THE DATA

Prerequisites. Cyclotomic fields: the degree of $\mathbb{Q}(\zeta_n)$, the splitting of primes in it, and the conductor–discriminant formula [Wa, Ch. 2–3]. The discriminant in a tower [Ne, Ch. III, §2]; finiteness of the class group [Ne, Ch. I, §6]. Quadratic reciprocity [IR, Ch. 5]. Chebyshev's function satisfies $\psi(u) \le 2u$ for $u \ge 1$ [RS, Thm. 12]. From the earlier chapters: the character χ_K and the weight $1 - \chi_K$ (Chapter 2), the infinite places of the CM field of Chapter 3 and the prime sums over them, sparse sets of places (Chapter 4), and the chain of $m \approx \sqrt{x}$ steps (Chapter 8).

Every later chapter of this part works with one collection of objects: two integers q_0 and d, a CM field E obtained by adjoining a root of unity to $\mathbb{Q}(\sqrt{-d})$, three scales $x < x_1 < b$, the number m of lifts, the ranks r and k and the step size t, a set of places of E with weights, and three large primes. This chapter lists them, checks that their sizes fit together, defines the direction amount, the main amount and the total remainder used in the later bounds, and states that such data exist for every large integer x. The spaces, forms and twists that the later chapters attach to the data are fixed in Chapter 34, *Spaces, forms and twists*. We write log for the natural logarithm.

33.1. The modulus and the prime d

How must d be chosen so that every prime dividing q_0 splits in $K = \mathbb{Q}(\sqrt{-d})$?

Definition 33.1.1. *Parameters* are natural numbers q_0 and d with $18480 \mid q_0$, d prime, $q_0 \mid 2(d+1)$ and $q_0 \nmid d+1$.

Let $K := \mathbb{Q}(\sqrt{-d}) \subset \mathbb{C}$, and let $\chi_K(n) := \left(\frac{n}{d}\right)$ be the Legendre symbol.

Problem 33.1.1. $18480 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Parameters satisfy $q_0 \ne 0$, $d \equiv q_0/2 - 1 \pmod{q_0}$ and $d \equiv 7 \pmod 8$. For $q_0 = 18480$ the least admissible d is 9239, and $\varphi(18480) = 3840$.

Problem 33.1.2. Let c, s be nonnegative integers. (i) Every prime $p \mid 3^c 2^s q_0$ divides $(d+1)/4$, and $\chi_K(p) = 1$. (ii) A prime p with $\chi_K(p) \ne 1$ satisfies $p \ge 13$.

Since $d \equiv 3 \pmod 4$, χ_K is the character of K (Problem 2.1.1), so the primes of Problem 33.1.2(i) split in K. For $d = 9239$ the least prime p with $\chi_K(p) = -1$ is 19.

33.2. The field and its places

For a nonnegative integer s let $\lfloor \log_3 s \rfloor$ be the floor logarithm (zero for $s = 0$), and

$$l_0(s) := 3^{\lfloor \log_3 s \rfloor + 4}, \qquad T(s) := 3^{\lfloor \log_3 s \rfloor + 5}\, 2^s, \qquad q_1 := q_0 T(s), \qquad q_2 := (q_0 d)^{s+6}.$$

Let $E = E_s := K(\zeta_{q_1})$, with ζ_{q_1} a primitive q_1-th root of unity, let Φ be the set of infinite places of E, $f := \#\Phi$, and let $\mathrm{rd}_E := |\mathrm{disc}\, E|^{1/[E:\mathbb{Q}]}$ be the root discriminant.

Date: November 26, 2026.

Fix an embedding $E \to \mathbb{C}$ over K. Composing it with the elements of $\mathrm{Gal}(E/K)$ gives a bijection between $\mathrm{Gal}(E/K)$ and Φ, through which Φ becomes a group; sending g to the unit u with $g(\zeta_{q_1}) = \zeta_{q_1}^u$ identifies it with $(\mathbb{Z}/q_1)^\times$. For $\nu \in \mathbb{Z}$ let $[\nu] \in \Phi$ be the place of $\nu \bmod q_1$ if $\gcd(\nu, q_1) = 1$, and the identity otherwise. The *class* of $\tau \in \Phi$ modulo $n \mid q_1$ is its image in $(\mathbb{Z}/n)^\times$. Let Φ_a be the set of places of class 1 modulo q_0.

Problem 33.2.1. $T(s) = 3l_0(s)2^s$, and $27s < l_0(s)$; if $s \geq 1$, then $l_0(s) \leq 81s$.

Problem 33.2.2. $\varphi(q_1) = T(s)\varphi(q_0)$, and $[E : K] = \varphi(q_1)$. Hence $f = T(s)\varphi(q_0)$, and exactly $T(s)$ places have class 1 modulo q_0, and exactly $T(s)$ have class -1.

Problem 33.2.3. $E \subset \mathbb{Q}(\zeta_{q_1 d})$, $q_1 d \mid q_2$, and $1 \leq \mathrm{rd}_E \leq q_1 d$. A prime $p \equiv 1 \pmod{q_1 d}$ splits completely in E.

Problem 33.2.4. For $s \geq 1$, $\mathrm{rd}_E \geq \mathrm{rd}_{\mathbb{Q}(\zeta_{2^s})} = 2^{s-1}$.

33.3. Scales, ranks and signs

Let γ be Euler's constant, $\mathrm{CS}(d) := \gamma - L'(1, \chi_K)/L(1, \chi_K)$, and

$$C := v_0 + (2d + 6) + q_0 + |\mathrm{CS}(d)| + \sum_w \big|\log|\Phi'_{q_0}(w)|\big|,$$

the sum over the primitive q_0-th roots of unity $w \in \mathbb{C}$, with Φ_{q_0} the cyclotomic polynomial, and $v_0 \geq 0$ the integer, depending only on q_0 and d, that the proof fixes for the integral vacuum (Chapter 34, Section 34.8). For a finite set $\mathcal{F} \subset \Phi$ and a nonnegative integer ℓ_0, call $\mathcal{F}$ *sparse up to* ℓ_0 if for every prime $\ell \leq \ell_0$ and all integers $0 < i < j < l_0(s)$ there are no $\sigma, \tau, \rho \in \mathcal{F}$, distinct or not, with $\tau/\sigma \equiv \pm\ell^i$ and $\rho/\sigma \equiv \pm\ell^j$ (the two signs independent) modulo the largest divisor of q_1 prime to ℓ. For $\kappa\colon \Phi \to \mathbb{Z}_{\geq 0}$, integers $m \geq 0$ and $M \geq 0$, and real L, let

$$L_-(\kappa, m, M, L) := \frac{m}{f} \sum_{\tau \in \Phi} \log \kappa(\tau) + (m - 1) \log \frac{M \mathrm{rd}_E}{2\pi} - \frac{15}{2} L,$$

with $\log 0 := 0$. It depends on s through Φ, f and rd_E.

Definition 33.3.1. *Data* for parameters (q_0, d) consist of the following.

1. Integers $x, x_1, b \geq 1$ with $10^{12} C \leq \log\log b$, $(\log b)^{100} \leq x$, $x^{10^6} \leq x_1$, $x_1^{10^6} \leq b$, and $(\log x_1)^6 \leq \log b$.
2. Integers $m, r, s \geq 0$ with $\sqrt{x} \leq m \leq 2\sqrt{x}$, $x^5 \leq r \leq 3x^5$, $m = 2^e$ and $s = 22e$ for some integer $e \geq 1$, $r = 3^{e'}$ for some integer $e' \geq 1$, $s \leq 32 \log x$, and $q_1 x_1 \mid b$, where $q_1 = q_0 T(s)$. The field is $E = E_s$.
3. A set $\Phi_b \subset \Phi$ of places of class -1 modulo q_0, with $T(s) \leq \#\Phi_b \log b$, sparse up to $(r + 1 - m) \cdot 5r$.
4. The weight $\kappa\colon \Phi \to \mathbb{Z}_{\geq 0}$: $\kappa(\tau) = b$ for $\tau \in \Phi_b$, and $\kappa(\tau) = \lfloor xb/x_1 \rfloor$ otherwise.
5. Distinct primes $p_0, p_1 \equiv 1 \pmod{q_2^2}$ in $[b^{10}, b^{11}]$, and $\alpha \in \mathcal{O}_K$ with $\alpha\bar{\alpha} = p_0 p_1$; let $\pi_M := \overline{\iota(\alpha)} \in \mathcal{O}_E$, where $\iota\colon \mathcal{O}_K \hookrightarrow \mathcal{O}_E$ is the inclusion.
6. A prime $N \equiv 1 \pmod{q_2^2}$ with $L_- \leq \log N \leq L_- + \sqrt{\log b}$, where $L_- := L_-(\kappa, m, p_0 p_1, \log b)$, and $\pi_N \in \mathcal{O}_E$ with $\pi_N \bar{\pi}_N = N$.

Write $a := xb$, $M := p_0 p_1$, $k := r + 1 - m$, $t := 5r$, and $n_j := k + j(t + 1)$ for nonnegative integers j. We call m the number of lifts, k the rank of the source and r the rank of the target, M the principal level and N the level.

Problem 33.3.1. $\log\log b \ge 10^{12}\cdot 18480$, and $\log b < x < x_1 < b$.

Problem 33.3.2. $m \ge 10000$, $2m \le r$, and $r/2 \le k \le r$; in particular $r+1 = k+m$ with $k \ge 1$.

Problem 33.3.3. $x^{11} \le T(s) \le x^{11}(\log b)^{1/5}$, and $x^{11}\varphi(q_0) \le f$.

The hermitian spaces $Y_0,\dots,Y_m$ form a chain over E. Section 34.3 specifies their adelic frames. For $0 \le j < m$ the Gram matrix of Y_j, in suitable coordinates, is the orthogonal sum of the identity matrix of size n_j and the matrix Σ_j of size $m-1-j$ with rows and columns indexed by $0,\dots,m-2-j$, whose (u,v) entry is 0 unless $u+v = m-2-j$, is 1 if $u+v = m-2-j$ and $u \ne v$, and is $-N$ if $u = v = (m-2-j)/2$. The space Y_m is the standard positive definite space of rank $n_m - 1$.

Problem 33.3.4. For $0 \le j \le m$, Y_j has rank $r + jt$ and exactly $\lfloor (m-j)/2 \rfloor$ negative eigenvalues at each infinite place. Y_0 is the orthogonal sum of the identity of size k, $m/2-1$ hyperbolic planes and $\langle -N\rangle$. Formally, for matrices defined in the same way with $m = 4$ (no data have $m = 4$), the numbers of negative eigenvalues of $Y_0,\dots,Y_4$ are $2,1,1,0,0$.

Write $\varrho := m/2 - 1$ for the number of hyperbolic planes displayed in the block Σ_0. Then $m = 2\varrho + 2$.

33.4. The weights and the two amounts

Let $\Lambda_K(\nu) := \Lambda(\nu)(1-\chi_K(\nu))$. For real y, $\sigma \in \Phi$ and integers $j \ge 0$ let

$$s_{\mathrm{fin}}(y,\sigma) := \sum_{\nu=1}^{a} \Lambda_K(\nu)\Big(\frac{y}{\nu} - \kappa([-\nu]\sigma)\Big)_+, \qquad s_\infty(j) := \log j! + j\log\frac{M}{\Omega},$$

where $\Omega := e^{\mathrm{CS}(d)}\,2\pi/\mathrm{rd}_E$ and $[-\nu]\sigma$ is the product in the group Φ. We call $s_\infty(j)$ the size of a derivative of order j, and use $s_{\mathrm{fin}}(\kappa(\sigma),\sigma)$ to measure its guaranteed divisibility when $j = \kappa(\sigma)$. The *direction amount* and the *main amount* are

$$h_{\mathrm{dir}} := \sum_{\sigma\in\Phi}\big(s_\infty(\kappa(\sigma)) - s_{\mathrm{fin}}(\kappa(\sigma),\sigma)\big), \qquad h_{\mathrm{main}} := mk\,h_{\mathrm{dir}}.$$

The *unit of error* is $U := fa\log^3 b$.

Definition 33.4.1. The *denominator budget* is $B := U/(mk) = fa\log^3 b/(mk)$.

With $c_1 := -1 - \mathrm{CS}(d)$, the *main prime sum* and the *total remainder* are

$$s_{\mathrm{main}} := a\Big(\log a - \frac{1}{f}\sum_{\tau\in\Phi}\log\kappa(\tau) + c_1\Big), \qquad \mathrm{rem} := \sum_{\tau\in\Phi_a}\big(s_{\mathrm{fin}}(a,\tau) - s_{\mathrm{main}}\big).$$

Chapter 3 expresses rem through remainders of prime sums in progressions.

Problem 33.4.1. $x_1 \mid a$, and $a/x_1 \le \kappa(\tau) \le b$ for every $\tau \in \Phi$.

Problem 33.4.2. Let $0 \le y \le a$. The term of $s_{\mathrm{fin}}(y,\sigma)$ at ν vanishes unless $\nu < x_1$, and $0 \le s_{\mathrm{fin}}(y,\sigma) \le 2y\sum_{\nu\le x_1}\Lambda(\nu)/\nu \le 2y(\log x_1 + 2) \le y\log b$.

Problem 33.4.3. $\Omega \le 1$, and $20\log b \le \log(M/\Omega) \le 23\log b$.

Problem 33.4.4. For integers $0 \le y \le a$, $20y\log b \le s_\infty(y) \le 25y\log b$. For every integer $y \ge 1$ there is a real λ_y such that

$$s_\infty(y) = y\log\frac{yM}{e\Omega} + \tfrac{1}{2}\log(2\pi y) + \frac{\lambda_y}{12y}, \qquad 0 < \lambda_y < 1.$$

Problem 33.4.5. For every $\tau \in \Phi$, $\kappa(\tau)\log b \le s_\infty(\kappa(\tau)) - s_{\mathrm{fin}}(\kappa(\tau),\tau) \le 25\kappa(\tau)\log b$. Hence $b\,\#\Phi_a \le h_{\mathrm{dir}} \le 25fb\log b$.

Problem 33.4.6. $h_{\mathrm{main}} \ge x^4 fa$.

Problem 33.4.7. With $\delta_b := \#\Phi_b/f$, $s_{\mathrm{main}} = a\big(\log x_1 - \delta_b\log(x_1/x) + c_1\big)$, and $1/(\varphi(q_0)\log b) \le \delta_b \le 1/\varphi(q_0)$.

33.5. The level primes

Problem 33.5.1. Let h be the class number of K, and let $p'_0,\dots,p'_h$ be distinct primes that split in K. Then there are $i \ne j$ and $\alpha \in \mathcal{O}_K$ with $\alpha\bar\alpha = p'_ip'_j$.

Problem 33.5.2. $\sqrt{-1} \in E$. For every prime $p \equiv 1 \pmod 4$ there exist $u, v \in \mathbb{Z}$ with $u^2 + v^2 = p$. The element $\pi := u + \sqrt{-1}\,v \in \mathcal{O}_E$ satisfies $\pi\bar\pi = p$.

Problem 33.5.3. Let $m \ge 2$, $L \ge 7$, $1 \le \kappa(\tau) \le e^L$ for all $\tau \in \Phi$, $e^{20L} \le M \le e^{22L}$ and $q_1 d \le e^L$. Then $mL \le L_-(\kappa, m, M, L) \le 24mL$.

Problem 33.5.4. For data, $b^{20} \le M \le b^{22}$, $m\log b \le \log N \le 30m\log b$, and $b < M < N$.

33.6. Existence

How should the scales be chosen, as functions of x, so that Definition 33.3.1(1)–(2) hold?

Problem 33.6.1. Let $x > 1$, let m be the least power of 2 with $m \ge \sqrt{x}$, and r the least power of 3 with $r \ge x^5$. Then $2 \le m < 2\sqrt{x}$ and $3 \le r < 3x^5$. If $c \ge 0$ and b is the least multiple of an integer $n \ge 1$ with $b > c$, then $b \le c + n$.

Problem 33.6.2. Fix parameters and $0 < \varepsilon < 1/100$, and for each x let $x_1 = \lfloor\exp(x^{\varepsilon/6})\rfloor$ and let b be an integer with $x^\varepsilon \le \log b \le x^\varepsilon + 1$. Then the five inequalities of Definition 33.3.1(1) hold for all large x. If instead $x_1 = \lfloor\exp(x^\beta)\rfloor$ with $\beta > \varepsilon/6$, then $(\log x_1)^6 > \log b$ for all large x. If instead $\varepsilon > 1/100$ and $x^\varepsilon \le \log b \le x^\varepsilon + 1$, then $(\log b)^{100} > x$ for all large x.

The other choices need more. The proof uses the following window theorem. Fix integers $n_0 \ge 1$ and $A \ge 0$ with $4 \mid n_0$. For every sufficiently large real w_0, every integer $v > 1$ with $n_0^v \le w_0^A$, and every real $u_0 \in [w_0, w_0^A]$, there is a prime $p \equiv 1 \pmod{n_0^v}$ with $u_0 \le \log p \le u_0 + w_0$. Taking $n_0 = q_0 d$ and $v = 2(s+6)$ gives the modulus q_2^2 for p_0, p_1, N. The proof combines these windows with the norm constructions of Problems 33.5.1 and 33.5.2. It obtains the sparse set Φ_b from Behrend's construction (Chapter 4). Its existence theorem is as follows.

Theorem 33.6.1. *Let (q_0, d) be parameters and $0 < \varepsilon < 1/100$. For every sufficiently large integer x there are data for (q_0, d) whose first scale is x, such that (1) $x_1 = \lfloor\exp(x^{\varepsilon/6})\rfloor$; (2) b is the least natural number that is divisible by q_1x_1 and exceeds $\exp(x^\varepsilon)$; (3) m is the least power of 2 with $\sqrt{x} \le m$, and r is the least power of 3 with $x^5 \le r$; (4) $x^{\varepsilon/6} - 1 \le \log x_1$ and $x^\varepsilon \le \log b \le x^\varepsilon + 1$.*

"Sufficiently large" depends on (q_0, d) and ε; the statement gives no explicit threshold. In its proof m, r, s and b are taken as above; the digits of the exponents defining Φ_b form vectors on a common sphere (Chapter 4); and the windows used to choose the primes have length $x^{\varepsilon/6}$ in $\log p$.

Problem 33.6.3. For the data of Theorem 33.6.1 and all large x: $\log b \le 2x^{\varepsilon}$ and $\log x_1 \ge x^{\varepsilon/12}$.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, with the namespace `New.` omitted below), Definition 33.1.1 is `Parameters` and Definition 33.3.1 is `Data`, with fields including `natX`, $\texttt{natX}_1$, `natB`, `m`, `r`, `towerExp`, `bPlaces`, `weight`, `levelPrime`, `piMBar`, `N`, `piN` (`New/Reduction/Data/FieldsAndPlaces.lean`, `New/Reduction/Data/AdmissibleData.lean`); h_{dir}, h_{main}, rem are `Data.directionAmount`, `Data.mainAmount`, `Data.totalRemainder`; U and B are `Data.errorUnit` and `Data.denominatorBudget`; the spaces Y_j are `Data.spaceY`, with Gram matrices for $j < m$ given by `Data.spaceY_gram_eq` and standard endpoint Y_m by `Data.isStd_spaceY_last`; ϱ is `Data.`ϱ, the number of hyperbolic planes of the shape `Data.shape` of Y_0; and Theorem 33.6.1 is `eventually_exists_data` (`New/Reduction/Data/Existence.lean`). The prime window is `exists_prime_modEq_one_log_mem` (`Lib/Analytic/Primes.lean`); the proof of existence uses `exists_three_term_free`, `Parameters.exists_prime_pair_norm` and `Parameters.exists_mul_star_eq_prime`. The constant v_0 is `Parameters.vacuumBoundConst`. Problems 33.1.1, 33.2.3, 33.2.4, 33.3.1, 33.4.7, 33.5.1, 33.6.1, 33.6.2 and 33.6.3 are derived here.

Hints

§33.1.

33.1.1: $d + 1 > 0$; $q_0/2$ divides $d + 1$ with odd quotient, and $8 \mid q_0/2$.

33.1.2: (i) Show $d \equiv -1 \pmod{4p}$ and apply quadratic reciprocity; for $p = 2$ use $d \equiv 7 \pmod 8$. (ii) Use (i) with $18480 \mid q_0$.

§33.2.

33.2.1: For $s \ge 1$, $3^{\lfloor \log_3 s \rfloor} \le s < 3^{\lfloor \log_3 s \rfloor + 1}$; treat $s = 0$ directly.

33.2.2: The primes $2, 3$ divide q_0; K is ramified only at d, and $d \nmid q_1$. Count the fibres of $(\mathbb{Z}/q_1)^{\times} \to (\mathbb{Z}/q_0)^{\times}$.

33.2.3: $K \subset \mathbb{Q}(\zeta_d)$ since $d \equiv 3 \pmod 4$. The conductor–discriminant formula.

33.2.4: $|\mathrm{disc}\, L| = |\mathrm{disc}\, F|^{[L:F]}\, N_{F/\mathbb{Q}}(\mathfrak{d}_{L/F})$ for $F \subset L$, with $\mathfrak{d}_{L/F}$ the relative discriminant ideal.

§33.3.

33.3.1: $C \ge q_0$.

33.3.2: $\sqrt{x} \ge (\log b)^{50}$.

33.3.3: Problem 33.2.1 and $s \le 32 \log x$ bound the power of 3; $\log b \ge (\log x_1)^6 \ge (10^6 \log x)^6$, and $\log x \ge 100 \log\log b$ is large.

33.3.4: Σ_j is a sum of hyperbolic planes and, when $m - 1 - j$ is odd, the middle entry.

§33.4.

33.4.1: $q_1 x_1 \mid b$, and $x \le x_1$.

33.4.2: $0 \le \Lambda_K \le 2\Lambda$ and Problem 33.4.1. For an integer $u \ge 1$, $\log u! = \sum_{n \le u} \Lambda(n) \lfloor u/n \rfloor$, and Chebyshev's bound $\psi(u) \le 2u$.

33.4.3: Problems 33.2.3 and 33.2.4, $|\mathrm{CS}(d)| \le C$, $2^s = m^{22}$, and $q_1 x_1 \mid b$.

33.4.4: $y! \le y^y$ and $a \le b^2$. Stirling's formula with Robbins' remainder [Rob].

33.4.5: Problems 33.4.2 and 33.4.4; on Φ_b the weight is b; Definition 33.3.1(3) and Problem 33.2.2.

33.4.6: Problems 33.3.2, 33.2.2 and 33.4.5, and $\varphi(q_0) \le C$.

33.4.7: Write $\log \kappa$ through $\log a$, $\log x$ and $\log x_1$; Problem 33.2.2.

§33.5.

33.5.1: Pigeonhole on the classes of primes $\mathfrak{p}_i \mid p_i'$.

33.5.2: $4 \mid q_1$. Fermat's two-squares theorem.

33.5.3: The mean of $\log \kappa$ lies in $[0, L]$, and $19L \le \log(M \mathrm{rd}_E / 2\pi) \le 23L$ by Problem 33.2.3 and $L \ge 7 > \log 2\pi$.

33.5.4: Problem 33.5.3 with $L = \log b$, using Problems 33.4.1 and 33.3.2, and $q_1 d \le b$ from $q_1 x_1 \mid b$ and $d \le C < x_1$.

§33.6.

33.6.2: Take logarithms to compare the five conditions; keep track of the floor in x_1.

33.6.3: $x^\varepsilon + 1 \le 2x^\varepsilon$; $\lfloor e^u \rfloor \ge e^{u/2}$ for $u \ge 2$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 1990.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[RS] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[Rob] H. Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.