recall (Chapter 5, [note, (2.17)–(2.18)]) that $h_k = H_k[0] = \widetilde{W}_k(0)$. Writing W around the node k ($y=-k+z$), the nonzero roots and poles of $\widetilde{W}_k$ are:

- $d = k-j-\frac{r}{3} = \frac{3k-3j-r}{3}$ for $0\le j<n$, $r\in\{1,2\}$: zeros of order 3;
- $d = k-\frac{n}{2} = \frac{2k-n}{2}$: a zero of order 1;
- $d = k-m$ for the other nodes $m\in\mathcal{N}\setminus\{k\}$: poles of order 4.

With e_d the order ($+3$, $+1$, -4), $\widetilde{W}_k(z) = h_k\prod_d (1-z/d)^{e_d}$, since both sides are rational functions with the same zeros and poles and the same value at $z=0$. Then [note, (5.15)] is

$$D_k := -v_p(h_k) = 4\sum_{m\neq k} v_p(k-m) - 3\sum_{0\le j<n,\ r=1,2} v_p(3k-3j-r) - v_p\Big(\frac{2k-n}{2}\Big)\,. \qquad (11.7)$$

Term by term. By [note, (2.18)], $h_k = \frac{(\frac{n}{2}-k)\prod_{j,r}(j+\frac{r}{3}-k)^3}{\prod_{m\neq k}(m-k)^4}$, and v_p turns the product into a sum. The poles give $+4v_p(k-m)$ each: only the poles at the nodes $m\equiv k \pmod p$ (the "partners" of k) count, with multiplicity given by how deep the partner sits in the tree. A triple zero gives $-3v_p(j+\frac{r}{3}-k) = -3v_p(3k-3j-r)$, because $v_p(3)=0$ for $p\neq 3$; it counts only if $3j+r\equiv 3k \pmod p$. The simple zero gives $-v_p(\frac{2k-n}{2})$. For odd p this is $-v_p(2k-n)$,

nonzero only if $p \mid 2k-n$. For $p=2$, $2k-n$ is odd (as n is odd), so $v_2(\frac{2k-n}{2}) = -1$ and the term is $+1$: the factor $\frac{1}{2}$ in the zero $y = -\frac{n}{2}$ is itself a denominator.

Example 11.8 (D_k by hand)**.** $n=5$, $p=2$, $k=1$. The even differences $k-m$ are $6,4,2,-2,-4,-6,-8$ (for $m=-5,-3,-1,3,5,7,9$), with $v_2 = 1,2,1,1,2,1,3$, sum 11. The even numbers $3k-3j-r = 3-(3j+r)$ are $2,-2,-4,-8,-10$, with $v_2 = 1,1,2,3,1$, sum 8. So $D_1 = 4\cdot 11 - 3\cdot 8 + 1 = 21$, and indeed $h_1 = \frac{1331}{711368217323163559015623221575 6800}$ has $v_2(h_1) = -21$. For $p=5$ and $k=0$: three partners $m=-5,5,10$ $(4\cdot 3)$, two zeros $3j+r \in \{5,10\}$ $(3\cdot 2)$ and $5 \mid 2k-n=-5$, so $D_0 = 12-6-1 = 5$.

For $n = 3,5,7$, all primes $p \le 6n$, $p \neq 3$, and all nodes (468 cases), the counting formula (11.7) agrees with $-v_p(h_k)$ computed from the closed form [note, (2.18)] and with $-v_p(h_k)$ computed from the power series of $\widetilde{W}_k$. Some rows:

(n,p)	D_k for $k = -n,\dots,2n$
$(5,2)$	$15,18,18,12,12,21,21,18,18,21,21,12,12,18,18,15$
$(5,5)$	$2,-1,2,2,2,5,2,2,2,2,5,2,2,2,-1,2$
$(5,7)$	$5,5,1,-2,-3,-2,1,5,5,1,-2,-3,-2,1,5,5$
$(7,7)$	$5,2,2,2,2,2,2,5,2,2,2,2,2,2,5,2,2,2,2,2,2,5$

D_k can be negative, i.e. p can divide h_k. At $n=5$, $p=7$, the node $k=-1$ has one partner, $m=6$ (contribution 4), two triple zeros with $7 \mid 3k-3j-r$, namely $3j+r = 4,11$ with $3k-3j-r = -7,-14$ (contribution -6), and $7 \mid 2k-n=-7$ (contribution -1): $D_{-1} = -3$, as in the table. In this row the negative values occur at $k=-2,-1,0$ and $k=5,6,7$.

11.7 Lemma 5.16: the Taylor coefficients and the harmonic sums

Lemma 11.9 ([note, Lemma 5.16])**.** *Let $\mu_k = \max_d v_p(d)$ over the nonzero roots and poles d of $\widetilde{W}_k$. Then $v_p(H_k[b]) \ge -D_k - b\mu_k$ for $b \ge 0$, and $v_p(\mathrm{HS}_3(k,M)) \ge -M \max_u v_p(u)$, the maximum over the u in [note, (2.14)].*

> **Intuition.** h_k carries the whole "static" denominator p^{D_k} of the node; each further Taylor order b can bring at most one more factor d^{-1} per order, and the worst d has valuation μ_k. So the denominators grow at most linearly in b, with slope μ_k.

Proof. One factor. For an integer e (positive or negative), $[z^b](1-z/d)^e = \binom{e}{b}(-1)^b d^{-b}$, and the generalized binomial coefficient $\binom{e}{b} = \frac{e(e-1)\cdots(e-b+1)}{b!}$ is an integer also for negative e: $\binom{-4}{b} = (-1)^b\binom{b+3}{3}$. For example, for a pole $d=4$ of order 4: $[z^b](1-z/4)^{-4} = 1, 1, \frac{5}{8}, \frac{5}{16}$ $(b=0,\dots,3)$, that is $\binom{b+3}{3}4^{-b}$; for a triple zero $d=-\frac{2}{3}$: $1, \frac{9}{2}, \frac{27}{4}, \frac{27}{8}$. So the coefficient of z^b has valuation at least $-b\,v_p(d)$ when $v_p(d) \ge 0$, and at least $+b \ge -b\mu_k$ for the one root $d = \frac{2k-n}{2}$ with $v_2(d) = -1$ at $p=2$ (here $\mu_k \ge 0$ because the poles $k-m$ are integers). *The product.* The coefficient of z^b in $\prod_d (1-z/d)^{e_d}$ is a sum over $b = \sum_d b_d$ of products of the coefficients of z^{b_d}; each product has valuation at least $-\sum_d b_d\mu_k = -b\mu_k$, and so does the sum (ultrametric inequality). Multiplying by h_k adds $v_p(h_k) = -D_k$. *The harmonic sums.* Every term $(3/u)^M$ of $\mathrm{HS}_3(k,M)$ has $v_p = -M\,v_p(u)$ (as $p \neq 3$), which is $\ge -M \max_u v_p(u)$; the ultrametric inequality does the rest. □

The remark after (2.14). Chapter 4 noted that after [note, (2.14)] the note says that the terms of HS_3 with $p \mid u$ have $v_p = -M$, while the exact value is $-M\,v_p(u)$. The lemma uses the exact form, $\max_u v_p(u)$, and so does the leaf lemma below, which bounds $\max_u v_p(u)$ by $\mathfrak{l}_p$.

At single-level primes ($p^2 > 6n$) the two agree. For instance, at $p = 2$: $v_2(\mathrm{HS}_3(2,3)) = -6 = -3 \cdot v_2(4)$, $v_2(\mathrm{HS}_3(3,3)) = -9 = -3 \cdot v_2(8)$, $v_2(\mathrm{HS}_3(6,4)) = -16 = -4 \cdot v_2(16)$; the lemma is sharp in these cases, and a bound $-M$ would be false.

For $n = 5$ and $n = 7$, all $p \le 6n$, $p \ne 3$, all nodes and $b = 0, \dots, 3$ (576 and 1056 nonzero cases) the bound $v_p(H_k[b]) \ge -D_k - b\mu_k$ holds, with equality in 546 and 1010 cases. For instance $n = 5$, $p = 2$, $k = 1$ ($\mu_1 = 3$, from $d = -8$): $v_2(H_1[b]) = -21, -24, -27, -30$, exactly the bound.

11.8 The leaf lemma

Let $\mathfrak{l}_p = \lceil \log_p(6n) \rceil$, the smallest ℓ with $p^\ell \ge 6n$; e.g. $\mathfrak{l}_2 = 5$ for $n = 5$ ($2^5 = 32 \ge 30$) and $\mathfrak{l}_2 = 6$ for $n = 7$. The leaf lemma and the lemmas on small and middle primes that follow are, as the note states, the analogues in its setting of three statements of [19].

Lemma 11.10 (leaf lemma; [note, Lemma 5.17]). *For every node k and $1 \le s \le 4$, $f_p(k,s) \le sD_k + 9s\mathfrak{l}_p$.*

Intuition. A node with s variables loses at most s copies of its static denominator D_k, plus a correction of size $\mathfrak{l}_p \approx \log_p(6n)$ per variable for the Taylor orders, the harmonic sums and the units of degree. The first term is the one that matters after summing over p: it is of order n per variable; the correction is of order $\log n$.

Proof, following [note, Appendix C]. (a) All valuations are at most $\mathfrak{l}_p$. The integers whose valuations enter are nonzero and of absolute value below $6n \le p^{\mathfrak{l}_p}$: $|k - m| \le 3n$; $3k - 3j - r \in [-6n+1, 6n-1]$, since $k \in [-n, 2n]$ and $3j + r \in [1, 3n-1]$; the u of [note, (2.14)] satisfy $|u| < 3|k| \le 6n$; and $|n - 2k| \le 3n$. Hence $\mu_k \le \mathfrak{l}_p$ (at $p = 2$ the root $\frac{2k-n}{2}$ has valuation -1, below $\mathfrak{l}_p$), $\eta_p(k) \le \mathfrak{l}_p$, and by Lemma 11.9 $v_p(\mathrm{HS}_3(k,M)) \ge -M\mathfrak{l}_p$. *(b) The local constants.* By [note, (2.21)], $\beta_{k,a} = \sum_{i=1}^{4-a} i(i+1)\mathrm{HS}_3(k, i+2)H_k[4-i-a]$. The term i has valuation at least $-(i+2)\mathfrak{l}_p - D_k - (4-i-a)\mathfrak{l}_p = -D_k - (6-a)\mathfrak{l}_p$, independently of i. And $\alpha_{k,a} = -2916H_k[1-a]$ ($a \le 1$) has valuation at least $-D_k - (1-a)\mathfrak{l}_p \ge -D_k - (6-a)\mathfrak{l}_p$, because $2916 = 2^2 \cdot 3^6$ is an integer. The weights $i(i+1)$ are integers too. So $v_p(c_{k,a}) \ge -D_k - (6-a)\mathfrak{l}_p$ for $a \le 3$. *(c) The minors.* A minor $\det C_k[R]$ is a signed sum of products $\prod_b c_{k,m_b}$ of s local constants with all $m_b \le 3$, so each product has valuation at least $-sD_k - \sum_b (6 - m_b)\mathfrak{l}_p \ge -sD_k - 6s\mathfrak{l}_p$. Hence $e_p(k,s,\ell) \le sD_k + 6s\mathfrak{l}_p$. *(d) The units.* $\ell\,\eta_p(k) \le s(4-s)\mathfrak{l}_p \le 3s\mathfrak{l}_p$, since $4 - s \le 3$ for $s \ge 1$. Adding (c) and (d) gives the claim. □

For $n = 3, 5, 7$, all $p \le 6n$, $p \ne 3$, all nodes and $s = 1, \dots, 4$ (228, 558, 1032 cases with $f_p > -\infty$) the lemma holds, with a smallest margin of 12. In Example 11.4: $f_2(1,s) = 32, 58, 78, 92$ against $sD_1 + 9s\mathfrak{l}_2 = 66, 132, 198, 264$. The lemma is crude, as intended: the margin grows with s. At $n = 7$, $p = 2$ the excess $f_2(k,s) - sD_k$ is at most 56, against $9s\mathfrak{l}_2 = 216$ for $s = 4$.

11.9 The small primes

Lemma 11.11 (small primes; [note, Lemma 5.18]). *For every prime $p \ne 3$, $T_p \le \dfrac{K(6n+4-K)}{p-1} + 9K\mathfrak{l}_p + 150n + K$.*

Intuition. After the leaf lemma, the local loss of a node is $s_k D_k$, and D_k is itself a sum over the levels j of the tree: "4× the number of other nodes in my class modulo p^j, minus 3× the number of zeros in it". So the whole objective of the tree bound splits into one quadratic problem per level. On a level with classes c, each class has a "net charge" B_c

(poles minus zeros, about $(6n+4)/q$) and the particles in it gain S_cB_c and pay S_c^2. The maximum of $\sum_c(S_cB_c - S_c^2)$ with $\sum S_c = K$ is found as in electrostatics or statistical mechanics with a chemical potential: price the constraint by a Lagrange multiplier λ, after which every class is a separate parabola. Summing $1/p^j$ over the levels gives $1/(p-1)$.

11.9.1 Proof, following [note, Appendix C]

Step 1: D_k level by level. For $j \ge 1$ and $q = p^j$ put

$$o_k^{(j)} = \#\{m \ne k : \ m \equiv k \ (q)\}, \qquad z_k^{(j)} = 3\,\#\{(i,r) : \ 0 \le i < n, \ r \in \{1,2\}, \ 3i + r \equiv 3k \ (q)\},$$

and $g_k^{(j)} = [q \mid n - 2k]$ for odd p, $g_k^{(j)} = 0$ for $p = 2$. By (11.2) applied to every term of (11.7),

$$D_k = \sum_{j \ge 1} (4o_k^{(j)} - z_k^{(j)} - g_k^{(j)}) + [p = 2] \ . \tag{11.8}$$

For example, for $n = 7$, $p = 2$, $k = 2$: $(o, z, g) = (10, 21, 0), (5, 9, 0), (2, 3, 0)$ for $j = 1, 2, 3$ and 0 beyond, so $D_2 = 4 \cdot 17 - 33 + 1 = 36$, the value of (11.7). Likewise (11.8) agrees with (11.7) for all nodes and primes at $n = 5, 7$.

The counts $o_k^{(j)}$ and $z_k^{(j)}$ depend only on the class c of k modulo q: for o this is clear, and for z because 3 is invertible modulo q ($p \ne 3$), so $3i + r \equiv 3k$ is a condition on k mod q. Write N_c for the number of nodes in c (so $o_k^{(j)} = N_c - 1$) and z_c for $z_k^{(j)}$.

Step 2: insert the leaf lemma. By Lemma 11.10, $\sum_k f_p(k, s_k) \le \sum_k s_k D_k + 9K\mathfrak{l}_p$. Insert (11.8) and group by levels and classes. Together with the cross term of (11.3), again level by level,

$$T_p \le 9K\mathfrak{l}_p + [p = 2]K + \max_s \sum_{j \ge 1} \Phi_j(s) \ ,$$

with [note, (C.1)]

$$\Phi_j(s) = \sum_{c \bmod q} \Big[S_c(4(N_c - 1) - z_c) - \sum_{k \in c} s_k g_k^{(j)} - S_c^2 + \sum_{k \in c} s_k^2 \Big] \ . \tag{11.9}$$

We bound each Φ_j separately (the maximum of a sum is at most the sum of the maxima).

Step 3: deep levels. If $q > 3n$, every class has $N_c \le 1$; then $S_c^2 = \sum_{k \in c} s_k^2$ and $4(N_c - 1) \le 0$, and the remaining terms $-S_c z_c$ and $-s_k g_k$ are ≤ 0. So $\Phi_j(s) \le 0$.

Step 4: shallow levels. If $q \le 3n$, use $\sum_{k \in c} s_k^2 \le 4S_c$ (as $s_k \le 4$) and drop $-\sum s_k g_k \le 0$:

$$\Phi_j(s) \le \sum_c (S_cB_c - S_c^2) \ , \qquad B_c = 4N_c - z_c \ .$$

Step 5: the B_c are nearly equal. The $3n + 1$ nodes are consecutive integers, so each class modulo q has $N_c \in \{\lfloor \frac{3n+1}{q} \rfloor, \lceil \frac{3n+1}{q} \rceil\}$. Since $i \mapsto 3i + r$ is a bijection of $\mathbb{Z}/q$, for each r the condition $3i + r \equiv 3k$ fixes i modulo q, and the number of $i \in [0, n)$ in one residue class is $\lfloor \frac{n}{q} \rfloor$ or $\lceil \frac{n}{q} \rceil$. So $4N_c$ takes at most two values 4 apart, and z_c, three times a sum of two such counts, takes values within 6 of each other. Hence all B_c lie in an interval of length 10. Their mean is

$$\bar{B} = \frac{1}{q} \sum_c (4N_c - z_c) = \frac{4(3n+1) - 6n}{q} = \frac{6n+4}{q} \ ,$$

because $\sum_c N_c = 3n + 1$ and every pair (i, r) is counted in exactly one class, $\sum_c z_c = 3 \cdot 2n$. The mean lies in the interval, so $|B_c - \bar{B}| \le 10$. The number $6n + 4$ is the net count of the poles (4 at each of $3n + 1$ nodes) minus the triple zeros (3 at each of $2n$ points).

Example 11.12 (the B_c for $n = 7$)**.** For $p = 2$: modulo 2, $B_c = 23, 23$ (mean $23 = \frac{46}{2}$); modulo 4, $N_c = 5, 6, 6, 5$, $z_c = 12, 9, 9, 12$, $B_c = 8, 15, 15, 8$ (mean $\frac{23}{2}$, spread 7); modulo 8, $B_c = 2, 6, 9, 6, 6, 9, 6, 2$ (mean $\frac{23}{4}$, spread 7); modulo 16, $B_c = 1, 1, 4, 4, 4, 4, 1, 1, 1, 5, 5, 2, 2, 5, 5, 1$ (mean $\frac{23}{8}$, spread 4). For $p = 5$: $B_c = 7, 10, 7, 11, 11$ (mean $\frac{46}{5}$). Over all odd $n < 32$ and all $q \le 3n$ prime to 3 the largest spread is 7, within the proof's 10.

Step 6: weak duality [note, (C.2)]. For real numbers S, B, λ, completing the square gives

$$SB - S^2 = \lambda S + (B - \lambda)S - S^2 = \lambda S + \tfrac{1}{4}(B - \lambda)^2 - \left(S - \tfrac{B-\lambda}{2}\right)^2 \le \lambda S + \tfrac{1}{4}(B - \lambda)^2 \ .$$

Sum over the classes, use $\sum_c S_c = K$, and choose $\lambda = \bar{B} - \frac{2K}{q}$. Then $B_c - \lambda = (B_c - \bar{B}) + \frac{2K}{q}$, and since $\sum_c (B_c - \bar{B}) = 0$ the cross term drops out of the sum of squares:

$$\sum_c (B_c - \lambda)^2 = \sum_c (B_c - \bar{B})^2 + q \cdot \frac{4K^2}{q^2} \ .$$

Hence

$$\sum_c (S_c B_c - S_c^2) \le K\bar{B} - \frac{2K^2}{q} + \frac{K^2}{q} + \frac{1}{4}\sum_c (B_c - \bar{B})^2 \le \frac{K(6n + 4 - K)}{q} + 25q \ , \quad (11.10)$$

using $K\bar{B} = \frac{K(6n+4)}{q}$ and $\frac{1}{4}\sum_c (B_c - \bar{B})^2 \le \frac{1}{4} \cdot q \cdot 10^2$. The choice of λ is the optimal one when all B_c are equal: then the best S_c are all K/q, the stationary point $S = \frac{B-\lambda}{2}$ of each parabola. In physics language, λ is the chemical potential that makes the classes absorb exactly K particles, and (11.10) is the dual (Legendre-transform) bound, valid for every λ and best near the optimum.

Example 11.13 (the chain of inequalities)**.** $n = 7$, $K = 21$, $p = 2$. The exact maximum of $\sum_c (S_c B_c - S_c^2)$ over integers $0 \le S_c \le 4N_c$ with $\sum S_c = 21$, the middle expression of (11.10), and its right side are, for $q = 2, 4, 8, 16$: $262 \le 262.50 \le 312.50$; $143 \le 143.50 \le 231.25$; $77 \le 78.00 \le 265.62$; $42 \le 44.25 \le 432.81$. The completed square loses almost nothing; the crude $25q$ dominates for large q.

Step 7: sum over the levels. Only the levels with $p^j \le 3n$ contribute (Step 3). Since $K \le 3n+1 < 6n+4$, the leading terms add up to at most $K(6n+4-K)\sum_{j\ge1} p^{-j} = \frac{K(6n+4-K)}{p-1}$, and the error terms to $\sum_{p^j \le 3n} 25p^j \le 25 \cdot 3n \cdot \frac{p}{p-1} \le 150n$ (a geometric sum is at most its last term times $\frac{p}{p-1} \le 2$). With the $[p = 2]K \le K$ of Step 2 this is the lemma. □

The small-primes lemma. The leaf lemma replaces each node's loss by $s_k D_k$ up to $9 s_k \mathfrak{l}_p$. The number D_k is a level-by-level count of p-divisible poles minus zeros, and the cross refund is a level-by-level count of pairs; so the tree bound splits into one problem per level. On a level, every class sees the same net charge $B_c \approx (6n + 4)/q$ up to 10, and a Lagrange multiplier turns the constrained maximum into $K(6n + 4 - K)/q$ plus $25q$. The geometric series over the levels gives $1/(p - 1)$.

11.9.2 A concrete test

For $n = 3, 5, 7$ and $K = 3n$ we compare the true $-v_p(\Delta_K)$ from the exact $\Delta_K(X)$, the exact T_p (by the recursion over the tree, with f_p from the exact minors), the same maximum T_p^{leaf} with $f_p(k, s)$ replaced by the leaf bound $sD_k + 9s\mathfrak{l}_p$, and the bound of Lemma 11.11:

$n=5$, $K=15$					$n=7$, $K=21$				
p	true	T_p	T_p^{leaf}	L. 5.18	p	true	T_p	T_p^{leaf}	L. 5.18
2	381	388	913	1725.0	2	740	745	1624	2730.0
5	96	100	447	1241.2	5	166	167	666	1769.2
7	97	99	317	1082.5	7	131	136	432	1536.5
11	65	65	285	1063.5	11	111	113	399	1501.5
13	36	36	278	1058.8	13	98	101	399	1492.8
17–29	0	0	270	≥ 1045	17	68	68	394	1481.8
					19	36	36	386	1478.2
					23–41	0	0	378	≥ 1462

(For $n=3$, $K=9$: true $183, 45, 35, 0$ against $T_p = 185, 51, 35, 0$ at $p = 2, 5, 7, 11$.) In every case true $\leq T_p$, as Theorem 11.5 asserts, and the tree bound is close: within 7 of the truth, and exact at most primes. It even gets 0 right for $p > 3n$. The leaf lemma and the small-primes lemma lose a lot at these n, but what they lose is of lower order: $9K\mathfrak{l}_p + 150n + K$ is $O(n \log n)$ per prime and is wiped out in the sum over $p \leq n^{0.9}$ (Section 11.11).

For $n = 101$, $K = 303$, where Δ_K is out of reach but T_p is not (the node data can be obtained from the logarithmic derivative of $\widetilde{W}_k$), the chain of the proof reads

p	T_p	T_p^{leaf}	after Step 5 (exact max per level)	after (C.2)	L. 5.18
2	99630	119837	120720	132980.6	135744.0
5	26015	33990	34267	37852.2	49616.2
7	17010	25959	26149	27495.1	41864.5
13	9562	15612	15998	20436.9	31385.8

The leading term $K(6n+4-K)/(p-1)$ is 93021 at $p=2$, 23255.25 at $p=5$, 7751.75 at $p=13$ (with $\mathfrak{l}_p = 10, 4, 3$); it accounts for most of T_p at $p = 2, 5$, and less at larger p, where the corrections of order $K\mathfrak{l}_p$ weigh more.

11.10 The middle primes

For p between $n^{0.9}$ and ϵn the error terms $9K\mathfrak{l}_p + 150n$ of Lemma 11.11, summed with weight $\log p$, would cost order n^2, more than the note can afford. There the tree has a single level, and a sharper count is possible. A prime $p \geq 5$ with $p^2 > 6n$ is *single-level* (Chapter 12): every integer in the local constants has absolute value below $6n < p^2$, so all its valuations are 0 or 1, and the classes modulo p^2 are single nodes.

Lemma 11.14 (middle primes; [note, Lemma 5.19])**.** *If $p \geq 5$, $p^2 > 6n$ and $p \leq 0.4n$, then*

$$T_p \leq \frac{K(6n+4-K)}{p} + 3K + 25p.$$

Proof, following [note, Appendix C]. Local constants. All d have $v_p(d) \leq 1$, so $\mu_k \leq 1$, and $v_p(\mathrm{HS}_3(k, M)) \geq -M$ by Lemma 11.9 (here $\max_u v_p(u) \leq 1$). As in the leaf lemma, the term i of $\beta_{k,m}$ has valuation at least $-D_k - (4-i-m) - (i+2) = -D_k - 6 + m$, and $v_p(\alpha_{k,m}) \geq -D_k - 1 + m$ (2916 is prime to $p \geq 5$). So $v_p(c_{k,m}) \geq -D_k - 6 + m$.

The minors. Write $\det C_k[R] = \sum_\pi \pm \prod_b c_{k,R_b+\pi(b)}$, the sum over the permutations π of $\{0, \dots, s-1\}$ (terms with an index ≥ 4 vanish). Each product has valuation at least $\sum_b(-D_k - 6 + R_b + \pi(b)) = -sD_k - 6s + \sum R + \binom{s}{2}$. At a single-level prime $\eta_p(k) = [o_k > 0] \leq 1$, where o_k is the number of partners of k. With $\ell = \sum R - \binom{s}{2} \geq 0$,

$$e_p(k, s, \ell) + \ell\eta_p(k) \leq sD_k + 6s - \textstyle\sum R - \binom{s}{2} + \left(\sum R - \binom{s}{2}\right) = sD_k + 6s - 2\binom{s}{2},$$

so $f_p(k, s) \leq sD_k + 6s - s(s-1)$, and $f_p(k, s) + s^2 \leq s(D_k + 7)$.

One level. The tree (11.3) has only the level $j = 1$, so

$$T_p \le \max_s \sum_{c \bmod p} \Big[\sum_{k \in c} (f_p(k, s_k) + s_k^2) - S_c^2 \Big] \le \max_s \sum_c \Big[S_c(D'_c + 7) - S_c^2 \Big] ,$$

where $D_k = 4(N_c - 1) - z_c - g_k \le D'_c := 4(N_c - 1) - z_c$ (single-level: $D_k = 4o_k - z_k - g_k$ with $z_k = z_c$, $g_k \in \{0, 1\}$).

Weak duality again. $D'_c + 7 = B_c + 3$ with the B_c of Step 5 above (for $q = p$), so these numbers lie in an interval of length 10, with mean $\frac{6n+4-4p}{p} + 7$. Step 6 with this mean gives

$$T_p \le K\Big(\frac{6n + 4 - 4p}{p} + 7\Big) - \frac{K^2}{p} + 25p = \frac{K(6n + 4 - K)}{p} + 3K + 25p \, . \qquad \square$$

The note routes the middle step through the relaxation [note, Lemma 5.28] (Chapter 13), which replaces f_p by a clipped version $f^+(k, s) = \max(0, \dots)$; to show that the clipping is inactive it proves $D_k \ge 0$: every class has $N_c \ge \lfloor \frac{3n+1}{p} \rfloor \ge 7$ nodes, and with $z_c \le 6\lceil \frac{n}{p} \rceil$, $g_k \le 1$, $D_k \ge 4(\frac{3n}{p} - 2) - 6(\frac{n}{p} + 1) - 1 = \frac{6n}{p} - 15 \ge 0$ for $p \le 0.4n$. In the direct argument above, which works with f_p itself, we did not need $D_k \ge 0$; as far as we can see, the hypothesis $p \le 0.4n$ enters only through this clipping. The note uses the lemma only for $p \le \epsilon n = 0.05n$ anyway.

For $n = 101$, $K = 303$, the middle primes are $p = 29, 31, 37$ ($29^2 = 841 > 606$, $37 \le 40.4$). Exact $T_p = 4123, 3937, 3467$, against the bound $4841.6, 4684.7, 4348.1$. Moreover $f_p(k, s) \le s(D_k + 6) - s(s - 1)$ at every node, $\min_k D_k = 15, 11, 9 \ge \frac{6n}{p} - 15$, $\min_c N_c = 10, 9, 8 \ge 7$, and the $D'_c + 7$ range over 22..26, 18..25, 17..24 with means $\frac{697}{29}, \frac{703}{31}, \frac{721}{37}$, which are $\frac{6n+4-4p}{p} + 7$.

Check yourself 11.15. Why does Lemma 11.11 have $p - 1$ in the denominator and Lemma 11.14 only p?

Answer. The small-primes bound sums the per-level bound $K(6n + 4 - K)/p^j$ over all levels $j \ge 1$, and $\sum_j p^{-j} = \frac{1}{p-1}$. At a single-level prime there is only $j = 1$, which gives $\frac{1}{p}$.

11.11 Summing over the primes: Mertens' theorem

Now weight each bound by $\log p$ and sum over $p \le \epsilon n$, $p \ne 3$. The main term of both lemmas is $K(6n+4-K)\frac{\log p}{p-1}$ (or $\frac{\log p}{p}$), and we need the sum of $\frac{\log p}{p-1}$ over the primes. This is a classical result.

Theorem 11.16 (Mertens; [29, (2.5), (2.8)])**.** $\sum_{p \le x} \frac{\log p}{p} = \log x + E + o(1)$ *as* $x \to \infty$, *with* $E = -\gamma - \sum_p \sum_{j \ge 2} \frac{\log p}{p^j}$ *and* $\gamma = 0.5772\dots$ *Euler's constant.*

Intuition. By the prime number theorem the primes near t have density $1/\log t$, so $\sum_{p \le x} \frac{\log p}{p} \approx \int^x \frac{\log t}{t} \frac{\mathrm{d}t}{\log t} = \log x$; the theorem pins down the constant. In our application the weight $\frac{\log p}{p-1} = \sum_{j \ge 1} \frac{\log p}{p^j}$ arises as the sum over the levels j of the tree, each level of p contributing $\frac{\log p}{p^j}$; Mertens' theorem says that all these level contributions together grow like $\log x$, the same as the first level alone, up to a constant.

Since $\frac{\log p}{p-1} = \frac{\log p}{p} + \frac{\log p}{p(p-1)}$ and $\sum_{j \ge 2} p^{-j} = \frac{1}{p(p-1)}$, the second part of E cancels and [note, (C.4)]

$$\sum_{p \le x} \frac{\log p}{p - 1} = \log x - \gamma + o(1) \, , \qquad \sum_{p \le x, \, p \ne 3} \frac{\log p}{p - 1} = \log x - \gamma - \frac{\log 3}{2} + o(1) \, , \tag{11.11}$$

the second because the term $p = 3$ is exactly $\frac{\log 3}{2}$.

Numerically, with the primes up to 10^7:

x	10	10^2	10^3	10^4	10^5	10^6	10^7
$\sum_{p\le x}\frac{\log p}{p-1}$	1.96913	4.11489	6.36389	8.64613	10.93965	13.23895	15.54107
$\log x-\gamma$	1.72537	4.02795	6.33054	8.63312	10.93571	13.23829	15.54088
difference	0.24376	0.08694	0.03335	0.01301	0.00394	0.00066	0.00019

Where $\kappa(6-\kappa)n^2\log n$ comes from. The note (proof of [note, Proposition 5.36], ranges (i) and (ii)) splits the primes $p\le\epsilon n$ at $Y=n^{0.9}$. For $p\le Y$ it uses Lemma 11.11; the main terms give, by (11.11),

$$K(6n+4-K)\Big(\log Y-\gamma-\frac{\log 3}{2}\Big)+o(n^2)\ ,$$

and the error terms at most $(9K\mathfrak{l}_2+154n)\vartheta(Y)$, where $\vartheta(Y)=\sum_{p\le Y}\log p\sim Y$ (prime number theorem; $\mathfrak{l}_p\le\mathfrak{l}_2$ and $150n+K\le 154n$). This is $O(n\cdot\log n\cdot n^{0.9})=o(n^2)$; here $Y<n^{1-\delta}$ is needed. For $Y<p\le\epsilon n$ it uses Lemma 11.14, which needs $p^2>6n$, i.e. $Y>\sqrt{6n}$; this is why any exponent in $(\frac12,1)$ would do. The main terms give $K(6n+4-K)\log\frac{\epsilon n}{Y}+o(n^2)$ by Mertens' theorem, and the errors $3K\vartheta(\epsilon n)+25\sum_{p\le\epsilon n}p\log p=(3\kappa\epsilon+12.5\epsilon^2)n^2+o(n^2)$, since $\sum_{p\le x}p\log p\sim\frac{x^2}{2}$. Adding, $\log Y+\log\frac{\epsilon n}{Y}=\log n+\log\epsilon$, and with $K(6n+4-K)=\kappa(6-\kappa)n^2+4\kappa n$:

$$\begin{aligned}\sum_{p\le\epsilon n,\,p\ne3}\max(T_p,0)\log p\le{}&\kappa(6-\kappa)\,n^2\log n-\kappa(6-\kappa)\Big(\gamma+\frac{\log 3}{2}+\log\frac{1}{\epsilon}\Big)n^2\\&+(3\kappa\epsilon+12.5\epsilon^2)n^2+o(n^2)\ .\end{aligned}\tag{11.12}$$

These are the first, second and last terms of [note, (5.38)].

Example 11.17 (the leading sum in numbers)**.** For $K=3n$ ($\kappa=3$, $\kappa(6-\kappa)=9$) and $\epsilon=\frac{1}{20}$ consider $\Sigma(n)=\sum_{p\le n/20,\,p\ne3}K(6n+4-K)\frac{\log p}{p-1}$ and compare $(\Sigma(n)-9n^2\log n)/n^2$ with the prediction of (11.11), $9(\log\epsilon-\gamma-\frac{\log 3}{2})=-37.1003$ (plus $12\log n/n$ from the $+4$):

n	10^3	10^4	10^5	10^6	10^7	10^8	$2\cdot10^8$
$\Sigma(n)/(n^2\ln n)$	3.859	5.032	5.790	6.318	6.699	6.986	7.059
$(\Sigma(n)-9n^2\ln n)/n^2$	−35.52	−36.55	−36.95	−37.06	−37.08	−37.09	−37.10

The ratio to $n^2\ln n$ creeps towards 9 only logarithmically (the constant -37.1 is large), but the second row settles quickly on the predicted constant.

Remark 11.18 (how large "$o(n^2)$" is here). The error term of range (i), $(9K\mathfrak{l}_2+154n)\vartheta(n^{0.9})/n^2$ with $K=3n$, is measured in nats (ϑ sums natural logarithms). It is 239.6, 217.7, 170.7 nats, i.e. 345.7, 314.0, 246.2 bits, at $n=10^3,10^5,10^7$ (exact ϑ), and, with $\vartheta(Y)\approx Y$, about 20.4 nats (29.5 bits) at $n=10^{20}$ and 0.05 nats (0.07 bits) at $n=10^{50}$. It does tend to 0, as the proof needs, but only for astronomically large n: the final margin of the note is 4.58 bits per n^2, and with $\vartheta(Y)\approx Y$ this error term alone falls below it only from about $n=10^{30}$ on. This is not a gap: the criterion needs the inequality only for some sufficiently large n. It does mean that the theorem's argument cannot be checked numerically at any feasible n, and that small-n comparisons such as Example 11.1 test the individual inequalities (as in Section 11.9.2), not the asymptotic balance.

Why it matches the size. The size estimate (Chapter 10, [note, Theorem 3.8]) has the main term $(\kappa^2-6\kappa)n^2\log_2 n$, and the denominators $\kappa(6-\kappa)n^2\log_2 n$, the exact negative. The small-primes lemma shows where each half comes from. In $\frac{K(6n+4-K)}{p-1}$ the part $\frac{K(6n+4)}{p-1}$ comes from the static denominators s_kD_k, i.e. from h_k: summed over the primes with weight $\log p$ by Mertens' theorem it is about $K\cdot6n\log n\approx6\kappa n^2\log n$, the logarithm of the $p\ne3$ denominator

of $\prod_k h_k^{s_k}$. Its counterpart in the size is $\sum_k s_k \log|h_k| \approx -6\kappa n^2 \log n$, because $|h_k| \approx n^{-6n}$. The part $-\frac{K^2}{p-1}$ comes from the cross refund, the p-adic size of $\prod_{k<m}(k-m)^{2s_k s_m}$: summed it gives $-\kappa^2 n^2 \log n$, whose counterpart in the size is $+\kappa^2 n^2 \log n$. In each case the same product of integers is measured once with $|\cdot|$ and once with $\sum_{p\neq 3} v_p(\cdot)\log p$, and the product formula (Chapter 2) says that these agree up to the 3-part. Chapter 7 illustrated this on the single Heine term with $s_k = 1$ for all nodes. The heuristic is exact for the main terms; the constants $F^\dagger$ and c are where it stops.

11.12 What is left

Equation (11.12) accounts for the primes $p \le \epsilon n$. The remaining primes $\epsilon n < p \le 6n$ are single-level, and for them neither lemma of this chapter is good enough: the error terms $3K + 25p$ of Lemma 11.14, summed over $p \sim n$, are of order n^2 with a large constant, and the crude bound $v_p(c_{k,m}) \ge -D_k - 6 + m$ ignores the cancellation between the zeros of W and the "virtual poles" coming from the harmonic sums. Chapter 12 explains the refined local lemma [note, Lemma 5.24] that captures this cancellation, and Chapter 13 turns the tree bound at these primes into an integral over a circle model and sums it with the prime number theorem, which gives the positive part of the constant c_i [note, (5.39)]. The table of Section 11.9.2 shows the outcome at small n: for $n = 3, 5, 7$ the primes $p > 3n$ do not occur in the denominators.

Summary of the chapter

The denominator of $\Delta_K(X)$ at a prime p is $p^{-v_p(\Delta_K)}$ with the Gauss valuation; for $n = 3, 5, 7$ they can be computed exactly (e.g. $2^{740}5^{166}7^{131}\cdots 19^{36}$ for $n = 7$, no prime above $3n$). The tree bound [note, Theorem 5.13] bounds $-v_p(\Delta_K)$ by a maximum over profiles of local losses $f_p(k, s_k)$, built from the minors $\det C_k[R]$ and the units of degree priced by $\eta_p(k)$, minus refunds from the cross factor, which by $v_p(x) = \#\{j : p^j \mid x\}$ become level-by-level pair counts on the tree of residue classes. We followed the proof of [note, Appendix B], illustrated (B.5) on a cross factor and (B.6) on an explicit profile, and evaluated T_p exactly by a recursion over the tree: for $n \le 7$ it is within 7 of the true value. The number $D_k = -v_p(h_k)$ [note, (5.15)] counts the p-divisible poles and zeros of $\widetilde{W}_k$ with their depth (plus 1 at $p = 2$ from the zero $-\frac{n}{2}$); [note, Lemma 5.16] bounds $H_k[b]$ by $D_k + b\mu_k$ and the harmonic sums by $M \max_u v_p(u)$ (the exact form, not the $-M$ of the remark after (2.14)). The leaf lemma gives $f_p \le sD_k + 9s\mathfrak{l}_p$; the small-primes lemma splits D_k and the refunds by levels and bounds each level by weak duality, $SB - S^2 \le \lambda S + \frac{1}{4}(B-\lambda)^2$ with $\lambda = \bar{B} - 2K/q$ and $\bar{B} = (6n+4)/q$, which gives $T_p \le K(6n+4-K)/(p-1) + O(n\log n)$; the middle-primes lemma does the same on the single level with $1/p$ and error $3K + 25p$.

Carried forward: [note, Theorem 5.13] and the notation T_p, f_p, e_p, η_p, S_c (Chapters 12 and 13); $D_k = 4o_k - z_k - g_k$ at single-level primes; the weak-duality step, reused in [note, Lemma 5.28]; and the contribution (11.12) of the primes $p \le \epsilon n$ to [note, Proposition 5.36], which produces the main term $\kappa(6-\kappa)n^2\log n$ and the negative constant $-\kappa(6-\kappa)(\gamma + \frac{\log 3}{2} + \log 20)$ of [note, (5.39)].

Chapter 12

Estimate 3b: single-level primes and virtual poles

Where we are. Chapter 11 bounded the denominators of $\Delta_K(X)$ at a prime $p \neq 3$ by the tree bound T_p [note, Theorem 5.13] and summed the bounds over the primes $p \leq \epsilon n$, $\epsilon = \frac{1}{20}$. The primes $\epsilon n < p \leq 6n$ remain. For them the tree of residue classes has a single level, and the local constants $c_{k,m}$ can be bounded much more precisely than in Chapter 11. This chapter covers [note, Section 5.3]: single-level primes, the three kinds of p-special points of $\widetilde{W}_k$, the node data of [note, Definition 5.20], the *virtual poles* [note, Lemma 5.22], the refined local lemma [note, Lemma 5.24] with its cancellation [note, (5.26)], and [note, Remark 5.27], which says that without this cancellation the note's argument would not close. The note names the refined local estimate [note, Lemma 5.24], which rests on this cancellation, as one of three steps that do not carry over from the case $p = 2$ treated in [19]. Chapter 13 feeds the refined bound into the circle model and sums over the primes. We use valuations and the ultrametric inequality (Chapter 2), the harmonic sums $\mathrm{HS}_3(k, M)$ [note, (2.14)] (Chapter 4), the node data $\widetilde{W}_k$, $H_k[b]$, h_k and the local constants [note, (2.21)] (Chapter 5), and from Chapter 11 the number $D_k = -v_p(h_k)$, [note, Lemma 5.16] and the tree bound.

12.1 Single-level primes

Chapter 11 ended with a problem: for primes of the size of n the error terms of the small- and middle-primes lemmas add up to order n^2 with a large constant. At such primes the p-adic structure is very simple, and the note exploits it.

Definition 12.1 ([note, Section 5.3])**.** A prime $p \geq 5$ with $p^2 > 6n$ is *single-level*.

The reason for the name is the following list. Every integer whose p-adic valuation enters the local constants has absolute value less than $6n$:

- the node differences $k - m$ ($k, m \in \mathcal{N} = \{-n, \dots, 2n\}$): $|k - m| \leq 3n$;
- the numerators $3k - 3j - r$ of the zeros $d = k - j - \frac{r}{3}$ of $\widetilde{W}_k$ ($0 \leq j < n$, $r = 1, 2$): since $3j + r \in [1, 3n - 1]$ and $3k \in [-3n, 6n]$, we get $3k - 3j - r \in [-6n + 1, 6n - 1]$;
- the integers u of $\mathrm{HS}_3(k, M)$ [note, (2.14)]: $0 < u < 3k \leq 6n$ for $k > 0$ and $-6n \leq 3k < u < 0$ for $k < 0$;
- $2k - n$: $|2k - n| \leq 3n$.

If $p^2 > 6n$, none of these integers is divisible by p^2, so each has $v_p \in \{0, 1\}$. In particular two nodes are never congruent modulo p^2 (their difference is at most $3n < p^2$), so in the tree of residue classes of Chapter 11 all classes modulo p^2 are single nodes: the tree has one level below the root, the classes modulo p. The condition $p \geq 5$ excludes 2 and 3.

Intuition. At a single-level prime, p-adic valuations are yes/no questions: an integer of the problem is either divisible by p ("p-special") or a p-adic unit. Nothing is divisible twice. So all the p-adic information of a node is a short list of which of its zeros and poles, and which of its harmonic-sum terms, are divisible by p. This chapter makes that list.

Example 12.2 ($n = 11$)**.** For $n = 11$, $6n = 66$. The prime 7 is not single-level ($49 < 66$), 11 is ($121 > 66$), so the single-level primes up to $6n$ are $11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61$. Our main examples are $p = 23$ (near $2n = 22$), $p = 31$ (just below $3n = 33$) and $p = 37$ (above $3n$). For $p = 23$ the classes modulo p of the 34 nodes $-11, \dots, 22$ are the pairs $\{k, k + 23\}$ for $k = -11, \dots, -1$ and the single nodes $0, \dots, 11$.

Two consequences used throughout: the quantity $\eta_p(k)$ of Chapter 11 (the deepest level at which k shares its class) is 1 if k has another node in its class modulo p and 0 otherwise; and the formula [note, (5.15)] for $D_k = -v_p(h_k)$ becomes a plain count, see (12.2) below.

12.2 The p-special points of a node

Recall (Chapter 5, [note, (2.17)]) that $\widetilde{W}_k(z) = z^4 W(-k + z)$ is W seen from the node $y = -k$, multiplied by z^4 to remove the pole there, and that (Chapter 11) its nonzero zeros and poles are

- $d = k - m$ for the other nodes $m \neq k$: poles of order 4;
- $d = k - j - \frac{r}{3} = \frac{3k-3j-r}{3}$, $0 \le j < n$, $r \in \{1, 2\}$: zeros of order 3;
- $d = k - \frac{n}{2} = \frac{2k-n}{2}$: a zero of order 1.

A nonzero root or pole d of $\widetilde{W}_k$ is *p-special* if $p \mid d$ (for the fractions: if p divides the numerator; the denominators 3 and 2 are prime to $p \ge 5$). There are three kinds [note, Section 5.3].

Partner poles. $p \mid k - m$ means $m \equiv k \pmod p$. The other nodes in the class of k are its *partners*; each gives a p-special pole of order 4.

The simple zero. $\frac{2k-n}{2}$ is p-special if $p \mid 2k - n$.

Triple zeros. As j runs over $0, \dots, n - 1$ and r over $\{1, 2\}$, the number $3j + r$ runs exactly once over the integers in $[1, 3n - 1]$ that are not divisible by 3. So $3k - 3j - r$ runs exactly once over the integers in the open interval $(3k - 3n, 3k)$ not divisible by 3. Such an integer is divisible by p when it equals pt for an integer t, and $3 \nmid pt$ means $3 \nmid t$ (as $p \neq 3$). So the p-special triple zeros are the points

$$d = \frac{pt}{3} \qquad \text{with} \quad t \in \mathbb{Z} \setminus 3\mathbb{Z}, \quad 3k - 3n < pt < 3k \ .$$

And one more thing: the harmonic sums. The local constants $\beta_{k,a}$ of [note, (2.21)] contain $\mathrm{HS}_3(k, M) = \pm \sum_u (3/u)^M$, where u runs over the integers prime to 3 in $(0, 3k)$ ($k > 0$) or $(3k, 0)$ ($k < 0$). A term with $p \mid u$, $u = pt$, is

$$\Big(\frac{3}{pt}\Big)^M = \rho_t^{-M} \ , \qquad \rho_t = \frac{pt}{3} \ , \tag{12.1}$$

and it has $v_p = -M$: it is p-adically large. These points ρ_t are not zeros or poles of W, but Lemma 12.7 below shows that they act like poles of order 3. That is why the note calls them *virtual poles*.

Intuition: a picture on the line. Return to the variable y of W, where the node k sits at $y = -k$ and the point z of $\widetilde{W}_k$ is $y = -k + z$. The triple zeros of W fill the "comb" of all points of $\frac{1}{3}\mathbb{Z} \setminus \mathbb{Z}$ in the interval $(-n, 0)$. The harmonic sum of the node k comes from the translation lemma [note, Lemma 2.15] (Chapter 4): the Volkenborn integral is not

translation invariant, and moving the pole from the origin to $y = -k$ leaves one correction term for every point $y = -k + \frac{u}{3}$ of $\frac{1}{3}\mathbb{Z} \setminus \mathbb{Z}$ swept over, i.e. for every such point between $-k$ and 0. A virtual pole of the node is such a point with $p \mid u$, and it lies at the same place $y = -k + \rho_t$ as a triple zero of W exactly when the sweep runs through the comb there. So: for $0 < k \le n$ the sweep $(-k, 0)$ lies inside the comb, and every virtual pole sits on a zero; for $k > n$ the part $(-k, -n]$ of the sweep lies outside; for $k < 0$ the sweep is $(0, |k|)$, on the other side of the origin, where W has no zeros at all. Figure 12.1 shows this for $n = 11$, $p = 23$.

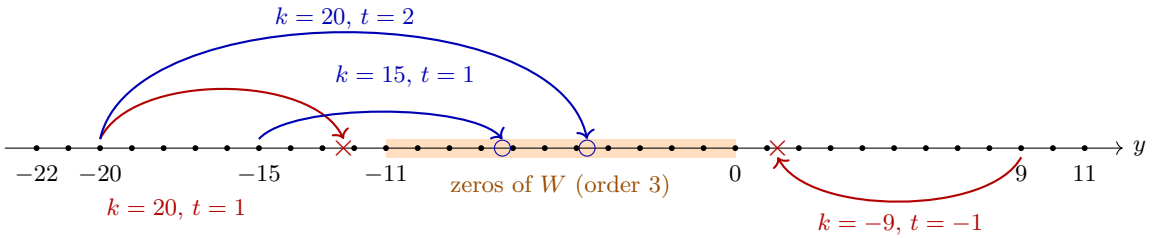


Figure 12.1: $n = 11$, $p = 23$, in the variable y of W: the nodes $y = -k$ (dots, $k = -11, \dots, 22$) and the comb of triple zeros on $\frac{1}{3}\mathbb{Z} \setminus \mathbb{Z}$ inside $(-11, 0)$ (shaded). An arrow goes from a node to one of its virtual poles $y = -k + \frac{23t}{3}$. Circles: covered (the point is a triple zero of W); crosses: uncovered. The node $k = 15$ has one virtual pole, covered; $k = 20$ has two, $t = 2$ covered and $t = 1$ at $y = -\frac{37}{3}$ outside the comb; $k = -9$ has one at $y = \frac{4}{3} > 0$, uncovered.

12.3 The node data

Definition 12.3 (node data; [note, Definition 5.20])**.** Let p be single-level and k a node. Let o_k be the number of partners of k, and $g_k = 1$ if $p \mid 2k - n$, $g_k = 0$ otherwise. Let

$$\mathrm{VP}_k = \{t \in \mathbb{Z} \setminus 3\mathbb{Z} :\ 0 < pt < 3k\}\ (k > 0)\ , \qquad \mathrm{VP}_k = \{t \in \mathbb{Z} \setminus 3\mathbb{Z} :\ 3k < pt < 0\}\ (k < 0)\ ,$$
$$\mathrm{VP}_0 = \emptyset\ ,$$

$$\mathcal{Z}_k = \{t \in \mathbb{Z} \setminus 3\mathbb{Z} :\ 3k - 3n < pt < 3k\}\ , \qquad z_k = 3|\mathcal{Z}_k|\ .$$

For $t \in \mathrm{VP}_k$ the point $\rho_t = \frac{pt}{3}$ is a *virtual pole* of the node; it is *covered* if $t \in \mathcal{Z}_k$. For $t \in \mathrm{VP}_k$ put $\mu_{k,t} = 0$ if t is covered and $o_k + z_k + g_k = 3$, and $\mu_{k,t} = 1$ otherwise.

So VP_k lists the virtual poles (the t with $p \mid u = pt$ in the harmonic sum), $\mathcal{Z}_k$ lists the p-special triple zeros, and z_k counts them with multiplicity 3. Covered means that a virtual pole sits exactly on a triple zero: $\rho_t = \frac{pt}{3}$ is then both. The note draws three consequences.

(i) D_k as a count. By [note, (5.15)], $D_k = -v_p(h_k)$ is $4\sum_m v_p(k-m) - 3\sum_{j,r} v_p(3k - 3j - r) - v_p(\frac{2k-n}{2})$, and at a single-level prime each valuation is 0 or 1. So

$$D_k = 4o_k - z_k - g_k\ : \tag{12.2}$$

four powers of p in the denominator for each partner pole, minus three for each p-special triple zero, minus one if the simple zero is p-special.

(ii) μ_k. The number $\mu_k = \max_d v_p(d)$ of [note, Lemma 5.16] is 1 if the node has any p-special point ($o_k + z_k + g_k > 0$) and 0 otherwise.

(iii) $\mu_{k,t} = 0$ means: t is covered, so $\mathcal{Z}_k \ni t$ and $z_k \ge 3$; and $o_k + z_k + g_k = 3$ then forces $o_k = 0$, $g_k = 0$, $\mathcal{Z}_k = \{t\}$. The covering zero is the *only* p-special point of the node; we say the virtual pole is *covered and alone*.

(iv) When is a virtual pole covered? For $k > 0$, $t \in \mathrm{VP}_k \cap \mathcal{Z}_k$ means $\max(0, 3k - 3n) < pt < 3k$. If $0 < k \le n$, then $3k - 3n \le 0$ and every virtual pole is covered. If $k > n$, a virtual pole is covered exactly when $pt > 3(k - n)$. For $k < 0$, VP_k needs $pt > 3k$ and $\mathcal{Z}_k$ needs $pt < 3k$, so no virtual pole of a negative node is ever covered. This is the picture of Figure 12.1 in formulas.

Intuition. Think of a node as carrying "p-adic charges": $+4$ for each partner pole, -3 for each p-special triple zero, -1 for a p-special simple zero; D_k is the total charge, the static denominator of the node. The virtual poles are extra charges $+3$ that appear only in the harmonic-sum part of the local constants. If such a charge sits on top of a zero of charge -3, the two neutralize; Lemma 12.9 makes this precise. The number $\mu_{k,t}$ records whether, after the neutralization, any p-special point is left at the node.

Example 12.4 (the node data for $n = 11$)**.** For all 808 pairs (single-level p, node k) at $n = 5, 7, 11$, the count $D_k = 4o_k - z_k - g_k$ agrees with $-v_p(h_k)$ from the exact Taylor coefficients, μ_k agrees with $\max_d v_p(d)$ over the zeros and poles of $\widetilde{W}_k$ (56 distinct ones for $n = 11$), and $\max_d v_p(d) \le 1$ always. Grouping nodes with the same data, for $p = 23$:

nodes k	o_k	g_k	VP_k	$\mathcal{Z}_k$	z_k	D_k	μ_k	virtual poles
$-11..-8$	1	0	$\{-1\}$	$\{-2\}$	3	1	1	$t = -1$ uncovered
$-7, -5$	1	0	$\emptyset$	$\{-2, -1\}$	6	-2	1	–
-6	1	1	$\emptyset$	$\{-2, -1\}$	6	-3	1	–
$-4..-1$	1	0	$\emptyset$	$\{-1\}$	3	1	1	–
0..3	0	0	$\emptyset$	$\{-1\}$	3	-3	1	–
4..7	0	0	$\emptyset$	$\emptyset$	0	0	0	–
8..11	0	0	$\{1\}$	$\{1\}$	3	-3	1	$t = 1$ covered, alone ($\mu_{k,1} = 0$)
12..15	1	0	$\{1\}$	$\{1\}$	3	1	1	$t = 1$ covered, $\mu_{k,1} = 1$
16, 18	1	0	$\{1, 2\}$	$\{1, 2\}$	6	-2	1	both covered, $\mu = 1$
17	1	1	$\{1, 2\}$	$\{1, 2\}$	6	-3	1	both covered, $\mu = 1$
19..22	1	0	$\{1, 2\}$	$\{2\}$	3	1	1	$t = 1$ uncovered, $t = 2$ covered

Let us redo one row by hand: $k = 20$. Its partner is $20 - 23 = -3 \in \mathcal{N}$, so $o_{20} = 1$. $2k - n = 29$ is prime to 23, so $g_{20} = 0$. Virtual poles: $0 < 23t < 60$ with $3 \nmid t$ gives $t = 1, 2$. Zeros: $27 < 23t < 60$ gives $t = 2$ only ($23 \le 27$). So $z_{20} = 3$, $D_{20} = 4 - 3 - 0 = 1$, and indeed $v_{23}(h_{20}) = -1$. The virtual pole $t = 1$, at $\rho_1 = \frac{23}{3}$, i.e. $y = -20 + \frac{23}{3} = -\frac{37}{3}$, lies outside the comb (Figure 12.1). For $k = -6$: $2k - n = -23$, so $g_{-6} = 1$. For $k = 8$: $3k = 24 > 23$ gives $\mathrm{VP}_8 = \{1\}$, and $3k - 3n = -9 < 23 < 24$ gives $\mathcal{Z}_8 = \{1\}$: the zero $8 - j - \frac{r}{3} = \frac{23}{3}$ with $3j + r = 1$ ($j = 0$, $r = 1$) is the covering one.

For $p = 31$ the groups are: $k = -11$ ($o = 1$, $\mathrm{VP} = \{-1\}$ uncovered, $\mathcal{Z} = \{-2\}$, $D = 1$); $k = -10$ ($o = 1$, $g = 1$, $\mathcal{Z} = \{-2, -1\}$, $D = -3$); $k = -9$ ($o = 1$, $\mathcal{Z} = \{-1\}$, $D = 1$); $k = -8..0$ ($\mathcal{Z} = \{-1\}$, $D = -3$); $k = 1..10$ (nothing special, $D = 0$); $k = 11..19$ ($\mathrm{VP} = \mathcal{Z} = \{1\}$, covered and alone, $D = -3$); $k = 20$ ($o = 1$, $\mathrm{VP} = \mathcal{Z} = \{1\}$, $D = 1$); $k = 21$ ($o = 1$, $g = 1$, $\mathrm{VP} = \mathcal{Z} = \{1, 2\}$, $D = -3$); $k = 22$ ($o = 1$, $\mathrm{VP} = \{1, 2\}$, $\mathcal{Z} = \{2\}$, $D = 1$). For $p = 37 > 3n$ there are only three kinds of nodes: $k = -11..-2$ ($\mathcal{Z} = \{-1\}$, $D = -3$), $k = -1..12$ (nothing special, $D = 0$) and $k = 13..22$ ($\mathrm{VP} = \mathcal{Z} = \{1\}$, covered and alone, $D = -3$).

Check yourself 12.5. For $n = 11$ and $p = 37$, why does no node have a partner, and why are all virtual poles covered?

Answer. Two nodes differ by at most $3n = 33 < 37$, so no two are congruent modulo 37. A virtual pole needs $0 < 37t < 3k \le 66$ (for $k > 0$; for $k < 0$ it needs $37t \in (3k, 0) \subseteq (-33, 0)$, impossible), so $t = 1$ and $k \ge 13$; it is covered iff $37 > 3(k - 11)$, i.e. $k < 23.3$, which holds for

all nodes. The same argument for any $p > 3n$ is the one the note gives in the proof of [note, Lemma 5.31].

12.4 Virtual poles: Lemma 5.22

Split each $\beta_{k,a}$ of [note, (2.21)] into two parts, $\beta_{k,a} = \beta^{\mathrm{HS}}_{k,a} + \beta^{\mathrm{rest}}_{k,a}$, where $\beta^{\mathrm{HS}}_{k,a}$ collects the terms of the harmonic sums with $p \mid u$ and $\beta^{\mathrm{rest}}_{k,a}$ the others. Recall

$$\beta_{k,a} = \sum_{i=1}^{4-a} i(i+1)\,\mathrm{HS}_3(k, i+2)\,H_k[4-i-a]\ , \qquad \alpha_{k,a} = \begin{cases} -2916\,H_k[1-a] & (a \le 1)\ , \\ 0 & (a \ge 2)\ . \end{cases}$$

The terms of β^{rest} are harmless: $(3/u)^M$ with $p \nmid u$ is a p-adic unit. The terms of β^{HS} are not, and the next lemma identifies their structure.

12.4.1 A generating function

Fact 12.6. *For $|x| < 1$ (or as formal power series), $\displaystyle\sum_{i\ge 1} i(i+1)\,x^{i-1} = \frac{2}{(1-x)^3}$.*

Proof. Differentiate the geometric series $\sum_{i\ge 0} x^i = (1-x)^{-1}$ twice: $\sum_{i\ge 2} i(i-1)x^{i-2} = 2(1-x)^{-3}$. Shift the index $i \to i+1$: $\sum_{i\ge 1}(i+1)i\,x^{i-1} = 2(1-x)^{-3}$. □

The coefficients of $2(1-x)^{-3}$ are $2, 6, 12, 20, 30, 42, 56, 72, \ldots$, which are $i(i+1)$ for $i = 1, \ldots, 8$; at $x = 0.3$ the partial sum up to $i = 59$ is 5.830903790087, and $2/0.7^3 = 5.830903790087$.

Put $x = z/\rho$ and multiply by ρ^{-3}. Since $\rho^{-3}(1 - z/\rho)^{-3} = (\rho - z)^{-3}$,

$$2(\rho - z)^{-3} = \sum_{i\ge 1} i(i+1)\,\rho^{-(i+2)}\,z^{i-1}\ . \tag{12.3}$$

For example, for $\rho = \frac{23}{3}$, $z = \frac{1}{2}$: both sides are 0.005433483844190 (right side summed to $i = 79$).

Intuition. The weights $i(i+1)$ of the local constants and the powers $\rho^{-(i+2)}$ of a harmonic-sum term combine, by (12.3), into the Taylor coefficients of a single function $2(\rho - z)^{-3}$: a pole of order 3 at $z = \rho$. The order 3 is "one more than the degree of the weight $i(i+1)$ in i".

12.4.2 The lemma

Lemma 12.7 (virtual poles; [note, Lemma 5.22])**.** *For every node k and $0 \le a \le 3$,*

$$\beta^{\mathrm{HS}}_{k,a} = 2\,\mathrm{sgn}(k) \sum_{t \in \mathrm{VP}_k} [z^{3-a}]\ \widetilde{W}_k(z)\,(\rho_t - z)^{-3}\ . \tag{12.4}$$

In words: the p-large part of the local constants is exactly what one would get if W had an additional pole of order 3 at each virtual pole ρ_t (with the factor $2\,\mathrm{sgn}(k)$).

Proof. Step 1: the p-divisible part of HS_3. For $k > 0$ the terms of $\mathrm{HS}_3(k, M)$ with $p \mid u$ are those with $u = pt$, $0 < pt < 3k$, $3 \nmid t$, i.e. $t \in \mathrm{VP}_k$, and by (12.1) each is ρ_t^{-M}. So this part is $\sum_{t\in\mathrm{VP}_k} \rho_t^{-M}$. For $k < 0$, $\mathrm{HS}_3(k, M) = -\sum_{3k<u<0}(3/u)^M$ and the same reasoning gives $-\sum_{t\in\mathrm{VP}_k} \rho_t^{-M}$. For $k = 0$ both sides are 0. In all cases it is $\mathrm{sgn}(k)\sum_{t\in\mathrm{VP}_k} \rho_t^{-M}$.

Step 2: insert into β. With $M = i + 2$,

$$\beta^{\mathrm{HS}}_{k,a} = \operatorname{sgn}(k) \sum_{t \in \mathrm{VP}_k} \sum_{i=1}^{4-a} i(i+1)\, \rho_t^{-(i+2)}\, H_k[4-i-a]\ .$$

Step 3: recognize a product of series. By (12.3) with $\rho = \rho_t$, the coefficient of z^{i-1} in $2(\rho_t - z)^{-3}$ is $i(i+1)\rho_t^{-(i+2)}$, and the coefficient of z^b in $\widetilde{W}_k(z)$ is $H_k[b]$. The coefficient of z^{3-a} in the product $\widetilde{W}_k(z) \cdot 2(\rho_t - z)^{-3}$ is the sum over the splittings $3 - a = b + (i-1)$, i.e. $b = 4 - a - i$:

$$[z^{3-a}]\, \widetilde{W}_k(z) \cdot 2(\rho_t - z)^{-3} = \sum_{i \geq 1} i(i+1)\, \rho_t^{-(i+2)}\, H_k[4-a-i]\ .$$

For $i > 4 - a$ the index $b = 4 - a - i$ is negative and $H_k[b] = 0$, so the sum stops at $i = 4 - a$, exactly as in Step 2. Summing over t gives (12.4). □

Example 12.8 (Lemma 12.7 in numbers)**.** For $n = 5, 7, 11$, every single-level prime $p \leq 6n$, every node and $a = 0, \dots, 3$ (3232 cases, 1244 of them with $\beta^{\mathrm{HS}}_{k,a} \neq 0$) one can compute $\beta^{\mathrm{HS}}_{k,a}$ in two ways: from [note, (2.21)] keeping only the terms with $p \mid u$, and from the right side of (12.4) by multiplying the Taylor series of $\widetilde{W}_k$ with $(\rho_t - z)^{-3} = \rho_t^{-3} \sum_c \binom{c+2}{2} (z/\rho_t)^c$. The two agree exactly in all cases.

What a virtual pole costs. Since $v_p(\rho_t) = v_p(p) + v_p(t) - v_p(3) = 1$ ($|t| < p$ here, as $|pt| < 6n < p^2$),

$$v_p\big([z^c](\rho_t - z)^{-3}\big) = v_p\Big(\binom{c+2}{2} \rho_t^{-3-c}\Big) = -3 - c$$

(the binomial coefficients $1, 3, 6, 10$ are prime to $p \geq 7$; for $p = 5$ one gets $\geq$). For example, for $p = 37$, $\rho_1 = \frac{37}{3}$: $-3, -4, -5, -6$ for $c = 0, \dots, 3$. So a virtual pole, multiplied naively into $\widetilde{W}_k$, costs $3 + c$ powers of p in the coefficient of z^c.

12.5 The refined local lemma

Lemma 12.9 (refined local lemma; [note, Lemma 5.24])**.** *Let p be single-level. For every node k and $0 \leq m \leq 3$,*

$$v_p(c_{k,m}) \geq \hat{v}_m(k) := \min\Big(-D_k - (3-m)\mu_k\ ,\ \min_{t \in \mathrm{VP}_k} \big[-D_k - 3 - (3-m)\mu_{k,t}\big]\ ,\ \hat{a}_m(k)\Big)\ , \tag{12.5}$$

where $\hat{a}_m(k) = -D_k - (1-m)\mu_k$ for $m \leq 1$, $\hat{a}_m(k) = +\infty$ for $m \geq 2$, and the minimum over t is $+\infty$ if $\mathrm{VP}_k = \emptyset$. The three terms bound $\beta^{\mathrm{rest}}_{k,m}$, $\beta^{\mathrm{HS}}_{k,m}$ and $\alpha_{k,m}$, respectively.

Here $v_p(c_{k,m})$ is the Gauss valuation of the polynomial $c_{k,m}(X) = \beta_{k,m} + X\alpha_{k,m}$, i.e. $\min(v_p(\beta_{k,m}), v_p(\alpha_{k,m}))$, and $\beta_{k,m} = \beta^{\mathrm{HS}}_{k,m} + \beta^{\mathrm{rest}}_{k,m}$, so by the ultrametric inequality it suffices to bound the three parts separately.

Intuition. Compare with the crude bound $v_p(c_{k,m}) \geq -D_k - 6 + m$ used for the middle primes (Chapter 11, proof of [note, Lemma 5.19]). The crude bound charges every node for harmonic-sum terms of the worst kind. The refined bound charges β^{rest} only for the Taylor orders of $\widetilde{W}_k$ (at most $3 - m$ of them, each worth $\mu_k \leq 1$), charges β^{HS} only at nodes that actually have virtual poles, and, for a virtual pole that is covered and alone, charges only 3 in every Taylor order. The last point is the cancellation.

12.5.1 Proof, following the note

Preliminaries. At a single-level prime every d has $v_p(d) \le 1$, so $\mu_k \le 1$, and every valuation entering [note, (5.15)] is 0 or 1, so $v_p(h_k) = -D_k$ with D_k as in (12.2). [note, Lemma 5.16] (Chapter 11) gives

$$v_p(H_k[b]) \ge -D_k - b\mu_k \qquad (b \ge 0)\ . \tag{12.6}$$

Recall why: $\widetilde{W}_k(z) = h_k \prod_d (1 - z/d)^{e_d}$, the coefficient of z^b in $(1-z/d)^e$ is the integer $\binom{e}{b}(-1)^b$ times d^{-b}, which has valuation $\ge -b\, v_p(d) \ge -b\mu_k$, and products and sums do not make it worse.

The part β^{rest}. Its terms are $i(i+1)\cdot(\text{terms } (3/u)^{i+2} \text{ with } p \nmid u)\cdot H_k[4-i-m]$. The first factor is an integer ($v_p \ge 0$), the second a p-adic unit, and the third has $v_p \ge -D_k - (4-i-m)\mu_k \ge -D_k - (3-m)\mu_k$ by (12.6), because $i \ge 1$ and $\mu_k \ge 0$. The ultrametric inequality gives $v_p(\beta^{\mathrm{rest}}_{k,m}) \ge -D_k - (3-m)\mu_k$, the first term of (12.5).

The part α. For $m \le 1$, $\alpha_{k,m} = -2916\, H_k[1-m]$, and $2916 = 2^2 \cdot 3^6$ is prime to $p \ge 5$. By (12.6), $v_p(\alpha_{k,m}) \ge -D_k - (1-m)\mu_k = \hat{a}_m(k)$. For $m \ge 2$, $\alpha_{k,m} = 0$.

The part β^{HS}. By Lemma 12.7 and the ultrametric inequality (the factor $2\,\mathrm{sgn}(k)$ is a unit), it suffices to show for each $t \in \mathrm{VP}_k$ separately

$$v_p\Big([z^{3-m}]\, \widetilde{W}_k(z)(\rho_t - z)^{-3}\Big) \ge -D_k - 3 - (3-m)\mu_{k,t}\ . \tag{12.7}$$

Case 1: t uncovered. Then $\mu_{k,t} = 1$ by definition. The coefficient of z^{3-m} of the product is $\sum_{b+c=3-m} H_k[b]\,[z^c](\rho_t - z)^{-3}$, and each term has valuation at least $(-D_k - b\mu_k) + (-3-c) \ge -D_k - 3 - (b+c) = -D_k - 3 - (3-m)$, using $\mu_k \le 1$. This is (12.7).

Case 2: t covered. Now ρ_t is a triple zero of $\widetilde{W}_k$, and the note first checks that the factor $(1 - z/\rho_t)$ occurs in $\widetilde{W}_k(z) = h_k \prod_d (1-z/d)^{e_d}$ with exponent *exactly* 3, i.e. no other root or pole sits at the same point:

- the triple zeros $k - j - \frac{r}{3}$ are pairwise distinct (different $3j + r$);
- ρ_t is not a pole: the poles $k - m$ are integers, and $\rho_t = \frac{pt}{3}$ is not, as $3 \nmid pt$;
- ρ_t is not the simple zero $\frac{2k-n}{2}$: $v_3(\rho_t) = -1$, while $v_3(\frac{2k-n}{2}) \ge 0$.

So $\widetilde{W}_k(z) = h_k(1 - z/\rho_t)^3 \prod_{d \ne \rho_t}(1 - z/d)^{e_d}$. Since $1 - z/\rho_t = (\rho_t - z)/\rho_t$, we have the identity [note, (5.26)]

$$\Big(1 - \frac{z}{\rho_t}\Big)^3 (\rho_t - z)^{-3} = \rho_t^{-3}\ , \tag{12.8}$$

and therefore

$$\widetilde{W}_k(z)\,(\rho_t - z)^{-3} = h_k\, \rho_t^{-3} \prod_{d \ne \rho_t} \Big(1 - \frac{z}{d}\Big)^{e_d}\ . \tag{12.9}$$

The virtual pole has disappeared; only the constant ρ_t^{-3} is left. The constant $h_k \rho_t^{-3}$ has valuation $-D_k - 3$. The remaining product has the coefficient of z^b of valuation at least $-b \cdot \max_{d \ne \rho_t} v_p(d)$, by the same argument as for (12.6). If $\mu_{k,t} = 0$, the covering zero was the only p-special point, so every remaining d is a p-adic unit and the maximum is 0. If $\mu_{k,t} = 1$, the maximum is at most 1. In both cases the maximum is at most $\mu_{k,t}$, so the coefficient of z^{3-m} in (12.9) has valuation at least $-D_k - 3 - (3-m)\mu_{k,t}$. This is (12.7), and the lemma is proved. □

The refined local lemma. The local constant splits into three pieces. β^{rest} and α only see the Taylor coefficients of $\widetilde{W}_k$, which lose D_k plus at most one power of p per order. β^{HS} is, by Lemma 12.7, a sum over the virtual poles of Taylor coefficients of $\widetilde{W}_k(z)(\rho_t - z)^{-3}$.

An uncovered virtual pole costs 3 plus one per order. A covered one cancels against its zero, (12.8), leaving the constant ρ_t^{-3} and the other points of the node; if there are no other p-special points, the cost is exactly 3 beyond D_k, whatever the order m.

12.5.2 The cancellation in one node

Example 12.10 ($n = 11$, $p = 37$, $k = 13$)**.** Here $\mathrm{VP}_{13} = \mathcal{Z}_{13} = \{1\}$, $o = g = 0$, $D_{13} = -3$: the node has one virtual pole, $\rho_1 = \frac{37}{3}$, covered by the triple zero $13 - 0 - \frac{2}{3} = \frac{37}{3}$ ($j = 0$, $r = 2$), and nothing else. So h_{13} is divisible by 37^3, and indeed $v_{37}(H_{13}[b]) = 3, 2, 1, 0$ for $b = 0, \dots, 3$: each Taylor order loses one power, as (12.6) allows. The naive product of the series:

c	0	1	2	3
$v_{37}([z^c](\rho_1 - z)^{-3})$	-3	-4	-5	-6
termwise bound $-D - 3 - c$ for $[z^c]\widetilde{W}_{13}(z)(\rho_1 - z)^{-3}$	0	-1	-2	-3
actual $v_{37}([z^c]\widetilde{W}_{13}(z)(\rho_1 - z)^{-3})$	0	0	0	0

The actual valuations are 0 in every order, the bound $-D_k - 3 - (3 - m)\mu_{k,t} = 0$ of (12.7). Dividing $\widetilde{W}_{13}(z)$ by $(1 - z/\rho_1)^3$ as a power series, the quotient $R(z)$ has coefficients of valuation $3, 3, 3, 3$ (the constant h_{13} with $v = 3$ times a product of unit factors), and $\rho_1^{-3}R(z)$ equals $\widetilde{W}_{13}(z)(\rho_1 - z)^{-3}$ exactly, which is (12.9). In terms of the local constants: $\beta^{\mathrm{HS}}_{13,0} = 2\sum_{i=1}^{4} i(i+1)\rho_1^{-(i+2)}H_{13}[4 - i]$ is a sum of four terms of valuation -3 each, and the sum has valuation 0. Three powers of 37 cancel between the four terms.

Intuition: why the cancellation happens. Write W near the node as a product of factors. A zero of order 3 at ρ is the factor $(1 - z/\rho)^3$; a pole of order 3 at the same ρ is $(1 - z/\rho)^{-3}$ up to a constant. Their product is the constant: the two have disappeared, not just partly cancelled. In the electrostatic picture of Chapter 10 ($\log|W|$ is the potential of charges $+$order at zeros and $-$order at poles), a charge -3 placed exactly on a charge $+3$ leaves no field. p-adically: the covering zero had lowered the static denominator, D_k, by 3; the virtual pole takes these 3 back through ρ_t^{-3}, and nothing else happens. In the example, $D_{13} = -3$ and the net result is $v_p = 0$: the node behaves as if it had no p-special point at all. Without the cancellation, the series of the zero and of the pole are expanded separately; each order z^c of the pole costs one more power of p, and the zero's series pays it back only through cancellations between terms, which a termwise bound cannot see.

12.5.3 The refined bound against the truth

Example 12.11 (all nodes, $n = 11$, $p = 23$)**.** Compute all 136 local constants $c_{k,m} = \beta^{\mathrm{HS}}_{k,m} + \beta^{\mathrm{rest}}_{k,m} + X\alpha_{k,m}$ exactly from [note, (2.21)], together with the valuations of the three parts and of $c_{k,m}$ (Gauss valuation). Grouped as in Example 12.4, with $m = 0, 1, 2, 3$:

nodes k	$v_{23}(c_{k,m})$	$\hat{v}_m(k)$ (12.5)	crude $-D_k - 6 + m$
$-11..-8$	$-7,-6,-5,-4$	$-7,-6,-5,-4$	$-7,-6,-5,-4$
$-7,-5$	$-1,0,1,2$	$-1,0,1,2$	$-4,-3,-2,-1$
-6	$0,1,3,3$	$0,1,2,3$	$-3,-2,-1,0$
$-4..-1$	$-4,-3,-2,-1$	$-4,-3,-2,-1$	$-7,-6,-5,-4$
0	$2,3,\infty,\infty$	$0,1,2,3$	$-3,-2,-1,0$
$1..3$	$0,1,2,3$	$0,1,2,3$	$-3,-2,-1,0$
$4..7$	$0,0,0,0$	$0,0,0,0$	$-6,-5,-4,-3$
$8..11$	$0,0,0,0$	$0,0,0,0$	$-3,-2,-1,0$
$12..15$	$-7,-6,-5,-4$	$-7,-6,-5,-4$	$-7,-6,-5,-4$
$16,18$	$-3,-3,-2,-1$	$-4,-3,-2,-1$	$-4,-3,-2,-1$
17	$-3,-2,-1,0$	$-3,-2,-1,0$	$-3,-2,-1,0$
$19..22$	$-6,-6,-5,-4$	$-7,-6,-5,-4$	$-7,-6,-5,-4$

($v=\infty$ at $k=0$, $m\geq 2$: $c_{0,m}=0$, as $\mathrm{HS}_3(0,\cdot)=0$ and $\alpha_{0,m}=0$ for $m\geq 2$.) The refined bound holds everywhere and is attained in 125 of the 136 cases; where it is not attained it is off by at most 2 (apart from the vanishing constants $c_{0,2}, c_{0,3}$). At the nodes 8..11 (one virtual pole, covered and alone) the truth is $v_{23}(c_{k,m})=0$ for all m, the refined bound gives exactly 0, and the crude bound $-3,-2,-1,0$ is off by 3 at $m=0$. At $k=8$ the three parts separately have $v_{23}(\beta^{\mathrm{HS}}_{8,m})=0,0,0,0$, $v_{23}(\beta^{\mathrm{rest}}_{8,m})=0,1,2,3$, $v_{23}(\alpha_{8,m})=2,3,\infty,\infty$, against the three terms $0,0,0,0$; $0,1,2,3$; $2,3$ of (12.5): each term is sharp for its own part. At the nodes 4..7, with no p-special point at all, the crude bound is off by 6 at $m=0$; this gain does not need the cancellation, only that these nodes have no virtual poles. At the nodes with a partner and a virtual pole ($k=-11..-8$ and 12..22) the refined and the crude bound coincide. In total, over $n=5,7,11$ and all their single-level primes (31 pairs (n,p), 3232 local constants), none of the three terms of (12.5) is violated, the refined bound is attained in 3000 cases, the truth exceeds it by at most 3 (apart from the vanishing constants $c_{0,2}, c_{0,3}$), and the truth exceeds the crude bound by up to 7.

12.6 The cancellation in action: the primes $p > 3n$

The cleanest consequence is at the primes above $3n$. [note, Remark 5.27] and the proof of [note, Lemma 5.31] (Chapter 13) argue as follows. For single-level $p>3n$: no node has a partner ($|k-m|\leq 3n<p$); $g_k=0$ ($|2k-n|\leq 3n<p$); a positive node has at most the virtual pole $t=1$, which is covered and alone; a negative node has none. So every node is of one of three types: nothing special ($D_k=0$, $\mu_k=0$); only the zero $t=-1$ ($D_k=-3$, no virtual pole); or $\mathrm{VP}_k=\mathcal{Z}_k=\{1\}$, covered and alone ($D_k=-3$, $\mu_{k,1}=0$). In the first type (12.5) gives $\hat{v}_m=\min(0,0)=0$; in the second $\hat{v}_m=\min(3-(3-m),3-(1-m))=m$; in the third $\hat{v}_m=\min(m,\ 3-3-0,\ 2+m)=0$. So $\hat{v}_m(k)\geq 0$ at every node, all local constants are p-integral, and p cannot appear in any denominator of Δ_K, by the tree bound.

For $n=5$ ($p=17,19,23,29$), $n=7$ ($p=23,29,31,37,41$) and $n=11$ ($p=37,\dots,61$) one finds at every node that $o_k=0$, every virtual pole is covered and alone, $\hat{v}_m(k)\geq 0$, and exactly the three types above occur.

Example 12.12 ($n=7$: the terms are large, the sums are not)**.** Take $n=7$ and the single-level primes $p\in(3n,6n)=(21,42)$: $23,29,31,37,41$. Each divides some u of a harmonic sum: $p=u<3k$ for the nodes $k>\frac{p}{3}$, namely $k=8,\dots,14$ for $p=23$, $k=10,\dots,14$ for 29, $k=11,\dots,14$ for 31, $k=13,14$ for 37 and $k=14$ for 41. The terms $(3/p)^M$, $M=3,\dots,6$, have $v_p=-3,-4,-5,-6$. At $p=23$, $k=8$ ($\mathrm{VP}=\mathcal{Z}=\{1\}$, $D_8=-3$, $v_{23}(H_8[b])=3,2,1,0$) the four terms $2\,i(i+1)\rho_1^{-(i+2)}H_8[4-i]$ of $\beta^{\mathrm{HS}}_{8,0}$ have $v_{23}=-3,-3,-3,-3$, and their sum has $v_{23}=0$; for $m=1,2,3$ the terms have $v_{23}=-2$, -1, 0 and the sums $0,0,0$. The other

parts: $v_{23}(\beta^{\mathrm{rest}}_{8,m}) = 0, 1, 2, 3$ and $v_{23}(\alpha_{8,m}) = 2, 3, \infty, \infty$. At all 22 nodes and all five primes, $\min_{k,m} v_p(c_{k,m}) = 0$.

Then the exact Hankel polynomial $\Delta_{21}(X)$ ($n = 7$, $K = 21$, as in Chapter 11): the lcm of its coefficient denominators has no prime factor other than $2, 3, 5, 7, 11, 13, 17, 19$, so none of $23, \ldots, 41$ occurs, in agreement with Chapter 11. The same holds for $n = 5$ ($p = 17, \ldots, 29$ absent) and for $n = 11$, $K = 33$: the primes $37, \ldots, 61$ do not divide any denominator of Δ_{33}, and no prime above $6n$ does either.

What would the crude bound charge? To answer this, we evaluate the *relaxed tree bound* T_p^+ of [note, Lemma 5.28] (explained in Chapter 13): the tree bound [note, (5.14)] with the local losses $f_p(k, s)$ replaced by the clipped quantity $f^+(k, s)$ of [note, (5.29)], built from a lower bound $\check{v}_m(k)$ for $v_p(c_{k,m})$. We use three choices of $\check{v}$: the crude $-D_k - 6 + m$; an *intermediate* bound, (12.5) with every $\mu_{k,t}$ set to 1 (every virtual pole charged as if uncovered); and the refined $\hat{v}$. We compare with the exact tree bound T_p (with f_p from the exact minors, as in Chapter 11) and with the true $-v_p(\Delta_K)$, $K = 3n$:

$n = 7$, $K = 21$						$n = 11$, $K = 33$					
p	crude	interm.	refined	T_p	true	p	crude	interm.	refined	T_p	true
7	136	136	136	136	131	11	208	208	208	208	203
11	113	113	113	113	111	13	219	219	219	219	213
13	109	101	101	101	98	17	175	175	175	175	171
17	103	79	68	68	68	19	171	163	163	163	159
19	99	56	36	36	36	23	165	147	139	139	139
23	95	28	0	0	0	29	155	99	68	68	68
29	108	20	0	0	0	31	151	72	36	36	36
31	112	16	0	0	0	37	155	40	0	0	0
37	120	8	0	0	0	41	163	36	0	0	0
41	124	4	0	0	0	43..61	≥ 168	32..8	0	0	0

Three observations. First, above $3n$ the refined bound gives 0, as the true value is, while the intermediate bound (no cancellation) is positive at every single-level prime up to $6n$, as [note, Remark 5.27] says; the crude bound is far larger still. The difference between "intermediate" and "refined" is entirely the cancellation (12.8). Second, the refined relaxed bound coincides with the exact tree bound T_p at all 31 single-level primes of $n = 5, 7, 11$: at these n the local bound (12.5) together with the relaxation loses nothing. Third, the tree bound is within 6 of the truth (the largest gap is 219 against 213 at $n = 11$, $p = 13$), and exact for $p \geq 23$ at $n = 11$.

Remark on the note: which "cruder bound" does Remark 5.27 mean?. [note, Remark 5.27] compares the refined lemma with "the cruder bound", and the sentence before it describes a bound that charges a covered virtual pole $-D_k - 6 + m$. Read literally as $\check{v}_m(k) = -D_k - 6 + m$ at *every* node, the crude bound also charges the nodes with no p-special point at all (in our table, f^+ up to 12 at such a node, e.g. 6 for $s = 1$), and at $n = 7, 11$ it gives 95 to 192 at the primes above $3n$. A rough extrapolation of ours (not in the note): at $n = 11$ the literal crude bound gives $T_p^+ \approx 14n$ to $17n$ at each prime in $(3n, 6n)$; if $T_p^+ \approx 15n$ persisted, the prime number theorem would turn this into about $15 \cdot 3/\ln 2 \approx 65$ bits per n^2 from these primes alone, where the refined bound gives 0. That is several times the difference $44 - 31.5 \approx 12.5$ of the remark. The intermediate bound, which charges only the actual virtual poles, gives 8 to 40 at these primes for $n = 11$, which is consistent in size with that difference. The circle-model evaluation of Chapter 13 strongly suggests the answer: at $\kappa = 3$ it gives about 44.1 bits per n^2 for the intermediate bound (virtual poles charged without the cancellation) and about 112 for the literal reading, so

the remark's "about 44" refers to the intermediate bound. Since the remark is explicitly not part of the proof, this affects only its interpretation.

The bits at small n. Summing $\max(\cdot, 0)\log_2 p$ over the single-level primes, one finds, per n^2: crude 88.3, 98.3, 99.5; intermediate 36.6, 42.3, 44.7; refined 25.4, 32.2, 33.7; true 25.2, 31.5, 33.1, for $n = 5, 7, 11$. These numbers include the $n^2 \log n$ part of the primes $p > \epsilon n$ and are dominated by lower-order terms at these n, so they are *not* comparable with the asymptotic constants of [note, Remark 5.27]; they only show that, already at small n, the cancellation removes between about a quarter and a third (24 to 31%) of the single-level bits of the intermediate bound, and that the refined bound is close to the truth.

12.7 Why order 3 meets order 3

The cancellation (12.8) is exact because two orders coincide: the virtual poles have order 3 and the zeros of W have order 3. The note attributes the first to "the single derivative" in the functional $L(P) = \sum_r \int_{\mathbb{Z}_3} (PW)'(t + \frac{r}{3})\mathrm{d}t$ [note, (1.3)]. Let us trace where the 3 comes from.

The weight $i(i+1)$. In the proof of purity [note, Lemma 2.19] (Chapter 5) a principal-part term $r_{k,i}(y+k)^{-i}$ of PW is differentiated: $-i\, r_{k,i}(y+k)^{-i-1}$. This is the factor i. The translation lemma [note, Lemma 2.15] with $m = i+1$ then gives $-m\,\mathrm{HS}_3(k, m+1) = -(i+1)\mathrm{HS}_3(k, i+2)$; the factor $m = i+1$ comes from (V1), which corrects a translation by the *derivative* f' of the integrand at the points swept over (Chapter 4). Together: $i(i+1)\mathrm{HS}_3(k, i+2)$, the weight in [note, (2.21)].

The order. A harmonic-sum term contributes $\rho^{-(i+2)}$ with the weight $i(i+1)$, a polynomial of degree 2 in i. By Fact 12.6, $\sum_i i(i+1)x^{i-1} = 2(1-x)^{-3}$. More generally, a weight that is a polynomial of degree e in i produces $(1-x)^{-(e+1)}$ up to lower-order terms (differentiate the geometric series e times). So the order 3 of a virtual pole is "degree 2 of the weight, plus 1".

The zeros. The order 3 of the zeros of W is a choice in its definition, $W \propto (y+\frac{1}{3})_n^3 (y+\frac{2}{3})_n^3$ [note, (1.2)]; the cubes serve the 3-adic gain (Chapter 8) and, as we have just seen, match the virtual poles.

Check yourself 12.13. Suppose the triple zeros of W were replaced by double zeros. What would a covered virtual pole that is alone at its node cost?

Answer. Then $(1 - z/\rho)^2(\rho - z)^{-3} = \rho^{-2}(\rho - z)^{-1}$: a simple pole survives. Its coefficient of z^c is ρ^{-3-c}, of valuation $-3-c$, and the zero lowers D_k by only 2. So the coefficient of z^{3-m} would cost $-D_k - 3 - (3-m)$, i.e. $-6 + m + 2 = m - 4$ relative to a node without special points, instead of 0. The cancellation needs the order of the zero to be at least the order of the virtual pole; with equal orders nothing is left over.

12.8 Remark 5.27: the cancellation is needed

Remark 12.14 ([note, Remark 5.27]). Without the refined lemma the note's argument does not close, at least at $\kappa = 3$. For primes $p > 3n$, no node has a partner, every virtual pole is covered and alone, the lemma gives $\hat{v} \geq 0$, and these primes cost nothing ([note, Lemma 5.31]). The cruder bound gives a positive relaxed tree bound at every single-level prime up to $6n$. Evaluated numerically in the circle model of [note, Section 5.4] at $\kappa = 3$, the cruder bound gives a denominator constant of about 44 bits per n^2, against about 31.5 with $\hat{v}$ (the bound $c_5 \leq 31.72$ of [note, Table 1] is larger because it holds on the whole interval I_5). Since $G(3) - F_5^\dagger$ is about 37.7, the comparison would then give no contradiction. The note states that this evaluation is not part of the proof.

All four numbers, 44, 31.5, 31.72 and 37.7, are the note's; Chapter 13 returns to them when it evaluates the circle model. The logic is the bookkeeping of Chapter 7: the proof needs gain $>$ size + denominators, i.e. $G - F^{\dagger} - c > 0$ in bits per n^2. With $c \approx 31.5$ the margin at $\kappa = 3$ is about $37.7 - 31.5 \approx 6$ bits per n^2 (the note's computed margin over all of $[2.8, 3]$ is 4.58); with $c \approx 44$ it would be about $37.7 - 44 \approx -6$, negative. The single-level primes in $(\epsilon n, 6n)$ are a large part of the prime sum, and on them the cancellation removes the difference.

What the examples of this chapter show is the mechanism at small n: the refined bound holds at every node for $n = 5, 7, 11$ (Example 12.11), it makes the primes above $3n$ free exactly as the true denominators are, and without the cancellation the relaxed tree bound is positive at all these primes (the table in Section 12.6).

Summary of the chapter

At a single-level prime ($p \geq 5$, $p^2 > 6n$) every integer of the problem has $v_p \in \{0, 1\}$, the tree of residue classes has one level, and all p-adic information of a node k is a list of p-special points: o_k partner poles of order 4, $z_k/3$ triple zeros at $\frac{pt}{3}$, $t \in \mathcal{Z}_k$, a possible simple zero (g_k), and the virtual poles $\rho_t = \frac{pt}{3}$, $t \in \mathrm{VP}_k$, coming from the harmonic-sum terms with $p \mid u$ ([note, Definition 5.20]); $D_k = 4o_k - z_k - g_k$. A virtual pole is covered when it sits on a triple zero of W, which happens for all virtual poles of the nodes $0 < k \leq n$, never for $k < 0$, and for $k > n$ iff $pt > 3(k - n)$. By [note, Lemma 5.22], proved with $\sum_i \widetilde{i(i+1)} x^{i-1} = 2(1-x)^{-3}$, the p-large part of the local constants is $\beta^{\mathrm{HS}}_{k,a} = 2\,\mathrm{sgn}(k) \sum_t [z^{3-a}] \widetilde{W_k}(z)(\rho_t - z)^{-3}$: virtual poles act like poles of order 3. The refined local lemma [note, Lemma 5.24] bounds β^{rest}, β^{HS} and α separately; its key case is a covered virtual pole, where $(1 - z/\rho_t)^3(\rho_t - z)^{-3} = \rho_t^{-3}$ [note, (5.26)] removes the pole entirely, so that a covered virtual pole alone at its node costs exactly 3 beyond D_k, in every Taylor order. At $n = 5, 7, 11$ and their single-level primes, [note, Lemma 5.22] holds exactly in all 3232 cases and the three bounds of [note, (5.25)] hold on all 3232 local constants (attained in 3000 cases); the cancellation is visible directly: terms of valuation -3 summing to valuation 0, and no prime in $(3n, 6n]$ in the denominators of the exact Δ_{3n} for $n = 5, 7, 11$, while the relaxed tree bound without the cancellation is positive at all of them.

Carried forward to Chapter 13: the node data of [note, Definition 5.20] and the bound $\hat{v}_m(k)$ [note, (5.25)], which enter the relaxation [note, Lemma 5.28] and, through their dependence on $(k/n, p/n)$ only, the circle model; the fact that for $p > 3n$ every node has $\hat{v} \geq 0$ ([note, Lemma 5.31]); and [note, Remark 5.27]'s comparison 44 versus 31.5 bits per n^2 (the note's numbers). Chapter 14 uses the exact leading term of β^{HS} at special nodes [note, (6.8)], which is built on [note, Lemma 5.22].

Chapter 13

Estimate 3c: the circle model and the prime sum

Where we are. The denominator estimate [note, Theorem 3.10] says that, uniformly for $K/n \in I_i$,

$$\sum_{p\neq 3} \big(-v_p(\Delta_K)\big)^+ \log_2 p \le \kappa(6-\kappa)\, n^2 \log_2 n + c_i\, n^2 + o(n^2)\ .$$

Chapter 11 bounded $-v_p(\Delta_K)$ by the tree bound T_p [note, Theorem 5.13] and summed it over the primes $p \le \epsilon n$, $\epsilon = \frac{1}{20}$, which produced the main term $\kappa(6-\kappa)n^2 \log n$ and a large negative constant. Chapter 12 sharpened the local bound at the single-level primes to $\hat{v}_m(k)$ [note, (5.25)]. This chapter completes the denominator estimate: it bounds $\sum_p \max(T_p, 0)\log p$ over the primes $p > \epsilon n$, which gives the *positive* part of c_i, and assembles the constants $c_1, \dots, c_5$. It covers [note, Section 5.4]: the relaxation [note, Lemma 5.28], the circle model, the cells [note, Lemma 5.31], the counting [note, Lemma 5.34], the prime sum [note, Proposition 5.36], the formula [note, (5.39)] and [note, Proposition 5.40]; their proofs in [note, Appendix C]; and the second part of [note, Appendix E], "The bound for c_i". We need from Chapter 11 the tree bound, the local losses $f_p(k,s)$ and the weak-duality step [note, (C.2)], Mertens' theorem and [note, Lemmas 5.18, 5.19]; from Chapter 12 the node data $o_k, g_k, \mathrm{VP}_k, \mathcal{Z}_k, z_k, D_k, \mu_k, \mu_{k,t}$ [note, Definition 5.20], the bound $\hat{v}_m(k)$ and the coverage rule; from Chapter 10 the idea of a Lagrange multiplier as a price and of a rigorous (ball-arithmetic) computation.

13.1 The goal

After Chapter 11 the primes split into three groups. For $p \le \epsilon n$ the small- and middle-primes lemmas give the first, second and last terms of [note, (5.38)],

$$\kappa(6-\kappa)\, n^2 \log n - \kappa(6-\kappa)\Big(\gamma + \frac{\log 3}{2} + \log\frac{1}{\epsilon}\Big) n^2 + (3\kappa\epsilon + 12.5\,\epsilon^2)\, n^2 + o(n^2)\ .$$

For $p > 3n$ the tree bound will turn out to be 0. What is left is the window $\epsilon n < p \le 3n$, about $\frac{3n}{\log n}$ primes, each of which can contribute up to order n to T_p (a class can hold $O(1)$ rows with a loss $O(1)$ per row, and there are $p \approx n$ classes), so the window contributes order $n \cdot n = n^2$ after weighting with $\log p$ and summing with the prime number theorem: a term $c^{\mathrm{win}} n^2$. The task of this chapter is to compute an explicit upper bound for c^{win}. The tool is a sequence of three simplifications, each costing only $O(1)$ per prime: (1) decouple the residue classes with a Lagrange multiplier; (2) observe that, for $p = \varrho n$, a class is a point on a circle of circumference ϱ, and its data depend only on where the point sits; (3) count the classes

of each kind with the length of an arc. Then $T_p \approx n\, g(\lambda, \varrho, \kappa)$, an explicit function, and the prime number theorem turns $\sum_p$ into $\int \mathrm{d}\varrho$.

Recall the objects. At a single-level prime ($p \geq 5$, $p^2 > 6n$) the tree of residue classes has one level below the root, and the tree bound [note, (5.14)] reads

$$-v_p(\Delta_K) \leq T_p = \max_s \Big[\sum_{k \in \mathcal{N}} f_p(k, s_k) - \sum_{c \bmod p} \Big(S_c^2 - \sum_{k \in c} s_k^2 \Big) \Big] , \tag{13.1}$$

the maximum over profiles $s = (s_k)_{k \in \mathcal{N}}$, $0 \leq s_k \leq 4$, $\sum_k s_k = K$, with $S_c = \sum_{k \in c} s_k$. Here $f_p(k, s) = \max_{0 \leq \ell \leq s(4-s)} \big(e_p(k, s, \ell) + \ell\, \eta_p(k) \big)$ is the local loss of the node k holding s rows, $e_p(k, s, \ell)$ the largest $-v_p$ of a minor $\det C_k[R]$ with $|R| = s$ and $\sum R - \binom{s}{2} = \ell$ [note, (5.12)], and $\eta_p(k) = \max_{m \neq k} v_p(k - m)$ (Chapter 11). The term $S_c^2 - \sum s_k^2$ is the refund from the cross factor: twice the number of pairs of rows that sit at different nodes of the same class.

13.2 The relaxation: Lemma 5.28

The maximum (13.1) couples all nodes through the single constraint $\sum s_k = K$, and its local losses need the exact minors. The relaxation replaces both by something that can be evaluated from the node data alone.

13.2.1 From f_p to f^+

Let $\check{v}_m(k)$, $0 \leq m \leq 3$, be any integers with $v_p(c_{k,m}) \geq \check{v}_m(k)$ (Gauss valuation), for instance the refined bound $\hat{v}_m(k)$ of Chapter 12. We bound $f_p(k, s)$ in three steps.

Step 1: a minor as a sum over permutations. The minor $\det C_k[R]$ is the determinant of the $s \times s$ matrix with entries $c_{k, R_b + b'}$, $b, b' < s$. The Leibniz formula gives $\det C_k[R] = \sum_\pi \operatorname{sgn}(\pi) \prod_{b<s} c_{k, R_b + \pi(b)}$, the sum over the permutations π of $\{0, \dots, s-1\}$. Since $c_{k,a} = 0$ for $a \geq 4$ ([note, Definition 2.23]), only the permutations with $R_b + \pi(b) \leq 3$ for all b contribute; call such pairs (R, π) *admissible*.

Step 2: the ultrametric inequality. The valuation of a product is the sum of the valuations, and the valuation of a sum is at least the minimum. So

$$v_p\big(\det C_k[R]\big) \geq \min_\pi \sum_b \check{v}_{R_b + \pi(b)}(k) , \qquad \text{i.e.} \qquad -v_p\big(\det C_k[R]\big) \leq \max_\pi \sum_b -\check{v}_{R_b + \pi(b)}(k) .$$

(If the minor is 0, the left side is $-\infty$ and the inequality is trivial.)

Step 3: the price of the degree units. At a single-level prime two nodes are never congruent modulo p^2, so $\eta_p(k) = 1$ if k has a partner (another node of its class modulo p) and 0 otherwise: $\eta_p(k) = [o_k > 0]$ in the notation of [note, Definition 5.20]. Inserting Steps 1–2 into the definition of f_p, with $\ell = \sum R - \binom{s}{2}$,

$$\begin{aligned} f_p(k, s) \leq f^+(k, s) := \max \Big(0,\ \max_{(R, \pi)} \Big[\sum_{b<s} -\check{v}_{R_b + \pi(b)}(k) \\ + \Big(\sum R - \binom{s}{2} \Big) [o_k > 0] \Big] \Big) \end{aligned} \qquad (1 \leq s \leq 4) , \tag{13.2}$$

and $f^+(k, 0) = 0$. This is [note, (5.29)]. The outer $\max(0, \cdot)$, the *clipping*, only increases the right side, so the inequality stays true.

Intuition: the two terms of f^+. The first term is the worst denominator a single product of s local constants can have: row b of the minor uses the Taylor order R_b of the polynomial and column $\pi(b)$ adds $\pi(b)$ to it, and every constant $c_{k,m}$ is charged its

worst-case p-adic size $-\check{v}_m(k)$. The second term is the cross factor's contribution, $\ell = |\lambda_k|$ units of degree (Chapters 9 and 11). Each unit is paid for by giving up one factor $(k-m)$ of a node difference; that factor is divisible by p exactly when m is a partner of k, so each unit can cost one power of p, and only at nodes with a partner. Choosing high rows R (large $\sum R$) uses higher Taylor orders, which are p-adically smaller by the linear growth of $\check{v}_m$ in m, but demands more degree units; the two effects compete, and f^+ is the worst case.

The note does not say why it clips; dropping the clipping would give an equally valid bound. One consequence of the clipping is $f^+ \geq 0$: a node is never credited with a *negative* loss.

Example 13.1 (f^+ for nodes of $n = 11$, $p = 23$)**.** Take the node data of Chapter 12 for $n = 11$, $p = 23$. The node $k = 18$ has $o = 1$, VP $= \mathcal{Z} = \{1, 2\}$, $D = -2$, and $\hat{v}(18) = (-4, -3, -2, -1)$ ([note, (5.25)]: every virtual pole has $\mu_{k,t} = 1$, and the second term $-D - 3 - (3 - m) = m - 4$ is the smallest). For $s = 2$ there are nine admissible pairs (R, π), e.g. $R = \{0, 1\}$, $\pi = \mathrm{id}$ uses $c_{k,0}c_{k,2}$ and gives $4 + 2 + (1 - 1) = 6$; $R = \{2, 3\}$ with the swap uses $c_{k,3}c_{k,3}$ and gives $1 + 1 + (5 - 1) = 6$. A direct computation gives the value 6 for all nine. This is no accident: $-\hat{v}_m(18) = 4 - m$ is affine in m with slope -1, so for any admissible pair the sum is $4s - \sum R - \binom{s}{2} + \sum R - \binom{s}{2} = 4s - s(s-1)$, independent of (R, π); the degree units exactly pay back what the higher Taylor orders save. So $f^+(18, s) = 0, 4, 6, 6, 4$ for $s = 0, \ldots, 4$. The same computation for $k = -5$ ($o = 1$, VP $= \emptyset$, $\mathcal{Z} = \{-2, -1\}$, $D = -2$, $\hat{v} = (-1, 0, 1, 2)$) gives $s - s(s-1) = 1, 0, -3, -8$ for $s = 1, \ldots, 4$, which the clipping turns into $f^+(-5, s) = 0, 1, 0, 0, 0$. The nodes with $\hat{v} = (-7, -6, -5, -4)$ (e.g. $k = 12$ and $k = -11$, $D = 1$) have $f^+ = 0, 7, 12, 15, 16$, and the nodes $k = 5$ (nothing special) and $k = 8$ (a covered virtual pole, alone) have $\hat{v} = (0, 0, 0, 0)$ and $f^+ \equiv 0$.

13.2.2 One problem per class

Group the sum in (13.1) by classes, and bound each f_p by f^+:

$$T_p \leq \max_s \sum_{c \bmod p} \Big[\sum_{k \in c} \big(f^+(k, s_k) + s_k^2\big) - S_c^2 \Big] . \tag{13.3}$$

The bracket depends only on the occupations inside the class c. If we fix the class totals S_c, the occupations inside different classes can be chosen independently, and the best choice inside c gives

$$V_c(S) = \max \Big\{ \sum_{k \in c} \big(f^+(k, s_k) + s_k^2\big) : \ 0 \leq s_k \leq 4, \ \sum_{k \in c} s_k = S \Big\} - S^2 , \qquad 0 \leq S \leq 4|c| , \tag{13.4}$$

the first line of [note, (5.30)]. Hence [note, (C.3)]

$$T_p \leq T_p^+ := \max \Big\{ \sum_c V_c(S_c) : \ \sum_c S_c = K \Big\} . \tag{13.5}$$

Intuition. $V_c(S)$ is the worst loss of the class c when it receives S rows: the rows are distributed over its nodes (at most 4 per node) to maximize the local losses minus the refund $S^2 - \sum s_k^2$, which penalizes rows at different nodes of the class. A single node ($|c| = 1$) has $V_c(S) = f^+(k, S)$. A class is a small subsystem with an internal optimization; the classes interact only through the total number of rows, K.

Example 13.2 (two classes for $n = 11$, $p = 23$)**.** The class $\{-5, 18\}$: with $a_{18}(s) = f^+(18, s) + s^2 = 0, 5, 10, 15, 20$ and $a_{-5}(s) = 0, 2, 4, 9, 16$,

$$V(1) = \max(5, 2) - 1 = 4, \qquad V(2) = \max(10,\ 5+2,\ 4) - 4 = 6,$$
$$V(4) = \max(20,\ 15+2,\ 10+4,\ 5+9,\ 16) - 16 = 4,$$
$$V(5) = \max(20+2,\ 15+4,\ 10+9,\ 5+16) - 25 = -3,$$

and in all $V_{\{-5,18\}}(S) = 0, 4, 6, 6, 4, -3, -10, -18, -28$ for $S = 0, \dots, 8$. For $S \le 5$ the best placement puts as many rows as possible at the node 18 (for $S = 6, 7$ the best splits are $(s_{18}, s_{-5}) = (2, 4)$ and $(3, 4)$, as $26 > 24$ and $31 > 29$): splitting the rows between the two partners costs a refund of $2s_{18}s_{-5}$. The class $\{-11, 12\}$ (both nodes with $\hat{v} = (-7, -6, -5, -4)$) has $V(S) = 0, 7, 12, 15, 16, 15, 12, 7, 0$: symmetric, because both nodes have $f^+(s) + s^2 = 8s$, so every split gives $8S$ and $V(S) = 8S - S^2$.

13.2.3 The price of a row: ψ_c and weak duality

(13.5) is a resource-allocation problem: K rows, p classes, a payoff $V_c(S_c)$ per class. Lagrange's idea: instead of enforcing $\sum S_c = K$, charge a price λ per row and let every class choose freely. Define the second line of [note, (5.30)],

$$\psi_c(\lambda) = \max_{0 \le S \le 4|c|} \left(V_c(S) - \lambda S\right) . \tag{13.6}$$

Lemma 13.3 (relaxation; [note, Lemma 5.28])**.** *Let p be single-level and $\check{v}_m(k) \le v_p(c_{k,m})$ integers, for instance $\hat{v}_m(k)$. With f^+, V_c, ψ_c as in (13.2), (13.4), (13.6): $T_p \le T_p^+$, and for every real λ*

$$T_p^+ \le \lambda K + \sum_{c \bmod p} \psi_c(\lambda) . \tag{13.7}$$

Proof, following [note, Appendix C]. The first inequality is (13.3)–(13.5), derived above from $f_p \le f^+$. For the second, take any (S_c) with $\sum_c S_c = K$. Then, adding and subtracting λS_c,

$$\sum_c V_c(S_c) = \lambda \sum_c S_c + \sum_c \left(V_c(S_c) - \lambda S_c\right) = \lambda K + \sum_c \left(V_c(S_c) - \lambda S_c\right) \le \lambda K + \sum_c \psi_c(\lambda) ,$$

because each bracket is one of the numbers whose maximum is $\psi_c(\lambda)$. The right side does not depend on (S_c), so it also bounds the maximum T_p^+. □

Intuition: chemical potential and Legendre transform. In statistical mechanics, a system that exchanges particles with a reservoir at chemical potential μ is described by the grand potential, in which the particle number is no longer fixed but priced. Here the rows are the particles, λ is the chemical potential, and each residue class becomes an independent subsystem in contact with the reservoir: it takes the number of rows $S_c(\lambda)$ that maximizes $V_c(S) - \lambda S$. A high price makes the classes take few rows, a low or negative price many. The bound (13.7) holds for *every* λ (weak duality), and it is best at the λ for which the classes together take about K rows. The function ψ_c is the Legendre–Fenchel transform of V_c (up to signs, the convex conjugate of $-V_c$): geometrically, $\psi_c(\lambda)$ is the intercept at $S = 0$ of the line of slope λ that touches the graph of V_c from above. Two consequences: ψ_c is convex and piecewise linear in λ, and it only sees the *upper concave hull* of V_c. If all V_c are concave, the bound is exact at the best λ (no duality gap); a non-concave V_c can leave a gap. This is the same device as [note, (C.2)] in Chapter 11, where every V_c was a parabola, and as the threshold c_* of the bathtub problem in Chapter 10.

Example 13.4 (ψ_c and the dual bound for $n = 11$, $p = 23$, $K = 33$)**.** For the class $\{-11, 12\}$, $V = 0, 7, 12, 15, 16, 15, 12, 7, 0$ is concave, and $\psi(\lambda) = 16, 9, 4, 1, 0, 0$ at $\lambda = 0, 2, 4, 6, 8, 10$, attained at $S = 4, 3, 2, 1, 0, 0$: as the price rises the class takes fewer rows. For $\{-5, 18\}$, $\psi = 6, 2, 0, 0, 0, 0$, attained at $S = 2, 1, 0, \dots$ (the smallest maximizers; there are ties at $S = 3, 2, 1$ for $\lambda = 0, 2, 4$). At $\lambda = 1$ one finds $\psi_c(1) = 12$ for the eight classes $\{k, k + 23\}$, $k \in \{-11, -10, -9, -8, -4, -3, -2, -1\}$, $\psi_c(1) = 4$ for $\{-7, 16\}$ and $\{-5, 18\}$, $\psi_c(1) = 2$ for $\{-6, 17\}$, and 0 for the twelve single nodes $0, \dots, 11$. So

$$\lambda K + \sum_c \psi_c(\lambda) = 33 + 8 \cdot 12 + 2 \cdot 4 + 2 = 139 \qquad (\lambda = 1)\ ,$$

and the exact T_p^+, computed by dynamic programming over the classes (max-plus convolution of the arrays V_c, as in Chapter 11), is also 139: no duality gap here. Chapter 12 found $T_{23}^+ = 139$, equal to the exact tree bound $T_{23} = 139$ and to the true $-v_{23}(\Delta_{33}) = 139$. This T_p^+ reproduces Chapter 12's whole column $208, 219, 175, 163, 139, 68, 36, 0, \dots, 0$ for the single-level primes $11, \dots, 61$ at $n = 11$.

The relaxation. Three inequalities, each elementary: a minor is bounded by its worst permutation term ($f_p \le f^+$); fixing the class totals decouples the classes ($T_p \le T_p^+$); and pricing the rows decouples the totals ($T_p^+ \le \lambda K + \sum_c \psi_c(\lambda)$ for every λ). The result is a sum over classes of a quantity, $\psi_c(\lambda)$, that depends only on the data $(\check{v}(k), [o_k > 0])_{k \in c}$ of the class.

13.3 The circle model

13.3.1 A residue class is a point on a circle

Fix $\varrho > 0$ and think of primes $p \approx \varrho n$. Rescale the nodes, $x = k/n \in [-1, 2]$, as in Chapter 10. The class of k_0 modulo p is $\{k_0 + mp\} \cap \mathcal{N}$; in the rescaled variable these are the points $x_0 + m\varrho$ in $[-1, 2]$, with $x_0 = k_0/n$ and $\varrho = p/n$. Points that differ by a multiple of ϱ give the same class, so a class is a point of the circle $\mathbb{R}/\varrho\mathbb{Z}$ of circumference ϱ. The p classes are the p points of the grid $\frac{1}{n}\mathbb{Z}/\varrho\mathbb{Z}$, with spacing $\frac{1}{n}$ around the circle.

Intuition. Wrap the segment $[-1, 2]$ around a circle of circumference ϱ. If $\varrho < 3$, the segment winds around more than once, and the nodes that land on top of each other are exactly the nodes of one class. For $\varrho = 2.2$, a point of the circle carries one or two nodes; for $\varrho = 0.05$ it carries 60 or 61.

13.3.2 The node data depend only on (x, ϱ)

Every condition in [note, Definition 5.20] is an inequality between integers of size $O(n)$, and dividing by n turns it into an inequality between $x = k/n$ and $\varrho = p/n$:

discrete condition	divided by n	role
$-n \le k \le 2n$	$-1 \le x \le 2$	k is a node
$0 < pt < 3k$	$0 < t\varrho < 3x$	$t \in \mathrm{VP}_k$ $(k > 0)$
$3k < pt < 0$	$3x < t\varrho < 0$	$t \in \mathrm{VP}_k$ $(k < 0)$
$3k - 3n < pt < 3k$	$3x - 3 < t\varrho < 3x$	$t \in \mathcal{Z}_k$
$m = k + jp \in \mathcal{N}$	$x + j\varrho \in [-1, 2]$	partners, o_k

So o_k, VP_k, $\mathcal{Z}_k$, $z_k = 3|\mathcal{Z}_k|$, and hence $\mu_{k,t}$, are functions of (x, ϱ). The exception is $g_k = [p \mid 2k - n]$, an arithmetic condition with no continuum analogue; the circle model sets $g = 0$, and the classes with $g_k = 1$ (all nodes with $2k \equiv n \pmod p$, a single class) are treated as exceptional in Section 13.5. With $g = 0$ the bound $\hat{v}(y) = (\hat{v}_0, \dots, \hat{v}_3)$ of [note, (5.25)] is a function of the position y of the node and of ϱ.

Definition 13.5 (type; [note, Section 5.4])**.** For $\varrho > 0$ and $x \in \mathbb{R}/\varrho\mathbb{Z}$, the *nodes of* x are the points $y \in (x + \varrho\mathbb{Z}) \cap [-1, 2]$, and $o + 1$ is their number. The *type* of x is the multiset of the pairs $(\hat{v}(y), [o > 0])$ over the nodes y of x, with $\hat{v}$ computed from (y, ϱ) and $g = 0$. For a type τ, ψ_τ is the function ψ_c of (13.6) for a class with these data.

By the definitions (13.2)–(13.6), ψ_c depends only on the type, so this is well defined.

Example 13.6 ($n = 11$, $p = 23$ as a point of the circle)**.** Here $\varrho = \frac{23}{11} = 2.0909$. The node $k = 18$ is $y = \frac{18}{11} = 1.6364$. VP: $0 < 2.0909\,t < 4.9091$ gives $t = 1, 2$. $\mathcal{Z}$: $1.9091 < 2.0909\,t < 4.9091$ gives $t = 1, 2$. Its class is $\{-5, 18\}$, $y \in \{-0.4545, 1.6364\}$, so $o = 1$. These are the data of Example 13.1, read off from (y, ϱ) alone.

13.4 Cells: Lemma 5.31

As x moves around the circle, its type changes only when one of its nodes crosses a *critical* position, where one of the conditions of the table switches. Which positions are critical?

- $y = -1$ and $y = 2$: a node enters or leaves $[-1, 2]$, so o changes;
- $y = 0$: the range of the virtual poles changes from $(0, 3y)$ to $(3y, 0)$;
- $3y = t\varrho$ with $3 \nmid t$: a virtual pole appears or the upper end of the zero range $\mathcal{Z}$ passes t;
- $3y - 3 = t\varrho$ with $3 \nmid t$: the lower end of $\mathcal{Z}$ passes t (this is the coverage rule $pt > 3(k - n)$ of Chapter 12).

Modulo ϱ, the third family reduces to $\frac{\varrho}{3}$ and $\frac{2\varrho}{3}$ ($t \equiv 1, 2 \pmod 3$) and the fourth to $1 + \frac{\varrho}{3}$ and $1 + \frac{2\varrho}{3}$. So all critical positions are, modulo ϱ, among the seven points [note, (5.32)]

$$-1, \quad 2, \quad 0, \quad \frac{\varrho}{3}, \quad \frac{2\varrho}{3}, \quad 1 + \frac{\varrho}{3}, \quad 1 + \frac{2\varrho}{3}\,. \tag{13.8}$$

They cut the circle into (at most) seven open arcs, and the type is constant on each arc.

Lemma 13.7 (cells; [note, Lemma 5.31])**.** *Let* $\mathcal{B} = \{3j/N : \ j \in \{1, 2, 3\},\ N \geq 1\}$. *On each open interval of* $(0, \infty) \setminus \mathcal{B}$ *(a* cell*) the cyclic order of the seven points* (13.8) *on* $\mathbb{R}/\varrho\mathbb{Z}$ *and the type of each open arc between consecutive points are constant. The arc lengths, computed with the winding numbers fixed at one interior point of the cell, are affine in* ϱ*, so the measure* $\mathrm{meas}_\tau(\varrho)$ *of the set of points of type* τ *is affine in* ϱ *on each cell;* $\mathrm{meas}_\tau^{[a,b]}$ *denotes its affine extension to the closed cell* $[a, b]$*. Moreover, for* $\varrho > 3$ *every node has* $\hat{v} \geq 0$*, and* $T_p^+ = 0$ *for every single-level prime* $p > 3n$*.*

Proof, following [note, Appendix C]. Coincidences. Each of the seven points has the form $\alpha + \beta\varrho$ with $\alpha \in \{-1, 0, 1, 2\}$ and $\beta \in \{0, \frac{1}{3}, \frac{2}{3}\}$. Two of them coincide modulo ϱ when $\alpha_1 + \beta_1\varrho = \alpha_2 + \beta_2\varrho + N'\varrho$ for an integer N', i.e. $\alpha_1 - \alpha_2 = (N' - \beta_1 + \beta_2)\varrho$. If $\alpha_1 = \alpha_2$, then $N' - \beta_1 + \beta_2 = 0$, impossible for two distinct points since then $\beta_1 \neq \beta_2$ and $\beta_1 - \beta_2 \in \{\pm\frac{1}{3}, \pm\frac{2}{3}\}$ is not an integer. If $\alpha_1 \neq \alpha_2$, multiply by 3: $\varrho = \frac{3(\alpha_1 - \alpha_2)}{3N' - 3\beta_1 + 3\beta_2}$, and up to sign this is $\frac{3j}{N}$ with $j = |\alpha_1 - \alpha_2| \in \{1, 2, 3\}$ and $N = |3N' - 3\beta_1 + 3\beta_2|$ a positive integer. So for $\varrho \notin \mathcal{B}$ the seven points are distinct.

Cyclic order. The seven points move continuously with ϱ. Inside a cell they never collide, so none can overtake another, and the cyclic order is constant.

Type. If x is not one of the seven points modulo ϱ, then no node of x is at a critical position, and every strict inequality of the table remains true under a small change of (x, ϱ);

so the type is locally constant on the set of such pairs. For an arc, the set of pairs (x, ϱ) with ϱ in the cell and x in the arc is connected (the arc's endpoints move continuously without colliding), and a locally constant function on a connected set is constant.

Lengths. Fix an interior point ϱ_* of the cell and write each point as $\alpha + (\beta + w)\varrho$ with the integer w chosen so that the value lies in $[0, \varrho_*)$. With these winding numbers fixed, a length is a difference of two such expressions (plus ϱ for the arc that wraps around), hence of the form $a + b\varrho$.

$\varrho > 3$. Since $[-1, 2]$ has length $3 < \varrho$, a class has at most one node: $o = 0$. Take a node $y > 0$. A virtual pole needs $0 < t\varrho < 3y \le 6$; as $2\varrho > 6$, only $t = 1$ is possible, and then $y > \frac{\varrho}{3} > 1$. It is covered, since $3y - 3 \le 3 < \varrho$; and it is alone, because $t = 2 \in \mathcal{Z}$ would need $2\varrho < 3y \le 6$, and $t = -1 \in \mathcal{Z}$ would need $3y - 3 < -\varrho$, i.e. $y < 1 - \frac{\varrho}{3} < 0$. A node $y < 0$ has no virtual pole, since $t\varrho \in (3y, 0) \subseteq (-3, 0)$ needs $|t|\varrho < 3$. So either VP $= \mathcal{Z} = \{1\}$ with $D = -3$ and $\mu_{k,1} = 0$, or VP $= \emptyset$ and $\mathcal{Z} \subseteq \{-1\}$ with $D \in \{0, -3\}$. Chapter 12 (Section "The cancellation in action") evaluated [note, (5.25)] in these cases: $\hat{v}_m = 0$, $\hat{v}_m = m$, or $\hat{v}_m = 0$; all are ≥ 0. Then every term in (13.2) is ≤ 0 ($\ell\,[o > 0] = 0$), so $f^+ \equiv 0$, $V_c(S) = f^+(k, S) = 0$, and $T_p^+ = 0$. For a single-level prime $p > 3n$ the discrete data equal these continuum data, because $|2k - n| \le 3n < p$ forces $g_k = 0$. □

Example 13.8 (the breakpoints)**.** The set $\mathcal{B}$ accumulates at 0, but $[\frac{1}{20}, 3]$ contains only 237 of its points (both ends belong to $\mathcal{B}$: $\frac{1}{20} = \frac{3}{60}$, $3 = \frac{3}{1}$), so $[\frac{1}{20}, 3]$ is cut into 236 cells. Their widths range from 0.000141 near $\frac{1}{20}$ to 0.75 for the last cell $(\frac{9}{4}, 3)$; the points of $\mathcal{B}$ in $[\frac{3}{2}, 3]$ are $\frac{3}{2}, \frac{9}{5}, 2, \frac{9}{4}, 3$. Above 3 the next points are $\frac{9}{2}$ and 6.

13.4.1 The picture for $\varrho = 2.2$

Example 13.9 ($\varrho = \frac{11}{5}$)**.** $\varrho = 2.2$ lies in the cell $(2, \frac{9}{4})$. Reduced to $[0, 2.2)$, the seven points are 0, $1 + \frac{2\varrho}{3} \equiv 0.2667$, $\frac{\varrho}{3} = 0.7333$, $-1 \equiv 1.2$, $\frac{2\varrho}{3} = 1.4667$, $1 + \frac{\varrho}{3} = 1.7333$, 2, in this cyclic order. The types at the midpoints of the arcs, computed in exact rational arithmetic, are:

arc	length	nodes y (midpoint)	data of the nodes	type
$0 \to 1 + \frac{2\varrho}{3}$	$1 - \frac{\varrho}{3} = 0.2667$	0.1333	$\mathcal{Z} = \{-1\}$, $D = -3$; $\hat{v} = (0, 1, 2, 3)$	A
$1 + \frac{2\varrho}{3} \to \frac{\varrho}{3}$	$\frac{2\varrho}{3} - 1 = 0.4667$	0.5	nothing special; $\hat{v} = (0, 0, 0, 0)$	B
$\frac{\varrho}{3} \to -1$	$\frac{2\varrho}{3} - 1 = 0.4667$	0.9667	VP $= \mathcal{Z} = \{1\}$, alone; $\hat{v} = (0, 0, 0, 0)$	B
$-1 \to \frac{2\varrho}{3}$	$1 - \frac{\varrho}{3} = 0.2667$	-0.8667, 1.3333	$o = 1$, $D = 1$ both; $\hat{v} = (-7, -6, -5, -4)$ both	C
$\frac{2\varrho}{3} \to 1 + \frac{\varrho}{3}$	$1 - \frac{\varrho}{3} = 0.2667$	-0.6, 1.6	$(-1, 0, 1, 2)$ and $(-4, -3, -2, -1)$	D
$1 + \frac{\varrho}{3} \to 2$	$1 - \frac{\varrho}{3} = 0.2667$	-0.3333, 1.8667	$(-4, -3, -2, -1)$ and $(-7, -6, -5, -4)$	E
$2 \to 0$	$\varrho - 2 = 0.2$	-0.1	$\mathcal{Z} = \{-1\}$, $D = -3$; $\hat{v} = (0, 1, 2, 3)$	A

The lengths add up to ϱ. Types C, D, E have $o = 1$ (flag $[o > 0] = 1$); A and B have one node. The functions:

type	$V(S)$, $S = 0, 1, \ldots$	$\psi(\lambda)$ at $\lambda = 0, 2, 4, 6, 8$
A, B	$0, 0, 0, 0, 0$	$0, 0, 0, 0, 0$
C	$0, 7, 12, 15, 16, 15, 12, 7, 0$	$16, 9, 4, 1, 0$
D	$0, 4, 6, 6, 4, -3, -10, -18, -28$	$6, 2, 0, 0, 0$
E	$0, 7, 12, 15, 16, 12, 6, -2, -12$	$16, 9, 4, 1, 0$

At $\varrho = 2.01$ and $\varrho = 2.24$ (same cell) the arcs, their affine lengths and their types are identical. Since $\frac{23}{11} \in (2, \frac{9}{4})$, the classes of $n = 11$, $p = 23$ are points of this very picture; the class $\{-5, 18\}$ of Example 13.2 is of type D, and $\{-11, 12\}$, whose point $\frac{12}{11} = \varrho - 1$ is the critical point -1 itself, has the data of the adjacent arc of type C.

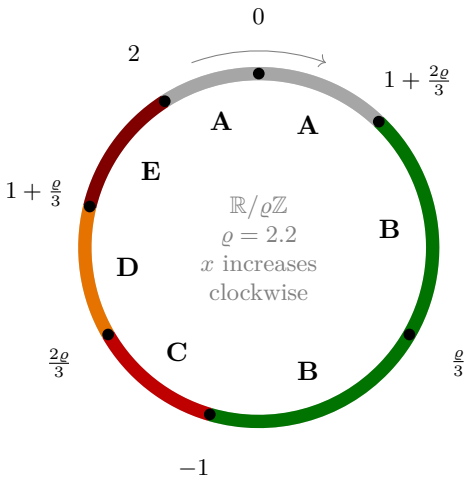


Figure 13.1: The circle $\mathbb{R}/\varrho\mathbb{Z}$ for $\varrho = 2.2$, with the seven points (13.8) (angle $90° - 360°x/\varrho$) and the type of each arc (Example 13.9). Grey (A): one node with a p-special zero only. Green (B): one node, no cost. Red and orange (C, D, E): two nodes with partners, where the losses sit. Every class of every prime p with $p/n \in (2, \frac{9}{4})$ is a point of this picture.

Intuition: why each of the seven points matters. Read Figure 13.1 clockwise. At 0 the single node of the point crosses $y = 0$ (the range of virtual poles switches sides; here the type happens not to change); from $1 + \frac{2\varrho}{3}$ on, its zero $t = -1$ has left the zero range (the node at $y = x$ in $(0.27, 0.73)$ has nothing special); at $\frac{\varrho}{3}$ the virtual pole $t = 1$ appears, covered and alone, so it costs nothing (type B again, but for a different reason); at $-1 \equiv 1.2$ a second node $y - \varrho \geq -1$ joins, and the class gets partners, which is where losses begin; at $\frac{2\varrho}{3}$ the virtual pole $t = 2$ appears at the upper node; at $1 + \frac{\varrho}{3}$ the virtual pole $t = 1$ of the upper node becomes uncovered ($3y - 3 > \varrho$), which raises its cost; at 2 the upper node leaves the node range, and the class is a single node again. The lower node changes at the same points: at $\frac{2\varrho}{3} \equiv -\frac{\varrho}{3}$ its uncovered virtual pole $t = -1$ disappears and the zero $t = -1$ enters $\mathcal{Z}$, and at $1 + \frac{\varrho}{3} \equiv 1 - \frac{2\varrho}{3}$ the zero $t = -2$ leaves $\mathcal{Z}$.

For $\varrho = 3.1, 4, 5, 6, 7$ a direct computation gives $\min \hat{v} = 0$ and $f^+ \equiv 0$ for all arc types, in line with the last part of Lemma 13.7; Chapter 12 found the same at the discrete level for $n = 5, 7, 11$.

13.5 Counting: Lemma 5.34

Put, for a closed cell $[a, b]$ and $\varrho \in [a, b]$, [note, (5.33)]

$$g_{[a,b]}(\lambda, \varrho, \kappa) = \lambda\kappa + \sum_{\tau} \operatorname{meas}_{\tau}^{[a,b]}(\varrho)\, \psi_{\tau}(\lambda) \ . \tag{13.9}$$

For fixed λ it is affine in ϱ (the measures are) and in κ. Its meaning: $n\, g$ is the dual bound $\lambda K + \sum_c \psi_c(\lambda)$ in which the number of classes of type τ is replaced by $n \operatorname{meas}_{\tau}$, the number of grid points of spacing $\frac{1}{n}$ that fit into the arcs of type τ.

Lemma 13.10 (counting; [note, Lemma 5.34], after [19]). *Fix a finite set $\mathcal{A} \subset \mathbb{R}$. There are C and n_0 such that for all $n \geq n_0$, all primes $p \in [\epsilon n, 3n]$, every closed cell $[a, b] \ni p/n$ and every $\lambda \in \mathcal{A}$,*

$$T_p \leq n\, g_{[a,b]}(\lambda, p/n, K/n) + C \ . \tag{13.10}$$

Proof, following [note, Appendix C]. Step 1: the relaxation applies. For $n \geq n_0$, $p \geq \epsilon n$ implies $p \geq 5$ and $p^2 \geq \epsilon^2 n^2 > 6n$, so p is single-level, and Lemma 13.3 with $\check{v} = \hat{v}$ gives $T_p \leq \lambda K + \sum_c \psi_c(\lambda)$.

Step 2: classes as grid points. $k_0 \mapsto k_0/n$ identifies $\mathbb{Z}/p$ with the grid $\frac{1}{n}\mathbb{Z}/\varrho\mathbb{Z}$ on $\mathbb{R}/\varrho\mathbb{Z}$, $\varrho = p/n$, and the data of the node $k_0 + mp$ are the continuum data at $y = x_0 + m\varrho$, except g_k (the table of Section 13.3).

Step 3: exceptional classes. Call a class exceptional if it contains a node with $g_k = 1$ or one of the nodes $-n, 0, 2n$ (which sit exactly at the critical positions $-1, 0, 2$). The nodes with $g_k = 1$ are those with $2k \equiv n \pmod{p}$, a single class, so there are at most 4 exceptional classes. A node of a non-exceptional class is never at a critical position: $3k = pt$ and $3k - 3n = pt$ with $3 \nmid t$ are impossible, since the right side is not divisible by 3 ($3 \nmid p$). So the type of a non-exceptional class is the type of the arc that contains its point, which is constant on the cell. If ϱ is an endpoint a or b of the closed cell, some arcs have length 0, and the arcs of positive length carry the types of the cell, by the local constancy of the type.

Step 4: grid points on arcs. An open arc of length ℓ contains between $n\ell - 1$ and $n\ell + 1$ points of a grid of spacing $\frac{1}{n}$. There are at most 7 arcs, so the number of non-exceptional classes of type τ is $n \operatorname{meas}_\tau^{[a,b]}(\varrho) + O(1)$, with $|O(1)| \leq 8$: at most ± 1 per arc, and the class with $g_k = 1$, which may lie on an open arc of type τ and is not counted.

Step 5: the size of ψ. $V_c(0) = 0$, so $\psi_c(\lambda) \geq V_c(0) - 0 = 0$. A class has at most $\frac{3n}{p} + 1 \leq \frac{3}{\epsilon} + 1$ nodes, and f^+ and $\hat{v}$ are bounded in terms of the number of nodes ($D_k \leq 4o_k$); so $0 \leq \psi_c(\lambda) \leq C_\epsilon(1 + |\lambda|)$ for every class, exceptional or not.

Step 6: assemble. Split $\sum_c \psi_c(\lambda)$ into the exceptional classes (at most $4C_\epsilon(1 + |\lambda|)$) and the others, $\sum_\tau (n \operatorname{meas}_\tau^{[a,b]} + O(1))\psi_\tau(\lambda)$. With $K = \kappa n$ this is $n\, g_{[a,b]}(\lambda, \varrho, \kappa) + O(1)$, and the $O(1)$ is uniform over $\lambda \in \mathcal{A}$ because $\mathcal{A}$ is finite. □

Example 13.11 (counting the classes of $n = 11$, $p = 23$)**.** With $\varrho = \frac{23}{11}$ the arcs of types C, D, E have length $1 - \frac{\varrho}{3} = \frac{10}{33}$ each, so $n \operatorname{meas} = \frac{10}{3} = 3.33$ for each; for A it is $\frac{13}{3} = 4.33$ and for B $\frac{26}{3} = 8.67$. The actual classes: type A: $\{0\}, \ldots, \{3\}$ (4); type B: $\{4\}, \ldots, \{11\}$ (8); type C: $\{-11, 12\}, \ldots, \{-8, 15\}$ (4); type D: $\{-7, 16\}, \{-5, 18\}$ (2); type E: $\{-4, 19\}, \ldots, \{-1, 22\}$ (4); and one class of no arc type, $\{-6, 17\}$, with $g_{-6} = g_{17} = 1$ ($2k - n = -23$ and 23). Three of these classes sit on critical points rather than on open arcs: $\{-11, 12\}$ (point -1) has the data of the adjacent arc C, $\{0\}$ (point 0) those of A, and $\{-1, 22\}$ (point 2) those of E; they are counted with these types. At $\lambda = 1$, $\psi_{\mathrm{C}} = \psi_{\mathrm{E}} = 12$, $\psi_{\mathrm{D}} = 4$, $\psi_{\mathrm{A}} = \psi_{\mathrm{B}} = 0$, so

$$n\, g(1, \tfrac{23}{11}, 3) = 11\Big(3 + \tfrac{10}{33}(12 + 4 + 12)\Big) = 126.33\ ,$$

against the discrete $33 + \sum_c \psi_c(1) = 139$ of Example 13.4. The difference 12.67 is: $+16$ from types C and E (4 classes instead of 3.33 each, i.e. $\frac{2}{3}$ of a class times 12, twice), -5.33 from type D (2 instead of 3.33, times 4), and $+2$ from the exceptional class.

Example 13.12 (the circle model against the exact T_p^+)**.** For $K = 3n$ the table compares the exact T_p^+ (dynamic programming over the classes, with the true g_k), the circle value $n\, g(\lambda^*, p/n, 3)$ at the λ^* that minimizes it on a grid of step 0.01, and the discrete dual bound at the same λ^*:

n	p	$\varrho = p/n$	λ^*	T_p^+	$n\,g(\lambda^*)$	$T_p^+ - n\,g$
11	13	1.1818	3.00	219	212.00	7.00
11	23	2.0909	1.00	139	126.33	12.67
11	31	2.8182	0.00	36	25.33	10.67
101	29	0.2871	3.00	4123	4091.67	31.33
101	53	0.5248	3.00	2731	2717.00	14.00
101	151	1.4950	3.00	1587	1572.00	15.00
101	223	2.2079	0.00	1024	1013.33	10.67
101	283	2.8020	0.00	264	253.33	10.67
1001	499	0.4985	3.00	27151	27129.00	22.00
1001	1499	1.4975	3.00	15559	15548.00	11.00
1001	2203	2.2008	0.00	10144	10133.33	10.67
1001	2803	2.8002	0.00	2544	2533.33	10.67

In all 27 computed cases (the table shows twelve of them) exactly one class has data different from the type of its point, and it is the class with $g_k = 1$. At λ^* the discrete dual bound $\lambda^* K + \sum_c \psi_c(\lambda^*)$ equals T_p^+ in all rows of the table (no duality gap); among the 27 cases it exceeds T_p^+ only at $n = 11$, $p = 11$ and 19, and $n = 101$, $p = 101$, by 2 to 3 (whether this comes from the grid for λ or from a non-concave V_c is left open here). Over all 27 cases the difference $T_p^+ - n\,g$ lies between 3.7 and 31.4, while T_p^+ ranges from 36 to 27151; at $\varrho \approx 2.8$ it is 10.67 for $n = 11$, 101 and 1001 alike, and at $\varrho \approx 2.2$ for $n = 101$ and 1001. This is the $O(1)$ of Lemma 13.10 seen in numbers. The price λ^* is 0 in all rows with $\varrho \geq 2.2$, 3 in those with $\varrho \leq 1.55$ except $\varrho = 1$, and 1 or 2 in between. A price 0 means that the costly classes (types C, D, E) already receive the numbers of rows they prefer and the remaining rows go to free classes (types A, B, with $V \equiv 0$) at no cost; when the costly classes would want more than K rows in total, the price becomes positive. At $\varrho = 2.2$, for instance, the classes of types C and E prefer 4 rows and those of type D 2 or 3 (Example 13.9); each of the three arcs has length 0.2667, so these classes take about $(4+4+2)\cdot 0.2667\,n = 2.67n$ to $(4+4+3)\cdot 0.2667\,n = 2.93n$ rows, fewer than $K = 3n$.

Check yourself 13.13. Why can no grid point k_0/n fall on the critical point $\frac{\varrho}{3}$ of the circle?

Answer. $k_0/n \equiv \frac{\varrho}{3} \pmod{\varrho}$ means $3k_0 = p(1+3m)$ for an integer m. The right side is not divisible by 3 (as $3 \nmid p$), the left side is. The same works for $\frac{2\varrho}{3}$, $1+\frac{\varrho}{3}$, $1+\frac{2\varrho}{3}$. Only $-1, 0, 2$ can be hit, by the nodes $-n, 0, 2n$.

13.6 The prime sum: Proposition 5.36

13.6.1 Three facts about primes

Fact 13.14 (prime number theorem; [16, 13])**.** $\vartheta(x) := \sum_{p \leq x} \log p = x + o(x)$ *as* $x \to \infty$.

Numerically, sieving the primes up to 10^7: $\vartheta(x)/x = 0.956245$, 0.989599, 0.996854, 0.998484, 0.999518 at $x = 10^3, \dots, 10^7$. For $n = 10^6$: $(\vartheta(3n) - \vartheta(0.05n))/n = 2.94838$ against 2.95, and $(\vartheta(2.25n) - \vartheta(2n))/n = 0.24982$ against 0.25. Intuitively, ϑ counts the primes with weight $\log p$, which exactly compensates their density $1/\log p$; so ϑ grows like the length of the interval, and the primes in $(an, bn]$ carry total weight $(b-a)n + o(n)$.

Partial summation. The note also uses $\sum_{p \leq x} p \log p = \frac{x^2}{2} + o(x^2)$. Partial summation is integration by parts for sums: if ϑ is the "antiderivative" of the weights $\log p$ (a step function jumping by $\log p$ at each prime), then $\sum_{p \leq x} p \log p = \int_{2-}^{x} t \, \mathrm{d}\vartheta(t)$, a Stieltjes integral, and

integrating by parts,

$$\sum_{p\le x} p\log p = x\,\vartheta(x) - \int_2^x \vartheta(t)\,\mathrm{d}t\ . \tag{13.11}$$

In discrete form: write $p\log p$ as $p\,(\vartheta(p)-\vartheta(p^-))$ and sum by parts (Abel summation), exactly as $\sum a_i b_i = A_N b_N - \sum A_i(b_{i+1}-b_i)$ for partial sums A_i. Inserting $\vartheta(t)=t+o(t)$: $x^2+o(x^2)-\frac{x^2}{2}+o(x^2)=\frac{x^2}{2}+o(x^2)$. Evaluating numerically, both sides of (13.11) agree (relative difference at most $2\cdot10^{-15}$, floating-point rounding) at $x=10^3,\dots,10^7$, and the ratio $\sum_{p\le x} p\log p/\frac{x^2}{2}$ is 0.969026, 0.995945, 0.998638, 0.998448, 0.999489.

Mertens' theorem with its constant. Chapter 11 stated it [29, (2.5), (2.8)]: $\sum_{p\le x}\frac{\log p}{p} = \log x + E + o(1)$ with $E=-\gamma-\sum_p\sum_{j\ge2}\frac{\log p}{p^j}$. The note needs the weight $\frac{\log p}{p-1}$ (the sum over the levels of the tree). Since $\frac{1}{p-1}=\frac{1}{p}+\frac{1}{p(p-1)}$ and $\sum_{j\ge2}p^{-j}=\frac{p^{-2}}{1-p^{-1}}=\frac{1}{p(p-1)}$,

$$\sum_{p\le x}\frac{\log p}{p-1} = \sum_{p\le x}\frac{\log p}{p} + \sum_{p\le x}\sum_{j\ge2}\frac{\log p}{p^j} = \log x - \gamma - \sum_{p>x}\sum_{j\ge2}\frac{\log p}{p^j} + o(1) = \log x - \gamma + o(1)\ ,$$

which is [note, (C.4)]; the tail $\sum_{p>x}\frac{\log p}{p(p-1)}$ tends to 0. The note excludes $p=3$ (the 3-adic part is the gain, Chapter 8); the term $p=3$ is $\frac{\log 3}{3-1}=\frac{\log 3}{2}=0.549306$, so

$$\sum_{p\le x,\,p\ne3}\frac{\log p}{p-1} = \log x - \gamma - \frac{\log 3}{2} + o(1)\ .$$

Chapter 11 checked [note, (C.4)] numerically up to $x=10^7$.

13.6.2 The statement

Proposition 13.15 (the prime sum; [note, Proposition 5.36])**.** *Let $\epsilon=a_0<a_1<\dots<a_M=3$ be a partition of $[\epsilon,3]$ that refines $\mathcal{B}\cap[\epsilon,3]$, let $\lambda_1,\dots,\lambda_M$ be rationals, and $[\kappa_1,\kappa_2]\subseteq[2.8,3]$. Put [note, (5.37)]*

$$\bar g_\nu = \max\big\{g_{[a,b]}(\lambda_\nu,\varrho,\kappa):\ \varrho\in\{a_{\nu-1},a_\nu\},\ \kappa\in\{\kappa_1,\kappa_2\}\big\}\ , \tag{13.12}$$

$[a,b]$ the closed cell containing $[a_{\nu-1},a_\nu]$. Then, uniformly for $K/n\in[\kappa_1,\kappa_2]$, [note, (5.38)]

$$\begin{aligned}\sum_{p\ne3}\max(T_p,0)\log p \le{}& \kappa(6-\kappa)\,n^2\log n - \kappa_1(6-\kappa_1)\Big(\gamma+\frac{\log3}{2}+\log\frac{1}{\epsilon}\Big)n^2\\ &+\Big(\sum_{\nu=1}^{M}\max(\bar g_\nu,0)(a_\nu-a_{\nu-1})+3\kappa_2\epsilon+12.5\,\epsilon^2\Big)n^2+o(n^2)\ .\end{aligned} \tag{13.13}$$

Intuition. The sum over ν is a Riemann sum (an upper one) for $\int_\epsilon^3\max\big(\min_\lambda g(\lambda,\varrho,\kappa),0\big)\mathrm{d}\varrho$: the primes near ϱn have total weight $n\,\mathrm{d}\varrho$ by the prime number theorem, and each costs about $n\,g$. The subcells and corners are there to make it a finite computation.

13.6.3 Proof, following [note, Appendix C]

Split the primes $p\ne3$ into four ranges, with $Y=n^{0.9}$.

(i) $p\le Y$. By [note, Lemma 5.18], $T_p\le\frac{K(6n+4-K)}{p-1}+9K\mathfrak{l}_p+150n+K$. With weight $\log p$ and the $p\ne3$ version of [note, (C.4)], the leading terms give $K(6n+4-K)(\log Y-\gamma-\frac{\log3}{2})+$

$o(n^2)$ (the $o(1)$ of Mertens times $K(6n+4-K) = O(n^2)$). The other terms are at most $(9K\mathfrak{l}_2 + 154n)\vartheta(Y) = O(n \log n \cdot n^{0.9}) = o(n^2)$. (Chapter 11 measured how slowly this tends to 0.)

(ii) $Y < p \le \epsilon n$. For large n these primes satisfy $p^2 > n^{1.8} > 6n$ and $p \le 0.4n$, so [note, Lemma 5.19] applies: $T_p \le \frac{K(6n+4-K)}{p} + 3K + 25p$. Mertens' theorem for $\frac{\log p}{p}$ over $(Y, \epsilon n]$ gives $\log \frac{\epsilon n}{Y} + o(1)$ (the constant E cancels in the difference of two Mertens sums). The other terms: $3K\vartheta(\epsilon n) = 3\kappa\epsilon n^2 + o(n^2)$, and $25\sum_{p \le \epsilon n} p \log p = 12.5\,\epsilon^2 n^2 + o(n^2)$ by partial summation. Total: $K(6n+4-K)\log \frac{\epsilon n}{Y} + (3\kappa\epsilon + 12.5\epsilon^2)n^2 + o(n^2)$.

(iii) $\epsilon n < p \le 3n$. Let $p/n \in [a_{\nu-1}, a_\nu]$. By Lemma 13.10 with $\mathcal{A} = \{\lambda_1, \dots, \lambda_M\}$, $T_p \le n\, g_{[a,b]}(\lambda_\nu, p/n, K/n) + C$. For fixed λ_ν the function $g_{[a,b]}$ is affine in ϱ and in κ, so on the rectangle $[a_{\nu-1}, a_\nu] \times [\kappa_1, \kappa_2]$ its maximum is at a corner: $g \le \bar{g}_\nu$. (An affine function on an interval is largest at an endpoint; on a rectangle, apply this in each variable.) Hence $\max(T_p, 0) \le n \max(\bar{g}_\nu, 0) + C$. Summing with weight $\log p$ over the primes in $(a_{\nu-1}n, a_\nu n]$:

$$\sum_\nu \big(n \max(\bar{g}_\nu, 0) + C\big)\big(\vartheta(a_\nu n) - \vartheta(a_{\nu-1} n)\big) = n^2 \sum_\nu \max(\bar{g}_\nu, 0)(a_\nu - a_{\nu-1}) + o(n^2)\ ,$$

by Fact 13.14 for each of the M (fixed) intervals; the C terms add up to $C\vartheta(3n) = O(n)$.

(iv) $p > 3n$. Such a prime is single-level (for $n \ge 2$), and $T_p \le T_p^+ = 0$ by Lemma 13.7.

Adding. The leading terms of (i) and (ii) combine, $\log Y + \log \frac{\epsilon n}{Y} = \log n - \log \frac{1}{\epsilon}$, into

$$K(6n+4-K)\Big(\log n - \gamma - \frac{\log 3}{2} - \log \frac{1}{\epsilon}\Big)\ ,$$

and $K(6n+4-K) = \kappa(6-\kappa)n^2 + 4\kappa n$, whose second part contributes $O(n \log n)$. The function $\kappa(6-\kappa)$ is increasing on $[2.8, 3]$ (derivative $6 - 2\kappa \ge 0$), so the negative constant $-\kappa(6-\kappa)(\gamma + \frac{\log 3}{2} + \log \frac{1}{\epsilon})$ is largest, i.e. least negative, at $\kappa = \kappa_1$, and $3\kappa\epsilon$ is largest at κ_2; this makes the bound uniform in $\kappa \in [\kappa_1, \kappa_2]$. The term $\kappa(6-\kappa)n^2 \log n$ keeps the exact κ, because it must cancel against the size estimate. □

The prime sum. Four ranges: the small primes give $\log Y - \gamma - \frac{\log 3}{2}$ per unit of $K(6n+4-K)$ (Mertens with constant, $p = 3$ removed), the middle primes $\log \frac{\epsilon n}{Y}$ (Mertens without constant) plus the error $(3\kappa\epsilon + 12.5\epsilon^2)n^2$, the window $(\epsilon n, 3n]$ the Riemann sum of the circle model, and the primes above $3n$ nothing. The $n^2 \log n$ term is the sum of (i) and (ii), and $\gamma + \frac{\log 3}{2} + \log \frac{1}{\epsilon}$ is what remains of the logarithms.

13.7 The constants c_i

13.7.1 Formula (5.39) and Proposition 5.40

Divide (13.13) by $\log 2$ (bits instead of nats) and put $\epsilon = \frac{1}{20}$, so $\log \frac{1}{\epsilon} = \log 20$, $3\kappa_2\epsilon = \frac{3\kappa_2}{20}$, $12.5\epsilon^2 = \frac{12.5}{400}$. For $[\kappa_1, \kappa_2] = I_i = [2.80 + 0.04(i-1),\ 2.84 + 0.04(i-1)]$ [note, (3.7)], the note defines [note, (5.39)]

$$c_i = \frac{1}{\log 2}\Big[-\kappa_{1,i}(6-\kappa_{1,i})\Big(\gamma + \frac{\log 3}{2} + \log 20\Big) + \sum_{\nu=1}^{M} \max(\bar{g}_\nu, 0)(a_\nu - a_{\nu-1}) + \frac{3\kappa_{2,i}}{20} + \frac{12.5}{400}\Big]\ , \quad (13.14)$$

for the partition and the λ_ν of [note, Appendix E]. By Proposition 13.15, any other admissible partition and rationals would give a valid (possibly worse) bound. With this definition, [note, Theorem 3.10] follows: $(-v_p(\Delta_K))^+ \le \max(T_p, 0)$ by the tree bound, then (13.13) divided by $\log 2$.

Proposition 13.16 ([note, Proposition 5.40])**.** *$c_1, \dots, c_5$ are at most* 30.471829, 30.783002, 31.093465, 31.403655, 31.713600.

Example 13.17 ((5.39) from the printed sums)**.** [note, Appendix E] prints the five sums $\sum_\nu \max(\bar g_\nu, 0)(a_\nu - a_{\nu-1})$ rounded to seven decimals: 57.5996087, 57.8686577, 58.1240232, 58.3660091, 58.5946334. We evaluate (13.14) in ball arithmetic (128 bits, see Chapter 10 for what a ball is), widening each sum by its rounding error $\pm 5 \cdot 10^{-8}$. Here $\gamma + \frac{\log 3}{2} + \log 20 = 4.1222541$.

i	$\kappa_{1,i}$	$-\kappa_1(6-\kappa_1)(\gamma + \frac{\log 3}{2} + \log 20)$	$\frac{3\kappa_{2,i}}{20}$	c_i (ball)	printed bound
1	2.80	−36.9353966	0.426	[30.4718286, 30.4718287]	30.471829
2	2.84	−36.9947570	0.432	[30.7830014, 30.7830015]	30.783002
3	2.88	−37.0409263	0.438	[31.0934639, 31.0934641]	31.093465
4	2.92	−37.0739043	0.444	[31.4036547, 31.4036549]	31.403655
5	2.96	−37.0936911	0.450	[31.7135997, 31.7135998]	31.713600

Rounding the upper ends up to six decimals gives exactly the printed bounds. So the arithmetic from the printed sums to [note, Proposition 5.40] is confirmed. (A change of δ in a sum changes c_i by $\delta/\log 2 = 1.4427\,\delta$.)

Compare the sizes: the circle model contributes about $58/\log 2 \approx 84$ bits per n^2, and the negative term $-\kappa_1(6-\kappa_1)(\gamma + \frac{\log 3}{2} + \log 20)$ removes about $37/\log 2 \approx 53$; c_i is their difference. Most of that negative term is not Mertens' constant: of the factor $\gamma + \frac{\log 3}{2} + \log 20 = 4.122$, the part $\log 20 = \log \frac{1}{\epsilon} = 2.996$ is the part of $\log n$ that the primes up to ϵn do not produce (Mertens' theorem gives $\log(\epsilon n)$ there), and only $\gamma + \frac{\log 3}{2} = 1.127$ is the constant. The final margin $G - F^\dagger - c \geq 4.58$ ([note, Table 1], Chapter 7) is less than 6% of the circle contribution, which is why the refined bound of Chapter 12 matters.

13.7.2 How the sums are computed: Appendix E, second part

[note, Appendix E] describes the computation as follows. (i) The points of $\mathcal{B}$ in $(\frac{1}{20}, 3)$, with $\frac{1}{20}$ and 3, cut $[\frac{1}{20}, 3]$ into cells. (ii) For each cell an interior point ϱ_* is fixed, the seven points are ordered on $\mathbb{R}/\varrho_*\mathbb{Z}$, and each arc's length is recorded as an affine function of ϱ, and its type at the midpoint of the arc (Lemma 13.7 guarantees that these choices do not matter). (iii) The type gives $\hat v$ at each node by [note, (5.25)], then f^+ by [note, (5.29)], V_c by a dynamic programming over the nodes of the class (max-plus convolution of the arrays $f^+(k,\cdot) + (\cdot)^2$), and $\psi_\tau(\lambda)$ as the maximum of $V_c(S) - \lambda S$ over the vertices of the upper concave hull of V_c; this is allowed because a linear function of S attains its maximum over a set at a vertex of the set's convex hull, so the non-hull points never win. (iv) Each cell is cut into 32 subcells of equal length: these are the a_ν. (v) On each subcell and for each I_i, a rational λ_ν with denominator at most 10^6 is chosen by numerical minimization of the corner maximum $\bar g_\nu$; the choice affects only the quality of the bound. (vi) $\bar g_\nu$ and the sum are then exact rationals, and only (13.14) uses ball arithmetic.

Intuition: why subcells. $g_{[a,b]}(\lambda, \varrho, \kappa)$ is affine in ϱ for a *fixed* λ, but the best λ changes with ϱ, so $\min_\lambda g$ is concave in ϱ on each cell (a minimum of affine functions), not affine; a single λ per cell would be poor on a wide cell such as $(\frac{9}{4}, 3)$. Cutting into subcells lets λ follow ϱ, and the corners make the bound valid on the whole subcell without evaluating g at every prime.

Example 13.18 (a floating-point evaluation of the sums)**.** We carry out steps (i)–(iv) from the definitions: exact rationals for the cells, the seven points, the arc lengths and the types; $\hat v$, f^+, V_c and the hull in integers. Steps (v)–(vi) are done differently from the note: for each subcell we take the exact real minimizer of the corner maximum (which is convex and piecewise linear in λ; the minimum is at a breakpoint of some ψ_τ, at 0, or at a crossing of the two ϱ-corners,

and all of these are examined), and we work in double precision. This is an estimate, not a proof. Results (236 cells, 7552 subcells):

	I_1	I_2	I_3	I_4	I_5
sum, ours, 32 subcells	57.5996087	57.8686577	58.1240232	58.3660091	58.5946334
sum, paper	57.5996087	57.8686577	58.1240232	58.3660091	58.5946334
c_i, ours	30.471829	30.783001	31.093464	31.403655	31.713600
sum, ours, 4 subcells	58.7201167	58.9921972	59.2515101	59.4955444	59.7255714
c_i, ours, 4 subcells	32.088380	32.403926	32.720084	33.033230	33.345198

With the note's 32 subcells our five sums agree with the printed ones in all seven decimals. (Our c_i are rounded to nearest; the note rounds the upper end of a ball upwards, hence the differences of 10^{-6}.) With only 4 subcells per cell the bound is about 1.6 bits worse, which shows what the subcells buy. The agreement means that the note's printed sums are what its definitions give, in the reading of the definitions given in the text. It does not test the definitions themselves; for those, Chapter 12 compared $\hat{v}$ with exact valuations, and Example 13.12 compared the circle model with the exact T_p^+.

Example 13.19 (the numbers of Remark 5.27)**.** [note, Remark 5.27] (Chapter 12) says that at $\kappa = 3$ the model gives "about 31.5" bits per n^2 with $\hat{v}$, and "about 44" with the cruder bound that does not use the cancellation. Chapter 12 deferred to this chapter the question which cruder bound is meant. Evaluating the sum at the single point $\kappa_1 = \kappa_2 = 3$, over $\varrho \in [\frac{1}{20}, 6]$ (with a cruder bound the primes in $(3n, 6n]$ are no longer free), for three local bounds gives:

local bound, $\kappa = 3$	32 subcells	128 subcells	512 subcells
refined $\hat{v}$ [note, (5.25)]	31.704	31.529	31.485
intermediate: [note, (5.25)] with all $\mu_{k,t} = 1$	44.075	43.836	43.776
crude $-D_k - 6 + m$	111.908	–	–

(in bits per n^2; with $\hat{v}$ the range $(3, 6]$ adds nothing, as Lemma 13.7 says). The "intermediate" bound of Chapter 12, which charges every virtual pole as if it were uncovered, reproduces the remark's "about 44"; the literal crude bound gives about 112. So the remark's cruder bound is, in all likelihood, the intermediate one. With the refined bound, the 32-subcell evaluation gives 31.70 at $\kappa = 3$ (close to $c_5 = 31.71$, as the remark says), and refining the subcells lowers it towards about 31.5, the remark's value; the remark's 31.5 is presumably such a finer evaluation, i.e. close to the integral $\int \max(\min_\lambda g, 0)\, \mathrm{d}\varrho$. The remark is not part of the proof.

Remark on the note: the explanation of 31.5 against 31.72 in Remark 5.27. [note, Remark 5.27] explains the difference between "about 31.5" at $\kappa = 3$ and $c_5 \le 31.72$ by the fact that c_5 holds on all of $I_5 = [2.96, 3]$. In our evaluation the uniformity over I_5 accounts for only about 0.01 bits (31.704 at $\kappa = 3$ against 31.714 for I_5, both with 32 subcells); the remaining 0.2 bits come from the discretization into 32 subcells, which the finer evaluations above remove. This concerns only the wording of a remark that is not part of the proof; [note, Proposition 5.40] itself is reproduced exactly.

Check yourself 13.20. In the table of Example 13.12, the circle model always lies *below* the exact T_p^+. Does that contradict Lemma 13.10?

Answer. No. The lemma says $T_p \le n\, g + C$ for some constant C; the 27 computed cases show $T_p^+ - n\, g$ between 3.7 and 31.4, which behaves like such a constant, independent of n at fixed ϱ. In the prime sum it costs $C\vartheta(3n) = O(n)$, which is $o(n^2)$.

Summary of the chapter

For the primes $\epsilon n < p \le 3n$ the tree bound is evaluated asymptotically. The relaxation [note, Lemma 5.28] bounds each minor by its worst permutation term, which turns the local loss into the explicit $f^{+}(k,s)$ [note, (5.29)] built from the refined bound $\hat{v}$ and the price $[o_k > 0]$ per degree unit; it then decouples the residue classes, $T_p \le T_p^{+} = \max\{\sum_c V_c(S_c) : \sum S_c = K\}$, and prices the rows with a multiplier λ, $T_p^{+} \le \lambda K + \sum_c \psi_c(\lambda)$ with ψ_c the Legendre-type transform [note, (5.30)]. With $\varrho = p/n$ a class is a point of the circle $\mathbb{R}/\varrho\mathbb{Z}$, its data depend only on the position (except g_k), the type of a point is constant on the arcs cut out by the seven points [note, (5.32)], and the order of these points changes only at $\varrho \in \mathcal{B} = \{3j/N\}$ [note, Lemma 5.31]; for $\varrho > 3$ all types are free. Counting grid points on arcs gives $T_p \le n\, g_{[a,b]}(\lambda, p/n, K/n) + O(1)$ [note, Lemma 5.34], and the prime number theorem, partial summation and Mertens' theorem with its constant assemble [note, (5.38)] and the constants c_i [note, (5.39)]. The arithmetic of [note, Proposition 5.40] follows from the printed sums; a floating-point evaluation with the exact optimal λ per subcell reproduces the five printed sums to seven decimals; exact computations up to $n = 1001$ show the $O(1)$ of the counting lemma; and the cruder bound of [note, Remark 5.27] is most likely the one that charges every virtual pole as uncovered (44.08 bits per n^2 at $\kappa = 3$).

Carried forward to Chapters 7 and 15: the bounds $c_i \le 30.471829, \dots, 31.713600$ of [note, Proposition 5.40], which enter [note, Table 1], and through them the denominator estimate [note, Theorem 3.10].

Chapter 14

Estimate 4: non-vanishing at an auxiliary prime

Where we are. The criterion of Chapter 7 can only be applied to $F = \Delta_K$ at the hypothetical value $\zeta_3(5) = a/b$ if $\Delta_K(a/b) \neq 0$. This chapter explains the note's argument for this, following [note, Section 6] and [note, Appendix D]: the non-vanishing theorem [note, Theorem 3.13]. The note names it as one of three steps that do not carry over from the case $p = 2$ treated in [19], and it is the most intricate of them. The plan is the dominance lemma [note, Lemma 3.4] (Chapter 7): we compute the p-adic valuation of the constant coefficient $[X^0]\Delta_K$ *exactly*, at an auxiliary prime p with $2.1n + 2 \le p < 3n$, and show that every other coefficient $[X^j]\Delta_K$ has valuation at least j larger. We cover the node types [note, Lemma 6.1] and [note, Table 2], the counts [note, (6.3)] and $K(n,p)$ [note, (6.4)], the functions Φ_k [note, (6.5)]–[note, (6.6)], the scaled local constants [note, Lemma 6.7], Wilson's theorem and the partner congruence [note, Lemma 6.10], Hermite interpolation [note, Lemma 6.12], the Gram matrix in an adapted basis [note, (6.13)]–[note, (6.15)], the weighted valuations [note, (6.16)] and [note, Lemma 6.17] with the full case analysis of [note, Appendix D], the field $\mathbb{Q}_p(\sqrt{p})$, the block reduction [note, Lemma 6.18], the block determinants [note, (6.21)], [note, Remark 6.22], and the proof of [note, Theorem 3.13]. We need: valuations, $\mathbb{Z}_p$, units and $\mathbb{F}_p$ (Chapter 2); the weight W, $\widetilde{W}_k$, h_k, $H_k[b]$ and the local constants $c_{k,a} = \beta_{k,a} + X\alpha_{k,a}$ [note, (2.21)] (Chapter 5); the Hankel polynomial, the change-of-basis rule $\det\left(THT^{\mathsf{T}}\right) = (\det T)^2 \det H$ and the jet form [note, (2.27)] (Chapter 6); the dominance lemma, the bound $K(n,p) \le 3n - 2$, and $K(n,p) > 2.8n$ when $p \le 2.159n$ (Chapter 7); single-level primes, the node data [note, Definition 5.20], virtual poles [note, Lemma 5.22] and the refined bound $\hat{v}_m(k)$ [note, (5.25)] (Chapter 12); the relaxed tree bound [note, Lemma 5.28] (Chapter 13).

14.1 The strategy

Recall the dominance lemma [note, Lemma 3.4] (Chapter 7): if $F = \sum_j f_j X^j \in \mathbb{Q}[X]$ and $v_p(f_0) < v_p(f_j)$ for every $j \ge 1$, then $F(a/b) \neq 0$ whenever $p \nmid b$, because f_0 is then p-adically larger than every other term $f_j(a/b)^j$ and nothing can cancel it. The note applies this to $F = \Delta_K$ at a prime p in the window $2.1n + 2 \le p < 3n$, and since the window contains many primes for large n, one of them does not divide b (Chapter 7). So the whole task is a statement about the p-adic valuations of the coefficients of one explicit polynomial.

Example 14.1 (what is to be proved, in numbers)**.** Take $n = 5$ and $p = 13$ (indeed $2.1 \cdot 5 + 2 = 12.5 \le 13 < 15$). The note's recipe [note, (3.12)] gives $K = 10n - \frac{10(p-1)}{3} = 10$ (as $13 \equiv 1 \bmod 3$). We compute $\Delta_{10}(X)$ exactly, from the definitions: the local constants

[note, (2.21)] with the harmonic sums [note, (2.14)], the moments $\Lambda(y^m)$ by the jet form [note, (2.27)], and the 10×10 determinant [note, (2.25)] over $\mathbb{Q}[X]$. The 13-adic valuations of its eleven coefficients $[X^0], \dots, [X^{10}]$ are

$$-36,\ -35,\ -34,\ -33,\ -30,\ -27,\ -24,\ -19,\ -14,\ -9,\ -3\ .$$

The constant coefficient has the lowest valuation, strictly: it is dominant, and $\Delta_{10}(a/b) \neq 0$ for every a/b with $13 \nmid b$. Moreover $v_{13}([X^j]) \geq v_{13}([X^0]) + j$, with equality for $j = 1, 2, 3$. The note predicts both facts, and even the number -36, for every admissible (n, p); we will see where $36 = 16 + 16 + 6 - 2$ comes from.

The coefficients are huge (the constant coefficient has a numerator of 1410 bits and a denominator of 1712 bits), and we cannot compute them for general n. The note instead finds the p-adic leading behavior of the Hankel matrix, by an argument whose structure, as the note states, is that of [19]. The steps are:

1. *Pair up the nodes* (Section 14.2). Since $p > 1.5n$, two nodes are congruent modulo p only if they differ by exactly p. The nodes in $[p - n, 2n]$ (R nodes) have a partner $k - p$ (an L node); the rest (U nodes) are alone. All p-adic information of each node is read off from a short list (Table 14.1).
2. *Choose a basis adapted to the R nodes* (Section 14.3): polynomials E_x that have prescribed Taylor coefficients at the R nodes (Hermite interpolation). Changing the basis does not change p-adic valuations, because the transition matrix is invertible modulo p.
3. *Rescale and reduce.* Multiply row and column x of the Gram matrix $[\Lambda(E_x E_{x'})]$ by p^{θ_x}, with half-integer weights θ_x chosen so that every entry becomes p-integral and the important ones become units. Modulo $\sqrt{p}$ the rescaled matrix is block diagonal, one block per R node, and each block is an explicit matrix built from a few numbers $\phi_{k,b}$.
4. *Compute the blocks.* Their determinants are units (products of powers of $2, 3, 7$ and of units ε_R); at the Ra nodes this needs the partner congruence $\varepsilon_{k-p} \equiv -8\,\varepsilon_k$: Wilson's theorem makes the ratio of the factorial parts $\equiv -1$ (so its fourth power is $\equiv 1$), and the factor $-8 = (-2)^3$ comes from the covering triple zero shared by the two partners.

Intuition: rescaling to leading order. A physicist knows this manoeuvre from perturbation theory and from nondimensionalization. Suppose a symmetric matrix has entries of wildly different orders of magnitude, $M_{xx'} \sim \epsilon^{-\theta_x - \theta_{x'}}$. Rescaling $\tilde{M} = \Theta M \Theta$ with $\Theta = \mathrm{diag}(\epsilon^{\theta_x})$ makes every entry of order one, and $\det M = \epsilon^{-2\sum \theta_x} \det \tilde{M}$. If the leading-order part $\tilde{M}_0$ of $\tilde{M}$ is nondegenerate, then $\det \tilde{M} \approx \det \tilde{M}_0 \neq 0$, and the order of magnitude of $\det M$ is exactly $\epsilon^{-2\sum \theta}$. In the p-adic world $\epsilon = p$, and the analogy becomes *exact* rather than approximate: a p-adic unit plus anything divisible by p is still a unit (ultrametric inequality, Chapter 2), so "$\det \tilde{M}_0 \neq 0$ modulo p" gives the valuation of $\det M$ with no error term at all. Where the analogy stops: over $\mathbb{R}$ a small correction can still change the determinant by a small amount; over $\mathbb{Z}_p$ it cannot change its valuation.

Example 14.2 (the rescaling at $n = 5$, $p = 13$)**.** In the adapted basis of step 2 (ten conditions $x = (R, j)$): orders $j = 0, 1, 2, 3$ at the node $R = 8$, orders $0, 1$ at $R = 9$, orders $0, 1, 2, 3$ at

$R = 10$), the 13-adic valuations of the entries of $\Gamma^\beta = [\beta(E_x E_{x'})]$ are

	8.0	8.1	8.2	8.3	9.0	9.1	10.0	10.1	10.2	10.3
8.0	−7	−6	−5	−4	−3	−3	−3	−3	−3	−3
8.1	−6	−5	−4	−3	−2	−2	−2	−2	−2	−2
8.2	−5	−4	−3	−2	−1	−1	−1	−1	−1	−1
8.3	−4	−3	−2	−1	−1	0	0	0	0	0
9.0	−3	−2	−1	−1	−3	−2	−1	−1	−1	−1
9.1	−3	−2	−1	0	−2	−1	1	1	0	1
10.0	−3	−2	−1	0	−1	1	−7	−6	−5	−4
10.1	−3	−2	−1	0	−1	1	−6	−5	−4	1
10.2	−3	−2	−1	0	−1	0	−5	−4	0	0
10.3	−3	−2	−1	0	−1	1	−4	1	0	0

No structure is visible in the matrix: the off-diagonal entries are as large as some diagonal ones. With the weights $\theta_x = \frac{7}{2}, \frac{5}{2}, \frac{3}{2}, \frac{1}{2}$ at $R = 8$ and $R = 10$ and $\frac{3}{2}, \frac{1}{2}$ at $R = 9$, the valuations $\theta_x + \theta_{x'} + v_{13}(\Gamma^\beta_{xx'})$ of the rescaled matrix are all ≥ 0; marking an entry "0" if this is 0 and "·" if it is ≥ 1:

0	0	0	0	·	·	·	·	·	·
0	0	0	0	·	·	·	·	·	·
0	0	0	0	·	·	·	·	·	·
0	0	0	0	·	·	·	·	·	·
·	·	·	·	0	0	·	·	·	·
·	·	·	·	0	0	·	·	·	·
·	·	·	·	·	·	0	0	0	0
·	·	·	·	·	·	0	0	0	·
·	·	·	·	·	·	0	0	·	·
·	·	·	·	·	·	0	·	·	·

Modulo 13 only the three diagonal blocks survive. The rest of the chapter explains why this happens for every admissible (n, p), and what the blocks are.

14.2 The nodes and their local constants

Throughout, n is odd and p is a prime with $2.1n + 2 \leq p < 3n$. For $n = 1$ this interval is $[4.1, 3)$, empty; for $n = 3$ it is $[8.3, 9)$, which contains no prime. So $n \geq 5$ and $p \geq 13$. Such a p is single-level (Chapter 12): $p \geq 5$ and $p^2 \geq (2.1n)^2 > 6n$. So every integer that enters the local constants has $v_p \in \{0, 1\}$, and all the node data of [note, Definition 5.20] apply.

14.2.1 Partners

Recall from Chapter 12 that the *partners* of a node k are the other nodes $m \in \mathcal{N} = \{-n, \ldots, 2n\}$ with $m \equiv k \pmod p$. Two nodes satisfy $|k - m| \leq 3n < 2p$ (because $p > 1.5n$). A nonzero multiple of p of absolute value less than $2p$ is $\pm p$. So

$$m \text{ is a partner of } k \iff m = k \pm p \ .$$

Since $m = k - p \geq -n$ requires $k \geq p - n$, and $m = k + p \leq 2n$ requires $k \leq 2n - p$, the nodes fall into three groups [note, Section 6.1]:

- *R nodes*, $k \in [p - n, 2n]$: the partner is $k - p$ (to the *left*);
- *L nodes*, $k \in [-n, 2n - p]$: the partner is $k + p$ (to the *right*); these are exactly the partners of the R nodes;
- *U nodes*, $2n - p < k < p - n$: no partner ("unpaired").

A node cannot have two partners: $k-p \geq -n$ and $k+p \leq 2n$ together would need $2p \leq 3n$. The U range is nonempty because $p-n-(2n-p) = 2p-3n > 0$. The numbers of R and of L nodes are both $3n-p+1$.

Example 14.3 ($n=5$, $p=13$)**.** The nodes are $-5,\dots,10$. R nodes: $[p-n, 2n] = [8,10]$; L nodes: $[-5, 2n-p] = [-5,-3]$; the pairs are $\{8,-5\}$, $\{9,-4\}$, $\{10,-3\}$; U nodes: $-2,\dots,7$ (ten nodes). In $\mathbb{F}_{13}$ the sixteen nodes give the residues $8,9,10,11,12,0,1,\dots,10$: the classes of $8,9,10$ are hit twice, the others once.

Intuition. Seen through p-adic glasses, two numbers are "close" if their difference is divisible by p. The nodes are $3n+1$ points on a line of length $3n$, and p is a little larger than $2n$; reading them modulo p means wrapping the line around a circle of circumference p (the circle of Chapter 13). The line is longer than the circle but shorter than twice the circle, so the wrapped line overlaps itself once, on an arc of $3n-p+1$ points. The overlapping points are the R/L pairs; the rest of the circle is covered once (U nodes).

14.2.2 The thresholds

The node data of [note, Definition 5.20] are decided by comparing k with a few numbers. Recall from Chapter 12: $t \in \mathrm{VP}_k$ (a *virtual pole* $\rho_t = \frac{pt}{3}$, from the harmonic sum) iff $3 \nmid t$ and $0 < pt < 3k$ (for $k>0$) or $3k < pt < 0$ (for $k<0$); $t \in \mathcal{Z}_k$ (a p-special triple zero of $\widetilde{W}_k$ at $d = \frac{pt}{3}$) iff $3 \nmid t$ and $3k-3n < pt < 3k$; $g_k = 1$ iff $p \mid 2k-n$; and $D_k = -v_p(h_k) = 4o_k - z_k - g_k$ with o_k the number of partners and $z_k = 3|\mathcal{Z}_k|$.

Only $t \in \{\pm 1, \pm 2\}$ occur. In both definitions $|pt| < \max(|3k|, |3k-3n|) \leq 6n < 3p$, since $p > 2n$. So $|t| < 3$, and $t \neq 0$; $t = \pm 3$ would anyway be excluded by $3 \nmid t$. Here we need $p > 2n$; the window gives $p \geq 2.1n + 2$.

When does each t occur? Dividing by 3:

- $1 \in \mathrm{VP}_k \iff k > \frac{p}{3}$; $\quad 2 \in \mathrm{VP}_k \iff k > \frac{2p}{3}$; $\quad -1 \in \mathrm{VP}_k \iff k < -\frac{p}{3}$; $\quad -2 \in \mathrm{VP}_k$ never, as it would need $3k < -2p$, i.e. $k < -\frac{2p}{3} < -n$ (since $2p > 3n$).
- $t \in \mathcal{Z}_k \iff \frac{pt}{3} < k < n + \frac{pt}{3}$. For $t=2$ the upper limit $n + \frac{2p}{3} > 2n$ is automatic (as $2p > 3n$), so $2 \in \mathcal{Z}_k \iff k > \frac{2p}{3}$. For $t=-2$ the lower limit $-\frac{2p}{3} < -n$ is automatic, so $-2 \in \mathcal{Z}_k \iff k < n - \frac{2p}{3}$.
- $g_k = 1 \iff 2k-n = \pm p$: $2k-n$ is odd (as n is odd) with $|2k-n| \leq 3n < 2p$, so the only possible nonzero multiples of p are $\pm p$. Hence $g_k = 1$ exactly at the two nodes $k = \frac{n \pm p}{2}$, which are integers since n and p are odd.

Lemma 14.4 (the thresholds; [note, (6.2)])**.** *If $1.5n < p < 3n$, then*

$$-n < -\frac{p}{3} < n - \frac{2p}{3} < 2n - p < p - n < \frac{2p}{3} < n + \frac{p}{3} < 2n\ , \tag{14.1}$$

and moreover $n - \frac{p}{3} < p - n$ and $2n - p < \frac{p}{3}$.

Proof. Each inequality reduces to $p < 3n$ or to $2p > 3n$:

- $-n < -\frac{p}{3} \iff p < 3n$; $\quad -\frac{p}{3} < n - \frac{2p}{3} \iff \frac{p}{3} < n \iff p < 3n$; $\quad n - \frac{2p}{3} < 2n - p \iff \frac{p}{3} < n$;
- $2n - p < p - n \iff 3n < 2p$; $\quad p - n < \frac{2p}{3} \iff \frac{p}{3} < n$; $\quad \frac{2p}{3} < n + \frac{p}{3} \iff \frac{p}{3} < n$; $n + \frac{p}{3} < 2n \iff p < 3n$;
- $n - \frac{p}{3} < p - n \iff 2n < \frac{4p}{3} \iff 3n < 2p$; $\quad 2n - p < \frac{p}{3} \iff 2n < \frac{4p}{3} \iff 3n < 2p$. $\square$

The note states (14.1) "since $2.1n < p < 3n$"; the proof shows that $1.5n < p < 3n$ suffices for the ordering. The stronger lower limit $p > 2n$ is used for $|t| \leq 2$ above, and $2.1n + 2 \leq p$ for $K \leq 3n-2$ (Chapter 7).

Example 14.5 (the thresholds for $n = 5$, $p = 13$)**.** $-5 < -4.333 < -3.667 < -3 < 8 < 8.667 < 9.333 < 10$, and $n - \frac{p}{3} = 0.667 < 8$, $2n - p = -3 < 4.333 = \frac{p}{3}$. The integers between consecutive thresholds: $k = -5$; $k = -4$ in $(-4.333, -3.667)$; $k = -3$; the ten U nodes $-2, \dots, 7$; $k = 8$; $k = 9$; $k = 10$.

14.2.3 The types: Lemma 6.1 and Table 2

Lemma 14.6 (node types; [note, Lemma 6.1])**.** *The nodes fall into the types of Table 14.1. The partner of an Ra (Rb, Rb_g, Rc) node is an La (Lb, Lb_g, Lc) node, and the two nodes $\frac{n\pm p}{2}$ are partners.*

type	nodes k	data	D_k
Ra	$p - n \le k < \frac{2p}{3}$	$\mathrm{VP}_k = \{1\}$, covered; $\mathcal{Z}_k = \{1\}$	1
Rb	$\frac{2p}{3} < k < n + \frac{p}{3}$, $k \ne \frac{n+p}{2}$	$\mathrm{VP}_k = \mathcal{Z}_k = \{1, 2\}$, both covered	-2
Rb_g	$k = \frac{n+p}{2}$	as Rb, and $g_k = 1$	-3
Rc	$n + \frac{p}{3} < k \le 2n$	$\mathrm{VP}_k = \{1, 2\}$, $\mathcal{Z}_k = \{2\}$	1
La	$-n \le k < -\frac{p}{3}$	$\mathrm{VP}_k = \{-1\}$, not covered; $\mathcal{Z}_k = \{-2\}$	1
Lb	$-\frac{p}{3} < k < n - \frac{2p}{3}$, $k \ne \frac{n-p}{2}$	$\mathrm{VP}_k = \emptyset$, $\mathcal{Z}_k = \{-1, -2\}$	-2
Lb_g	$k = \frac{n-p}{2}$	as Lb, and $g_k = 1$	-3
Lc	$n - \frac{2p}{3} < k \le 2n - p$	$\mathrm{VP}_k = \emptyset$, $\mathcal{Z}_k = \{-1\}$	1
U	$2n - p < k < p - n$	no partner; U_1: $\frac{p}{3} < k$, $\mathrm{VP}_k = \mathcal{Z}_k = \{1\}$	-3
		U_2: $k < n - \frac{p}{3}$, $\mathrm{VP}_k = \emptyset$, $\mathcal{Z}_k = \{-1\}$	-3
		U_0: otherwise, $\mathrm{VP}_k = \mathcal{Z}_k = \emptyset$	0

Table 14.1: [note, Table 2]: the nodes at a prime p with $2.1n + 2 \le p < 3n$. R and L nodes have exactly one partner; $g_k = 0$ except at $\frac{n\pm p}{2}$. The names U_0, U_1, U_2 for the three U cases are ours.

Proof. We go through the eight intervals cut out by (14.1) and apply the rules of the previous subsection. Every R and L node has $o_k = 1$; every U node has $o_k = 0$.

Ra: $p - n \le k < \frac{2p}{3}$. $k \ge p - n > \frac{p}{3}$ (since $p - n > \frac{p}{3} \iff 2p > 3n$), so $1 \in \mathrm{VP}_k$; $k < \frac{2p}{3}$, so $2 \notin \mathrm{VP}_k$; $k > 0$, so no negative t. $\mathrm{VP}_k = \{1\}$. Zeros: $1 \in \mathcal{Z}_k$ needs $\frac{p}{3} < k < n + \frac{p}{3}$, true since $k < \frac{2p}{3} < n + \frac{p}{3}$; $2 \notin \mathcal{Z}_k$ as $k < \frac{2p}{3}$; $-1 \in \mathcal{Z}_k$ would need $k < n - \frac{p}{3}$, false since $k \ge p - n > n - \frac{p}{3}$; $-2 \in \mathcal{Z}_k$ would need $k < n - \frac{2p}{3} < 0$, false. $\mathcal{Z}_k = \{1\}$, and the virtual pole $t = 1$ is covered. $g_k = 0$, since $\frac{n+p}{2} > \frac{2p}{3}$ (equivalent to $3n > p$) and $\frac{n-p}{2} < 0$. $D_k = 4 \cdot 1 - 3 - 0 = 1$.

Rb and Rb_g: $\frac{2p}{3} < k < n + \frac{p}{3}$. $k > \frac{2p}{3}$ gives $1, 2 \in \mathrm{VP}_k$ and $2 \in \mathcal{Z}_k$; $\frac{p}{3} < k < n + \frac{p}{3}$ gives $1 \in \mathcal{Z}_k$; negative t are excluded as before. $\mathrm{VP}_k = \mathcal{Z}_k = \{1, 2\}$, both covered, $z_k = 6$. The node $\frac{n+p}{2}$ lies in this interval: $\frac{2p}{3} < \frac{n+p}{2} \iff p < 3n$, and $\frac{n+p}{2} < n + \frac{p}{3} \iff p < 3n$. So $D_k = 4 - 6 - 0 = -2$ for Rb and $D_k = 4 - 6 - 1 = -3$ for Rb_g.

Rc: $n + \frac{p}{3} < k \le 2n$. $\mathrm{VP}_k = \{1, 2\}$ as for Rb; $1 \notin \mathcal{Z}_k$ because $k > n + \frac{p}{3}$; $2 \in \mathcal{Z}_k$. $\mathcal{Z}_k = \{2\}$: the virtual pole $t = 2$ is covered and $t = 1$ is not. $g_k = 0$. $D_k = 4 - 3 = 1$.

La: $-n \le k < -\frac{p}{3}$. $k < 0$ and $3k < -p$, so $-1 \in \mathrm{VP}_k$; $-2 \notin \mathrm{VP}_k$ always. $-1 \in \mathcal{Z}_k$ needs $k > -\frac{p}{3}$: false. $-2 \in \mathcal{Z}_k$ needs $k < n - \frac{2p}{3}$: true, since $k < -\frac{p}{3} < n - \frac{2p}{3}$. Positive t need $k > \frac{p}{3}$: false. $\mathcal{Z}_k = \{-2\}$, and the virtual pole $t = -1$ is not covered. (A negative node's virtual poles are never covered, Chapter 12.) $g_k = 0$, since $\frac{n-p}{2} > -\frac{p}{3}$ ($\iff 3n > p$). $D_k = 4 - 3 = 1$.

Lb and Lb_g: $-\frac{p}{3} < k < n - \frac{2p}{3}$. Here $k < n - \frac{2p}{3} < 0$, and $k > -\frac{p}{3}$, so $\mathrm{VP}_k = \emptyset$. $-1 \in \mathcal{Z}_k$ since $-\frac{p}{3} < k < n - \frac{p}{3}$; $-2 \in \mathcal{Z}_k$ since $k < n - \frac{2p}{3}$. $\mathcal{Z}_k = \{-1, -2\}$. The node $\frac{n-p}{2}$ lies here: $-\frac{p}{3} < \frac{n-p}{2} \iff p < 3n$, $\frac{n-p}{2} < n - \frac{2p}{3} \iff p < 3n$. $D_k = -2$, resp. -3.

Lc: $n - \frac{2p}{3} < k \le 2n - p$. $k \le 2n - p < 0$ and $k > -\frac{p}{3}$, so $\mathrm{VP}_k = \emptyset$. $-1 \in \mathcal{Z}_k$ (as $k \le 2n - p < n - \frac{p}{3}$, by $n < \frac{2p}{3}$), $-2 \notin \mathcal{Z}_k$. $D_k = 4 - 3 = 1$.

U: $2n - p < k < p - n$. No partner, $o_k = 0$; $g_k = 0$ since $\frac{n \pm p}{2}$ are R/L nodes. Negative t in VP_k need $k < -\frac{p}{3}$, but $k > 2n - p > -\frac{p}{3}$; $2 \in \mathrm{VP}_k$ needs $k > \frac{2p}{3} > p - n$: impossible. So $\mathrm{VP}_k = \{1\}$ if $k > \frac{p}{3}$ and $\emptyset$ otherwise. Zeros: $1 \in \mathcal{Z}_k \iff k > \frac{p}{3}$ (the upper limit $n + \frac{p}{3} > p - n$ is automatic); $-1 \in \mathcal{Z}_k \iff k < n - \frac{p}{3}$ (the lower limit $-\frac{p}{3} < 2n - p < k$ is automatic); ± 2 are impossible ($k < \frac{2p}{3}$ and $k > n - \frac{2p}{3}$). The two ranges $k > \frac{p}{3}$ and $k < n - \frac{p}{3}$ are disjoint because $n - \frac{p}{3} < \frac{p}{3}$. This gives U_1 ($D_k = 0 - 3 - 0 = -3$), U_2 ($D_k = -3$), U_0 ($D_k = 0$).

Partners. $k \mapsto k - p$ maps $[p - n, \frac{2p}{3})$ onto $[-n, -\frac{p}{3})$, $(\frac{2p}{3}, n + \frac{p}{3})$ onto $(-\frac{p}{3}, n - \frac{2p}{3})$, $(n + \frac{p}{3}, 2n]$ onto $(n - \frac{2p}{3}, 2n - p]$, and $\frac{n+p}{2}$ to $\frac{n-p}{2}$. □

Intuition: what the letters mean. Think of the node as an observer at $y = -k$ looking at the line through p-adic glasses. Its p-special points are: its partner (a pole of order 4 at distance $\pm p$); the triple zeros of W at distance $\frac{p}{3}$ or $\frac{2p}{3}$ (or their negatives) that lie inside the comb $(-n, 0)$ of zeros; possibly the simple zero at $-\frac{n}{2}$; and the virtual poles at distance $\frac{p}{3}, \frac{2p}{3}$ in the direction of the origin (Chapter 12). The letter a/b/c says how many of the two triple zeros on its side are inside the comb: for Ra only the one at distance $\frac{p}{3}$, for Rb both, for Rc only the far one at $\frac{2p}{3}$. The L letters are those of the partner; for L nodes the roles of the near and the far zero are exchanged (La: $\mathcal{Z} = \{-2\}$, Lc: $\mathcal{Z} = \{-1\}$). For an R node the partner pole (charge $+4$) and one zero (charge -3) give $D = 1$; with both zeros, $D = -2$.

Example 14.7 (the full node table for $n = 5$, $p = 13$)**.** We compute $o_k, g_k, \mathrm{VP}_k, \mathcal{Z}_k, D_k$ from [note, Definition 5.20], read off the type, compare it with the interval rules of Table 14.1, and compare D_k with $-v_{13}(h_k)$ computed from the exact h_k:

k	type	o_k	g_k	VP_k	$\mathcal{Z}_k$	D_k	partner
-5	La	1	0	$\{-1\}$	$\{-2\}$	1	8
-4	Lb_g	1	1	$\emptyset$	$\{-2, -1\}$	-3	9
-3	Lc	1	0	$\emptyset$	$\{-1\}$	1	10
$-2, -1, 0$	U_2	0	0	$\emptyset$	$\{-1\}$	-3	–
$1, \ldots, 4$	U_0	0	0	$\emptyset$	$\emptyset$	0	–
$5, 6, 7$	U_1	0	0	$\{1\}$	$\{1\}$	-3	–
8	Ra	1	0	$\{1\}$	$\{1\}$	1	-5
9	Rb_g	1	1	$\{1, 2\}$	$\{1, 2\}$	-3	-4
10	Rc	1	0	$\{1, 2\}$	$\{2\}$	1	-3

All types agree with the table, and $D_k = -v_{13}(h_k)$ at all sixteen nodes. Note that $\frac{n+p}{2} = 9$ is the only node in the Rb range: here $N_{\mathrm{Rb}} = 1$ and there is no plain Rb node. By hand for $k = 9$: the virtual poles are $0 < 13t < 27$, $t = 1, 2$; the triple zeros are $12 < 13t < 27$, $t = 1, 2$ (the zeros $9 - j - \frac{r}{3} = \frac{13}{3}$ and $\frac{26}{3}$, from $3j + r = 14$ and 1); and $2k - n = 13$, so $g_9 = 1$. The same comparison, at every node, holds for all 14 pairs (n, p) with $n \le 17$ tested in Section 14.4, and for $(n, p) = (45, 97)$.

14.2.4 The counts and the number $K(n, p)$

Let N_{Ra}, N_{Rc} be the numbers of Ra and Rc nodes, and N_{Rb} the number of Rb and Rb_g nodes together (so $N_{\mathrm{Rb}} \ge 1$, the Rb_g node being one of them).

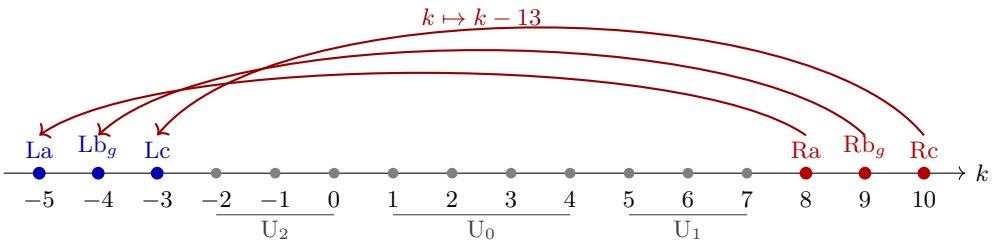


Figure 14.1: $n = 5$, $p = 13$: the nodes $-5, \dots, 10$ with their types (Example 14.7); arrows join each R node to its partner.

Proposition 14.8 (counts; [note, (6.3)], [note, (6.4)])**.**

$$N_{\mathrm{Ra}} = N_{\mathrm{Rb}} = N_{\mathrm{Rc}} = n - \frac{p-1}{3} \qquad (p \equiv 1 \bmod 3)\ ,$$

$$N_{\mathrm{Ra}} = N_{\mathrm{Rc}} = n - \frac{p-2}{3}\ , \quad N_{\mathrm{Rb}} = n - \frac{p+1}{3} \qquad (p \equiv 2 \bmod 3)\ ,$$

and in both cases the number $K(n,p)$ of [note, (3.12)] equals $4(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 2N_{\mathrm{Rb}}$.

Proof. Since $3 \nmid p$, the thresholds $\frac{2p}{3}$ and $n + \frac{p}{3}$ are not integers. For $p \equiv 1 \pmod 3$: the largest integer below $\frac{2p}{3}$ is $\frac{2p-2}{3}$, so $N_{\mathrm{Ra}} = \frac{2p-2}{3} - (p-n) + 1 = n - \frac{p-1}{3}$. The Rb range runs from $\frac{2p+1}{3}$ to $n + \frac{p-1}{3}$, so $N_{\mathrm{Rb}} = n + \frac{p-1}{3} - \frac{2p+1}{3} + 1 = n - \frac{p-1}{3}$. The Rc range runs from $n + \frac{p+2}{3}$ to $2n$, so $N_{\mathrm{Rc}} = n - \frac{p+2}{3} + 1 = n - \frac{p-1}{3}$. For $p \equiv 2 \pmod 3$: the Ra range ends at $\frac{2p-1}{3}$, giving $N_{\mathrm{Ra}} = n - \frac{p-2}{3}$; the Rb range runs from $\frac{2p+2}{3}$ to $n + \frac{p-2}{3}$, giving $N_{\mathrm{Rb}} = n - \frac{p+1}{3}$; the Rc range starts at $n + \frac{p+1}{3}$, giving $N_{\mathrm{Rc}} = n - \frac{p-2}{3}$. Finally, for $p \equiv 1$: $4 \cdot 2 + 2 = 10$ times $n - \frac{p-1}{3}$ is $10n - \frac{10(p-1)}{3}$; for $p \equiv 2$: $8(n - \frac{p-2}{3}) + 2(n - \frac{p+1}{3}) = 10n - \frac{8p-16+2p+2}{3} = 10n - \frac{10p-14}{3}$. Both are [note, (3.12)]. □

The bounds $K \le 3n - 2$ (from $p \ge 2.1n + 2$) and $K > 2.8n$ (if $p \le 2.159n$) were derived in Chapter 7. Why K has the form $4(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 2N_{\mathrm{Rb}}$ will become clear in Section 14.3.1: it is the number of rows that the p-adic tree bound wants to place in the R/L pairs.

For all 14 pairs (n,p) with $n \le 17$ odd and p prime in $[2.1n+2, 3n)$, and for $(n,p) = (45, 97)$, the counts read off from the computed types agree with [note, (6.3)], and $4(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 2N_{\mathrm{Rb}}$ agrees with [note, (3.12)]. For $n = 5$, $p = 13$: $N_{\mathrm{Ra}} = N_{\mathrm{Rb}} = N_{\mathrm{Rc}} = 1$ and $K = 10$.

14.2.5 The functions Φ_k: zooming in by a factor p

At the R nodes and the La nodes the virtual poles make the harmonic-sum part $\beta^{\mathrm{HS}}_{k,m}$ of the local constants p-adically large, and the note computes its leading term exactly. Recall [note, Lemma 5.22] (Chapter 12):

$$\beta^{\mathrm{HS}}_{k,m} = 2\,\mathrm{sgn}(k) \sum_{t \in \mathrm{VP}_k} [z^{3-m}]\, \widetilde{W}_k(z)\, (\rho_t - z)^{-3}\ , \qquad \rho_t = \frac{pt}{3}\ . \tag{14.2}$$

All the p-special points of $\widetilde{W}_k$ (partner pole, special zeros) and the virtual poles ρ_t sit at distances that are multiples of $\frac{p}{3}$, while all other zeros and poles are at distances that are p-adic units. The idea is to use p as the unit of length: substitute $z = pw$.

Definition 14.9 ([note, (6.5)])**.** For an R or La node k, write the p-special points of $\widetilde{W}_k$ as $d = p\delta$, with their orders e ($e = -4$ for the partner pole, $e = 3$ for a special triple zero, $e = 1$ for the special simple zero), and put

$$\Phi_k(w) = \mathrm{sgn}(k) \prod_{d = p\delta \ p\text{-special}} \Big(1 - \frac{w}{\delta}\Big)^{e} \sum_{t \in \mathrm{VP}_k} \Big(\frac{t}{3} - w\Big)^{-3}, \qquad \phi_{k,b} = [w^b]\, \Phi_k(w)\ .$$

Intuition. Φ_k is the node seen through a "p-adic microscope": only the features at distance of order p from the node are kept, measured in units of p, and everything at unit distance is blurred to the constant 1. Since the features depend only on the type of the node, so does Φ_k. The sum over t is the virtual poles, rescaled: $(\rho_t - pw)^{-3} = p^{-3}(\frac{t}{3} - w)^{-3}$.

We now derive each Φ from Table 14.1. The partner of an R node k is $k-p$, so the partner pole is at $d = k-(k-p) = p$, $\delta = 1$, $e = -4$: factor $(1-w)^{-4}$. A special triple zero with $t \in \mathcal{Z}_k$ is at $d = \frac{pt}{3}$, $\delta = \frac{t}{3}$: factor $(1 - \frac{3w}{t})^3$. The simple zero (Rb_g) is at $d = k - \frac{n}{2} = \frac{2k-n}{2} = \frac{p}{2}$, $\delta = \frac{1}{2}$, $e = 1$: factor $(1-2w)$.

- Ra: $\mathcal{Z} = \{1\}$, VP $= \{1\}$, sgn $= +1$: $\Phi_{\mathrm{Ra}} = (1-w)^{-4}(1-3w)^3(\frac{1}{3} - w)^{-3}$. Since $1 - 3w = 3(\frac{1}{3} - w)$, the zero and the virtual pole cancel to the constant 27 (the cancellation [note, (5.26)] of Chapter 12): $\Phi_{\mathrm{Ra}} = 27(1-w)^{-4}$.
- Rb: $\mathcal{Z} = \mathrm{VP} = \{1, 2\}$: $\Phi_{\mathrm{Rb}} = (1-w)^{-4}(1-3w)^3(1-\frac{3}{2}w)^3\,\Sigma(w)$ with $\Sigma(w) = (\frac{1}{3} - w)^{-3} + (\frac{2}{3} - w)^{-3}$.
- Rb_g: the same, times $(1-2w)$.
- Rc: $\mathcal{Z} = \{2\}$, VP $= \{1, 2\}$: $\Phi_{\mathrm{Rc}} = (1-w)^{-4}(1-\frac{3}{2}w)^3\,\Sigma(w)$.
- La: the partner is $k+p$, so $d = k-(k+p) = -p$, $\delta = -1$: factor $(1+w)^{-4}$; $\mathcal{Z} = \{-2\}$, $\delta = -\frac{2}{3}$: factor $(1+\frac{3}{2}w)^3$; VP $= \{-1\}$: $(-\frac{1}{3} - w)^{-3}$; and $\mathrm{sgn}(k) = -1$, so $-(-\frac{1}{3} - w)^{-3} = (\frac{1}{3} + w)^{-3}$. Hence $\Phi_{\mathrm{La}} = (1+w)^{-4}(1+\frac{3}{2}w)^3(\frac{1}{3} + w)^{-3}$.

Example 14.10 (the coefficients [note, (6.6)])**.** Expanding in exact rational arithmetic, the coefficients $\phi_{\bullet,b}$ for $b = 0, 1, 2, 3$ are

type	$b=0$	1	2	3
Ra	27	108	270	540
Rb	$\frac{243}{8}$	$-\frac{243}{8}$	$-\frac{243}{8}$	0
Rb_g	$\frac{243}{8}$	$-\frac{729}{8}$	$\frac{243}{8}$	$\frac{243}{4}$
Rc	$\frac{243}{8}$	243	$\frac{2673}{2}$	$\frac{50301}{8}$
La	27	$-\frac{459}{2}$	$\frac{5211}{4}$	$-\frac{49761}{8}$

These agree with all values printed in [note, (6.6)] (the note prints only the ones it needs: Ra and La for $b \le 3$, Rb and Rb_g for $b = 1, 2, 3$, Rc for $b = 0$). By hand for Ra: $27(1-w)^{-4} = 27(1 + 4w + 10w^2 + 20w^3 + \dots)$, i.e. $27, 108, 270, 540$. For Rc at $b = 0$: $\Phi_{\mathrm{Rc}}(0) = \Sigma(0) = 27 + \frac{27}{8} = \frac{243}{8}$. All denominators are powers of 2: they come from $(\frac{2}{3} - w)^{-3} = \frac{27}{8}(1 - \frac{3}{2}w)^{-3}$ and from $(1 \pm \frac{3}{2}w)^3$. Since $p \ge 13$, every $\phi_{\bullet,b}$ is p-integral.

14.2.6 Lemma 6.7: the scaled local constants

Lemma 14.11 ([note, Lemma 6.7])**.** *Let $\varepsilon_k = 2h_k p^{D_k}$, a p-adic unit. For the nodes of types Ra, Rb, Rb_g, Rc and La,*

$$\beta^{\mathrm{HS}}_{k,m} = \varepsilon_k\, p^{-D_k+m-6}(\phi_{k,3-m} + O(p)) \qquad (0 \le m \le 3)\ , \tag{14.3}$$

where $O(p)$ is an element of $p\mathbb{Z}_p$. Moreover $v_p(\beta^{\mathrm{rest}}_{k,m}) \ge -4+m$ and $v_p(\alpha_{k,m}) \ge -2+m$ at Ra, Rc, La, Lc; $v_p(\beta^{\mathrm{rest}}_{k,m}) \ge -1+m$ and $v_p(\alpha_{k,m}) \ge 1+m$ at Rb, Lb; $v_p(\beta^{\mathrm{rest}}_{k,m}) \ge m$ and $v_p(\alpha_{k,m}) \ge 2+m$ at Rb_g, Lb_g. At the U nodes all of $\beta^{\mathrm{HS}}_{k,m}$, $\beta^{\mathrm{rest}}_{k,m}$, $\alpha_{k,m}$ have $v_p \ge 0$.

Proof. ε_k is a unit because $v_p(h_k) = -D_k$ (Chapter 12) and $v_p(2) = 0$.

Step 1: the substitution. For any power series f, $f(pw) = \sum_b f_b p^b w^b$, so $[z^b]f(z) = p^{-b}[w^b]f(pw)$. Apply this with $b = 3-m$ to (14.2).

Step 2: factor $\widetilde{W}_k$. Write $\widetilde{W}_k(z) = h_k \prod_d (1 - z/d)^{e_d}$ over all nonzero zeros and poles d (Chapter 12), and split the product into the p-special $d = p\delta$ and the rest:

$$\widetilde{W}_k(pw) = h_k \prod_{p \mid d} \Big(1 - \frac{w}{\delta}\Big)^{e_d} U_k(pw) \ , \qquad U_k(z) = \prod_{p \nmid d} \Big(1 - \frac{z}{d}\Big)^{e_d} \ ,$$

using $1 - \frac{pw}{p\delta} = 1 - \frac{w}{\delta}$. Also $(\rho_t - pw)^{-3} = (p(\frac{t}{3} - w))^{-3} = p^{-3}(\frac{t}{3} - w)^{-3}$. This is [note, (6.9)].

Step 3: $U_k(pw) = 1 + O(p)$. Every non-special d is a p-adic unit (at a single-level prime each d has $v_p(d) \in \{0, 1\}$, and "non-special" means 0). The coefficient of z^b in $(1 - z/d)^e$ is the integer $\binom{e}{b}(-1)^b$ times d^{-b}, hence in $\mathbb{Z}_p$, so $U_k(z) \in \mathbb{Z}_p[[z]]$ with constant term 1. Substituting $z = pw$ multiplies the coefficient of w^b by p^b, so every coefficient of $U_k(pw) - 1$ lies in $p\mathbb{Z}_p$.

Step 4: assemble. Combining, $2\,\mathrm{sgn}(k)\,\widetilde{W}_k(pw) \sum_t (\rho_t - pw)^{-3} = 2h_k p^{-3}\,\Phi_k(w)\,U_k(pw)$, so

$$\beta^{\mathrm{HS}}_{k,m} = p^{-(3-m)} \cdot 2h_k p^{-3}\,[w^{3-m}](\Phi_k(w)U_k(pw)) = \varepsilon_k p^{-D_k+m-6}\,[w^{3-m}](\Phi_k(w)U_k(pw)) \ .$$

The coefficient is $\sum_{b+c=3-m} \phi_{k,b}[w^c]U_k(pw)$; the term $c = 0$ is $\phi_{k,3-m}$, and the terms $c \geq 1$ are p-integral numbers times elements of $p\mathbb{Z}_p$. This proves (14.3).

Step 5: the other bounds. They are the first and the third term of the refined bound [note, (5.25)] (Chapter 12), $-D_k - (3-m)\mu_k$ and $-D_k - (1-m)\mu_k$, with $\mu_k = 1$ (every R, L node has a special point) and D_k from the table: $D = 1$ gives $m-4$ and $m-2$; $D = -2$ gives $m-1$ and $m+1$; $D = -3$ gives m and $m+2$. At a U_1 node ($D = -3$, $\mu_k = 1$, the virtual pole covered and alone, $\mu_{k,1} = 0$) the three terms of [note, (5.25)] are $3-(3-m) = m$, $3-3-0 = 0$, $3-(1-m) = 2+m$; at a U_2 node ($D = -3$, no virtual pole) they are m and $2+m$; at a U_0 node $D = 0$, $\mu_k = 0$, and all terms are 0. □

Example 14.12 ([note, Lemma 6.7] at the Ra node $k = 8$, $n = 5$, $p = 13$)**.** $h_8 = -\frac{545719070217959}{428138278944496586444588050022400}$ has $v_{13}(h_8) = -1$, so $D_8 = 1$, and $\varepsilon_8 = 2h_8 \cdot 13 \equiv 1 \pmod{13}$. The exact $\beta^{\mathrm{HS}}_{8,m}$ have $v_{13} = -7, -6, -5, -4$ for $m = 0, 1, 2, 3$, i.e. $m - 7$ as (14.3) says. The residues of $\beta^{\mathrm{HS}}_{8,m} p^{D-m+6}/\varepsilon_8$ modulo 13 are $7, 10, 4, 1$, and those of $\phi_{\mathrm{Ra},3-m} = 540, 270, 108, 27$ are $7, 10, 4, 1$. In all 14 cases with $n \leq 17$, at every R and La node and every m, the difference $\beta^{\mathrm{HS}}_{k,m} p^{D_k-m+6}/\varepsilon_k - \phi_{k,3-m}$ lies in $p\mathbb{Z}_p$, all the bounds of the lemma on β^{rest} and α hold, all local constants at U nodes are p-integral, and $\beta^{\mathrm{HS}} = 0$ at the Lb, Lb_g, Lc nodes (which have no virtual pole).

14.2.7 Wilson's theorem

The units ε_k and ε_{k-p} of an Ra node and its La partner will meet in the same block of the reduced matrix, so we need their ratio modulo p. The tool is a classical theorem.

Theorem 14.13 (Wilson's theorem)**.** *For every prime p, $(p-1)! \equiv -1 \pmod{p}$. (E.g. Hardy and Wright,* An Introduction to the Theory of Numbers*, Ch. VI.)*

Proof. For $p = 2$: $1! = 1 \equiv -1$. Let p be odd. In the field $\mathbb{F}_p$ (Chapter 2) every $a \in \{1, \ldots, p-1\}$ has a unique inverse a^{-1}. If $a = a^{-1}$, then $a^2 \equiv 1$, so $p \mid (a-1)(a+1)$, and since p is prime, $a \equiv \pm 1$: only $a = 1$ and $a = p-1$ are their own inverses. All other elements fall into pairs $\{a, a^{-1}\}$ with $a \neq a^{-1}$, and each pair contributes $a \cdot a^{-1} \equiv 1$ to the product $(p-1)!$. So $(p-1)! \equiv 1 \cdot (p-1) \equiv -1$. □

Example 14.14 ($\mathbb{F}_{13}$)**.** The inverses of $1, \ldots, 12$ modulo 13 are $1, 7, 9, 10, 8, 11, 2, 5, 3, 4, 6, 12$ (as in Chapter 2). The pairs are $\{2, 7\}, \{3, 9\}, \{4, 10\}, \{5, 8\}, \{6, 11\}$, and 1, 12 are self-inverse. So $12! \equiv 1 \cdot 12 \cdot 1^5 = 12 \equiv -1$. Directly: $12! = 479001600 = 13 \cdot 36846276 + 12$. A direct computation confirms $(p-1)! \equiv -1$ for all primes $p < 200$, and that $1, p-1$ are the only square roots of 1 in each of these $\mathbb{F}_p$; for the composite 12, $11! \equiv 0 \pmod{12}$, so primality matters.

Intuition. The product of all nonzero elements of a finite field is -1 because almost everything cancels against its inverse. A useful corollary, used next: *any* p consecutive integers contain exactly one multiple of p, and the product of the other $p-1$ is $\equiv -1$, because they run through each nonzero residue exactly once.

14.2.8 Lemma 6.10: the partner congruence

Lemma 14.15 (partner congruence; [note, Lemma 6.10])**.** *If k is an Ra node, then $\varepsilon_{k-p} \equiv -8\,\varepsilon_k \pmod p$.*

Proof. Step 1. Both k (Ra) and $k-p$ (La) have $D=1$, so $\varepsilon_{k-p}/\varepsilon_k = h_{k-p}/h_k$.

Step 2: a formula for h_k. Write $W = N_W/\prod_{m\in\mathcal{N}}(y+m)^4$ with the numerator $N_W(y) = (y+\frac{n}{2})(y+\frac{1}{3})_n^3(y+\frac{2}{3})_n^3$ (Chapter 5). Then $\widetilde{W}_k(z) = z^4 W(-k+z)$, and at $z=0$ the factor $(y+k)^4 = z^4$ cancels, leaving

$$h_k = \frac{N_W(-k)}{\Pi(k)^4}\,, \qquad \Pi(k) = \prod_{m\neq k}(m-k) = (-1)^{k+n}(k+n)!\,(2n-k)!\,,$$

the last formula being [note, (2.18)] (Chapter 5).

Step 3: the ratio of the Π's. From the factorials,

$$\frac{\Pi(k)}{\Pi(k-p)} = (-1)^p\,\frac{(k+n)!\,(2n-k)!}{(k-p+n)!\,(2n-k+p)!} = (-1)^p\,\frac{\prod_{i=1}^{p}(n+k-p+i)}{\prod_{i=1}^{p}(2n-k+i)}\,,$$

which is [note, (6.11)]. The numerator runs over the p consecutive integers $n+k-p+1,\dots,n+k$, which lie in $[1,3n]$ because $k\geq p-n$ and $k\leq 2n$; the denominator over $2n-k+1,\dots,2n-k+p$, also in $[1,3n]$ because $k\leq 2n$ and $k\geq p-n$. Since $2p>3n$, the only multiple of p in $[1,3n]$ is p itself, and each run of p consecutive integers contains exactly one multiple of p; so each product contains the factor p exactly once. Cancel it. The remaining $p-1$ factors of each product run through every nonzero residue modulo p once, so by Wilson's theorem each is $\equiv -1$. Hence $\Pi(k)/\Pi(k-p) \equiv (-1)^p\cdot\frac{-1}{-1} = -1$ (as p is odd), and its fourth power is $\equiv 1$.

Step 4: the ratio of the numerators. N_W is a product of linear factors $y+c$, with $c=\frac{n}{2}$ or $c=j+\frac{r}{3}$ ($0\leq j<n$, $r=1,2$, each with multiplicity 3). The factor $y+c$ contributes $\frac{c-k+p}{c-k} = 1+\frac{p}{c-k}$ to $N_W(-k+p)/N_W(-k)$. If $p\nmid(c-k)$ (meaning: $c-k$ has $v_p=0$; its denominator is 1, 2 or 3), this is $\equiv 1 \pmod p$. The factors with $p\mid c-k$ are exactly the p-special zeros $d=k-c$ of $\widetilde{W}_k$, and at an Ra node there is only one, the covering triple zero $d=\frac{p}{3}$, i.e. $c-k=-\frac{p}{3}$, with multiplicity 3. It contributes *exactly*

$$\Big(\frac{-\frac{p}{3}+p}{-\frac{p}{3}}\Big)^3 = \Big(\frac{\frac{2p}{3}}{-\frac{p}{3}}\Big)^3 = (-2)^3 = -8\,.$$

Step 5. $h_{k-p}/h_k = \frac{N_W(-k+p)}{N_W(-k)}\cdot\big(\frac{\Pi(k)}{\Pi(k-p)}\big)^4 \equiv -8\cdot 1.$ □

Intuition: where -8 comes from. The Ra node and its La partner see the same triple zero of W, at $y=-k+\frac{p}{3}$: from $y=-k$ it is at distance $\frac{p}{3}$, from $y=-k+p$ at distance $-\frac{2p}{3}$. The two leading coefficients h differ by the ratio of these distances, cubed. Everything else in h_k (the many other zeros, and the $3n$ poles through the factorials) cancels to ± 1 modulo p, the poles by Wilson's theorem.

Example 14.16 ($n=5$, $p=13$, $k=8$)**.** [note, (6.11)]: the numerator runs over $1,\dots,13$, the denominator over $3,\dots,15$. Without the factor 13, both products are $\equiv 12\equiv -1 \pmod{13}$, and $\Pi(8)/\Pi(-5)\equiv 12\equiv -1$. One finds $\varepsilon_8\equiv 1$, $\varepsilon_{-5}\equiv 5$, and $5\equiv -8 \pmod{13}$. For $n=13$, $p=31$ at the three Ra nodes $18,19,20$: $\varepsilon_{k-p}/\varepsilon_k \equiv 23 \equiv -8 \pmod{31}$ each time. The congruence holds at every Ra node in all 14 cases with $n\leq 17$.

14.3 An adapted basis and the reduction

14.3.1 Why $K(n,p)$, and the weights

The choice of the basis and of the scaling comes from the tree bound at the prime p. Recall from Chapter 13 the relaxation [note, Lemma 5.28]: $-v_p(\Delta_K) \le T_p^+ = \max\{\sum_c V_c(S_c) : \sum_c S_c = K\}$, where c runs over the residue classes modulo p and $V_c(S)$ is the largest local loss of the class c when it receives S of the K rows; V_c is built from $f^+(k,s)$ [note, (5.29)], which needs lower bounds $\check{v}_m(k) \le v_p(c_{k,m})$. Here a class is a single U node or an R/L pair.

The bounds. By Lemma 14.11 the refined bound $\hat{v}_m(k)$ is $m-7$ at the Ra, Rc and La nodes (β^{HS} dominates), $m-4$ at Rb and Lc, $m-3$ at Rb_g, $m-1$ at Lb, m at Lb_g, and ≥ 0 at the U nodes. At every node with a partner it has the form $\hat{v}_m = m - D^*$, with $D^* = 7,4,3,1,0$.

f^+ for an affine bound. As Chapter 13 showed in an example, for $\check{v}_m = m - D^*$ and a node with a partner, every admissible pair (R,π) in [note, (5.29)] gives the same value $\sum_b (D^* - R_b - \pi(b)) + \sum R - \binom{s}{2} = sD^* - s(s-1)$: the higher Taylor orders save exactly what the degree units cost. So $f^+(k,s) = \max(0, sD^* - s(s-1))$ and, for $s \le 4$,

$$f^+(k,s) + s^2 = \begin{cases} (D^*+1)s & D^* \ge 3\ , \\ \max(s^2, 2s) & D^* = 1\ , \\ s^2 & D^* = 0\ . \end{cases}$$

The class values. $V_c(S) = \max_{s_R+s_L=S} \left[f^+(R,s_R) + s_R^2 + f^+(L,s_L) + s_L^2 \right] - S^2$:

- a-pair (Ra, La; $D^* = 7,7$): $8s_R + 8s_L = 8S$, so $V_c(S) = 8S - S^2$, with marginal values $V_c(S) - V_c(S-1) = 9 - 2S = 7,5,3,1$ for the first four rows and negative after;
- c-pair (Rc, Lc; $D^* = 7,4$): $\max(8s_R + 5s_L) = 8S$ for $S \le 4$ (all rows on Rc), so again $V_c(S) = 8S - S^2$ and the marginal values $7,5,3,1$;
- b-pair (Rb, Lb; $D^* = 4,1$): $V_c(1) = 5 - 1 = 4$, $V_c(2) = 10 - 4 = 6$, $V_c(3) = 15 - 9 = 6$: marginal values $4,2$, then 0 and negative;
- b_g-pair (Rb_g, Lb_g; $D^* = 3,0$): $V_c(1) = 4 - 1 = 3$, $V_c(2) = 8 - 4 = 4$: marginal values $3,1$, then negative;
- a U node: $\hat{v} \ge 0$ and no partner give $f^+ = 0$ and $V_c \equiv 0$: no row is placed at a positive marginal value.

Computing f^+ by brute force over all admissible (R,π) from [note, (5.29)], with $\hat{v}$ from [note, (5.25)] at the actual nodes, and V_c by brute force over all profiles of each class, one finds the marginal values $7,5,3,1,-1,-3,-5,-7$ for a-pairs, $7,5,3,1,-4,-6,-8,-10$ for c-pairs, $4,2,0,-2,-7,\dots$ for b-pairs, $3,1,-1,\dots$ for the b_g-pair and $0,0,0,0$ for U nodes, in all 14 cases with $n \le 17$.

Since the marginal values decrease, the best way to place K rows is to take the largest marginal values first. All positive ones together give

$$T_p^+ = 16(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 6(N_{\mathrm{Rb}} - 1) + 4 = 16(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 6N_{\mathrm{Rb}} - 2\ ,$$

using $4(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 2N_{\mathrm{Rb}}$ rows, which is $K(n,p)$ by Proposition 14.8. For $n = 5$, $p = 13$: $T_p^+(K)$ is largest, 36, first at $K = 10$; in all 14 cases the maximum over K of $T_p^+(K)$ is attained first at $K = K(n,p)$ and equals $16(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 6N_{\mathrm{Rb}} - 2$.

Intuition: why this K. The tree bound is an upper bound for the denominator of Δ_K at p. For a non-vanishing proof one wants the opposite: a coefficient whose valuation is *exactly* known. The note's choice is to take K such that the tree bound is at its largest and to show that the constant coefficient actually attains it. "Attaining the worst case" is a rigid situation: every row sits where it costs the most, and the leading term has nowhere to hide. The note's argument gives $v_p([X^0]\Delta_K) = -T_p^+$ exactly.

The conditions. Accordingly, on polynomials of degree $< K$ the note prescribes the Taylor coefficients of orders $0,1,2,3$ at the Ra and Rc nodes and of orders $0,1$ at the Rb and Rb_g nodes, the *condition nodes*; there are $4(N_{\mathrm{Ra}}+N_{\mathrm{Rc}})+2N_{\mathrm{Rb}}=K$ conditions $x=(R_x,j_x)$. The conditions sit at the R nodes and not at their partners, because two partners are congruent modulo p, and the interpolation lemma below needs condition nodes that are pairwise incongruent modulo p (Example 14.18 shows what goes wrong otherwise). The partners still matter: they will enter through Taylor's formula (14.5).

The weights. Each condition x gets the weight θ_x, *half* its marginal value:

$$\theta_x=\tfrac{7}{2}-j_x\ (\mathrm{Ra},\ \mathrm{Rc}),\qquad \theta_x=2-j_x\ (\mathrm{Rb}),\qquad \theta_x=\tfrac{3}{2}-j_x\ (\mathrm{Rb}_g)\ .$$

Half, because a row and the corresponding column of the symmetric Gram matrix are scaled together: an entry $\Gamma_{xx'}$ will be scaled by $p^{\theta_x+\theta_{x'}}$, a diagonal entry by $p^{2\theta_x}$, the full marginal value. Note $\theta_x\geq\frac{1}{2}$ always, and $2\sum_x\theta_x=T_p^+$.

14.3.2 Hermite interpolation and the Chinese remainder theorem over $\mathbb{F}_p$

Taylor coefficients. Recall that a node R sits at $y=-R$, and $P_j(R)=[z^j]P(-R+z)$ is the j-th Taylor coefficient there (Chapter 5). Prescribing $P_0(R),\dots,P_{d-1}(R)$ is the same as prescribing P modulo $(y+R)^d$: $P(y)=\sum_j P_j(R)(y+R)^j$, and the terms with $j\geq d$ are divisible by $(y+R)^d$.

Fact 14.17 (Chinese remainder theorem for polynomials)**.** *Let F be a field and $Q_1,\dots,Q_r\in F[y]$ pairwise coprime of degrees $d_1,\dots,d_r$, $\sum d_i=K$. Then the map $P\mapsto(P \bmod Q_1,\dots,P \bmod Q_r)$ from polynomials of degree $<K$ to the product of the residue spaces is a bijection. (Any algebra text; e.g. Lang,* Algebra*, Ch. II.)*

Proof. Both sides are F-vector spaces of dimension K, and the map is linear, so it suffices to show it is injective. If $P\equiv 0$ modulo every Q_i, then each Q_i divides P; since they are pairwise coprime, their product (of degree K) divides P (unique factorization in $F[y]$), and $\deg P<K$ forces $P=0$. □

In our application $F=\mathbb{F}_p$, $Q_R=(y+R)^{d_R}$, and $(y+R)$, $(y+R')$ are coprime over $\mathbb{F}_p$ exactly when $R\not\equiv R'\pmod p$. Combined with the Taylor-coefficient description, the theorem says: over a field, one may prescribe any d_R Taylor coefficients at each of several distinct points, and there is exactly one polynomial of degree $<\sum d_R$ with these data. This is *Hermite interpolation*, the generalization of Lagrange interpolation to repeated points.

Example 14.18 (Hermite interpolation over $\mathbb{F}_5$)**.** Take two "nodes" $R=1,3$ with $d_R=2$ conditions each ($K=4$), the values and first derivatives at $y=-1$ and $y=-3$. The matrix of the conditions on $1,y,y^2,y^3$, with entries $(y^i)_j(R)=\binom{i}{j}(-R)^{i-j}$, is

$$\Xi=\begin{pmatrix}1&-1&1&-1\\0&1&-2&3\\1&-3&9&-27\\0&1&-6&27\end{pmatrix},\qquad \det\Xi=16=2^4\ ,$$

a unit modulo 5. The dual basis, E_x with $(E_x)_{j'}(R')=\delta_{x,x'}$, is for instance $E_{(1,0)}=-\frac{1}{4}y^3-\frac{3}{2}y^2-\frac{9}{4}y$; its coefficients have denominators 2 and 4, units in $\mathbb{Z}_5$, and modulo 5 it is y^3+y^2+4y. Now move the second node to $R=6\equiv 1\pmod 5$: then $\det\Xi=625=5^4$, which vanishes modulo 5. Over $\mathbb{F}_5$ the two nodes coincide, and the four conditions are two conditions (value and derivative at one point) repeated, so they cannot be independent. This is why the conditions are placed only at the R nodes, never at both members of a pair.

Lemma 14.19 ([note, Lemma 6.12])**.** *There are polynomials $E_x \in \mathbb{Z}_p[y]$ of degree $< K$ with $(E_x)_{j_{x'}}(R_{x'}) = \delta_{x,x'}$ for all conditions x, x', and the transition matrix from the monomials y^i, $i < K$, to the E_x has determinant in $\mathbb{Z}_p^\times$.*

Proof. Let Ξ be the $K \times K$ matrix of the conditions $P \mapsto P_j(R)$ on the monomials, $\Xi_{x,i} = (y^i)_{j_x}(R_x) = \binom{i}{j_x}(-R_x)^{i-j_x}$, an integer matrix. The condition nodes lie in $[p-n, 2n]$, an interval of length $3n - p < p$ (as $p > 1.5n$), so they are pairwise incongruent modulo p, and the polynomials $(y+R)^{d_R}$ are pairwise coprime in $\mathbb{F}_p[y]$. By Fact 14.17 and the remark before it, the map $P \mapsto (P_j(R))_{(R,j)}$ is injective on $\mathbb{F}_p$-polynomials of degree $< K$; its matrix is Ξ reduced modulo p. A square matrix over a field with trivial kernel is invertible, so $\det \Xi \not\equiv 0 \pmod p$, i.e. $\det \Xi \in \mathbb{Z}_p^\times$ (an integer not divisible by p is a unit of $\mathbb{Z}_p$, Chapter 2). By Cramer's rule Ξ^{-1} has entries in $\mathbb{Z}_p$ (integers divided by $\det \Xi$). Let $T = (\Xi^{\mathsf{T}})^{-1}$ and $E_x = \sum_i T_{x,i} y^i$; then $(E_x)_{j_{x'}}(R_{x'}) = \sum_i T_{x,i}\Xi_{x',i} = (T\Xi^{\mathsf{T}})_{x,x'} = \delta_{x,x'}$, and $\det T = 1/\det \Xi \in \mathbb{Z}_p^\times$. □

For $n = 5$, $p = 13$ the condition nodes are 8 (Ra), 9 (Rb_g), 10 (Rc), and $\det \Xi = 65536 = 2^{16} \equiv 3 \pmod{13}$. In all 14 cases with $n \le 17$, $\det \Xi$ equals, up to sign, $\prod_{R<R'}(R'-R)^{d_R d_{R'}}$ (here $(9-8)^8(10-8)^{16}(10-9)^8 = 2^{16}$), a product of numbers smaller than p; the E_x lie in $\mathbb{Z}_p[y]$ and satisfy the duality exactly. (The product formula is the known evaluation of a confluent Vandermonde determinant; here it is only observed in these cases, and the proof does not need it.)

14.3.3 The Gram matrix in the new basis

By the change-of-basis rule of Chapter 6, with T the matrix of coefficients of the E_x,

$$[\Lambda(E_x E_{x'})]_{x,x'} = T\,[\Lambda(y^{i+j})]_{i,j<K}\,T^{\mathsf{T}}\ , \qquad \det[\Lambda(E_x E_{x'})] = (\det T)^2\,\Delta_K(X)\ .$$

Since $(\det T)^2$ is a p-adic unit, every coefficient of $\det[\Lambda(E_x E_{x'})]$ (a polynomial in X) has the same p-adic valuation as the corresponding coefficient of $\Delta_K(X)$. Write [note, (6.13)]

$$\begin{aligned} \Lambda(E_x E_{x'}) &= \Gamma^{\beta}_{xx'} + X\,\Gamma^{\alpha}_{xx'}, \qquad \Gamma^{\beta} = \Gamma^{\mathrm{HS}} + \Gamma^{\mathrm{rest}}, \\ \Gamma^{\bullet}_{xx'} &= \sum_{k\in\mathcal{N}} \sum_{a+b\le 3} c^{\bullet}_{k,a+b}\,(E_x)_a(k)\,(E_{x'})_b(k)\ , \end{aligned} \tag{14.4}$$

with $c^{\mathrm{HS}} = \beta^{\mathrm{HS}}$, $c^{\mathrm{rest}} = \beta^{\mathrm{rest}}$, $c^{\alpha} = \alpha$. This is the jet form [note, (2.27)] of Chapter 6 with E_x in place of y^i: by the Leibniz rule $(E_x E_{x'})_m(k) = \sum_{a+b=m}(E_x)_a(k)(E_{x'})_b(k)$, and $c_{k,m} = 0$ for $m \ge 4$. Setting $X = 0$: $[X^0]\det[\Lambda(E_x E_{x'})] = \det \Gamma^{\beta}$.

For all 14 cases, $\det \Gamma^{\beta} = (\det T)^2\,[X^0]\Delta_K$ exactly, with $v_p(\det T) = 0$; for the cases with $K \le 18$ also every entry of $T[\beta(y^{i+j})]T^{\mathsf{T}}$ equals the jet-form sum (14.4).

14.3.4 Taylor coefficients at the partners

To evaluate (14.4) we need the Taylor coefficients of E_x at *every* node; all lie in $\mathbb{Z}_p$ because $E_x \in \mathbb{Z}_p[y]$. At a condition node R the prescribed ones are 0 or 1. At the partner $\bar{R} = R - p$, at $y = -R + p$, Taylor's formula gives [note, (6.14)]

$$(E_x)_b(\bar{R}) = \sum_{j\ge b} \binom{j}{b} (E_x)_j(R)\,p^{j-b}\ , \tag{14.5}$$

because $E_x(-R+p+z) = \sum_j (E_x)_j(R)(p+z)^j$ and the coefficient of z^b in $(p+z)^j$ is $\binom{j}{b}p^{j-b}$.

Reading off valuations. If $R = R_x$ and $b \le j_x$, the term $j = j_x$ is $\binom{j_x}{b}p^{j_x-b}$. All the other prescribed orders j at R have $(E_x)_j(R) = 0$. Unprescribed orders are $j \ge 4$ at an Ra/Rc node

and $j \geq 2$ at an Rb/Rb$_g$ node, and they contribute terms of valuation $\geq j - b$. Hence: at the partner of an Ra or Rc node,

$$(E_x)_b(\bar{R}) = \xi_{x,b} + \xi'_{x,b} \ , \qquad \xi_{x,b} = \binom{j_x}{b} p^{j_x - b} \text{ if } R_x = R,\ b \leq j_x \ , \qquad \xi_{x,b} = 0 \text{ otherwise} \ , \tag{14.6}$$

with $v_p(\xi'_{x,b}) \geq 4 - b$ [note, (6.15)]. At the partner of an Rb or Rb$_g$ node, outside the case $R_x = R$, $b \leq j_x$, the valuation is $\geq \max(0, 2 - b)$.

Intuition. At the R node, E_x is a "spike": all its low Taylor coefficients there are 0 except one. At the partner, p-adically close by, the spike is seen through Taylor's formula: the coefficient of order j_x is smeared down to the lower orders $b < j_x$ with factors $\binom{j_x}{b} p^{j_x - b}$, p-adically small but known exactly. The unknown higher Taylor coefficients at R contribute even smaller amounts (p^{4-b}). This is how the La partner of an Ra node enters the Ra block.

In all 14 cases, (14.5) holds exactly (with all Taylor orders $j < K$ of E_x at R), $v_p(\xi'_{x,b}) \geq 4 - b$ at every partner of an Ra/Rc node, and the bound $\max(0, 2 - b)$ holds at every partner of an Rb/Rb$_g$ node.

14.3.5 Weighted valuations: Lemma 6.17

A *contribution* to $\Gamma^{\bullet}_{xx'}$ is one term $c^{\bullet}_{k,a+b}(E_x)_a(k)(E_{x'})_b(k)$ of (14.4); at a partner of an Ra or Rc node each term is split by (14.6) into four products ($\xi\xi$, $\xi\xi'$, $\xi'\xi$, $\xi'\xi'$), counted as separate contributions. Its *weighted valuation* is [note, (6.16)]

$$\omega = v_p(c^{\bullet}_{k,a+b}) + v_p((E_x)_a(k)) + v_p((E_{x'})_b(k)) + \theta_x + \theta_{x'} \in \tfrac{1}{2}\mathbb{Z} \ , \tag{14.7}$$

i.e. the valuation the contribution will have after the entry $\Gamma_{xx'}$ is multiplied by $p^{\theta_x + \theta_{x'}}$. With these weights the leading contributions at a condition node have $\omega = 0$: at an Ra/Rc node with $R_x = R_{x'} = R$, $a = j_x$, $b = j_{x'}$, (14.3) with $D_R = 1$ gives $v_p(\beta^{\mathrm{HS}}_{R,j_x+j_{x'}}) = j_x + j_{x'} - 7$ and $\theta_x + \theta_{x'} = 7 - j_x - j_{x'}$.

Lemma 14.20 (weighted valuations; [note, Lemma 6.17])**.** *Every contribution to Γ^{β} has $\omega \geq 0$, and every contribution to Γ^{α} has $\omega \geq 1$. If $R_x \neq R_{x'}$, every contribution to $\Gamma^{\beta}_{xx'}$ has $\omega \geq \frac{1}{2}$. If $R_x = R_{x'} = R$, the contributions to $\Gamma^{\beta}_{xx'}$ with $\omega = 0$ are the terms of β^{HS} at R with $(a, b) = (j_x, j_{x'})$ and, if R is of type Ra, the products $\beta^{\mathrm{HS}}_{\bar{R},a+b}\xi_{x,a}\xi_{x',b}$ at its partner $\bar{R}$.*

The proof ([note, Appendix D]) goes through the nodes k by type. We use the bounds of Lemma 14.11 and the Taylor bounds above, write $m = a + b \leq 3$, and recall $\theta_x \geq \frac{1}{2}$.

(1) U nodes. All local constants have $v_p \geq 0$ and the Taylor coefficients are in $\mathbb{Z}_p$, so $\omega \geq \theta_x + \theta_{x'} \geq 1$.

(2) An Ra or Rc node R. If $R_x \neq R$, all $(E_x)_a(R)$, $a \leq 3$, vanish (they are prescribed, and the δ is 0); so a contribution needs $R_x = R_{x'} = R$, and then only $a = j_x$, $b = j_{x'}$ survive, with Taylor coefficients 1. The part β^{HS} has $v_p \geq m - 7$, so $\omega \geq (j_x + j_{x'} - 7) + (\frac{7}{2} - j_x) + (\frac{7}{2} - j_{x'}) = 0$. The part β^{rest} has $v_p \geq m - 4$, three better: $\omega \geq 3$; α has $v_p \geq m - 2$: $\omega \geq 5$.

(3) An Rb node R. Here $\theta_x = 2 - j_x$ for the conditions at R, β^{HS} has $v_p \geq m - 4$ ($D = -2$). Orders $0, 1$ are prescribed at R, orders $2, 3$ are not; since $m \leq 3$, at most one of a, b is ≥ 2.

(3i) $R_x = R_{x'} = R$, $a = j_x$, $b = j_{x'}$: $\omega \geq (a + b - 4) + (2 - j_x) + (2 - j_{x'}) = 0$.

(3ii) $R_x = R_{x'} = R$, $a \in \{2, 3\}$: then $b \leq 1$ is prescribed, so $b = j_{x'}$ (else the factor is 0), and $v_p((E_x)_a(R)) \geq 0$: $\omega \geq (a + b - 4) + (2 - j_x) + (2 - b) = a - j_x \geq 1$. Likewise with a, b exchanged.

(3iii) $R_x = R \neq R_{x'}$: $(E_{x'})_b(R) = 0$ for $b \leq 1$, so $b \in \{2,3\}$, hence $a \leq 1$, $a = j_x$: $\omega \geq (j_x + b - 4) + (2 - j_x) + \theta_{x'} = b - 2 + \theta_{x'} \geq \frac{1}{2}$. Likewise with x, x' exchanged.
(3iv) $R_x \neq R$ and $R_{x'} \neq R$: then $a, b \geq 2$, $m \geq 4$: no contribution.
β^{rest} ($v_p \geq m-1$) and α ($v_p \geq m+1$) are better by 3 and 5.

(3′) The Rb_g node R. The same with the bound $m-3$ for β^{HS} and $\theta_x = \frac{3}{2} - j_x$: $\omega \geq 0$ in (3i), $\omega \geq a - j_x \geq 1$ in (3ii), and $\omega \geq (j_x + b - 3) + (\frac{3}{2} - j_x) + \theta_{x'} = b - \frac{3}{2} + \theta_{x'} \geq 1$ in (3iii). β^{rest} ($v_p \geq m$) and α ($v_p \geq m+2$) are better by 3 and 5.

(4) An La node $\bar{R}$, partner of an Ra node R. β^{HS} has $v_p \geq m-7$. Use (14.6). If $R_x = R_{x'} = R$: the product with $\xi_{x,a}\xi_{x',b}$ (nonzero only for $a \leq j_x$, $b \leq j_{x'}$) has $\omega \geq (m-7) + (j_x - a) + (j_{x'} - b) + (7 - j_x - j_{x'}) = 0$; replacing $\xi_{x,a}$ by $\xi'_{x,a}$ replaces $j_x - a$ by $4 - a \geq j_x - a + 1$ and raises ω by at least 1, likewise for x'. If $R_x = R \neq R_{x'}$: $v_p((E_x)_a(\bar{R})) \geq j_x - a$ (from (14.6), $j_x - a \leq 4 - a$) and $v_p((E_{x'})_b(\bar{R})) \geq 4 - b$ (only ξ'), so $\omega \geq (a + b - 7) + (j_x - a) + (4 - b) + (\frac{7}{2} - j_x) + \theta_{x'} = \frac{1}{2} + \theta_{x'} \geq 1$. If neither condition is at R: $\omega \geq (m-7) + (4-a) + (4-b) + \theta_x + \theta_{x'} = 1 + \theta_x + \theta_{x'} \geq 2$. β^{rest} ($m-4$) and α ($m-2$) are better by 3 and 5.

(4′) An Lc node, partner of an Rc node. No virtual pole, so only β^{rest} ($v_p \geq m-4$) and α ($v_p \geq m-2$) occur, and the Taylor bounds are those of (4): $\omega \geq 3$ and $\omega \geq 5$.

(5) An Lb or Lb_g node $\bar{R}$, partner of an Rb or Rb_g node R. No virtual pole. At Lb, β^{rest} has $v_p \geq m-1$, α has $v_p \geq m+1$; at Lb_g, m and $m+2$. Put $w_x(a) = a + v_p((E_x)_a(\bar{R}))$. If $R_x = R$: for $a \leq j_x$, $w_x(a) \geq j_x$ (the term $\binom{j_x}{a}p^{j_x - a}$ and higher ones); for $a > j_x$ only unprescribed orders $j \geq 2$ contribute, $w_x(a) \geq \max(a, 2) \geq 2$. So $w_x(a) + \theta_x \geq 2$ at Rb ($\theta_x = 2 - j_x$, $j_x \leq 1$) and $\geq \frac{3}{2}$ at Rb_g. If $R_x \neq R$: $w_x(a) \geq \max(a, 2) \geq 2$ and $w_x(a) + \theta_x \geq \frac{5}{2}$. Then β^{rest} at Lb has $\omega \geq (m-1) - a - b + (w_x(a) + \theta_x) + (w_{x'}(b) + \theta_{x'}) \geq -1 + 2 + 2 = 3$, and at Lb_g $\omega \geq 0 + \frac{3}{2} + \frac{3}{2} = 3$; α has $\omega \geq 5$ at both.

Collecting. At a condition node different from R_x and $R_{x'}$ there is no contribution, by (2), (3iv), (3′); the partners of such nodes are covered by (4), (4′), (5). So every contribution to Γ^β has $\omega \geq 0$, and to Γ^α has $\omega \geq 1$ (the best α case is (1), all others give ≥ 5). The contributions to $\Gamma^\beta_{xx'}$ with $R_x \neq R_{x'}$ are those of (1), (3iii), (3′iii), (4) with one or no condition at R, (4′) and (5): all $\geq \frac{1}{2}$. The contributions with $\omega = 0$ can only be those of (2), (3i), (3′i) for β^{HS}, and the products $\beta^{\text{HS}}_{\bar{R},a+b}\xi_{x,a}\xi_{x',b}$ of (4). □

Lemma 6.17. The weights θ were chosen so that the most negative valuations allowed by Lemma 14.11, at the condition nodes themselves, are exactly compensated. Everywhere else something is gained: at U nodes the full $\theta_x + \theta_{x'} \geq 1$; at partner nodes without virtual poles the three powers of p that β^{rest} is better than β^{HS}; at the La partners, nothing for the leading Taylor-shift terms (these are the second kind of $\omega = 0$ contribution) but at least 1 for everything else. The only case in which ω can equal $\frac{1}{2}$ is (3iii): an Rb condition (θ an integer) meeting a condition with half-integer θ through an unprescribed Taylor coefficient at the Rb node.

Example 14.21 (Lemma 14.20 in examples)**.** We compute the weighted valuation of every single contribution, for every node k, every (a, b) with $a + b \leq 3$, every pair (x, x'), each of the three parts, with the four-fold split at the Ra/Rc partners. For $n = 5$, $p = 13$: the minimum of ω is 0 for β^{HS}, 1 for β^{rest} and 1 for α (both at U nodes; at R/L nodes the minima are 3 and 5, as in the proof), 1 for contributions with $R_x \neq R_{x'}$, and the 109 contributions with $\omega = 0$ are all of the two kinds named in the lemma. For $n = 13$, $p = 31$, which has two plain Rb nodes, the minimum over contributions with $R_x \neq R_{x'}$ is exactly $\frac{1}{2}$: the half-integer case (3iii) does occur. All statements of the lemma hold in all 14 cases with $n \leq 17$.

14.3.6 The field $\mathbb{Q}_p(\sqrt{p})$

Lemma 14.20 allows $\omega = \frac{1}{2}$, so the scaled entries $p^{\theta_x+\theta_{x'}}\Gamma_{xx'}$ can involve $p^{1/2}$: we need a number system containing $\sqrt{p}$.

Why $\sqrt{p} \notin \mathbb{Q}_p$. Every nonzero element of $\mathbb{Q}_p$ has an integer valuation. If $s^2 = p$ then $2v_p(s) = 1$, impossible. So we adjoin a square root.

Definition 14.22 ($\mathbb{Q}_p(\sqrt{p})$)**.** $\mathbb{Q}_p(\sqrt{p}) = \{a + b\sqrt{p} : \ a, b \in \mathbb{Q}_p\}$, with $(\sqrt{p})^2 = p$ and the obvious addition and multiplication.

Fact 14.23. *(i) $Y^2 - p$ is irreducible over $\mathbb{Q}_p$, so $\mathbb{Q}_p(\sqrt{p})$ is a field, a quadratic extension of $\mathbb{Q}_p$. (ii) The valuation extends: $v_p(a + b\sqrt{p}) = \min(v_p(a), v_p(b) + \frac{1}{2})$, with values in $\frac{1}{2}\mathbb{Z}$, and it still satisfies $v(xy) = v(x) + v(y)$ and the ultrametric inequality. (iii) The elements with $v \geq 0$ form the ring $\mathbb{Z}_p[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}_p\}$, those with $v > 0$ the ideal $(\sqrt{p})$, and $\mathbb{Z}_p[\sqrt{p}]/(\sqrt{p}) \cong \mathbb{F}_p$. (Koblitz,* p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Ch. III.)*

Reasons. (i) $Y^2 - p$ is an *Eisenstein polynomial*: monic, all lower coefficients divisible by p, constant term not divisible by p^2; such a polynomial is irreducible (Eisenstein's criterion, same reference), and here it is clear directly since a root in $\mathbb{Q}_p$ would have valuation $\frac{1}{2}$. (ii) The two numbers $v_p(a)$ (an integer) and $v_p(b) + \frac{1}{2}$ (a half-integer) are never equal, so there is no cancellation between a and $b\sqrt{p}$, and the smaller one wins. Equivalently, $v(x) = \frac{1}{2}v_p(N(x))$ with the norm $N(a + b\sqrt{p}) = (a + b\sqrt{p})(a - b\sqrt{p}) = a^2 - pb^2 \in \mathbb{Q}_p$, which is multiplicative; this gives $v(xy) = v(x) + v(y)$. (iii) If $v(a + b\sqrt{p}) \geq 0$ then $v_p(a) \geq 0$ and $v_p(b) \geq -\frac{1}{2}$, i.e. $v_p(b) \geq 0$; so the ring is $\mathbb{Z}_p[\sqrt{p}]$. Reducing modulo $\sqrt{p}$ kills $b\sqrt{p}$ and $p\mathbb{Z}_p$, and keeps a mod p: $a + b\sqrt{p} \mapsto a \bmod p \in \mathbb{F}_p$, a ring homomorphism. The extension is called *totally ramified*: the valuation group doubles ($\frac{1}{2}\mathbb{Z}$ instead of $\mathbb{Z}$) while the residue field stays $\mathbb{F}_p$.

Example 14.24 (valuations in $\mathbb{Q}_{13}(\sqrt{13})$)**.** $v(13 + 2\sqrt{13}) = \min(1, 0 + \frac{1}{2}) = \frac{1}{2}$, and $N = 169 - 52 = 117 = 9 \cdot 13$, $\frac{1}{2}v_{13}(117) = \frac{1}{2}$. $v(26 + 13\sqrt{13}) = \min(1, \frac{3}{2}) = 1$, and $N = 676 - 2197 = -1521 = -9 \cdot 13^2$, $\frac{1}{2}v_{13} = 1$. $v(5 + 3\sqrt{13}) = 0$, $N = -92$, a unit. Reduction modulo $\sqrt{13}$: $5 + 3\sqrt{13} \mapsto 5 \in \mathbb{F}_{13}$, $13 + 2\sqrt{13} \mapsto 0$.

Intuition: why half-integers are needed, and why they are harmless. The weights θ_x at Ra, Rc and Rb_g nodes are half-integers because their marginal values ($7, 5, 3, 1$ and $3, 1$) are odd, and halving them is forced by the symmetric scaling. The only entries where $\theta_x + \theta_{x'}$ is a half-integer are those between an Rb condition (integer θ) and a condition at an Ra, Rc or Rb_g node (half-integer θ). Such an entry is $\sqrt{p}$ times an element of $\mathbb{Q}_p$; if its valuation is ≥ 0 it is *automatically* $\equiv 0 \pmod{\sqrt{p}}$, because a valuation in $\frac{1}{2} + \mathbb{Z}$ that is ≥ 0 is $\geq \frac{1}{2}$. So the half-integer entries never contribute to the reduced matrix; the extension is a bookkeeping device that lets us scale rows by $p^{1/2}$ without leaving a ring with residue field $\mathbb{F}_p$. Determinants of the reduced matrix are computed in $\mathbb{F}_p$ as usual.

14.3.7 The scaled matrix and its block structure

Let $\Theta = \mathrm{diag}(p^{\theta_x})$, viewed in $\mathbb{Q}_p(\sqrt{p})$, and $\widetilde{\Gamma}^\beta = \Theta\Gamma^\beta\Theta$, $\widetilde{\Gamma}^\alpha = \Theta\Gamma^\alpha\Theta$. Each entry $\widetilde{\Gamma}_{xx'} = p^{\theta_x+\theta_{x'}}\Gamma_{xx'}$ is the sum of its contributions, each multiplied by $p^{\theta_x+\theta_{x'}}$, i.e. each of valuation ω. By the ultrametric inequality and Lemma 14.20:

- $\widetilde{\Gamma}^\beta$ has entries in $\mathbb{Z}_p[\sqrt{p}]$ (all $\omega \geq 0$);
- its entries with $R_x \neq R_{x'}$ vanish modulo $\sqrt{p}$ (all $\omega \geq \frac{1}{2}$);
- $\widetilde{\Gamma}^\alpha$ has entries in $p\mathbb{Z}_p[\sqrt{p}]$ (all $\omega \geq 1$).

So modulo $\sqrt{p}$, $\widetilde{\Gamma}^\beta$ is *block diagonal*, one block per condition node, and within a block only the $\omega = 0$ contributions survive.

Example 14.25 (the block structure for $n = 13$, $p = 31$)**.** Here $N_{\mathrm{Ra}} = N_{\mathrm{Rb}} = N_{\mathrm{Rc}} = 3$, $K = 30$; the condition nodes are $18, 19, 20$ (Ra), 21 (Rb), 22 (Rb_g), 23 (Rb), $24, 25, 26$ (Rc). We compute $\widetilde{\Gamma}^{\beta}$ exactly, tracking $\theta_x + \theta_{x'} \in \frac{1}{2}\mathbb{Z}$. Marking an entry "0" if its valuation is 0, "h" if it is exactly $\frac{1}{2}$, "·" if it is ≥ 1 (rows and columns in the order of the conditions: four per Ra node, two at 21, two at 22, two at 23, four per Rc node):

```
0000.....................      ...h...h...h.0.h.....h...h...h
0000.....................      ...h...h...h00.h.....h...h...h
0000.....................      ..............00..............
0000........hh..hh.......      ............hh00hh............
....0000.................      ...h...h...h...h.0...h...h...h
....0000.................      ...h...h...h...h00...h...h...h
....0000.................      ..................0000........
....0000....hh..hh.......      ..................000.........
........0000.............      ..................00..........
........0000.............      ............hh..hh0...........
........0000.............      ......................0000....
........0000hh..hh.......      ......................000.....
                               ......................00......
                               ............hh..hh....0.......
                               ........................0000
                               ........................000.
                               ........................00..
                               ............hh..hh........0...
```

(left: rows 1–12; right: rows 13–30). All 900 entries have valuation ≥ 0; off the blocks the valuation is $\geq \frac{1}{2}$; 208 entries have half-integer $\theta_x + \theta_{x'}$, and 56 of them have valuation exactly $\frac{1}{2}$: they are the "h" entries, all in the rows and columns of the two Rb nodes, as case (3iii) predicts. So the reduction really has to be made modulo $\sqrt{p}$ and not modulo p: modulo p these 56 entries would not vanish (they are not even in $\mathbb{Z}_p$). All entries of $\widetilde{\Gamma}^{\alpha}$ have valuation ≥ 1.

14.3.8 The blocks: Lemma 6.18

Lemma 14.26 ([note, Lemma 6.18])**.** *Modulo $\sqrt{p}$, the block of $\widetilde{\Gamma}^{\beta}$ at a condition node R is*

$$\varepsilon_R\, A_{\mathrm{Rc}} \quad (Rc), \qquad \varepsilon_R \begin{pmatrix} \phi_{\mathrm{Rb},3} & \phi_{\mathrm{Rb},2} \\ \phi_{\mathrm{Rb},2} & \phi_{\mathrm{Rb},1} \end{pmatrix} \quad (Rb), \qquad \varepsilon_R \begin{pmatrix} \phi_{\mathrm{Rb}_g,3} & \phi_{\mathrm{Rb}_g,2} \\ \phi_{\mathrm{Rb}_g,2} & \phi_{\mathrm{Rb}_g,1} \end{pmatrix} \quad (Rb_g),$$
$$\varepsilon_R(A_{\mathrm{Ra}} - 8\, B^{\mathsf{T}} A_{\mathrm{La}} B) \quad (Ra), \tag{14.8}$$

where $A_\bullet = [\phi_{\bullet,3-a-b}]_{0\leq a,b\leq 3}$ with $\phi_b = 0$ for $b < 0$, and $B = [\binom{j}{a}]_{0\leq a,j\leq 3}$.

Proof. Rc, Rb, Rb_g. By Lemma 14.20 the only $\omega = 0$ contributions are $\beta^{\mathrm{HS}}_{R,j_x+j_{x'}} \cdot 1 \cdot 1$. By (14.3), multiplied by $p^{\theta_x+\theta_{x'}}$, which is $p^{D_R+6-j_x-j_{x'}}$ in each case (Rc: $7 - j_x - j_{x'}$, $D = 1$; Rb: $4 - j_x - j_{x'}$, $D = -2$; Rb_g: $3 - j_x - j_{x'}$, $D = -3$), each becomes $\varepsilon_R(\phi_{R,3-j_x-j_{x'}} + O(p))$. For Rb and Rb_g, $j_x, j_{x'} \in \{0, 1\}$: the entries are $\phi_3, \phi_2; \phi_2, \phi_1$. For Rc, $j_x, j_{x'} \in \{0, \ldots, 3\}$, and for $j_x + j_{x'} \geq 4$ there is no local constant ($c_{k,m} = 0$ for $m \geq 4$), which is the convention $\phi_b = 0$ for $b < 0$.

Ra. In addition to the same contribution $\varepsilon_R \phi_{\mathrm{Ra},3-j_x-j_{x'}}$ from R itself, the partner $\bar{R}$ (La, $D = 1$) contributes the products $\beta^{\mathrm{HS}}_{\bar{R},a+b} \xi_{x,a} \xi_{x',b}$ for $a \leq j_x$, $b \leq j_{x'}$. Scaled, using (14.3) at $\bar{R}$ and (14.6):

$$p^{7-j_x-j_{x'}} \cdot \varepsilon_{\bar{R}} p^{a+b-7} (\phi_{\mathrm{La},3-a-b} + O(p)) \cdot \binom{j_x}{a} p^{j_x-a} \binom{j_{x'}}{b} p^{j_{x'}-b} = \varepsilon_{\bar{R}} \binom{j_x}{a} \binom{j_{x'}}{b} \phi_{\mathrm{La},3-a-b} + O(p)\,.$$

All powers of p cancel exactly. Summing over a, b [note, (6.20)]:

$$\varepsilon_{\bar{R}} \sum_{a\leq j_x,\, b\leq j_{x'}} \binom{j_x}{a} \binom{j_{x'}}{b} \phi_{\mathrm{La},3-a-b} = \varepsilon_{\bar{R}} (B^{\mathsf{T}} A_{\mathrm{La}} B)_{j_x j_{x'}}\,,$$

since $(B^{\mathsf T}AB)_{jj'} = \sum_{a,b} B_{aj}A_{ab}B_{bj'} = \sum_{a,b}\binom{j}{a}\binom{j'}{b}A_{ab}$, and $\binom{j}{a} = 0$ for $a > j$. Finally $\varepsilon_{\bar R} \equiv -8\varepsilon_R$ by Lemma 14.15. □

Example 14.27 (the reduced blocks for $n = 5$, $p = 13$)**.** We reduce the exactly computed $\widetilde\Gamma^\beta$ modulo 13 (all entries have integer $\theta_x + \theta_{x'}$ here, as there is no plain Rb node). With residues written in $\{-6, \dots, 6\}$:

$$R = 8\ (\varepsilon_8 \equiv 1):\ \begin{pmatrix} 4 & -2 & -1 & -2 \\ -2 & -1 & -2 & -1 \\ -1 & -2 & -1 & 6 \\ -2 & -1 & 6 & -3 \end{pmatrix}, \qquad R = 10\ (\varepsilon_{10} \equiv 8):\ \begin{pmatrix} 4 & 6 & -6 & -4 \\ 6 & -6 & -4 & 0 \\ -6 & -4 & 0 & 0 \\ -4 & 0 & 0 & 0 \end{pmatrix},$$

$$R = 9\ (\varepsilon_9 \equiv 8):\ \begin{pmatrix} 5 & -4 \\ -4 & -1 \end{pmatrix},$$

and every off-block entry is $\equiv 0$. These are exactly ε_R times the matrices of (14.8) reduced modulo 13. By hand: the Rb_g block is $8 \cdot \left(\begin{smallmatrix} 243/4 & 243/8 \\ 243/8 & -729/8 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 486 & 243 \\ 243 & -729 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 5 & -4 \\ -4 & -1 \end{smallmatrix}\right)$; the Rc anti-diagonal is $8 \cdot \frac{243}{8} = 243 \equiv -4$. The determinant of the reduced 10×10 matrix is $2 \in \mathbb{F}_{13}$, nonzero, and equals the product of the block determinants. The same agreement (every block entry, every case) holds in all 14 cases with $n \le 17$, including the plain Rb blocks of $n = 13$, $p = 31$, e.g. $\left(\begin{smallmatrix} 0 & 7 \\ 7 & 7 \end{smallmatrix}\right) = 5 \cdot \frac{243}{8}\left(\begin{smallmatrix} 0 & -1 \\ -1 & -1 \end{smallmatrix}\right)$ modulo 31 at $R = 21$.

14.3.9 The block determinants

Proposition 14.28 ([note, Section 6.2], after Lemma 6.18)**.** *The determinants of the blocks (14.8) are $\varepsilon_R^4\, 3^{20}/2^{12}$ (Rc), $-\varepsilon_R^2\, 3^{10}/2^6$ (Rb), $-\varepsilon_R^2\, 7 \cdot 3^{10}/2^6$ (Rb_g) and $\varepsilon_R^4\, 3^{20}$ (Ra). All are p-adic units for $p \ge 13$.*

Proof. Rc. A_{Rc} vanishes below the anti-diagonal ($a + b > 3$) and has $\phi_{\mathrm{Rc},0} = \frac{243}{8} = \frac{3^5}{2^3}$ on it. Expanding, only the anti-diagonal permutation ($a \mapsto 3 - a$) contributes; it is a product of two transpositions, sign $+1$. So $\det = (\varepsilon_R\, 3^5/2^3)^4 = \varepsilon_R^4\, 3^{20}/2^{12}$.

Rb. With Example 14.10: $\phi_3 = 0$, $\phi_2 = \phi_1 = -\frac{243}{8}$, the block is $\varepsilon_R \frac{243}{8}\left(\begin{smallmatrix} 0 & -1 \\ -1 & -1 \end{smallmatrix}\right)$, of determinant $\varepsilon_R^2 \frac{3^{10}}{2^6}(0 - 1)$.

Rb_g. $\phi_3 = \frac{243}{4}$, $\phi_2 = \frac{243}{8}$, $\phi_1 = -\frac{729}{8}$: the block is $\varepsilon_R \frac{243}{8}\left(\begin{smallmatrix} 2 & 1 \\ 1 & -3 \end{smallmatrix}\right)$, of determinant $\varepsilon_R^2 \frac{3^{10}}{2^6}(-6 - 1)$.

Ra. $(B^{\mathsf T}A_{\mathrm{La}}B)_{jj'} = \sum_{a,b}\binom{j}{a}\binom{j'}{b}\phi_{\mathrm{La},3-a-b} = \sum_m \binom{j+j'}{m}\phi_{\mathrm{La},3-m}$ by Vandermonde's identity $\sum_{a+b=m}\binom{j}{a}\binom{j'}{b} = \binom{j+j'}{m}$; it depends only on $j + j'$. The explicit matrix is computed in the example below; it is 3^5 times an integer matrix of determinant 1, so the determinant is $\varepsilon_R^4(3^5)^4 = \varepsilon_R^4\, 3^{20}$.

All four are products of units ε_R with powers of 2, 3, 7, hence units for $p \ge 13$. □

Example 14.29 (the Ra block [note, (6.21)] and [note, Remark 6.22])**.** With the La coefficients of Example 14.10, the first row of $B^{\mathsf T}A_{\mathrm{La}}B$ is $-\frac{49761}{8}, -\frac{39339}{8}, -\frac{30753}{8}, -\frac{23787}{8}$ (e.g. the $(0,1)$ entry is $\phi_{\mathrm{La},2} + \phi_{\mathrm{La},3} = \frac{5211}{4} - \frac{49761}{8} = -\frac{39339}{8}$). A direct computation gives

$$A_{\mathrm{Ra}} - 8\, B^{\mathsf T}A_{\mathrm{La}}B = 3^5 \begin{pmatrix} 207 & 163 & 127 & 98 \\ 163 & 127 & 98 & 75 \\ 127 & 98 & 75 & 57 \\ 98 & 75 & 57 & 43 \end{pmatrix},$$

the integer matrix has determinant 1, and the whole determinant is $3^{20} = 3486784401$, as [note, (6.21)] states. (By hand for the $(0,0)$ entry: $\phi_{\mathrm{Ra},3} - 8\phi_{\mathrm{La},3} = 540 + 49761 = 50301 = 243 \cdot 207$.)

With a general number r in place of -8, a symbolic computation gives

$$\det\left(A_{\mathrm{Ra}} + r\, B^{\mathsf{T}} A_{\mathrm{La}} B\right) = 3^{12}(r-1)^4 \ ,$$

as [note, Remark 6.22] states; at $r=0$ this is $\det A_{\mathrm{Ra}} = 3^{12}$, and at $r=-8$ it is $3^{12}\cdot 9^4 = 3^{20}$.

Intuition: Remark 6.22: why Wilson is needed. The Ra block is a unit precisely when $r \not\equiv 1 \pmod p$. If the units of the two partners were related by $r=1$, i.e. $\varepsilon_{k-p} \equiv \varepsilon_k$, the Ra and La contributions would combine into a matrix singular modulo p, the leading term of $\det \widetilde{\Gamma}^\beta$ would vanish, and the argument would say nothing. Wilson's theorem shows that the two leading coefficients differ, modulo p, only through the shared covering zero, which gives $r=(-2)^3=-8$, and $-8-1=-9$ is prime to p. In words: the Ra node and its partner see their common zero at distances $\frac{p}{3}$ and $-\frac{2p}{3}$, and the ratio -2 of these distances is what keeps the block nondegenerate.

Check yourself 14.30. Why does the factor $p^{\theta_x+\theta_{x'}}$ cancel *exactly* against the powers of p in the Ra partner contribution, and not only up to a unit?

Answer. Because each factor is an exact power of p times a p-integral number: $\xi_{x,a} = \binom{j_x}{a} p^{j_x-a}$ exactly, and (14.3) gives $\beta^{\mathrm{HS}}_{\bar R, a+b} = \varepsilon_{\bar R} p^{a+b-7}(\phi + O(p))$. The exponents add to $(7-j_x-j_{x'})+(a+b-7)+(j_x-a)+(j_{x'}-b)=0$. The weights $\theta_x = \frac{7}{2} - j_x$ were chosen to make this exact at R; that it is also exact at $\bar R$ is because the La node has the same $D=1$ and the same β^{HS} bound $m-7$ as the Ra node.

14.3.10 Proof of Theorem 3.13

Theorem 14.31 (non-vanishing; [note, Theorem 3.13])**.** *Let p be a prime with $2.1n+2 \le p < 3n$, and $K = K(n,p)$. Then $K \le 3n-2$, and $\Delta_K(a/b) \neq 0$ for every $a/b \in \mathbb{Q}$ with $p \nmid b$. If moreover $p \le 2.159n$, then $K > 2.8n$. More precisely,*

$$v_p([X^0]\Delta_K) = -(16(N_{\mathrm{Ra}}+N_{\mathrm{Rc}})+6N_{\mathrm{Rb}}-2), \qquad v_p([X^j]\Delta_K) \ge v_p([X^0]\Delta_K) + j \quad (j \ge 1)\ . \tag{14.9}$$

Proof. The bounds on K were proved in Chapter 7.

Step 1: $\det \widetilde{\Gamma}^\beta$ is a unit. The reduction $\mathbb{Z}_p[\sqrt{p}] \to \mathbb{F}_p$ is a ring homomorphism, and the determinant is a polynomial in the entries, so the reduction of $\det \widetilde{\Gamma}^\beta$ is the determinant of the reduced matrix. That matrix is block diagonal (Lemma 14.20), its determinant is the product of the block determinants, and each block determinant is the reduction of a unit (Lemma 14.26, Proposition 14.28), hence nonzero in $\mathbb{F}_p$. A nonzero element of $\mathbb{F}_p$ comes from an element of valuation 0. So $v_p(\det \widetilde{\Gamma}^\beta) = 0$.

Step 2: the constant coefficient. $\det \widetilde{\Gamma}^\beta = \det\Theta \cdot \det \Gamma^\beta \cdot \det \Theta = p^{2\sum_x \theta_x} \det \Gamma^\beta$. So $v_p(\det \Gamma^\beta) = -2\sum_x \theta_x$. The weights at one node add up to $\frac{7}{2}+\frac{5}{2}+\frac{3}{2}+\frac{1}{2} = 8$ (Ra, Rc), $2+1=3$ (Rb), $\frac{3}{2}+\frac{1}{2}=2$ (the single Rb_g node), so $2\sum_x \theta_x = 16(N_{\mathrm{Ra}}+N_{\mathrm{Rc}})+6(N_{\mathrm{Rb}}-1)+4 = 16(N_{\mathrm{Ra}}+N_{\mathrm{Rc}})+6N_{\mathrm{Rb}}-2$. Since $[X^0]\Delta_K = (\det T)^{-2}\det\Gamma^\beta$ with $\det T$ a unit, this is (14.9), first part [note, (6.23)].

Step 3: the other coefficients. The determinant is multilinear in the columns. Write column x' of $\widetilde{\Gamma}^\beta + X\widetilde{\Gamma}^\alpha$ as $\widetilde{\Gamma}^\beta_{\cdot x'} + X\,\widetilde{\Gamma}^\alpha_{\cdot x'}$ and expand: $\det\left(\widetilde{\Gamma}^\beta + X\widetilde{\Gamma}^\alpha\right)$ is the sum over subsets J of the columns of $X^{|J|}$ times the determinant of the matrix whose columns in J come from $\widetilde{\Gamma}^\alpha$ and the others from $\widetilde{\Gamma}^\beta$. So $[X^j]$ is a sum of such determinants with $|J|=j$. In each, the j columns from $\widetilde{\Gamma}^\alpha$ have entries in $p\mathbb{Z}_p[\sqrt{p}]$; pulling a factor p out of each of them leaves a matrix with entries in $\mathbb{Z}_p[\sqrt{p}]$, whose determinant is in $\mathbb{Z}_p[\sqrt{p}]$. So $[X^j]\det\left(\widetilde{\Gamma}^\beta + X\widetilde{\Gamma}^\alpha\right) \in p^j\mathbb{Z}_p[\sqrt{p}]$, valuation $\ge j$.

Undoing the scaling and the change of basis, $[X^j]\Delta_K = (\det T)^{-2}p^{-2\sum\theta}[X^j]\det\left(\widetilde{\Gamma}^\beta + X\widetilde{\Gamma}^\alpha\right)$, so $v_p([X^j]\Delta_K) \geq j - 2\sum\theta = v_p([X^0]\Delta_K) + j$.

Step 4. Hence $v_p(f_0) < v_p(f_j)$ for all $j \geq 1$ (including $f_j = 0$, valuation $+\infty$), and [note, Lemma 3.4] gives $\Delta_K(a/b) \neq 0$ for $p \nmid b$. □

the proof of Theorem 3.13 in one paragraph. At a prime $p \in [2.1n + 2, 3n)$ the nodes pair up $(k,\ k-p)$ or stay alone, and each node's p-adic data is one row of Table 14.1. The tree bound says the denominator of Δ_K at p is at most $16(N_{\mathrm{Ra}}+N_{\mathrm{Rc}})+6N_{\mathrm{Rb}}-2$, largest for $K = K(n,p)$. In a basis of Hermite interpolation polynomials at the R nodes (unimodular change of basis), rescaled by half the marginal values, the Gram matrix becomes, modulo $\sqrt{p}$, block diagonal with explicit blocks of determinants $\pm$ (powers of $2, 3, 7$) $\times$ units; the Ra block needs the partner's unit, which is -8 times the node's unit (Wilson's theorem makes the ratio of the factorial parts $\equiv -1$ (so its fourth power is $\equiv 1$), and the factor $-8 = (-2)^3$ comes from the covering triple zero shared by the two partners), and $-8 \not\equiv 1$ modulo p. So the constant coefficient attains the tree bound exactly, and the X-part, which is p-adically smaller by at least one power of p per column, cannot compete.

14.4 The worked example and further cases

Here we collect exact computations that do not use the note's argument: $\Delta_K(X)$ is computed from the definitions (local constants [note, (2.21)] with the harmonic sums [note, (2.14)], moments by [note, (2.27)], the exact $K \times K$ determinant at $K+1$ integer values of X, interpolated exactly), and its valuations are read off. Nothing from [note, Section 6] enters except the choice of K.

Example 14.32 ($n = 5$, $p = 13$, from start to finish)**.** *Window:* $12.5 \leq 13 < 15$; $13 \equiv 1 \pmod 3$. *Nodes:* Example 14.7, Figure 14.1: one Ra pair $\{8, -5\}$, the Rb_g pair $\{9, -4\}$, one Rc pair $\{10, -3\}$, ten U nodes. *Counts:* $N_{\mathrm{Ra}} = N_{\mathrm{Rb}} = N_{\mathrm{Rc}} = 1$; $K = 10n - \frac{10(p-1)}{3} = 50 - 40 = 10 = 4 \cdot 2 + 2$. *Prediction:* $v_{13}([X^0]\Delta_{10}) = -(16 \cdot 2 + 6 \cdot 1 - 2) = -36$, and $v_{13}([X^j]) \geq -36 + j$. *Computation:* the valuations of the eleven coefficients are $-36, -35, -34, -33, -30, -27, -24, -19, -14, -9, -3$ (Example 14.1): the prediction for $[X^0]$ is exact, the bound for $[X^j]$ holds and is attained for $j = 1, 2, 3$. *Tree bound:* $T_{13}^{+} = 36$ at $K = 10$, so at this prime the tree bound is exact. *Mechanism:* $\det\Xi = 2^{16}$, a unit; $\det\Gamma^\beta = (\det T)^2[X^0]\Delta_{10}$; 109 contributions with $\omega = 0$, all of the predicted kinds; the rescaled matrix modulo 13 is block diagonal with the blocks of Example 14.27; $\varepsilon_{-5} \equiv 5 \equiv -8\varepsilon_8$; the reduced determinant is $2 \neq 0$.

Example 14.33 (all cases with $n \leq 17$)**.** The same computations for every odd $n \leq 17$ and every prime p with $2.1n + 2 \leq p < 3n$:

n	p	K	N_{Ra}	N_{Rb}	N_{Rc}	$v_p([X^0]\Delta_K)$	predicted	$v_p([X^j]) \geq v_p([X^0]) + j$
5	13	10	1	1	1	-36	-36	yes
7	17	18	2	1	2	-68	-68	yes
7	19	10	1	1	1	-36	-36	yes
9	23	18	2	1	2	-68	-68	yes
11	29	18	2	1	2	-68	-68	yes
11	31	10	1	1	1	-36	-36	yes
13	31	30	3	3	3	-112	-112	yes
13	37	10	1	1	1	-36	-36	yes
15	37	30	3	3	3	-112	-112	yes
15	41	18	2	1	2	-68	-68	yes
15	43	10	1	1	1	-36	-36	yes
17	41	38	4	3	4	-144	-144	yes
17	43	30	3	3	3	-112	-112	yes
17	47	18	2	1	2	-68	-68	yes

In every case the prediction (14.9) for the constant coefficient is exact, every coefficient satisfies $v_p([X^j]) \geq v_p([X^0]) + j$ (with equality for some $j \geq 1$ in every case), and all the intermediate statements above (Table 14.1, Proposition 14.8, Lemma 14.11, Lemma 14.15, Lemma 14.19, (14.5), Lemma 14.20, Lemma 14.26, the reduced determinant $\neq 0$) hold. For example, for $n = 13$, $p = 31$ the valuations of $[X^0], \ldots, [X^{30}]$ are $-112, -111, -110, -109, -108, -107, -106, -104, -102, -99, \ldots, -8$.

None of these cases lies in the window $p \leq 2.159n$ that the proof of [note, Theorem 1.1] uses: that window $[2.1n + 2, 2.159n]$ has length $0.059n - 2$ and first contains a prime at $n = 45$ ($p = 97$). Their K values are therefore below $2.8n$ (e.g. $K = 10 = 2n$ for $n = 5$); [note, Theorem 3.13] does not need $p \leq 2.159n$ for the non-vanishing, so they test the same statement. In the window, at $n = 45$, $p = 97$ ($K = 130$, $\kappa = 2.889$, $N_{\mathrm{Ra}} = N_{\mathrm{Rb}} = N_{\mathrm{Rc}} = 13$, types as in Table 14.1), the constant coefficient $[X^0]\Delta_{130} = \det[\beta(y^{i+j})]_{i,j<130}$, computed exactly as a single 130×130 rational determinant, has $v_{97} = -492 = -(16 \cdot 26 + 6 \cdot 13 - 2)$, as predicted. So the examples in which every coefficient is computed ($n \leq 17$, the table) all lie below the window, and at $(45, 97)$ only the constant coefficient was computed, not the higher ones.

Check yourself 14.34. In the $n = 5$, $p = 13$ example, $v_{13}([X^j]) = v_{13}([X^0]) + j$ exactly for $j = 1, 2, 3$. Where in the proof could one see that the bound of Step 3 is sharp for small j?

Answer. The entries of $\widetilde{\Gamma}^\alpha$ are in $p\mathbb{Z}_p[\sqrt{p}]$, and Lemma 14.20 says the best α contributions have $\omega = 1$; for $n = 5$ the minimum is 1 (at U nodes, Example 14.21). So some columns of $\widetilde{\Gamma}^\alpha$ have entries of valuation exactly 1, and replacing one or a few columns of the unit-determinant matrix $\widetilde{\Gamma}^\beta$ by such columns can give a determinant of valuation exactly j. The proof only needs the inequality; that it is attained for $j \leq 3$ is an observation in this example, not a statement of the note.

Summary of the chapter

At a prime p with $2.1n + 2 \leq p < 3n$, two nodes are congruent modulo p only if they differ by p, so the nodes split into R nodes $[p - n, 2n]$, their L partners, and unpaired U nodes; by [note, Lemma 6.1] each has one of the types of [note, Table 2], determined by the thresholds [note, (6.2)], with $D_k \in \{1, -2, -3, 0\}$. The counts [note, (6.3)] give $K(n, p) = 4(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 2N_{\mathrm{Rb}}$ [note, (6.4)], the number of rows that maximizes the relaxed tree bound, whose marginal values are $7, 5, 3, 1$ (a/c pairs), $4, 2$ (b pairs), $3, 1$ (the b_g pair); its maximum is $16(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 6N_{\mathrm{Rb}} - 2$. Zooming in by $z = pw$, the virtual-pole part of the local constants at R and La nodes

is $\beta^{\mathrm{HS}}_{k,m} = \varepsilon_k p^{-D_k+m-6}(\phi_{k,3-m} + O(p))$ with explicit ϕ [note, (6.6)] ([note, Lemma 6.7]), and $\varepsilon_{k-p} \equiv -8\varepsilon_k$ at an Ra node ([note, Lemma 6.10]): Wilson's theorem makes the ratio of the factorial parts $\equiv -1$ (so its fourth power is $\equiv 1$), and the factor $-8 = (-2)^3$ comes from the covering triple zero shared by the two partners. In the Hermite basis E_x at the R nodes ([note, Lemma 6.12], unimodular), scaled by p^{θ_x} with θ_x half the marginal values, every contribution has weighted valuation $\omega \geq 0$ ([note, Lemma 6.17], [note, Appendix D]), so modulo $\sqrt{p}$ in $\mathbb{Z}_p[\sqrt{p}]$ the Gram matrix is block diagonal with the explicit blocks of [note, Lemma 6.18], of unit determinants $(3^{20}/2^{12}$, $-3^{10}/2^6$, $-7 \cdot 3^{10}/2^6$, 3^{20} times units; $\det\left(A_{\mathrm{Ra}} + rB^{\mathsf{T}} A_{\mathrm{La}} B\right) = 3^{12}(r-1)^4)$. Hence $v_p([X^0]\Delta_K) = -(16(N_{\mathrm{Ra}} + N_{\mathrm{Rc}}) + 6N_{\mathrm{Rb}} - 2)$ exactly and $v_p([X^j]\Delta_K) \geq v_p([X^0]\Delta_K) + j$, and the dominance lemma gives $\Delta_K(a/b) \neq 0$ for $p \nmid b$ ([note, Theorem 3.13]). An exact computation of $\Delta_K(X)$ from the definitions for all 14 admissible (n, p) with $n \leq 17$ shows: the predicted valuation of the constant coefficient is exact in every case, the dominance inequality holds for every coefficient, and every intermediate statement of [note, Section 6] holds; for $(n, p) = (45, 97)$, inside the window of [note, Theorem 1.1], the constant coefficient has the predicted valuation -492 (its higher coefficients were not computed).

Carried forward to Chapters 7 and 15: [note, Theorem 3.13], i.e. $\Delta_K(a/b) \neq 0$ for $p \nmid b$ with $K = K(n, p)$, which is the hypothesis $F(a/b) \neq 0$ of the criterion. The exact formula (14.9) also shows that at the auxiliary prime the tree bound of Chapters 11 and 13 is attained.

Chapter 15

Looking back: the whole proof on two pages

Where we are. The four estimates are now explained. Each step below is the note's claim; none has been checked by an expert. This chapter puts the main proof back together in one pass, without the details, so that the architecture is visible; then it records what the note takes from outside, which of its numbers depend on a computer, what the worked examples show, and the remarks on the note made along the way. It covers no new mathematics. The second proof ([note, Appendix F]) is summarized at the end of Chapter 17 and compared with the first in Section 15.5.

15.1 The proof in ten steps

Step 1: the number. $\zeta_3(5) = L_3(5, \mathbf{1})$ is the value at $s = 5$ of the Kubota–Leopoldt 3-adic L-function of the trivial character [note, (2.4)]. It is an element of $\mathbb{Q}_3$, of valuation -1, and the theorem says it is not in $\mathbb{Q}$ (Chapter 3).

Step 2: the number as an integral. Washington's formula for L_3 turns into a Volkenborn integral, $\zeta_3(5) = \frac{1}{972}\sum_{r=1,2}\int_{\mathbb{Z}_3}(t+\frac{r}{3})^{-4}\,\mathrm{d}t$ [note, Lemma 2.11], and shifting the integration variable by an integer costs a harmonic sum [note, Lemma 2.15] (Chapter 4).

Step 3: the functional. For odd n, the weight W [note, (1.2)] has poles of order 4 at the $3n+1$ nodes and zeros of order 3 on the two classes $\frac{1}{3}+\mathbb{Z}$, $\frac{2}{3}+\mathbb{Z}$. The functional $L(P) = \sum_r \int_{\mathbb{Z}_3}(PW)'(t+\frac{r}{3})\,\mathrm{d}t$ takes values $\beta(P) + \zeta_3(5)\alpha(P)$ with rational α, β: partial fractions plus Step 2, with $\zeta_3(3)$ removed by the derivative and the residue theorem [note, Lemma 2.19] (Chapter 5).

Step 4: the polynomial. Replacing $\zeta_3(5)$ by an indeterminate X in the moments gives the Hankel polynomial $\Delta_K(X) = \det\big[\beta(y^{i+j}) + X\alpha(y^{i+j})\big]_{i,j<K}$, of degree at most K, with $\Delta_K(\zeta_3(5)) = \det\big[L(y^{i+j})\big]$ for $K \le 3n+1$ [note, Definition 2.23, (2.26)] (Chapter 6).

Step 5: the criterion. If $\zeta_3(5) = a/b$ and $\Delta_K(a/b) \neq 0$, clearing denominators gives a nonzero integer, and the product formula gives

$$\underbrace{v_3(\Delta_K(\zeta_3(5)))\log_2 3}_{\text{gain}} \le \underbrace{\log_2\|\Delta_K\|_1}_{\text{size}} + \underbrace{\sum_{p\neq 3}(-v_p(\Delta_K))^+\log_2 p}_{\text{denominators}} + K\log_2\max(|a|,b)$$

[note, Lemma 3.1] (Chapter 7).

Step 6: the gain [note, Theorem 3.5]. On the integration set $S = 3^{-1}\mathbb{Z}_3^\times$ every node is at 3-adic distance 3, so the poles give $4(3n+1)$ trits per entry; the zeros and the linear factor cost $3n+1$; the integral Pochhammer symbol gives $3v_3(n!) \approx 1.5n$. Writing the determinant

in the integer-valued basis F_i costs $K^2/4$ trits. Total: $G(\kappa)n^2 = (10.5\kappa - \kappa^2/4)n^2 \log_2 3$ bits (Chapter 8).

Step 7: the size [note, Theorem 3.8]. Heine's expansion writes Δ_K as a sum over ways of placing K "charges" on the nodes, at most 4 per node [note, Proposition 5.1]; the triangle inequality and a continuum limit turn the largest term into the energy of a density in an electrostatic field, bounded by a trial density plus a duality gap. Result: $(\kappa^2 - 6\kappa)n^2 \log_2 n + F^\dagger n^2$, with $F^\dagger \le 8.65$ by computer (Chapters 9 and 10).

Step 8: the denominators [note, Theorem 3.10]. The same expansion with the ultrametric inequality, prime by prime: the tree bound [note, Theorem 5.13]; for small primes a crude count summed with Mertens' theorem gives $\kappa(6-\kappa)n^2 \log_2 n$; for primes of size about n, the virtual poles coming from harmonic sums cancel against the zeros of W [note, Lemma 5.24], and a circle model summed with the prime number theorem gives the constant $c \le 31.72$ by computer (Chapters 11 to 13).

Step 9: non-vanishing [note, Theorem 3.13]. For a prime $p \in [2.1n + 2, 2.159n]$ not dividing b, and $K = K(n,p) \in (2.8n, 3n-2]$, the constant coefficient of Δ_K is strictly p-adically dominant: in an adapted basis, after scaling by half-integer powers of p, the Gram matrix is block diagonal modulo $\sqrt{p}$ with invertible blocks, the Ra block being invertible because the units of the two partners differ by the factor -8 [note, Lemma 6.10]: Wilson's theorem makes the factorial parts agree, and the shared covering zero contributes $(-2)^3$ (Chapter 14).

Step 10: the contradiction. The $n^2 \log n$ terms of Steps 7 and 8 cancel exactly. By the note's Table 1, what remains is $G(\kappa) - F_i^\dagger - c_i \ge 4.58$ bits per n^2 on all of $\kappa \in [2.8, 3]$ [note, Table 1], against an $o(n^2)$ error and the $O(n)$ term $K \log_2 \max(|a|, b)$. If the estimates hold, this is impossible for n large [note, Theorem 1.1] (Chapter 7).

item	value, bits per n^2	where
gain $G(\kappa)$	$+43.49$	Chapter 8
size, $n^2 \log n$ part	$-8.96 \log_2 n$	Chapter 10
denominators, $n^2 \log n$ part	$+8.96 \log_2 n$	Chapter 11
size constant $F_1^\dagger$	8.43	Chapter 10
denominator constant c_1	30.48	Chapter 13
margin	4.58	[note, Table 1]

Table 15.1: The balance sheet on the first interval $I_1 = [2.80, 2.84]$, with the note's numbers: G at $\kappa_{1,1} = 2.8$, the $n^2 \log n$ coefficients at $\kappa = 2.8$, and the bounds $F_1^\dagger$, c_1, which hold on all of I_1. The margin is $G - F_1^\dagger - c_1$. The two $n^2 \log n$ terms appear with opposite signs on the same side of the inequality and cancel.

15.2 What the note takes from outside

The main proof uses, besides its own lemmas: the existence of the Kubota–Leopoldt function and Washington's formula [note, Theorem 2.1] [34]; the basic theory of the Volkenborn integral [33, 28]; the prime number theorem [16, 13] and Mertens' theorem with its constant [29]; Wilson's theorem; and two computer evaluations, of $F_i^\dagger$ [note, Proposition 5.11] and of c_i [note, Proposition 5.40], in ball arithmetic [17]. Everything else is given a proof in the note, including the results it adapts from the preprint [19] [note, Appendices A–C]. The second proof depends in addition on published theorems on overconvergent modular forms [10, 11, 6] and four standard facts listed after [note, Proposition F.24] (Chapter 17).

15.3 What the worked examples show

Every chapter illustrates its objects with exact computations in small cases, and several of these computations test a statement of the note directly. The definition of $\zeta_3(5)$ and its integral representation agree digit by digit when computed in three different ways: from Washington's series, from the Kummer limit of Bernoulli numbers, and from Riemann sums of the Volkenborn integral (Chapters 3 and 4). The purity lemma, the heart of the construction, can be tested by computing $L(P)$ directly from Riemann sums of $(PW)'$ for $n = 1$ and $n = 3$ and comparing with $\beta(P) + \zeta_3(5)\alpha(P)$: the agreement improves by one 3-adic digit per level, and in a case excluded by the lemma ($\deg PW = -1$) the two differ by exactly the predicted $\zeta_3(3)$ term with coefficient -54 (Chapter 5).

For the gain, the note's explicit lower bound [note, (4.9)] holds against the exact valuation $v_3(\Delta_K(\zeta_3(5)))$ in every case computed ($n = 1$, $K \le 4$; $n = 3$, $K \le 10$), at 62 to 90% of the true value (Chapter 8). The Heine expansion reproduces Δ_K exactly for $n \le 3$, $K \le 5$, and exactly the predicted terms vanish (Chapter 9). The tree bound lies above the true exponent of every prime in the denominators of Δ_{3n} for $n = 3, 5, 7$, within 7 of it (Chapter 11); the refined local lemma holds in all 3232 local constants computed, and the cancellation of virtual poles can be seen term by term (Chapter 12). The non-vanishing theorem's prediction for the valuation of the constant coefficient, and strict dominance, hold exactly in all 14 admissible cases with $n \le 17$, and the constant coefficient at $(n, p) = (45, 97)$, the first case inside the window $p \le 2.159n$, has the predicted valuation -492 (Chapter 14).

A floating-point evaluation following the note's description gives the five bounds for $F_i^\dagger$ to six decimals (Chapter 10) and the five sums entering c_i to all seven printed decimals (Chapter 13); such an evaluation is not a proof. The arithmetic of [note, Table 1] is redone in Chapters 1 and 7.

15.4 What the examples cannot show

The estimates of Steps 6–8 are asymptotic: they hold with error terms $O(n \log n)$ or $o(n^2)$ whose constants the note does not make explicit, and the contradiction appears only for n large. No computation at feasible n can exhibit the margin; one error term alone is still about 29 bits per n^2 (about 20 in natural-logarithm units) at $n = 10^{20}$ (Chapter 11). The examples test the formulas, the lemmas in small cases and the printed numbers; they cannot detect an error in an asymptotic argument that is correct in every small case. A floating-point evaluation of $F_i^\dagger$ and c_i is not a substitute for the note's ball-arithmetic bounds. The exact non-vanishing examples lie below the window used in the proof ($K < 2.8n$), except for the constant coefficient at one n. The note has not been checked by an expert, and neither have these notes.

15.5 The two proofs side by side

The second proof (Chapters 16 and 17) has the same architecture as the first: a nonzero rational number built from $\zeta_3(5)$, which is 3-adically tiny, has controlled denominators and controlled absolute value, so that the product formula gives a contradiction. Everything else differs. The first proof builds its number from a Volkenborn integral and a Hankel determinant, gets non-vanishing from an auxiliary prime, and bounds its two order-n^2 costs by computer; its external inputs are classical (the Kubota–Leopoldt function, the prime number theorem, Mertens' theorem). The second proof builds a determinant of Taylor coefficients of functions on the modular curve $X_0(3)$; non-vanishing follows from the linear independence of the functions involved (no auxiliary prime is needed), the margin is about 1.52 (in natural logarithms per d^2) instead of 4.58 bits per n^2, and the 3-adic estimate rests on published theorems on

overconvergent modular forms, whose statements the note quotes and whose proofs it has not checked. Logically, the two proofs share only the statement and the normalization of $\zeta_3(5)$, so an error in one need not invalidate the other; both were, however, produced by the same process, and neither has been checked by an expert.

15.6 Remarks on the note

Writing the proof out raised the following points. None of them, as far as we can tell, affects the validity of the argument; they are collected so that a reader or a referee can decide.

- After [note, (2.14)] the note says that the terms of $\mathrm{HS}_3(k, M)$ with $p \mid u$ have p-adic valuation $-M$. The exact valuation is $-Mv_p(u)$, which differs when $p^2 \mid u$ (already at $p = 2$, $u = 4$). The bounds that use it, [note, Lemma 5.16] and the leaf lemma, use the correct form, and at single-level primes the two agree (Chapters 4 and 11).
- [note, Remark 5.27] compares the refined local lemma with "the cruder bound". Its "about 44 bits per n^2" matches the bound that charges each virtual pole without the cancellation (about 44.08 in our evaluation), not the literal $-D_k - 6 + m$ at every node (about 112) (Chapters 12 and 13). The same remark explains the gap between $c_5 \le 31.72$ and "about 31.5" by the uniformity over I_5; that accounts for about 0.01 bits, the rest coming from the 32 subcells of the computation. The remark is not part of the proof.
- The note's introduction calls the F_i "the natural basis" of $\mathrm{Int}(S)$; [note, Lemma 4.1] proves only $F_i \in \mathrm{Int}(S)$, which is all the proof needs. Bhargava's theory of p-orderings, as explained in Chapter 8, supports the stronger reading.
- The note's sentence that the cross factor of the Heine expansion "carries the node differences up to corrections" is descriptive: at $n = 1$ the corrections dominate. The size estimate does not rely on them being small; Cauchy's estimate absorbs them into a factor $e^{O(n)}$ (Chapters 9 and 10).
- The hypothesis $p \le 0.4n$ of [note, Lemma 5.19] appears to be used only for the clipping in the relaxed bound (Chapter 11); the ordering [note, (6.2)] needs only $1.5n < p < 3n$ (Chapter 14). Neither affects the proof.
- For the second proof, the 3-adic estimate [note, Proposition F.24] rests on a chain of published results (Coleman, Coleman–Mazur, Buzzard, Katz) and four facts the note lists as unchecked. The steps an expert should confirm first are that Coleman's overconvergence at tame level 1 agrees with Buzzard's notion at level 5, and that the trace construction gives H_{η_5} on the whole disc. The observed decay $v_3([x^n]H_{\eta_5}) \approx 6n$ for $n \le 129$ is consistent with the claim but proves nothing (Chapter 17).

Summary of the chapter

The main proof is a balance of four estimates, three of order n^2 after an exact cancellation of $n^2 \log n$ terms, and a non-vanishing argument at an auxiliary prime. Its external inputs are standard theorems plus two constants bounded by computer (ball arithmetic). The worked examples agree with the note's definitions, with its lemmas in small cases and with its printed constants; the asymptotic estimates themselves, and the ball-arithmetic certificates, have not been checked by an expert.

Part V

The second proof

Chapter 16

A crash course in modular forms on $X_0(3)$

Where we are. The note contains a second proof of the theorem [note, Appendix F], independent of the first, which adapts the determinant argument of the preprint [35] for $\zeta_7(3)$. It shares with the first proof only the statement and the number $\zeta_3(5) = L_3(5, \mathbf{1})$ of Chapter 3, and it is built from modular forms, which this companion has not used so far and which we do not assume the reader knows. This chapter supplies exactly the modular forms that [note, Appendix F] needs, from scratch: the upper half plane, the groups $\mathrm{SL}_2(\mathbb{Z})$ and $\Gamma_0(3)$, fundamental domains, cusps and elliptic points, q-expansions, modular forms and functions, the Dedekind η function, the coordinate x (the "Hauptmodul") with its q-expansion [note, (F.1)], the function j, the Fricke involution, the weight-2 form B and the Eichler integral G_5 [note, (F.2)], and then the modular identities of [note, Section F.1]: [note, Lemma F.5] (the curve, x and j), [note, Lemma F.6] (the zeros of B), [note, Lemma F.7] (two rational functions V and R_5), the recursion [note, (F.8)] with [note, Lemma F.9], and the differential operator L_5 of [note, Lemma F.10] with its coefficients [note, (F.11)]. The chapter ends by saying how Chapter 17 uses these objects. From earlier chapters we need only the 3-adic absolute value of Chapter 2 (in one remark) and $\zeta_3(5)$ from Chapter 3 (in the definition of η_5). The series in this chapter are built from their definitions in exact rational arithmetic; the values of functions at points of the upper half plane are 40-digit floating-point evaluations, which illustrate the statements but do not prove them.

Two textbooks cover far more than we need: Apostol [2] (the note's reference for η; Chapters 1–3 contain $\mathrm{SL}_2(\mathbb{Z})$, Eisenstein series, j and η) and Diamond–Shurman [14] (the note's reference for $\Gamma_0(3)$; Chapters 1–3). We prove what is elementary and state the rest with a reference.

16.1 The upper half plane and the modular group

16.1.1 Moebius maps

The upper half plane is $\mathbb{H} = \{\tau \in \mathbb{C} : \operatorname{Im}\tau > 0\}$. A real 2×2 matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with determinant $ad - bc = 1$ acts on it by the Moebius map

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}\,, \qquad \operatorname{Im}(\gamma\tau) = \frac{\operatorname{Im}\tau}{|c\tau + d|^2}\,, \qquad \frac{\mathrm{d}(\gamma\tau)}{\mathrm{d}\tau} = \frac{1}{(c\tau + d)^2}\,. \tag{16.1}$$

The second formula follows from $\gamma\tau = \frac{(a\tau+b)(c\bar{\tau}+d)}{|c\tau+d|^2}$, whose numerator has imaginary part $(ad - bc)\operatorname{Im}\tau = \operatorname{Im}\tau$; so γ maps $\mathbb{H}$ to itself. The third is the quotient rule: $\frac{a(c\tau+d)-c(a\tau+b)}{(c\tau+d)^2} =$

$\frac{ad-bc}{(c\tau+d)^2}$. Composition of maps is multiplication of matrices, and γ and $-\gamma$ give the same map. The *modular group* is $\mathrm{SL}_2(\mathbb{Z})$, the integer matrices of determinant 1. Two elements play a special role:

$$T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) : \ \tau \mapsto \tau + 1 \ , \qquad S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) : \ \tau \mapsto -\frac{1}{\tau} \ .$$

Intuition: the upper half plane is Euclidean AdS_2. With the metric $\mathrm{d}s^2 = (\mathrm{d}X^2 + \mathrm{d}Y^2)/Y^2$ ($\tau = X + iY$), $\mathbb{H}$ is the hyperbolic plane, that is, Euclidean AdS_2 in Poincaré coordinates, and the maps (16.1) with real entries are exactly its orientation-preserving isometries. The real line together with ∞ is the conformal boundary. The modular group is a *discrete* subgroup of the isometries, and the objects of this chapter are functions on the quotient of AdS_2 by it, an orbifold. Geodesics are vertical lines and half circles centred on the real axis; all the boundaries in Figure 16.1 are of this kind.

Fact 16.1 (generators and fundamental domain; [2, Ch. 2])**.** *(a) S and T generate $\mathrm{SL}_2(\mathbb{Z})$. (b) Every $\tau \in \mathbb{H}$ can be moved by an element of $\mathrm{SL}_2(\mathbb{Z})$ into the closed region $\mathcal{F} = \{|\mathrm{Re}\,\tau| \le \frac{1}{2},\ |\tau| \ge 1\}$, and two distinct points of the interior of $\mathcal{F}$ are never related by an element of $\mathrm{SL}_2(\mathbb{Z})$.*

$\mathcal{F}$ is called the standard *fundamental domain*: one copy of each orbit, up to identifications on the boundary (T glues the two vertical sides, S glues the left half of the bottom arc to the right half). The proof of (b) is an algorithm, which we run.

Example 16.2 (moving a point into $\mathcal{F}$)**.** Repeat: translate by a power of T so that $|\mathrm{Re}\,\tau| \le \frac{1}{2}$; if then $|\tau| < 1$, apply S. By (16.1), S multiplies $\mathrm{Im}\,\tau$ by $1/|\tau|^2 > 1$, so the imaginary part grows at each S-step, and the algorithm stops (there are only finitely many $c\tau + d$ with $|c\tau + d| < 1$). Start from $\tau_0 = 0.27 + 0.06\,i$:

$$\tau_0 \xrightarrow{S} -3.5294 + 0.7843\,i \xrightarrow{T^4} 0.4706 + 0.7843\,i \xrightarrow{S} -0.5625 + 0.9375\,i \xrightarrow{T} 0.4375 + 0.9375\,i \ .$$

(The first step by hand: $-1/\tau_0 = -100/(27+6i) = -100(27-6i)/765$.) The end point $\frac{7}{16} + \frac{15}{16}i$ has $|\tau| = 1.0346 \ge 1$ and lies in $\mathcal{F}$. The four steps compose to $g = TST^4S = \left(\begin{smallmatrix} 3 & -1 \\ 4 & -1 \end{smallmatrix}\right)$, and indeed $g\tau_0 = \frac{3\tau_0 - 1}{4\tau_0 - 1} = 0.4375 + 0.9375\,i$. The imaginary part went $0.06 \to 0.78 \to 0.94$.

16.1.2 The group $\Gamma_0(3)$

Definition 16.3 ($\Gamma_0(3)$)**.** $\Gamma_0(3) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \ 3 \mid c\}$.

It is a subgroup: the lower left entry of a product is $c_1a_2 + d_1c_2$, divisible by 3 when c_1 and c_2 are, and the inverse $\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ keeps c up to sign. It contains T but not S. The second proof lives on $\Gamma_0(3)$ because of the prime 3: the 3-adic properties of the forms on $\Gamma_0(3)$ (Chapter 17) are what gives the 3-adic gain.

Proposition 16.4 (index 4)**.** $\mathrm{SL}_2(\mathbb{Z})$ *is the disjoint union of the four cosets $\Gamma_0(3)\alpha$ with $\alpha \in \{I,\ S,\ ST,\ ST^{-1}\}$.*

Proof. Attach to $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ its bottom row modulo 3, read as a point $(c : d)$ of the projective line over $\mathbb{F}_3$ (pairs $(c, d) \ne (0, 0)$ modulo 3 up to a common nonzero factor). The row is never $(0, 0)$ modulo 3, because $\gcd(c, d) = 1$. The projective line over $\mathbb{F}_3$ has 4 points, $(0 : 1), (1 : 0), (1 : 1), (1 : 2)$. Now $\gamma_1\gamma_2^{-1} \in \Gamma_0(3)$ if and only if the lower left entry of $\gamma_1\gamma_2^{-1} = \gamma_1 \left(\begin{smallmatrix} d_2 & -b_2 \\ -c_2 & a_2 \end{smallmatrix}\right)$, which is $c_1d_2 - d_1c_2$, is divisible by 3, that is, if and only if $(c_1 : d_1) = (c_2 : d_2)$. So the cosets $\Gamma_0(3)\gamma$ correspond one-to-one to points of the projective line that occur. The bottom rows of I, $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ and $ST^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ are $(0 : 1), (1 : 0), (1 : 1), (1 : 2)$, all four points. □

For the point of Example 16.2, $g = \left(\begin{smallmatrix} 3 & -1 \\ 4 & -1 \end{smallmatrix}\right)$ has bottom row $(1:2)$; then $Sg = \left(\begin{smallmatrix} -4 & 1 \\ 3 & -1 \end{smallmatrix}\right)$ lies in $\Gamma_0(3)$, and it moves τ_0 to $(Sg)\tau_0 = -0.4088 + 0.8759\,i$.

16.1.3 A fundamental domain for $\Gamma_0(3)$

If $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_\alpha \Gamma_0(3)\alpha$, then $\bigcup_\alpha \alpha\mathcal{F}$ is a fundamental domain for $\Gamma_0(3)$: for $\tau \in \mathbb{H}$ write $\tau = g^{-1}\tau_F$ with $g \in \mathrm{SL}_2(\mathbb{Z})$, $\tau_F \in \mathcal{F}$, and $g^{-1} = \gamma\alpha$ with $\gamma \in \Gamma_0(3)$; then $\gamma^{-1}\tau = \alpha\tau_F \in \alpha\mathcal{F}$. Here this gives four copies of $\mathcal{F}$. Following the edges of $\mathcal{F}$ under the maps S, ST, ST^{-1} (for example, S maps the line $\mathrm{Re}\,\tau = \frac{3}{2}$ to the circle $\left|\tau + \frac{1}{3}\right| = \frac{1}{3}$, and $\frac{3}{2} + \frac{\sqrt{3}}{2}i$ to $-\frac{1}{2} + \frac{i}{2\sqrt{3}}$) one finds that their union is

$$\mathcal{F}_3 = \left\{\tau \in \mathbb{H} : \ |\mathrm{Re}\,\tau| \le \tfrac{1}{2},\ \left|\tau - \tfrac{1}{3}\right| \ge \tfrac{1}{3},\ \left|\tau + \tfrac{1}{3}\right| \ge \tfrac{1}{3}\right\}, \tag{16.2}$$

shown in Figure 16.1. Its hyperbolic area is $\iint \mathrm{d}X\,\mathrm{d}Y/Y^2 = 2\int_0^{1/2} \mathrm{d}X/\sqrt{\frac{1}{9} - (X - \frac{1}{3})^2} = 2[\arcsin(3X-1)]_0^{1/2} = 2(\frac{\pi}{6} + \frac{\pi}{2}) = \frac{4\pi}{3}$, four times the area $\frac{\pi}{3}$ of $\mathcal{F}$, as it must be. Numerical quadrature gives $4.18879020478639 = 4\pi/3$. In Example 16.2, the point $(Sg)\tau_0 = -0.4088 + 0.8759\,i$ lies in $\mathcal{F}_3$: its distances to $\frac{1}{3}$ and $-\frac{1}{3}$ are 1.148 and 0.879, both $\ge \frac{1}{3}$.

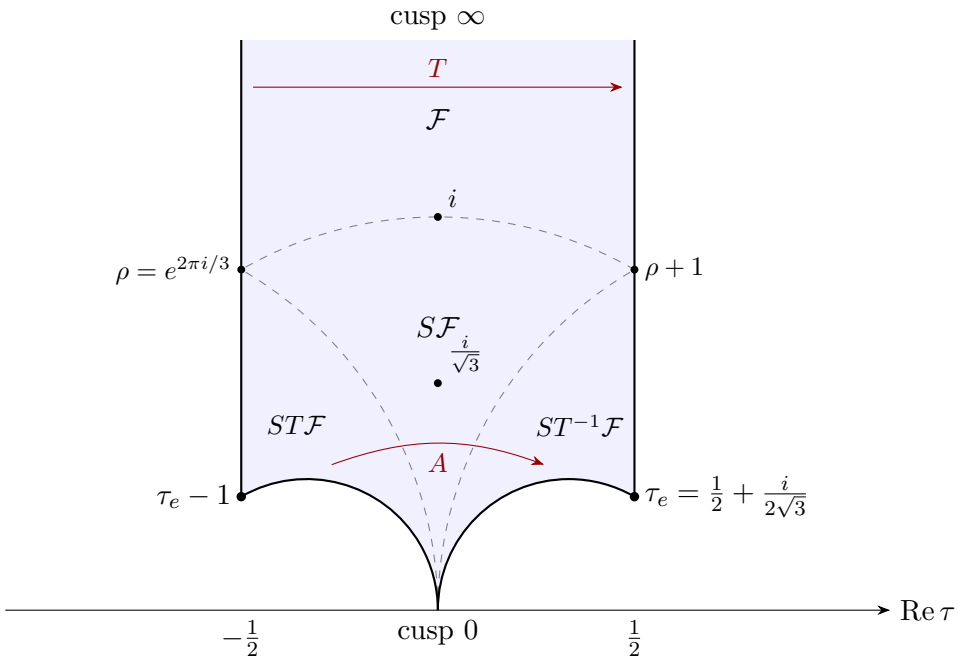


Figure 16.1: The fundamental domain $\mathcal{F}_3$ of $\Gamma_0(3)$ (shaded, bold boundary), the union of four copies of the standard domain $\mathcal{F}$ of $\mathrm{SL}_2(\mathbb{Z})$ (dashed lines separate the copies). T glues the two vertical sides, $A = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)$ glues the left arc $\left|\tau + \frac{1}{3}\right| = \frac{1}{3}$ to the right arc $\left|\tau - \frac{1}{3}\right| = \frac{1}{3}$. The domain touches the real axis only at the cusp 0; the two lower corners $\tau_e - 1$ and τ_e are glued by T and form one elliptic point.

16.1.4 Gluing: cusps, the elliptic point, and a sphere

The quotient $\Gamma_0(3)\backslash\mathbb{H}$ is obtained from $\mathcal{F}_3$ by gluing its sides. The vertical sides are glued by T. The left arc is glued to the right arc by $A = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right) \in \Gamma_0(3)$, $A\tau = \tau/(3\tau + 1)$: A fixes 0, and it maps $\tau_e - 1$ to τ_e, since $3(\tau_e - 1) + 1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i = e^{2\pi i/3}$ and $\tau_e - 1 = \frac{1}{\sqrt{3}}e^{5\pi i/6}$, so $A(\tau_e - 1) = \frac{1}{\sqrt{3}}e^{i\pi/6} = \frac{1}{2} + \frac{i}{2\sqrt{3}} = \tau_e$.

Cusps. The domain reaches the boundary $\mathbb{R}\cup\{\infty\}$ at two points, ∞ and 0. These are the two *cusps* of $\Gamma_0(3)$: every rational number a/c in lowest terms is $\Gamma_0(3)$-equivalent to ∞ if $3 \mid c$, and to 0 if $3 \nmid c$ [14]. That the two classes cannot mix is elementary: $\gamma = \left(\begin{smallmatrix} a' & b' \\ 3c' & d' \end{smallmatrix}\right) \in \Gamma_0(3)$ sends a/c to $(a'a+b'c)/(3c'a+d'c)$, a fraction again in lowest terms (because γ is invertible over $\mathbb{Z}$), whose denominator is $\equiv d'c \pmod 3$ with $3 \nmid d'$; so 3 divides the new denominator exactly when it divides c. Near the cusp ∞ the quotient looks like a half-infinite cylinder ($\tau \sim \tau+1$, $\operatorname{Im}\tau \to \infty$), which in the variable $q = e^{2\pi i\tau}$ of Section 16.2 becomes a punctured disc around $q=0$; filling in the puncture adds one point. The same happens at 0.

The elliptic point. The matrix $\gamma_e = \left(\begin{smallmatrix} 2 & -1 \\ 3 & -1 \end{smallmatrix}\right) \in \Gamma_0(3)$ fixes $\tau_e = \frac{1}{2} + \frac{i}{2\sqrt{3}}$: $2\tau_e - 1 = \frac{i}{\sqrt{3}}$ and $3\tau_e - 1 = e^{i\pi/3}$, so $\gamma_e\tau_e = \frac{1}{\sqrt{3}}e^{i\pi/2 - i\pi/3} = \frac{1}{\sqrt{3}}e^{i\pi/6} = \tau_e$. It has trace 1, so by Cayley–Hamilton $\gamma_e^2 = \gamma_e - I$ and $\gamma_e^3 = \gamma_e^2 - \gamma_e = -I$: as a map, γ_e has order 3. It is a hyperbolic rotation about τ_e by $2\pi/3$. A point with a nontrivial stabilizer is called *elliptic*. Numerically, $\gamma_e\tau_e - \tau_e = O(10^{-41})$; multiplying out, $\gamma_e^2 = \left(\begin{smallmatrix} 1 & -1 \\ 3 & -2 \end{smallmatrix}\right)$, $\gamma_e^3 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\gamma_e^3\tau = \tau$ at a generic point. In Figure 16.1 the interior angles of $\mathcal{F}_3$ at τ_e and at $\tau_e - 1$ are each $\pi/3$ (the vertical line and the arc $\left|\tau - \frac{1}{3}\right| = \frac{1}{3}$, whose radius at τ_e points in the direction $60°$, meet at $60°$), and gluing the two corners gives a cone of total angle $2\pi/3$, as it must around a point fixed by a rotation of order 3.

$\Gamma_0(3)$ has no elliptic point of order 2: such a point would be fixed by an element of trace 0, $\left(\begin{smallmatrix} a & b \\ 3c & -a \end{smallmatrix}\right)$, with determinant $-a^2 - 3bc = 1$, so $a^2 \equiv -1 \pmod 3$, which has no solution. It has exactly one orbit of elliptic points of order 3, that of τ_e [14]; we found it explicitly.

A sphere. After gluing, the compactified quotient $X_0(3)$ (cusps added) is a closed surface. We count its cells: the vertices are the cusp ∞, the cusp 0 and the glued corner $\{\tau_e - 1, \tau_e\}$, so $V = 3$; the edges are the glued pair of vertical sides and the glued pair of arcs, $E = 2$; there is one face, $F = 1$. The Euler characteristic is $V - E + F = 2$, so $X_0(3)$ is a sphere: genus 0. The same follows from the genus formula $g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2} = 1 + \frac{4}{12} - 0 - \frac{1}{3} - \frac{2}{2} = 0$ with index $\mu = 4$, $\nu_2 = 0$, $\nu_3 = 1$ elliptic points and $\nu_\infty = 2$ cusps [14].

Lemma 16.5 (the curve; [note, Lemma F.5(a)], first sentence)**.** *$\Gamma_0(3)$ has genus 0, two cusps ∞ and 0, and one elliptic point, of order 3, the orbit of $\tau_e = \frac{1}{2} + \frac{i}{2\sqrt{3}}$ [14].*

Intuition: what the points of $X_0(3)$ are. A point τ of $\mathbb{H}$ defines the torus $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$, an elliptic curve E; two values of τ give the same torus exactly when they differ by an element of $\mathrm{SL}_2(\mathbb{Z})$. So $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is the space of tori, the moduli space familiar from one-loop string amplitudes. A point of $\Gamma_0(3)\backslash\mathbb{H}$ is a torus together with a cyclic subgroup C of order 3 (for instance the one generated by $\frac{1}{3}$); there are four such subgroups, matching the index 4 [14]. The pair (E, C) returns in the 3-adic part of Chapter 17.

16.2 q-expansions and modular forms

A function f on $\mathbb{H}$ with $f(\tau+1) = f(\tau)$ is a function of $q = e^{2\pi i\tau}$, because $\tau \mapsto q$ identifies the strip $0 \le \operatorname{Re}\tau < 1$ with the punctured unit disc. $|q| = e^{-2\pi \operatorname{Im}\tau}$, so the cusp ∞ ($\operatorname{Im}\tau \to \infty$) is $q = 0$, and if f is holomorphic it has a Laurent expansion $f = \sum_n a_n q^n$, its *q-expansion*. These expansions converge fast in the part of $\mathbb{H}$ that matters: at the elliptic point $|q(\tau_e)| = e^{-\pi/\sqrt{3}} = 0.16303$ ($q(\tau_e)$ is real and negative). The derivative in τ is, up to a constant, the Euler operator in q:

$$\theta = q\frac{\mathrm{d}}{\mathrm{d}q} = \frac{1}{2\pi i}\frac{\mathrm{d}}{\mathrm{d}\tau}\,, \qquad \theta\sum_n a_n q^n = \sum_n n a_n q^n\,. \tag{16.3}$$

Definition 16.6 (modular forms and functions on $\Gamma_0(3)$)**.** Let $k \in \mathbb{Z}$. A *modular form of weight* k on $\Gamma_0(3)$ is a holomorphic function f on $\mathbb{H}$ with

$$f(\gamma\tau) = (c\tau + d)^k f(\tau) \qquad \text{for all } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(3)\ , \tag{16.4}$$

which is holomorphic at the two cusps: its q-expansion has no negative powers of q, and the same holds at the cusp 0 after moving 0 to ∞ (we do this with the Fricke map in Section 16.4.2). A *modular function* is a meromorphic function with $f(\gamma\tau) = f(\tau)$ (weight 0), meromorphic also at the cusps (finitely many negative powers of q).

For $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ the factor in (16.4) is 1, so every such f has a q-expansion. For $-I$ the factor is $(-1)^k$, so nonzero forms of odd weight do not exist on $\Gamma_0(3)$; all our weights are even.

Intuition: a primary field, and a section of a line bundle. By (16.1), $\mathrm{d}(\gamma\tau) = (c\tau + d)^{-2}\mathrm{d}\tau$. So (16.4) says exactly that $f(\tau)\,(\mathrm{d}\tau)^{k/2}$ is *invariant*: a weight-k form transforms like a holomorphic primary field of conformal weight $h = k/2$ under the Moebius maps in $\Gamma_0(3)$, and geometrically it is a section of the $k/2$-th power of the bundle of differentials on $X_0(3)$ (with extra care at cusps and elliptic points). A weight-0 form is a function on $X_0(3)$. The ratio of two forms of weight k is a modular function, and the product of forms of weights k and k' has weight $k + k'$; the note uses this when it multiplies an object of weight -4 by B^2, of weight 4, to obtain a function. Where the analogy stops: covariance is required only for the discrete group $\Gamma_0(3)$, not for all Moebius maps (covariance under all real Moebius maps would force $f = 0$ for $k \neq 0$, because the rotations about a point τ_0 multiply $f(\tau_0)$ by a nonconstant phase, and f constant for $k = 0$); the condition at the cusps has no counterpart for primary fields; and what makes modular forms useful in number theory, the arithmetic of their q-coefficients (integers, divisor sums, congruences), has no analogue in conformal field theory.

16.3 The Dedekind eta function

Definition 16.7 (Dedekind η)**.** $\eta(\tau) = q^{1/24}\prod_{n\geq 1}(1 - q^n)$, with $q^{1/24} = e^{2\pi i\tau/24}$.

The product converges for $|q| < 1$ and has no zeros there, so η is holomorphic and nonvanishing on $\mathbb{H}$. Obviously from the definition, $\eta(\tau + 1) = e^{2\pi i/24}\eta(\tau)$. The deep property is the behaviour under S:

Theorem 16.8 ([2, Theorem 3.1])**.** $\eta(-1/\tau) = \sqrt{\tau/i}\,\eta(\tau)$ *for* $\tau \in \mathbb{H}$*, with the branch of the square root that is positive for* $\tau \in i\mathbb{R}_{>0}$*.*

Intuition: the free boson. $1/\eta(\tau)$ is the partition function of the oscillators of one chiral free boson on a circle of length 2π at inverse temperature $2\pi\,\mathrm{Im}\,\tau$: $\prod_n(1 - q^n)^{-1}$ counts the oscillator states and $q^{-1/24}$ is the Casimir energy $-c/24$ with $c = 1$. The torus with modulus τ and the torus with modulus $-1/\tau$ are the same torus with space and time exchanged, which is why the partition function can change only by a simple factor; in the partition function $1/(\sqrt{\mathrm{Im}\,\tau}\,|\eta(\tau)|^2)$ of the full non-chiral, non-compact boson, the factor $\sqrt{\mathrm{Im}\,\tau}$ from the zero-mode integral exactly compensates $\left|\sqrt{\tau/i}\right|$ (since $\mathrm{Im}(-1/\tau) = \mathrm{Im}\,\tau/|\tau|^2$), making it invariant. This is the physicist's reason; the proof in [2] is a contour-integral argument.

Example 16.9 (checking Theorem 16.8)**.** At $\tau = 0.3 + 0.8\,i$ a 40-digit evaluation gives $\eta(-1/\tau) = 0.746934157680233 - 0.0802643491900496\,i$ and the same value for $\sqrt{\tau/i}\,\eta(\tau)$, in agreement to the working precision of 40 digits; likewise at $\tau = -0.12 + 0.45\,i$. Likewise $\eta(\tau + 1)/\eta(\tau) = e^{2\pi i/24} = 0.965925826289068 + 0.258819045102521\,i$.

16.4 The coordinate x on $X_0(3)$

16.4.1 Definition and q-expansion

Since $X_0(3)$ is a sphere, it has a global coordinate, as the Riemann sphere has the coordinate z: a function with exactly one simple pole, which then takes every value exactly once. That every compact Riemann surface of genus 0 is isomorphic to the Riemann sphere is a standard consequence of the Riemann–Roch theorem (e.g. Forster, *Lectures on Riemann Surfaces*). Such a coordinate is unique up to a Moebius map of the sphere; it is fixed by asking for a zero at the cusp ∞, a pole at the cusp 0, and $x = q + O(q^2)$. A coordinate of this kind on a genus-0 quotient is called a *Hauptmodul*. For $\Gamma_0(3)$ it has a closed form [note, (F.1)]:

$$x(\tau) = \left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12} = q\prod_{n\geq 1}\frac{(1-q^{3n})^{12}}{(1-q^n)^{12}}\ . \tag{16.5}$$

The factor q comes from $(q^{3/24}/q^{1/24})^{12} = q$.

Example 16.10 (the q-expansion of x)**.** Multiplying out the product,

$$x = q+12q^2+90q^3+508q^4+2391q^5+9828q^6+36428q^7+124188q^8+395199q^9+1186344q^{10}+\dots,$$

all coefficients through q^{25} are integers, as the note states in general: $x \in q + q^2\mathbb{Z}[[q]]$. The inverse series, q as a function of x, is $q(x) = x-12x^2+198x^3-3748x^4+76629x^5-1646064x^6+\dots$, again in $x + x^2\mathbb{Z}[[x]]$. At $\tau = 0.05 + 0.9\,i$ the eta product and the q-series truncated after 25 terms both give $x = 0.00345036359210233 + 0.00117131817086523\,i$.

16.4.2 The Fricke relation and the invariance of x

Lemma 16.11 (Fricke relation; [note, Lemma F.5(b)])**.** $x(-1/(3\tau)) = 3^{-6}/x(\tau)$.

Proof. Put $\tau' = -1/(3\tau)$. Then $3\tau' = -1/\tau$, and $\tau' = -1/(3\tau)$ is $-1/\sigma$ with $\sigma = 3\tau$. By Theorem 16.8, $\eta(3\tau') = \eta(-1/\tau) = \sqrt{\tau/i}\,\eta(\tau)$ and $\eta(\tau') = \eta(-1/\sigma) = \sqrt{3\tau/i}\,\eta(3\tau)$. Dividing, $\eta(3\tau')/\eta(\tau') = 3^{-1/2}\eta(\tau)/\eta(3\tau)$, and the twelfth power gives $x(\tau') = 3^{-6}/x(\tau)$. □

The map $W : \tau \mapsto -1/(3\tau)$ is the *Fricke involution*; $W(W\tau) = \tau$. Its matrix $\left(\begin{smallmatrix}0 & -1\\ 3 & 0\end{smallmatrix}\right)$ has determinant 3, so $W \notin \mathrm{SL}_2(\mathbb{Z})$, but it normalizes $\Gamma_0(3)$: a direct multiplication gives $W\left(\begin{smallmatrix}a & b\\ 3c & d\end{smallmatrix}\right)W^{-1} = \left(\begin{smallmatrix}d & -c\\ -3b & a\end{smallmatrix}\right) \in \Gamma_0(3)$. So W acts on $X_0(3)$, and by Lemma 16.11 it acts on the coordinate as $x \mapsto 3^{-6}/x$. It exchanges the cusps ($W\infty = 0$), so x has a simple pole at the cusp 0 because it has a simple zero at ∞. Its fixed points on the sphere are $x^2 = 3^{-6}$, i.e. $x = \pm\frac{1}{27}$. On $\mathbb{H}$, W fixes $\tau = i/\sqrt{3}$ (since $-1/(3\cdot i/\sqrt{3}) = i/\sqrt{3}$), where $q = e^{-2\pi/\sqrt{3}}$ is real and positive and so is the product (16.5); hence $x(i/\sqrt{3}) = +\frac{1}{27}$. The other fixed point $-\frac{1}{27}$ will turn out to be the elliptic point: indeed $W\tau_e = -1/(3\tau_e) = -\frac{1}{\sqrt{3}}e^{-i\pi/6} = -\frac{1}{2} + \frac{i}{2\sqrt{3}} = \tau_e - 1$, which is τ_e moved by T^{-1}.

Example 16.12 (Fricke and invariance, numerically)**.** At $\tau = 0.1 + 0.6\,i$ and at $\tau = 0.4 + 0.3\,i$ a numerical evaluation gives $x(-1/(3\tau))\,x(\tau) = 0.0013717421124828532236$ (imaginary part $< 10^{-43}$), which is 3^{-6} to all printed digits. Also $x(i/\sqrt{3}) = 0.037037037037037037 = \frac{1}{27}$. At $\tau = 0.1+0.6\,i$, $x(\gamma\tau)-x(\tau)$ is of size 10^{-42} for $\gamma = T$, $A = \left(\begin{smallmatrix}1 & 0\\ 3 & 1\end{smallmatrix}\right)$ and γ_e, but $x(S\tau)-x(\tau) = -0.0202 - 0.0208\,i$: x is invariant under $\Gamma_0(3)$ and not under $\mathrm{SL}_2(\mathbb{Z})$.

Why is x invariant under $\Gamma_0(3)$? The note takes this from [7, Section 3]. Here is an elementary route, granting one fact for which we give no reference: $\Gamma_0(3)$ is generated by T, $A = \left(\begin{smallmatrix}1 & 0\\ 3 & 1\end{smallmatrix}\right)$ and $-I$, the side pairings of Figure 16.1 (this is the analogue of Fact 16.1(a) and follows from Poincaré's theorem on side pairings of a fundamental polygon). Invariance

under T is clear, since x is a power series in q. For A, a one-line computation gives $W(A\tau) = -\frac{3\tau+1}{3\tau} = W\tau - 1$. So, using Lemma 16.11 twice and T-invariance,

$$x(A\tau) = \frac{3^{-6}}{x(W(A\tau))} = \frac{3^{-6}}{x(W\tau - 1)} = \frac{3^{-6}}{x(W\tau)} = x(\tau)\ .$$

For example $\gamma_e = -TA^{-1}$ (indeed $TA^{-1} = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\-3&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}-2&1\\-3&1\end{smallmatrix}\right)$).

16.4.3 The sphere in the coordinate x

Lemma 16.13 ([note, Lemma F.5(a)], second sentence)**.** *The function x is $\Gamma_0(3)$-invariant, holomorphic and nonvanishing on $\mathbb{H}$, has a simple zero at the cusp ∞ and a simple pole at the cusp 0, and identifies $X_0(3)$ with the Riemann sphere $\mathbb{P}^1$ [7, Section 3].*

The note's argument: $\Delta = \eta^{24}$, so $x = (\Delta(3\tau)/\Delta(\tau))^{1/2}$ is Calegari's Hauptmodul; x is holomorphic and nonzero on $\mathbb{H}$ because η is; the simple zero at ∞ is read off from $x = q + \dots$, and the simple pole at 0 follows from the Fricke relation. That a function on the sphere with a single simple pole is a coordinate is the Riemann sphere fact above.

Example 16.14 (how x wraps $\mathcal{F}_3$ around the sphere)**.** x is real on the whole boundary of $\mathcal{F}_3$ and on the imaginary axis, and the right half of $\mathcal{F}_3$ is mapped onto the upper half x-plane, the left half onto the lower half. Numerically:

imaginary axis, $\tau = it$: t	1.2	0.8	0.57735	0.3	0.15
x	0.000535	0.00710	0.037037	1.4601	1589.1
right side, $\tau = \frac{1}{2} + it$: t	1.2	0.8	0.5	0.35	0.2887
x	−0.000528	−0.00607	−0.0266	−0.03648	−0.037037
right arc, angle at $\frac{1}{3}$	70°	100°	150°		
x	−0.03761	−0.07625	−169.53		

(imaginary parts below 10^{-37}), and $\operatorname{Im} x = +0.06628$ at $\tau = 0.2 + 0.35\,i$, -0.06628 at $\tau = -0.2 + 0.35\,i$. Walking around the right half of $\mathcal{F}_3$, from ∞ down the imaginary axis to 0 (x runs from 0 through $\frac{1}{27}$ to $+\infty$), up the arc from 0 to τ_e (x runs from $-\infty$ to $-\frac{1}{27}$), and up the side from τ_e to ∞ (x runs from $-\frac{1}{27}$ to 0), x runs once along the real line. The right half is a hyperbolic triangle with angles $0, 0, \frac{\pi}{3}$, and x maps it conformally onto a half plane, like a Schwarz triangle map.

Near the elliptic point the map $\tau \mapsto x$ is 3-to-1: a small disc around τ_e contains three copies of each nearby orbit (related by the rotation γ_e), and all three have the same x. So $x - x(\tau_e)$ vanishes to order 3 in $\tau - \tau_e$. Numerically, with $x_e = -\frac{1}{27}$ (Lemma 16.16 below), one finds $(x(\tau_e + h) - x_e)/h^3 = -0.0172 + 3.30905\,i$ for $h = 10^{-3}$ and $-0.00172 + 3.309105\,i$ for $h = 10^{-4}$: a finite nonzero limit $\approx 3.3091\,i$, while the same difference divided by h^2 tends to 0. At every other point of $\mathbb{H}$, x is a local coordinate.

16.5 The j-function and Lemma F.5(c)

Definition 16.15 (Eisenstein series, Δ, j)**.** $\sigma_k(n) = \sum_{a|n} a^k$. $E_4 = 1 + 240\sum_{n\ge1}\sigma_3(n)q^n$ and $E_6 = 1 - 504\sum_{n\ge1}\sigma_5(n)q^n$ are modular forms of weight 4 and 6 on $\mathrm{SL}_2(\mathbb{Z})$, $\Delta = \eta^{24} = q\prod(1-q^n)^{24}$ is one of weight 12, and $j = E_4^3/\Delta$ is a modular function on $\mathrm{SL}_2(\mathbb{Z})$ with a simple pole at ∞ and no other pole; it is the Hauptmodul of $\mathrm{SL}_2(\mathbb{Z})$, and $j(\rho) = 0$ for $\rho = e^{2\pi i/3}$, with a zero of order 3 in $\tau - \rho$ [2, Ch. 1–2].

Expanding, $j = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$.

Lemma 16.16 ([note, Lemma F.5(c)]). *$j = \dfrac{(1+27x)(1+243x)^3}{x}$, and $x(\tau_e) = x_e = -\frac{1}{27}$.*

The note's argument, step by step. (1) j is invariant under $\mathrm{SL}_2(\mathbb{Z})$, hence under $\Gamma_0(3)$, and holomorphic on $\mathbb{H}$. So it is a meromorphic function on the sphere $X_0(3)$, and every meromorphic function on the Riemann sphere is a rational function of the coordinate. So j is a rational function of x, with poles only at the cusps, i.e. at $x = 0$ and $x = \infty$.

(2) At the cusp ∞: $j = q^{-1} + O(1)$ and $x = q + O(q^2)$, so j has a simple pole at $x = 0$.

(3) At the cusp 0: move it to ∞ with W. $j(W\tau) = j(-1/(3\tau)) = j(3\tau)$ (invariance under S, applied to 3τ), which is $q^{-3} + O(1)$, while $x(W\tau) = 3^{-6}q^{-1} + O(1)$ by Lemma 16.11. So $j \sim 3^{18}x^3$ near $x = \infty$: a pole of order 3.

(4) Hence $j = c/x +$ (polynomial of degree ≤ 3), and xj is a polynomial of degree at most 4, determined by its first five Taylor coefficients at $x = 0$. These come from the q-expansions: compute xj as a q-series and substitute $q = q(x)$.

(5) The fiber over $j = 0$: by (4), $xj = (1+27x)(1+243x)^3$ vanishes at $x = -\frac{1}{243}$ to order 3 and at $x = -\frac{1}{27}$ to order 1. Every τ_0 with $j(\tau_0) = 0$ is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to ρ, so j vanishes to order 3 in $\tau - \tau_0$ (as it does at ρ). If τ_0 is not elliptic for $\Gamma_0(3)$, x is a local coordinate there, $x - x(\tau_0)$ vanishes to order 1 in $\tau - \tau_0$, and j vanishes to order 3 in $x - x(\tau_0)$. If τ_0 is elliptic for $\Gamma_0(3)$, $x - x(\tau_0)$ vanishes to order 3 in $\tau - \tau_0$, and j vanishes to order $3/3 = 1$ in $x - x(\tau_0)$. So the simple root $-\frac{1}{27}$ is the image of the elliptic point: $x(\tau_e) = -\frac{1}{27}$, and $-\frac{1}{243}$ is the image of the non-elliptic points over $j = 0$ (for example ρ itself, which is not fixed by any element of $\Gamma_0(3)$ of order 3; numerically, $x(\rho) = -0.004115226337448559670\,8 = -\frac{1}{243}$ to 20 digits). □

Example 16.17 (checking Lemma 16.16)**.** By hand, the first two coefficients: $xj = (q + 12q^2 + \dots)(q^{-1} + 744 + \dots) = 1 + 756q + \cdots = 1 + 756x + \dots$, and $(1+27x)(1+243x)^3 = 1 + (27 + 3\cdot 243)x + \cdots = 1 + 756x + \dots$. Computing $xj = E_4^3 \prod (1-q^{3n})^{12}(1-q^n)^{-36}$ as a q-series and composing with $q(x)$ gives

$$xj = 1 + 756x + 196830x^2 + 19131876x^3 + 387420489x^4 + 0\cdot x^5 + \cdots + 0\cdot x^{15} \ ,$$

which is the expansion of $(1+27x)(1+243x)^3$; the vanishing of the coefficients of $x^5, \dots, x^{15}$ is a consistency check of step (4). Conversely, $xj - (1+27x)(1+243x)^3$ with $x = x(q)$ vanishes to q^{20}. The identity also holds far outside the disc of convergence of the x-series: at $\tau = 0.3\,i$, where $x = 1.4601$, both sides equal 1246931562.71795. At the special points: $x(\tau_e) = -0.037037037037037037037$ and $j(\tau_e) = O(10^{-118})$; at the Fricke point, $j(i/\sqrt{3}) = 54000.0$ (to 20 digits), which is $(1+1)(1+9)^3 \cdot 27 = 54000$ from the formula with $x = \frac{1}{27}$.

16.6 The weight-2 form B

16.6.1 Definition and q-expansion

The note's notation paragraph [note, (F.2)] defines, with $\sigma_k^{(3)}(n) = \sum_{a \mid n,\, 3\nmid a} a^k$,

$$B = \theta \log x = \frac{\theta x}{x} = 1 + 12 \sum_{n \ge 1} \sigma_1^{(3)}(n) q^n \ . \tag{16.6}$$

Derivation of the series. $\log x = \log q + 12 \sum_{n\ge1} \big(\log(1-q^{3n}) - \log(1-q^n)\big)$. Apply $\theta = q\,\mathrm{d}/\mathrm{d}q$: $\theta \log q = 1$ and $\theta \log(1-q^n) = -nq^n/(1-q^n) = -\sum_{k\ge1} nq^{nk}$. Collecting the coefficient of q^m: $\sum_n \frac{nq^n}{1-q^n} = \sum_m \sigma_1(m) q^m$ and $\sum_n \frac{3nq^{3n}}{1-q^{3n}} = \sum_m 3\sigma_1(m/3) q^m$ (zero unless $3 \mid m$). So $B = 1 + 12\sum_m (\sigma_1(m) - 3\sigma_1(m/3)) q^m$, and $\sigma_1(m) - 3\sigma_1(m/3) = \sigma_1^{(3)}(m)$, since the divisors of m divisible by 3 are $3b$ with $b \mid m/3$, and they sum to $3\sigma_1(m/3)$. □

Example 16.18. $B = 1 + 12q + 36q^2 + 12q^3 + 84q^4 + 72q^5 + 36q^6 + 96q^7 + 180q^8 + 12q^9 + \dots$ For instance $\sigma_1^{(3)}(2) = 1 + 2 = 3$ gives 36, and $\sigma_1^{(3)}(3) = 1$ (the divisor 3 is excluded) gives 12. Through q^{24}, (16.6) agrees with $\theta x/x$ computed from the eta product. Two further identities hold to q^{25} (not used by the note): $B = \frac{1}{2}(3E_2(3\tau) - E_2(\tau))$ with $E_2 = 1 - 24\sum \sigma_1(n)q^n$, and $B = a(q)^2$ with the theta series of the hexagonal lattice, $a(q) = \sum_{m,n\in\mathbb{Z}} q^{m^2+mn+n^2} = 1 + 6q + 6q^3 + 6q^4 + 12q^7 + \dots$, a modular form of weight 1. We do not prove these two identities here and use them only in Remark 16.30.

16.6.2 Weight 2 and Lemma F.6

Lemma 16.19 ([note, Lemma F.6])**.** *B is a holomorphic modular form of weight 2 on $\Gamma_0(3)$ with $B(-1/(3\tau)) = -3\tau^2 B(\tau)$. It does not vanish at the two cusps, and its zeros in $\mathbb{H}$ are exactly the orbit of τ_e, each of order 2 in $\tau - \tau_e$.*

The note's argument, step by step. (1) *Weight* 2. By (16.3), $B = (2\pi i)^{-1}x'(\tau)/x(\tau)$. Differentiate $x(\gamma\tau) = x(\tau)$ with the chain rule and (16.1): $x'(\gamma\tau)(c\tau + d)^{-2} = x'(\tau)$. Dividing by $x(\gamma\tau) = x(\tau)$ gives $B(\gamma\tau) = (c\tau + d)^2 B(\tau)$. The derivative of an invariant function has weight 2, because $\mathrm{d}\tau$ has weight -2.

(2) *Fricke.* Take logarithms in Lemma 16.11: $\log x(W\tau) = -\log x(\tau) - 6\log 3$. Differentiate, using $\frac{\mathrm{d}}{\mathrm{d}\tau}(-\frac{1}{3\tau}) = \frac{1}{3\tau^2}$: $\frac{x'(W\tau)}{x(W\tau)} \cdot \frac{1}{3\tau^2} = -\frac{x'(\tau)}{x(\tau)}$, i.e. $B(W\tau) = -3\tau^2 B(\tau)$.

(3) *Cusps.* $B = 1 + O(q)$ at ∞. At the cusp 0, by (2), $B(W\tau)/(-3\tau^2) = B(\tau) \to 1$ as $\tau \to i\infty$: after the weight factor is removed, B tends to 1 there too.

(4) *Zeros.* $x \neq 0$ on $\mathbb{H}$, so $B = 0$ exactly where $x' = 0$. At a non-elliptic point x is a local coordinate, so $x' \neq 0$. At a point of the orbit of τ_e, $x - x_e$ vanishes to order 3 (Section 16.4), so x' vanishes to order exactly 2. □

Example 16.20 (checking Lemma 16.19)**.** At $\tau = 0.1 + 0.6\,i$: $B(A\tau) = -2.75287484943888 + 5.47432582171538\,i = (3\tau+1)^2 B(\tau)$; the same agreement for γ_e; $B(W\tau) = 1.35629073327554 - 0.252668662496537\,i = -3\tau^2 B(\tau)$; but $B(S\tau) = 0.99994 - 0.00045\,i \neq \tau^2 B(\tau) = -0.452 + 0.084\,i$, so B is not a form on $\mathrm{SL}_2(\mathbb{Z})$. At the elliptic point, $B(\tau_e) = O(10^{-41})$ and $\theta B(\tau_e) = O(10^{-42})$, while $\theta^2 B(\tau_e) = 2.161155826$. So the zero is double, and $B(\tau_e + h) \approx \frac{1}{2}(2\pi i)^2\theta^2 B(\tau_e)h^2 = -42.6595\,h^2$; directly, $B(\tau_e + h)/h^2 = -42.6582$ for $h = 10^{-3}$ and -42.65949 for $h = 10^{-4}$.

16.6.3 The operators D and θ, and the logarithmic derivative u

The note works with series in x rather than in q, with the Euler operator $D = x\,\mathrm{d}/\mathrm{d}x$. On a function of τ, the chain rule gives $\theta f = (\theta x)\frac{\mathrm{d}f}{\mathrm{d}x} = xB\frac{\mathrm{d}f}{\mathrm{d}x}$, that is,

$$\theta = B\,D\ , \qquad D = B^{-1}\theta = \frac{1}{2\pi i B}\frac{\mathrm{d}}{\mathrm{d}\tau}\ , \qquad D\tau = \frac{1}{2\pi i B}\ . \tag{16.7}$$

D is singular where $B = 0$, i.e. at the elliptic points, where x is not a coordinate. We write B also for the series $B(q(x)) \in 1 + x\mathbb{Z}[[x]]$, and put

$$u = \frac{DB}{B} \in x\mathbb{Z}[[x]]\ , \qquad P = 1 + 27x\ , \qquad x_e = -\frac{1}{27}\ . \tag{16.8}$$

Note $P(x_e) = 0$: the polynomial P marks the elliptic point.

As series in x, $B(q(x)) = 1 + 12x - 108x^2 + 1524x^3 - 25884x^4 + \dots$, $u = 12x - 360x^2 + 10188x^3 - 282960x^4 + \dots$ (integer coefficients to x^{25}), and $\theta x = xB$ holds as q-series.

16.7 Eisenstein series, G_5 and Eichler integrals

16.7.1 A weight-6 form on $\Gamma_0(3)$

The note defines [note, (F.2)]

$$G_5(q) = \sum_{3\nmid a} \frac{q^a}{a^5(1-q^a)} = \sum_{n\geq 1} \sigma_{-5}^{(3)}(n) q^n \ . \tag{16.9}$$

The two forms agree because $\frac{q^a}{1-q^a} = \sum_{k\geq 1} q^{ak}$, so the coefficient of q^n is $\sum_{a|n,\,3\nmid a} a^{-5}$.

Proposition 16.21 (from the proof of [note, Lemma F.7]). *$\theta^5 G_5 = \sum_{n\geq 1}(\sigma_5(n) - \sigma_5(n/3))q^n = \frac{1}{504}(E_6(3\tau) - E_6(\tau))$, a holomorphic modular form of weight 6 on $\Gamma_0(3)$.*

Proof. θ^5 multiplies the coefficient of q^n by n^5: $n^5 \sum_{a|n,3\nmid a} a^{-5} = \sum_{a|n,3\nmid a}(n/a)^5$. Substituting $b = n/a$, this is the sum of b^5 over divisors b of n with $3 \nmid n/b$, i.e. $\sigma_5(n)$ minus the sum over the b with $3 \mid n/b$, i.e. with $b \mid n/3$, which is $\sigma_5(n/3)$. On the other side, $E_6(3\tau) - E_6(\tau) = -504\sum \sigma_5(n/3)q^n + 504\sum \sigma_5(n)q^n$. Modularity: E_6 has weight 6 on $\mathrm{SL}_2(\mathbb{Z}) \supset \Gamma_0(3)$; for $E_6(3\tau)$ and $\gamma = \left(\begin{smallmatrix} a & b \\ 3c & d \end{smallmatrix}\right) \in \Gamma_0(3)$ write $3\gamma\tau = \frac{a(3\tau)+3b}{c(3\tau)+d} = \gamma'(3\tau)$ with $\gamma' = \left(\begin{smallmatrix} a & 3b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$; then $E_6(3\gamma\tau) = (c\cdot 3\tau + d)^6 E_6(3\tau)$, the factor required for weight 6 on $\Gamma_0(3)$. □

Example 16.22. $E_6 = 1 - 504q - 16632q^2 - 122976q^3 - 532728q^4 - \ldots$; $G_5 = q + \frac{33}{32}q^2 + q^3 + \frac{1057}{1024}q^4 + \frac{3126}{3125}q^5 + \frac{33}{32}q^6 + \ldots$; $\theta^5 G_5 = q + 33q^2 + 243q^3 + 1057q^4 + 3126q^5 + 8019q^6 + \ldots$ For $n = 3$: $\sigma_5(3) - \sigma_5(1) = 244 - 1 = 243$. Both equalities of Proposition 16.21 hold to q^{25}.

16.7.2 G_5 is an Eichler integral

G_5 is a fivefold antiderivative of the weight-6 form $f = \theta^5 G_5$: $\theta^5 G_5 = f$, and θ is $\frac{1}{2\pi i}\frac{\mathrm{d}}{\mathrm{d}\tau}$. An antiderivative is determined up to a constant; a fivefold antiderivative up to a polynomial of degree at most 4 in τ, because $\theta^5 p(\tau) = 0$ exactly for $p \in \mathrm{span}(1, \tau, \tau^2, \tau^3, \tau^4)$. The choice in (16.9) is the one with no constant term in q. Such an antiderivative of a modular form is called an *Eichler integral*. It is not modular, but it misses being modular of weight $2 - 6 = -4$ only by such polynomials. The reason is Bol's identity (L. Bol, 1949): for any holomorphic F and $\gamma \in \mathrm{SL}_2(\mathbb{R})$,

$$\frac{\mathrm{d}^5}{\mathrm{d}\tau^5}\Big((c\tau + d)^4 F(\gamma\tau)\Big) = (c\tau + d)^{-6} F^{(5)}(\gamma\tau) \ . \tag{16.10}$$

Apply it to $F = G_5$ and $\gamma \in \Gamma_0(3)$. The right side is $(2\pi i)^5 (c\tau + d)^{-6} f(\gamma\tau) = (2\pi i)^5 f(\tau) = G_5^{(5)}(\tau)$, by weight 6. So θ^5 kills the difference, and

$$(c\tau + d)^4 G_5(\gamma\tau) - G_5(\tau) = p_\gamma(\tau) \ , \qquad p_\gamma \text{ a polynomial of degree} \leq 4 \ . \tag{16.11}$$

p_γ is the *period polynomial* of γ; it measures how the Eichler integral changes under γ, as the periods of an abelian differential measure how its integral changes around closed loops, and its coefficients play the role of the "periods" of f.

Example 16.23 (the period polynomial of A). For $A = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)$ we evaluate $p_A(\tau) = (3\tau + 1)^4 G_5(A\tau) - G_5(\tau)$ from the q-series at seven points $\tau_k = -0.15 + 0.40\,i + (k + k^2 i)/50$, fit a polynomial of degree 4 through the first five values and predicts the other two: at $\tau = -0.05 + 0.9\,i$ the value is $12.5902102686 + 22.3530640287\,i$ and the fit gives the same twelve digits, at $\tau = -0.03 + 1.12\,i$ both are $16.4127668827 + 60.8433646032\,i$. The fitted coefficients of $\tau^0, \ldots, \tau^4$ are $2.42540\,i$, $-6.19596 + 14.55238\,i$, $-27.88184 + 38.61977\,i$, $-55.76367 + 50.37361\,i$, $-41.82275 + 22.66812\,i$: nonzero, so G_5 is not a modular form of weight -4. Under T, $G_5(\tau + 1) = G_5(\tau)$ (difference 10^{-42}).

Intuition: why the note wants $B^2(G_5+c)$. Multiply the "almost weight -4" object G_5+c by B^2, of weight 4. Then for $\gamma\in\Gamma_0(3)$, using (16.11),

$$B(\gamma\tau)^2\,(G_5(\gamma\tau)+c) = B(\tau)^2\left(G_5(\tau)+c+p_\gamma(\tau)+c((c_\gamma\tau+d_\gamma)^4-1)\right),$$

where c_γ, d_γ are the entries of γ. So the note's function $H_c = B^2(G_5+c)$ [note, (F.3)] is a function on the sphere *up to adding* B^2 times a polynomial of degree ≤ 4 in τ. Going around a loop on the sphere changes H_c by an element of the five-dimensional space spanned by $B^2, B^2\tau, \dots, B^2\tau^4$. An operator that kills this space turns H_c into an honest function of x; that operator is L_5 (Section 16.10), and the honest function is R_5.
The 3-adic counterpart, quoted in Chapter 17 [note, (F.21)]: with the specific constant $c=\eta_5=\zeta_3(5)/2$, $G_5+\eta_5$ is a genuine (3-adic, overconvergent) modular form of weight -4, and then H_{η_5} is a 3-adic function of x on a large disc.

16.8 Lemma F.7: two rational functions

Lemma 16.24 ([note, Lemma F.7])**.**

$$V := 2Du+u^2 = \frac{24x}{P^2}\,, \qquad R_5 := B^{-3}\theta^5 G_5 = \frac{x(1+39x)}{P^2}\,.$$

Example 16.25 (the identities as series and at points)**.** As series in x, from $q(x)$ and the q-series of B and $\theta^5 G_5$:

$$V = 24x - 1296x^2 + 52488x^3 - 1889568x^4 + 63772920x^5 - \dots,$$
$$R_5 = x - 15x^2 + 81x^3 + 6561x^4 - 413343x^5 + \dots,$$

and both identities hold exactly through x^{25}. (By hand: $P^{-2} = 1-54x+2187x^2-\dots$, so $24x/P^2 = 24x-1296x^2+52488x^3-\dots$, and the x^2-coefficient of $x(1+39x)/P^2$ is $39-54=-15$.) The x-series converge only for $|x|<\frac{1}{27}$, so we also test the identities at points of $\mathbb{H}$ through q-series, with $V = 2\theta^2 B/B^3 - 3(\theta B)^2/B^4$ (from $u=\theta B/B^2$ and $D=B^{-1}\theta$): at $\tau = 0.3\,i$ ($x=1.460061838$) $V = 0.0214463799154705$ and $R_5 = 0.0517772906017759$, equal to $24x/P^2$ and $x(1+39x)/P^2$ to 15 digits; at $\tau = 0.45+0.32\,i$, close to the elliptic point ($x=-0.03758+0.0002i$), $V = -2808.38771414781 - 2405.32440267853\,i$ and $R_5 = 55.2703850494574 + 45.7395111762197\,i$, again equal to the rational functions to 15 digits.

Intuition: V is a Schwarzian derivative. Write $t=\log x$, so $D=\mathrm{d}/\mathrm{d}t$, and regard τ as a (many-valued) function of t. By (16.7), $\tau_t = 1/(2\pi i B)$, so $u = D\log B = -\tau_{tt}/\tau_t$, and then

$$V = 2Du+u^2 = -2\left(\frac{\tau_{ttt}}{\tau_t} - \frac{3}{2}\frac{\tau_{tt}^2}{\tau_t^2}\right) = -2\{\tau,t\}\,,$$

with the Schwarzian derivative $\{\tau,t\}$ (by direct differentiation, for a generic function $\tau(t)$). The Schwarzian is the term that appears in the transformation law of a CFT stress tensor, and it is unchanged when τ is replaced by a Moebius map $\gamma\tau$, the reason why the stress tensor transforms as a primary under global conformal maps. Here this says: changing the branch of τ by $\gamma\in\Gamma_0(3)$ does not change V. So V is a function on the sphere. The first part of the proof below is exactly the check of this invariance.

The note's argument for V, step by step. (1) *u under $\Gamma_0(3)$.* Let $\gamma\in\Gamma_0(3)$ with entries c_γ, d_γ and $J = c_\gamma\tau + d_\gamma$. Since $x(\gamma\tau)=x(\tau)$, D commutes with $\tau\mapsto\gamma\tau$: $(Df)(\gamma\tau) = D(f(\gamma\tau))$.

With $B(\gamma\tau) = J^2 B$ and $DJ = c_\gamma D\tau = c_\gamma/(2\pi i B)$ (16.7),

$$u(\gamma\tau) = D\log\left(J^2 B\right) = u + 2\frac{DJ}{J} = u + \delta\ , \qquad \delta = \frac{2c_\gamma}{2\pi i B\, J}\ .$$

Numerically, at $\tau = 0.1 + 0.6\,i$ and $\gamma = A$: $u(A\tau) - u(\tau) = -0.307024591928619 - 0.15959464901546\,i = \delta$.

(2) *$D\delta$.* $D\log\delta = -D\log B - D\log J = -u - \frac{c_\gamma}{2\pi i B J} = -u - \frac{\delta}{2}$, so $D\delta = -u\delta - \frac{\delta^2}{2}$.

(3) *Invariance.* $V(\gamma\tau) = 2D(u+\delta) + (u+\delta)^2 = 2Du + u^2 + \left(2D\delta + 2u\delta + \delta^2\right) = V + \left(-2u\delta - \delta^2 + 2u\delta + \delta^2\right) = V$.

(4) *Fricke.* Under W, $x \mapsto 3^{-6}/x$, so $D = x\,\mathrm{d}/\mathrm{d}x$ becomes $-D$ (as $\log x \mapsto -\log x + \text{const}$). With $B(W\tau) = -3\tau^2 B(\tau)$ one finds in the same way $u(W\tau) = -u - \delta'$ with $\delta' = 2/(2\pi i\tau B)$ and $D\delta' = -u\delta' - \delta'^2/2$, and the same algebra as in (3) gives $V(W\tau) = V(\tau)$.

(5) *V is rational.* By (3), V is a meromorphic function on the sphere, hence a rational function of x. Where $B \neq 0$, it is holomorphic, since $u = (2\pi i)^{-1}B'/B^2$ is.

(6) *The pole at x_e.* Near τ_e, B vanishes to order 2, B' to order 1, so $u = (2\pi i)^{-1}B'/B^2$ has a pole of order $1 - 4 = 3$ in $\tau - \tau_e$. $D = (2\pi i B)^{-1}\mathrm{d}/\mathrm{d}\tau$ differentiates (one more order of pole) and divides by B (two more), so Du has a pole of order $3 + 1 + 2 = 6$, as has u^2. So V has order ≥ -6 in $\tau - \tau_e$; since $x - x_e$ vanishes to order 3 in $\tau - \tau_e$, this is order ≥ -2 in $x - x_e$.

(7) *The values at the cusps.* $u = 12x + O(x^2)$ has integer coefficients, so $V \in \mathbb{Z}[[x]]$ and $V(0) = 0$. By (4), $V(\infty) = V(0) = 0$.

(8) *Conclusion.* By (5) and (6), $P^2 V$ has no poles in $\mathbb{C}$, so it is a polynomial; since V is bounded at ∞ and $P^2 \sim 729x^2$, its degree is at most 2, with x^2-coefficient $729\,V(\infty) = 0$; and it vanishes at $x = 0$. So $P^2 V = \alpha x$, and $V = 24x + O(x^2)$ gives $\alpha = 24$. □

The note's argument for R_5, step by step. (1) $\theta^5 G_5$ has weight 6 (Proposition 16.21) and B^3 has weight 6, so R_5 has weight 0: an invariant, meromorphic function on the sphere, hence rational in x. Its only possible poles in $\mathbb{H}$ are at the zeros of B^3, of order 6 in $\tau - \tau_e$, i.e. order ≤ 2 in $x - x_e$.

(2) At $x = 0$: $R_5 = x + O(x^2)$ (Example 16.25).

(3) At $x = \infty$, i.e. the cusp 0: by Proposition 16.21,

$$\theta^5 G_5(W\tau) = \frac{1}{504}\left(E_6(-1/\tau) - E_6(-1/(3\tau))\right) = \frac{1}{504}\left(\tau^6 E_6(\tau) - (3\tau)^6 E_6(3\tau)\right)\ ,$$

using the weight 6 of E_6 under S. With $B(W\tau)^3 = -27\tau^6 B(\tau)^3$ (Lemma 16.19),

$$R_5(W\tau) = \frac{729E_6(3\tau) - E_6(\tau)}{13608\,B(\tau)^3} \xrightarrow{\tau\to i\infty} \frac{728}{13608} = \frac{13}{243}\ ,$$

since $E_6 \to 1$, $B \to 1$, and $728 = 8\cdot 7\cdot 13$, $13608 = 8\cdot 7\cdot 243$. So R_5 is not Fricke-invariant: it is 0 at one cusp and $\frac{13}{243}$ at the other.

(4) As before, $P^2 R_5$ is a polynomial of degree ≤ 2 vanishing at 0, with x-coefficient 1 by (2) and x^2-coefficient $729 \cdot \frac{13}{243} = 39$ by (3). So $P^2 R_5 = x + 39x^2$. □

Numerically, the formula of step (3) agrees with the direct evaluation of R_5 at $W\tau$ for $\tau = 0.1 + 0.6\,i$ (both $0.0258790437461 - 0.0116036432248\,i$), and at $\tau = 3i$ it gives 0.05349793, against $\frac{13}{243} = 0.05349794$.

What just happened. V and R_5 are functions of τ that turn out to be invariant under $\Gamma_0(3)$ (for V because it is a Schwarzian, for R_5 because it is a ratio of two forms of weight 6). Invariant functions are rational in the coordinate x. Their only possible pole in $\mathbb{H}$ is at the elliptic point, where B vanishes, and counting orders of vanishing in τ and converting with "order 3 in τ is order 1 in x" bounds that pole by 2. The values at the two cusps,

read from q-expansions (the second one after the Fricke involution), fix the remaining two or three coefficients. This invariance-plus-pole-counting argument is the standard way identities between modular objects are proved: no infinite computation is needed, only finitely many coefficients.

16.9 The recursion (F.8) and Lemma F.9

16.9.1 What the recursion computes

The goal of [note, Lemma F.10] is a differential operator in D that kills $B^2\tau^a$ for $a \le 4$. Since θ acts on q-series simply and kills τ^a when applied five times, the note rewrites $D^i(B^2Y)$, for any function Y of τ, in terms of $B^{2-m}\theta^m Y$. Take $i = 1$. With $DB = uB$ and $DY = B^{-1}\theta Y$ (16.7),

$$D(B^2Y) = 2B(DB)Y + B^2DY = B^2\Big(2u\,Y + B^{-1}\theta Y\Big)\ .$$

For the next step one needs Du. Here the Riccati form of Lemma 16.24 enters: $V = 2Du + u^2$ gives

$$Du = \frac{V - u^2}{2}\ , \tag{16.12}$$

so derivatives of u are polynomials in u with coefficients in $\mathbb{Q}(x)$, and the computation closes. The note formalizes this with an indeterminate u: on $\mathfrak{R} = \mathbb{Q}(x)[u]$ the derivation $\tilde{D}$ acts as $D = x\,\mathrm{d}/\mathrm{d}x$ on $\mathbb{Q}(x)$ and by $\tilde{D}u = (V - u^2)/2$. Then $N_{i,m} \in \mathfrak{R}$ are defined by $N_{0,0} = 1$ and [note, (F.8)]

$$N_{i+1,m} = (2-m)\,u\,N_{i,m} + \tilde{D}N_{i,m} + N_{i,m-1}\ , \qquad N_{i,m} = 0 \text{ unless } 0 \le m \le i\ . \tag{16.13}$$

Lemma 16.26 ([note, Lemma F.9])**.** *(a) For every holomorphic function Y of τ, $D^i(B^2Y) = B^2\sum_{m=0}^{i} N_{i,m}(u)\,B^{-m}\theta^m Y$, with $u = DB/B$. (b) If V is kept as a symbol on which $\tilde{D}$ acts as D, then $N_{i,m} \in \mathbb{Z}[\frac{1}{2}][u, V, DV, D^2V, \dots]$ is isobaric of weight $i - m$ (u of weight 1, D^jV of weight $2 + j$), and $N_{i,i} = 1$. (c) $\partial N_{i,m}/\partial u = c_m N_{i,m+1}$ with $c_m = (m+1)(4-m)/2$, i.e. $(c_0, \dots, c_4) = (2, 3, 3, 2, 0)$.*

The note's argument, step by step. (a) Induction on i. The inductive step is the product rule applied to one term:

$$D\Big(B^{2-m}\,\theta^m Y\,N\Big) = B^{2-m}\theta^m Y\,\big((2-m)uN + DN\big) + B^{1-m}\theta^{m+1}Y\,N\ ,$$

because $D(B^{2-m}) = (2-m)B^{2-m}u$ and $D(\theta^m Y) = B^{-1}\theta^{m+1}Y$. The first part goes into $N_{i+1,m}$, the second into $N_{i+1,m+1}$, which is (16.13). Computing with $\tilde{D}$ on the indeterminate u and then substituting $u = DB/B$ gives the same result as computing with the actual function, because the actual u satisfies (16.12): substitution is a homomorphism of differential rings.

(b) Each step of (16.13) raises the weight by one: $u\cdot$ adds 1; $\tilde{D}$ adds 1 (it sends u, of weight 1, to $(V - u^2)/2$, of weight 2, and D^jV to $D^{j+1}V$); the term $N_{i,m-1}$ has weight $i - (m-1) = (i+1) - m$. The only division is by 2 in $\tilde{D}u$. And $N_{i+1,i+1} = N_{i,i} = 1$.

(c) First a commutator: for $f \in \mathfrak{R}$, $\partial\tilde{D}f = \partial(xf_x + \frac{V-u^2}{2}f_u) = \tilde{D}\partial f - u\,\partial f$ (with $\partial = \partial/\partial u$; the extra term comes from differentiating $\frac{V-u^2}{2}$). Assume (c) at level i. Then, differentiating (16.13),

$$\partial N_{i+1,m} = (2-m)N_{i,m} + (2-m)u\,c_m N_{i,m+1} + \tilde{D}(c_m N_{i,m+1}) - u\,c_m N_{i,m+1} + c_{m-1}N_{i,m}\ ,$$

while by (16.13) at index $m+1$,

$$c_m N_{i+1,m+1} = c_m\Big((1-m)u\,N_{i,m+1} + \tilde{D}N_{i,m+1} + N_{i,m}\Big)\ .$$

The $uN_{i,m+1}$ terms agree ($(2-m)-1=1-m$), the $\tilde{D}$ terms agree, and the $N_{i,m}$ terms agree because $c_m - c_{m-1} = \frac{(m+1)(4-m)-m(5-m)}{2} = 2-m$, with $c_{-1}=0$. The case $i=0$ is trivial. □

Example 16.27 (the first $N_{i,m}$)**.** By hand from (16.13): $N_{1,0} = 2u\cdot 1 = 2u$, $N_{1,1}=1$; $N_{2,0} = 2u\cdot 2u + \tilde{D}(2u) = 4u^2 + (V-u^2) = 3u^2+V$; $N_{2,1} = (2-1)u\cdot 1 + \tilde{D}1 + N_{1,0} = u+0+2u = 3u$. Running the recursion symbolically, with $u, V, DV, D^2V, \dots$ as symbols, reproduces the note's printed list

$$N_{3,0} = 3u^3 + 5Vu + DV, \quad N_{3,1} = \tfrac{1}{2}(9u^2+5V), \quad N_{3,2} = 3u,$$
$$N_{4,0} = \tfrac{1}{2}(3u^4 + 24Vu^2 + 14\,DV\,u + 5V^2 + 2D^2V), \quad N_{4,1} = \tfrac{1}{2}(6u^3 + 24Vu + 7DV),$$
$$N_{4,2} = 3u^2 + 4V, \quad N_{4,3} = 2u,$$

all ten entries. The same computation confirms (b) and (c) for all $i \le 6$ (for $m \ge 5$ the formula for c_m gives negative values, and (c) still holds) and that all denominators are powers of 2, and it gives the row needed next:

$$N_{5,0} = \tfrac{1}{2}\Big(30Vu^3 + 34V^2u + 45\,DV\,u^2 + 18\,D^2V\,u + 17V\,DV + 2D^3V\Big),$$
$$N_{5,1} = \tfrac{1}{2}\Big(45Vu^2 + 17V^2 + 45\,DV\,u + 9D^2V\Big),$$
$$N_{5,2} = \tfrac{15}{2}(2Vu + DV), \quad N_{5,3} = 5V, \quad N_{5,4} = 0, \quad N_{5,5} = 1\ .$$

Finally, part (a) for $i=2$, $Y=G_5$ at $\tau = 0.15 + 0.5\,i$: numerical differentiation of B^2G_5 twice with $D = (2\pi i B)^{-1}\mathrm{d}/\mathrm{d}\tau$ gives $-0.0047607430564 + 0.144890440583\,i$, and $B^2\big((3u^2+V)Y + 3uB^{-1}\theta Y + B^{-2}\theta^2 Y\big)$ gives the same.

Intuition: the $\mathfrak{sl}_2$ and Sym^4 structure. This is our reading; the note states (c) without comment. The numbers $c_m = \frac{(m+1)(4-m)}{2}$ equal $\frac{1}{2}(j(j+1) - m'(m'+1))$ with $j=2$ and $m' = m-2$: they are one half of the squared matrix elements of the ladder operators $J_\pm$ in the spin-2 representation of $\mathfrak{sl}_2$, the five-dimensional representation, which is the fourth symmetric power Sym^4 of the two-dimensional one. That representation is visible in the solutions: $\Gamma_0(3)$ acts on $(\tau,1)$ by $\tau \mapsto \gamma\tau$, i.e. on the pair as a 2-dimensional representation, and on $B^2\tau^a$, $0\le a\le 4$, as on the monomials X^aY^{4-a} of degree 4 (continuation sends $B^2\tau^a$ to $B^2(a_\gamma\tau + b_\gamma)^a(c_\gamma\tau + d_\gamma)^{4-a}$). The vanishing $c_4 = 0$ is the top of the spin-2 multiplet: it is why the chain $N_{i,0}, N_{i,1}, \dots$ closes after five steps and why the operator of the next section has order exactly 5. Chapter 17 uses Sym^4 twice: for the irreducibility of L_5 [note, Lemma F.13] and in the congruences of [note, Proposition F.31].

16.10 Lemma F.10: the operator L_5

Lemma 16.28 ([note, Lemma F.10])**.** *Let $L_5 = D^5 + \mathfrak{a}_3D^3 + \mathfrak{a}_2D^2 + \mathfrak{a}_1D + \mathfrak{a}_0$ with [note, (F.11)]*

$$\mathfrak{a}_3 = -\frac{120x}{P^2}, \quad \mathfrak{a}_2 = \frac{180x(27x-1)}{P^3},$$
$$\mathfrak{a}_1 = -\frac{36x(2187x^2 - 388x + 3)}{P^4}, \quad \mathfrak{a}_0 = \frac{24x(27x-1)(729x^2 - 366x + 1)}{P^5}. \tag{16.14}$$

Then $L_5(B^2Y) = B^{-3}\theta^5 Y$ for every holomorphic Y of τ. Consequently $L_5H_c = R_5$ for every constant c, where $H_c = B^2(G_5 + c)$, and $L_5(B^2\tau^a) = 0$ for $0\le a\le 4$.

The note's argument, with the "direct computation" written out. By Lemma 16.26(a), with $\mathfrak{a}_5 = 1$ and $\mathfrak{a}_4 = 0$,

$$L_5(B^2Y) = B^2\sum_{m=0}^{5}\Big(\sum_{j=m}^{5}\mathfrak{a}_j N_{j,m}(u)\Big)B^{-m}\theta^m Y\ .$$

We want the inner sums to be 0 for $m \le 4$ and 1 for $m = 5$; then $L_5(B^2 Y) = B^{2-5}\theta^5 Y$. The conditions form a triangular system, solved from $m = 4$ downwards with $N_{m,m} = 1$ and the row $N_{5,m}$ of Example 16.27:

- $m = 5$: $N_{5,5} = 1$. $m = 4$: $N_{5,4} + \mathfrak{a}_4 = 0$, and $N_{5,4} = 0$, so $\mathfrak{a}_4 = 0$.
- $m = 3$: $N_{5,3} + \mathfrak{a}_3 = 0$, so $\mathfrak{a}_3 = -5V$.
- $m = 2$: $\mathfrak{a}_2 = -N_{5,2} - \mathfrak{a}_3 N_{3,2} = -\frac{15}{2}(2Vu + DV) + 5V \cdot 3u = -\frac{15}{2}DV$.
- $m = 1$: $\mathfrak{a}_1 = -N_{5,1} - \mathfrak{a}_3 N_{3,1} - \mathfrak{a}_2 N_{2,1} = \frac{1}{2}\big(-45Vu^2 - 17V^2 - 45DV\,u - 9D^2V + 45Vu^2 + 25V^2 + 45DV\,u\big) = 4V^2 - \frac{9}{2}D^2V$.
- $m = 0$: similarly, $\mathfrak{a}_0 = -N_{5,0} - \mathfrak{a}_3 N_{3,0} - \mathfrak{a}_2 N_{2,0} - \mathfrak{a}_1 N_{1,0} = 4V\,DV - D^3V$, where the terms in u^3, u^2, u cancel in pairs.

In every step u drops out. This is what makes L_5 an operator with coefficients in $\mathbb{Q}(x)$ rather than in $\mathbb{Q}(x)[u]$, and it is a consequence of Lemma 16.26(c): $\partial/\partial u$ of the inner sum at level m is c_m times the inner sum at level $m+1$, which vanishes. Now insert $V = 24x/P^2$: $DV = x\frac{\mathrm{d}}{\mathrm{d}x}\frac{24x}{(1+27x)^2} = \frac{24x(1-27x)}{P^3}$, so $\mathfrak{a}_2 = -\frac{15}{2}DV = \frac{180x(27x-1)}{P^3}$, and $\mathfrak{a}_3 = -5V = -\frac{120x}{P^2}$; $\mathfrak{a}_1$ and $\mathfrak{a}_0$ follow in the same way. Finally $L_5 H_c = B^{-3}\theta^5(G_5 + c) = B^{-3}\theta^5 G_5 = R_5$, and $L_5(B^2\tau^a) = B^{-3}\theta^5\tau^a = 0$ for $a \le 4$. □

Example 16.29 (checking Lemma 16.28)**.** (i) Solving the triangular system symbolically, with $V = 24x/P^2$ inserted from the start, one obtains $\mathfrak{a}_4 = 0$ and $\mathfrak{a}_3, \mathfrak{a}_2, \mathfrak{a}_1, \mathfrak{a}_0$ free of u and equal to the printed (16.14); with these, $\sum_j \mathfrak{a}_j N_{j,m} = 0, 0, 0, 0, 0, 1$ for $m = 0, \dots, 5$. This also confirms the forms $-5V$, $-\frac{15}{2}DV$, $4V^2 - \frac{9}{2}D^2V$, $4V\,DV - D^3V$ derived above. (ii) Series: with exact rational arithmetic, $P^5 L_5(B^2 G_5) = P^3 x(1 + 39x)$ and $P^5 L_5(B^2) = 0$ hold through x^{15}. Since $H_c = B^2 G_5 + cB^2$ and L_5 is linear, $L_5 H_c = R_5$ through x^{15} for every c, symbolic c included. (iii) The solutions: $\tau = \frac{\log q}{2\pi i}$ and $\log q = \log x + \log(q(x)/x)$, a formal $\log x$ (with $D \log x = 1$) plus a power series. One finds $P^5 L_5(B^2(\log q)^a) = 0$ through x^{15} for $a = 0, 1, 2, 3, 4$, while this fails for $a = 5$, as it must, since $\theta^5\tau^5 \neq 0$.

Remark 16.30 (L_5 is a symmetric fourth power). Again our addition, not used by the note. Let y satisfy the second-order equation $D^2 y = \frac{V}{4}y$. A symbolic computation, for an arbitrary V, shows that then $L_5(y^4) = 0$ with $\mathfrak{a}_3, \dots, \mathfrak{a}_0$ in the forms above. So L_5 is the fourth symmetric power of $D^2 - \frac{V}{4}$: its solutions are the degree-4 products of solutions of the second-order equation. The latter has the two solutions a and $a\tau$, where $a = \sqrt{B}$ is the weight-1 theta series of Example 16.18 ($(D^2 - \frac{V}{4})a(q(x)) = 0$ holds through x^{25}), and their fourth powers and products are $a^4\tau^k = B^2\tau^k$. A physicist may recognize the structure of a Picard–Fuchs equation, whose two solutions are periods and whose ratio, here τ, gives the coordinate $q = e^{2\pi i\tau}$ with integral expansion $x(q)$, as for mirror maps; we offer this only as an analogy.

Check yourself 16.31. Why does $\Gamma_0(3)$ have no elliptic point of order 2, while $\mathrm{SL}_2(\mathbb{Z})$ does (at $\tau = i$, fixed by S)?

Answer. An elliptic element of order 2 (as a map) has trace 0. In $\Gamma_0(3)$ it would be $\left(\begin{smallmatrix} a & b \\ 3c & -a \end{smallmatrix}\right)$ with $-a^2 - 3bc = 1$, i.e. $a^2 \equiv -1 \pmod 3$; the squares mod 3 are $0, 1$, so this is impossible. $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has trace 0 but lower left entry 1.

Check yourself 16.32. Use (16.6) and $x = q + 12q^2 + \dots$ to find the coefficient of x in $u = DB/B$.

Answer. $B = 1 + 12q + O(q^2) = 1 + 12x + O(x^2)$, so $DB = 12x + O(x^2)$ and $u = 12x + O(x^2)$: the coefficient is 12. Then $V = 2Du + u^2 = 24x + O(x^2)$, the constant 24 of Lemma 16.24.

16.11 How Chapter 17 uses these objects

The second proof works with the six *germs* [note, (F.3)]

$$g_0 = 1, \qquad g_i = D^{i-1}H_c \quad (1 \le i \le 5), \qquad H_c = B^2(G_5(q(x)) + c),$$

power series in x with rational coefficients for rational c. Lemma F.10 says that $Dg_5 = D^5H_c = R_5\,g_0 - \mathfrak{a}_0 g_1 - \mathfrak{a}_1 g_2 - \mathfrak{a}_2 g_3 - \mathfrak{a}_3 g_4$: the span of the germs over $\mathbb{Q}(x)$ is closed under D, a "differential module" of rank 6. In Chapter 17 this is used three ways. First, the germs are linearly independent over $\mathbb{C}(x)$ for every c [note, Lemmas F.12–F.13, Proposition F.14]; the proof uses that L_5 has no rational solution of $L_5 v = R_5$ (exploiting the poles of the coefficients (16.14) at $x = 0, x_e, \infty$) and that its monodromy, the action of $\Gamma_0(3)$ on $B^2\tau^a$, is Sym^4 of $\Gamma_0(3)$ and irreducible. Second, a zero estimate [note, Proposition F.15] and the determinant $\mathcal{D}_d$ [note, (F.18)], a $5d \times 5d$ determinant of Taylor coefficients of $x^k g_i$, whose size is then estimated at every place. Third, the three estimates: at 3, the germs with $c = \eta_5$ converge on the 3-adic disc $|x|_3 < 3^6$, which is where the overconvergence of $G_5 + \eta_5$ and the formula for j of Lemma 16.16 enter (the elliptic point $x_e = -\frac{1}{27}$ has $|x_e|_3 = 27$ and lies in the "supersingular annulus" $1 < |x|_3 < 3^6$ [note, Lemma F.19]); at primes $\ell \neq 3$, the quotient $E_{\ell-1}/B^{(\ell-1)/2}$, a rational function of x by the same invariance-and-poles argument as in Lemma 16.24, controls u modulo ℓ [note, Lemma F.27]; at the real place, the q-expansions are estimated on circles in the q-disc [note, Section F.5].

Summary of the chapter

We built the modular forms that [note, Appendix F] needs. The group $\Gamma_0(3)$ has index 4 in $\mathrm{SL}_2(\mathbb{Z})$; its fundamental domain $\mathcal{F}_3$ glues to a sphere $X_0(3)$ with two cusps (∞ and 0) and one elliptic point of order 3 ($\tau_e = \frac{1}{2} + \frac{i}{2\sqrt{3}}$) [note, Lemma F.5(a)]. The function $x = (\eta(3\tau)/\eta(\tau))^{12} = q + 12q^2 + \dots$ is a coordinate on this sphere, with $x(-1/(3\tau)) = 3^{-6}/x(\tau)$ (from $\eta(-1/\tau) = \sqrt{\tau/i}\,\eta(\tau)$), $j = (1+27x)(1+243x)^3/x$ and $x(\tau_e) = -\frac{1}{27}$ [note, Lemma F.5(b,c)]. The logarithmic derivative $B = \theta \log x = 1 + 12\sum \sigma_1^{(3)}(n) q^n$ is a weight-2 form whose only zeros are double zeros on the elliptic orbit [note, Lemma F.6]. The series G_5 is an Eichler integral: $\theta^5 G_5 = (E_6(3\tau) - E_6(\tau))/504$ has weight 6, and G_5 itself transforms with weight -4 up to polynomials of degree ≤ 4 in τ. By invariance and pole counting, $V = 2Du + u^2 = 24x/P^2$ (a Schwarzian derivative) and $R_5 = B^{-3}\theta^5 G_5 = x(1+39x)/P^2$ [note, Lemma F.7]. The recursion [note, (F.8)] expresses $D^i(B^2 Y)$ through $\theta^m Y$ with the $\mathfrak{sl}_2$-coefficients of [note, Lemma F.9], and the order-5 operator L_5 [note, Lemma F.10], with coefficients [note, (F.11)], kills $B^2\tau^a$ for $a \le 4$ and sends $H_c = B^2(G_5 + c)$ to R_5. The examples illustrate all these identities as exact series in q and x (to q^{25}, x^{25} or x^{15}) and numerically at points of $\mathbb{H}$, including points far outside the disc of convergence of the x-series.

Carried forward to Chapter 17: the coordinate x with $P = 1+27x$ and $x_e = -\frac{1}{27}$; the formula for j (for the supersingular annulus); B, its zeros and its Fricke rule; $D = x\,\mathrm{d}/\mathrm{d}x = B^{-1}\theta$, $u = DB/B$; the germs $g_i = D^{i-1}H_c$; the equation $L_5 H_c = R_5$ with (16.14); the solutions $B^2\tau^a$ and their Sym^4 monodromy.

Chapter 17

The second proof

Where we are. This chapter explains the second proof of the theorem [note, Appendix F, Sections F.2–F.5]. Its method is the determinant argument that the preprint [35] uses for $\zeta_7(3)$ on $X_0(7)$, carried over to the modular curve $X_0(3)$. It builds on Chapter 16, which constructed the coordinate x on $X_0(3)$, the weight-2 form B, the Eichler integral G_5, the operator $D = x\,\mathrm{d}/\mathrm{d}x$, the logarithmic derivative $u = DB/B$, the rational functions $V = 24x/P^2$ and $R_5 = x(1+39x)/P^2$ ($P = 1+27x$), the polynomials $N_{i,m}$ and the order-5 operator L_5 with $L_5 H_c = R_5$ [note, Lemmas F.5–F.10]. From earlier chapters we need 3-adic valuations and Newton-polygon-free facts about $\mathbb{Q}_3$ (Chapter 2), the value $\zeta_3(5)$ and the von Staudt–Clausen theorem (Chapter 3), the product formula and the bookkeeping idea (Chapter 1, Chapter 7), and the language of logarithmic potentials and energies (Chapter 10). We cover: the plan and its balance sheet; the determinant $\mathcal{D}_d$ and the zero estimate [note, Lemmas F.12, F.13, Propositions F.14, F.15, (F.16)–(F.18)]; the 3-adic estimate [note, Lemma F.19, Theorems F.20, F.23, Lemma F.22, Propositions F.24, F.26]; the primes $\ell \neq 3$ [note, Lemmas F.27, F.29, Propositions F.31, F.36, Lemmas F.38, F.39, Theorem F.40, Proposition F.42, Remark F.46]; and the archimedean estimate [note, Lemmas F.47–F.54, Proposition F.52, (F.55)–(F.58)]. The series in the examples are computed from their definitions in exact rational arithmetic, with $\zeta_3(5)$ computed as in Chapter 3; the archimedean numbers are 40-digit floating-point evaluations, not ball arithmetic, so they illustrate the note's bounds but do not certify them.

17.1 The plan in plain words

17.1.1 One rational number, measured at every place

Recall the germs [note, (F.3)]: for a constant c,

$$H_c = B^2(G_5(q(x)) + c)\ , \qquad g_0 = 1\ , \qquad g_i = D^{i-1}H_c \quad (1 \le i \le 5)\ , \tag{17.1}$$

power series in x, with rational coefficients when c is rational. Suppose, for contradiction, that $\eta_5 = \zeta_3(5)/2$ is rational. For each integer $d \ge 1$ the note builds one nonzero rational number $\mathcal{D}_d = \mathcal{D}_d(\eta_5)$, the determinant of a $5d \times 5d$ matrix of Taylor coefficients of the series $x^k g_i$ ($1 \le i \le 5$, $0 \le k < d$). The product formula of Chapter 1 says that for a nonzero rational number

$$\log|\mathcal{D}_d| = v_3(\mathcal{D}_d)\log 3 + \sum_{\ell \neq 3} v_\ell(\mathcal{D}_d)\log \ell\ . \tag{17.2}$$

The note's three estimates are the following, all of order d^2:

(i) *gain at* 3: $v_3(\mathcal{D}_d) \ge 15(6-\epsilon)d^2 - O(d)$ for every $0 < \epsilon < 6$ [note, Proposition F.26];

(ii) *denominators*: $\sum_{\ell\neq 3} v_\ell(\mathcal{D}_d)\log\ell \geq -\frac{13289}{168}d^2 - o(d^2)$ [note, Proposition F.42];
(iii) *size*: $\log|\mathcal{D}_d| \leq U\,d^2 + o(d^2)$ with $U \leq 16.6040183$ [note, Proposition F.52, (F.58)].
Inserting (i) and (ii) on the right of (17.2) and (iii) on the left gives, with $\epsilon = \frac{1}{10}$ (so $15(6-\epsilon) = \frac{177}{2}$) [note, (F.4)],

$$\Big(\tfrac{177}{2}\log 3 - \tfrac{13289}{168}\Big)d^2 - o(d^2) \leq \log|\mathcal{D}_d| \leq U\,d^2 + o(d^2)\ , \tag{17.3}$$

which is impossible for large d once $\frac{177}{2}\log 3 - \frac{13289}{168} - U > 0$. Numerically, $\frac{177}{2}\log 3 = 97.2271875471$, $\frac{13289}{168} = 79.1011904762$, $U = J - 3I = 16.6040182182$ (Section 17.5.5), and the margin 1.52197885; with the note's rounded $U = 16.6040183$ the margin is $1.52197877 > 1.52$, as claimed.

Intuition: why each estimate holds, in one sentence each. (i) For $c = \eta_5$ (and, as the computations of Example 17.16 suggest, only for this c) the germs are 3-adic functions on the large disc $|x|_3 < 3^6$, so their n-th coefficients are divisible by about 3^{6n}; a determinant of such coefficients is divisible by a power of 3 quadratic in d. (ii) The denominators of the coefficients come from the divisor sums $\sum a^{-5}$ in G_5; modulo powers of a prime ℓ they are governed by a few rational functions with few poles, and counting dimensions of spaces of such rational functions bounds how many factors of ℓ can occur. (iii) Over $\mathbb{C}$ the coefficients are bounded by the size of the functions on circles in the q-disc (Cauchy, sharpened to Jensen), and the remaining freedom is an electrostatic energy, as in Chapter 10.

17.1.2 The balance sheet, compared with the main proof

	main proof (bits per n^2, $\kappa = 2.8$)	second proof (nats per d^2, $\epsilon = \frac{1}{10}$)
gain at 3	43.49	$\frac{177}{2}\log 3 = 97.23$
size	$F^\dagger = 8.43$	$U = 16.60$
denominators	$c = 30.48$	$\frac{13289}{168} = 79.10$
margin	4.58	1.52
margin / gain	about 10.5%	about 1.6%

The left column is the note's [note, Table 1] as reproduced in Chapter 1; the right column is (17.3); the last row is our arithmetic on the printed numbers. The two columns are not directly comparable (different units, and n and d are unrelated parameters), but the last row shows that the second proof is the tighter of the two: 98.4% of its gain is consumed. There are two structural differences. First, the main proof needs an exact cancellation of terms of order $n^2\log n$ between size and denominators (Chapter 1); here no such terms appear, because the denominators of the coefficients are of the type $\mathrm{lcm}(1,\dots,n)^5$, which grows like e^{5n}, and not like a factorial. Second, here the gain $15(6-\epsilon)$ comes with a free parameter ϵ, and letting $\epsilon \to 0$ would raise the margin towards $90\log 3 - \frac{13289}{168} - U = 3.170$. For every ϵ the constant Θ_ϵ of [note, (F.25)] is not explicit (and it may grow as $\epsilon \to 0$), so the proof gives no explicit d at which the contradiction occurs.

How much the careful denominator count matters: the crude bound [note, (F.45)] below gives $\nu_\ell \leq 25d\lfloor \log N_d/\log\ell\rfloor$ for most primes, and summing $\lfloor\log N/\log\ell\rfloor\log\ell$ over $\ell \leq N$ gives $\log\mathrm{lcm}(1,\dots,N) \approx N$ by the prime number theorem, so the crude total is about $25d\cdot N_d \approx 150d^2$ (a rough estimate of ours, not in the note). That exceeds the gain of about $97d^2$. The refined count of Section 17.4 brings it down to $79.1d^2$.

17.1.3 What rests on what

The second proof uses nothing from Chapters 4–14. Its ingredients are of three kinds.

- *Proved in the note*: the modular identities of Chapter 16, the zero estimate, the denominator count, the energy bound, and the numerical bound for U (computed by the note in ball arithmetic; Example 17.50 evaluates it in floating point).
- *Textbook facts*: the product formula, von Staudt–Clausen, the prime number theorem, Jensen's formula, the energy inequality of Saff–Totik, the fact that 0 is the only supersingular j-invariant in characteristic 3.
- *Published research-level theorems, quoted but not proved or checked by the note*: Coleman's and Coleman–Mazur's theorem on the overconvergence of p-adic Eisenstein series [note, Theorem F.20], Buzzard's analytic continuation theorem [note, Theorem F.23], and four further facts listed after [note, Proposition F.24] (Katz's canonical subgroup, Conrad's comparison of Tate curves, a compatibility of definitions, and the q-expansion principle). They enter only estimate (i), through [note, Proposition F.24].

17.2 The determinant

17.2.1 The germs, concretely

Example 17.1 (the first coefficients of H_c)**.** Writing $[x^n]F$ for the coefficient of x^n, one finds $[x^n]B^2G_5(q(x)) = 0,\ 1,\ \frac{417}{32},\ -161,\ \frac{2254497}{1024},\dots$ and $[x^n]B^2 = 1,\ 24,\ -72,\ 456,\ -3528,\dots$ for $n = 0, 1, 2, 3, 4$. So $[x^n]H_c = [x^n]B^2G_5 + c\,[x^n]B^2$, and for $c = \frac{1}{2}$:

$$H_{1/2} = \tfrac{1}{2} + 13x - \tfrac{735}{32}x^2 + 67x^3 + \tfrac{448161}{1024}x^4 - \tfrac{8701709247}{400000}x^5 + \dots$$

The denominators are powers of 2 and 5 here: they come from $\sigma^{(3)}_{-5}(2) = 1 + 2^{-5} = \frac{33}{32}$, $\sigma^{(3)}_{-5}(4) = \frac{1057}{1024}$ and $\sigma^{(3)}_{-5}(5) = 1 + 5^{-5}$ inside G_5 (Chapter 16). The germ $g_i = D^{i-1}H_c$ has coefficients $n^{i-1}[x^n]H_c$, since $D = x\,\mathrm{d}/\mathrm{d}x$ multiplies x^n by n.

17.2.2 Differential modules

The independence of the germs is proved in the language of differential modules. This is linear algebra with one extra operation.

Definition 17.2 (differential module)**.** A *differential module* over the field $\mathbb{C}(x)$ of rational functions is a finite-dimensional $\mathbb{C}(x)$-vector space $\mathcal{M}$ with an additive map $D : \mathcal{M} \to \mathcal{M}$ satisfying the Leibniz rule $D(fm) = (Df)\,m + f\,Dm$ for $f \in \mathbb{C}(x)$, where $Df = x\,f'(x)$. A *submodule* is a subspace mapped into itself by D.

Intuition. A differential module is a linear differential equation written without choosing unknowns. If $m_1, \dots, m_r$ is a basis and $Dm_j = \sum_i C_{ij}m_i$, then an element $\sum_j f_j m_j$ is "constant" (D of it is 0) exactly when the column (f_j) solves the first-order system $Df = -Cf$. A submodule is a subsystem that closes on itself; an irreducible module is a system that cannot be decoupled into smaller systems over $\mathbb{C}(x)$. Physicists know the analogue from coupled linear ODEs that split into blocks after a rational change of variables.

Example 17.3 (the two modules of the note)**.** (a) $\mathcal{M}_5 = \mathbb{C}(x)[D]/\mathbb{C}(x)[D]L_5$ [note, Lemma F.13]: elements are differential operators modulo left multiples of L_5; a basis is $1, D, D^2, D^3, D^4$, and D acts by left multiplication, with the rule $D \cdot D^4 = D^5 \equiv -\mathfrak{a}_3D^3 - \mathfrak{a}_2D^2 - \mathfrak{a}_1D - \mathfrak{a}_0$ (the coefficients $\mathfrak{a}_j$ of L_5, Chapter 16). If f is any function with $L_5 f = 0$, the map $\mathcal{L} \mapsto \mathcal{L}f$ sends this module to functions, compatibly with D. (b) $\mathcal{W}$ [note, Proposition F.14]: basis $e_0, \dots, e_5$ with

$$De_0 = 0\ , \qquad De_i = e_{i+1}\ (1 \le i \le 4)\ , \qquad De_5 = R_5e_0 - \mathfrak{a}_0e_1 - \mathfrak{a}_1e_2 - \mathfrak{a}_2e_3 - \mathfrak{a}_3e_4\ .$$

This is the abstract version of the six germs: by [note, Lemma F.10], $D(D^4H_c) = R_5 - \sum_j \mathfrak{a}_j D^j H_c$, so $e_0 \mapsto 1$, $e_i \mapsto D^{i-1}H_c$ respects D. The line $\mathbb{C}(x)e_0$ is a submodule (constants), and $\mathcal{W}/\mathbb{C}(x)e_0 \cong \mathcal{M}_5$.

17.2.3 No rational solution: Lemma F.12

Lemma 17.4 ([note, Lemma F.12])**.** *There is no rational function $v \in \mathbb{C}(x)$ with $L_5 v = R_5$.*

Why we need it: if such a v existed, the module $\mathcal{W}$ of Example 17.3 would split as $\mathbb{C}(x)e_0$ plus a D-stable complement (spanned by $e_1 - ve_0$ and its derivatives), and the argument of the zero estimate, which needs every D-stable subspace not contained in $\mathbb{C}(x)e_0$ to be all of $\mathcal{W}$, would break down. The proof is a pole count, and the tool for counting poles at singular points is the indicial polynomial.

Definition 17.5 (indicial polynomial)**.** Let x_0 be a point and $t = x - x_0$. Apply L_5 to a trial power t^ρ. If $x_0 \neq 0$ and each coefficient $\mathfrak{a}_j$ has a pole of order at most $5 - j$ in t (a *regular singular point*; Fuchs' condition), then $L_5 t^\rho = \chi(\rho)\, t^{\rho-5} + O(t^{\rho-4})$. At $x_0 = 0$, where $D = x\,\mathrm{d}/\mathrm{d}x$ is already the Euler operator, the condition is that each $\mathfrak{a}_j$ be regular at 0, and then $L_5 x^\rho = \chi(\rho)x^\rho + O(x^{\rho+1})$. In both cases χ is a polynomial of degree 5, the *indicial polynomial*. Its roots are the possible leading exponents of local solutions.

Intuition. This is the Frobenius method for ODEs with regular singular points, familiar from the hypergeometric and Bessel equations: near x_0 the equation looks like an Euler equation, whose solutions are powers t^ρ with ρ a root of the indicial polynomial. A pole of order k_0 in a function v is a "trial power" t^{-k_0}, and L_5 maps it to $\chi(-k_0)t^{-k_0-5}$ at a point other than 0; so unless $-k_0$ is an indicial root, L_5 increases the pole order by exactly 5.

Example 17.6 (the indicial polynomials of L_5)**.** Recall from Chapter 16 the forms $\mathfrak{a}_3 = -5V$, $\mathfrak{a}_2 = -\frac{15}{2}DV$, $\mathfrak{a}_1 = 4V^2 - \frac{9}{2}D^2V$, $\mathfrak{a}_0 = 4V\,DV - D^3V$ with $V = 24x/P^2$. Since V vanishes at 0 and has a double pole at $x_e = -\frac{1}{27}$, and D^jV has a pole of order $2 + j$ there, each $\mathfrak{a}_j$ vanishes at $x = 0$ and has a pole of order exactly $5 - j$ at x_e: both points are regular singular. At $x = 0$ all $\mathfrak{a}_j(0) = 0$, so $L_5 x^\rho = \rho^5 x^\rho + O(x^{\rho+1})$ and $\chi_0(\rho) = \rho^5$. At x_e, with $t = x - x_e$ and $P = 27t$, one finds $\lim t^{5-j}\mathfrak{a}_j = \frac{40}{6561}, \frac{40}{59049}, \frac{2200}{43046721}, \frac{2240}{1162261467}$ for $j = 3, 2, 1, 0$, and, using $D = (x_e + t)\,\mathrm{d}/\mathrm{d}t$ exactly,

$$\chi_{x_e}(\rho) = -\frac{(\rho-2)(3\rho-4)(3\rho-5)(3\rho-7)(3\rho-8)}{3^{19}}\,, \qquad \text{roots } \tfrac{4}{3}, \tfrac{5}{3}, 2, \tfrac{7}{3}, \tfrac{8}{3}\,.$$

These are the exponents the note names. Their origin: near τ_e, B^2 vanishes to order 4 in $\tau - \tau_e$ and $x - x_e$ to order 3 (Chapter 16), so the solutions $B^2(\tau - \tau_e)^k$, $k = 0, \dots, 4$, behave like $(x - x_e)^{(4+k)/3}$. At $x = \infty$, $x\,\mathfrak{a}_j \to -\frac{40}{243}, \frac{20}{81}, -\frac{4}{27}, \frac{8}{243}$ ($j = 3, 2, 1, 0$): all $\mathfrak{a}_j = O(1/x)$. Finally $P^5\mathfrak{a}_0$ has degree 4 and $P^5 R_5 = x(1 + 27x)^3(1 + 39x)$ has degree 5.

The note's argument, step by step. Suppose $L_5 v = R_5$ with v rational. (1) *No poles outside* $\{0, x_e, \infty\}$. There the $\mathfrak{a}_j$ are regular, so a pole of v of order k_0 produces in $D^5 v$ a pole of order $k_0 + 5$ and in the other terms poles of order at most $k_0 + 3$; $L_5 v$ has a pole, but R_5 is regular there. (2) *No pole at* 0. The indicial polynomial is ρ^5, so $L_5 x^{-k_0} = (-k_0)^5 x^{-k_0} + \dots$, a pole of order exactly k_0; $R_5(0) = 0$. (3) *No pole at* x_e. A pole of order $k_0 \geq 1$ gives $L_5 v \sim \chi_{x_e}(-k_0)t^{-k_0-5}$ with $\chi_{x_e}(-k_0) \neq 0$ (its roots are positive; explicitly $\chi_{x_e}(-1), \chi_{x_e}(-2), \chi_{x_e}(-3)$ are $\frac{6160}{3^{18}}, \frac{80080}{3^{19}}, \frac{247520}{3^{19}}$), a pole of order ≥ 6, while R_5 has a pole of order 2 at x_e. (4) So v is a polynomial, of degree m say. Since $D^5 x^m = m^5 x^m$ and each $\mathfrak{a}_j D^j v$ has degree at most $m - 1$ (because $\mathfrak{a}_j = O(1/x)$), the top term of $L_5 v$ is m^5 times that of v; R_5 is bounded at ∞, so $m = 0$. (5) A constant v gives $L_5 v = \mathfrak{a}_0 v$, and $P^5\mathfrak{a}_0 v$ has degree at most 4 while $P^5 R_5$ has degree 5: impossible. $\square$

17.2.4 Irreducibility through monodromy: Lemma F.13

Lemma 17.7 ([note, Lemma F.13])**.** *The differential module* $\mathcal{M}_5 = \mathbb{C}(x)[D]/\mathbb{C}(x)[D]L_5$ *is irreducible.*

Monodromy. Near a point $x_0 \notin \{0, x_e, \infty\}$ the solutions of $L_5 f = 0$ form a five-dimensional space, spanned by $B^2\tau^a$, $0 \le a \le 4$ (Chapter 16, [note, Lemma F.10]). Continue a solution analytically along a closed loop in $\mathbb{P}^1 \setminus \{0, x_e, \infty\}$: it comes back as another solution, and the resulting linear map of the solution space is the *monodromy* of the loop. The note computes it through the upper half plane: x makes $\mathbb{H}$ minus the elliptic orbit a covering of $\mathbb{P}^1 \setminus \{0, x_e, \infty\}$ with deck group $\Gamma_0(3)/\{\pm 1\}$, so a loop lifts to a path from τ_0 to $\gamma\tau_0$, $\gamma \in \Gamma_0(3)$, and every γ occurs. Continuation replaces τ by $\gamma\tau$, and with $B(\gamma\tau) = (c\tau + d)^2 B(\tau)$,

$$B^2(\gamma\tau)\,(\gamma\tau)^a = B^2(\tau)\,(a_\gamma\tau + b_\gamma)^a (c_\gamma\tau + d_\gamma)^{4-a}\ . \tag{17.4}$$

In the variables $(X, Y) = (\tau, 1)$ the solution $B^2\tau^a$ is the binary quartic monomial $X^a Y^{4-a}$, and γ acts by the substitution $X \mapsto a_\gamma X + b_\gamma Y$, $Y \mapsto c_\gamma X + d_\gamma Y$. This five-dimensional representation of $\Gamma_0(3)$ is Sym^4, the fourth symmetric power of the standard two-dimensional one (spin 2, in physics language; Chapter 16).

Example 17.8 (the two generators on binary quartics)**.** In the basis $Y^4, XY^3, X^2Y^2, X^3Y, X^4$ (columns are the images of the basis vectors), $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ $(X \mapsto X + Y)$ and $A = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)$ $(Y \mapsto 3X + Y)$ act by

$$\mathrm{Sym}^4 T = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 & 6 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \mathrm{Sym}^4 A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 12 & 1 & 0 & 0 & 0 \\ 54 & 9 & 1 & 0 & 0 \\ 108 & 27 & 6 & 1 & 0 \\ 81 & 27 & 9 & 3 & 1 \end{pmatrix}.$$

For instance the last column of $\mathrm{Sym}^4 T$ is $(X+Y)^4 = Y^4 + 4XY^3 + 6X^2Y^2 + 4X^3Y + X^4$, and the first column of $\mathrm{Sym}^4 A$ is $(3X + Y)^4$. Both are *unipotent*: $(\mathrm{Sym}^4 T - 1)^5 = 0$. Their logarithms, computed from the finite series $\log(1+N) = N - \frac{N^2}{2} + \frac{N^3}{3} - \frac{N^4}{4}$, are

$$\log \mathrm{Sym}^4 T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = Y\partial_X, \qquad \log \mathrm{Sym}^4 A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 12 & 0 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \end{pmatrix} = 3X\partial_Y,$$

and their commutator is $\mathrm{diag}(12, 6, 0, -6, -12) = 3(Y\partial_Y - X\partial_X)$, with eigenvalue $3\big((4-a)-a\big)$ on $X^a Y^{4-a}$. Moreover $\exp\Big(\log \mathrm{Sym}^4 T\Big) = \mathrm{Sym}^4 T$, the elliptic element $\gamma_e = \left(\begin{smallmatrix} 2 & -1 \\ 3 & -1 \end{smallmatrix}\right)$ has $(\mathrm{Sym}^4 \gamma_e)^3 = 1$ (since $\gamma_e^3 = -1$ and $(-1)^4 = 1$), and the words in the two logarithms applied to Y^4 span all five dimensions.

> **Intuition: ladder operators.** $Y\partial_X$ and $3X\partial_Y$ are (up to the factor 3) the raising and lowering operators $J_\pm$ of spin 2, and their commutator is a multiple of J_z, with the five distinct eigenvalues $m = 2, 1, 0, -1, -2$ (times 6). An invariant subspace of an irreducible spin-2 multiplet must be all of it; the proof below is exactly the textbook argument that the spin-j representation is irreducible.

The note's argument, step by step. (1) *From group elements to logarithms.* If U is unipotent, $\log U = \sum_{k=1}^{4} (-1)^{k+1}(U-1)^k/k$ is a polynomial in U. A subspace mapped into itself by U

is mapped into itself by every polynomial in U, hence by $\log U$. So a monodromy-invariant subspace S of the quartics is invariant under $Y\partial_X$ and $3X\partial_Y$, and therefore under their commutator $\mathcal{J} = 3(Y\partial_Y - X\partial_X)$. (2) *$S$ contains a monomial.* $\mathcal{J}$ is diagonal with distinct eigenvalues $12, 6, 0, -6, -12$ on the monomials. For a diagonalizable operator with distinct eigenvalues the projector onto each eigenline is a polynomial in the operator (Lagrange interpolation: $\prod_{\mu' \neq \mu}(\mathcal{J} - \mu')/(\mu - \mu')$), so S is a sum of eigenlines. If $S \neq 0$, it contains some $X^a Y^{4-a}$. (3) *S contains all monomials.* $Y\partial_X$ sends $X^a Y^{4-a}$ to $aX^{a-1}Y^{5-a}$ and $3X\partial_Y$ sends it to $3(4-a)X^{a+1}Y^{3-a}$, with nonzero factors until the ends; so from one monomial we reach all five. Thus the solution space has no monodromy-invariant subspace other than 0 and itself. (4) *From the module to solutions.* Suppose $\mathcal{M}_5$ had a submodule S' with $0 \neq S' \neq \mathcal{M}_5$. The quotient $\mathcal{M}_5/S'$ is generated by the image of 1 (as $\mathcal{M}_5$ is), of dimension $k \in \{1, \dots, 4\}$. The operators $\mathcal{L}$ with $\mathcal{L} \cdot 1 \in S'$ form a left ideal of $\mathbb{C}(x)[D]$ containing L_5; such ideals are generated by one monic operator L'' (division with remainder works for differential operators), of order k. So $L_5 = L'L''$. Every solution of $L''f = 0$ solves $L_5 f = 0$, these solutions form a k-dimensional space, and analytic continuation maps solutions of L'' (an equation with rational coefficients) to solutions of L''. This is a monodromy-invariant subspace of dimension $1 \leq k \leq 4$, contradicting (3). □

17.2.5 Independence of the germs: Proposition F.14

Proposition 17.9 ([note, Proposition F.14])**.** *The only proper nonzero submodule of $\mathcal{W}$ is $\mathbb{C}(x)e_0$. For every $c \in \mathbb{C}$ the map $e_0 \mapsto 1$, $e_i \mapsto D^{i-1}H_c$ is injective; in particular $1, H_c, DH_c, \dots, D^4 H_c$ are linearly independent over $\mathbb{C}(x)$.*

The note's argument, step by step. (1) $\mathcal{W}/\mathbb{C}(x)e_0 \cong \mathcal{M}_5$, with $\bar{e}_1 \mapsto 1$, $\bar{e}_i \mapsto D^{i-1}$; under it $L_5\bar{e}_1 = 0$, which is the relation defining $\mathcal{M}_5$. (2) Let S be a proper nonzero submodule. Its image in $\mathcal{M}_5$ is a submodule, so by Lemma 17.7 it is 0 or $\mathcal{M}_5$. If it is 0, $S \subseteq \mathbb{C}(x)e_0$, a line, so $S = \mathbb{C}(x)e_0$. (3) If the image is $\mathcal{M}_5$: $e_0 \in S$ would give $S \supseteq \mathbb{C}(x)e_0$ plus a full preimage of $\mathcal{M}_5$, i.e. $S = \mathcal{W}$; so $e_0 \notin S$ and S meets the line $\mathbb{C}(x)e_0$ only in 0. Hence S is a complement of that line, and it contains an element $s_1 = e_1 - ve_0$ for some $v \in \mathbb{C}(x)$ (the element of S mapping to $\bar{e}_1$). (4) Since $De_0 = 0$, $D^k s_1 = e_{k+1} - (D^k v)e_0$ for $k \leq 4$, and $D^5 s_1 + \sum_j \mathfrak{a}_j D^j s_1 = (R_5 - L_5 v)e_0$. The left side lies in S, the right side in $\mathbb{C}(x)e_0$, so both vanish, and $L_5 v = R_5$, which Lemma 17.4 excludes. (5) The map to functions respects D by [note, Lemma F.10]. Its kernel is a submodule; it does not contain e_0 (which maps to $1 \neq 0$), so by the first part it is 0. □

17.2.6 The zero estimate: Proposition F.15

Proposition 17.10 (zero estimate; [note, Proposition F.15])**.** *Let $\mathcal{F} = \sum_{j=0}^{5} a_j g_j \neq 0$ with polynomials a_j of degree $< d$, and $c \in \mathbb{C}$. Then $\operatorname{ord}_0 \mathcal{F} \leq 6d + 69$.*

> **Intuition: a Wronskian with polynomial entries.** With $6d$ free coefficients one can always make $\mathcal{F}$ vanish to order about $6d-1$ (linear algebra: $6d$ unknowns, one equation per coefficient). The zero estimate says that one cannot do much better: the excess is at most a constant (70), independent of d. The tool is a Wronskian. For six functions $f_0, \dots, f_5$, the determinant of $(D^k f_j)$ vanishes identically exactly when they are dependent; here the six columns $\mathcal{F}, D\mathcal{F}, \dots, D^5\mathcal{F}$ are expanded in the frame $e_0, \dots, e_5$, the determinant Δ of the coefficient columns is a polynomial of controlled degree, and a high order of vanishing of $\mathcal{F}$ at 0 would force Δ to vanish to high order, more than its degree allows.

The note's argument, step by step. (1) If only $a_0 \neq 0$, $\mathcal{F} = a_0$ has order $\leq d-1$. Otherwise $\mathcal{F} \notin \mathbb{C}(x)e_0$ (identifying $\mathcal{W}$ with its image). The $\mathbb{C}(x)$-span of $\mathcal{F}, D\mathcal{F}, D^2\mathcal{F}, \dots$ is a submodule not

contained in $\mathbb{C}(x)e_0$, hence all of $\mathcal{W}$ by Proposition 17.9; and $\mathcal{F}, D\mathcal{F}, \dots, D^5\mathcal{F}$ are independent (if $D^k\mathcal{F}$ depended on the earlier ones for some $k < 6$, the span would be D-stable of dimension $k < 6$). (2) Write $De = e\,\mathcal{C}$ for the row of basis vectors $e = (e_0, \dots, e_5)$. By Example 17.3, the columns of $\mathcal{C}$ are 0, then the unit vectors, and finally $(R_5, -\mathfrak{a}_0, -\mathfrak{a}_1, -\mathfrak{a}_2, -\mathfrak{a}_3, 0)^{\mathsf{T}}$; so $P^5\mathcal{C}$ has polynomial entries of degree ≤ 5. (3) Put $P^{5k}D^k\mathcal{F} = e\,p^{(k)}$ with $p^{(0)} = (a_0, \dots, a_5)^{\mathsf{T}}$. Applying D with the Leibniz rule, $D(P^{5k}e\,p^{(k)}) = 5kP^{5k-1}(DP)\,e\,p^{(k)} + P^{5k}e\,(Dp^{(k)} + \mathcal{C}p^{(k)})$; multiplying by P^5 and subtracting the first term gives [note, (F.16)]:

$$p^{(k+1)} = P^5 Dp^{(k)} - 5k\,P^4(DP)\,p^{(k)} + (P^5\mathcal{C})\,p^{(k)}\ . \tag{17.5}$$

Each step raises the degree by at most 5 (D does not raise degrees, $DP = 27x$), so $\deg p^{(k)} \le d - 1 + 5k$. (4) $\Delta = \det\left(p^{(0)}, \dots, p^{(5)}\right)$ is a nonzero polynomial (by (1)) of degree $\le \sum_{k=0}^{5}(d - 1 + 5k) = 6d + 69$. (5) In the matrix, add to the row of e_0 the row of e_j times the germ g_j, for $j = 1, \dots, 5$. The determinant is unchanged, and the k-th entry of the new first row is $\sum_j g_j p_j^{(k)} = P^{5k}D^k\mathcal{F}$, a series of order $\ge \operatorname{ord}_0 \mathcal{F}$. Expanding along that row (the other rows are polynomials), $\operatorname{ord}_0 \Delta \ge \operatorname{ord}_0 \mathcal{F}$. Since $\Delta \ne 0$, $\operatorname{ord}_0 \Delta \le \deg \Delta \le 6d + 69$. □

Example 17.11 (the zero estimate for $d = 1$)**.** For $d = 1$ and $c = \frac{1}{2}$, the combination of highest order is $a = (-12, 24, -50, 35, -10, 1)$, that is,

$$\mathcal{F} = -12 + 24H - 50DH + 35D^2H - 10D^3H + D^4H = (D-1)(D-2)(D-3)(D-4)H - 12\ ,$$

since $(D-1)(D-2)(D-3)(D-4) = D^4 - 10D^3 + 35D^2 - 50D + 24$. The operator multiplies $[x^n]H$ by $(n-1)(n-2)(n-3)(n-4)$, which kills $n = 1, 2, 3, 4$, and at $n = 0$ it gives $24 \cdot \frac{1}{2} - 12 = 0$. So $\operatorname{ord}_0 \mathcal{F} = 5$. Running the recursion (17.5): $\deg p^{(k)} = 0, 5, 10, 15, 20, 25$ (the bound $d - 1 + 5k$ is attained), Δ has degree exactly $75 = 6d + 69$, and $\operatorname{ord}_0 \Delta = 5 \ge \operatorname{ord}_0 \mathcal{F} = 5$.

17.2.7 Jumps, the matrix M, and $\mathcal{D}_d \ne 0$

Let $\Phi_d : \mathbb{C}[x]^6_{<d} \to \mathbb{C}[[x]]$, $a \mapsto \sum_j a_j g_j$, a linear map from a $6d$-dimensional space, injective by Proposition 17.9. Its image is a $6d$-dimensional space of power series.

Definition 17.12 (jumps; [note, (F.17)])**.** The *jumps* $\lambda_0 < \lambda_1 < \cdots < \lambda_{6d-1}$ are the orders $\operatorname{ord}_0 \Phi_d(a)$ that occur. Equivalently, λ is a jump if and only if the coefficient row $([x^\lambda](x^k g_i))_{i,k}$ is not a linear combination of the rows for smaller exponents.

There are exactly $6d$ of them: the subspaces $\{\operatorname{ord}_0 \Phi_d \ge n\}$ shrink by at most one dimension each time n increases by one (two series of the same order n have a combination of higher order), and they go from dimension $6d$ to 0. Since the block of a_0 (multiples of $g_0 = 1$) gives the orders $0, \dots, d-1$, $\lambda_j = j$ for $j < d$. All jumps are $\le 6d + 69$ by Proposition 17.10, and since they are distinct integers, the j-th one is at least j and at most $6d + 69$ minus the number $6d - 1 - j$ of jumps above it:

$$j \le \lambda_j \le j + 70\ . \tag{17.6}$$

Definition 17.13 (M and $\mathcal{D}_d$; [note, (F.18)])**.** Let $I_d = \{\lambda_d, \dots, \lambda_{6d-1}\} \subset [d, N_d)$, $N_d = 6d + 70$, and

$$M_{\lambda,(i,k)} = [x^{\lambda-k}]\,g_i \qquad (\lambda \in I_d,\ 1 \le i \le 5,\ 0 \le k < d)\ , \qquad \mathcal{D}_d(c) = \det M\ .$$

Why $\mathcal{D}_d \ne 0$: the big $6d \times 6d$ matrix $\tilde{M}$ of coefficients $[x^\lambda](x^k g_i)$ on the rows $\lambda_0, \dots, \lambda_{6d-1}$, columns (i, k) with $0 \le i \le 5$, is nonsingular: in a basis of the source in which the j-th basis vector has order exactly λ_j (Gaussian elimination by order), the matrix is triangular with nonzero diagonal. The columns with $i = 0$ are x^k, the unit vectors of the rows $\lambda_j = j < d$; expanding along them leaves $\pm \det M$. For rational c everything is defined over $\mathbb{Q}$, so $\mathcal{D}_d(c)$ is a nonzero rational number, the same whether we view it in $\mathbb{C}$ or in $\mathbb{Q}_3$.

Example 17.14 ($d = 1$: a Vandermonde determinant)**.** For $d = 1$ the only k is 0 and $M_{\lambda,i} = [x^\lambda]D^{i-1}H_c = \lambda^{i-1}h_\lambda$ with $h_\lambda = [x^\lambda]H_c$. If the jumps are $0, \dots, 5$, then $I_1 = \{1, \dots, 5\}$ and

$$\mathcal{D}_1 = \det\left(\lambda^{i-1}h_\lambda\right)_{\lambda,i=1}^{5} = h_1h_2h_3h_4h_5 \prod_{1\le\lambda<\lambda'\le5}(\lambda' - \lambda) = 288\, h_1h_2h_3h_4h_5 \ .$$

For $c = \frac{1}{2}$, with the coefficients of Example 17.1, the jumps are indeed $0, \dots, 5$, and

$$\mathcal{D}_1(\tfrac{1}{2}) = \frac{4493829881274213891411}{81920000} = \frac{3^6 \cdot 7^5 \cdot 11 \cdot 13 \cdot 37 \cdot 67 \cdot 21341 \cdot 48481}{2^{17} \cdot 5^4} \ ,$$

equal to $288\, h_1 \cdots h_5$. The product formula (17.2) is visible: $\log|\mathcal{D}_1| = 31.6357$, of which $6\log 3$ is the 3-part, $-17\log 2 - 4\log 5$ the denominators, and the rest the primes $7, 11, \dots, 48481$ of the numerator.

Example 17.15 (jumps and $\mathcal{D}_d$ for $d = 1, 2, 3$)**.** For $c = \frac{1}{2}$ and for $c = \eta_5^{\mathrm{tr}}$ (a rational number with $v_3(\eta_5 - \eta_5^{\mathrm{tr}}) \ge 799$, see Section 17.3.1), and $d = 1, 2, 3$, the jumps are $\lambda_j = j$ for all $j < 6d$: the slack $\lambda_j - j$ in (17.6) is 0, not 70, in all six cases. Then $I_d = \{d, \dots, 6d-1\}$ and $\mathcal{D}_d \neq 0$. For $c = \frac{1}{2}$:

d	$\log\lvert\mathcal{D}_d\rvert$	$v_3(\mathcal{D}_d)$	denominator of $\mathcal{D}_d$
1	31.64	6	$2^{17}5^4$
2	127.05	22	$2^{86}5^{34}7^{23}11^5$
3	247.96	57	$2^{159}5^{60}7^{55}11^{35}13^{25}17^4$

The primes in the denominator are all $\le 17 < N_d$, in line with [note, (F.45)] below. For $c = \eta_5^{\mathrm{tr}}$ the 3-adic valuations are much larger: $v_3(\mathcal{D}_d) = 53,\ 263,\ 635$ for $d = 1, 2, 3$ (Section 17.3.5).

What just happened. Six germs, independent over $\mathbb{C}(x)$ because L_5 has irreducible monodromy (Sym^4 of $\Gamma_0(3)$) and $L_5 v = R_5$ has no rational solution. A Wronskian-type determinant bounds the order of vanishing of any combination with polynomial coefficients of degree $< d$ by $6d+69$. This pins the $6d$ jumps between j and $j+70$, and the determinant $\mathcal{D}_d$ of the $5d \times 5d$ matrix of coefficients at the rows I_d is a nonzero rational number. In practice, for the cases computed, the jumps are exactly $0, 1, \dots, 6d-1$.

17.3 The 3-adic estimate

17.3.1 What is needed, and what it looks like

The 3-adic estimate needs one analytic fact [note, (F.25)]: for $c = \eta_5$ and every $\epsilon > 0$ there is Θ_ϵ with

$$v_3([x^n]\, g_i) \ge (6 - \epsilon)n - \Theta_\epsilon \qquad (n \ge 0,\ 1 \le i \le 5) \ . \tag{17.7}$$

By the convergence test of Chapter 2, a series $\sum a_n x^n$ converges on the 3-adic disc $|x|_3 \le R$ exactly when $|a_n|_3 R^n \to 0$, i.e. $v_3(a_n) - n\log_3 R \to \infty$. So (17.7) says that the germs converge on every closed disc of radius $3^{6-\epsilon}$, that is, on the open disc $|x|_3 < 3^6$.

Example 17.16 (the empirical face of [note, Proposition F.24])**.** The series [note, (2.13)] with 801 terms (as in Chapter 3) gives $\eta_5 = \zeta_3(5)/2$ modulo 3^{799}. With the resulting rational truncation η_5^{tr}, every valuation below 799 is exact. The valuations $v_3([x^n]H_c)$ are:

n	$c=\eta_5$	$6n$	difference	$c=0$	$c=\frac{1}{2}$	$c=-\eta_5$	$[x^n]B^2$
1	2	6	−4	0	0	0	1
2	5	12	−7	1	1	1	2
3	11	18	−7	0	0	0	1
4	14	24	−10	1	1	1	2
5	19	30	−11	2	2	2	3
6	24	36	−12	1	1	1	2
9	43	54	−11	0	0	0	1
10	47	60	−13	1	1	1	2
18	91	108	−17	1	1	1	2
19	102	114	−12	2	2	2	3
27	146	162	−16	0	0	0	1
30	162	180	−18	1	1	1	2
55	315	330	−15				
81	465	486	−21				
108	623	648	−25				
129	750	774	−24				

(the last column is $v_3([x^n]B^2)$). For $c=\eta_5$ the valuation grows almost exactly like $6n$: the difference v_3-6n stays between -25 and -4 for all $n\le 129$ (its minimum over $n\le 30$, $n\le 60$, $n\le 129$ is -18, -22, -25), drifting down slowly, which is what convergence on the open disc of radius 3^6 (but not on the closed one) allows. For every other c in the table the valuations stay at most 5 for $n\le 30$. The reason is the identity $[x^n]H_c=[x^n]H_{\eta_5}+(c-\eta_5)[x^n]B^2$: the first term is highly divisible, so $v_3([x^n]H_c)=v_3(c-\eta_5)+v_3([x^n]B^2)$, and here $v_3(c-\eta_5)=-1$ while $v_3([x^n]B^2)\le 8$ for all $n\le 129$. The table confirms this column by column. For $g_5=D^4H_{\eta_5}$ the extra factor n^4 only adds $4v_3(n)$: $2,5,15,14,19,28,\dots$ for $n=1,\dots,6$.

This is evidence, not proof: 129 coefficients cannot decide the radius of convergence. The proof is [note, Proposition F.24], which rests on the published theorems explained next.

17.3.2 Ordinary and supersingular, and Newton polygons

Elliptic curves modulo 3. By Chapter 16, a point of $X_0(3)$ is a pair (E,C): an elliptic curve and a subgroup of order 3. Over $\mathbb{Q}_3$ (or a finite extension), a curve with integral j-invariant can be reduced modulo 3. A curve $\bar{E}$ over a field of characteristic 3 is *supersingular* if it has no point of order 3 over the algebraic closure, and *ordinary* if its 3-torsion points form a group $\mathbb{Z}/3$. A textbook fact [31, Theorem V.4.1(c) and its proof]: in characteristic 3 the only supersingular j-invariant is $j=0$. So for a curve over $\mathbb{Q}_3$ with $|j|_3\le 1$, the reduction is supersingular exactly when $|j|_3<1$. Curves with $|j|_3>1$ (near the cusps) are Tate curves (below) and count as ordinary. Altogether: a point is *ordinary* if $v_3(j)\le 0$ and *supersingular* if $v_3(j)>0$.

Intuition. Think of $v_3(j)$ as a height function on the 3-adic modular curve. The ordinary points are where the curve "remembers" its 3-torsion after reduction; the supersingular ones are a thin region around $j=0$ where the 3-torsion collapses. Everything 3-adically subtle about modular forms happens in that region.

Newton polygons. To find $v_3(j)$ as a function of $v=v_3(x)$, we need the valuation of a polynomial $f(x)=\sum_k c_kx^k$ at a point with $v_3(x)=v$. The k-th term has valuation $v_3(c_k)+kv$. By the ultrametric inequality (Chapter 2), if one term has strictly smaller valuation than all the others, $v_3(f(x))$ equals it; only when the minimum is attained twice can there be cancellation. So, away from finitely many values of v,

$$v_3(f(x))=\min_k\left(v_3(c_k)+kv\right)\ ,$$

a concave piecewise linear function of v. Plotting the points $(k, v_3(c_k))$, its corners correspond to the edges of the lower convex hull of these points, the *Newton polygon*; an edge of slope σ and horizontal length m means f has m roots of valuation $-\sigma$ (counted with multiplicity). This is a standard tool (e.g. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Ch. IV.3).

Example 17.17 (the Newton polygon of xj)**.** By [note, Lemma F.5(c)] (Chapter 16), $xj = (1+27x)(1+243x)^3 = 1 + 756x + 196830x^2 + 19131876x^3 + 387420489x^4$, with v_3 of the coefficients $0, 3, 9, 14, 18$. The lower convex hull of $(0,0), (1,3), (2,9), (3,14), (4,18)$ has an edge of slope 3 from $(0,0)$ to $(1,3)$ and an edge of slope 5 from $(1,3)$ to $(4,18)$ (the points $(2,9)$ and $(3,14)$ lie above the line $3+5(k-1)$, at 8 and 13). So xj has one root of valuation -3 and three of valuation -5: indeed $-\frac{1}{27}$ and $-\frac{1}{243}$ (triple).

Lemma 17.18 ([note, Lemma F.19])**.** *With $v = v_3(x)$: $v_3(j) = -v$ for $v > -3$; $v_3(j) = 3$ for $-5 < v < -3$; $v_3(j) = 18 + 3v$ for $v < -5$; and $v_3(j) \geq 3$ for $v = -3, -5$. Hence the ordinary locus is $\{|x|_3 \leq 1\} \sqcup \{|x|_3 \geq 3^6\}$, containing the cusps ∞ ($x = 0$) and 0 ($x = \infty$) respectively, the supersingular locus is the annulus $1 < |x|_3 < 3^6$, and $W_0(3)$, the complement of the ordinary component of the cusp 0, is the open disc $|x|_3 < 3^6$. The elliptic point $x_e = -\frac{1}{27}$, with $|x_e|_3 = 27$, lies in the annulus.*

Computation. $v_3(j) = v_3(1+27x) + 3v_3(1+243x) - v$. The first factor has terms of valuation 0 and $3+v$, so $v_3(1+27x) = \min(0, 3+v)$ unless $v = -3$; likewise $v_3(1+243x) = \min(0, 5+v)$ unless $v = -5$. For $v > -3$: $0 + 0 - v$. For $-5 < v < -3$: $(3+v) + 0 - v = 3$. For $v < -5$: $(3+v) + 3(5+v) - v = 18 + 3v$. At $v = -3$ the first factor may cancel, so $v_3(1+27x) \geq 0$ and $v_3(j) \geq 0 + 0 + 3$; at $v = -5$, $v_3(1+243x) \geq 0$ and $v_3(j) \geq (3-5) + 0 + 5 = 3$. Now $v_3(j) \leq 0$ exactly when $-v \leq 0$ (i.e. $v \geq 0$) or $18 + 3v \leq 0$ (i.e. $v \leq -6$); in terms of $|x|_3 = 3^{-v}$ this is $|x|_3 \leq 1$ or $|x|_3 \geq 3^6$. Each ordinary piece is a disc (around $x = 0$, respectively $x = \infty$), hence connected. □

For $v = -9, \ldots, 3$ and ten units $u \in \{1, 2, 4, 5, 7, -1, -2, 11, 13, 22\}$, the exact value of $v_3(j)$ at $x = 3^v u$ agrees with the formula for every $v \neq -3, -5$ (e.g. $-9, -6, -3, 0, 3, 2, 1, 0, -1$ for $v = -9, -8, -7, -6, -4, -2, -1, 0, 1$); at $v = -5$ it is 3 or 6 or $+\infty$ (for $u = -1$, $x = -\frac{1}{243}$, where $j = 0$), and at $v = -3$ it is 3 or 4 or $+\infty$ (for $x = x_e$). A Fricke check: the involution $x \mapsto 3^{-6}/x$ of Chapter 16 sends $v \mapsto -6 - v$, exchanging the two ordinary discs and mapping the annulus $-6 < v < 0$ to itself.

17.3.3 Overconvergent modular forms: the black boxes

The Tate curve. Over $\mathbb{C}$, the torus $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ is $\mathbb{C}^\times/q^{\mathbb{Z}}$ via $z \mapsto e^{2\pi i z}$. Tate observed that the quotient $E_q = \bar{\mathbb{Q}}_3^\times/q^{\mathbb{Z}}$ makes sense 3-adically for $|q|_3 < 1$ and is an elliptic curve; this is how q-expansions acquire a 3-adic meaning near the cusp ∞, and on E_q the subgroup μ_3 of cube roots of unity is a distinguished subgroup of order 3. The comparison of the algebraic and rigid analytic versions of this construction is in Conrad [12, Section 3.1].

The canonical subgroup (Katz [18, Ch. 3]). On an ordinary curve, among the four subgroups of order 3 there is exactly one that reduces to the kernel of Frobenius (the "infinitesimal" part of the 3-torsion); it is the *canonical subgroup*. On the Tate curve it is μ_3. Katz showed that it still exists, continuously, slightly into the supersingular region. In the coordinate x: on the ordinary disc $|x|_3 \leq 1$ (containing the cusp ∞, i.e. the Tate curve with $C = \mu_3$) the subgroup C is canonical; on the other disc it is not.

p-adic and overconvergent forms, intuitively. A 3-adic modular form (Serre, Katz) is, roughly, a 3-adic limit of classical q-expansions; geometrically it is a function (more precisely a section of a power of $\underline{\omega}$, the bundle whose sections of degree k are weight-k forms) on the ordinary disc $|x|_3 \leq 1$. It is *overconvergent* if it extends to a slightly larger region, a strict neighbourhood $|x|_3 < 3^r$, $r > 0$, reaching into the supersingular annulus.

Example 17.19 ($G_5 + \eta_5$ as a limit of classical forms)**.** This is Serre's construction, which we use only as motivation. For even $k \geq 2$, the classical weight-k Eisenstein series on $\Gamma_0(3)$ with the divisors divisible by 3 removed has coefficients $\sigma^{(3)}_{k-1}(n) = \sum_{a|n, 3\nmid a} a^{k-1}$. Along $k_N = 2 \cdot 3^N - 4$ one has $a^{k_N - 1} = a^{-5} a^{2 \cdot 3^N}$, and $a^{2 \cdot 3^N} \equiv 1 \pmod{3^{N+1}}$ for $3 \nmid a$ (Euler's theorem). So $\sigma^{(3)}_{k_N-1}(n) \to \sigma^{(3)}_{-5}(n)$ 3-adically: for instance $\min_{n \leq 40} v_3(\sigma^{(3)}_{k_N-1}(n) - \sigma^{(3)}_{-5}(n)) = 2, 3, 4, 5$ for $N = 1, 2, 3, 4$ ($k_N = 2, 14, 50, 158$). The constant terms $-(1 - 3^{k_N - 1}) B_{k_N}/(2k_N)$ of these Eisenstein series converge to $\zeta_3(5)/2 = \eta_5$: that is route (i) of Chapter 3. So $\eta_5 + G_5$ is a 3-adic limit of classical forms of weights $k_N \to -4$; it has "weight -4".

Theorem 17.20 (Coleman; Coleman–Mazur; [note, Theorem F.20])**.** *Let $p > 2$. If $\kappa(a) = \langle\langle a \rangle\rangle^k \chi(a)$ with $k \in \mathbb{Z}$ and χ a finite-order character of $\mathbb{Z}_p^\times$ with $\chi(-1) = 1$, then $G^*_\kappa(q) = \zeta^*(\kappa)/2 + \sum_{n \geq 1} \sigma^*_\kappa(n) q^n$ is the q-expansion of an overconvergent modular form of weight k on $\Gamma_1(\mathrm{lcm}(p, f_\chi))$ with character $\chi\omega^{-k}$ [10, Section B1], [11, Corollary 2.2.6].*

Here ω is the Teichmüller character, $\langle\langle a \rangle\rangle = a/\omega(a)$, $\sigma^*_\kappa(n) = \sum_{a|n, p\nmid a} \kappa(a) a^{-1}$, and ζ^* is Coleman's p-adic zeta function. The note applies it with $p = 3$, $\kappa(a) = a^{-4}$: since ω has order 2 at $p = 3$ (Chapter 3), $a^{-4} = \langle\langle a \rangle\rangle^{-4}$, so $k = -4$, $\chi = \mathbf{1}$; the level is $\Gamma_1(3)$ with character $\omega^4 = \mathbf{1}$, i.e. $\Gamma_0(3)$; $\sigma^*_\kappa(n) = \sum a^{-5} = \sigma^{(3)}_{-5}(n)$, and $\zeta^*(\kappa) = L_3(5, \mathbf{1}) = \zeta_3(5)$. Hence [note, (F.21)]

$$G^*_{-4} = \eta_5 + \sum_{n \geq 1} \sigma^{(3)}_{-5}(n) q^n = \eta_5 + G_5(q)$$

is overconvergent of weight -4. The note remarks that Coleman states this theorem with a sketch of proof, and that Coleman and Mazur give a complete proof for the characters trivial on $\mu(\mathbb{Z}_3) = \{\pm 1\}$. The character $a \mapsto a^{-4}$ is one of them, since $(-1)^{-4} = 1$.

Intuition: why the constant must be η_5. The constant term of an Eisenstein series is not free: classically, $G_k = \zeta(1-k)/2 + \sum \sigma_{k-1}(n) q^n$ is modular only with this constant. Chapter 16 showed that $G_5 + c$ is modular of weight -4 "up to period polynomials" for every c; 3-adically, overconvergence singles out exactly one c, the 3-adic zeta value. Changing c adds $c' B^2 \cdot$ (weight -4 constant), and the constant function 1 is not an overconvergent form of weight -4; this is why in Example 17.16 only $c = \eta_5$ shows the decay.

Lemma 17.21 ([note, Lemma F.22])**.** *The operator $U_3 : \sum a_n q^n \mapsto \sum a_{3n} q^n$ fixes G^*_{-4}.*

Proof. $\sigma^{(3)}_{-5}(3n) = \sigma^{(3)}_{-5}(n)$: the divisors of $3n$ prime to 3 are exactly those of n prime to 3. The constant term is unchanged. □

For example, $\sigma^{(3)}_{-5}(6) = \sigma^{(3)}_{-5}(2) = \frac{33}{32}$ and $\sigma^{(3)}_{-5}(30) = \sigma^{(3)}_{-5}(10) = \frac{51579}{50000}$.

Theorem 17.22 (Buzzard; [note, Theorem F.23])**.** *Let p be prime, $N \geq 5$ prime to p, $k \in \mathbb{Z}$. Let $X_1(N; p)$ be the modular curve of level $\Gamma_1(N) \cap \Gamma_0(p)$ and $W_0(p) \subset X_1(N; p)^{\mathrm{an}}$ the complement of the ordinary component containing the cusp 0. If f is an overconvergent modular form of level N and weight k which is an eigenvector of U_p with nonzero eigenvalue, then f extends to a section of $(\underline{\omega}^{\mathrm{an}})^{\otimes k}$ on $W_0(p)$ [6, Theorem 5.2(2)].*

Intuition: analytic continuation by a functional equation. The operator U_p comes from a correspondence: it averages f over the p points $(E/D, \dots)$ obtained by dividing E by the subgroups $D \neq C$ of order p. Dividing by a non-canonical subgroup moves a point towards the ordinary region. So the eigen-equation $f = \lambda^{-1} U_p f$ expresses the value of f at a point through its values at points closer to where f is already known to be defined; iterating the equation continues f step by step through the whole supersingular annulus, up

to (but not into) the other ordinary component. This is how we understand the mechanism of [6]; it is an intuition, not a summary of the proof. Lemma F.22 says that G^*_{-4} satisfies this equation with $\lambda = 1$.

17.3.4 Proposition F.24 in outline

Proposition 17.23 ([note, Proposition F.24]). *$H_{\eta_5} = B^2(G_5(q(x)) + \eta_5)$ and all $D^i H_{\eta_5}$ converge on $|x|_3 < 3^6$; hence (17.7) holds.*

The note's argument, in outline:

1. Buzzard's theorem needs tame level $N \geq 5$. So pass to $X_1(5;3)$ with the forgetful map $\pi_5 : (E, \iota, C) \mapsto (E, C)$ to $X_0(3)$, finite flat of some degree δ, with a trace Tr satisfying $\mathrm{Tr} \circ \pi_5^* = \delta$.
2. Membership in $W_0(3)$ depends only on (E, C) (supersingular, or ordinary with C canonical); by Lemma 17.18 it is the disc $|x|_3 < 3^6$ on $X_0(3)$, and its preimage W_5 is Buzzard's $W_0(3)$ on $X_1(5;3)$.
3. By Theorem 17.20, G^*_{-4} is overconvergent of weight -4; its pullback is overconvergent of level 5, with the same q-expansion, hence (by Lemma 17.21 and the q-expansion principle) a U_3-eigenvector with eigenvalue 1.
4. Theorem 17.22 extends it to a section ϕ of $\underline{\omega}^{\otimes -4}$ on W_5.
5. Multiply by $\pi_5^*(B^2)$, a classical form of weight 4 (Chapter 16), to obtain a function $\tilde{\mathcal{H}}$ on W_5; its normalized trace $\mathcal{H} = \delta^{-1}\mathrm{Tr}\,\tilde{\mathcal{H}}$ is a rigid analytic function on the disc $|x|_3 < 3^6$, i.e. a power series in x converging there.
6. Near the cusp ∞, $\mathcal{H} = B^2 G^*_{-4}$, which in the Tate parameter is $B^2(q)(G_5(q) + \eta_5)$ with $x = x(q)$, i.e. $H_{\eta_5}(x)$. By uniqueness of Taylor expansions, H_{η_5} is the expansion of $\mathcal{H}$ on the whole disc. The elliptic point inside the disc does not matter because $\mathcal{H}$ is a function on the coarse curve.
7. D preserves convergence on an open disc, and convergence on the closed disc of radius $3^{6-\epsilon}$ gives (17.7).

The published inputs, exactly as the note lists them, none of which the note proves or checks:

- Theorem 17.20 (Coleman [10, Section B1]; complete proof for these characters in Coleman–Mazur [11, Corollary 2.2.6]);
- Theorem 17.22 (Buzzard [6, Theorem 5.2(2)]), including that his setting covers $p = 3$ and the reduction to auxiliary level [6, Section 3];
- that membership in $W_0(3)$ depends only on (E, C), via Katz's canonical subgroup [18, Ch. 3], [6, Sections 3–4];
- the agreement of the algebraic and rigid Tate curves [12, Section 3.1];
- that Coleman's overconvergence at tame level 1 pulls back to Buzzard's notion at level 5;
- the q-expansion principle on the ordinary component of the cusp ∞;
- and, in Lemma 17.18, the textbook fact that 0 is the only supersingular j-invariant in characteristic 3 [31, Theorem V.4.1(c) and its proof].

Calegari uses the same description of the ordinary locus of $X_0(3)$ for $\zeta_3(3)$ [7, Section 3].

Remark on the note: estimate (i) rests on a chain of research-level black boxes. The note states the hypotheses of [note, Theorems F.20 and F.23] and takes these theorems, together with the four facts listed after [note, Proposition F.24], from the literature without checking their proofs. Of these, the compatibility of Coleman's notion of overconvergence (tame level 1) with Buzzard's (level 5) and the identification of the trace with H_{η_5} on the whole disc are the steps whose details rest most on rigid geometry; the note gives each in one or two sentences. The coefficients of Example 17.16 ($v_3([x^n]H_{\eta_5}) - 6n \in [-25, -4]$ for $n \leq 129$) are consistent with the conclusion, but finitely many coefficients say nothing

about the radius of convergence.

17.3.5 The gain: Proposition F.26

Proposition 17.24 ([note, Proposition F.26])**.** *If $\eta_5 \in \mathbb{Q}$, then for every $0 < \epsilon < 6$, $v_3(\mathcal{D}_d(\eta_5)) \geq 15(6-\epsilon)d^2 - 5\Theta_\epsilon d$.*

The note's argument, with the counting in full. (1) The entry $M_{\lambda,(i,k)}$ is the coefficient of index $n = \lambda - k$ of g_i, and $n \geq 1$ since $\lambda \geq d > k$. By (17.7) its valuation is $\geq (6-\epsilon)(\lambda-k) - \Theta_\epsilon$. (2) A term of the Leibniz expansion of $\det M$ is a product of $5d$ entries, one from each row λ and one from each column (i,k), matched by a permutation. Its valuation is at least

$$\sum_{\text{pairs}} \big((6-\epsilon)(\lambda-k) - \Theta_\epsilon\big) = (6-\epsilon)\Big(\sum_{\lambda\in I_d}\lambda - \sum_{(i,k)} k\Big) - 5d\,\Theta_\epsilon \ ,$$

the same for every permutation, since each row and each column appears once. By the ultrametric inequality the determinant has at least this valuation. (3) I_d consists of $5d$ distinct integers $\geq d$, so their sum is at least that of the smallest possible choice $d, d+1, \dots, 6d-1$: $\sum_{n=d}^{6d-1} n = \frac{(6d-1)6d}{2} - \frac{(d-1)d}{2} = \frac{35d^2-5d}{2}$. (4) The columns: k runs over $0,\dots,d-1$ for each of the 5 values of i, so $\sum k = 5\cdot\frac{d(d-1)}{2} = \frac{5d^2-5d}{2}$. (5) The difference is $\frac{35d^2-5d-5d^2+5d}{2} = 15d^2$. □

Example 17.25 (the gain for $d = 1, 2, 3$)**.** With $c = \eta_5^{\mathrm{tr}}$ (exact for valuations below 799) the jumps are $0,\dots,6d-1$, so $\sum_{I_d}\lambda - \sum k = 15d^2$ exactly $(15, 60, 135)$, and one finds $v_3(\mathcal{D}_d) = 53,\ 263,\ 635$, against $6\cdot 15d^2 = 90,\ 360,\ 810$. For $d = 1$ this can be seen by hand from Example 17.14: $v_3(\mathcal{D}_1) = v_3(288) + \sum_{\lambda=1}^{5} v_3(h_\lambda) = 2 + (2+5+11+14+19) = 53$, and $\sum(6\lambda - v_3(h_\lambda)) = 4+7+7+10+11 = 39$ is the "$5d\Theta$" loss at $d = 1$. For comparison, $c = \frac{1}{2}$ gives $v_3(\mathcal{D}_d) = 6, 22, 57$ (Example 17.15).

17.4 The primes $\ell \neq 3$

Throughout, $\nu_\ell = -v_\ell(\mathcal{D}_d)$, the number of factors ℓ in the denominator (negative if ℓ divides the numerator). Goal: $\sum_{\ell\neq 3}\nu_\ell \log\ell \leq \frac{13289}{168}d^2 + o(d^2)$.

17.4.1 Where denominators come from

B and $q(x)$ have integer coefficients (Chapter 16), so all denominators of H_c come from c and from $G_5 = \sum_{3\nmid a} a^{-5}q^a/(1-q^a)$: the term with a contributes a^{-5} from x^a on. Splitting off the terms with $\ell \mid a$,

$$G_5 = G_5^{[\ell]} + \ell^{-5}G_5(q^\ell) \ ,$$

where $G_5^{[\ell]}$ is ℓ-integral (its coefficients have no ℓ in the denominator). In Example 17.1, 5^5 enters at x^5 ($400000 = 2^7\cdot 5^5$).

The crude bound [note, (F.45)]. $[x^n]G_5(q(x))$ involves $\sigma_{-5}^{(3)}(m)$ only for $m \leq n$, so $b_c\,\mathrm{lcm}(1,\dots,n)^5[x^n]H_{\eta_5} \in \mathbb{Z}$, where b_c is the denominator of η_5; D multiplies by integers. Every entry of M thus has denominator dividing $b_c\,\mathrm{lcm}(1,\dots,N_d)^5$, and each of the $5d$ rows of M can be cleared separately, so

$$\nu_\ell \leq 5d(v_\ell(b_c) + 5\lfloor \log N_d/\log\ell\rfloor) \ . \tag{17.8}$$

By hand, for $d = 3$, $c = \frac{1}{2}$ ($b_c = 2$, $N_3 = 88$): the bound is $15(1+5\cdot 6) = 465$ for $\ell = 2$, 150 for $\ell = 5$ and $\ell = 7$; the actual values (Example 17.15) are 159, 60, 55. In particular $\nu_\ell \leq 0$ for $\ell > N_d$, $\ell \nmid b_c$. As computed in Section 17.1, this bound alone would cost about $150d^2$; it is used only for the *small primes* ($\ell = 2$, $\ell \mid b_c$, $\ell \leq \sqrt{N_d}$), whose total is $O(d^{3/2}\log d)$.

From now on $\ell \geq 5$ is a *large prime*: $\ell^2 > N_d$, $c \in \mathbb{Z}_{(\ell)}$ (no ℓ in the denominator of c).

17.4.2 The Eisenstein series $E_{\ell-1}$ and Lemma F.27

The key to the denominators is that $u = DB/B$ is, modulo ℓ, the logarithmic derivative of a rational function. The source is the Eisenstein series of weight $\ell - 1$ on $\mathrm{SL}_2(\mathbb{Z})$,

$$E_{\ell-1} = 1 - \frac{2(\ell-1)}{\beta_{\ell-1}} \sum_{n\geq 1} \sigma_{\ell-2}(n) q^n \ ,$$

with the Bernoulli number $\beta_{\ell-1}$. By von Staudt–Clausen (Chapter 3), $v_\ell(\beta_{\ell-1}) = -1$, so the factor $2(\ell-1)/\beta_{\ell-1}$ is divisible by ℓ, and $E_{\ell-1} \equiv 1 \pmod{\ell}$ coefficientwise.

Example 17.26 ($E_{\ell-1} \equiv 1$)**.** $\beta_4 = -\frac{1}{30}$, $\beta_6 = \frac{1}{42}$, $\beta_{10} = \frac{5}{66}$, $\beta_{12} = -\frac{691}{2730}$ have $v_\ell = -1$ for $\ell = 5, 7, 11, 13$, and the coefficients $-2(\ell-1)/\beta_{\ell-1}$ are $240 = 5 \cdot 48$, $-504 = -7 \cdot 72$, $-264 = -11 \cdot 24$, $\frac{65520}{691} = 13 \cdot \frac{5040}{691}$, each with $v_\ell = 1$.

Intuition. $E_{\ell-1}$ is a modular form of weight $\ell - 1$ which is $\equiv 1$ modulo ℓ: modulo ℓ, it looks like a "constant of weight $\ell - 1$". (It reduces to the Hasse invariant; this is the role it plays in [note, Lemma F.27].) Dividing it by $B^{(\ell-1)/2}$, of the same weight, gives a function on $X_0(3)$, i.e. a rational function of x; modulo ℓ, this rational function is $B^{-(\ell-1)/2}$. Taking logarithmic derivatives: modulo ℓ, $u = D \log B$ is $-\frac{2}{\ell-1}$ times the logarithmic derivative of a rational function.

Lemma 17.27 ([note, Lemma F.27])**.** *Let $s = \lfloor (\ell-1)/3 \rfloor$. Then $E_{\ell-1}(q(x))/B^{(\ell-1)/2} = Q_\ell(x)/P^s$ with $Q_\ell \in \mathbb{Z}_{(\ell)}[x]$, $Q_\ell(0) = 1$, $\deg Q_\ell = s$, leading coefficient $27^s(-3)^{(\ell-1)/2}$. The function $r = -\frac{2}{\ell-1} D \log(Q_\ell/P^s)$ has only simple poles, at the roots of Q_ℓ and at x_e, is bounded at ∞ and lies in $\mathbb{Z}_{(\ell)}[[x]]$, and $\xi = (u - r)/\ell \in \mathbb{Z}_{(\ell)}[[x]]$.*

The note's argument, step by step. This is the invariance-plus-pole-counting technique of Chapter 16. (1) $E_{\ell-1}/B^{(\ell-1)/2}$ has weight 0 on $\Gamma_0(3)$, so it is a rational function of x. (2) Its only poles in $\mathbb{H}$ are at zeros of B, i.e. at the elliptic orbit, where $B^{(\ell-1)/2}$ vanishes to order $\ell - 1$ in $\tau - \tau_e$; since $x - x_e$ vanishes to order 3, the pole has order at most $\lfloor (\ell-1)/3 \rfloor = s$ in $x - x_e$. (3) At $x = 0$ the value is 1. (4) At $x = \infty$ (the cusp 0), using $E_{\ell-1}(-1/(3\tau)) = (3\tau)^{\ell-1} E_{\ell-1}(3\tau)$ and $B(-1/(3\tau)) = -3\tau^2 B(\tau)$, the value tends to $3^{\ell-1}(-3)^{-(\ell-1)/2} = (-3)^{(\ell-1)/2}$, finite. (5) So $Q_\ell = P^s E_{\ell-1}/B^{(\ell-1)/2}$ has no poles, i.e. is a polynomial, of degree $\leq s$; its leading coefficient is 27^s times the value $(-3)^{(\ell-1)/2}$ of $E_{\ell-1}/B^{(\ell-1)/2}$ at $x = \infty$, nonzero, so the degree is exactly s. Its Taylor series is ℓ-integral because $E_{\ell-1}(q(x))$ and B^{-1} are. (6) $D \log(Q_\ell/P^s) = D \log E_{\ell-1}(q(x)) - \frac{\ell-1}{2} u$, so $u - r = \frac{2}{\ell-1} D \log E_{\ell-1}(q(x))$. Since $E_{\ell-1}(q(x)) = 1 + \ell y$ with y integral, $D \log(1 + \ell y) = \ell \, Dy/(1 + \ell y) \in \ell \mathbb{Z}_{(\ell)}[[x]]$. □

Example 17.28 (Q_5, Q_7, Q_{11}, Q_{13})**.** Computing $P^s E_{\ell-1}(q(x))/B^{(\ell-1)/2}$ as a series to x^{39}, one finds that all coefficients beyond x^s vanish and

$$Q_5 = 1 + 243x, \qquad Q_7 = 1 - 486x - 19683x^2, \qquad Q_{11} = 1 - 243x - 137781x^2 - 4782969x^3,$$
$$Q_{13} = 1 + \tfrac{90396}{691}x + 196830x^2 + 19131876x^3 + 387420489x^4,$$

with leading coefficients $243 = 27 \cdot 9$, $-19683 = 27^2(-27)$, $-4782969 = 27^3(-243)$, $387420489 = 3^{18} = 27^4 \cdot 3^6$, as predicted. Also r and $\xi = (u - r)/\ell$ are ℓ-integral through x^{39} for these four primes.

17.4.3 Lemma F.29: Q_ℓ is squarefree modulo ℓ

Lemma 17.29 ([note, Lemma F.29])**.** *$\bar{Q}_\ell \in \mathbb{F}_\ell[x]$ has degree s, is squarefree and prime to $\bar{P}$. Hence Q_ℓ has s distinct ℓ-integral roots, different from 0 and x_e.*

The note's argument, step by step. (1) Modulo ℓ, $E_{\ell-1} \equiv 1$, so $\bar{B}^{(\ell-1)/2} = \bar{P}^s/\bar{Q}_\ell$, and $\frac{2}{\ell-1} \equiv -2$ (as $\ell - 1 \equiv -1$). Hence $\bar{u} = D\log\!\left(\bar{Q}_\ell^2/\bar{P}^{2s}\right)$, and the Riccati identity $2Du + u^2 = V$ of Chapter 16 reduces to [note, (F.30)] $2D\bar{u} + \bar{u}^2 = \bar{V} = 24x/\bar{P}^2$. (2) Let α be a root of $\bar{Q}_\ell$ of multiplicity μ, $1 \le \mu \le s < \ell$; $\alpha \neq 0$ since $Q_\ell(0) = 1$; $t = x - \alpha$. (3) If $\bar{P}(\alpha) \neq 0$: $\bar{u} = x \cdot 2\mu/t + O(1) = 2\mu\alpha/t + O(1)$, and $D\bar{u} = (\alpha + t)\frac{\mathrm{d}}{\mathrm{d}t}(2\mu\alpha/t) + \cdots = -2\mu\alpha^2/t^2 + O(1/t)$. The coefficient of t^{-2} in $2D\bar{u} + \bar{u}^2$ is $-4\mu\alpha^2 + 4\mu^2\alpha^2 = 4\mu(\mu-1)\alpha^2$. $\bar{V}$ is regular at α, so this vanishes; as $\alpha \neq 0$ and $1 \le \mu < \ell$, $\mu = 1$. (4) If $\alpha = x_e$: now $\bar{P}$ also vanishes there, $\bar{u} = \rho x_e/t + O(1)$ with $\rho = 2\mu - 2s$, and the same computation gives the t^{-2} coefficient $(\rho^2 - 2\rho)x_e^2$. On the other side $\bar{V} = 24x/(27t)^2 = \frac{24x_e}{729}t^{-2} + \cdots = -\frac{8}{9}x_e^2 t^{-2} + \ldots$ (using $x_e = -\frac{1}{27}$). So $\rho^2 - 2\rho + \frac{8}{9} = 0$, i.e. $(3\rho - 2)(3\rho - 4) = 0$ in $\mathbb{F}_\ell$. (5) With $\mu = s + \rho/2$: $\rho = \frac{2}{3}$ gives $3\mu = 3s + 1$, $\rho = \frac{4}{3}$ gives $3\mu = 3s + 2$. If $\ell = 3s + 1$, these say $\mu \equiv 0$, resp. $3\mu \equiv 1$, i.e. $\mu \equiv 2s+1$ (as $3(2s+1) = 2\ell+1$). If $\ell = 3s+2$: $3\mu \equiv -1$, i.e. $\mu \equiv 2s+1$ (as $3(2s+1) = 2\ell-1$), resp. $\mu \equiv 0$. Neither 0 nor $2s + 1$ lies in $[1, s]$ modulo ℓ (note $2s + 1 < \ell$). So x_e is not a root. (6) The leading coefficient is a unit, so $\deg \bar{Q}_\ell = s$ and the roots of Q_ℓ are integral and reduce to the s distinct roots of $\bar{Q}_\ell$. □

Example 17.30 (the reductions)**.** $\bar{Q}_5 = 3(x + 2)$; $\bar{Q}_7 = x^2 + 4x + 1$ (irreducible over $\mathbb{F}_7$); $\bar{Q}_{11} = 7(x + 1)(x + 2)(x + 4)$; $\bar{Q}_{13} = (x^2 + 3x + 1)(x^2 + 7x + 1)$. In each case $\gcd(\bar{Q}_\ell, \bar{Q}'_\ell) = 1$ (squarefree) and $\gcd(\bar{Q}_\ell, \bar{P}) = 1$. Also $2Dr + r^2 \equiv V \pmod{\ell}$ through x^{39} for all four primes.

17.4.4 The Sym^4 congruence: Proposition F.31

Put $T_m = (\theta^m G_5)(q(x)^\ell)$. The coefficient of Y^n in $\theta^m G_5(Y)$ is $n^m \sigma_{-5}^{(3)}(n)$, ℓ-integral for $n < \ell$; and $q(x)^\ell$ starts at x^ℓ; so T_m is ℓ-integral below x^{ℓ^2}. Also $DT_m = \ell B^{-1} T_{m+1}$ because $D\log q(x) = B^{-1}$.

Proposition 17.31 ([note, Proposition F.31])**.** *With* $C_{m,j} = \binom{m+j}{m}\frac{(4-m)!}{(4-m-j)!\,2^j}$ *and* $b_n = \sum_{m+j=n} C_{m,j}\xi^j B^{2-m} T_m$ *(*$0 \le n \le 4$*), for* $0 \le i \le 4$ *one has the exact identity*

$$\ell^5 D^i H_c = \sum_{n=0}^{i} \ell^n \, N_{i,n}(r)\, b_n + \ell^5 \mathcal{E}_i \,, \qquad \mathcal{E}_i = D^i\Big(B^2(G_5^{[\ell]} + c)\Big) \in \mathbb{Z}_{(\ell)}[[x]] \,, \tag{17.9}$$

and every b_n *is* ℓ*-integral below* x^{ℓ^2}*.*

What it says. Multiply the germs by ℓ^5 to clear the worst denominators. Then, modulo ℓ^j, the combination $\ell^5 \sum_i a_i D^{i-1} H_c$ depends on the coefficients a_i only through the j rational functions $F_0(a), \ldots, F_{j-1}(a)$, where

$$F_n(a) = \sum_{i=1}^{5} a_i \, N_{i-1,n}(r) = a_{n+1} + \sum_{i>n+1} a_i N_{i-1,n}(r) \,, \tag{17.10}$$

because the n-th term of (17.9) carries a factor ℓ^n [note, (F.35)]. The functions $N_{i,n}$ are the polynomials of Chapter 16 [note, (F.8)], evaluated at the rational function r in place of the series u.

Why. (1) $\ell^5 H_c = B^2 T_0 + \ell^5 B^2(G_5^{[\ell]} + c)$. (2) By [note, Lemma F.9(a)] (Chapter 16), $D^i(B^2 T_0) = \sum_m N_{i,m}(u) B^{2-m} \ell^m T_m$ (each θ acting on $G_5(q^\ell)$ produces a factor ℓ). (3) Substitute $u = r + \ell\xi$ and Taylor-expand the polynomial $N_{i,m}$ in its first argument: $N_{i,m}(r + \ell\xi) = \sum_j \frac{(\ell\xi)^j}{j!}\partial_u^j N_{i,m}(r)$. (4) By [note, Lemma F.9(c)], $\partial_u N_{i,m} = c_m N_{i,m+1}$ with $c_m = \frac{(m+1)(4-m)}{2}$, so $\frac{1}{j!}\partial_u^j N_{i,m} = C_{m,j} N_{i,m+j}$ with $C_{m,j} = \frac{1}{j!}\prod_{t=m}^{m+j-1} c_t$; the product is $\frac{(m+j)!}{m!} \cdot \frac{(4-m)!}{(4-m-j)!} \cdot 2^{-j}$, and dividing it by $j!$ gives the closed form. (5) Collect the powers $\ell^{m+j} = \ell^n$. The "Sym^4" in the name is the $\mathfrak{sl}_2$ structure of the coefficients c_m (Chapter 16): shifting u by $\ell\xi$ is a translation acting on binary quartics. Yi's preprint [35, (27)] states the analogous congruence for weight -2 and three germs on $X_0(7)$ [35, (27)].

17.4.5 Smith normal form, from scratch

To count factors of ℓ in a determinant one uses the Smith normal form over the ring $\mathbb{Z}_{(\ell)}$ of rationals without ℓ in the denominator. In that ring a number is a unit (invertible) exactly when its numerator is also prime to ℓ, so every nonzero element is ℓ^e times a unit.

Fact 17.32 (Smith normal form)**.** *Every square matrix A over $\mathbb{Z}_{(\ell)}$ with $\det A \neq 0$ can be written $A = U\,\mathrm{diag}(\ell^{e_1},\dots,\ell^{e_n})\,V$ with U, V invertible over $\mathbb{Z}_{(\ell)}$ and $0 \le e_1 \le \cdots \le e_n$. The e_i (valuations of the* elementary divisors*) are unique, and $v_\ell(\det A) = \sum e_i$.*

Algorithm (and proof of existence). Choose an entry of smallest valuation and move it to position $(1,1)$ by swapping rows and columns. Every other entry of its row and column is a $\mathbb{Z}_{(\ell)}$-multiple of it (its valuation is at least as large), so subtracting multiples of the first row and column clears them. Repeat on the remaining block.

Example 17.33 (a 2×2 case)**.** Over $\mathbb{Z}_{(2)}$, $A = \left(\begin{smallmatrix} 2 & 4 \\ 6 & 8 \end{smallmatrix}\right)$. The entry 2 has the smallest 2-valuation, 1. Row 2 minus 3×row 1 gives $\left(\begin{smallmatrix} 2 & 4 \\ 0 & -4 \end{smallmatrix}\right)$; column 2 minus 2×column 1 gives $\left(\begin{smallmatrix} 2 & 0 \\ 0 & -4 \end{smallmatrix}\right)$. So $(e_1, e_2) = (1, 2)$, and $\det A = -8$ has $v_2 = 3 = 1 + 2$. Interpretation: the solutions of $Aa \equiv 0 \pmod{2^j}$ for $a \in \mathbb{Z}_{(2)}^2$, reduced modulo 2, form a space of dimension $\#\{i : e_i \ge j\}$: 2 for $j = 1$, 1 for $j = 2$, 0 for $j = 3$.

Apply this to $A = \ell^5 M$, which is ℓ-integral by (17.9) (its entries are coefficients below x^{N_d}, and $N_d < \ell^2$). With $h_j = \#\{i : e_i < j\}$ and $\det A = \ell^{25d}\mathcal{D}_d$ [note, (F.34)]:

$$\nu_\ell = -v_\ell(\mathcal{D}_d) = 25d - \sum_i e_i \le \sum_i \max(0, 5 - e_i) = \sum_{j=1}^{5} h_j \ .$$

The last equality counts, for each i, the number of $j \in \{1,\dots,5\}$ with $e_i < j$.

17.4.6 Proposition F.36, Lemma F.38, Lemma F.39 and the layer theorem

Proposition 17.34 ([note, Proposition F.36])**.** *For $1 \le j \le 5$, $h_j \le \min\big(5d,\ \#\{\lambda \in I_d : \lambda \ge \ell\},\ \sum_{n<j} \dim F_n(K_n)\big)$, where $K_n = \{a \in \mathbb{Q}[x]^5_{<d} : F_0(a) = \cdots = F_{n-1}(a) = 0\}$.*

Why. $h_j = 5d - \dim \bar{S}_j$, where $\bar{S}_j$ is the reduction modulo ℓ of $\{a : Aa \equiv 0 \bmod \ell^j\}$ (as in Example 17.33). *Kernel bound:* every a in K_j (with ℓ-integral entries) satisfies $Aa \equiv 0 \bmod \ell^j$, because in (17.9) only the terms $n \ge j$ survive, each with a factor ℓ^n, and $F_n(a)$, b_n, $\mathcal{E}_i$ are ℓ-integral; so $\dim \bar{S}_j \ge \dim K_j$ and $h_j \le 5d - \dim K_j = \mathrm{rank}(F_0,\dots,F_{j-1}) = \sum_{n<j} \dim F_n(K_n)$. *Row bound:* the rows $\lambda < \ell$ of A are $\equiv 0 \bmod \ell^5$, since the coefficients of H_c up to $x^{\ell-1}$ involve no a^{-5} with $\ell \mid a$; so modulo ℓ^j at most $\#\{\lambda \ge \ell\}$ rows are nonzero, and h_j is at most that.

Lemma 17.35 (weight count; [note, Lemma F.38])**.** *One has*

$$F_n(\mathbb{Q}[x]^5_{<d}) \subseteq (PQ_\ell)^{-(4-n)}\,\mathbb{Q}[x]_{\le d-1+(4-n)(s+1)} \ ,$$

a space of dimension $d + (4-n)(s+1)$.

Why. $N_{i-1,n}$ is isobaric of weight $i - 1 - n$ in r (weight 1) and D^jV (weight $2 + j$) ([note, Lemma F.9(b)]). r has simple poles at the $s+1$ roots of PQ_ℓ; D^jV has a pole of order $2 + j$ at x_e only; all are bounded at ∞. A monomial of weight w therefore has at most a pole of order w at each root of PQ_ℓ, so $(PQ_\ell)^w N_{i-1,n}(r)$ is a polynomial of degree $\le w(s+1)$.

Lemma 17.36 (local lemma; [note, Lemma F.39])**.** *For a root α of Q_ℓ and $a \in K_j$ $(0 \le j \le 4)$:* $\mathrm{ord}_\alpha F_j(a) \ge 2j - 4$.

Outline of the note's argument. Near α (a simple root, not 0 or x_e), $r = w + \tilde{r}$ with $w = \rho_\alpha/t$ and $\tilde{r}$ regular. The Taylor formula of the previous subsection, now in w, turns (F_m) into a binary quartic: with $f_m = F_m/((4-m)!2^m)$ and $f(Z) = \sum f_m Z^m$, one gets $f(Z) = \tilde{f}(Z+w)$, a translation by w. The hypothesis $a \in K_j$ says $f_0 = \cdots = f_{j-1} = 0$, i.e. Z^j divides f. Writing $y = tZ + \rho_\alpha$ and $\hat{f}(y) = t^4\tilde{f}(y/t)$, this becomes divisibility of a polynomial in y with coefficients in $\mathbb{C}[[t]]$ by $(y-\rho_\alpha)^j$, and comparing degrees in y with powers of t shows that the low powers of t cannot occur, giving $f_j = O(t^{2j-4})$. So a pole of order up to $4-n$ at α (allowed by the weight count) is reduced to $\max(0, 4-2n)$, and for $n \geq 3$ becomes a zero of order $2n-4$.

Theorem 17.37 (layer theorem; [note, Theorem F.40])**.** *For the large primes,* $\dim F_n(K_n) \leq \mathcal{L}_n$ *with* $\mathcal{L}_n = d + (4-n) + (4-2n)s$ *for* $n = 0, 1, 2$, $\mathcal{L}_3 = \max(0, d+1-2s)$, $\mathcal{L}_4 = \max(0, d-4s)$*; hence* $h_j \leq \min(5d, \#\{\lambda \in I_d : \lambda \geq \ell\}, \mathcal{L}_0 + \cdots + \mathcal{L}_{j-1})$.

Why. For $a \in K_n$, $F_n(a)$ has a pole of order $\leq 4-n$ at x_e, of order $\leq \max(0, 4-2n)$ at each of the s roots of Q_ℓ (distinct by Lemma 17.29; Lemma 17.36), no other finite pole, and grows at most like x^{d-1}. For $n \leq 2$, $P^{4-n}Q_\ell^{4-2n}F_n(a)$ is then a polynomial of degree $\leq d-1+(4-n)+(4-2n)s$: dimension $\leq \mathcal{L}_n$. For $n=3$, $PF_3(a)$ is a polynomial of degree $\leq d$ divisible by Q_ℓ^2 (zeros of order ≥ 2): dimension $\leq d+1-2s$. For $n=4$, $F_4(a) = a_5$ has degree $< d$ and is divisible by Q_ℓ^4: dimension $\leq d-4s$.

Example 17.38 (the dimensions, computed)**.** Build $N_{i,n}$ by the recursion [note, (F.8)] and substitute $u = r$ and $V = 24x/P^2$. Then $(PQ_\ell)^{4-n}N_{i,n}(r)$ is indeed a polynomial (Lemma 17.35), and $\dim F_n(K_n)$, computed as successive rank increments of the stacked maps $(F_0, \ldots, F_n)$, is:

ℓ	s	d	$\dim F_n(K_n)$, $n = 0, \ldots, 4$	layer bounds $\mathcal{L}_n$	(weight count)
7	2	3	$15, 0, 0, 0, 0$	$15, 10, 5, 0, 0$	$(15, 12, 9, 6, 3)$
7	2	8	$20, 14, 6, 0, 0$	$20, 15, 10, 5, 0$	$(20, 17, 14, 11, 8)$
11	3	3	$15, 0, 0, 0, 0$	$19, 12, 5, 0, 0$	$(19, 15, 11, 7, 3)$
11	3	8	$24, 16, 0, 0, 0$	$24, 17, 10, 3, 0$	$(24, 20, 16, 12, 8)$
13	4	3	$15, 0, 0, 0, 0$	$23, 14, 5, 0, 0$	$(23, 18, 13, 8, 3)$
13	4	8	$28, 12, 0, 0, 0$	$28, 19, 10, 1, 0$	$(28, 23, 18, 13, 8)$

All dimensions respect the layer bounds, which are attained for $n = 0$ at $d = 8$. (The layer theorem is a statement about rational functions, valid for every d; the condition $\ell^2 > N_d$ matters only for its use in Proposition 17.34.)

Example 17.39 (elementary divisors against the bound)**.** For $c = \frac{1}{2}$ and $d = 3$ ($N_3 = 88$, so every $\ell \geq 11$ is large) we compute the Smith form of $\ell^5 M$ over $\mathbb{Z}_{(\ell)}$ for $\ell = 11, \ldots, 83$. For $\ell = 11$: $h_j = 7$ for $j = 1, \ldots, 5$, $\nu_{11} = 35$, and the bound of Theorem 17.37 is 35: attained, through the row count (there are 7 rows $\lambda \in \{11, \ldots, 17\}$). For $\ell = 13$: $\nu = 25$, bound 25. For $\ell = 17$: $\nu = 4 \leq \sum h_j = 5 =$ bound. For $\ell \geq 19$ there are no rows $\lambda \geq \ell$ and $\nu_\ell \leq 0$ ($\nu_{83} = -2$: 83^2 divides the numerator). For $d = 2$: $\nu_{11} = 5 =$ bound, and 0 beyond. At these small d the row count is the binding term; the layer bounds bind only when ℓ is small compared to d, which is where most of the integral below comes from.

17.4.7 The sum over primes: Proposition F.42

Proposition 17.40 ([note, Proposition F.42])**.** *If* $\eta_5 \in \mathbb{Q}$, *then* $\sum_{\ell \neq 3} \nu_\ell \log \ell \leq \left(\int_0^6 \Psi\right) d^2 + o(d^2)$ *with*

$$\Psi(z) = \sum_{j=1}^{5} \min\Big(\mathrm{rc}(z),\ \sum_{n<j} \Lambda_n(z)\Big), \qquad \mathrm{rc}(z) = \min(5, (6-z)^+),$$

$(\Lambda_0, \ldots, \Lambda_4) = (1 + \frac{4}{3}z,\ 1 + \frac{2}{3}z,\ 1,\ (1 - \frac{2}{3}z)^+,\ (1 - \frac{4}{3}z)^+)$, *and* $\int_0^6 \Psi = \frac{13289}{168}$.

Intuition. Measure primes in units of d: $z = \ell/d$. A prime $\ell \approx zd$ costs at most $d\Psi(z)$ factors of ℓ. rc is the normalized row count ($5d$ rows, of which about $6d - \ell$ have $\lambda \geq \ell$), and $\Lambda_n = \mathcal{L}_n/d$ (with $s \approx \ell/3$). Then $\sum_\ell d\Psi(\ell/d)\log\ell$ is a Riemann sum: by the prime number theorem the primes near zd have density $1/\log\ell$, and the weight $\log\ell$ cancels it, so the sum is $\approx \int d\Psi(z)\,\mathrm{d}(zd) = d^2\int\Psi$.

The note's argument, step by step. (1) Small primes: (17.8), total $O(d^{3/2}\log d)$. (2) Large primes: $\nu_\ell \leq \sum_{j=1}^5 h_j$ and Theorem 17.37. (3) The row count: by (17.6), $\#\{\lambda \in I_d : \lambda \geq \ell\} \leq \#\{j \leq 6d-1 : j+70 \geq \ell\} \leq (6d-\ell)^+ + 70$. (4) $|s - \ell/3| \leq 1$ gives $\mathcal{L}_n \leq d\Lambda_n(\ell/d) + 4$: e.g. $\mathcal{L}_0 = d + 4 + 4s \leq d(1 + \frac{4}{3}\frac{\ell}{d}) + 4$; $\mathcal{L}_4 = \max(0, d - 4s) \leq \max(0, d - \frac{4}{3}\ell + 4)$. (5) Hence, in each of the five minima, the second argument exceeds its normalized value by at most 70 and the third by at most 20, so each minimum exceeds the normalized one by at most 70, and $\nu_\ell \leq d\Psi(\ell/d) + 350$. (6) Summation: $\vartheta(X) = \sum_{\ell\leq X}\log\ell = X + o(X)$ (prime number theorem, Chapter 7) and partial summation with the continuous piecewise linear Ψ give $\sum_{\ell<N_d} d\Psi(\ell/d)\log\ell = d^2\int_0^6\Psi + o(d^2)$, and $\sum_{\ell<N_d} 350\log\ell = O(d)$. □

Example 17.41 (computing Ψ and its integral)**.** On $[0, \frac{3}{4}]$: rc $= 5$, and the partial sums are $S_1 = 1 + \frac{4}{3}z$, $S_2 = 2 + 2z$, $S_3 = 3 + 2z$, $S_4 = 4 + \frac{4}{3}z$, $S_5 = 5$. Each is ≤ 5 there (e.g. $S_4 \leq 5$ iff $z \leq \frac{3}{4}$), so $\Psi = 15 + \frac{20}{3}z$. Continuing in the same way at the kinks $z = \frac{3}{4}$ (Λ_4 hits 0 and S_4 hits 5), 1 (rc starts to drop), $\frac{4}{3}$, $\frac{15}{7}$, one gets the note's [note, (F.44)]:

$$\Psi = 15 + \tfrac{20}{3}z,\ 16 + \tfrac{16}{3}z,\ 21 + \tfrac{1}{3}z,\ 25 - \tfrac{8}{3}z,\ 30 - 5z \quad \text{on} \quad [0,\tfrac{3}{4}],[\tfrac{3}{4},1],[1,\tfrac{4}{3}],[\tfrac{4}{3},\tfrac{15}{7}],[\tfrac{15}{7},6].$$

Evaluating Ψ in exact fractions from its definition, with the breakpoints found as intersections of the linear pieces, confirms [note, (F.44)]; the values at the breakpoints are $\Psi(0), \Psi(\frac{3}{4}), \Psi(1), \Psi(\frac{4}{3}), \Psi(\frac{15}{7}), \Psi(6) = 15, 20, \frac{64}{3}, \frac{193}{9}, \frac{135}{7}, 0$, and integrating exactly (trapezoids are exact for linear functions) gives

$$\int_0^6 \Psi = \frac{13289}{168} = 79.1011905\ .$$

By hand, piece by piece: $13.125 + 5.1667 + 7.1296 + 16.486 + 37.19 \approx 79.10$.

Remark 17.42 (the pessimistic variant; [note, Remark F.46])*.* Without the local lemma and the layer theorem, only the weight count gives $\Lambda_n = 1 + \frac{4-n}{3}z$. Then $\int_0^6\Psi = \frac{33569}{420} = 79.9261905$, and the margin $\frac{177}{2}\log 3 - \frac{33569}{420} - 16.6040183 = 0.69698$, still positive. So the local lemma is not needed for the conclusion; it more than doubles the margin.

What just happened. Denominators come only from a^{-5} with $\ell \mid a$ in G_5. Since $E_{\ell-1} \equiv 1 \pmod\ell$, modulo ℓ the series u becomes the logarithmic derivative r of the rational function Q_ℓ/P^s, whose $s \approx \ell/3$ zeros are simple. Expanding in powers of ℓ, the matrix $\ell^5 M$ modulo ℓ^j only sees the rational functions $F_0(a), \ldots, F_{j-1}(a)$, whose poles are counted by weight and by the local lemma. The Smith normal form turns these dimension counts into a bound for ν_ℓ, and summing over primes with the prime number theorem gives $\frac{13289}{168}d^2$.

17.5 The archimedean estimate

17.5.1 Jensen's formula

Theorem 17.43 (Jensen's formula)**.** *Let ψ be holomorphic on a neighbourhood of $|q| \leq r$, $\psi(0) \neq 0$, with zeros $a_1, \ldots, a_m$ in $|q| < r$ and none on $|q| = r$. Then*

$$\int_0^{2\pi} \log\left|\psi(re^{i\vartheta})\right| \frac{\mathrm{d}\vartheta}{2\pi} = \log|\psi(0)| + \sum_{k=1}^m \log\frac{r}{|a_k|}\ .$$

In particular $\log|\psi(0)| \le$ *the mean of* $\log|\psi|$ *on the circle (Jensen's inequality). (E.g. Ahlfors,* Complex Analysis*, or any complex analysis text.)*

Intuition. $\log|\psi|$ is the electrostatic potential of unit point charges at the zeros of ψ (in two dimensions, $\log|q-a|$ is the Coulomb potential), plus a harmonic part. The mean value of a harmonic function on a circle is its value at the centre; a charge inside the circle contributes $\log r$ to the circle mean instead of $\log|a|$ at the centre, which is Gauss's law. Each zero inside makes the circle mean larger than the value at 0.

Example 17.44. $\psi(q) = (q-0.3)(q+0.5i)(2-q)$, $r = 0.8$: zeros 0.3, $-0.5i$ inside, 2 outside. Numerical quadrature gives a circle mean of 0.246860077931526; the right side is $\log 0.3 + \log\frac{0.8}{0.3} + \log\frac{0.8}{0.5} = -1.2039728 + 0.9808293 + 0.4700036 = 0.246860077931526$.

17.5.2 The idea, and the measure μ

The leading Taylor coefficient of a combination $\mathcal{F}$ of germs is $\psi(0)$ for $\psi(q) = \mathcal{F}(x(q))/q^n$, and Jensen's inequality bounds it by the mean of $\log|\mathcal{F}(x(q))|$ on a circle $|q| = r$ in the q-disc, plus $n\log(1/r)$. The germs are evaluated as functions of q (they are meromorphic on $|q|<1$, with poles only at zeros of B, which a fixed polynomial $\Pi(q)$ clears), so the x-series need not converge there. The size of the polynomial coefficients $a_j(x)$ on the image curve $x(|q|=r)$ is controlled by a potential. The note uses several circles $|q| = r_i = e^{-2\pi y_i}$ with weights ω_i, the pushforward measures μ_i (normalized arc length on the circle, transported to the x-plane by $x(q)$), their mixture $\mu = \sum\omega_i\mu_i$, and its logarithmic potential $\mathcal{P}_\mu(z) = \int\log|z-w|\,\mathrm{d}\mu(w)$ and energy $I = \iint\log|z-w|\,\mathrm{d}\mu\,\mathrm{d}\mu$ (these notions are explained in Chapter 10; note the sign convention: here I is the integral of $+\log$).

[note, Lemma F.47]: $\mathcal{P}_\mu$ is continuous and I is finite. *Why:* near a point of a circle, $x(q)-x(q_0)$ is an m_0-th power of a local coordinate, so the μ-mass of a small disc of radius ϱ is at most $C\varrho^{1/m_1}$; a logarithm integrated against such a measure converges uniformly.

17.5.3 Leading coefficients and the Gram determinant

[note, Lemma F.48]: if a source vector of norm one (in the norm below) has image $\mathcal{F} = \mathfrak{c}_n x^n + O(x^{n+1})$, then for every circle i

$$\log|\mathfrak{c}_n| \le dW_i + 2\pi n y_i + d\,m_\mu(h) + C_h\ , \qquad W_i = \int\mathcal{P}_\mu\,\mathrm{d}\mu_i\ . \tag{17.11}$$

The norm on polynomials of degree $<d$ is $\|a\|_d^2 = \int_\Omega|a|^2e^{-2d\mathcal{P}_\mu}\mathrm{d}A$ over a disc Ω containing the curves. *The key inequalities:* (a) sub-mean value property of $|a_j|^2$ on a small disc of radius h: $|a_j(z)| \le (\pi h^2)^{-1/2}e^{d(\mathcal{P}_\mu(z)+m_\mu(h))}\|a_j\|_d$, with m_μ a modulus of continuity of $\mathcal{P}_\mu$ (Lemma F.47); (b) Cauchy–Schwarz over the six blocks, with fixed bounds for Πg_j; (c) Jensen's inequality for $\psi = \Pi\,\mathcal{F}(x(q))/q^n$ on $|q| = r_i$, whose $\log r_i = -2\pi y_i$ gives the term $2\pi n y_i$, while the circle mean of $\mathcal{P}_\mu(x(q))$ is W_i.

The Gram determinant [note, (F.49)]: the Gram matrix $\mathcal{G}_d$ of $1, z, \dots, z^{d-1}$ in this norm satisfies, by Andréief's identity (Chapter 9),

$$\det\mathcal{G}_d = \frac{1}{d!}\int_{\Omega^d}\prod_{i<j}|z_i-z_j|^2e^{-2d\sum_i\mathcal{P}_\mu(z_i)}\prod_i\mathrm{d}A(z_i)\ ,$$

a two-dimensional Coulomb gas of d charges in the external field $2d\mathcal{P}_\mu$.

Lemma 17.45 (energy inequality; [note, Lemma F.50])**.** *For every probability measure* ν *on* Ω*:* $I(\nu) - 2\int\mathcal{P}_\mu\,\mathrm{d}\nu \le -I$.

Why: with $\sigma = \nu - \mu$ (total mass 0) the claim is $I(\sigma) \le 0$; and the energy of a signed measure of total mass zero is $-\frac{1}{2\pi}\int |\nabla \mathcal{P}_\sigma|^2 \le 0$, the electrostatic field energy with the sign of our convention. This is [30, Lemma I.1.8] applied to $\nu - \mu$, in our sign convention; the note includes a proof by smoothing. *Example* (using the standard fact that the uniform measure on $|z| = R$ has potential $\log\max(R, |z|)$): for μ uniform on the unit circle, $I = 0$; ν uniform on $|z| = \frac{1}{2}$ gives $I(\nu) - 2\int \mathcal{P}_\mu \mathrm{d}\nu = \log\frac{1}{2} - 0 = -0.693 \le 0$, and ν uniform on $|z| = 2$ gives $\log 2 - 2\log 2 = -0.693 \le 0$; equality only for $\nu = \mu$.

[note, Lemma F.51]: $\limsup_d d^{-2}\log\det \mathcal{G}_d \le -I$. *Why:* the integrand of the Gram formula is at most $e^{d^2(I(\nu_d) - 2\int \mathcal{P}_\mu \mathrm{d}\nu_d) + O(d)}$ for the empirical measure ν_d of the charges (with a truncation of log near the diagonal), and Lemma 17.45 bounds the exponent by $-Id^2$.

Example 17.46 (the Gram bound for the unit circle)**.** For μ uniform on $|z| = 1$ ($\mathcal{P}_\mu = \log\max(1, |z|)$, $I = 0$) and Ω the disc of radius 2, rotation invariance makes $\mathcal{G}_d$ diagonal with entries $2\pi\big(\frac{1}{2b+2} + \int_1^2 \rho^{2b+1-2d}\mathrm{d}\rho\big)$. Numerically, $d^{-2}\log\det\mathcal{G}_d = 0.0664,\ -0.0148,\ -0.0038$ for $d = 10, 100, 1000$, approaching the bound $-I = 0$.

Proposition 17.47 ([note, Proposition F.52])**.** $\limsup_d d^{-2}\log|\mathcal{D}_d(c)| \le U(\mu) = \int_0^6 \min_i\,(W_i + 2\pi y_i k)\mathrm{d}k - 3I$.

Why. Take an orthonormal basis $v_0, \dots, v_{6d-1}$ of the source adapted to the jumps, $\Phi_d(v_j) = \mathfrak{c}_j x^{\lambda_j} + \dots$. In it the coefficient matrix on the rows λ_j is triangular with diagonal $\mathfrak{c}_j$, each bounded by (17.11) with $n = \lambda_j$. The change of basis from monomials to the v_j has $|\det| = (\det\mathcal{G}_d)^{-1/2}$ per block, $(\det\mathcal{G}_d)^{-3}$ for six blocks. So [note, (F.53)]

$$\log|\mathcal{D}_d| \le 3\log\det\mathcal{G}_d + \sum_{j=0}^{6d-1} \min_i\,(dW_i + 2\pi y_i\lambda_j) + 6d^2 m_\mu(h) + O_h(d)\ .$$

With $\lambda_j = j + O(1)$, the sum is a Riemann sum for $d^2\int_0^6 \min_i(W_i + 2\pi y_i k)\,\mathrm{d}k$ ($k = j/d$), and Lemma F.51 bounds the first term by $-3Id^2$. In words: the leading coefficients pay $W_i + 2\pi y_i k$ per unit, choosing the best circle for each k (large circles, i.e. small y_i, for large k, and small circles for small k, since $2\pi y_i k$ is the Cauchy factor r_i^{-k}); the Gram determinant gives back $3I$.

17.5.4 The kernel formula: Lemma F.54

Lemma 17.48 ([note, Lemma F.54])**.** *With Euler's function φ, the mutual energy of the circle measures of y and y' is*

$$\mathcal{I}(y, y') = -2\pi\min(y, y') + \sum_{j\ge1,\ 9j^2yy'<1} \frac{4\pi\varphi(3j)}{9j^2}\Big(\arccos a_j - a_j\sqrt{1 - a_j^2}\Big), \qquad a_j = 3j\sqrt{yy'}\ .$$

Euler's function $\varphi(n)$ counts the integers in $[1, n]$ prime to n; e.g. $\varphi(3) = 2$, $\varphi(6) = 2$, $\varphi(9) = 6$, $\varphi(12) = 4$.

Outline of the proof. Fix $w = x(e^{2\pi i\tau})$, $\tau = u_0 + iy$. Since x is a coordinate on $X_0(3)$, the solutions of $x(q) = w$ in the disc are the $e^{2\pi i\gamma\tau}$, one for each coset $\gamma \in \Gamma_\infty\backslash\Gamma_0(3)$: the identity, and one for each primitive bottom row $(3j, m)$, $\gcd(3j, m) = 1$, with $\operatorname{Im}\gamma\tau = y/((3ju_0 + m)^2 + 9j^2y^2)$. Jensen's formula on $|q| = e^{-2\pi y'}$ gives

$$\int \log|x(q) - w|\frac{\mathrm{d}\vartheta}{2\pi} = \log|w| + \sum_\gamma 2\pi\big(\operatorname{Im}\gamma\tau - y'\big)^+\ ,$$

since a zero at height Y has $|q| = e^{-2\pi Y}$ and contributes $\log(r/|q|) = 2\pi(Y - y')$ when inside. Averaging over $u_0 \in [0, 1)$: the mean of $\log|w|$ is $-2\pi y$ (as $\log|x(q)/q|$ is harmonic and 0 at $q = 0$), which with the identity coset gives $-2\pi\min(y, y')$. For fixed j, substituting

$v = 3ju_0 + m$ and using that almost every real v lies in exactly $\varphi(3j)$ of the intervals $[m, m+3j]$ with $\gcd(3j, m) = 1$, the cosets contribute $\frac{\varphi(3j)}{3j} \int_{\mathbb{R}} \big(\frac{2\pi y}{v^2+9j^2y^2} - 2\pi y'\big)^+ \mathrm{d}v$, an elementary integral that gives the arccos term.

Example 17.49 (the kernel against a direct double integral)**.** Independently of the coset argument, one can evaluate $\iint \log|x(q) - x(q')|$ over the two circles directly, by a 3000×3000-point trapezoidal rule with offset grids, with $x(q)$ from the eta product:

(y, y')	terms j	formula	direct
$(\frac{1}{10}, \frac{1}{5})$	$j = 1, 2$	1.5375927001	1.537593
$(\frac{3}{20}, \frac{2}{5})$	$j = 1$	−0.252841124883	−0.252841
$(\frac{1}{4}, \frac{1}{4})$	$j = 1$	−0.937853715203	−0.937738

The off-diagonal pairs agree to all six printed digits; the self-energy, where the integrand is singular along the whole diagonal, agrees to $1.2 \cdot 10^{-4}$, as expected of the trapezoidal rule there.

17.5.5 The 34 circles of Table 3

The note chooses 34 circles with rational y_i (from 0.04811 to 2.36896), weights ω_i and segments $[\alpha_i, \beta_i]$ tiling $[0, 6]$ [note, Table 3]. On segment i it uses circle i instead of the minimum, which gives [note, (F.57)]

$$U(\mu) \le J - 3I \ , \qquad J = \sum_i \Big((\beta_i - \alpha_i) W_i + \pi y_i (\beta_i^2 - \alpha_i^2) \Big) \ ,$$
$$W_i = \sum_j \omega_j \mathcal{I}(y_i, y_j) \ , \qquad I = \sum_i \omega_i W_i \ .$$

Example 17.50 (evaluating I, J, U)**.** For the data of [note, Table 3], $\sum \omega_i = 1$ exactly, the segments tile $[0, 6]$, and each condition $9j^2 y_i y_j < 1$ can be decided exactly (the largest j needed is 6). The table below evaluates [note, (F.55)] in 40-digit floating point. This is *not* ball arithmetic: the result is not a certified bound, but it is far more precise than the digits compared.

	floating point	paper
I	2.3300529587286721031	2.3300529587…
J	23.594177094364057531	23.5941770943…
$U = J - 3I$	16.604018218178041221	$\le$ 16.6040183

Some potentials: $W_1 = 3.7210$ (the largest circle, $y_1 = 0.04811$), $W_{17} = 0.6749$, $W_{34} = -1.1069$. Replacing the segment assignment by the true minimum over the 34 circles (computed from the exact lower envelope of the 34 lines $W_i + 2\pi y_i k$) gives $U(\mu) = 16.6040182182$, only about $4 \cdot 10^{-13}$ below $J - 3I$: the note's segments are essentially optimal for this μ.

17.6 The final inequality

Collecting: (i) $v_3(\mathcal{D}_d) \log 3 \ge \frac{177}{2} \log 3 \cdot d^2 - O(d)$ with $\epsilon = \frac{1}{10}$; (ii) $\sum_{\ell \ne 3} v_\ell(\mathcal{D}_d) \log \ell \ge -\frac{13289}{168} d^2 - o(d^2)$; (iii) $\log|\mathcal{D}_d| \le U d^2 + o(d^2)$. By the product formula,

$$\Big(\tfrac{177}{2} \log 3 - \tfrac{13289}{168} - U \Big) d^2 \le o(d^2) \ .$$

The bracket is $97.2271875 - 79.1011905 - 16.6040183 = 1.5219788 > 1.52$ (with the note's rounded U), so, if the three estimates hold (estimate (i) rests on the published theorems

listed above), the inequality fails for large d, and η_5, hence $\zeta_3(5)$, could not be rational. With the pessimistic denominator count of Remark 17.42 the bracket is 0.69698, still positive. All margins are measured in nats per d^2.

Check yourself 17.51. For $d = 1$ and $c = \frac{1}{2}$, why does $(D-1)(D-2)(D-3)(D-4)H_c - 12$ vanish to order 5 at $x = 0$, and what would replace the 12 for a general c?

Answer. D multiplies x^n by n, so the operator multiplies $[x^n]H_c$ by $(n-1)(n-2)(n-3)(n-4)$, which is 0 for $n = 1, \dots, 4$ and 24 for $n = 0$. The constant term is $24\,[x^0]H_c = 24c$; so the combination is $(D-1)\cdots(D-4)H_c - 24c$, and $24c = 12$ for $c = \frac{1}{2}$.

Check yourself 17.52. Where does the Fricke involution $x \mapsto 3^{-6}/x$ send the ordinary disc $|x|_3 \le 1$, the supersingular annulus, and the disc $W_0(3)$?

Answer. $v_3(3^{-6}/x) = -6 - v_3(x)$. So $v \ge 0$ goes to $v \le -6$: the two ordinary discs are exchanged (as are the cusps, and the canonical and non-canonical subgroups); $-6 < v < 0$ goes to itself; and $W_0(3) = \{v > -6\}$ goes to $\{v < 0\}$, the complement of the ordinary disc of the cusp ∞.

Check yourself 17.53. Why is the local lemma not needed for the conclusion, and what would be lost without the Smith normal form, using only the crude bound (17.8)?

Answer. Without the local lemma the integral is $\frac{33569}{420}$ and the margin $0.697 > 0$ (Remark 17.42). With only the crude bound the denominators cost about $150d^2$ (Section 17.1), more than the gain of about $97d^2$, and the argument fails.

Summary of the chapter

The second proof assumes $\eta_5 = \zeta_3(5)/2 \in \mathbb{Q}$ and studies one rational number $\mathcal{D}_d$ at every place. It is the determinant of a $5d \times 5d$ matrix of Taylor coefficients of the germs $D^{i-1}H_c$, taken at the rows given by the jumps, and it is nonzero because the germs are independent over $\mathbb{C}(x)$ (no rational solution of $L_5 v = R_5$, by indicial polynomials; irreducible Sym^4 monodromy, by unipotent logarithms and the eigenvalues $12, 6, 0, -6, -12$) and because of the zero estimate $\mathrm{ord}_0 \le 6d + 69$, proved with a Wronskian-type determinant. At 3, published theorems of Coleman, Coleman–Mazur and Buzzard, with Katz's canonical subgroup and the Newton polygon of $j = (1 + 27x)(1 + 243x)^3/x$, give convergence of H_{η_5} on $|x|_3 < 3^6$ and hence $v_3(\mathcal{D}_d) \ge 15(6 - \epsilon)d^2 - O(d)$; these black boxes are quoted, not checked, by the note. At $\ell \ne 3$, $E_{\ell-1} \equiv 1 \pmod{\ell}$ makes u a logarithmic derivative of the rational function Q_ℓ/P^s modulo ℓ, and Smith normal forms with pole counting give $\frac{13289}{168}d^2$. Over $\mathbb{C}$, Jensen's formula on 34 circles in the q-disc and an energy inequality give $U = 16.604$.

Worked out explicitly in the examples: the indicial roots, the Sym^4 matrices, the zero-estimate determinant for $d = 1$, jumps and $\mathcal{D}_d$ for $d \le 3$ (jumps $\lambda_j = j$ in all cases), the formula for $v_3(j)$, the 3-adic decay $v_3([x^n]H_{\eta_5}) - 6n \in [-25, -4]$ for $n \le 129$, the polynomials Q_ℓ and their squarefreeness for $\ell \le 13$, dimension counts and elementary divisors against the layer bounds, the integrals $\frac{13289}{168}$ and $\frac{33569}{420}$, the kernel [note, (F.55)] against a direct double integral, and I, J, U for [note, Table 3], with final margin 1.522. Nothing from this chapter is used in other chapters; Section 15.5 compares the two proofs.

Appendix A

Glossary of symbols

Each symbol is listed with its meaning, the place where the note defines it, and the chapter of this companion that explains it. Symbols of the second proof are listed separately at the end.

symbol	meaning	note	here
Numbers and p-adic tools			
$v_p(x)$, $\lvert x\rvert_p$	exponent of p in x; $\lvert x\rvert_p = p^{-v_p(x)}$	§1	2
$\mathbb{Q}_p$, $\mathbb{Z}_p$, $\mathbb{Z}_p^\times$	p-adic numbers, integers ($v_p \geq 0$), units ($v_p = 0$)	—	2
$\mathbb{F}_p$	integers modulo p	§6	2
S	$3^{-1}\mathbb{Z}_3^\times = \{v_3 = -1\} = (\frac{1}{3} + \mathbb{Z}_3) \cup (\frac{2}{3} + \mathbb{Z}_3)$, the integration points	(2.8)	2
$v_p(F)$	Gauss valuation $\min_j v_p(f_j)$ of a polynomial	§1	2
$\lVert F\rVert_1$	sum of the absolute values of the coefficients	§1	2
$s_p(q)$	sum of the base-p digits of q; $v_p(q!) = (q - s_p(q))/(p-1)$	(4.4)	2
x^+, $[\,\cdot\,]$, $[z^a]F$	$\max(x, 0)$; indicator; coefficient of z^a	§1	7, 5
bit, trit	units $\log_2$ and $\log_3$; 1 trit $= \log_2 3 \approx 1.585$ bits	§1	1
Zeta values			
B_k, $B_k(x)$	Bernoulli numbers and polynomials	§2.1	3
ω, $\langle a\rangle$	Teichmüller character (± 1 at $p = 3$); $a/\omega(a)$	Thm 2.1	3
χ, $B_{k,\chi}$	Dirichlet character; generalized Bernoulli numbers	Thm 2.1	3
$L_p(s, \chi)$	Kubota–Leopoldt p-adic L-function	Thm 2.1	3
$\zeta_p(s)$, $\zeta_3(5)$	$L_p(s, \omega^{1-s})$; $\zeta_3(5) = L_3(5, \mathbf{1})$, of valuation -1	(2.4)	3
The integral and the functional			
$\int_{\mathbb{Z}_3} f(t)\,\mathrm{d}t$	Volkenborn integral, $\lim 3^{-N} \sum_{t<3^N} f(t)$	(2.5)	4
(V1)–(V3)	shift rule, values on $\binom{t}{c}$ and t^c, the bound $3M$	Lem 2.6	4
$\mathrm{HS}_3(k, M)$	harmonic sum produced by shifting the integral by k	(2.14)	4
972, 2916, -54	$4 \cdot 3^5$; $3 \cdot 4 \cdot 3^5$; coefficient of $\zeta_3(3)$	2.11, 2.19	4, 5
$(x)_n$	Pochhammer symbol $x(x+1)\cdots(x+n-1)$	(1.2)	5
$W(y)$	the weight: poles of order 4 at $y = -k$, triple zeros at $-(j + \frac{r}{3})$, zero at $-\frac{n}{2}$	(1.2)	5
$\mathcal{N}$, node k	$\{-n, \ldots, 2n\}$; the node k sits at $y = -k$	§2.2	5
$L(P)$	$\sum_{r=1,2} \int_{\mathbb{Z}_3} (PW)'(t + \frac{r}{3})\,\mathrm{d}t$	(1.3)	5
$\widetilde{W}_k$, $H_k[b]$, h_k	$z^4 W(-k+z)$; its Taylor coefficients; $h_k = H_k[0]$	(2.17), (2.18)	5
$P_a(k)$	Taylor coefficient $[z^a]P(-k+z)$	§2.2	5
$r_{k,i}$	coefficient of $(y+k)^{-i}$ in PW	(2.22)	5

symbol	meaning	note	here
$\beta_{k,a}$, $\alpha_{k,a}$, $c_{k,a}$	local constants; $c_{k,a} = \beta_{k,a} + X\alpha_{k,a}$	(2.20), (2.21), Def 2.23	5
$\beta(P)$, $\alpha(P)$	rational parts of $L(P) = \beta(P) + \zeta_3(5)\alpha(P)$	Lem 2.19	5
Hankel polynomial and criterion			
L_k, Λ	node functional; $\Lambda = \sum_k L_k = \beta + X\alpha$	(2.24)	6
$\Delta_K(X)$	Hankel polynomial $\det\big[\Lambda(y^{i+j})\big]_{i,j<K}$	(2.25)	6
C_k	4×4 matrix $[c_{k,a+b}]$, zero below the anti-diagonal	(2.27)	6
K, κ	size of the determinant; $\kappa = K/n$	§3	7
c_F, Q, N	content of F, primitive part, the integer $b^K Q(a/b)$	Lem 3.1	7
I_i, $\kappa_{1,i}$, $\kappa_{2,i}$	the five κ-intervals covering $[2.8, 3]$	(3.7)	7
$G(\kappa)$	gain constant $(10.5\kappa - \kappa^2/4)\log_2 3$	(3.6)	8
$F_i^\dagger$, c_i	size and denominator constants, bits per n^2	(5.10), (5.39)	10, 13
$K(n, p)$	K fixed by the auxiliary prime	(3.12)	14
Gain			
$\mathrm{Int}(S)$	polynomials with values in $\mathbb{Z}_3$ on S	§4	8
F_i, ν_i	integer-valued basis on S; $-v_3$ of its leading coefficient	(4.2)	8
$Q_r(t)$	unit series in the factorization of W on S	(4.5)	8
A_3, d_K	$9n + 3 + 3v_3(n!)$ trits per entry; degree bound $2K - 2 + 3n$	§4, proof of Thm 3.5	8
P_c, $\left\{ {i \atop m} \right\}$, $\psi(m)$	Mahler coefficients; Stirling numbers; $m + v_3(m!)$	App A	8
Heine expansion and size			
$V(w)$	Vandermonde product $\prod_{i<i'}(w_{i'} - w_i)$	App B	9
$\Lambda'^{\otimes s}$	tensor power of a functional	App B	9
profile $s = (s_k)$	occupation numbers of the nodes, $0 \le s_k \le 4$, $\sum s_k = K$	Prop 5.1	9
Q_s, $\mathrm{coef}_\lambda(s)$	cross factor and its coefficients	(5.3)	9
λ_k, m_μ	partitions per node; monomial symmetric polynomials	Prop 5.1; App B	9
$M_{k,\lambda}$, $C_k[R]$	local factor; minor of C_k with rows R	Prop 5.1	9
$x = k/n$, σ	rescaled position; density with $0 \le \sigma \le 4$, $\int \sigma = \kappa$	§5.1	10
$\mathcal{L}f$, $\langle f, g\rangle$	logarithmic potential; pairing	(5.4)	10
$\mathcal{V}$, I, O	external field $2\mathcal{L}\mathbf{1}_I - 4\mathcal{L}\mathbf{1}_O$; $I = (0,1)$, $O = [-1,0] \cup [1,2]$	(5.5)	10
$F[\sigma]$, P_σ, $\mathrm{gap}(\sigma)$	energy; first variation; duality gap	(5.6)	10
$B(d)$, $E_B(s)$	$\frac{1}{2}\log\big(1 + d^2\big)$; discrete energy	(B.7)	10
$w(\delta)$	modulus of continuity of $\mathcal{L}$	(B.15)	10
σ_0, m_0, σ_κ	trial density, its mass $\frac{463}{160}$, its rescaling	(5.9)	10
A_0, B_0, P_t, c_*	$\langle \sigma_0, \mathcal{V}\rangle$, $\langle \sigma_0, \mathcal{L}\sigma_0\rangle$, $\mathcal{V} + 2t\mathcal{L}\sigma_0$, threshold	App E	10
Denominators			
$\eta_p(k)$	$\max_{m \ne k} v_p(k - m)$	§5.2	11
e_p, f_p, T_p	local losses and the tree bound	(5.12), (5.14)	11
S_c	number of rows placed in the class c	(5.14)	11
D_k, μ_k	$-v_p(h_k)$; largest v_p of a root or pole of $\widetilde{W}_k$	(5.15), 5.16	11
$\mathfrak{l}_p$	$\lceil \log_p(6n) \rceil$	§5.2	11
$\vartheta(x)$	$\sum_{p \le x} \log p$	App C	11
single-level prime	$p \ge 5$ with $p^2 > 6n$	§5.3	12

symbol	meaning	note	here
o_k, g_k	number of partners; $[p \mid 2k-n]$	Def 5.20	12
VP_k, ρ_t	virtual poles $\rho_t = pt/3$	(5.21)	12
$\mathcal{Z}_k$, z_k, $\mu_{k,t}$	p-special triple zeros; $3\lvert\mathcal{Z}_k\rvert$; 0 if the virtual pole t is covered and alone at its node, 1 otherwise	Def 5.20	12
β^{HS}, β^{rest}	parts of β with and without $p \mid u$	§5.3	12
$\hat{v}_m(k)$	refined lower bound for $v_p(c_{k,m})$	(5.25)	12
f^+, V_c, ψ_c	relaxed local loss; class value; its Legendre-type transform	(5.29), (5.30)	13
λ, T_p^+	price per row; relaxed tree bound	Lem 5.28	13
ϱ, type τ	p/n; node data of a point of $\mathbb{R}/\varrho\mathbb{Z}$	§5.4	13
$\mathcal{B}$, cell, meas_τ	breakpoints $3j/N$; intervals between them; arc length of type τ	Lem 5.31	13
$g_{[a,b]}$, $\bar{g}_\nu$	circle-model bound; its corner maximum	(5.33), (5.37)	13
Non-vanishing			
R, L, U nodes	with partner $k-p$; the partners; without partner	§6.1	14
Ra, Rb, Rb_g, Rc, La, ...	node types	Table 2	14
N_{Ra}, N_{Rb}, N_{Rc}	numbers of Ra, Rb (with Rb_g), Rc nodes	(6.3)	14
Φ_k, $\phi_{k,b}$, Σ	the node at scale p; its coefficients; $\Sigma(w) = (\frac{1}{3}-w)^{-3} + (\frac{2}{3}-w)^{-3}$	(6.5), (6.6)	14
ε_k	unit $2h_k p^{D_k}$	Lem 6.7	14
$x = (R_x, j_x)$, E_x, T	conditions; dual Hermite basis; its matrix	Lem 6.12	14
Γ^β, Γ^α	Gram matrix in the basis E_x	(6.13)	14
ξ, ξ', θ_x, ω	leading part at the partner; weights; weighted valuation	(6.15), (6.16)	14
$\mathbb{Q}_p(\sqrt{p})$	ramified quadratic extension, $v_p(\sqrt{p}) = \frac{1}{2}$	§6.2	14
$A_\bullet$, B	ϕ-matrices; binomial matrix	(6.19)	14
Second proof			
$\mathbb{H}$, q, θ	upper half plane; $e^{2\pi i\tau}$; $q\,\mathrm{d}/\mathrm{d}q$	App F	16
$\Gamma_0(3)$, $X_0(3)$, τ_e	congruence subgroup; its curve (a sphere); elliptic point	F.5	16
x, $q(x)$, P, x_e	Hauptmodul $(\eta(3\tau)/\eta(\tau))^{12}$; inverse; $1+27x$; $-\frac{1}{27}$	(F.1); App F notation, F.5	16
B, D, u	weight-2 form $\theta \log x$; $x\,\mathrm{d}/\mathrm{d}x$; DB/B	(F.2)	16
G_5, H_c, η_5	Eichler integral; $B^2(G_5+c)$; $\zeta_3(5)/2$	(F.2), (F.3)	16
V, R_5	$24x/P^2$; $x(1+39x)/P^2$	F.7	16
$N_{i,m}$, L_5	coefficients of $D^i(B^2Y)$; the order-5 operator	(F.8), F.10	16
$g_0, \ldots, g_5$	germs 1, $D^{i-1}H_c$	(F.3)	17
λ_j, M, $\mathcal{D}_d$	jumps; coefficient matrix; its determinant	(F.17), (F.18)	17
$W_0(3)$	the disc $\lvert x\rvert_3 < 3^6$	F.19	17
G_{-4}^*, U_3	overconvergent form $\eta_5 + G_5$; the operator $a_n \mapsto a_{3n}$	(F.21), F.22	17
$E_{\ell-1}$, Q_ℓ, r, ξ	Eisenstein series; its polynomial; mod-ℓ model r of u; $\xi = (u-r)/\ell$	F.27	17

symbol	meaning	note	here
ν_ℓ, e_i, h_j	$-v_\ell(\mathcal{D}_d)$; Smith exponents; their counts	(F.34), F.36	17
$\mathcal{L}_n$, Ψ	layer bounds; normalized cost per prime	(F.41), (F.43)	17
μ, I, W_i, U	circle measures, energy, potentials, archimedean constant	F.47–F.52	17

Bibliography

[1] R. Apéry, Irrationalité de $\zeta(2)$ et $\zeta(3)$, Astérisque 61 (1979), 11–13, https://www.numdam.org/item/AST_1979__61__11_0/.

[2] T. M. Apostol, Modular Functions and Dirichlet Series in Number Theory, 2nd ed., Grad. Texts in Math. 41, Springer, New York, 1990, https://doi.org/10.1007/978-1-4612-0999-7.

[3] K. Ball and T. Rivoal, Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs, Invent. Math. 146 (2001), 193–207, https://doi.org/10.1007/s002220100168.

[4] F. Beukers, Irrationality of some p-adic L-values, Acta Math. Sin. (Engl. Ser.) 24 (2008), 663–686, https://doi.org/10.1007/s10114-007-1029-2; arXiv:math/0603277.

[5] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, J. Reine Angew. Math. 490 (1997), 101–127, https://doi.org/10.1515/crll.1997.490.101.

[6] K. Buzzard, Analytic continuation of overconvergent eigenforms, J. Amer. Math. Soc. 16 (2003), 29–55, https://doi.org/10.1090/S0894-0347-02-00405-8.

[7] F. Calegari, Irrationality of certain p-adic periods for small p, Int. Math. Res. Not. 2005, no. 20, 1235–1249, https://doi.org/10.1155/IMRN.2005.1235; arXiv:math/0408214.

[8] F. Calegari, V. Dimitrov and Y. Tang, The linear independence of 1, $\zeta(2)$, and $L(2, \chi_{-3})$, preprint (2024), arXiv:2408.15403.

[9] F. Calegari, V. Dimitrov and Y. Tang, Arithmetic holonomy bounds and effective Diophantine approximation, in: Proceedings of the International Congress of Mathematicians 2026, Vol. 3, SIAM (2026), 356–376, https://doi.org/10.1137/25M1806776; arXiv:2510.04156.

[10] R. F. Coleman, p-adic Banach spaces and families of modular forms, Invent. Math. 127 (1997), 417–479, https://doi.org/10.1007/s002220050127.

[11] R. Coleman and B. Mazur, The eigencurve, in: Galois Representations in Arithmetic Algebraic Geometry (Durham, 1996), London Math. Soc. Lecture Note Ser. 254, Cambridge Univ. Press, Cambridge, 1998, 1–114, https://doi.org/10.1017/CBO9780511662010.003.

[12] B. Conrad, Modular curves and rigid-analytic spaces, Pure Appl. Math. Q. 2 (2006), 29–110, https://doi.org/10.4310/PAMQ.2006.v2.n1.a3.

[13] Ch.-J. de la Vallée Poussin, Recherches analytiques sur la théorie des nombres premiers, Ann. Soc. Sci. Bruxelles 20 (1896), part 2, 183–256.

[14] F. Diamond and J. Shurman, A First Course in Modular Forms, Grad. Texts in Math. 228, Springer, New York, 2005, https://doi.org/10.1007/978-0-387-27226-9.

[15] A. Fauzan, $\zeta(5)$ is irrational, preprint dated 17 September 2026, Zenodo, https://doi.org/10.5281/zenodo.22826419.

[16] J. Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, Bull. Soc. Math. France 24 (1896), 199–220, https://doi.org/10.24033/bsmf.545.

[17] F. Johansson, Arb: efficient arbitrary-precision midpoint-radius interval arithmetic, IEEE Trans. Comput. 66 (2017), 1281–1292, https://doi.org/10.1109/TC.2017.2690633; arXiv:1611.02831.

[18] N. M. Katz, p-adic properties of modular schemes and modular forms, in: Modular Functions of One Variable III (Antwerp, 1972), Lecture Notes in Math. 350, Springer, Berlin, 1973, 69–190, https://doi.org/10.1007/978-3-540-37802-0_3.

[19] I. Kilani, $\zeta_2(7)$ is irrational via Hankel determinants, preprint dated 25 September 2026 and signed I. K., Zenodo, version 2 of 30 September 2026, https://doi.org/10.5281/zenodo.23058762 (all versions: https://doi.org/10.5281/zenodo.22961248).

[20] I. Kilani, On the irrationality of $\zeta_3(5)$, preprint dated October 2026, Zenodo, 7 October 2026, https://doi.org/10.5281/zenodo.23203596; Lean 4 formalization at https://github.com/Ijtihed/zeta3-5-lean, accessed 19 October 2026.

[21] S. Kintali, Irrationality of the 5-adic zeta value $\zeta_5(3)$, preprint dated 15 August 2026, https://shivakintali.github.io/papers/Zeta-5-3.pdf, accessed 4 October 2026.

[22] L. Lai, On the irrationality of certain 2-adic zeta values, Int. J. Number Theory 21 (2025), 207–235, https://doi.org/10.1142/S1793042125500113; arXiv:2304.00816.

[23] L. Lai, C. Lupu and J. Sprang, On the irrationality of certain p-adic zeta values, Res. Math. Sci. 12 (2025), no. 4, Paper No. 77, https://doi.org/10.1007/s40687-025-00559-x; arXiv:2505.23088.

[24] L. Lai and J. Sprang, Many p-adic odd zeta values are irrational, Michigan Math. J., advance publication (2026), https://doi.org/10.1307/mmj/20236490; arXiv:2306.10393.

[25] L. Lai, J. Sprang and W. Zudilin, A note on the irrationality of $\zeta_2(5)$, Int. Math. Res. Not. IMRN 2026, no. 16, rnag180, https://doi.org/10.1093/imrn/rnag180; arXiv:2505.05005.

[26] C. D. Long, Hybrid arithmetic holonomy and twenty-two individual p-adic zeta values, preprint dated 24 August 2026, https://github.com/octonion/p-adic-zeta-irrationality, accessed 19 October 2026.

[27] C. D. Long, Multiweight arithmetic holonomy and density-one irrationality of p-adic zeta values, preprint dated 26 August 2026, https://github.com/octonion/p-adic-zeta-density, accessed 19 October 2026.

[28] A. M. Robert, A Course in p-adic Analysis, Grad. Texts in Math. 198, Springer, New York, 2000, https://doi.org/10.1007/978-1-4757-3254-2.

[29] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962), 64–94, https://doi.org/10.1215/ijm/1255631807.

[30] E. B. Saff and V. Totik, Logarithmic Potentials with External Fields, Grundlehren Math. Wiss. 316, Springer, Berlin, 1997, https://doi.org/10.1007/978-3-662-03329-6.

[31] J. H. Silverman, The Arithmetic of Elliptic Curves, 2nd ed., Grad. Texts in Math. 106, Springer, New York, 2009, https://doi.org/10.1007/978-0-387-09494-6.

[32] G. Szegő, Orthogonal Polynomials, 4th ed., Amer. Math. Soc. Colloq. Publ. 23, Amer. Math. Soc., Providence, RI, 1975, https://doi.org/10.1090/coll/023.

[33] A. Volkenborn, Ein p-adisches Integral und seine Anwendungen I, Manuscripta Math. 7 (1972), 341–373, https://doi.org/10.1007/BF01644073.

[34] L. C. Washington, Introduction to Cyclotomic Fields, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997, https://doi.org/10.1007/978-1-4612-1934-7.

[35] T. Yi, A determinant argument for the irrationality of $\zeta_7(3)$. Proposed unconditional proof, preprint dated 15 September 2026, https://github.com/TaifengYi/zeta7-irrationality, accessed 4 October 2026.