hexagon:2611.01307v1

THE RIEMANN HYPOTHESIS FOR THE DEDEKIND ZETA FUNCTION OF A NON-ABELIAN CUBIC FIELD

MANVIR JASWAL

Abstract. We prove the Riemann hypothesis for the Dedekind zeta function of the non-abelian totally real cubic field of discriminant 148; equivalently, for the Hecke L-function of a cubic ray class character of $\mathbb{Q}(\sqrt{37})$. The proof runs Alpöge's argument for Dirichlet L-functions over a CM field containing the Galois closure, so that its sum over primes involves this L-function. Our argument for this field is not formalized; it rests on the public Lean rewriting of Alpöge's proof by Sernau and colleagues, the main conjecture for totally real fields at odd primes, proved by Wiles, and Brumer–Stark over $\mathbb{Z}$, proved by Dasgupta, Kakde, Silliman and Wang.

Contents

1. Introduction 1
2. The method over $\mathbb{Q}$ 4
3. The field and its L-functions 7
4. Primes of the data that split completely 10
5. The choice of d 12
6. Polarity 15
7. The cohomology step 17
8. The Weil data and the tight frames 23
9. Proof of the theorem 29
Appendix A. The development and the re-check 40
Declarations 46
References 46

1. Introduction

In November 2026 Alpöge, working with Claude, proved the generalized Riemann hypothesis for Dirichlet L-functions and presented the proof in Lean 4 [1]. He expects the method to give the extended Riemann hypothesis. We carry it to a field that is not abelian.

Theorem 1.1. *Let $K = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha^2 - 3\alpha + 1 = 0$, the totally real cubic field of discriminant 148. Every zero of the Dedekind zeta function $\zeta_K(s)$ with $0 < \operatorname{Re} s < 1$ has real part $\frac{1}{2}$. Equivalently, the Riemann hypothesis holds for the Hecke L-function $L_F(s, \psi_3)$ of a cubic character ψ_3 of the ray class group of $F = \mathbb{Q}(\sqrt{37})$ modulo 2, and the extended Riemann hypothesis holds for the Galois closure L of K.*

Date: November 28, 2026.

2020 *Mathematics Subject Classification.* Primary 11M26, 11R42; Secondary 11R23, 11R37, 11M41.

Key words and phrases. Extended Riemann hypothesis, Dedekind zeta function, Hecke L-functions, theta lifts, Brumer–Stark conjecture.

The field K is the totally real cubic field of least discriminant that is not abelian; the two of smaller discriminant, 49 and 81, are cyclic [25]. Before this, the zeros of ζ_K were known to avoid a half-plane $\operatorname{Re} s > \theta$ with $\theta < 1$ [2, Thm. 1.1], [8, Thm. 1.2], [12, Thm. 7.33]. Its Galois closure L is totally real with group S_3 and contains F, and L is the class field of the ray class group of F modulo 2, which is cyclic of order three. Of its two characters of order three, either may be taken for ψ_3. The other one is $\psi_3 \circ \sigma = \psi_3^{-1}$, with σ the non-trivial automorphism of F, and so it has the same L-function. With χ_{37} the quadratic Dirichlet character of conductor 37,

$$\zeta_K(s) = \zeta(s)\, L_F(s, \psi_3), \qquad \zeta_L(s) = \zeta(s)\, L(s, \chi_{37})\, L_F(s, \psi_3)^2 \tag{1.1}$$

(Lemmas 3.1 and 3.2). As ψ_3 is not trivial, $L_F(s, \psi_3)$ is entire, so by (1.1) the zeros of $\zeta_K(s)$ with $0 < \operatorname{Re} s < 1$ are those of $\zeta(s)$ and of $L_F(s, \psi_3)$, and those of $\zeta_L(s)$ are these and those of $L(s, \chi_{37})$. Alpöge's theorem covers $\zeta(s)$ and $L(s, \chi_{37})$, so the three statements of Theorem 1.1 are equivalent. Let std be the two-dimensional irreducible representation of $S_3 = \operatorname{Gal}(L/\mathbb{Q})$. Its Artin L-function is $L(s, \mathrm{std}) = L_F(s, \psi_3)$, of degree one over F and two over $\mathbb{Q}$, and it is the L-function of a Maass cusp form of weight 0, level 148, Laplace eigenvalue $\frac{1}{4}$ and character χ_{37} [24, Thm. 1.1 and the remark after it, Thm. 3.2(2)].

Alpöge's argument descends from Stepanov's method for curves over finite fields [23]. The multiplicity of Stepanov's auxiliary function has no analogue over the integers, and Alpöge gains it instead along a chain of theta lifts between unitary groups over a CM field, of length about $\sqrt{x}$ for the primes up to x. A shorter rewriting of his Lean proof, by Sernau with colleagues at Anthropic and Claude, is public [19]; we use its compact edition at commit `72fead10` and call it the development. It proves in Lean 4 [4], on Mathlib [26], that every zero of $\zeta(s)$ and of every Dirichlet L-function with $0 < \operatorname{Re} s < 1$ has real part $\frac{1}{2}$. The method is Alpöge's.

For an abelian field K' the extended Riemann hypothesis is the development's theorem, since $\zeta_{K'}$ is a product of Dirichlet L-functions. For a field that is not abelian the method does not apply as it stands. Its prime side weights a prime power ν prime to d by the Frobenius of ν in the Galois group over $\mathbb{Q}$ of the field over which the lifts are taken, and a power of d, which ramifies in that field, by the Frobenius of the prime of k_d above d. In the development that field is $k_d(\zeta_{N_1})$, with $k_d = \mathbb{Q}(\sqrt{-d})$ imaginary quadratic and N_1 growing with x. It is abelian over $\mathbb{Q}$, and the prime side is a combination of Dirichlet L-functions. To bring in ζ_K the field must contain the Galois closure L of K, and it must remain CM, as the lifts start from forms on a unitary group that is definite at every infinite place, and such a group needs a CM field. As L is totally real, the field $E = L \cdot k_d(\zeta_{N_1})$ does both. But E is not abelian over $\mathbb{Q}$, while the development proves its steps for a cyclotomic extension of k_d, often through that structure.

Table 1 gives each property of the development's field that its proof uses and that fails for E or must be proved again, with what replaces it for E; Section 9 says why the other steps hold for E unchanged, and Appendix A gives the development's statements, its commit and the files of the declarations we cite. The development is checked by Lean for its own field; our argument for E is not formalized, and the machine checks of Section 9 and Appendix A only locate where the development uses the cyclotomic structure of its field, each replacement being proved here.

1.1. **The proof.** We run the development's argument on E, taking its parameter N_0, a multiple of 18480, to be divisible by 37, so that $F \subset \mathbb{Q}(\zeta_{37}) \subset k_d(\zeta_{N_1})$. Section 2 states the argument in words. A step that holds for E as the development proves it is cited by its

declaration and not proved again; the others are proved here in full, and they are what this paper adds.

The analytic inputs come first. The twists of ζ_K/ζ by Dirichlet characters are Hecke L-functions over F of characters whose order is divisible by three, so that none is real (Lemma 3.3), and the twists by $(\frac{\cdot}{d})$ have conductors explicit in d (Lemma 3.4). The primes of the development's data, two auxiliary primes and the level of the lifts, must now split completely in L as well as satisfy its congruences, a Chebotarev condition at moduli that grow with x. We count them with Thorner and Zaman's Chebotarev theorem, which keeps a possible exceptional zero in the main term [27], and Stark's bound for that zero [22]; so nothing is assumed about exceptional zeros (Section 4). The prime d must be chosen so that, for every character ξ modulo N_0, the twists by $(\frac{\cdot}{d})$ of $L(s, \mathrm{std} \otimes \xi)$, which have degree two, and of the Dirichlet L-functions have no zero in a box. We carry the development's proof of this, a three-lines argument with theta series and a mean value over d, to Hecke L-functions over F. Poisson summation becomes the theta transformation over F, which we derive from Hecke's functional equation in Rademacher's form [16]. The mean value needs Heath-Brown's large sieve for real characters [7], since the Pólya–Vinogradov bound is too weak in degree two (Section 5). The prime side for E involves the Frobenius in $\mathrm{Gal}(L/\mathbb{Q})$ as well, and we prove that the function it defines has, on $\mathbb{C}$, the analytic properties that Landau's lemma needs (Section 6).

The rest concerns E as a field. Of the Tate-twisted Selmer groups of its field, the development's argument uses only the subgroup of odd classes at each twist index $e \geq 1$, and the class group at $e = 0$, through one length bound (`exists_length_shaOdd_le`). We prove that bound for E. We bound the odd classes by special values of L-functions of E^+, for every CM field E with $[E^+ : \mathbb{Q}] \geq 2$. At odd primes the bound comes from Wiles's main conjecture for totally real fields [28], in the form Kolster gives for CM extensions [11, Prop. 1.1]. At the prime 2 it comes from the Brumer–Stark conjecture over $\mathbb{Z}$, proved by Dasgupta, Kakde, Silliman and Wang [3], applied at every layer of $E(\mu_{2^\infty})/E^+$ and evaluated at the twist through Deligne and Ribet's measures [5]. It gives an annihilator of the minus quotient $M/(1+c)M$, which a detecting set of Galois elements turns into a length bound. For our E these values have the size the argument needs (Section 7). Section 8 gives the Weil data of E, its tight frames at the constants the argument asks for, and a generator of its different whose size is bounded at every infinite place. In Section 9, which puts everything into the development's argument, the infinite places of E form a group that is not commutative, on which Frobenius acts by left multiplication, in place of the development's places labeled by $(\mathbb{Z}/N_1)^\times$. Particular to K are the facts of Section 3 about it (its discriminant $148 = 4 \cdot 37$, $F = \mathbb{Q}(\sqrt{37})$, and L/F ramified only above 2, tamely), the condition $37 \mid N_0$, which puts F in $k_d(\zeta_{N_1})$, the two relative frames and the Kummer generator of Section 8.2, built from the roots of $x^3 - x^2 - 3x + 1$, and the dyadic different of row 12 of Table 1; everything else in Section 9 is stated for the group $\mathrm{Gal}(E/k_d)$ and its central subgroups.

Put together, the proof has five steps. Fix $\varepsilon \in (0, \frac{1}{100})$.

(1) For each of the development's primes d, its argument, run on E, gives $R_E(x) \leq x^{8\varepsilon - 1/2}$ for all large x (Section 9). Here $R_E(x)$ is the sum of $\Lambda(\nu)(1/\nu - 1/x)$ over the prime powers $\nu \leq x$ with $\nu \equiv 1 \bmod N_0$, weighted by $1 - (\frac{\nu}{d})$ and by the indicator that the Frobenius of ν is trivial on L, less its main term. As a class function on S_3 this indicator is $f = (1 + \mathrm{sgn} + 2\chi_{\mathrm{std}})/6$ (Section 6).

(2) This function is polar. Its Laplace transform continues meromorphically to $\mathbb{C}$, with at most simple poles on $\mathrm{Re}\, s > 0$, whose residues are combinations of the orders of zeros

of $L(s, \mathrm{std} \otimes \xi)$ and of Dirichlet L-functions, for the characters ξ modulo N_0, and of their twists by $(\frac{\cdot}{d})$ (Proposition 6.1).

(3) Given ρ with $\frac{1}{2} + 8\varepsilon < \operatorname{Re}\rho < 1$, the prime d can be chosen so that these twists have no zero with $\operatorname{Re} s \geq \frac{1}{2} + 8\varepsilon$ and $|\operatorname{Im} s| \leq |\operatorname{Im}\rho|$ (Theorem 5.1).

(4) With the twists zero-free in the box, the residue at ρ is a non-zero multiple of a combination, with the positive weights $f_1 = f_{\mathrm{sgn}} = \frac{1}{6}$ and $f_{\mathrm{std}} = \frac{1}{3}$, of the orders at ρ of $L(s, \xi)$, $L(s, \chi_{37}\xi)$ and $L(s, \mathrm{std} \otimes \xi)$. Landau's lemma forces it to vanish, so each of these orders vanishes, that of $L(s, \mathrm{std}) = L_F(s, \psi_3)$ included (Proposition 6.2). As ε is arbitrary, this excludes zeros of $L_F(s, \psi_3)$ in $\frac{1}{2} < \operatorname{Re} s < 1$; on $\operatorname{Re} s \geq 1$ it does not vanish by (P) in Section 6.

(5) By (1.1), and as $\zeta(s)$ has no zero with $\frac{1}{2} < \operatorname{Re} s < 1$, neither has $\zeta_K(s)$. Its functional equation reflects this to $0 < \operatorname{Re} s < \frac{1}{2}$.

Steps (2)–(5) are the development's analytic end (Section 2.2) with the twists of degree two added; step (1) is the rest of its argument, run on E.

2. The method over $\mathbb{Q}$

The development proves the Riemann hypothesis for Dirichlet L-functions by playing a size side, built from a chain of theta lifts over a CM field, against a prime side, a sum over prime powers. We state its argument as it stands, step by step (for an account in classical terms see [18]).

2.1. **The chain.** Fix a Dirichlet character. The development puts $N_0 = 18480$ times its modulus and works with the primes d such that $N_0 \mid 2(d+1)$ and $N_0 \nmid d+1$, that is, $d \equiv N_0/2 - 1 \bmod N_0$; since $16 \mid N_0$, every such d is $\equiv 7 \bmod 8$ (`Parameters`). Write $k_d = \mathbb{Q}(\sqrt{-d})$, the development's K, and $h(k_d)$ for its class number. At the scale x it fixes $\varepsilon \in (0, 1/100)$, a number b with $\log b = x^{\varepsilon}$ and an integer $1 \leq r \leq 32 \log x$, the development's s (`Data.s_le`), and puts

$$N_1 = N_0 \cdot 3^{\lfloor \log_3 r \rfloor + 5} \cdot 2^r, \qquad N = N_1 d.$$

The field of the lifts is $k_d(\zeta_{N_1})$. In words, the chain runs as follows.

(a) *Data* (`exists_data`). Two primes $g_0 \neq g_1$ with $g_i \equiv 1 \bmod N$, $(N_0 d)^{2(r+6)} \mid g_i - 1$, $b^{10} \leq g_i \leq b^{11}$ and $g_0 g_1 = \varpi\bar{\varpi}$ for some $\varpi \in \mathcal{O}_{k_d}$; and, for every $U \in [100 \log b, 2^r]$, a prime $p \equiv 1 \bmod (N_0 d)^{2(r+6)}$ with $\log p \in [U, U + \sqrt{\log b}]$ (`Data.exists_prime_window`). The level of the lifts is a third prime $\mathcal{N}$, taken from one of these windows at a point fixed by the data (`Data.N`); it is not the modulus $N = N_1 d$.

(b) *Theta products.* The theta products are products of theta functions of the elliptic curve with complex multiplication by $\mathcal{O}_{k_d}$, taken along a tight frame of the field (`Parameters.exists_isTightFrame`). At a prime p not split in k_d the development fixes λ_p and η_p in $\mathbb{C}_p$ with $|\lambda_p| = p^{-\rho_p}$, where ρ_p depends only on p and d, and $|\eta_p|$ equal to p^{-1} at inert p and to $d^{-1/2}$ at d. Along a tight frame whose constant is prime to p, translated by points of order prime to p and scaled by an element of absolute value at most 1, the theta products are then integral on the null cone (`IsIntegralOnNullCone`). That is, let ϑ be one of them, a power series in variables indexed by the pairs (σ, i) of a place σ and a copy i, let $n \geq 1$, and let the $Z_{\sigma,i}$ be power series without constant term over the valuation ring of $\mathbb{C}_p$ whose couplings $\sum_{\sigma,i} Z_{\sigma,i}^{p^j} Z_{v_{-p^j}\sigma,i}$, with v_ν the place of class ν (Lemma 2.1), lie in the ideal generated by p and η_p for every odd j with $p^j \leq n$,

and at $p = d$ for every $j \geq 0$ with $p^j \leq n$; then the coefficients of total degree at most n of $\vartheta((\lambda_p Z_{\sigma,i})_{\sigma,i})$ are integral. At an inert prime, with the frame scaled by a unit, the theta products have an explicit normal form (`Parameters.thetaProducts_normal_form`).

(c) *Iterated lifts and masses.* The columns are algebraic forms on a definite unitary group over the field, and the rows are cusp forms on an indefinite one. A seesaw identity compares the chain of theta lifts of a column between definite groups, of length about $\sqrt{x}$, with the chain of lifts of its Poincaré series between indefinite ones, so that two bounds on one covolume meet (`Data.seesaw`). The norms of the lifts are compared through the Siegel–Weil mass formula, and the ratio of consecutive masses is controlled for every CM field with Weil data (`abs_log_mass_ratio_sub_le`). The masses bound the dimensions of the rows (`Data.finrank_rows_le_mass`).

(d) *Denominators.* The indices of the integral structures are bounded by lengths of Tate-twisted Selmer groups (`denominatorLe_rowBudget`). Three constructions enter. Ribet's method turns congruences between lifts into columns, the Ribet columns (`ribet_columns`). Twists, one for each ℓ-adic embedding, whose first powers have few congruences form the fit families (`exists_isFitFamily`). Taylor–Wiles primes in triangular order, each new Frobenius killing the earlier reciprocity laws for the even classes but not the new one, remove the even classes without a bound for them; they are the triangle primes (`exists_isPrimeTriangle`). The allowance at ℓ per unit of rank is the row budget (`rowBudget`). The only bound used on the Selmer groups of the field itself is `exists_length_shaOdd_le` (Section 7).

(e) *The inequality.* The forms of the chain are short (`Data.short_forms`). There are enough of them (`Data.enough_forms`). Control of the index of a large independent family of rows bounds the covolume of its lifts from below (`Data.integral_forms_long`). These three bounds are played against the prime sum (`Data.primeSum`). That sum runs over the prime powers ν not split in k_d up to the largest scale a of the data (Lemma 2.1), weighted by $\Lambda(\nu)(1 - (\frac{\nu}{d}))$ and by how the Frobenius of ν moves the embeddings of the field. The output is a one-sided bound for the prime error R_{N_0} of Section 2.2 (`eventually_primeError_le_rpow`). For every such d,

$$R_{N_0}(x) \leq x^{8\varepsilon - 1/2} \qquad \text{for all large } x. \tag{2.1}$$

2.2. **The analytic end.** For a modulus M and a prime $d \equiv 7 \bmod 8$ with $d \nmid M$, the prime error is

$$R_M(x) = \sum_{\substack{\nu \leq x \\ \nu \equiv 1 \ (M)}} \Lambda(\nu)\Big(1 - \Big(\frac{\nu}{d}\Big)\Big)\Big(\frac{1}{\nu} - \frac{1}{x}\Big) - \frac{\log x}{\varphi(M)} - \kappa,$$

with a real constant κ that removes the pole at $s = 1$ below (`primeError`). As $\int_\nu^\infty (1/\nu - 1/x)x^{-s}\,dx = \nu^{-s}/(s(s-1))$, on $\operatorname{Re} s > 1$ its Laplace transform is

$$\int_1^\infty R_M(x)\, x^{-s}\, dx = \frac{1}{\varphi(M)\, s(s-1)} \sum_{\xi} \Big(\frac{L'}{L}(s, \xi(\tfrac{\cdot}{d})) - \frac{L'}{L}(s, \xi) \Big) - \frac{1}{\varphi(M)(s-1)^2} - \frac{\kappa}{s-1},$$

the sum over the characters ξ modulo M, with ξ and $\xi(\frac{\cdot}{d})$ taken as characters modulo M and Md. The development proves that it is polar (`isPolar_primeError`). In the sense of its definition (`IsPolar`), this means that it continues meromorphically, it is analytic on

$\operatorname{Re} s \geq 1$ after multiplication by $s-1$, and in $\operatorname{Re} s > 0$ it has at most simple poles, the residue at a point s with $0 < \operatorname{Re} s < 1$ being

$$\sum_{\xi \bmod M} \frac{\operatorname{ord}_s L(s,\xi) - \operatorname{ord}_s L(s,\xi(\frac{\cdot}{d}))}{\varphi(M)\, s(1-s)}.$$

Landau's lemma for Laplace transforms of functions of one sign turns (2.1) into non-vanishing (`entireL_ne_zero_of_primeError_le`). Given $\beta > \frac{1}{2}$ and a zero ρ with $\operatorname{Re}\rho > \beta$, choose d so that the twists $L(s,\xi(\frac{\cdot}{d}))$ have no zero with $\operatorname{Re} s \geq \beta$ and $|\operatorname{Im} s| \leq |\operatorname{Im}\rho|$ (`exists_entireL_quadTwist_ne_zero`). Then the residue at ρ is a non-zero multiple of $\sum_\xi \operatorname{ord}_\rho L(s,\xi)$, and Landau's lemma forces it to vanish. With $\beta = \frac{1}{2} + 8\varepsilon$ and $\varepsilon \to 0$ this is the half-plane form of GRH (`New.grh`). The functional equation then puts the zeros on the line (`New.zeros_on_line`). The development also uses polarity inside the proof of (2.1). There the only term of its main inequality indexed by primes is, up to a term free of primes, a combination of two prime errors, and its window lemma `IsPolar.exists_window_sub_mul_le`, applied to these, turns the inequality into (2.1). The combination comes from the following identity, which Section 9 carries to E.

Lemma 2.1. *The infinite places of $k_d(\zeta_{N_1})$ form a group isomorphic to $\operatorname{Gal}(k_d(\zeta_{N_1})/k_d) \cong (\mathbb{Z}/N_1)^\times$. For ν prime to N_1 let v_ν be the place of class ν, and let $v_\nu = 1$ otherwise. The data of the chain fix scales $x < x_1 < a$, a set Θ of thick places, each of class -1 modulo N_0, and the set $\mathcal{T}$ of tops, the places of class 1 modulo N_0. Put $w(\sigma) = a/x$ for $\sigma \in \Theta$ and $w(\sigma) = a/x_1$ for the other places. For real y and a place σ, the prime sum at σ is*

$$P(y,\sigma) = \sum_{1 \leq \nu \leq a} \Lambda(\nu)\Big(1 - \Big(\frac{\nu}{d}\Big)\Big)\Big(\frac{y}{\nu} - w(v_{-\nu}\sigma)\Big)^+. \tag{2.2}$$

Then

$$\sum_{\tau \in \mathcal{T}} \big(P(a,\tau) - A\big) = a\Big(\#\Theta\,\big(R_{N_0}(x) - R_{N_0}(x_1)\big) + \#\mathcal{T}\, R_1(x_1)\Big), \tag{2.3}$$

where $A = a(\log a - 1 - c_d - \bar{w})$, with c_d a constant depending only on d and $\bar{w}$ the mean of $\log w$ over the infinite places.

The prime sum (2.2) is `Data.primeSum`. The identity (2.3) is `Data.remainder_eq`, and it rests on a count. As the tops have class 1 and the thick places class -1 modulo N_0, a place $v_{-\nu}\tau$ with $\tau \in \mathcal{T}$ can be thick only if $\nu \equiv 1 \bmod N_0$. For such ν the map $\tau \mapsto v_{-\nu}\tau$ sends $\mathcal{T}$ onto the places of class -1 modulo N_0, so exactly $\#\Theta$ tops are sent into Θ.

The main inequality. Let m be the number of lifts in the chain, an integer in $[\sqrt{x}, 2\sqrt{x}]$, let a be the least multiple of N_1 that is at least xb, and let $\mathcal{W}$ be the space of rows. The error unit is $\mathcal{B} = \varphi(N_1)\, a\, (\log b)^3$, with $\varphi(N_1)$ the number of infinite places of the field (`Data.budget`). The remainder $\operatorname{rem} = \sum_{\tau\in\mathcal{T}}(P(a,\tau) - A)$ is the left side of (2.3), the prime sum at the tops at order a less its expected value (`Data.remainder`). For a family $\mathcal{F}$ of rows, $e^{\mathcal{V}}$ bounds the squared covolume of their lifts at every automorphism of $\mathbb{C}$, and $\mathcal{I}$ bounds the logarithm of the index that makes the lifts integral at every prime (`Data.IndexLe`). The main term $\mathfrak{h}$ is m times the rank of the columns times the cost of one direction (`Data.mainHeight`). That cost is a sum over the infinite places σ of the logarithmic size of a jet at σ, the value at 0 of a derivative of a theta product, less the divisibility $P(w(\sigma),\sigma)$ forced on it.

The development's Theorems A (short forms) and B (enough forms) give a family of $\#\mathcal{F} \geq (1 - 4b^{-2}) \dim \mathcal{W}$ independent rows with $\mathcal{I} \leq 5 \dim \mathcal{W}\, \mathcal{B} \log(1+b^2)$ and $\mathcal{V} = \#\mathcal{F}\,(\mathfrak{h} - m \operatorname{rem} + \mathcal{B} \log b)$ (`Data.exists_family_covolumeSq_le`). Its Theorem C (integral forms are

long) bounds the covolume of every such family from below (`Data.integral_forms_long`). For this family the two bounds give

$$\mathfrak{h} - 3\,\mathcal{B}\log b \;\le\; \frac{\mathcal{V}+2\mathcal{I}}{\dim \mathcal{W}} \;\le\; \mathfrak{h} - m\,\mathrm{rem} + \mathcal{B}\log b + 4x^{99} + 10\,\mathcal{B}\log(1+b^2).$$

Both bounds are needed, the upper and the lower, and the main term $\mathfrak{h}$ they share cancels; over E both are proved again (Section 9.3). The errors are at most $(\log b)^2\mathcal{B}$ on the scales of the data, which gives the main inequality (`star_inequality`):

$$m\,\mathrm{rem} \le (\log b)^2\,\mathcal{B}. \tag{$\star$}$$

How it counts primes. Primes enter through divisibility. For p inert in k_d and $\nu = p^e$ with e positive and odd, the Frobenius partner $v_{-\nu}\sigma$ of a place σ is its image under the Frobenius at ν followed by complex conjugation (Section 9.1). The contribution of ν to the local divisibility asked at order y and place σ is exactly $(y/\nu - w(v_{-\nu}\sigma))^+$, with w the weight of Lemma 2.1. At $p = d$ each positive exponent contributes half this positive part. These local asks, multiplied by $\log p$ and summed, give the divisibility asked at σ at order y, which is $P(y,\sigma)/2$ for $y \le a$. Each of the m lifts gains this divisibility at order a at the tops, and at the weight $w(\sigma)$ at every place, which $\mathfrak{h}$ accounts for (`Data.gain`). Dividing the lifts by these powers of the primes $p < x_1$, less losses of total logarithm at most $\mathcal{B}$, keeps them integral up to a small index and divides every squared norm by $\exp(m\sum_{\tau\in\mathcal{T}} P(a,\tau))$, besides the prime sums inside $\mathfrak{h}$. The level $\mathcal{N}$ is chosen so that $\#\mathcal{T}\,a\log\mathcal{N}$ balances $m\,\#\mathcal{T}$ times the excess of the size of a jet of order a over A (`Data.heightPerRow_le`). The lower bound, the product formula for the ratio of the covolumes of the chain and of its twists, one twist for each p-adic embedding, contains $\mathfrak{h}$ but not the prime sum at the tops. So ($\star$) bounds that sum above its mean. Where the place $v_{-\nu}\tau$ of a top τ is thick, which happens for $\nu \equiv 1 \bmod N_0$ at exactly $\#\Theta$ tops, $P(a,\tau)$ counts ν up to x, with weight $a(1/\nu - 1/x)$, and elsewhere up to x_1; summed over the tops this is (2.3). As the errors do not grow with m, dividing ($\star$) by $m\,a\,\#\Theta$, with $\#\Theta \ge \#\mathcal{T}/\log b$ and $\varphi(N_1) = \varphi(N_0)\,\#\mathcal{T}$, gives

$$R_{N_0}(x) - R_{N_0}(x_1) + \frac{\#\mathcal{T}}{\#\Theta}\,R_1(x_1) \le \frac{\varphi(N_0)(\log b)^6}{m} \le \varphi(N_0)\,x^{6\varepsilon-1/2}.$$

The saving is $1/m$, and $m \ge \sqrt{x}$ makes it $x^{-1/2}$. The place $v_{-\nu}\sigma$ is what this paper changes. Over E it is σ multiplied on the left by an element restricting to the Frobenius of ν in $S_3 = \mathrm{Gal}(L/\mathbb{Q})$, and as the tops and the thick places are trivial on L, the count of thick places weights ν by $f = (1 + \mathrm{sgn} + 2\chi_{\mathrm{std}})/6$ (Lemmas 9.2 and 9.6).

3. The field and its L-functions

We take $37 \mid N_0$ throughout and run the chain on

$$E = L \cdot k_d(\zeta_{N_1}).$$

Then $F = \mathbb{Q}(\sqrt{37}) \subset \mathbb{Q}(\zeta_{37}) \subset k_d(\zeta_{N_1})$, so $\mathrm{Gal}(E/k_d(\zeta_{N_1})) \cong \mathrm{Gal}(L/F)$ is cyclic of order three and E is not abelian over $\mathbb{Q}$; E is CM (Lemma 3.6), and Figure 1 shows the fields. The facts special to K are collected here. The point is that $\zeta_K(s)/\zeta(s)$ is the Hecke L-function of a cubic ray class character of the real quadratic field $F = \mathbb{Q}(\sqrt{37})$. So the twists the method needs are Hecke L-functions of F with explicit conductors, and none of them is attached to a real character.

Lemma 3.1. *Let $K = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha^2 - 3\alpha + 1 = 0$, let L be its Galois closure, and $F = \mathbb{Q}(\sqrt{37})$.*

(a) *$\mathbb{Z}[\alpha]$ is the ring of integers of K, of discriminant $148 = 2^2 \cdot 37$; K is totally real; $L = K(\sqrt{37})$ is totally real of degree 6 with group S_3, and $F \subset L$.*

(b) *F has class number one, fundamental unit $6 + \sqrt{37}$ of norm -1, and 2 is inert in F.*

(c) *The ray class group of F modulo $2\mathcal{O}_F$, and also modulo $2\infty_1\infty_2$, is cyclic of order three, and its class field is L.*

(d) *If ψ_3 generates its characters and σ generates $\mathrm{Gal}(F/\mathbb{Q})$, then $\psi_3 \circ \sigma = \psi_3^{-1}$.*

(e) *$|d_L| = 2^4 \cdot 37^3 = 810448$, and the root discriminant of L is $810448^{1/6} < 10$.*

Proof. (a) and (b) are the records 3.3.148.1 and 2.2.37.1 of the LMFDB [25]. In (a), $\sqrt{148} = 2\sqrt{37}$ lies in L and not in K, so $L = K(\sqrt{37})$. In (b), the fundamental unit $2a + 5$ of the record, with $a = (1 + \sqrt{37})/2$, is $6 + \sqrt{37}$, of norm $36 - 37 = -1$.

(c) The sequence $\mathcal{O}_F^\times \to (\mathcal{O}_F/2)^\times \cong \mathbb{F}_4^\times \to \mathrm{Cl}_2(F) \to \mathrm{Cl}(F) = 1$ is exact, and $-1 \equiv 6 + \sqrt{37} \equiv 1 \bmod 2$, so $\mathrm{Cl}_2(F) \cong \mathbb{Z}/3$. With the real places added, -1 has signs $(-,-)$ and $6 + \sqrt{37}$ has signs $(+,-)$, which generate $\{\pm 1\}^2$, so the narrow group is also $\mathbb{Z}/3$. The extension L/F is cyclic of degree three. It is unramified above 37, where L and F both have ramification index two; it is totally and tamely ramified at the inert prime 2; and it is unramified elsewhere, at the real places included. So its conductor is $2\mathcal{O}_F$, and L is the class field.

(d) The non-trivial automorphism of F acts on $\mathcal{O}_F/2 = \mathbb{F}_4$ by $x \mapsto x^2$, which is inversion on $\mathbb{F}_4^\times$.

(e) By the conductor–discriminant formula for the characters 1, sgn and the two-dimensional std of S_3, whose conductors are 1, 37 and 148, we get $|d_L| = 37 \cdot 148^2$. □

Lemma 3.2. *Let* std *be the two-dimensional irreducible representation of* $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ *and χ_{37} the quadratic character of conductor* 37*. Then*

$$\zeta_K(s) = \zeta(s)\, L(s, \mathrm{std}), \qquad L(s, \mathrm{std}) = L_F(s, \psi_3), \qquad \zeta_L(s) = \zeta(s)\, L(s, \chi_{37})\, L(s, \mathrm{std})^2.$$

Proof. The permutation representation of S_3 on the three embeddings of K is $1 + \mathrm{std}$, and the regular representation is $1 + \mathrm{sgn} + 2\mathrm{std}$, with sgn cutting out F; Artin's formalism gives the first and third identities. The restriction of std to $A_3 = \mathrm{Gal}(L/F)$ is $\psi_3 + \psi_3^{-1}$, so $\mathrm{std} = \mathrm{Ind}_F^{\mathbb{Q}} \psi_3$ by Frobenius reciprocity, and Artin L-functions are invariant under induction [13, VII (10.4)]. □

For a Dirichlet character χ write Ψ_χ for the primitive Hecke character of F that induces $\psi_3 \cdot (\chi \circ \mathrm{N})$. By the projection formula $\mathrm{Ind}(\psi_3) \otimes \chi \cong \mathrm{Ind}(\psi_3 \cdot \chi|_{G_F})$ [20, §7.2], and $\chi|_{G_F}$ corresponds to $\chi \circ \mathrm{N}$, so

$$L(s, \mathrm{std} \otimes \chi) = L_F(s, \Psi_\chi), \qquad \mathrm{cond}(\mathrm{std} \otimes \chi) = 37 \cdot \mathrm{N}\mathfrak{f}_{\Psi_\chi}$$

[13, VII (11.7)].

Lemma 3.3. *For every Dirichlet character χ, the order of Ψ_χ is divisible by three. In particular no Ψ_χ is trivial or real, and every $L_F(s, \Psi_\chi)$ is entire.*

Proof. $\chi \circ \mathrm{N}$ is fixed by σ, so $\Psi_\chi/(\Psi_\chi \circ \sigma) = \psi_3/(\psi_3 \circ \sigma) = \psi_3^2$ by Lemma 3.1(d). If the order of Ψ_χ were prime to three, so would be the order of this quotient, which is three. As Ψ_χ is not trivial, $L_F(s, \Psi_\chi)$ is entire by Hecke's theorem [27, §2C]. □

The twists the method uses are the following. Fix a character ξ modulo N_0 and let $\Psi = \Psi_\xi$. Let $\mathcal{D}$ be the set of primes $d \equiv 7 \bmod 8$ with $d \nmid 74N_0$, and for $d \in \mathcal{D}$ put $\Psi_d = \Psi \cdot (\chi_{-d} \circ \mathrm{N})$, where χ_{-d} is the Kronecker character of $\mathbb{Q}(\sqrt{-d})$.

Lemma 3.4. *Let $d \in \mathcal{D}$.*

(a) $(\frac{n}{d}) = \chi_{-d}(n)$ *for every $n \geq 1$, so $\xi(\frac{\cdot}{d})$ and $\xi\chi_{-d}$ agree on integers prime to $N_0 d$, and $L(s, \mathrm{std} \otimes \xi(\frac{\cdot}{d}))$ and $L_F(s, \Psi_d)$ differ by finitely many Euler factors at primes dividing $N_0 d$.*

(b) *Ψ_d is primitive of conductor $\mathfrak{f}_\Psi \cdot d\mathcal{O}_F$, so its analytic conductor is $Q_{\Psi_d} = 37 \cdot \mathrm{N}\mathfrak{f}_\Psi \cdot d^2$.*

(c) *Ψ_d has the same sign at both real places, given by the parity $\mu = 1 - \mu(\xi) \in \{0, 1\}$, where $\xi(-1) = (-1)^{\mu(\xi)}$.*

(d) *With $a_\Psi(n) = \sum_{\mathrm{N}\mathfrak{a}=n} \Psi(\mathfrak{a})$ one has $a_{\Psi_d}(n) = \chi_{-d}(n) a_\Psi(n)$, and likewise for the coefficients $\check{a}_\Psi(n)$ of $1/L_F(s, \Psi)$.*

(e) *$2 \mid \mathfrak{f}_\Psi$.*

Proof. (a) For odd n prime to d, quadratic reciprocity and $d \equiv 3 \bmod 4$ give $(\frac{-d}{n}) = (\frac{n}{d})$; at $n = 2$ both sides are 1, since $d \equiv 7 \bmod 8$. (b) The prime d is unramified in F and $-d \equiv 1 \bmod 4$, so $\chi_{-d} \circ \mathrm{N}$ is unramified away from d and has exponent one at each prime above d, the local norm being onto $\mathbb{Z}_d^\times$; and $d \nmid \mathfrak{f}_\Psi$, which divides $N_0 \mathcal{O}_F$. (c) ψ_3 is trivial at the real places by Lemma 3.1(c), $\xi \circ \mathrm{N}$ has the sign $\xi(-1)$ at each of them, and $\chi_{-d}(-1) = -1$. (d) $(\chi_{-d} \circ \mathrm{N})(\mathfrak{a}) = \chi_{-d}(\mathrm{N}\mathfrak{a})$, and both sides are multiplicative. (e) On $\mathcal{O}_{F,2}^\times$ the component of ψ_3 has order three, while every finite-order character of $\mathbb{Z}_2^\times \cong \mathbb{Z}/2 \times \mathbb{Z}_2$, and so the component of $\xi \circ \mathrm{N}$, has order a power of two. □

Lemma 3.5. *Let M be a multiple of 74 and ψ a Dirichlet character modulo M, and put $L(s, \mathrm{std} \otimes \psi) = \prod_{p \nmid M} \det(1 - \psi(p)\mathrm{std}(\mathrm{Frob}_p) p^{-s})^{-1}$. Then*

$$L(s, \mathrm{std} \otimes \psi) = L_F(s, \Psi_\psi) \prod_{\mathfrak{p} \mid M,\ \mathfrak{p} \nmid \mathfrak{f}_{\Psi_\psi}} (1 - \Psi_\psi(\mathfrak{p}) \mathrm{N}\mathfrak{p}^{-s}).$$

No factor is removed at 2, and the factor at the prime above 37 is removed exactly when it does not divide $\mathfrak{f}_{\Psi_\psi}$. On $\mathrm{Re}\, s > 1$, $-\frac{L'}{L}(s, \mathrm{std} \otimes \psi) = \sum_{p \nmid M} \sum_{i \geq 1} \psi(p)^i \,\mathrm{tr}\,\mathrm{std}(\mathrm{Frob}_p^i) \log p\, p^{-is}$.

Proof. For $p \nmid M$ the inverse local factor of $L_F(s, \Psi_\psi)$ at p is the determinant: if p splits in F, $\mathrm{Frob}_p \in A_3$ has eigenvalues $\psi_3(\mathfrak{p})$ and $\psi_3(\mathfrak{p}')$; if p is inert, Frob_p is a transposition and the inverse factor is $1 - \psi(p)^2 p^{-2s}$, as $\psi_3(p\mathcal{O}_F) = 1$ for odd p. At $\mathfrak{p} \mid M$ the left side has no factor. The prime 2 divides $\mathfrak{f}_{\Psi_\psi}$ by the argument of Lemma 3.4(e). The last formula follows from the Euler product. □

Lemma 3.6. *Let $37 \mid N_0$. Then $L \cap k_d(\zeta_{N_1}) = F$, $[E : \mathbb{Q}] = 3[k_d(\zeta_{N_1}) : \mathbb{Q}]$, and E is CM with maximal totally real subfield $E^+ = L \cdot k_d(\zeta_{N_1})^+$. The extension E/E^+ is unramified at every finite place, E contains a primitive 5040-th root of unity, and $\mathrm{rd}_E \leq \mathrm{rd}_L \cdot \mathrm{rd}_{k_d(\zeta_{N_1})}$.*

Proof. $L \cap k_d(\zeta_{N_1})$ is abelian over $\mathbb{Q}$, contains F and lies in L, so it is F. The compositum of a totally real field and a CM field $C = C^+(\sqrt{-\gamma})$ is $TC^+(\sqrt{-\gamma})$ with TC^+ totally real and $-\gamma$ totally negative. Since $4 \mid N_1$ and N_1 is not a prime power, $\mathbb{Q}(\zeta_{N_1})/\mathbb{Q}(\zeta_{N_1})^+$ is unramified at the finite places, and E/E^+ is its base change. $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ divides N_1. The root discriminant of a compositum is at most the product of those of its factors. □

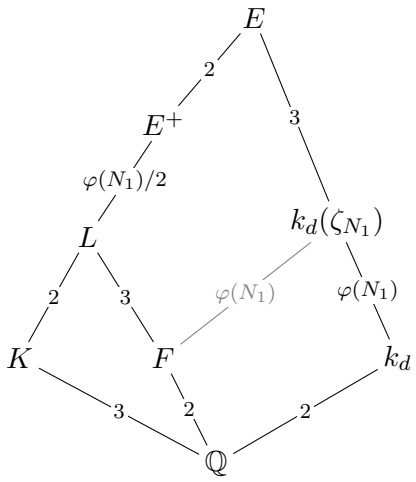

FIGURE 1. The fields of the proof, with the degrees of the extensions, for $37 \mid N_0$. The grey edge is the inclusion $F \subset \mathbb{Q}(\zeta_{37}) \subset k_d(\zeta_{N_1})$; $E = L \cdot k_d(\zeta_{N_1})$ and $E^+ = L \cdot k_d(\zeta_{N_1})^+$.

4. Primes of the data that split completely

For an abelian field the primes of the data split completely by a congruence alone. For $E \supseteq L$ they must also split completely in L, a Chebotarev condition, and the moduli grow with x. So the count has to be uniform in the modulus and has to survive an exceptional zero. Thorner and Zaman's Chebotarev theorem keeps the exceptional zero in the main term [27, Thm. 1.4], and Stark's bound for it [22, Thm. 1′], in the form of [27, Thm. 3.3], then gives a lower bound on every interval $(X, 2X]$ with $\log X \geq C_1 n_A (\log \mathcal{Q})^2$ (Lemma 4.1). At the moduli the data use, powers of $N_0 d$, no exceptional zero occurs for large x. A real character of $\mathrm{Gal}(L(\zeta_m)/L)$, a subgroup of index at most two in $(\mathbb{Z}/m)^\times$, extends to a character ϕ of $(\mathbb{Z}/m)^\times$ with $\phi^4 = 1$, whose conductor divides $16\,\mathrm{rad}(N_0 d)$. So these characters and their L-functions are finitely many and fixed, while $1 - \lambda_1/\log \mathcal{Q} \to 1$. Stark's bound is kept because Proposition 4.2 is stated for every m.

Lemma 4.1. *Let J/k be a Galois extension of number fields with group G, let $A \leq G$ be abelian, and let n_A and D_A be the degree and absolute discriminant of J^A. Let Q_A be the largest absolute norm of the conductor of a character of A, and put $\mathcal{Q} = D_A\, Q_A\, n_A^{n_A}$ ([27, (1-11), (3-1)]); assume $\mathcal{Q} \geq 3$. There are absolute effective constants $C_1 \geq 1$ and $c_1 > 0$ such that, if $\log X \geq C_1 n_A (\log \mathcal{Q})^2$,*

$$\#\{\mathfrak{p} \subset \mathcal{O}_k \text{ prime} : X < \mathrm{N}\mathfrak{p} \leq 2X,\ \mathfrak{p} \text{ unramified in } J,\ \mathrm{Frob}_{\mathfrak{p}} = 1\} \ \geq\ \frac{c_1 X}{|G|\, \mathcal{Q}^2 \log X}.$$

Proof. Write $\pi_1(y)$ for the number of such primes with $\mathrm{N}\mathfrak{p} \leq y$. By [27, Thm. 1.4] with the class $\{1\}$, for $y \geq \mathcal{Q}^{c_2}$,

$$\pi_1(y) = \mathrm{MT}(y)(1 + R(y)), \qquad \mathrm{MT}(y) = \frac{\mathrm{Li}(y) - \vartheta_1 \,\mathrm{Li}(y^{\beta_1})}{|G|}, \qquad |R(y)| \leq C_0\, \mathcal{E}(y),$$

with $\mathcal{E}(y) = \exp(-c_3 \log y/\log \mathcal{Q}) + \exp(-(c_3 \log y/n_A)^{1/2})$ and absolute $C_0 \geq 1$, c_2, c_3. Here $\vartheta_1 = 1$ if the exceptional zero $\beta_1 = 1 - \lambda_1/\log \mathcal{Q}$, with $0 < \lambda_1 < 1/8$, exists and $\vartheta_1 = 0$

otherwise. As $\mathcal{E}$ decreases,

$$\pi_1(2X)-\pi_1(X)\ge\big(\mathrm{MT}(2X)-\mathrm{MT}(X)\big)-C_0\mathcal{E}(X)\big(\mathrm{MT}(2X)+\mathrm{MT}(X)\big).$$

If β_1 exists, then $\beta_1>7/8$, as $\log\mathcal{Q}\ge1$, and

$$\begin{aligned}\mathrm{MT}(2X)-\mathrm{MT}(X)&=\frac{1}{|G|}\int_{\beta_1}^{1}\big((2X)^u-X^u\big)\frac{du}{u}\ge\frac{(2^{7/8}-1)(X-X^{\beta_1})}{|G|\log X}\\&\ge\frac{0.52\min\big(1,(1-\beta_1)\log X\big)X}{|G|\log X};\end{aligned}$$

if it does not, the difference is at least $0.5X/(|G|\log X)$. Also $\mathrm{MT}(2X)+\mathrm{MT}(X)\le 8X/(|G|\log X)$ for large X. Stark's bound [27, Thm. 3.3], $\lambda_1\ge c_S\mathcal{Q}^{-2}$ with $c_S\in(0,1]$ absolute, gives $(1-\beta_1)\log X\ge c_S\mathcal{Q}^{-2}$ once $\log X\ge\log\mathcal{Q}$. So

$$\pi_1(2X)-\pi_1(X)\ge\frac{X}{|G|\log X}\big(0.5\,c_S\mathcal{Q}^{-2}-8C_0\mathcal{E}(X)\big).$$

With $c'=\log(64C_0/c_S)\ge0$ and $\log\mathcal{Q}\ge1$, each term of $\mathcal{E}(X)$ is at most $c_S\mathcal{Q}^{-2}/(64C_0)$ as soon as $\log X\ge n_A(2+c')^2(\log\mathcal{Q})^2/c_3$. So $C_1\ge\max((2+c')^2/c_3,c_2,1)$, taken large enough for the bound on MT, gives the lemma with $c_1=c_S/4$. □

Proposition 4.2. *Let L' be a Galois number field of degree $n\ge2$ and absolute discriminant D. For every $m\ge1$ and every X with $\log X\ge C_1 n\,(n\log m+\log(Dn^n))^2$,*

$$\#\{p\in(X,2X]:\ p\equiv1\bmod m,\ p\text{ splits completely in }L'\}\ \ge\ \frac{c_1X}{n\,\varphi(m)\,D^2m^{2n}n^{2n}\log X}.$$

Proof. Apply Lemma 4.1 with $k=\mathbb{Q}$, $J=L'(\zeta_m)$ and $A=\mathrm{Gal}(J/L')$, which restriction embeds in $(\mathbb{Z}/m)^\times$. The Artin symbol of a prime $\mathfrak{P}\nmid m$ of L' sends ζ_m to $\zeta_m^{\mathrm{N}\mathfrak{P}}$, so a totally positive $\gamma\equiv1\bmod{}^\times m\mathcal{O}_{L'}$, whose norm $\prod_\tau\tau(\gamma)$ is $\equiv1\bmod m$ as L' is Galois, has trivial symbol. So every character of A has finite conductor dividing $m\mathcal{O}_{L'}$. Hence $Q_A\le m^n$, $\mathcal{Q}\le Dm^nn^n$, $\mathcal{Q}\ge D\ge3$ and $|G|\le n\varphi(m)$. A prime $p\in(X,2X]$ counted by the lemma is prime to m, and $\mathrm{Frob}_p=1$ in J gives $p\equiv1\bmod m$ and p split completely in L'. □

We apply this to $L'=L$, with $n=6$ and $D=2^4\cdot37^3$.

Corollary 4.3. *Let M be a positive multiple of 4 and $A\ge1$ an integer. For all large W, every integer $k\ge2$ with $M^k\le W^A$ and every $U\in[W,W^A]$, there is a prime $p\equiv1\bmod M^k$ that splits completely in L, with $\log p\in[U,U+W]$.*

This is the development's window lemma `exists_prime_modEq_one_log_mem` with complete splitting in L added.

Proof. Put $m=M^k$ and $X=e^U$, and apply Proposition 4.2 with $L'=L$. As $\log m\le A\log W$, the threshold $C_1n(n\log m+\log(Dn^n))^2$ is $O_A((\log W)^2)$, which is at most $W\le\log X$ for large W. The count is then at least $c_1e^U/(6\varphi(m)D^2m^{12}6^{12}U)\ge c\,e^W/W^{14A}$ for a constant $c>0$, which is at least 1 for large W. The interval $(X,2X]$ lies in $[e^U,e^{U+W}]$, as $\log2\le W$. Finally $16\mid m$, so $p\equiv1\bmod16$ and $p\ne2,37$; so p is unramified in L, and its complete splitting means that x^3-x^2-3x+1 has three distinct roots modulo p. □

The development's construction of the data (`exists_data`) makes one call of its window lemma, at $M=N_0d$, a fixed A, $W=x^{\varepsilon/6}$ and $k=2(r+6)$. From it come the windows of the class-group pigeonhole, at $U=10W^6+2iW$ for $0\le i\le h(k_d)$, and the windows of the level, at $U\in[100\log b,2^r]$ with length $\sqrt{\log b}$ (`Data.exists_prime_window`), after widening

$W \le \sqrt{\log b}$. With Corollary 4.3 in place of the window lemma, each of these windows contains primes that split completely in L. The pigeonhole, which produces $g_0 g_1 = \varpi\bar{\varpi}$, uses only that the primes of its windows are $\equiv 1 \bmod N$ and lie in disjoint windows, and is unchanged. For E the window property of the data asks in addition that its prime split completely in L, and the level $\mathcal{N}$ is chosen from it as in the development, at a point of $[100\log b, 2^r]$ that depends on x_1. The stronger property implies the development's, so the level keeps every property that the development's proofs read of it, and it splits completely in L. As the property holds at every point of $[100\log b, 2^r]$, the level of every datum the chain uses, the datum D' of Section 9.3 included, splits completely in L. The primes g_0, g_1 are chosen among the primes of their windows that split completely in L, and D' keeps those of D. A prime $\equiv 1 \bmod N_1 d$ that splits completely in L splits completely in E (Lemma 9.2(e)), so the level has residue degree 1 at every prime of E above it, which the lifts use (`Data.isSplitLevel_nonInducedPlaces`).

5. The choice of d

The endgame needs, besides the development's choice of d for Dirichlet L-functions, one for the degree-two family $L(s, \mathrm{std} \otimes \xi(\frac{\cdot}{d}))$, equal to $L_F(s, \Psi_d)$ up to the finitely many Euler factors at primes dividing $N_0 d$ that Lemma 3.5 removes, each vanishing only on $\operatorname{Re} s = 0$ (Lemma 3.4).

Theorem 5.1 (the choice of d)**.** *Let $37 \mid N_0$, $\beta > \frac{1}{2}$, $y \ge 0$, and let a be a unit modulo N_0 such that every prime $\equiv a \bmod N_0$ is $\equiv 7 \bmod 8$. There is a prime $d \equiv a \bmod N_0$ such that, for every character ξ modulo N_0, none of*

$$L(s, \xi(\tfrac{\cdot}{d})), \qquad L(s, \chi_{37}\xi(\tfrac{\cdot}{d})), \qquad L(s, \mathrm{std} \otimes \xi(\tfrac{\cdot}{d}))$$

vanishes on $\operatorname{Re} s \ge \beta$, $|\operatorname{Im} s| \le y$.

The development deduces its choice of d (`exists_entireL_quadTwist_ne_zero`) from a zero-density bound by a sum over the primes of a residue class. We follow its proof of that bound (`zero_density_quadTwist`, its form of the zero-density estimates for real characters of Jutila [10] and Heath-Brown [7, Thm. 3]), a three-lines argument with theta series and a mean value over d. The argument carries over to the twists of $L(s, \mathrm{std} \otimes \xi)$, of degree two over $\mathbb{Q}$, with three changes. The gamma factor becomes $\Gamma_{\mathbb{R}}(s+\mu)^2$, with kernel $x^\mu K_0(2\pi x)$; Poisson summation becomes Hecke's theta transformation over F; and the Pólya–Vinogradov mean square becomes Heath-Brown's large sieve for real characters [7, Cor. 3]. Write $g_\mu(x) = x^\mu e^{-\pi x^2}$ and $\Gamma_\mu(s) = \int_0^\infty g_\mu(x) x^{s-1} dx = \Gamma_{\mathbb{R}}(s+\mu)/2$, with $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$, as in the development.

Lemma 5.2. *Let $\mu \in \{0, 1\}$ and, for $x > 0$, $k_\mu(x) = \int_0^\infty g_\mu(x/v) g_\mu(v)\, dv/v$. Then $k_\mu(x) = x^\mu K_0(2\pi x)$, $\int_0^\infty k_\mu(x) x^{s-1} dx = \Gamma_\mu(s)^2$ on $\operatorname{Re} s > 0$, $|k_\mu(x)| \le C(1 + \log^+(1/x))e^{-x}$ and $|k_\mu'(x)| \le C(1 + 1/x)e^{-x}$.*

Proof. The Mellin transform of a Mellin convolution is the product of the transforms. The integrand is $x^\mu \exp(-\pi(x^2/v^2 + v^2))$; the substitution $w = \pi v^2$ and $K_0(z) = \frac{1}{2}\int_0^\infty \exp(-w - z^2/(4w))\, dw/w$ [6, 10.32.10] give $x^\mu K_0(2\pi x)$. The bounds follow from $k_\mu'(x) = \mu x^{\mu-1} K_0(2\pi x) - 2\pi x^\mu K_1(2\pi x)$, as $K_0' = -K_1$ [6, 10.29.3], and from $K_0(z) \sim -\log z$ and $K_1(z) \sim 1/z$ at 0 [6, 10.30.2–3] and $K_0(z) \le (\pi/2z)^{1/2} e^{-z}$, $K_1(z) \le (\pi/2z)^{1/2} e^{-z}(1 + 3/(8z))$ for $z > 0$ [6, 10.40.2 and §10.40(ii)]. □

Lemma 5.3 (the theta transformation over F)**.** *Let $\Psi \neq 1$ be a primitive Hecke character of finite order of F with the sign μ at both real places, $Q_\Psi = 37 \cdot \mathrm{N}\mathfrak{f}_\Psi$, and $\Theta_\Psi(u) = \sum_{n\geq 1} a_\Psi(n) k_\mu(nu)$ for $u > 0$.*

(a) $\int_0^\infty \Theta_\Psi(u) u^{s-1} du = \Gamma_\mu(s)^2 L_F(s,\Psi)$ *for* $\operatorname{Re} s > 1$*, and the same holds for* $\Theta_c = \sum c(n) k_\mu(nu)$*,* $|c(n)| \leq \tau(n)$*, with* $\sum c(n) n^{-s}$ *in place of* L*.*

(b) $\sqrt{Q_\Psi}\, u\, \Theta_\Psi(u) = W(\Psi)\, \overline{\Theta_\Psi(1/(Q_\Psi u))}$ *with* $|W(\Psi)| = 1$*.*

(c) $|\Theta_\Psi(u)| \leq C_\Psi e^{-u}$*; the identity of (a) for* Θ_Ψ *holds on* $\operatorname{Re} s > 0$*; and if* $T > 0$ *and* $Q_\Psi \leq T^2$*, then* $\int_0^\infty |\Theta_\Psi(u)| u^{-1/2} du \leq 2 \int_{1/T}^\infty |\Theta_\Psi(u)| u^{-1/2} du$*.*

In the development, part (a) is `mellin_gaussianTheta_char`. Part (b) is `norm_gaussianTheta_functional_equation`, used there too only in absolute value. The last clause of (c) is `thetaTailIntegral_zero_le_two_mul`.

Proof. (a) $|a_\Psi(n)| \leq \tau(n)$, so Fubini applies for $\operatorname{Re} s > 1$. (b) By Hecke's functional equation in the form given by Rademacher [16, §8, pp. 202–203], $\Lambda(s) = Q_\Psi^{s/2} \Gamma_{\mathbb{R}}(s+\mu)^2 L_F(s,\Psi)$ is entire, as Ψ has finite order and is not trivial, and $\Lambda(s) = W(\Psi)\Lambda(1-s,\bar\Psi)$ with $|W(\Psi)| = 1$. Moreover $L_F(s,\Psi)$ has polynomial growth in $|\operatorname{Im} s|$ on $-\frac12 \leq \operatorname{Re} s \leq \frac32$ [16, Thm. 5, p. 204], hence, by the functional equation and Stirling's formula, on $-1 \leq \operatorname{Re} s \leq 2$. By Mellin inversion of (a), $\Theta_\Psi(u) = \frac{1}{2\pi i}\int_{(2)} \Gamma_\mu(s)^2 L_F(s,\Psi) u^{-s} ds$. The factor $\Gamma_\mu(s)^2$ decays like $e^{-\pi|\operatorname{Im} s|/2}$, and $\Gamma_\mu(s)^2 L_F(s,\Psi) = Q_\Psi^{-s/2}\Lambda(s)/4$ is entire, so the line moves to $\operatorname{Re} s = -1$. There the integrand is $W(\Psi) Q_\Psi^{1/2-s} \Gamma_\mu(1-s)^2 L_F(1-s,\bar\Psi) u^{-s}$, and the substitution $w = 1-s$ gives $\Theta_\Psi(u) = W(\Psi)(\sqrt{Q_\Psi}\, u)^{-1} \Theta_{\bar\Psi}(1/(Q_\Psi u))$. Finally $\Theta_{\bar\Psi} = \overline{\Theta_\Psi}$, as k_μ is real. (c) For $u \geq 1$, $|\Theta_\Psi(u)| \leq \sum \tau(n) |k_\mu(nu)| \ll e^{-u}$. For $u < 1$ the same trivial bound gives $|\Theta_\Psi(u)| \ll u^{-1} \log^2(2/u)$, which is $\ll Q_\Psi (1 + \log Q_\Psi)^2$ on $[1/Q_\Psi, 1]$, and below $1/Q_\Psi$ we use (b). So the Mellin transform is holomorphic on $\operatorname{Re} s > 0$, and (a) extends by the identity theorem. For the fold, the substitution $v = 1/(Q_\Psi u)$ on $(0, 1/T)$ turns the integrand, by (b), into $|\Theta_\Psi(v)| v^{-1/2}$ on $(T/Q_\Psi, \infty)$, and $T/Q_\Psi \geq 1/T$. □

Lemma 5.4 (three lines in degree two)**.** *Fix $\mu \in \{0,1\}$. For c with $|c(n)| \leq \tau(n)$ put $\mathrm{Tail}(c, 1/T) = \int_{1/T}^\infty |\Theta_c(u)| u^{-1/2} du$. There is C such that the following holds for all $\eta \in (0, 1/18]$, $T \geq 2$, every Ψ as in Lemma 5.3 with $Q_\Psi \leq T^2$, and every zero s of $L_F(s,\Psi)$ with $\frac12 + 9\eta \leq \operatorname{Re} s \leq 1$: if $\mathrm{Tail}(a_\Psi, 1/T) + \mathrm{Tail}(\check a_\Psi, 1/T) \leq T^{2\eta}$, then $|\Gamma_\mu(s)|^4 \leq C T^{-2\eta} \log^2(2T)$.*

This is `three_lines_bound_of_LFunction_eq_zero` with Γ_μ^2 in place of Γ_μ; the factor $\log^2(2T)$ comes from the logarithmic singularity of K_0.

Proof. We have $|\check a_\Psi(n)| \leq \tau(n)$: at p the inverse Euler polynomial is $\prod_{\mathfrak{p}\mid p,\, \mathfrak{p}\nmid \mathfrak{f}_\Psi} (1 - \Psi(\mathfrak{p}) X^{f_\mathfrak{p}})$, with $f_\mathfrak{p}$ the residue degree, of degree at most two, with coefficient of absolute value at most two at X and at most one at X^2. Put $\gamma = \Gamma_\mu^2$, $f = \mathbf{1}_{(1/T,\infty)} \Theta_{\check a_\Psi}$ and

$$\Phi(z) = \gamma(z)^2 - \gamma(z) L_F(z,\Psi) \int_0^\infty f(u) u^{z-1} du.$$

By Lemma 5.3(c) and the decay of f, Φ is holomorphic and bounded on $\frac12 \leq \operatorname{Re} z \leq 2$; let B_μ bound $|\Gamma_\mu|$ there. On $\operatorname{Re} z = \frac12$, Lemma 5.3(c) gives $|\gamma L_F(z,\Psi)| \leq 2\,\mathrm{Tail}(a_\Psi, 1/T)$, and the integral is at most $\mathrm{Tail}(\check a_\Psi, 1/T)$; so $|\Phi| \leq B_\mu^4 + T^{4\eta}$. On $\operatorname{Re} z = 2$, Lemma 5.3(a) for $c = \check a_\Psi$ gives $\gamma/L_F = \int_0^\infty \Theta_{\check a_\Psi} u^{z-1} du$, so $\Phi(z) = \gamma L_F(z,\Psi) \int_0^{1/T} \Theta_{\check a_\Psi}(u) u^{z-1} du$. Since $|\Theta_{\check a_\Psi}(u)| \ll u^{-1} \log^2(2/u)$ for $u \leq 1$ and $\int_0^{1/T} \log^2(2/u)\, du \leq 3.5 \log^2(2T)/T$, we get $|\Phi| \leq$

$C_2T^{-1}\log^2(2T)$. Put $A=(B_\mu^4+C_2)T^{4\eta}$. Hadamard's three-lines theorem with $\lambda=(\operatorname{Re}s-\frac12)/\frac32\ge 6\eta$ gives $|\Phi(s)|\le A^{1-\lambda}(AT^{-1}\log^2(2T))^{\lambda}\le AT^{-6\eta}\log^2(2T)$. At the zero, $\Phi(s)=\Gamma_\mu(s)^4$. □

Lemma 5.5 (the mean value)**.** *Let $|c(n)|\le\tau(n)$ and $\mu\in\{0,1\}$. For every $\varepsilon>0$, uniformly in $X,T\ge 2$,*

$$\sum_{d\in\mathcal{D},\,d\le X}\operatorname{Tail}(c\chi_{-d},1/T)\ \ll_\varepsilon\ X^\varepsilon(XT^\varepsilon+X^{1/2}T^{1/2+\varepsilon});$$

in particular the sum is $\ll X^{1+2\varepsilon}$ for $T\ll X$.

Proof. Heath-Brown's Corollary 3 [7, p. 238] states that

$$\sum_{\chi\in\mathcal{R}(Q)}\Big|\sum_{n\le Y}a_n\chi(n)\Big|^2\ll_\varepsilon Q^\varepsilon Y^{1+\varepsilon}(Q+Y)\max_n|a_n|^2,$$

where $\mathcal{R}(Q)$ is the set of real primitive characters of conductor at most Q. The χ_{-d} with $d\in\mathcal{D}$, $d\le X$, are distinct elements of $\mathcal{R}(X)$. On a dyadic block, partial summation with $S(v)=\sum_{V<n\le v}c(n)\chi(n)$ and $w(v)=u|k_\mu'(vu)|$, and Cauchy–Schwarz, give

$$\Big|\sum_{V<n\le 2V}c(n)\chi(n)k_\mu(nu)\Big|^2\le 2|S(2V)|^2k_\mu(2Vu)^2+2\int_V^{2V}w\,dv\int_V^{2V}|S(v)|^2w(v)\,dv.$$

Summing over d and applying Corollary 3 to each $S(v)$ bounds the block sum by $X^\varepsilon V^{1+3\varepsilon}(X+V)K_V(u)^2$, where $K_V(u)=|k_\mu(2Vu)|+\int_{Vu}^{2Vu}|k_\mu'|\ll(1+\log^+(1/(Vu)))e^{-Vu/2}$ by Lemma 5.2. Summing the $O(\log(2/u))$ blocks with $Vu\le 1$ by Cauchy–Schwarz and the others by their exponential decay gives, after renaming ε, $\sum_d|\Theta_{c\chi_{-d}}(u)|^2\ll X^\varepsilon(X+1/u)u^{-1-2\varepsilon}$ for $u\le 1$; for $u\ge 1$ the sum is $\ll Xe^{-u}$ trivially, as $|\Theta_{c\chi_{-d}}(u)|\ll e^{-u}$ there. By Cauchy–Schwarz over d,

$$\begin{aligned}\sum_d\operatorname{Tail}(c\chi_{-d},1/T)&\le\int_{1/T}^\infty X^{1/2}\Big(\sum_d|\Theta_{c\chi_{-d}}(u)|^2\Big)^{1/2}\frac{du}{u^{1/2}}\\&\ll X^{\varepsilon/2}\int_{1/T}^1(Xu^{-1}+X^{1/2}u^{-3/2})u^{-\varepsilon}\,du+X,\end{aligned}$$

which is the bound stated. □

Remark 5.6. The development's own mean square (`sum_sq_gaussianTheta_jacobiSym_le`) expands the square, bounds the diagonal and the pairs $m\ne n$ with mn or $2mn$ a square trivially, and each other pair by Pólya–Vinogradov. In degree one the conductor is about d and the theta sums have length about $\sqrt{X}$, and this suffices. In degree two the conductor is about d^2 and the length about X: there are about X^2 other pairs, and for the pairs with mn of size comparable to X^2 the Pólya–Vinogradov bound for $\sum_{d\le X}(\frac{mn}{d})$ is no better than the trivial one. The method then gives $X^{3/2+\varepsilon}$ in place of $X^{1+\varepsilon}$, which fails for every $\eta<\frac14$. The saving has to come from cancellation over the pairs, which is what Heath-Brown's theorem provides.

Proposition 5.7. *Let ξ be a character modulo N_0, $\eta\in(0,1/18]$ and $y\ge 0$. The number of $d\in\mathcal{D}$, $d\le x$, for which $L(s,\mathrm{std}\otimes\xi(\frac{\cdot}{d}))$ has a zero with $\operatorname{Re}s\ge\frac12+9\eta$ and $|\operatorname{Im}s|\le y$ is $O(x^{1-\eta})$.*

This is the counterpart of `zero_density_quadTwist`. For the quadratic twists of a fixed modular elliptic curve an estimate of this kind is due to Perelli and Pomykała [15, Thm. 4], from the same large sieve.

Proof. By Lemma 3.4(a) the zeros in question are zeros of $L_F(s,\Psi_d)$, since the removed Euler factors vanish only on $\operatorname{Re} s=0$; they have $\operatorname{Re} s\le 1$ by the Euler product. Each Ψ_d is primitive and non-trivial (Lemma 3.4(b), Lemma 3.3) with the sign μ at both real places, and $a_{\Psi_d}=\chi_{-d}a_\Psi$, $\check a_{\Psi_d}=\chi_{-d}\check a_\Psi$. Put $T^2=37\mathfrak{N}\mathfrak{f}_\Psi\, x^2$, so that $Q_{\Psi_d}\le T^2$ for $d\le x$, and let $\gamma_0>0$ be the minimum of $|\Gamma_\mu(s)|^4$ on $[\frac12,1]\times[-y,y]$. For large x, $CT^{-2\eta}\log^2(2T)<\gamma_0$, so by Lemma 5.4 every bad d has $\operatorname{Tail}(a_\Psi\chi_{-d},1/T)+\operatorname{Tail}(\check a_\Psi\chi_{-d},1/T)>T^{2\eta}$. Summing with Lemma 5.5 at $\varepsilon=\eta/4$, the number of bad d is $\ll T^{-2\eta}x^{1+\eta/2}\ll x^{1-\eta}$. □

Proof of Theorem 5.1. Let $\eta=\min(\beta-\frac12,\frac12)/9$. The primes $d\le x$ with $d\equiv 7 \bmod 8$ and $d\nmid N_0$ for which $L(s,\psi(\frac{\cdot}{d}))$ has a zero in the box, for $\psi=\xi$ or $\chi_{37}\xi$, characters modulo N_0, number $O(x^{1-\eta/2})$ by `zero_density_quadTwist`. Those bad for $\mathrm{std}\otimes\xi$ number $O(x^{1-\eta})$ by Proposition 5.7, and the primes dividing $74N_0$ are finitely many. There are $\varphi(N_0)$ characters ξ. If every prime $\equiv a \bmod N_0$ were bad, $\sum_{p\equiv a\,(N_0)}1/p$ would converge, which it does not; this is the development's last step, now over three families. □

6. Polarity

For E the prime error weights a prime power by its Frobenius in $\mathrm{Gal}(L/\mathbb{Q})$ as well. Let $f=f_1+f_{\mathrm{sgn}}\,\mathrm{sgn}+f_{\mathrm{std}}\chi_{\mathrm{std}}$ be a real class function on $S_3=\mathrm{Gal}(L/\mathbb{Q})$, let M be a multiple of 74 and d an odd prime not dividing M. For a prime power $n=p^k$, $k\ge1$, with $p\nmid 74$, write $\mathrm{Frob}_n=\mathrm{Frob}_p^k$, a conjugacy class of S_3, as L is unramified outside 74. Put $\lambda_E(n)=0$ unless $n=p^k$ with $k\ge1$ and $n\equiv1 \bmod M$, so that $p\nmid 74$, and put

$$\lambda_E(n)=\Lambda(n)\Big(1-\Big(\frac{n}{d}\Big)\Big)\,f(\mathrm{Frob}_n),$$

and

$$R_E(x)=\sum_{n\le x}\lambda_E(n)\Big(\frac1n-\frac1x\Big)-f_{\mathrm{pole}}\frac{\log x}{\varphi(M)}-\kappa_E,\qquad f_{\mathrm{pole}}=f_1+f_{\mathrm{sgn}},$$

with the real constant κ_E fixed below. For $f=1$ this is the development's `primeError`. For $\pi\in\{1,\mathrm{sgn},\mathrm{std}\}$ and a character ψ modulo M or Md, write $L(s,1\otimes\psi)=L(s,\psi)$, $L(s,\mathrm{sgn}\otimes\psi)=L(s,\chi_{37}\psi)$ and $L(s,\mathrm{std}\otimes\psi)$ as in Lemma 3.5. Call $\pi\otimes\psi$ *trivial* when $L(s,\pi\otimes\psi)$ is the L-function of the principal character of the same modulus; as $37\mid M$, this happens exactly for $(1,1)$ and (sgn,χ_{37}), and never for std (Lemma 3.3) or for a twist by $(\frac{\cdot}{d})$. Let $\tilde L(s,\pi\otimes\psi)$ be $L(s,\pi\otimes\psi)$, multiplied by $s-1$ when $\pi\otimes\psi$ is trivial, and put

$$G_E(s)=\frac{1}{\varphi(M)}\Big[\sum_\pi f_\pi\sum_{\xi \bmod M}\Big(\frac{\tilde L'}{\tilde L}(s,\pi\otimes\xi(\tfrac{\cdot}{d}))-\frac{\tilde L'}{\tilde L}(s,\pi\otimes\xi)\Big)-f_{\mathrm{pole}}\Big],\qquad \kappa_E=\operatorname{Re}G_E(1).$$

Write $\Phi_E(s)=\int_0^\infty R_E(e^v)e^{(1-s)v}dv$ for $\operatorname{Re}s>2$, and

$$\mathrm{res}_E(s)=\sum_\pi f_\pi\sum_{\xi \bmod M}\frac{\operatorname{ord}_s\tilde L(s,\pi\otimes\xi)-\operatorname{ord}_s\tilde L(s,\pi\otimes\xi(\frac{\cdot}{d}))}{\varphi(M)\,s(1-s)}$$

for $s\ne0,1$, and $\mathrm{res}_E(0)=\mathrm{res}_E(1)=0$.

Proposition 6.1. *The function $v \mapsto R_E(e^v)$ is polar with residue function res_E, in the sense of the development (*`IsPolar`*). That is, it is measurable and $O(e^v)$ on $v \geq 0$; Φ_E continues meromorphically to $\mathbb{C}$; $(s-1)\Phi_E$ is analytic on $\operatorname{Re} s \geq 1$; and $\lim_{z\to\rho}(z-\rho)\Phi_E(z) = \operatorname{res}_E(\rho)$ for every ρ with $\operatorname{Re}\rho > 0$.*

We follow the proof of `isPolar_primeError` clause by clause, with f in place of 1. One classical fact on Hecke L-functions of F enters, for the characters Ψ_ψ of Lemma 3.5, their non-vanishing on $\operatorname{Re} s \geq 1$ [27, §2C]:

$$L_F(s, \Psi_\psi) \neq 0 \qquad (\operatorname{Re} s \geq 1). \tag{P}$$

Proof. On $\operatorname{Re} s > 1$, Lemma 3.5 and its counterparts for $\pi = 1, \operatorname{sgn}$ give the following identity, the sum being over the prime powers $n = p^k$, $k \geq 1$, with p prime to the modulus of ψ, which is a multiple of 74, so that Frob_n is defined:

$$\sum_n \Lambda(n)\psi(n) \operatorname{tr} \pi(\operatorname{Frob}_n) n^{-s} = \frac{\mathbf{1}[\pi \otimes \psi \text{ trivial}]}{s-1} - \frac{\tilde{L}'}{\tilde{L}}(s, \pi \otimes \psi).$$

Orthogonality, $\mathbf{1}[n \equiv 1 \bmod M] = \varphi(M)^{-1} \sum_\xi \xi(n)$, and $\xi(n)(1 - (\frac{n}{d})) = \xi(n) - \xi(\dot{\frac{}{d}})(n)$ give

$$\sum_n \lambda_E(n) n^{-s} = G_E(s) + \frac{f_{\text{pole}}}{\varphi(M)} \Big(\frac{1}{s-1} + 1 \Big).$$

The coefficients satisfy $|\lambda_E(n)| \leq 2(|f_1| + |f_{\text{sgn}}| + 2|f_{\text{std}}|)\Lambda(n)$, which gives measurability and the bound $O(e^v)$, and a direct computation of the transform gives

$$\Phi_E(s) = \frac{G_E(s)/s - \kappa_E}{s-1} \qquad (\operatorname{Re} s > 2).$$

Every $\tilde{L}(s, \pi \otimes \psi)$ is entire and none vanishes identically. For $\pi = \text{std}$ it is $L_F(s, \Psi_\psi)$, which is entire by Lemma 3.3, times the finite Euler polynomials of Lemma 3.5. For $\pi = 1$ and sgn it is a Dirichlet L-function, entire unless $\pi \otimes \psi$ is trivial, and for the trivial pairs $(1,1)$ and $(\operatorname{sgn}, \chi_{37})$ it is $(s-1)L$, again entire. So G_E is meromorphic on $\mathbb{C}$, and hence so is Φ_E. By (P) and its Dirichlet counterpart no $\tilde{L}$ vanishes on $\operatorname{Re} s \geq 1$, and the removed Euler factors of Lemma 3.5 do not vanish on $\operatorname{Re} s > 0$; so $(s-1)\Phi_E = G_E(s)/s - \kappa_E$ is analytic on $\operatorname{Re} s \geq 1$. As λ_E is real, G_E is real on $(2, \infty)$ and hence on $[1, \infty)$, so $(s-1)\Phi_E$ vanishes at $s = 1$, which is the limit $\operatorname{res}_E(1) = 0$. At $\rho \neq 1$ with $\operatorname{Re}\rho > 0$, $(z-\rho)\frac{\tilde{L}'}{\tilde{L}}(z) \to \operatorname{ord}_\rho \tilde{L}$, the order being finite as $\tilde{L}$ is entire and not identically zero; so $(z-\rho)\Phi_E(z) \to \operatorname{res}_E(\rho)$. □

Proposition 6.2 (the Landau step for E)**.** *Let $\beta > \frac{1}{2}$, let ρ be a point with $\operatorname{Re}\rho > \beta$, and let $M = N_0$ and d be as in Theorem 5.1 with $y \geq |\operatorname{Im}\rho|$. Suppose $f_\pi \geq 0$ for all π and $f_{\text{std}} > 0$. If $R_E(x) \leq x^{\beta-1}$ for all large x, then $L_F(\rho, \psi_3) \neq 0$.*

Proof. By the choice of d, no twist $\tilde{L}(s, \pi \otimes \xi(\dot{\frac{}{d}}))$ vanishes on $\operatorname{Re} s \geq \beta$, $|\operatorname{Im} s| \leq y$, so the twisted orders in res_E vanish at ρ and on the real interval $(\beta, 1)$. For real $s \in (\beta, 1)$ the remaining terms $f_\pi \operatorname{ord}_s \tilde{L}(s, \pi \otimes \xi)$ are non-negative, as $\tilde{L}$ is analytic there, and $s(1-s) > 0$, so $\operatorname{res}_E(s) \geq 0$; and $\operatorname{res}_E(s) = 0$ for real $s \geq 1$, by (P) and the value at 1. By Proposition 6.1 the function $v \mapsto R_E(e^v)$ is polar in the development's sense with residue function res_E, and it is at most $e^{(\beta-1)v}$ for large v. Landau's lemma (`IsPolar.landau`) then gives $\operatorname{res}_E(\rho) = 0$. Suppose $L_F(\rho, \psi_3) = 0$. Then $\tilde{L}(s, \text{std} \otimes 1)$, which is $L(s, \text{std})$ without its Euler factors at the primes dividing N_0, vanishes at ρ, as these factors do not vanish on $\operatorname{Re} s > 0$. So the numerator of $\operatorname{res}_E(\rho)$, a sum of non-negative terms, is at least $f_{\text{std}} \operatorname{ord}_\rho \tilde{L}(s, \text{std} \otimes 1) > 0$, a contradiction. □

This is the development's `entireL_ne_zero_of_primeError_le` with res_E in place of its residue function.

7. The cohomology step

The method bounds the denominators of its lattices by lengths of Tate-twisted Selmer groups of E. Of these it uses, at each twist index $e \geq 1$, only the subgroup of odd classes (Definition 7.1), and at $e = 0$ the whole class group. No splitting into odd and even halves is used, and at $\ell = 2$ one need not exist. In the development the field lies in a cyclotomic field and the step is written for that case. For a CM field the odd classes are a statement about its totally real subfield and characters of order at most two. The main conjecture for totally real fields at odd primes and Brumer–Stark over $\mathbb{Z}$ at the prime 2 bound them by special values of L-functions, for every CM field whose maximal totally real subfield is not $\mathbb{Q}$.

7.1. **What the step uses.** Let E be a CM field, c a complex conjugation, ℓ a prime, $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_\ell$, $e \geq 0$ and $\nu \geq 0$, and let χ_{cyc} be the ℓ-adic cyclotomic character.

Definition 7.1. $\mathrm{Sel}^-(\ell, E, \mathcal{O}, e, \nu)$ (`shaOdd`) is the $\mathcal{O}$-module of continuous cocycles $z\colon G_E \to \mathcal{O}/\ell^\nu$ for the action through χ_{cyc}^{-e} such that z vanishes on the inertia groups at the places not above ℓ; z vanishes, at each place $w \mid \ell$, on the inertia group if $e = 0$ and on $D_w \cap \ker \chi_{\mathrm{cyc}}$ if $e \neq 0$; and, if $e \neq 0$, $z(cgc) = -z(g)$ for all $g \in G_E$.

For $e \geq 1$, the character components used in the cyclotomic development have $\psi(-1) = (-1)^{e+1}$; these are exactly the parities for which the primitive Dirichlet L-value at $-e$ is non-zero. In the development the other cocycles never enter a length bound. The triangle-prime relations annihilate specified multiples of their tame values and give a coboundary relation for twice an even cocycle (`exists_isPrimeTriangle`). The existence of these primes uses a detecting set of Galois elements and reciprocity laws that hold for every field of the development's kind (`exists_isLaw`). The length of the odd classes enters the cost of the Tate-twisted cocycles as a hypothesis (`hasTriangleCost_tateTwist`). Its proof takes sums and differences of cocycles and never divides by 2. For positive twists the sum with the conjugate supplies the even relations at the triangle primes, and the difference maps to the odd cocycles whose length enters the denominator bound. The only length bound on the Selmer groups of the field is `exists_length_shaOdd_le`, which the row budget, the Ribet columns and the fit families use. Carried to $E = L \cdot k_d(\zeta_{N_1})$, the step's uses of the structure of its field are the four changes of Section 7.2, the places above g_0 and g_1 included, the odd-class bound (7.1) in place of that bound, and the labels of the places and the size bounds of Section 7.3. Here $N = N_1 d$, t is the development's number of twists, and $v_{\mathcal{O}}$ is the normalized valuation of $\mathcal{O}$.

At $E = L \cdot k_d(\zeta_{N_1})$ the chain uses the odd-class bound. There is an integer $X \geq 1$ with

$$X \leq 2^{4(N+t+3)^{27}} h_E \qquad \text{and} \qquad \operatorname{length}_{\mathcal{O}} \mathrm{Sel}^-(\ell, E, \mathcal{O}, e, \nu) \leq v_{\mathcal{O}}(X) \tag{7.1}$$

for every prime ℓ, every $\mathcal{O}$ containing the roots of unity of order the exponent of $(\mathbb{Z}/N)^\times$, every $0 \leq e < t$ and every ν. The Ribet columns use the clause $X \neq 0$ and the lengths, and the fit families use the size only through $\log X$ (`exists_isFitFamily`). The case $e = 0$ is immediate: the module is then $\mathrm{Hom}(\mathrm{Cl}(E), \mathcal{O}/\ell^\nu)$, of length at most $v_{\mathcal{O}}(h_E)$, for every totally complex field.

7.2. **The four changes.** Fix an embedding of E in $\bar{\mathbb{Q}}$ extending the development's embedding of $k_d(\zeta_{N_1})$.

(D0) *The embedding.* E is a CM field containing a primitive 5040-th root of unity (Lemma 3.6), and it lies in $L \cdot \mathbb{Q}(\zeta_N)$, as $k_d(\zeta_{N_1}) \subset \mathbb{Q}(\zeta_N)$. This replaces `Data.algebraMap_mem_cycloField`.

(D1) *A detecting set* (replacing `exists_detecting_points_cocycles`). Let E be a CM field contained in $L \cdot \mathbb{Q}(\zeta_N)$. For every prime ℓ there is a finite set $\Sigma \subset G_E$ such that every cocycle $G_E \to (\mathcal{O}/\ell^\nu)(-e)$ unramified outside ℓ that vanishes on Σ is zero, for all $\mathcal{O}$, ν and e; and $\#\Sigma \le y^{20}$ whenever $N \le y$, $\ell \le y^2$ and $y \ge 3$.

(D2) *Inertia above a large prime.* If $\ell \nmid N \cdot d_L$, an element of an inertia group above ℓ fixes E. This is used in `exists_cycChar_pow_sub_one_dvd`, where $\ell > N$.

(D3) *Roots of unity.* If g fixes μ_N and fixes L pointwise, then g fixes E (replacing `fixes_emb_of_fixes_rootsOfUnity`, which for E is false as stated, since an element that fixes μ_N can move L). It is applied at the primes g_0, g_1 of the data, where it needs them split completely in L (Corollary 4.3), and at an inertia element above a prime not dividing Nd_L, which fixes L. The same splitting gives what the step uses at the places above g_0, g_1. As $g_i \equiv 1 \bmod N$ splits completely in $k_d(\zeta_{N_1})$ and in L, it splits completely in E, so its Frobenius in $\mathrm{Gal}(E/\mathbb{Q})$ is trivial and the residue fields above it have g_i elements.

Proofs. (D0) and (D3) hold because E is generated by L and $k_d(\zeta_{N_1})$. For (D2), an inertia group above ℓ acts trivially on every subfield of $\bar{\mathbb{Q}}$ unramified at ℓ. For (D1), detection modulo π^k, for a uniformizer π of $\mathcal{O}$, follows from detection modulo π by induction on k. If z vanishes on Σ, its reduction modulo π is a cocycle of the same kind, hence zero, so $z = \pi z'$ with z' a cocycle of the same kind modulo π^{k-1} that vanishes on Σ. Modulo π, the proof of `exists_detecting_points_cocycles` applies with $\mathbb{Q}(\zeta_{N'})$, $N' = N\ell^2$, replaced by $E' = L(\zeta_{N'})$, which contains E, is Galois over $\mathbb{Q}$ and is totally complex: $G_{E'}$ lies in G_E and in the kernel of χ_{cyc} mod ℓ^2. The set Σ consists of coset representatives of $G_E/G_{E'}$, at most $n' = [E' : \mathbb{Q}] \le 6N'$ of them, and the detecting points for homomorphisms on $G_{E'}$ that class field theory gives (`exists_detecting_points_hom`). Their number is at most $\log_2$ of $h_{E'}$ times the index of the N'-th powers at the places above ℓ. The class number is at most $(2^{n'}|d_{E'}|)^{n'+1}$ (`classNumber_le`). The index is at most $N'^{3n'}$ (`index_pow_at_places_le`). With $|d_{E'}| \le |d_L|^{\varphi(N')}|d_{\mathbb{Q}(\zeta_{N'})}|^6 \le 810448^{N'}N'^{6N'}$ (the different of E' over one factor divides the different of the other, extended to E'), $\log_2 810448 < 20$ and $\log_2 N' \le N'$, one gets

$$\#\Sigma \le 6N' + (6N'+1)(26N' + 6N'^2) + 18N'^2 = 36N'^3 + 180N'^2 + 32N'.$$

As $N' \le y^5$ and $u^3 - 36u^2 - 180u - 32 > 0$ for $u \ge 243$, this is at most y^{20} for $y \ge 3$. □

7.3. **The places, their labels and the size bounds.**

The places and their labels. The infinite places of E form a group, transported from $\mathcal{G} = \mathrm{Gal}(E/k_d)$, and for E this group is not commutative. The class of a place (`Parameters.placeClass`) is its image under the restriction $\mathcal{G} \to \mathrm{Gal}(B/k_d) \cong (\mathbb{Z}/N_1)^\times$, a homomorphism, with $B = k_d(\zeta_{N_1})$ the development's field. The cohomology step uses the places only through the group law and the class, that is, through the CM type and the thick places. The one statement of the step that takes the ratio of two places, the spacing of the thick places (`placeClass_ratio`), uses the ratio only through its class, in a commutative group, so the order of the two factors does not matter; for E the ratio of v to v' is $v'^{-1}v$. The action of Frobenius on the places, the tops and the thick places are the subject of Section 9.1.

The size bounds. The step uses three size statements whose terms depend on the field: bounds for the number of infinite places, for the root discriminant, and for the order of the group it chooses (`Data.HasLogBound`). Their constant is the development's `Parameters.c`, which we write c_*: the sum of the constant C of the generator of the vacuum (Section 8.3), $2d+6$, N_0, $|c_d|$ and $\sum_\xi |\log|\Phi'_{N_0}(\xi)||$ over the primitive N_0-th roots of unity ξ. For E the generator constant is $C_E = C_0 + 240^2 + 240$, so $c_* \geq C_0 + 240^2 + 240$, and $c_* \geq \max(64, N_0, d, \varphi(N_0))$ (`Data.c_ge`). Let $\mathfrak{n} \in [x^5, 3x^5]$ be the rank of the development's spaces and $t = 5\mathfrak{n}$. Lemma 7.2 replaces these three statements, which the development proves from the cyclotomic structure of B (`Data.hasLogBound_f`, `Data.hasLogBound_rootDisc`, and the bound for `Data.chosenGroupOrder`).

Lemma 7.2. *At every datum:*

(a) $x^{11} \leq \#\mathcal{G} \leq e^{c_*} x^{11} (\log b)^{1/5}$, *and* $\#\mathcal{G}$ *is even and at most* N_1*;*

(b) $x^{10} \leq \mathrm{rd}_E \leq x^{12}$*;*

(c) *the product of the groups* $\mathrm{GL}_{\mathfrak{n}t}(\mathcal{O}_E/w)$ *over the primes* w *of* E *that divide* $\bar{\varpi}$ *has order at most* $\exp(x^{32})$.

Proof. Put $X = \log x$, $H = \log\log b$ and $U = N_1/N_0$. The scale conditions of the data give $H \geq 10^{12} c_*$, $X \geq 100H$ and $6\log(10^6 X) \leq H$ (`Data.scale`), and $x^{11} \leq U \leq x^{11} e^{H/5}$, as $U = 3^{\lfloor \log_3 r \rfloor + 5} 2^r$, where $2^r = m^{22}$ for the number m of lifts, $x^{1/2} \leq m \leq 2x^{1/2}$ and $r \leq 32X$.

(a) As N_0 and N_1 have the same prime divisors, $\#\mathcal{G} = 3\varphi(N_1) = 3\varphi(N_0)U$. So $\#\mathcal{G} \geq x^{11}$, and $\log \#\mathcal{G} \leq \log(3c_*) + 11X + H/5$, which is below $c_* + 11X + H/5$ by $c_* - \log(3c_*) > 58$. The number $\#\mathcal{G}$ is even, and $3\varphi(N_1) \leq N_1$, as $6 \mid N_0$ gives $N_1/\varphi(N_1) \geq 3$.

(b) At the place of B where $\zeta \mapsto \eta$, the development's generator γ_B of $\mathfrak{D}_{B/\mathbb{Q}}$ has absolute value $\sqrt{d}\,|\Phi'_{N_1}(\eta)| = U\sqrt{d}\,|\Phi'_{N_0}(\eta^U)|$ (`Parameters.infinitePlace_apply_varpi`), by differentiating $\Phi_{N_1}(Y) = \Phi_{N_0}(Y^U)$, and η^U runs over the primitive N_0-th roots of unity, each equally often. The geometric mean of these sizes is rd_B, so $|\log \mathrm{rd}_B - \log U| \leq \frac{1}{2}\log d + \sum_\xi |\log|\Phi'_{N_0}(\xi)|| \leq c_*$. As $\mathrm{rd}_B \leq \mathrm{rd}_E$ in the tower E/B, and $\mathrm{rd}_E \leq \mathrm{rd}_L\,\mathrm{rd}_B$ (Lemma 3.6) with $\mathrm{rd}_L = (2^4 \cdot 37^3)^{1/6} < 10$,

$$10X \leq 11X - c_* \leq \log \mathrm{rd}_E \leq 11X + H/5 + c_* + \log 10 \leq 12X,$$

with margins $X - c_*$ and $X - H/5 - c_* - \log 10$.

(c) As $\varpi\bar{\varpi} = g_0 g_1$, the ideal $(\bar{\varpi})$ is the product of a prime of k_d above g_0 and one above g_1, and as g_0, g_1 split completely in E (Section 4), each has $\#\mathcal{G}$ primes of E above it, of norm g_i. So the logarithm of the order is at most $\#\mathcal{G}(\mathfrak{n}t)^2 \log(g_0 g_1)$. By (a), $(\mathfrak{n}t)^2 \leq 2025x^{20}$ and $g_0 g_1 \leq b^{22}$, the logarithm of this bound is at most $(11X + H/5 + c_*) + (20X + 22) + (H + 100)$, which is below $32X$ by $X - 6H/5 - c_* - 122 > 0$. □

Bound (a) is used by the denominator bound, the one-place defect, the Ribet element and the twist fitting, and its last clause by the generator of the vacuum and the Gaussian estimate for the Galois conjugates of the jets; (b) by the class-number bound of the twist fitting; and (c) by the twist fitting. These include the size inequality that the bound (7.1) must meet. The separate bounds for the generator of the different are proved in Section 8.4.

7.4. **The odd half by *L*-values.** Let E be a CM field with $n_+ = [E^+ : \mathbb{Q}] \geq 2$, $e \geq 1$, and let φ_e be the trivial character of G_{E^+} if e is odd and the quadratic character η of E/E^+ if e is even, so that $\varphi_e(c) = (-1)^{e+1}$. Let S' be the set of places of E^+ ramified in E/E^+ together

with the real places, S_ℓ the places above ℓ and ∞, and $w_{e+1}(E) = \#H^0(E, \mathbb{Q}/\mathbb{Z}(e+1))$. Put

$$Y_e = w_{e+1}(E)\, L_{E^+,S'}(-e, \varphi_e), \qquad \delta_e(v) = \begin{cases} \ell^{\,1+v_\ell([E_v^+:\mathbb{Q}_\ell])+v_\ell(e)} & \text{if } [E_v^+(\mu_\ell) : E_v^+] \mid 2e, \\ 1 & \text{otherwise,} \end{cases}$$

for a place $v \mid \ell$ of E^+. For $\ell = 2$ let $S = S' \cup S_2$, let $q \notin S$ be a prime of E^+ of residue characteristic greater than $n_+ + 1$, and put

$$a_e = 2^{1-n_+}(1 - \varphi_e(q)\mathrm{N}q^{1+e})L_{E^+,S}(-e, \varphi_e).$$

Both are rational by Siegel's theorem [5, §0, pp. 230–231], as φ_e takes rational values and the removed Euler factors are rational, and the parity of φ_e makes them non-zero.

Theorem 7.3. *Let E be a CM field with $[E^+ : \mathbb{Q}] \geq 2$ and $e \geq 1$.*

(a) *If ℓ is odd,* $\mathrm{length}_{\mathcal{O}} \mathrm{Sel}^-(\ell, E, \mathcal{O}, e, \nu) \leq v_{\mathcal{O}}(Y_e) + \sum_{v|\ell} v_{\mathcal{O}}(\delta_e(v))$.

(b) *If $\ell = 2$, then $a_e \in \mathbb{Z}_2$ and $2a_e$ annihilates* $\mathrm{Sel}^-(2, E, \mathcal{O}, e, \nu)$*; and for every finite $\Sigma \subset G_E$ such that every cocycle $G_E \to (\mathcal{O}/2^\nu)(-e)$ unramified outside 2 that vanishes on Σ is zero (for E as in (D1), the set given there),*

$$\mathrm{length}_{\mathcal{O}} \mathrm{Sel}^-(2, E, \mathcal{O}, e, \nu) \leq \#\Sigma \cdot v_{\mathcal{O}}(2^{1+v_2(a_e)}).$$

The first step passes from E to E^+. Let A_e be $\mathcal{O}/\ell^\nu$ with G_{E^+} acting through $\chi_e = \chi_{\mathrm{cyc}}^{-e}\varphi_e$; then c acts by -1.

Lemma 7.4. *Restriction to G_E is a bijection from the continuous cocycles $Z\colon G_{E^+} \to A_e$ with $Z(c) = 0$ onto the continuous cocycles $z\colon G_E \to (\mathcal{O}/\ell^\nu)(-e)$ with $z(cgc) = -z(g)$, for every prime ℓ.*

Proof. If $Z(c) = 0$, then $Z(cgc) = c \cdot Z(gc) = c \cdot Z(g) = -Z(g)$ for $g \in G_E$. Conversely, given an odd z, put $Z(h) = Z(hc) = z(h)$ for $h \in G_E$. Using $ch = (chc)c$ and $z(chc) = -z(h)$, the cocycle rule for the products $h_1 \cdot h_2 c$, $h_1 c \cdot h_2$ and $h_1 c \cdot h_2 c$ reduces to that of z. Uniqueness: $Z(hc) = Z(h) + h \cdot Z(c) = Z(h)$. □

The only arithmetic input at odd ℓ is the following lemma.

Lemma 7.5 (the orders at odd primes)**.** *Let ℓ be odd and S a finite set of places of E^+ containing S' and the places above ℓ; if e is odd, it suffices that S contain the infinite places and those above ℓ. Then*

$$v_\ell \#H^2(\mathcal{O}_{E^+,S}, \mathbb{Z}_\ell(e+1) \otimes \varphi_e) = v_\ell(w_{e+1}(E)\, L_{E^+,S}(-e, \varphi_e)).$$

Proof. Write $n = e+1$. For a number field Ω and finite sets $P \subseteq P'$ of places of Ω containing those above ℓ and ∞, the localization sequence

$$0 \to H^2(\mathcal{O}_{\Omega,P}, \mathbb{Z}_\ell(n)) \to H^2(\mathcal{O}_{\Omega,P'}, \mathbb{Z}_\ell(n)) \to \bigoplus_{w \in P' \smallsetminus P} H^1(k_w, \mathbb{Z}_\ell(e)) \to 0$$

is exact, as $H^0(k_w, \mathbb{Z}_\ell(e)) = 0$, and $H^1(k_w, \mathbb{Z}_\ell(e)) \cong \mathbb{Z}_\ell/(\mathrm{N}w^e - 1)$.

Let e be odd, so that $\varphi_e = 1$ and n is even. By Wiles's theorem [28, Thm. 1.6] for the totally real field E^+, $\zeta_{E^+}(-e)$ and $\#H^2(\mathcal{O}_{E^+}[1/\ell], \mathbb{Z}_\ell(n))/\#H^1(\mathcal{O}_{E^+}[1/\ell], \mathbb{Z}_\ell(n))$ have the same ℓ-adic valuation. The group $H^1(\mathcal{O}_{E^+}[1/\ell], \mathbb{Z}_\ell(n))$ is finite of order $\#H^0(E^+, \mathbb{Q}_\ell/\mathbb{Z}_\ell(n))$ [11, p. 669], which is the ℓ-part of $w_n(E)$, as c acts on $\mathbb{Q}_\ell/\mathbb{Z}_\ell(n)$ by $(-1)^n = 1$. The localization sequence for $\Omega = E^+$ then multiplies the order by $|1 - \mathrm{N}w^e|_\ell^{-1}$ for each finite $w \in S$ not above ℓ: these are the Euler factors removed from $L_{E^+,S}(-e, 1)$, apart from those at $w \mid \ell$, which are ℓ-adic units.

Let e be even, so that $\varphi_e = \eta$ and $n \geq 3$ is odd, and let a superscript $-$ denote the part on which c acts by -1. Kolster's formula [11, Prop. 1.1] rests on Wiles's main conjecture [28, Thm. 1.3] for the even character $\eta\omega^n$, with ω the Teichmüller character modulo ℓ ($\psi = \chi\omega^{-n}$ on p. 670 of [11], with $\chi = \eta$; the two relations Kolster states after it hold for $\chi\omega^n$), and on the equality of μ-invariants for the ℓ-ramified module [11, p. 671], which comes from [28, Thm. 1.4] by Iwasawa's reflection. With the isomorphism $H^1(\mathcal{O}_E[1/\ell], \mathbb{Q}_\ell/\mathbb{Z}_\ell(n))^- \cong H^2(\mathcal{O}_E[1/\ell], \mathbb{Z}_\ell(n))^-$ of the proof of [11, Prop. 1.2], it gives

$$v_\ell \# H^2(\mathcal{O}_E[1/\ell], \mathbb{Z}_\ell(n))^- = v_\ell\big(w_n(E)\, L_{E^+,S'}(-e, \eta)\big).$$

The localization sequence for $\Omega = E$, from the places above ℓ and ∞ to those above S, commutes with c. For a finite $v \in S$ not above ℓ, the minus part of $\bigoplus_{w|v} H^1(k_w, \mathbb{Z}_\ell(e))$ has order $|1 - \eta(v)\mathrm{N}v^e|_\ell^{-1}$: if v splits, c exchanges the two summands; if v is inert, c acts on $\mathbb{Z}_\ell/(\mathrm{N}v^{2e} - 1)$ by $\mathrm{N}v^e$; if v is ramified, it acts trivially. These are the Euler factors removed from $L_{E^+,S}(-e, \eta)$ and not from $L_{E^+,S'}(-e, \eta)$, apart from those at $v \mid \ell$, which are units. Finally, as S contains the places ramified in E/E^+, Shapiro's lemma identifies $H^2(\mathcal{O}_{E^+,S}, \mathbb{Z}_\ell(n) \otimes \eta)$ with $H^2(\mathcal{O}_{E,S}, \mathbb{Z}_\ell(n))^-$, ℓ being odd. □

Proof of Theorem 7.3(a). Let $S = S' \cup S_\ell$ if e is even and $S = S_\ell$ if e is odd. By Lemma 7.4 the module is that of the cocycles Z on G_{E^+} with $Z(c) = 0$ whose restrictions satisfy the local conditions. A coboundary $(g-1)a$ takes the value $-2a$ at c, so these cocycles inject into $H^1(G_{E^+}, A_e)$; the local conditions concern subgroups of G_E on which χ_e is trivial, so they are conditions on classes. Let $\mathcal{S}$ be the image.

Away from ℓ. For $v \nmid \ell$ the class vanishes on $I_v \cap G_E$, of index at most two in I_v, so it vanishes on I_v, ℓ being odd. Thus $\mathcal{S} \subseteq H^1(G_{E^+,S}, A_e)$; for e odd this uses that A_e is unramified outside ℓ, and for e even that χ_e is unramified outside S. If e is even and $v \in S'$ is finite and prime to ℓ, the class is moreover trivial on the decomposition group D_v: an element of $I_v \smallsetminus G_E$ acts on A_e by -1, so $A_e^{I_v} = A_e[2] = 0$ and $H^1(D_v, A_e) \to H^1(I_v, A_e)$ is injective. At the real places H^1 vanishes.

Above ℓ. Let $U_v = D_v \cap G_E \cap \ker \chi_{\mathrm{cyc}}$ and $\Pi_v = D_v/U_v \cong \mathrm{Gal}(E_w(\mu_{\ell^\infty})/E_v^+)$, an abelian group with a finite part Π_v' of order prime to ℓ and an open pro-ℓ part $\cong \mathbb{Z}_\ell$. The local condition says the class lies in $H^1(\Pi_v, A_e)$. If χ_e is non-trivial on Π_v' this group is zero; otherwise $\chi_{\mathrm{cyc}}^{2e} = \chi_e^{-2}$ is trivial on Π_v', which maps onto $\mathrm{Gal}(E_v^+(\mu_\ell)/E_v^+)$, so $\chi_{\mathrm{cyc}}^{2e} \equiv 1 \bmod \ell$ there, that is, $[E_v^+(\mu_\ell) : E_v^+] \mid 2e$; and the group is $A_e/(\chi_{\mathrm{cyc}}(\gamma)^{-e} - 1)A_e$ for a generator γ of the pro-ℓ part. Since $\chi_{\mathrm{cyc}}(\gamma)$ generates $1 + \ell^{1+j}\mathbb{Z}_\ell$ with $j \leq v_\ell([E_v^+ : \mathbb{Q}_\ell])$, the length is at most $v_{\mathcal{O}}(\delta_e(v))$. So $\mathcal{S}$ maps to $\bigoplus_{v|\ell} H^1(\Pi_v, A_e)$ with kernel in $Ш^1(G_{E^+,S}, A_e)$.

Duality. At each real place c_v acts on $\mathbb{Q}_\ell/\mathbb{Z}_\ell(\chi_e)$ by -1, so $H^0(G_{E^+,S}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(\chi_e)) = 0$ and $Ш^1(G_{E^+,S}, A_e)$ injects into $Ш^1(G_{E^+,S}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(\chi_e)) \otimes_{\mathbb{Z}_\ell} \mathcal{O}$. Before the coefficients are extended, Poitou–Tate duality [14, (8.6.7)], at finite levels and in the limit, identifies the dual of $Ш^1(G_{E^+,S}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(\chi_e))$ with a subgroup of $H^2(G_{E^+,S}, \mathbb{Z}_\ell(e+1) \otimes \varphi_e)$. The length inequality then extends to $\mathcal{O}$ by $\mathrm{length}_{\mathcal{O}}(T \otimes_{\mathbb{Z}_\ell} \mathcal{O}) = v_{\mathcal{O}}(\#T)$ for finite T. For e odd, $S = S_\ell$ and this group injects into the one at level $S' \cup S_\ell$, as the localization sequence has $H^0(k_v, \mathbb{Z}_\ell(e)) = 0$ at the added places. Lemma 7.5 at level $S' \cup S_\ell$ then bounds the length by $v_{\mathcal{O}}(w_{e+1}(E) L_{E^+,S' \cup S_\ell}(-e, \varphi_e)) = v_{\mathcal{O}}(Y_e)$, since the Euler factors $1 - \varphi_e(v)\mathrm{N}v^e$ at the places $v \mid \ell$ not in S' are ℓ-adic units. □

Proof of Theorem 7.3(b). Let $E_\infty = E(\mu_{2^\infty})$, $E_m = E(\mu_{2^m})$ for $m \geq 2$, and $\chi_e = \chi_{\mathrm{cyc}}^{-e}\varphi_e$ on G_{E^+}, so $\chi_e(c) = -1$; the group $\mathrm{Gal}(E_\infty/E^+)$ is abelian.

To equivariant homomorphisms. Let $z \in \mathrm{Sel}^-(2, E, \mathcal{O}, e, \nu)$. On G_{E_∞}, $\chi_{\mathrm{cyc}} = 1$, so z restricts to a homomorphism z_∞, which by the local conditions kills every inertia and every decomposition group above 2 of E_∞. The cocycle rule and oddness give $z_\infty(gxg^{-1}) = \chi_e(g)z_\infty(x)$ for $g \in G_{E^+}$. So z_∞ factors through the Galois group X'_∞ of the maximal abelian pro-2 extension of E_∞ unramified everywhere and split above 2, and, since $z_\infty((1+c)x) = (1+\chi_e(c))z_\infty(x) = 0$, through the minus quotient $X'^-_\infty = X'_\infty/(1+c)X'_\infty$. Here $M^- = M/(1+c)M$ for a module M on which c acts, as in [3]. If $z_\infty = 0$, then z factors through the abelian group $\mathrm{Gal}(E_\infty/E)$, where cgc and g have the same image, so $z(g) = -z(g)$ and $2z = 0$.

Brumer–Stark at the layers. E_m/E^+ is abelian and CM, ramified only in S, and $T = \{q\}$ satisfies the Deligne–Ribet condition. By Dasgupta, Kakde, Silliman and Wang [3, Thm. 2.4], $\Theta_m = \Theta_{S,T}(E_m/E^+)/2^{n_+-1}$ annihilates $\mathrm{Cl}^T(E_m)^-$, hence its quotient A_m^-, where $A_m = \mathrm{Cl}(E_m) \otimes \mathbb{Z}_2$.

The limit. The Θ_m are compatible, as S contains every place ramified in every E_m, and define $\Theta_\infty \in \mathbb{Z}_2[[\mathrm{Gal}(E_\infty/E^+)]]^-$. For m_0 large, E_∞/E_{m_0} is a $\mathbb{Z}_2$-extension in which every prime above 2 is totally ramified, so the unramified Iwasawa module X_∞ is the limit of the A_m [14, (11.1.5)], equivariantly. As the A_m are finite, the limit is exact on them, so $X_\infty^- = X_\infty/(1+c)X_\infty = \varprojlim A_m^-$. So Θ_∞ annihilates X_∞^- and its quotient X'^-_∞.

Evaluation. $z_\infty(\Theta_\infty x) = \chi_e(\Theta_\infty)z_\infty(x)$, so $\chi_e(\Theta_\infty)z_\infty = 0$. Let $\mathfrak{f} = \mathfrak{f}(E/E^+)\prod_{v|2} v$, and let P be the image in $\mathbb{Z}_2[[\mathrm{Gal}(E_\infty/E^+)]]^-$ of Deligne and Ribet's measure $\mu_{[q],1}$ on the ray class group of conductor $\mathfrak{f}^\infty$ [5, (0.4)–(0.5)], which applies as $E^+ \neq \mathbb{Q}$, under restriction followed by $g \mapsto g^{-1}$. At each layer, $\mathbb{Z}_2[\mathrm{Gal}(E_m/E^+)]^-$ is free over $\mathbb{Z}_2$ on one element of each pair $\{g, cg\}$, so it embeds in its scalar extension, the product of the factors of the odd characters. For every odd finite-order character ψ of $\mathrm{Gal}(E_m/E^+)$, $\psi(P_m) = L_{S,T}(\psi^{-1}, 0) = 2^{n_+-1}\psi(\Theta_m)$, so $P_m = 2^{n_+-1}\Theta_m$, and hence $P = 2^{n_+-1}\Theta_\infty$. Since χ_e is odd and continuous, (0.5) of [5] at $k = e+1$ gives $2^{n_+-1}\chi_e(\Theta_\infty) = \chi_e(P) = (1-\varphi_e(q)\mathrm{N}q^{1+e})L_{E^+,S}(-e, \varphi_e)$. Therefore $\chi_e(\Theta_\infty) = a_e$, which lies in $\mathbb{Z}_2$ as Θ_∞ is integral. So $a_e z$ vanishes on G_{E_∞}, and by the first step $2a_e z = 0$. Finally $z \mapsto (z(g))_{g\in\Sigma}$ embeds the module in $(\mathcal{O}/2^\nu)^{\#\Sigma}$, with image killed by $2^{1+v_2(a_e)}$. □

For our field this gives the statement the chain uses.

Corollary 7.6. *Let $E = L \cdot k_d(\zeta_{N_1})$ with $37 \mid N_0$, $y = N + t + 3$, Σ the set of (D1) for $\ell = 2$, and q a prime of E^+ above the least prime $p > n_+ + 1$ with $p \nmid 2d_E$. For a non-zero rational Y write $|Y|_{\mathrm{odd}} = \prod_{\ell \text{ odd}} \ell^{v_\ell(Y)}$, and put $\Delta_e = \prod_{\ell \text{ odd}} \prod_{v|\ell} \delta_e(v)$ and*

$$X = h_E \prod_{1 \le e < t} |Y_e|_{\mathrm{odd}}\, \Delta_e\, 2^{\#\Sigma(1+v_2(a_e))}.$$

Then X is a positive integer, $X \le \exp(O(y^{24}))\, h_E$, and the odd-class bound (7.1) holds with this X.

Proof. By Lemma 7.5 with $S = S' \cup S_\ell$, $v_\ell(Y_e) \ge 0$ for every odd ℓ, so $|Y_e|_{\mathrm{odd}}$ is an integer; and $v_2(a_e) \ge 0$. The lengths are bounded by Theorem 7.3 for $e \ge 1$ and by $v_\mathcal{O}(h_E)$ for $e = 0$, and in each case the length bound is at most $v_\mathcal{O}(X)$ by the product formula for X. The size has three inputs, for $1 \le e < t$, where $t < y$. First, $\#\Sigma \le y^{20}$ by (D1). Second, $\log_2 |Y_e| \le 8y^3$ and $\log \Delta_e \le 60y^3$. Here $[E : \mathbb{Q}] \le 6N$ by Lemma 3.6, so $n_+ \le 3y$; $\log |d_E| \le N^2$, as E is unramified outside $74dN_1$ and the exponents of the discriminant are bounded as in [21, III §6]; the functional equations of ζ_E and ζ_{E^+} then give $\log |L_{E^+}(-e, \varphi_e)| \le 3y^3$, and $w_{e+1}(E) \le (4(e+1)[E : \mathbb{Q}])^{\pi(4(e+1)[E:\mathbb{Q}])}$ is bounded by [17]; a factor $\delta_e(v) \neq 1$ needs

$\ell - 1 \le 2en_+$, so $\ell \le 7y^2$, and $\delta_e(v) \le \ell\,[E_v^+ : \mathbb{Q}_\ell]\,e$. So $\prod_{v|\ell}\delta_e(v) \le (\ell n_+ e)^{n_+}$, and as $7y^2 n_+ e \le (7y^2)^2$ and $\pi(u) < 1.25506\,u/\log u$ [17], $\log\Delta_e \le n_+\pi(7y^2)\cdot 2\log(7y^2) < 60y^3$. Third, $v_2(a_e) \le 10y^3$ and $\log_2|Y_e|_{\mathrm{odd}} \le 10y^3$. The Euler factors above 2 are odd, $n_+ \ge 2$ and $w_{e+1}(E)$ is even, so $v_2(a_e) \le v_2(Y_e) + v_2(1-\varphi_e(q)\mathrm{N}q^{1+e})$ with $v_2(Y_e) \le \log_2|Y_e|$, and, as $a_e \in \mathbb{Z}_2$, $-v_2(Y_e) \le v_2(1-\varphi_e(q)\mathrm{N}q^{1+e}) \le 2y^3$, since $\log_2 \mathrm{N}q \le n_+\log_2 p \le y^2$, where $p \le 6N^2\log N$ as at most $2N^2$ primes divide d_E and at most $3N+1$ are at most $n_+ + 1$, while $\pi(u) \ge u/\log u$ for $u \ge 17$ [17]. Summing gives $\log_2(X/h_E) \le 12y^{24} \le 4y^{27}$. □

Remark 7.7. For $E = L\cdot k_d(\zeta_{N_1})$ the extension E/E^+ is unramified at every finite place (Lemma 3.6), so S' consists of the real places and both parities in the proof of Theorem 7.3(a) use $S = S_\ell$.

8. The Weil data and the tight frames

Write $B = k_d(\zeta_{N_1})$ for the development's field, so that $E = L\cdot B$, and ζ for its primitive N_1-th root of unity. Throughout, $37 \mid N_0$, and the CM type of E consists of the embeddings that extend $\sqrt{-d} \mapsto i\sqrt{d}$. Fix one of them, Φ_1, extending the development's embedding of B. Then $\sigma \mapsto \Phi_\sigma = \Phi_1\circ\sigma$ identifies the group $\mathcal{G} = \mathrm{Gal}(E/k_d)$ with the CM type, and as complex conjugation c is central in $\mathrm{Gal}(E/\mathbb{Q})$, since L is Galois and totally real and B is abelian, $\overline{\Phi_\sigma(x)} = \Phi_\sigma(\bar{x})$. This section gives the Weil data of E, the tight frames that the theta products and the generator of the vacuum use, and a generator of the different of E with its size at every infinite place.

8.1. **The Weil data.** The development's Weil data on a CM field E that contains a primitive 5040-th root of unity (`WeilData`) are an element $j \in E$ with $\bar{j} = -j$, $\mathrm{Im}\,\Phi_\sigma(j) > 0$ for all σ and $(1-j^{-1})/2$ integral; a finite idele α with

$$\mathrm{ord}_w(j\alpha\bar{\alpha}) = -\,\mathrm{ord}_w\,\mathfrak{D}_{E/\mathbb{Q}} \qquad \text{at every finite place } w; \tag{8.1}$$

and a splitting character υ, a unitary character of the ideles of E trivial on $E^\times$, with $\upsilon(\bar{x}) = \upsilon(x)^{-1}$, equal to $\prod_\sigma x_\sigma/|x_\sigma|$ whenever all the finite components of x are units and to -1 at the uniformizers of the places $w = \bar{w}$. The mass ratio is controlled for every CM field with Weil data (`abs_log_mass_ratio_sub_le`), so for E only the data themselves and their period factor are needed. Write $\chi_{\mathrm{fin}}(x) = \upsilon_{\mathrm{fin}}(x)\,|x|_{\mathrm{f}}^{-1/2}$ for the normalized finite part of υ, with $|x|_{\mathrm{f}} = \prod_w(\mathrm{N}w)^{-\,\mathrm{ord}_w x_w}$, let s_0 be the principal $[E:k_d]$-th root of $\chi_{\mathrm{fin}}(\alpha)^{-1}$, and let $S_E = s_0/u_0$ be the period factor, with u_0 the development's Chowla–Selberg unit.

Proposition 8.1. *Let $c_0 = (1+\sqrt{-d})/2$ and $j = -1/\sqrt{-d}$. Let α_E be the finite idele with $\alpha_w = \pi_w^{-r_w}$, $r_w = \mathrm{ord}_w\,\mathfrak{D}_{E/k_d}$ and π_w a uniformizer, at every place w above a prime of k_d dividing c_0, and $\alpha_w = 1$ elsewhere.*

(a) *There is a splitting character υ such that (j, α_E, υ) are Weil data for E.*

(b) *The lattice $\mathfrak{a} = \{x \in E : \alpha_E^{-1}x$ is integral at every finite place$\}$ is its own dual for $h(x,y) = \mathrm{Tr}_{E/k_d}(x\bar{y})$; in particular $h(\mathfrak{a},\mathfrak{a}) \subset \mathcal{O}_{k_d}$.*

(c) *For every σ and every extension $\widetilde{\Phi}_\sigma$ of Φ_σ to $E(s_0)$, $|\widetilde{\Phi}_\sigma(s_0)|^2 = \mathrm{rd}_E/\sqrt{d}$.*

(d) *For every prime p, every embedding ι of $\bar{\mathbb{Q}}$ in $\bar{\mathbb{Q}}_p$ and every σ, $|\iota(S_E)|_p = |\alpha_{w_\sigma}|_p^{-1}$, where w_σ is the place of $\iota\circ\Phi_\sigma\circ c$; and $|\iota(S_E)|_p = 1$ if $p \nmid N_1$.*

Proof. The element j satisfies $\bar{j} = 1/\sqrt{-d} = -j$, $\Phi_\sigma(j) = i/\sqrt{d}$, and $(1-j^{-1})/2 = c_0$, which is integral as $d \equiv 3 \bmod 4$.

For (8.1), $\mathfrak{D}_{E/\mathbb{Q}} = \mathfrak{D}_{E/k_d}\mathfrak{D}_{k_d/\mathbb{Q}}$ and $(j) = (\sqrt{-d})^{-1} = \mathfrak{D}_{k_d/\mathbb{Q}}^{-1}$, so it says $\operatorname{ord}_w(\alpha_E\bar{\alpha}_E) = -r_w$. By Lemma 3.1, L/F is ramified only above 2, so E/k_d is ramified only above the primes dividing N_1. Each such p divides $c_0\bar{c}_0 = (d+1)/4$, as $N_0 \mid 2(d+1)$ and $16 \mid N_0$, so p splits in k_d and, as $c_0 + \bar{c}_0 = 1$, exactly one of its two primes divides c_0. At a place w above that prime $\operatorname{ord}_w \alpha_E = -r_w$ and $\operatorname{ord}_w \bar{\alpha}_E = \operatorname{ord}_{\bar{w}} \alpha_E = 0$, and at $\bar{w}$ the roles are exchanged; as the different is stable under c, $\operatorname{ord}_w(\alpha_E\bar{\alpha}_E) = -r_w$ at every w.

For the splitting character, the commutator subgroup of $\mathrm{Gal}(E/\mathbb{Q})$ maps onto $[S_3, S_3]$ and lies in $\mathrm{Gal}(E/B)$, so B is the maximal abelian subfield of E and every root of unity y of E is a power ζ^m. Put $u = \zeta^{N_1/4}(\zeta - 1)$. Then $\bar{u} = \zeta^{-1}u$, and $\mathrm{N}_{B/k_d}u = 1$, as $\mathrm{N}_{B/k_d}\zeta = 1$ and $\mathrm{N}_{B/k_d}(\zeta - 1) = \Phi_{N_1}(1) = 1$, the cyclotomic polynomial being irreducible over k_d and N_1 not a prime power. So the unit $\delta = u^m$ has $\delta/\bar{\delta} = y$, and its product over the CM type of E is $\mathrm{N}_{E/k_d}\delta = (\mathrm{N}_{B/k_d}\delta)^3 = 1$. These are the inputs of the development's construction of a splitting character (`nonempty_splittingChar`). Its value at the uniformizers of the places $w = \bar{w}$ is -1, as for B (`exists_eq_principalIdele_mul_norm`). For `Data.exists_char_hasWeight`, an integral unitary element is a root of unity, hence a power of ζ. Its constant-weight contribution is trivial as $\mathrm{N}_{E/k_d}\zeta = 1$, the rounded weights are multiples of N_1, and the tame contribution is trivial by the level congruence.

(b) The dual of a fractional ideal $\mathfrak{b}$ under $\mathrm{Tr}_{E/k_d}(xy)$ is $\mathfrak{b}^{-1}\mathfrak{D}_{E/k_d}^{-1}$, so the dual of $\mathfrak{a}$ under h is $\bar{\mathfrak{a}}^{-1}\mathfrak{D}_{E/k_d}^{-1}$. By (8.1), $\mathfrak{a}\bar{\mathfrak{a}} = \mathfrak{D}_{E/k_d}^{-1}$, so this is $\mathfrak{a}$.

(c) By (b), $|\alpha_E|_{\mathrm{f}}^2 = \mathrm{N}\mathfrak{D}_{E/k_d} = |d_E|/d^{[E:k_d]}$, and $|\chi_{\mathrm{fin}}(\alpha_E)| = |\alpha_E|_{\mathrm{f}}^{-1/2}$. So $|\widetilde{\Phi}_\sigma(s_0)|^2 = |\alpha_E|_{\mathrm{f}}^{1/[E:k_d]} = |d_E|^{1/(2[E:k_d])}/\sqrt{d} = \mathrm{rd}_E/\sqrt{d}$; the modulus is the same at every σ and every extension, as a power of $\chi_{\mathrm{fin}}(\alpha_E)$ is a norm from E to k_d.

(d) The p-adic absolute value of $\iota(\chi_{\mathrm{fin}}(\alpha_E))$ is $\prod_{\sigma\in\mathcal{G}} |\alpha_{w_\sigma}|_p$ (`WeilData.norm_map_chiFin`). All Φ_σ agree on k_d, so the w_σ lie above one prime $\mathfrak{q}$ of k_d, and as σ runs over $\mathcal{G}$ they run over the places above $\mathfrak{q}$, each equally often. If $\mathfrak{q} \nmid c_0$ every factor is 1. If $\mathfrak{q} \mid c_0$ every factor has order $-r_w$, the same for all $w \mid \mathfrak{q}$, since the different is Galois-stable and $\mathcal{G}$ is transitive on these places, which have one ramification index and one residue degree. So all factors are equal, $|\iota(s_0)|_p = |\alpha_{w_\sigma}|_p^{-1}$, and $|\iota(u_0)|_p = 1$. If $p \nmid N_1$, no place above p ramifies in E/k_d and $\alpha_E = 1$ there. □

For B the development's Weil data are `Parameters.instWeilDataE`, and its norm statement for the period factor is `Parameters.norm_iota_periodFactor`. Its idele α_B has the component $1/\Phi'_{N_1}(\zeta)$ at the places of B above the primes of k_d dividing c_0 and 1 elsewhere, and $\Phi'_{N_1}(\zeta)$ generates $\mathfrak{D}_{B/k_d}$ and divides N_1. The development uses elsewhere (row 12 of Table 1) that $N_1\alpha_B$ and α_B^{-1} are integral and that $N_1 d$ lies in $\mathfrak{D}_{B/\mathbb{Q}}$. The following lemma gives these for E, and it compares α_E with the extension of α_B to E: their fractional ideals agree away from 2.

Lemma 8.2. *Let $a_2 = \operatorname{ord}_2 N_1$ and $e_2 = 2^{a_2-1}$.*

(a) *E/B is unramified outside 2, and at each place of B above 2 it is totally and tamely ramified of degree 3.*

(b) *Let w be a place of E above a prime p dividing N_1. If p is odd, $\operatorname{ord}_w \mathfrak{D}_{E/k_d} = \operatorname{ord}_w \mathfrak{D}_{B/k_d}$. If $p = 2$, $\operatorname{ord}_w \mathfrak{D}_{E/k_d} = 3(a_2 - 1)e_2 + 2$ and $\operatorname{ord}_w N_1 = 3a_2e_2$. In both cases $\operatorname{ord}_w \mathfrak{D}_{E/k_d} \le \operatorname{ord}_w N_1$, so $\mathfrak{D}_{E/k_d}$ divides N_1.*

(c) *$N_1\alpha_E$ and α_E^{-1} are integral at every finite place of E.*

(d) *$N_1 d$ lies in the absolute different $\mathfrak{D}_{E/\mathbb{Q}}$.*

(e) $\operatorname{ord}_w(\alpha_E^{-1}\alpha_B) = 2$ *at each place* w *of* E *above the prime of* k_d *above* 2 *that divides* c_0*, and* 0 *at every other finite place. In particular these orders are non-negative.*

Proof. (a) $\mathrm{Gal}(E/B) \cong \mathrm{Gal}(L/F)$ is cyclic of order three, and a prime of B ramifies in E only if the prime of F below it ramifies in L. By Lemma 3.1, L/F is ramified only above 2, and 2 is inert in F, so the ramification index of 2 in L is 3. In B it is e_2: k_d is unramified at 2, as $-d \equiv 1 \bmod 8$, and $\mathbb{Q}(\zeta_{N_1})$ has index $\varphi(2^{a_2}) = e_2$ at 2. The index of 2 in E is divisible by 3 and by e_2, which are coprime, and it is at most $3e_2$, as $[E : B] = 3$. So it is $3e_2$, and E/B is totally ramified of degree 3 at every place above 2, tamely as $2 \nmid 3$.

(b) The different is transitive, $\mathfrak{D}_{E/k_d} = \mathfrak{D}_{E/B}\mathfrak{D}_{B/k_d}$, and by (a) and the tame case of the different [13, III (2.6)], $\mathfrak{D}_{E/B} = \prod_{w|2} w^2$. If p is odd, $\operatorname{ord}_w \mathfrak{D}_{E/B} = 0$, and $\operatorname{ord}_w \mathfrak{D}_{B/k_d} \le \operatorname{ord}_w N_1$, as $\Phi'_{N_1}(\zeta)$ divides N_1. If $p = 2$, let W be the place of B below w and v the place of k_d below W. Then $k_{d,v} = \mathbb{Q}_2$, and B_W is unramified over $\mathbb{Q}_2(\zeta_{2^{a_2}})$, so $\operatorname{ord}_W \mathfrak{D}_{B/k_d}$ is the exponent of the different of $\mathbb{Q}_2(\zeta_{2^{a_2}})/\mathbb{Q}_2$. For a prime p and ζ' a primitive p^a-th root of unity, $\mathbb{Z}_p[\zeta']$ is the ring of integers of $\mathbb{Q}_p(\zeta')$, so the different is generated by $\Phi'_{p^a}(\zeta') = p^a {\zeta'}^{p^a-1}/({\zeta'}^{p^{a-1}} - 1)$. In the normalized valuation, of index $\varphi(p^a)$ over p, the numerator has order $a\varphi(p^a)$, and the denominator, a primitive p-th root of unity less 1, has order p^{a-1}. So the exponent is $p^{a-1}(a(p-1)-1)$, which at $p = 2$, $a = a_2$ is $(a_2 - 1)e_2$. As $e(w/W) = 3$, $\operatorname{ord}_w \mathfrak{D}_{B/k_d} = 3(a_2 - 1)e_2$, and adding $\operatorname{ord}_w \mathfrak{D}_{E/B} = 2$ gives the formula. Also $\operatorname{ord}_w N_1 = a_2\, e(w/2) = 3a_2e_2$, and the difference is $3e_2 - 2 > 0$.

(c) At a place w above a prime of k_d dividing c_0, $\operatorname{ord}_w(N_1\alpha_E) = \operatorname{ord}_w N_1 - r_w$. If w lies above a prime dividing N_1, this is non-negative by (b). Otherwise $r_w = 0$, as E/k_d is unramified away from N_1: B/k_d is ramified only above N_1, and E/B only above 2. At every other place $\alpha_w = 1$, and N_1 is integral. The orders of α_E are $-r_w \le 0$ at the places above c_0 and 0 elsewhere (Proposition 8.1), so α_E^{-1} is integral.

(d) $\mathfrak{D}_{E/\mathbb{Q}} = \mathfrak{D}_{E/k_d}\mathfrak{D}_{k_d/\mathbb{Q}}$ and $\mathfrak{D}_{k_d/\mathbb{Q}} = (\sqrt{-d})$, as $-d \equiv 1 \bmod 4$. By (b), $\mathfrak{D}_{E/k_d}$ divides N_1, and $\sqrt{-d}$ divides d. So $\mathfrak{D}_{E/\mathbb{Q}}$ divides $N_1 d$.

(e) At a place w above a prime of k_d dividing c_0, with W the place of B below it, $\operatorname{ord}_w \alpha_B = -e(w/W)\operatorname{ord}_W \mathfrak{D}_{B/k_d}$ and $\operatorname{ord}_w \alpha_E = -\operatorname{ord}_w \mathfrak{D}_{E/k_d}$, so by transitivity $\operatorname{ord}_w(\alpha_E^{-1}\alpha_B) = \operatorname{ord}_w \mathfrak{D}_{E/B}$. By (a) this is 2 above 2 and 0 above odd primes. Elsewhere both components are 1. The dyadic prime exists: $\mathrm{N}c_0 = (1+d)/4$ is even, as $d \equiv 7 \bmod 8$, and exactly one of the two primes of k_d above 2 divides c_0, as $c_0 + \bar{c}_0 = 1$. □

8.2. **Tight frames.** A tight frame of E of constant q (`IsTightFrame`) is a family of vectors $w_i \in \mathfrak{a}$ with multiplicities $c_i \ge 0$ such that

$$\sum_i c_i\, \Phi_\sigma(w_i)\overline{\Phi_\tau(w_i)} = q\, \delta_{\sigma\tau} \qquad (\sigma, \tau \in \mathcal{G}).$$

The development builds the frames of B from the powers of ζ (`Parameters.isTightFrame_zeta_pow`). These do not give frames of E, as two embeddings of E that agree on B give equal rows, and the frames of E are built here.

Proposition 8.3. *There is an odd integer* Q *with* $15 \le Q \le 15 + 20250\, d^2\varphi(N_1)^5$ *with the following property. For every prime* p*, every embedding* ι *of* $\bar{\mathbb{Q}}$ *in* $\bar{\mathbb{Q}}_p$*, every integer* $R \ge 0$ *and every integer*

$$q \ge (dN_1)^6(R+1)(9Q+52) + 27Q + 112,$$

E has a tight frame of constant q with every multiplicity at least R and with one index i such that $|\iota(S_E\, \overline{\Phi_\sigma(w_i)})|_p = 1$ *for every* $\sigma \in \mathcal{G}$.

The scalar S_E here is the period factor of Proposition 8.1, which enters the jet scale as $S_E(2\pi/\sqrt{d})^{1/2}/\Omega_0$, with $\Omega_0\mathcal{O}_{k_d}$ the lattice of the chosen elliptic curve (Section 8.3). The theta products use the proposition at $q = g_0g_1$ with R three times the degree (`Data.depth_indicator_jet`), and the conjugates of the jets at $q = (p(dN_1)^6+1)^2$ with $R = 0$ (`Parameters.norm_jetSeries_le`). Both lie above the threshold. With $U = (dN_1)^6$ one has $Q \le U/100$, as $d > 64$ and $N_1 \ge 18480$, so at $R = 0$ the threshold is below $(2U+1)^2 \le (pU+1)^2$. It is also below $2U^2(R+1)$. As the degree is at most $2b$ at each of the $\#\mathcal{G}$ places (`Data.nominalWeight_add_le`), $R \le 6\#\mathcal{G}\,b$, so $2U^2(R+1) \le 2U^2(6\#\mathcal{G}\,b+1) < b^3 \le g_0g_1$, as U and $\#\mathcal{G}$ are at most a fixed power of x and $\log b \ge 10^{12}\log x$ (`Data.scale`). So neither bound changes.

Proof. Products. Let ρ generate $\mathrm{Gal}(E/B) \cong \mathrm{Gal}(L/F)$. A relative frame of constant n is a family $\mu_k \in E$ with multiplicities $m_k \ge 1$ such that $\sum_k m_k\,\rho^j(\mu_k)\bar{\mu}_k = n\,\delta_{j0}$ in E for $j \in \mathbb{Z}/3$. If (v_i, c_i) is a tight frame of B of constant A with v_i in the development's lattice of B, and (μ_k, m_k) is a relative frame of constant n with $\alpha_E^{-1}\alpha_B\mu_k$ integral, then $(v_i\mu_k, c_im_k)$ is a tight frame of E of constant An. Indeed the sum for σ, τ factors as $\sum_i c_i\Phi_\sigma(v_i)\overline{\Phi_\tau(v_i)}$ times $\sum_k m_k\Phi_\sigma(\mu_k)\overline{\Phi_\tau(\mu_k)}$. The first factor vanishes unless σ and τ agree on B, and then it is A and $\tau = \sigma\rho^j$ for some j, so the second is $\Phi_\sigma\big(\sum_k m_k\mu_k\overline{\rho^j(\mu_k)}\big) = n\,\delta_{j0}$, using $\overline{\rho^j x} = \rho^j\bar{x}$ and applying ρ^{-j}.

Two relative frames from L. Number the roots $\alpha_1, \alpha_2, \alpha_3$ of $x^3 - x^2 - 3x + 1$ so that ρ permutes them cyclically. Their elementary symmetric functions are $1, -3, -1$, so $\sum \alpha_i^2 = 7$; and $\alpha_i^2 - 1$ are the roots of $x^3 - 4x^2 + 4$. As L is real, the family $1, \alpha_1, \alpha_2, \alpha_3$ with multiplicities $6, 2, 2, 2$ has correlations $6 + 2\cdot 7 = 20$ at $j = 0$ and $6 + 2\cdot(-3) = 0$ at $j \ne 0$, and the family $\alpha_i^2 - 1$ with multiplicities $2, 2, 2$ has $2\cdot 16 = 32$ and $2\cdot 0 = 0$. They are relative frames of constants 20 and 32 in $\mathcal{O}_L$. The orders of $\alpha_E^{-1}\alpha_B$ are non-negative (Lemma 8.2(e)), so both integral relative frames satisfy the local integrality condition.

A Kummer generator. Let $\zeta_3 = \zeta^{N_1/3}$ and $\theta = \alpha_1 + \zeta_3^2\alpha_2 + \zeta_3\alpha_3$. Then $\rho\theta = \zeta_3\theta$, $\bar{\theta} = \alpha_1 + \zeta_3\alpha_2 + \zeta_3^2\alpha_3$, $\theta\bar{\theta} = 7 + 3 = 10$ and $\theta^3 + \bar{\theta}^3 = 2$. So $\theta^3 \in B$ is $1 \pm 3\sqrt{-111}$, with $\theta^3\bar{\theta}^3 = 1000$. As 2 splits in $\mathbb{Q}(\sqrt{-111})$ and the 2-adic valuation of $\theta^3 + \bar{\theta}^3$ is 1, the two roots have valuations 1 and 2 in the two completions. Let $a_2 = \mathrm{ord}_2 N_1$ and $e_2 = 2^{a_2 - 1}$, the ramification index of B at 2 (2 splits in k_d as $d \equiv 7 \bmod 8$). For each place W of B above 2, $b_W = \mathrm{ord}_W\,\theta^3$ is e_2 or $2e_2$, $b_W + b_{\bar{W}} = 3e_2$, and b_W is prime to 3. The extension E/B is tamely and totally ramified of degree 3 at W, so at the place of E above W the order of θ is b_W, and θ is integral everywhere. Let $\sigma_3 \in \mathcal{G}$ be trivial on L and invert ζ_3; it exists as $L \cap B = F$ (Lemma 3.6) and the class of $u \in (\mathbb{Z}/N_1)^\times$ with $u \equiv -1 \bmod 3$ and $u \equiv 1 \bmod 37$ has $(\frac{u}{37}) = 1$. Then $\sigma_3\theta = \bar{\theta}$.

A coefficient with prescribed orders. By Lemma 8.2(e), an element $x\theta$ with $x \in B$ satisfies $\alpha_E^{-1}\alpha_B x\theta$ integral at the place above W if and only if $3\,\mathrm{ord}_W\,x + b_W \ge c_W$, where $c_W = -2$ if W divides c_0 and $c_W = 0$ otherwise. Put $k_W = \lceil (c_W - b_W)/3 \rceil$. In both cases $k_W + k_{\bar{W}} = -e_2$ and $-e_2 \le k_W \le 0$. Choose $s_W \in B_W$ of order k_W at each $W \mid c_0$, and put $s_{\bar{W}} = \overline{(10s_W)^{-1}}$, of order $k_{\bar{W}}$. By the Chinese remainder theorem in $\mathcal{O}_B/4$ there is $t \in B$, integral away from 2, with $2t \equiv 2s_W \bmod 4$ at every W, taking the coordinates of $2t$ in the integral basis $\zeta^i, c_0\zeta^i$ $(0 \le i < \varphi(N_1))$ of $\mathcal{O}_B$ in $\{0, 1, 2, 3\}$. Then $t - s_W \in 2\mathcal{O}_W$ has order at least $e_2 > k_W$, so t has order exactly k_W, and $10t\bar{t} - 1 \in 2\mathcal{O}_W$, as $10s_W$ and $10\bar{s}_{\bar{W}}$ are integral. So $X = 10t\bar{t}$ and $T = (X-1)/2$ lie in $\mathcal{O}_{B^+}$. Under every embedding $|t| \le \frac{3}{2}\varphi(N_1)(1 + \sqrt{(d+1)/4}) \le 3\varphi(N_1)\sqrt{d}$, so $|T| \le 45\varphi(N_1)^2 d$.

A positive completion. Take the list of coefficients consisting of t five times, $T+\zeta_3$ once, and $\gamma(T)$ once for each $\gamma \neq 1$ in $\mathrm{Gal}(B^+/\mathbb{Q})$. As $\zeta_3+\bar{\zeta}_3=-1$,

$$\sum_x 10x\bar{x} = 5X + 10(T^2-T+1) + 10(\mathrm{Tr}_{B^+/\mathbb{Q}}(T^2)-T^2) = 15 + 10\,\mathrm{Tr}_{B^+/\mathbb{Q}}(T^2) =: Q,$$

an odd integer with $15 \le Q \le 15 + 10\varphi(N_1)(45\varphi(N_1)^2 d)^2 = 15 + 20250\,d^2\varphi(N_1)^5$. All coefficients but t are integral, so every $x\theta$ satisfies the condition above.

The relative frame of constant $9Q$. Mark one copy of t and put $v_0 = 1 + t\theta + \sigma_3(t)\bar{\theta}$. Take the vector v_0, the vector 1 with multiplicity $Q-1$, and, for every other coefficient x of the list, the vectors $x\theta$ and $\sigma_3(x)\bar{\theta}$; and for each vector v take $v, \rho v, \rho^2 v$. For $v = a + b\theta + b'\bar{\theta}$ with $a, b, b' \in B$,

$$\sum_{k\in\mathbb{Z}/3} \rho^{k+j}(v)\,\overline{\rho^k(v)} = 3(a\bar{a} + 10\,\zeta_3^j\, b\bar{b} + 10\,\zeta_3^{2j}\, b'\bar{b}'),$$

as the mixed terms carry $\sum_k \zeta_3^{\pm k} = 0$. Summed over the family the three energies are $1+(Q-1) = Q$, $\sum_x 10x\bar{x} = Q$ and $\sigma_3(Q) = Q$, so the correlations are $3Q(1+\zeta_3^j+\zeta_3^{2j}) = 9Q\,\delta_{j0}$. As the condition is stable under $\mathcal{G}$, all these vectors satisfy it.

The unit vector. At a place w of E above 2 the three terms of v_0 have orders congruent to 0, b_W and $-b_W$ modulo 3, so the order of v_0 is their minimum. If $W \mid c_0$ the two non-constant orders are -2 and -1, and otherwise they are 1 and 2. So $\mathrm{ord}_w\, v_0 = \mathrm{ord}_w(\alpha_E/\alpha_B)$ at every such w, and v_0 is integral elsewhere. By Proposition 8.1(d), if v^* is a vector of a frame of B with $|\iota(S_B\overline{\Phi_\sigma(v^*)})|_p = 1$ for all σ, then $v^* v_0$ satisfies the unit clause of the proposition at $p=2$, and $v^*\cdot 1$ at odd p, since α_E/α_B has unit components above odd primes.

Every large constant. Put $A_0 = (dN_1)^6(R+1)$. The development gives, for every $A \ge A_0$ and every p, a tight frame of B of constant A with multiplicities at least R and a vector v^* as above (`Parameters.exists_isTightFrame`). Given $q \ge A_0(9Q+52)+27Q+112$, choose $x \in \{0,1,2,3\}$ with $9Qx \equiv q - A_0(9Q+52) \bmod 4$. Then $q - A_0(9Q+52) - 9Qx = 4h$ with $h \ge 28$, and $h = 5j' + 8k'$ with $j', k' \ge 0$, as every integer above $27 = 5\cdot 8 - 5 - 8$ is so. The union of the products of frames of B of constants $A_0 + x$, $A_0 + j'$ and $A_0 + k'$ with the relative frames of constants $9Q$, 20 and 32 has constant $A_0(9Q+52) + 9Qx + 4(5j'+8k') = q$, multiplicities at least R, and the unit vector of the first product. □

8.3. **The generator of the vacuum.** The development's theta functions in n variables over its field form a standard space V of rank n, a model of the Weil representation on which the finite adeles act by translations $\varrho(x)$. In it vac is the vacuum vector, $\mathcal{W}_f$ the span of the translates of vac under the finite Heisenberg group (`Space.finitePart`), θ the theta functional, and $T_a f$ the Taylor series at 0 of the theta function of f with its variables scaled by a (`Space.jetSeries`). The jets are taken at the scale $\mathrm{per} = S_E(2\pi/\sqrt{d})^{1/2}/\Omega_0$, with S_E the period factor of Proposition 8.1 and $\Omega_0\mathcal{O}_{k_d}$ the lattice of the chosen elliptic curve with complex multiplication by $\mathcal{O}_{k_d}$ (`Parameters.jetScale`), and $\Omega = e^{c_d}\,2\pi/\mathrm{rd}_E$, with c_d the constant of Lemma 2.1. The development's generator lemma (`Parameters.exists_isJetConjugate_generator`) states (a)–(c) of the following proposition for its field B, with a constant C_0 for B that its argument provides, depending only on (N_0, d). Its proof uses the frame of powers of ζ to translate a theta series to its conjugates.

Proposition 8.4. *Put $C_E = C_0 + 240^2 + 240$. For every r there are finite adeles β_σ of E, one for each automorphism σ of $\mathbb{C}$ over k_d, such that every standard space V over E of rank n has the following properties, where x runs over the vectors of length n of finite adeles of E, each read as an adele vector with infinite component 0.*

(a) *There is $c \neq 0$ such that, for every x, $c\,\mathrm{vac}(x)$ is integral at every finite place and $|\sigma(c\,\mathrm{vac}(x))| \le \exp(C_E N_1^2 n)$ for every σ.*

(b) *There is $F \in \mathcal{W}_f$ with $\theta F = 1$ whose translates $\varrho(x)F$ span $\mathcal{W}_f$ and which satisfies (c).*

(c) *For every σ there are $t \in \mathbb{C}$ with $|t|^2 = 1/\Omega$ and $F' \in \mathcal{W}_f$ such that, for every x, applying σ to the coefficients of $T_{\mathrm{per}}\,\varrho(x)F$ gives $T_t\,\varrho(\beta_\sigma x)F'$ with the places of its variables permuted by σ.*

Proof. We follow the development's proof, with the frame of powers of ζ replaced by the vectors $\zeta^j \mu_k$ ($0 \le j < N_1$, $0 \le k \le 3$), $\mu = (1, \alpha_1, \alpha_2, \alpha_3)$, with multiplicities $20N_1 \cdot (6,2,2,2)_k$. Over B the three relative rows of (μ_k) have Gram matrix $20\,I$ (Section 8.2), and the powers of ζ have Gram matrix $N_1\,I$ on the embeddings of B. By the product rule of Section 8.2 the family therefore has Gram matrix $(20N_1)^2\,I$, and the relative factor separates the embeddings of E that agree on B. With the multiplicities taken as repeated vectors, the development's proof runs with this family. In it the place group becomes $\mathcal{G}$ acting by left composition, the trace is $\mathrm{Tr}_{E/k_d} = \sum_\sigma \Phi_\sigma$, the rational shift is $-\mathrm{Tr}_{E/k_d}(\gamma_i\,\overline{\zeta^j \mu_k})/(20N_1)$, and the number of places is $[E : k_d] = 3\varphi(N_1) \le 3N_1$. The theta product has $240N_1^2$ factors per coordinate, as the multiplicities sum to $20 \cdot 12 = 240$ times N_1, and the number of shifts is $(20N_1)^{4[E:k_d]n}$ in a standard space of rank n. In the development's argument $C_0 = \lceil M \rceil + 4$, with $M \ge 1$ a bound for the elliptic theta factors at zero. The logarithm of the number of shifts is at most $240N_1^2 n$, and $240 \log M \le M + 240^2$, which gives the constant C_E. For the conjugate curve the development's proof takes $\Omega_\sigma \neq 0$ and a positive integer e_σ with $e_\sigma\Omega_\sigma$ in its lattice, whose area is $|\Omega_\sigma|^2\sqrt{d}/2$, and calls the frame a second time, with the same family, of Gram matrix $(20N_1)^2\,I$, the lattice point $e_\sigma\Omega_\sigma$ and the shift denominator $20N_1 e_\sigma$. The factor e_σ cancels in the shift, $e_\sigma\Omega_\sigma/(20N_1 e_\sigma) = \Omega_\sigma/(20N_1)$, and in the area that the call asks of the lattice, $|e_\sigma\Omega_\sigma|^2(20N_1)^2\sqrt{d}/(2(20N_1 e_\sigma)^2) = |\Omega_\sigma|^2\sqrt{d}/2$. The vacuum root has the norm the lemma needs by Proposition 8.1(c). □

8.4. **A generator of the different.** The development's filling step, which shows that few translates of a Bessel function at the real places almost span the rows, uses a skew generator of the absolute different of its field (`Parameters.different_eq_span_varpi`). It also uses the size of the generator at every infinite place (`Data.hasLogBound_varpi`). For B it is an element γ_B with $\bar\gamma_B = -\gamma_B$, $(\gamma_B) = \mathfrak{D}_{B/\mathbb{Q}}$ and $x^{10} \le |v\gamma_B| \le x^{12}$ at every infinite place v of B.

Proposition 8.5. *Let $a_2 = \mathrm{ord}_2 N_1$, $e_2 = 2^{a_2 - 1}$, $m_2 \in \{\pm 1\}$ with $e_2 m_2 \equiv 1 \bmod 3$, $n_2 = (1 - e_2 m_2)/3$, and I the set of positions of the binary digits 1 of $|n_2|$. With $\zeta_{2^k} = \zeta^{N_1/2^k}$, put*

$$\Delta = (\alpha - 1)^{m_2} \prod_{i \in I} (1 - \zeta_{2^{a_2 - i}})^{\operatorname{sgn} n_2}, \qquad \gamma_E = \gamma_B\,\Delta\,\bar\Delta.$$

Then Δ has order 1 at every place of E above 2 and 0 elsewhere, γ_E is integral and skew and generates $\mathfrak{D}_{E/\mathbb{Q}}$, and $\gamma_E/\sqrt{-d}$ generates $\mathfrak{D}_{E/k_d}$. At every infinite place v of E,

$$\big|\log |v\gamma_E|\big| \le 1200 (\log x)^2 \le \tfrac{1}{2} \log b,$$

and $\prod_\sigma |\Phi_\sigma(\gamma_E)| = \mathrm{rd}_E^{[E:\mathbb{Q}]/2}$.

Proof. By Lemma 3.1, L/F is unramified away from 2, so E/B is. At 2 the ramification index of B is e_2, and that of E is divisible by e_2 and by 3 and at most $3e_2$; so E/B is tame of index 3 at every place above 2, and $\mathfrak{D}_{E/B} = \mathfrak{J}^2$, with $\mathfrak{J}$ the product of the places of E above 2. The norm of $\alpha - 1$ from K is $-(1-1-3+1) = 2$; in L the only prime above 2 has norm 4, which is the norm of $\alpha - 1$ from L, so $(\alpha-1)\mathcal{O}_L$ is that prime and $(\alpha-1) = \mathfrak{J}^{e_2}$ in E. For $k \geq 2$, $1 - \zeta_{2^k}$ generates the prime above 2 of $\mathbb{Q}(\zeta_{2^k})$, of ramification index 2^{k-1}, so $(1-\zeta_{2^k}) = \mathfrak{J}^{3\cdot 2^{a_2-k}}$. As $16 \mid N_0$, $a_2 \geq 4$ and $0 < |n_2| < e_2$, so $a_2 - i \geq 2$ for $i \in I$, and the order of Δ at every place above 2 is $e_2 m_2 + 3n_2 = 1$. Neither factor has other prime divisors, so $(\Delta) = \mathfrak{J} = (\bar{\Delta})$, $(\gamma_E) = \mathfrak{D}_{B/\mathbb{Q}}\mathfrak{J}^2 = \mathfrak{D}_{E/\mathbb{Q}}$, and $\bar{\gamma}_E = \bar{\gamma}_B \bar{\Delta}\Delta = -\gamma_E$. As $\mathfrak{D}_{k_d/\mathbb{Q}} = (\sqrt{-d})$, $\gamma_E/\sqrt{-d}$ generates $\mathfrak{D}_{E/k_d}$.

For the size, restricting v to B gives $|\log|v\gamma_B|| \leq 12 \log x$. The roots of the cubic have modulus at most 4, so $|\alpha_i - 1| \leq 5$, and as $\prod_i |\alpha_i - 1| = 2$ each is at least $2/25$; so $|\log|v(\alpha-1)|| < 3$. For odd u and $k \geq 2$, $2^{2-k} \leq |1 - e^{2\pi i u/2^k}| \leq 2$, so $|\log|v(1-\zeta_{2^k})|| \leq k \log 2$; the conductors $a_2 - i$ are distinct and at most a_2, so $|\log|v\Delta|| \leq 3 + \frac{1}{2}a_2(a_2+1)\log 2$, and $|v\bar{\Delta}| = |v\Delta|$. Write $X = \log x$. The scale conditions of the data (`Data.scale`, `Data.s_le`) give $N_0 \leq X$, $r \leq 32X$, $X \geq 2$ and $\log b \geq (10^6 X)^6$, so $a_2 \leq N_0 + r \leq 33X$ and

$$|\log|v\gamma_E|| \leq 12X + 6 + a_2(a_2+1)\log 2 \leq 1200X^2 \leq \tfrac{1}{2}\log b.$$

Finally $\prod_\sigma |\Phi_\sigma(\gamma_E)|^2 = |\mathrm{N}_{E/\mathbb{Q}}\gamma_E| = |d_E| = \mathrm{rd}_E^{[E:\mathbb{Q}]}$. □

The filling step takes γ_E in place of γ_B. Its three inequalities hold. With $g = g_0 g_1$ and $b^{20} \leq g \leq b^{22}$, the proposition gives $|v\gamma_E| \leq b$ and $1 \leq g|v\gamma_E|/(2\pi) \leq b^{23}$, using $b \geq 1000$. Its grading constant $-1/(jg\gamma_E)$ is real and non-zero, as j and γ_E are skew, and (8.1) reads $\mathrm{ord}_w(j\alpha_E\bar{\alpha}_E) = -\mathrm{ord}_w \gamma_E$. The development's lower bound $x^{10} \leq |v\gamma_B|$, which can fail for γ_E, is used twice, for the root discriminant bound (`Data.hasLogBound_rootDisc`) and for the admissibility of the filling data. For E the first follows from the product formula of the proposition and $\mathrm{rd}_E \leq \mathrm{rd}_L \mathrm{rd}_B$, at the cost of $\log 10$ in the upper exponent, and the second from the three inequalities just stated.

9. Proof of the theorem

Theorem 9.1. *Let $37 \mid N_0$, let d be a prime with $d \equiv N_0/2 - 1 \bmod N_0$ (Section 2.1), let $0 < \varepsilon < \frac{1}{100}$, and let R_E be the prime error of Section 6 at $M = N_0$ with f the indicator of the identity, $f = (1 + \mathrm{sgn} + 2\chi_{\mathrm{std}})/6$. Then*

$$R_E(x) \leq x^{8\varepsilon - 1/2} \qquad \text{for all large } x.$$

Here $f_\pi \geq 0$ for all π and $f_{\mathrm{std}} = \frac{1}{3}$. The proof is the development's proof of (2.1), run on E at the data whose primes g_0, g_1 and level $\mathcal{N}$ split completely in L (Section 4). Table 1 gives each fact of the old field that a step of the development uses and that fails for E or must be proved again, where it is used, what replaces it for E and what that needs, and the statements of this paper that prove the replacement. Sections 9.1 and 9.2 prove the replacements not proved earlier, the proof of Theorem 9.1 ends in Section 9.3, and Theorem 1.1 follows in Section 9.4.

A step of the development not in Table 1 is used for E unchanged, by three checks (Appendix A). Its values: Lean's kernel accepts the step with the values of the field's set-up replaced by axioms of the same type, and each constant it rejects lies in a row of Table 1. Its statements: every statement of the set-up that it names is true for E, under the reading of Appendix A, or is one of the twenty that are false for E or cannot be formed for it, and

then every user of that statement is in a row. Its structure: the step compiles when the places are given only a group structure, and with the abelian-extension instances of the field replaced by the facts that it is Galois over $\mathbb{Q}$ and over k_d and is CM.

In the development the field is $B = k_d(\zeta_{N_1})$, cyclotomic over k_d and abelian over $\mathbb{Q}$, and its infinite places are identified with $\mathrm{Gal}(B/k_d) \cong (\mathbb{Z}/N_1)^\times$, a commutative group. Here the field is $E = L \cdot B$, with $H = \mathrm{Gal}(E/B)$ of order three, and its places are identified, as in Section 8, with

$$\mathcal{G} = \mathrm{Gal}(E/k_d) = \Big\{(t,u) \in S_3 \times (\mathbb{Z}/N_1)^\times : \operatorname{sgn} t = \Big(\frac{u}{37}\Big)\Big\},$$

which is not commutative; we write its elements as pairs of their restrictions to L and to B. The class of a place is its second coordinate; the class map onto $(\mathbb{Z}/N_1)^\times$ has the cosets of H as fibers, of three elements each, and the class map modulo N_0 has fibers of $3\varphi(N_1)/\varphi(N_0)$ elements. Complex conjugation c is central in $\mathrm{Gal}(E/\mathbb{Q})$, as L is Galois and totally real and B is abelian (row 5), and so are the elements $(1,u)$ of $\mathcal{G}$. Three central subgroups enter: the group generated by $z = (1,-1)$; the tops

$$\mathcal{T}_1 = \{(1,u) : u \equiv 1 \bmod N_0\},$$

of order $\varphi(N_1)/\varphi(N_0)$, as $(\frac{u}{37}) = 1$ for these u; and $C = \{(1,u) : (\frac{u}{37}) = 1\}$, which contains z and $\mathcal{T}_1$. For a prime p inert in k_d and unramified in E, and a prime $\mathfrak{P}$ of E above it, put $t_p = \mathrm{Frob}_{\mathfrak{P}}|_L$ and

$$h_{\mathfrak{P}} = c\,\mathrm{Frob}_{\mathfrak{P}} = (t_p, -p) \in \mathcal{G},$$

and at d let t_d be the restriction to L of the Frobenius of a prime of E above d over k_d (Lemma 9.2).

Table 1: Each use of the old field and its replacement. The declarations are located in Appendix A.

	Fact of the old field that is used	Where it is used	What replaces it for E, and what that needs	Proved in
1	B has the power basis $1, \zeta, \dots$ over k_d, which gives its tight frames	`Parameters.isTightFrame_zeta_pow`, `Parameters.exists_isTightFrame`	Frames of E, products of frames of B with relative frames from L, at every constant above a threshold that the theta products and the conjugates of the jets meet; the generator of the vacuum takes its own frame. Needs $37 \mid N_0$ and the Weil data of row 13.	Props. 8.3 and 8.4
2	Norms from B to k_d: $\mathrm{N}\zeta = 1$ and $\mathrm{N}(\zeta^{N_1/4}(\zeta-1)) = 1$	`Data.exists_char_hasWeight`; the Weil data	The same elements, as $\mathrm{N}_{E/k_d} = \mathrm{N}^3_{B/k_d}$ on B. Needs N_1 not a prime power and Φ_{N_1} irreducible over k_d.	Prop. 8.1
3	B embeds in $\mathbb{Q}(\mu_{N_1 d})$	`Parameters.toCycloField`, `Data.algebraMap_mem_cycloField`; used by the twist fitting, the denominator bound and the odd-class bound	Every embedding of E lies in $L \cdot \mathbb{Q}(\zeta_{N_1 d})$, and the three users hold for that field. Needs the CM field with a primitive 5040-th root of unity of Lem. 3.6, the odd-class bound (7.1), and the size bounds.	Cor. 7.6 and Lem. 7.2

	Fact of the old field that is used	Where it is used	What replaces it for E, and what that needs	Proved in
4	An element of a local Galois group at ℓ that fixes $\mu_{N_1 d}$ fixes B	`fixes_emb_of_fixes_rootsOfUnity`; used by the one-place defect	It fixes E if it also fixes L: at $\ell = g_0, g_1$, which split completely in L, and at an inertia element above $\ell \nmid N$, as every prime dividing d_L divides 74, which divides N. No bound changes.	§§ 7.2 and 4
5	B is abelian over $\mathbb{Q}$, so it is CM with central complex conjugation, and $\mathrm{Gal}(B/\mathbb{Q})$ is transitive on the primes above p	the abelian instance and the CM type; `Parameters.exists_smul_eq_or_star`	E is Galois over $\mathbb{Q}$ and CM, with central complex conjugation, as L is Galois and totally real and B is abelian. No bound changes.	Lems. 3.6 and 9.2
6	The places of B form a commutative group	the group law, as a group law only	The places are $\mathcal{G}$, with its own group law; E/k_d is Galois. No bound changes.	§ 9.1
7	Commutativity of the places: commuting factors, canceling a ratio, normalizing products, three-term-free sets in a commutative group	the existence of data, the marked primes, the frame rows, the induced places, the thick spacing, the remainder and the split level	Left multiplication by $h_{\mathfrak{P}}$ and the partners; orbits, marking, collisions and the thick set built from the central $\mathcal{T}_1$, z and C; a ratio of places is $v'^{-1}v$. The groups of uses and their lemmas are listed after Lem. 9.6.	Lems. 9.2, 9.3, 9.4, 9.5 and 9.6
8	The permutation of the places by $\sigma \in \mathrm{Aut}(\mathbb{C}/k_d)$, and the trace as a sum over places	`Parameters.placePerm`; the Galois conjugates of the lift; `Parameters.coe_trace_eq_sum`	Left multiplication by the place of $\sigma \circ \Phi_1$, and $\mathrm{Tr}_{E/k_d}\, y = \sum_\tau \Phi_\tau(y)$, true for every CM field Galois over k_d. No bound changes.	§ 8
9	The class of a place modulo N_1 is a cyclotomic character, with a global inverse that labels integers by places	`Parameters.placeClass`, `Parameters.placeOfInt`, used by the marking, the admissible pairings of places and the frame rows; `placeClass_ratio`	The class map modulo N_1 is the cyclotomic character of $\mathcal{G}$, onto with fibers the cosets of H; the integers are labeled by their partners u_j, with the exact residue degree $\mathrm{lcm}(2, \mathrm{ord}\, h_{\mathfrak{P}})$ and Frobenius $\sigma^{-1}\,\mathrm{Frob}_{\mathfrak{P}}\,\sigma$ at the prime of σ. The return order becomes $o_{\mathfrak{P}}$. Needs p inert in k_d and unramified in E.	Lems. 9.2, 9.3 and 9.4
10	The Frobenius at a prime is the label of the prime	`Parameters.frobElem_eq_one`, `Parameters.frob_ext`, `Parameters.frob_iff_eq_frobElem_pow`	False for E in general. At inert p and at d the congruence with the partner u_j, at d for every $j \geq 0$; at g_0, g_1 and $\mathcal{N}$, complete splitting in E. The data's window property and the choice of the level from it (`Data.exists_prime_window`, `Data.N`) carry this splitting at every datum. Needs these three primes split completely in L, which Cor. 4.3 gives in every window for large x.	Lem. 9.2, § 4

	Fact of the old field that is used	Where it is used	What replaces it for E, and what that needs	Proved in
11	There are $[B : k_d] = \varphi(N_1)$ places, of which $\varphi(N_1)/\varphi(N_0)$ have class 1 modulo N_0	`Parameters.card_infinitePlace_E`, used by the size bound, the generator of the vacuum, the Gaussian estimate, the Hecke trace and the remainder; `Parameters.card_placeClass_eq`, used by the remainder and the prime sum	There are $\#\mathcal{G} = 3\varphi(N_1)$ places, and the tops are $\mathcal{T}_1$, of order $\varphi(N_1)/\varphi(N_0)$; the thick count gains the factor $[t_p^j = 1]$. The size bounds hold with the same c_*, as $3\varphi(N_0) \le 3c_* \le e^{c_*}$.	Lems. 7.2 and 9.6 and Prop. 9.8
12	The relative different of B/k_d is generated by $\Phi'_{N_1}(\zeta)$, which divides N_1	`Parameters.relDifferentGen`, `Parameters.relDifferent_spec`; used by the valuation identity, the strong size control (`Data.hasLogBound_varpi`) and `Parameters.herm_mem_quadInt`	The generator $\gamma_E/\sqrt{-d}$ of $\mathfrak{D}_{E/k_d}$, with γ_E the skew generator of $\mathfrak{D}_{E/\mathbb{Q}}$ of Prop. 8.5, and the idele α_E of Prop. 8.1: equal orders above each prime of k_d, by the component choices in Prop. 8.1 and the Galois stability of the relative different, and $\mathfrak{a}\bar{\mathfrak{a}} = \mathfrak{D}_{E/k_d}^{-1}$ by (8.1), hence $h(\mathfrak{a}, \mathfrak{a}) \subset \mathcal{O}_{k_d}$; the norms of the period factor and of the vacuum root (Prop. 8.1(c),(d)); $\mathrm{ord}_w(j\alpha_E\bar{\alpha}_E) = -\mathrm{ord}_w \gamma_E$, the sizes of γ_E at the infinite places and the product of its conjugates (Prop. 8.5 and the paragraph after it, Lem. 7.2(b)); $N_1\alpha_E$ and α_E^{-1} integral and $N_1 d \in \mathfrak{D}_{E/\mathbb{Q}}$ (Lem. 8.2(c),(d)). Needs $37 \mid N_0$.	Props. 8.1 and 8.5 and Lems. 8.2 and 7.2
13	The Weil data and the period factor of B	`Parameters.instWeilDataE`, `Parameters.norm_iota_periodFactor`	The Weil data of Prop. 8.1, with α_E above c_0, and its norm statement. Needs $37 \mid N_0$, so that F is the maximal abelian subfield of L and B that of E, and the CM type.	Prop. 8.1

9.1. **The places.** This section proves the replacements of rows 5, 7, 9 and 10 of Table 1. Let p be a prime, ι_p an embedding of $\bar{\mathbb{Q}}$ in $\bar{\mathbb{Q}}_p$, and v_p the valuation of $\bar{\mathbb{Q}}_p$ with $v_p(p) = 1$. Let $\mathfrak{P}$ be the prime of E induced by $\iota_p \circ \Phi_1$; for $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ the prime induced by $\iota_p \circ \Phi_1 \circ \sigma$ is $w_\sigma = \sigma^{-1}\mathfrak{P}$, and $\bar{w}_\sigma = w_{c\sigma}$. Lemma 9.2 replaces the development's rule that Frobenius moves the places by the class of $-p$ (`Parameters.frob_ext`, `Parameters.frob_iff_eq_frobElem_pow`, `Parameters.smul_eq_iff_inert`, `Parameters.smul_eq_star_iff_inert`, `Parameters.q_eq_inert`) and its statements at the primes $\equiv 1 \bmod N_1 d$ (`Parameters.frobElem_eq_one`, `Parameters.smul_ne_star`, `Parameters.q_eq_of_modEq_one`).

Lemma 9.2. (a) *Let p be inert in k_d and unramified in E, $\mathrm{Fr} = \mathrm{Frob}_{\mathfrak{P}}$ and $h = h_{\mathfrak{P}} = c\mathrm{Fr}$. For $\sigma, \sigma' \in \mathcal{G}$, $w_{\sigma'} = w_\sigma$ if and only if $\sigma' \in \langle h^2 \rangle \sigma$, and $w_{\sigma'} = \bar{w}_\sigma$ if and only if $\sigma' \in h\langle h^2 \rangle \sigma$. The residue degree of w_σ over p is $\mathrm{lcm}(2, \mathrm{ord}\, h)$, with $\mathrm{ord}\, h = \mathrm{lcm}(\mathrm{ord}\, t_p, \mathrm{ord}(-p \bmod N_1))$, and its Frobenius is $\sigma^{-1}\mathrm{Fr}\sigma$.*

(b) *Let $p = d$, let j_0 generate the inertia group of $\mathfrak{P}$ in $\mathrm{Gal}(E/\mathbb{Q})$, and let $\mathrm{Fr}_d \in \mathcal{G}$ be the Frobenius of $\mathfrak{P}$ over the prime $\mathfrak{d}$ of k_d above d. Then j_0 is central, $cj_0 = z$ and $\mathrm{Fr}_d = (t_d, d)$, and $w_{\sigma'} = w_\sigma$ or $w_{\sigma'} = \bar{w}_\sigma$ according as $\sigma' \in \langle \mathrm{Fr}_d \rangle \sigma$ or $\sigma' \in z\langle \mathrm{Fr}_d \rangle \sigma$. The residue degree of w_σ over d is $\mathrm{ord}\, \mathrm{Fr}_d$, and its Frobenius over $\mathfrak{d}$ is $\sigma^{-1}\mathrm{Fr}_d\sigma$.*

(c) *Put $u_j = h^j$ in (a) and $u_j = z\mathrm{Fr}_d^j = (t_d^j, -d^j)$ in (b), for every $j \geq 0$. For odd j in (a) and every $j \geq 0$ in (b), and for every $y \in \mathcal{O}_E$ and every $\sigma \in \mathcal{G}$,*

$$v_p\big(\iota_p \Phi_{u_j\sigma}(y) - \iota_p \Phi_\sigma(\bar{y})^{p^j}\big) \geq \tfrac{1}{2}\big(1 - \big(\tfrac{p}{d}\big)\big),$$

that is, at least 1 in (a) and at least $\frac{1}{2}$ in (b); and u_j is the only element of $\mathcal{G}$ with this property.

(d) *In (a) and (b), let (w_i) be a tight frame of E of constant q, each vector repeated by its multiplicity, and put $z_{\sigma,i} = \iota_p \Phi_\sigma(\bar{w}_i)$. Then every $z_{\sigma,i}$ is integral, and for every j as in (c) and all $\sigma, \sigma' \in \mathcal{G}$*

$$\sum_i z_{\sigma,i}^{p^j} z_{\sigma',i} \equiv q\,[\sigma' = u_j\sigma]$$

modulo the elements of valuation at least $\frac{1}{2}(1 - (\frac{p}{d}))$.

(e) *If $p \equiv 1 \bmod N_1 d$ splits completely in L, it splits completely in E: the $2\#\mathcal{G}$ primes w_σ and $\bar{w}_\sigma$, $\sigma \in \mathcal{G}$, are distinct, and each has norm p.*

Proof. (a) As p is unramified, the decomposition group of $\mathfrak{P}$ is $\langle \mathrm{Fr} \rangle$. The equation $w_{\sigma'} = w_\sigma$ says $\sigma'\sigma^{-1}\mathfrak{P} = \mathfrak{P}$, and $w_{\sigma'} = \bar{w}_\sigma$ says $c\sigma'\sigma^{-1}\mathfrak{P} = \mathfrak{P}$, as c is central. So the two conditions are $\sigma'\sigma^{-1} \in \langle \mathrm{Fr} \rangle \cap \mathcal{G}$ and $\sigma'\sigma^{-1} \in c\langle \mathrm{Fr} \rangle \cap \mathcal{G}$. As p is inert in k_d, Fr^i lies in $\mathcal{G}$ exactly for even i, and $c\mathrm{Fr}^i$ exactly for odd i; as c is central and $c^2 = 1$, $\mathrm{Fr}^i = c^i h^i$, so these two sets are $\langle h^2 \rangle$ and $h\langle h^2 \rangle$. Since $c \notin \mathcal{G}$, $\mathrm{Fr}^i = c^i h^i = 1$ exactly when i is even and divisible by $\mathrm{ord}\, h$; so the residue degree $\mathrm{ord}\, \mathrm{Fr}$ is $\mathrm{lcm}(2, \mathrm{ord}\, h)$, and $\mathrm{ord}\, h$ is the lcm of the orders of its two coordinates. Transporting the residue map by σ^{-1} gives $\mathrm{Frob}_{\sigma^{-1}\mathfrak{P}} = \sigma^{-1}\mathrm{Fr}\sigma$.

(b) The field $L(\zeta_{N_1})$ is unramified at d, as L is ramified only at 2 and 37 and $d \nmid N_1$, while k_d is ramified there. So the inertia group $\langle j_0 \rangle$ has order two, and j_0 is the element of $\mathrm{Gal}(E/\mathbb{Q})$ trivial on $L(\zeta_{N_1})$ and non-trivial on k_d. As E is the compositum of these two fields, which meet in $\mathbb{Q}$, $\mathrm{Gal}(E/\mathbb{Q})$ is the product of their groups and j_0 is central; and cj_0 is trivial on k_d and equal to c on $L(\zeta_{N_1})$, so $cj_0 = z$. As $\mathfrak{d}$ is the only prime above d and E/k_d is unramified at $\mathfrak{d}$, the decomposition group of $\mathfrak{P}$ is $\langle \mathrm{Fr}_d \rangle \cup j_0\langle \mathrm{Fr}_d \rangle$, with $\langle \mathrm{Fr}_d \rangle$ its intersection with $\mathcal{G}$. The argument of (a) gives the two cosets, as $c\langle \mathrm{Fr}_d \rangle \cap \mathcal{G}$ is empty and $cj_0\langle \mathrm{Fr}_d \rangle = z\langle \mathrm{Fr}_d \rangle$. The residue field of $\mathfrak{d}$ is $\mathbb{F}_d$, so the residue degree of $\mathfrak{P}$ over d is $\mathrm{ord}\, \mathrm{Fr}_d$, and Fr_d acts on ζ as the Frobenius at d, $\zeta \mapsto \zeta^d$; so $\mathrm{Fr}_d = (t_d, d)$, and the Frobenius at $\sigma^{-1}\mathfrak{P}$ is $\sigma^{-1}\mathrm{Fr}_d\sigma$.

(c) In (a), for odd j, $u_j\sigma y = c\mathrm{Fr}^j\sigma y = \mathrm{Fr}^j(\sigma\bar{y})$, as c is central; Fr^j induces $x \mapsto x^{p^j}$ on $\mathcal{O}_E/\mathfrak{P}$, and $\iota_p \circ \Phi_1$ maps $\mathfrak{P}$ into the elements of valuation at least 1, as $\mathfrak{P}$ is unramified. In (b), $u_j\sigma y = cj_0\mathrm{Fr}_d^j\sigma y = j_0\mathrm{Fr}_d^j(\sigma\bar{y})$; j_0 acts trivially on $\mathcal{O}_E/\mathfrak{P}$, Fr_d as $x \mapsto x^d$, and $\iota_d \circ \Phi_1$ maps $\mathfrak{P}$ into the elements of valuation at least $\frac{1}{2}$, as $\mathfrak{P}$ has ramification index 2 over d. If $u \in \mathcal{G}$ has the same property, then $g = uu_j^{-1}$ satisfies $gx - x \in \mathfrak{P}$ for every $x \in \mathcal{O}_E$, so g stabilizes $\mathfrak{P}$ and acts trivially on its residue field; that is, g lies in the inertia group, which meets $\mathcal{G}$ trivially (in (b), $j_0 \notin \mathcal{G}$). So $u = u_j$.

(d) The vectors of a tight frame lie in the lattice $\mathfrak{a}$ of Proposition 8.1, and $N_1\alpha_E$ is integral (Lemma 8.2(c)), so $N_1 w_i \in \mathcal{O}_E$; as $p \nmid N_1$, every $z_{\sigma,i}$ is integral. By (c) for $y = N_1 w_i$, and as $N_1^{p^j} \equiv N_1 \bmod p$ and N_1 is a unit at p, $z_{\sigma,i}^{p^j} \equiv \iota_p \Phi_{u_j\sigma}(w_i)$. As c is central, $z_{\sigma',i} = \iota_p\big(\overline{\Phi_{\sigma'}(w_i)}\big)$, and the frame identity $\sum_i \Phi_{u_j\sigma}(w_i)\overline{\Phi_{\sigma'}(w_i)} = q\,[\sigma' = u_j\sigma]$ holds in $\Phi_1(E)$; applying ι_p gives the congruence.

(e) Such a prime splits completely in B, as $p \equiv 1 \bmod N_1$ and $(\frac{-d}{p}) = (\frac{p}{d}) = 1$, and so in the compositum $E = L \cdot B$. So every decomposition group above p is trivial, $\sigma \mapsto \sigma^{-1}\mathfrak{P}$ is a bijection from $\mathrm{Gal}(E/\mathbb{Q}) = \mathcal{G} \cup c\mathcal{G}$ onto the primes above p, and every residue degree is 1. □

At the primes g_0, g_1 and $\mathcal{N}$ of the data, which split completely in L (Section 4), part (e) is what the development's statements at these primes use. At each prime not split in k_d the development's partner $v_{-p^j\sigma}$ becomes $u_j\sigma$, for every $j \geq 0$. The development forms the partner also at a zero multiplicity and at the even powers of an inert prime, where the prime sum has weight $1 - (\frac{\nu}{d}) = 0$, and it reads the congruences of (c) and (d) only for odd j at an inert prime and for every $j \geq 0$ at d.

Lemma 9.3 replaces the development's return order, the order of $-p$ modulo N_0 (`Data.o₀`, `Data.placeOfInt_mul_mem_tops_iff`), and the divisibility of the orbit length at a served prime (`Data.IsServed.m_dvd_orderOf`).

Lemma 9.3. *Let p,* Fr *and h be as in Lemma 9.2(a), $D = \mathrm{ord}\, h$, and*

$$o = o_{\mathfrak{P}} = \mathrm{lcm}\big(\mathrm{ord}\, t_p, \mathrm{ord}(-p \bmod N_0)\big).$$

(a) *For $\tau \in \mathcal{T}_1$ and $e \in \mathbb{Z}$, $h^e\tau \in \mathcal{T}_1$ if and only if $o \mid e$. So $o \mid D$, and the tops in $\langle h\rangle\tau$ are the D/o distinct places $h^{ko}\tau$, $0 \leq k < D/o$.*

(b) *o differs from* $\mathrm{ord}(-p \bmod N_0)$ *exactly when t_p is a 3-cycle and $3 \nmid \mathrm{ord}(-p \bmod N_0)$, and then it is three times that order. In particular o and* $\mathrm{ord}(-p \bmod N_0)$ *have the same parity.*

(c) *Let $m = 2^{r/22}$ be the number of lifts, $\mathfrak{r}$ the least integer with $p^{\mathfrak{r}} \geq m$, and call p* served *if it is inert in k_d, $p \not\equiv \pm 1 \bmod m$, and o is odd with $o \leq \mathfrak{r}$. Then $m \mid D$ for every served p.*

Proof. (a) The integers e with $h^e\tau \in \mathcal{T}_1$ are those with $h^e \in \mathcal{T}_1$, the preimage of the subgroup $\mathcal{T}_1$ under $e \mapsto h^e$, so a subgroup of $\mathbb{Z}$ containing D. As $h^e = (t_p^e, (-p)^e)$ and $\mathcal{T}_1 = \{(1,u) : u \equiv 1 \bmod N_0\}$, it is $o\mathbb{Z}$. The exponent e matters only modulo D.

(b) If t_p is a transposition, $(\frac{-p}{37}) = \mathrm{sgn}\, t_p = -1$, as $h \in \mathcal{G}$, so $\mathrm{ord}(-p \bmod 37)$ is even and $o = \mathrm{ord}(-p \bmod N_0)$. If $t_p = 1$ there is nothing to prove, and if t_p is a 3-cycle, $o = \mathrm{lcm}(3, \mathrm{ord}(-p \bmod N_0))$.

(c) Write $m = 2^{b_0+1}$, so that $r = 22(b_0+1)$, and $p' = -p$. As $h^D = 1$, $p'^D \equiv 1 \bmod N_1$, hence modulo 2^{r+1}, so 2^r divides $(p'-1)D$ or $(p'+1)D$ (`two_pow_dvd_or_of_pow_eq_one`). At a served prime $p'-1$ and $p'+1$ have 2-adic valuation at most b_0, so $2^{r-b_0} \mid D$, and $m \mid D$ as $r - b_0 \geq b_0 + 1$. □

The change in (b) occurs at served primes. For $N_0 = 683760$ and $d = 341879$, the prime $p = 10256399$ is inert in k_d and $\equiv -1 \bmod N_0$, and the cubic is irreducible modulo p, so $o = 3$, where the development's order is 1. For all large x, $p < x_1$ and $m > p^2$, so p is not $\equiv \pm 1 \bmod m$, $\mathfrak{r} \geq 3$, and p is served.

For a prime w of E above p put $A_w = a\,\#\{\tau \in \mathcal{T}_1 : w_\tau = w\}$, with a the scale of Lemma 2.1 (`Data.markExponent`). A set Λ of primes above p is *marked* if $p < x_1$, p is not

split in k_d, Λ contains no conjugate pair, each of its primes is induced by a top, and p is served when $\Lambda \neq \varnothing$; it is *fully marked* if moreover every top induces a prime in Λ or the conjugate of one (`Data.IsMarked`, `Data.IsFullMark`).

Lemma 9.4 replaces the cyclic data that the development builds at a marked prime from the class of $-p$ (`Data.IsMarked.hasType_markOperator`).

Lemma 9.4. *Let p, Fr, h, D and o be as in Lemma 9.3.*

(a) *Suppose o is odd and D even, let $\tau \in \mathcal{T}_1$, $w = w_\tau$ and $n = D/o$. The n tops $h^{ko}\tau$, $0 \le k < n$, are all the tops that induce w or $\bar{w}$, and they alternate between the two. So $A_w = A_{\bar{w}} = an/2$. For a fully marked Λ, $\sum_{w\in\Lambda} A_w = a\#\mathcal{T}_1/2$, and for a marked Λ, $\sum_{w\in\Lambda} A_w \le a\#\mathcal{T}_1/2$.*

(b) *Let p be served, let w be a prime of a marked Λ, and let $\tau \in \mathcal{T}_1$ be a top with $w_\tau = w$. The embeddings $\iota_p \circ \Phi_1 \circ \mathrm{Fr}^{ko}\tau$, $0 \le k < n$, all induce w; for every y integral at w,*

$$\iota_p\Phi_1(\mathrm{Fr}^{(k+1)o}\tau y) \equiv \left(\iota_p\Phi_1(\mathrm{Fr}^{ko}\tau y)\right)^{p^o} \pmod{p};$$

and the residue field of w has $p^D = (p^o)^n$ elements.

(c) *In (b) the development's twisted Hecke estimate applies at w with this cycle of embeddings. Let I be the integral columns. For every truncation J, the operator $p^{A_w}T_{w,\mathfrak{r}}$ maps I into itself, and the index of $p^{A_w}T_{w,\mathfrak{r}}I + p^J I$ in I divides p^e for an integer e at most the dimension of the columns times*

$$128A_w \log b/(mp) + J/x^{14} + x^{40}.$$

Here a submodule I' of I has index dividing p^e when every finite family in I is carried into I' by a square matrix over the coefficient ring whose determinant divides p^e (`IndexDvd`).

Proof. (a) By Lemma 9.2(a), $w_{h^e\tau}$ is w for even e and $\bar{w}$ for odd e, the parity being well defined modulo the even number D. The tops inducing w or $\bar{w}$ lie in $\langle h\rangle\tau$, so by Lemma 9.3(a) they are the $h^{ko}\tau$, and as o is odd, ko has the parity of k. So n is even and each of the two primes is induced by $n/2$ of them. A fully marked Λ contains exactly one prime of each pair met by the tops, so exactly half the tops induce a prime of Λ; a marked Λ contains at most one prime of each pair.

(b) As c is central, $c^{ko}h^{ko}\tau = \mathrm{Fr}^{ko}\tau$: the labels $h^{ko}\tau$ with k odd are corrected by conjugation. The prime induced by $\iota_p \circ \Phi_1 \circ \mathrm{Fr}^{ko}\tau$ is $\tau^{-1}\mathrm{Fr}^{-ko}\mathfrak{P} = \tau^{-1}\mathfrak{P} = w$. As Fr^o induces $x \mapsto x^{p^o}$ on $\mathcal{O}_E/\mathfrak{P}$, the reductions advance by the p^o-power map, and modulo p this holds on the local valuation ring, as p is unramified. By Lemma 9.2(a) the residue field has $p^{\mathrm{lcm}(2,D)} = p^D$ elements, as $m \mid D$ (Lemma 9.3(c)) and m is even.

(c) A square root of p is integral in the valuation ring of the coefficients, p is a uniformizer at $w \neq \bar{w}$, and $p < x_1 \le \min(g_0, g_1, \mathcal{N})$ gives maximal compact level at w. With (b) these are the range, signs, residue maps and cardinality of the cyclic twisting data of the estimate (`Columns.hasType_markOperator`). Its numerical hypotheses (`HeckeSizes`) hold as for B. Put $\ell = n/2$, $Y = x^{40}$, $\kappa = x^{-14}$ and $X = \log x$, and let $k' = \mathfrak{n} + 1 - m$ (`Data.k`). By the data and Lemma 7.2(a), $D, n \le \#\mathcal{G} \le x^{12}$, $1 \le o \le \mathfrak{r} \le 32X$, $e^{-2}x^5 \le k' \le x^6$, $x^{1/2} \le m \le 2x^{1/2}$ and $bx \le a \le ebx$. So $2\mathfrak{r} \le k'$, $\kappa \le 1 \le Y$ and $2\ell = n$. As $p \ge 13$ and $m \mid D$, $nak'(\ell+2) + a + k' \le 10bx^{31} < b^2 \le e^m \le P^\ell$, with $P = p^o$. Also $6(2(k'+k'^2)Dn+2)+2 \le 24x^{36}+14 \le Y$, and $2(n+2)k'/Y \le 6x^{-22} \le \kappa$. With $Z = \log x_1$, $10^6X \le Z$ and $Z^6 \le \log b$, so $3\mathfrak{r}o\log p \le 3(32X)^2Z \le \frac{1}{2}\log b$, and

$(Y+n(k'+1))k'P^{3\mathfrak{r}}+k'+2 \le 4x^{46}b^{1/2} \le a/Y$. Finally $P^{2\mathfrak{r}} \ge mp$ and $m\mathfrak{r}^2 \le k'$, so the last error $na(P^{-2\mathfrak{r}}+\mathfrak{r}^2/(k'P))$ is at most $2na/(mp) \le 128A_w \log b/(mp)$. □

For the ordered product of these operators over Λ, repeated m times, take $J = \lceil 2m\#\mathcal{G}\, a/p \rceil$ and add the exponents. Each of the three resulting terms is at most $L_p = \#\mathcal{G}\, a(\log b)^2/p$: the first as $\sum_{w\in\Lambda} A_w \le a\#\mathcal{G}/2$; the second as $m\#\Lambda J/x^{14} \le (\#\mathcal{G}\, a/p)(8/x)+m\#\mathcal{G}/x^{14}$; and the third as $m\#\Lambda x^{40} \le m\#\mathcal{G}\, x^{40}$ and $p < x_1 \le b^{10^{-6}}$. This gives $3\,\mathrm{loss}(p)$ per dimension, the development's bound for this product (`Data.IsMarked.hasType_prod_markOperator_pow`), where $\mathrm{loss}(p) = L_p$, multiplied by m if $p \equiv \pm 1 \bmod m$ (`Data.loss`).

For a set S of places, a *collision* outside S at p is a pair (τ, e) with $e \ge 1$, e odd or $p = d$, and τ and $u_e\tau$ both in $\mathcal{T}_1 \setminus S$; its weight is a/p^e, and $B_p(S)$ is the total weight of the collisions outside S (`Data.IsCollision`, `Data.collisionSum`). Lemma 9.5 replaces the development's count of collisions and its avoidance of the thick places, which use the class of $-p^e$.

Lemma 9.5. *Let $p < x_1$ be inert in k_d or $p = d$.*

(a) *At inert p every collision exponent is odd and divisible by o, so there is no collision if o is even. At d, for every $e \ge 0$ and $\tau \in \mathcal{T}_1$, the class of $u_e\tau$ modulo N_0 is $-d^e \not\equiv 1$, so $u_e\tau$ is not a top (`Data.ne_d_of_placeClass_eq`); in particular there is no collision.*

(b) *If every collision exponent outside S is at least v, then $B_p(S) \le 2\#\mathcal{G}\, a/p^v$.*

(c) *If p is not served, $m\,B_p(\varnothing) \le \mathrm{loss}(p)$. If p is served and Λ is fully marked, then $B_p(S) = 0$ for the set S of tops that induce a prime of Λ.*

(d) *At inert p with o odd, no place $h^e\tau$ with $\tau \in \mathcal{T}_1$ and $e \in \mathbb{Z}$ is thick.*

Proof. (a) At inert p this is Lemma 9.3(a). At d, the class of $u_e\tau$ modulo N_0 is $-d^e$. As $d \equiv N_0/2 - 1 \bmod N_0$ and $4 \mid N_0$, $d^2 \equiv 1 \bmod N_0$, so $-d^e$ is -1 or $-d$ modulo N_0, and neither is 1, as $N_0 \nmid d+1$.

(b) There are at most $\#\mathcal{T}_1 \le \#\mathcal{G}$ tops, and $\sum_{e\ge v} p^{-e} \le 2p^{-v}$.

(c) If $p \equiv \pm 1 \bmod m$, take $v = 1$: $mB_p(\varnothing) \le 2m\#\mathcal{G}\, a/p \le \mathrm{loss}(p)$, as $(\log b)^2 \ge 2$. Otherwise a collision at inert p forces o odd by (a), and as p is not served, $o > \mathfrak{r}$, so every collision exponent is at least $\mathfrak{r}+1$; as $p^{\mathfrak{r}} \ge m$, $mB_p(\varnothing) \le 2m\#\mathcal{G}\, a/p^{\mathfrak{r}+1} \le \mathrm{loss}(p)$. At d, $B_d(\varnothing) = 0$ by (a). If p is served, a collision (τ, e) has e odd, so τ and $h^e\tau$ induce conjugate primes (Lemma 9.2(a)), one of which is in Λ; so τ or $h^e\tau$ lies in S.

(d) The map $\pi\colon \mathcal{G} \to (\mathbb{Z}/N_0)^\times$, $(t,u) \mapsto u \bmod N_0$, is a homomorphism. The image of h is $-p$, of order dividing the odd number o, and every top maps to 1, so $\pi(h^e\tau)$ lies in a subgroup of odd order; every thick place maps to -1, of order two. □

Lemma 9.6 replaces the development's thick set, built in the commutative group of places (`exists_three_term_free`, `exists_data`), and its count of the thick places met by the translates of the tops (`Data.remainder_eq`).

Lemma 9.6. *Let $M = N_0 3^{\lfloor \log_3 r \rfloor + 5}$ and $\phi\colon C \to (\mathbb{Z}/2^{r+1})^\times$, $(1,u) \mapsto u \bmod 2^{r+1}$.*

(a) *For all large x there is a set $\Theta \subset z\mathcal{T}_1$ with $\#\Theta \ge (N_1/N_0)/\log b$, whose elements have second coordinate $\equiv -1 \bmod M$, such that for $\sigma, \tau, \rho \in \Theta$ and $0 < i < j \le 324r$, $\phi(\sigma^{-1}\tau)^j = \phi(\sigma^{-1}\rho)^i$ implies $\phi(\sigma^{-1}\tau) = 1$.*

(b) *Let $\nu = p^j$, with p inert in k_d and j odd or $p = d$, and let u_j be its partner (Lemma 9.2(c)). The number of tops τ with $u_j\tau \in \Theta$ is*

$$n(\nu) = \#\Theta \cdot [\nu \equiv 1 \bmod N_0] \cdot [t_p^j = 1].$$

Proof. (a) The base $z = (1, -1)$ lies in C, as $37 \equiv 1 \bmod 4$, and so does $g = (1, M + 1)$, as $37 \mid M$ and every prime divisor of N_1 divides M; and $g \in \mathcal{T}_1$, as $N_0 \mid M$. Apply `exists_three_term_free` to ϕ on the commutative group C, with base z and step g, as `exists_data` does in $(\mathbb{Z}/N_1)^\times$. The order a_0 of $\phi(g)$ satisfies $2^r \le (M+2)a_0$ (`two_pow_le_of_pow_eq_one`). Put $W = x^{\varepsilon/6}$, so that $\log b = W^6$. In the construction for large x, fix its dimension n_0 with $2^r \le W^{n_0}$, and take a power of two Y with $Y^{n_0} \le 2^r/W < (2Y)^{n_0}$. As $r \le 32 \log x$ and $M \le 243 N_0 r$, for large x one has $(M+2)(324r)^{n_0} \le W$ and $2^{n_0} n_0 \cdot 243 r \le W^3$, hence $(324rY)^{n_0} \le a_0$. The construction gives $\Theta \subset \{zg^e : e \ge 0\} \subset z\mathcal{T}_1$ of size at least $Y^{n_0}/(n_0 Y^2) > 2^r/(2^{n_0} n_0 W^3) \ge (N_1/N_0)/\log b$, as $Y \le W$; its second coordinates are $\equiv -1 \bmod M$, and it has the stated property, with $\sigma^{-1}\tau$ for the ratio.

(b) Multiplication by $(1, u) \in C$ on either side of (t, v) gives (t, uv), so the count is the same with right multiplication. As $u_j = (t_p^j, -\nu)$ (with t_d at $p = d$), each $\theta = (1, \theta_2) \in \Theta$ has the one candidate $\tau = u_j^{-1}\theta$, whose first coordinate is t_p^{-j}; so it can be a top only if $t_p^j = 1$, and then it is $(1, -\nu^{-1}\theta_2)$, a top exactly when $\nu \equiv -\theta_2 \equiv 1 \bmod N_0$. □

With these lemmas the proofs of the development's two column files, JetExponentBound and LocalStatement, run for E at the small nonsplit primes of the local argument, with h and the partners u_j acting on the left in place of the class of $-p$ and the places it names. Lemma 9.2(a) tells which places induce a prime and which its conjugate, so that at a served p the odd partners of a place inducing w induce $\bar{w}$, and it gives the residue field of a marked prime, with $p^{\mathrm{lcm}(2,D)} = (p^{D/2})^2$ elements, as D is even at a served prime (Lemma 9.3(c)); as an inert prime is unramified in E, p is a uniformizer at its primes. By Lemma 9.3(a),(c), $h^e\tau$ returns to the tops exactly when $o \mid e$, and $m \mid D$ at a served prime. Lemma 9.5 restricts the collision exponents, bounds the weight of the collisions by a geometric tail, gives the allowance at an unserved prime and the absence of collisions outside a full mark, and shows that at d the partners of the tops have the classes $-d^e \not\equiv 1$, and at inert p with o odd that the orbits of the tops avoid the thick places. These facts, with the marking of Lemma 9.4(a), the estimate at one marked prime in part (c) and the estimate for the product that follows its proof, the frame congruences of Lemma 9.2(c),(d) and the period norm of Proposition 8.1(d) at $p \nmid N_1$, give the marked-sum, jet, low-column and Hecke estimates of the two files, and hence the local divisibility at served and unserved primes, with the same index bound and thresholds.

The uses of commutativity that row 7 of Table 1 replaces fall into the following groups.

- The prime dictionary: the equal-or-conjugate and the odd shifts, the frame row, and the solution $v = \tau^{-1}\sigma$ of $\tau v = \sigma$ at the split primes (Lemma 9.2).
- The cyclic ordering of the marked operator and the full marking (Lemmas 9.3 and 9.4).
- The thick construction and the spacing of the thick places, with the ratio $v'^{-1}v$ (Lemma 9.6, Section 7.3).
- The admissible pairings of places and their extraction, through $h^{-1}v$ and $(h^i\sigma)\sigma^{-1} = h^i$ in the three-term test (Lemmas 9.2, 9.5 and 9.6).
- The thick correction of the remainder (Lemma 9.6(b)).
- The field set-up: left composition permutes the embeddings, Galois transitivity up to c gives transitivity up to conjugation, and summing the embeddings gives the relative trace (row 8).

- The period norm: the primes induced above the fixed prime of k_d have equal multiplicity and equal idele norms (Proposition 8.1(d)).
- The remaining uses: the group law itself, the old abelian instance and the CM type (rows 5 and 6).

All of these use only the group law of $\mathcal{G}$ and the embeddings extending the fixed embedding of k_d.

Two of these uses also depend on the scales of the data. In the three-term test, for $p \le k' = \mathfrak{n}+1-m$ and $0 < i \le 324r$, a trivial projected power would force $x^{11} \le 2^r \le (p+1)i \le (k'+1)324r$, which is impossible at these scales. In the spacing of the thick places, three places σ, ρ, τ with $\sigma^{-1}\rho \equiv \pm\ell^n$ and $\sigma^{-1}\tau \equiv \pm\ell^i$ modulo the divisors of N_1 prime to ℓ (`placeClass_ratio`), where $\ell \le k't$ is prime, $t = 5\mathfrak{n}$ and $0 < i < n \le 27r$, are not all thick. For odd ℓ, Lemma 9.6(a) at $(2i, 2n)$, as $2n \le 324r$, would give $\ell^{2i} \equiv 1 \bmod 2^{r+1}$, forcing $x^{11} \le 2^r \le (\ell+1)\,2i \le 54(k't+1)r$, which is impossible (`Data.HasLogBound`), as $k't \le 5\mathfrak{n}(\mathfrak{n}+1) < 46x^{10}$ and $r \le 32\log x$. For $\ell = 2$, as σ and τ have second coordinates $\equiv -1 \bmod M$, $\sigma^{-1}\tau \equiv 1 \bmod M$, so $4^i \equiv 1 \bmod 3^{\lfloor \log_3 r \rfloor + 5}$; as 4 has order $3^{\lfloor \log_3 r \rfloor + 4}$ there, $3^{\lfloor \log_3 r \rfloor + 4} \le i < 27r$, which is false, as $r < 3^{\lfloor \log_3 r \rfloor + 1}$.

For example, take $N_0 = 683760$ and $d = 341879$. The prime 4102561 is $\equiv 1 \bmod N_0$ and its t_p is a 3-cycle, so at $\nu = p$ the development's tops meet $\#\Theta$ thick places and $\mathcal{T}_1$ meets none; its first return to the tops is at $j = 2$ in the development and at $j = 6 = o_{\mathfrak{P}}$ for $\mathcal{T}_1$.

9.2. **The prime sum.** Every prime that ramifies in E divides $N_1 d$, and every prime dividing N_1 splits in k_d (proof of Proposition 8.1); so a prime inert in k_d is unramified in E. For each prime p inert in k_d, and for $p = d$, fix a reference embedding ι_p, and with it the partners $u_{p,j}$ of Lemma 9.2(c): $h^j_{\mathfrak{P}}$ for odd j, and $z\mathrm{Fr}_d^j$ at d. The prime sum at a place σ is that of Lemma 2.1 with these partners,

$$P(y,\sigma) = \sum_{\nu = p^j \le a} \Lambda(\nu)\Big(1 - \Big(\frac{\nu}{d}\Big)\Big)\big(y/\nu - w(u_{p,j}\sigma)\big)^+,$$

the sum over the prime powers $\nu = p^j \le a$ with p inert in k_d and j odd, or $p = d$ and $j \ge 1$; at the remaining prime powers $(\nu/d) = 1$, so their terms are zero. By Lemma 9.6(b) the translate of $\mathcal{T}_1$ by $u_{p,j}$ meets Θ in $n(\nu) = \#\Theta \cdot [\nu \equiv 1 \bmod N_0] \cdot [t_p^j = 1]$ places.

Lemma 9.7 replaces the development's single embedding at each prime.

Lemma 9.7. *Let p be inert in k_d or $p = d$, let ι' be another embedding of $\bar{\mathbb{Q}}$ in $\bar{\mathbb{Q}}_p$, whose prime is $k\mathfrak{P}$ with $k \in \mathcal{G}$, and let u'_j be its partners. Then $u'_j = k u_{p,j} k^{-1}$. Let $\nu = p^j$, and let y be a real function on $\mathcal{G}$ with $y(k\sigma k^{-1}) = y(\sigma)$ for all $k, \sigma \in \mathcal{G}$. Then for every top τ*

$$\big(y(\tau)/\nu - w(u'_j\tau)\big)^+ = \big(y(\tau)/\nu - w(u_{p,j}\tau)\big)^+,$$

and

$$\sum_{\sigma\in\mathcal{G}} \big(y(\sigma)/\nu - w(u'_j\sigma)\big)^+ = \sum_{\sigma\in\mathcal{G}} \big(y(\sigma)/\nu - w(u_{p,j}\sigma)\big)^+.$$

Proof. The element k exists as $\mathcal{G}$ is transitive on the primes above the prime of k_d below $\mathfrak{P}$. Transporting the residue map by k gives $\mathrm{Frob}_{k\mathfrak{P}} = k\,\mathrm{Frob}_{\mathfrak{P}}\,k^{-1}$, so $h_{k\mathfrak{P}} = k h_{\mathfrak{P}} k^{-1}$, as c is central; the same holds for Fr_d, and z is central. So $u'_j = k u_{p,j} k^{-1}$. The tops and the thick places are central, so conjugation by k fixes each top and maps Θ and its complement onto themselves; hence $w(k\sigma k^{-1}) = w(\sigma)$, as w is a/x on Θ and a/x_1 elsewhere. At a top, $u'_j\tau = k(u_{p,j}\tau)k^{-1}$, which gives the first identity, and the change of variable $\sigma \mapsto k\sigma k^{-1}$ in the sum, with $y(k\sigma k^{-1}) = y(\sigma)$, gives the second. □

The development's quantities built from these terms are of two kinds. The local divisibility asked at a top at order a (`Data.localAsk`) and the prime sum at a top (`Data.primeSum`) are top terms. The forced divisibility (`Data.forcedPart`), the sum of the local asks at $y = w(\sigma)$ over all places σ, and the cost of a direction (`Data.dirCost`), the sum over all places σ of a term that does not depend on the reference less $P(w(\sigma), \sigma)$, are sums over all places. The divisibility asked of the chain (`Data.gain`) is m times the sum of the top asks at order a plus mk' times the forced divisibility, with $k' = \mathfrak{n} + 1 - m$. At a place that is not a top, a local ask or a prime sum can change with the reference. For $N_0 = 683760$ and $d = 341879$, 13 is inert in k_d and t_{13} is a transposition; take $x > 13$, $\theta \in \Theta$ and $\sigma = u_{13,1}^{-1}\theta$. At order a the term of $\nu = 13$ is $a/13 - a/x$ for this reference and $a/13 - a/x_1$ for a reference whose t_{13} is another transposition, with coefficient 1 in the local ask and $2\log 13$ in the prime sum; for the second reference the partner of σ at each odd power 13^j, $j \geq 3$, lies outside Θ, so that its term can only increase.

For $y \leq a$ and every integer $U \geq \lceil x_1 \rceil$, the prime sum at a place is the sum over the primes $p < U$ of its local asks times $2\log p$, with the same reference on both sides (`Data.primeSum_eq_sum_localAsk`), and the development builds identities on this. Otherwise it reads local asks and prime sums through the top terms and the sums over all places, through the summability of the terms of one local ask inside its proofs at one embedding, through the vanishing of the local ask at a split prime, and in bounds that hold for every choice of partners. So the identities that sum over primes hold with the reference embeddings. Where an estimate at one p-adic embedding, which keeps that embedding's own partners, meets these quantities, in the Frobenius packing (`Data.exists_isFrobPacking`) and in the lower bound for the jet exponent, Lemma 9.7 moves the top terms and the sums over all places to those partners.

Proposition 9.8 (the remainder identity)**.** *In the notation of Lemma 2.1, with the tops $\mathcal{T}_1$,*

$$\sum_{\tau \in \mathcal{T}_1} \big(P(a,\tau) - A\big) = a\Big(\#\Theta\big(R_E(x) - R_E(x_1)\big) + \#\mathcal{T}_1\, R_1(x_1)\Big). \tag{9.1}$$

Proof. Write $\lambda_1(\nu) = \Lambda(\nu)(1 - (\frac{\nu}{d}))$ and $b_y(\nu) = (1/\nu - 1/y)^+$. At each ν, $\#\mathcal{T}_1 - n(\nu)$ tops are sent outside Θ, where $w = a/x_1$, and $n(\nu)$ into Θ, where $w = a/x$. So

$$\frac{1}{a}\sum_{\tau \in \mathcal{T}_1} P(a,\tau) = \#\mathcal{T}_1 \sum_{\nu} \lambda_1(\nu) b_{x_1}(\nu) + \#\Theta \sum_{\nu} \lambda_1(\nu)[\nu \equiv 1 \bmod N_0][t_p^j = 1]\big(b_x(\nu) - b_{x_1}(\nu)\big).$$

The first sum is $R_1(x_1) + \log x_1 - 1 - c_d$. In the second, $[t_p^j = 1] = f(\mathrm{Frob}_\nu)$, so it is $R_E(x) - R_E(x_1) + \delta(\log x - \log x_1)$, with $\delta = f_{\mathrm{pole}}/\varphi(N_0) = 1/(3\varphi(N_0))$; the constant κ_E cancels. As w is a/x on Θ and a/x_1 elsewhere, $\bar{w} = \log a - \log x_1 - (\#\Theta/\#\mathcal{G})(\log x - \log x_1)$, and $\#\mathcal{T}_1/\#\mathcal{G} = 1/(3\varphi(N_0)) = \delta$. So $\#\mathcal{T}_1 A$ equals a times $\#\mathcal{T}_1(\log x_1 - 1 - c_d) + \#\Theta\,\delta(\log x - \log x_1)$, and subtracting gives (9.1). By Lemma 9.7 the actual top sums may be used in this computation. □

9.3. **The last step.** For every large x the development gives a datum D (`exists_data`), whose primes g_0, g_1 and level $\mathcal{N}$ are chosen among the primes of their windows that split completely in L (Corollary 4.3). At every such datum the development's Theorems A, B and C, run on E with the replacements of Table 1, give the two covolume bounds of Section 2.2 for a family $\mathcal{F}$ of independent rows, with $\#\mathcal{F}$, $\mathcal{I}$ and $\mathcal{V}$ as there, $\mathcal{B} = \#\mathcal{G}\, a(\log b)^3$ and rem the left side of (9.1); the space of rows is non-zero, by the filling step run with γ_E

(Section 8.4; `Data.finrank_rows_ne_zero`), so the bounds may be divided by $\dim \mathcal{W}$:

$$\mathfrak{h} - 3\,\mathcal{B}\log b \;\le\; \frac{\mathcal{V}+2\mathcal{I}}{\dim \mathcal{W}} \;\le\; \mathfrak{h} - m\,\mathrm{rem} + \mathcal{B}\log b + 4x^{99} + 10\,\mathcal{B}\log(1+b^2).$$

The main term $\mathfrak{h}$ common to the two bounds cancels, the errors are at most $(\log b)^2\mathcal{B}$ as over $\mathbb{Q}$, and $(\star)$ holds for E: $m\,\mathrm{rem} \le (\log b)^2\mathcal{B}$. Both bounds use the frames, the generator of the vacuum, the Weil data and the different (Propositions 8.3, 8.4 and 8.1, Lemma 8.2, and Proposition 8.5), the size bounds (Lemma 7.2), and the partners, the thick places and the change of embedding at p (Lemmas 9.2, 9.6 and 9.7). The upper bound also uses the return orders, the marking and the collisions (Lemmas 9.3, 9.4 and 9.5), and the lower bound the computation at d in Lemma 9.5(a) and the odd-class bound (Corollary 7.6).

The development's last step moves the second scale. For all large x its window lemma (`IsPolar.exists_window_sub_mul_le`), applied to $v \mapsto R_E(e^v)$, polar by Proposition 6.1, and to $v \mapsto R_1(e^v)$, polar by the development's `isPolar_primeError` at modulus 1, gives a point $u \in [10^6 \log x, (10^6 \log x)^2]$ at which

$$R_E(e^u) - \frac{\#\mathcal{T}_1}{\#\Theta}\,R_1(e^u) \le x^{-10^6},$$

as the lemma allows any multiplier of R_1 in $[0, x^{10^6}]$, and $\#\mathcal{T}_1/\#\Theta$ lies in $[0, \log b]$ by Lemma 9.6(a), with $\log b = x^{\varepsilon} \le x^{10^6}$. Let D' be D with $\log x_1$ replaced by u. It is again a datum. Of its scale conditions, those that involve the second scale are $10^6 \log x \le u$, which holds by the choice of u, and $10^6 u \le \log b$ and $6 \log u \le \log\log b$, which hold at $\log x_1$ and so at u, as $u \le (10^6 \log x)^2 \le \log x_1$ by the construction of the data. Its other entries are those of D, and its level is chosen again, in its own window, among the primes that split completely in L (Section 4). At D', whose second scale is $x_1 = e^u$, divide the main inequality by $m\,a\,\#\Theta$, and use Proposition 9.8, $\#\Theta \ge \#\mathcal{T}_1/\log b$ (Lemma 9.6(a)) and $\#\mathcal{G}/\#\mathcal{T}_1 = 3\varphi(N_0)$. This gives

$$R_E(x) - R_E(x_1) + \frac{\#\mathcal{T}_1}{\#\Theta}\,R_1(x_1) \le \frac{3\varphi(N_0)(\log b)^6}{m} \le 3\varphi(N_0)\,x^{6\varepsilon-1/2},$$

as $m \ge \sqrt{x}$. So, at fixed (N_0, d) and $0 < \varepsilon < \frac{1}{100}$,

$$R_E(x) \le 3\varphi(N_0)\,x^{6\varepsilon-1/2} + x^{-10^6} \le x^{8\varepsilon-1/2}$$

for all large x. This proves Theorem 9.1.

9.4. **Proof of Theorem 1.1.** Let ρ be a zero of $L_F(s,\psi_3)$ with $\mathrm{Re}\,\rho > \frac{1}{2}$. Choose $\varepsilon \in (0, \frac{1}{100})$ with $\beta = \frac{1}{2} + 8\varepsilon < \mathrm{Re}\,\rho$, take $37 \mid N_0$, and let d be the prime that Theorem 5.1 gives for β and $y = |\,\mathrm{Im}\,\rho|$, with $d \equiv N_0/2 - 1 \bmod N_0$, so that d is one of the development's primes. By Theorem 9.1, $R_E(x) \le x^{\beta-1}$ for all large x, and Proposition 6.2 gives $L_F(\rho,\psi_3) \ne 0$, a contradiction. So $L_F(s,\psi_3)$ has no zero with $\mathrm{Re}\,s > \frac{1}{2}$, and by (1.1) and the development's theorem for $\zeta(s)$ (`riemannZeta_eq_zero_re`), neither has $\zeta_K(s)$ with $\frac{1}{2} < \mathrm{Re}\,s < 1$. The functional equation of ζ_K reflects this to $0 < \mathrm{Re}\,s < \frac{1}{2}$. As $\zeta_L = \zeta_K\,L(s,\chi_{37})\,L_F(s,\psi_3)$, and the development's theorem covers $L(s,\chi_{37})$ (`LFunction_eq_zero_re`), the extended Riemann hypothesis for L follows. □

Appendix A. The development and the re-check

The development. The development is the compact edition, `grh-compact`, of [19] at commit `72fead102f663d5c7a407964a13dc0cf9d977207`, on Lean `v4.35.0` and Mathlib at commit `56a005855ea17e0b0958f73ec801ae140b0a1679`. Below, files of the development are named

by their last component, and lines are those of the development at this commit. Its main theorem, `New.grh`, states that $L(s,\chi) \neq 0$ for every Dirichlet character χ and $\operatorname{Re} s > \frac{1}{2}$, except at $s = 1$ for principal χ. From it, `New.zeros_on_line` and `New.zeta_zeros_on_line` put on the line every zero with $0 < \operatorname{Re} s < 1$ of every Dirichlet L-function and every non-trivial zero of $\zeta(s)$; `src/Main.lean` states the results without hypotheses, among them `LFunction_eq_zero_re` and `riemannZeta_eq_zero_re`. Their axioms are `propext`, `Classical.choice` and `Quot.sound`. A formalization of this paper's argument against the development is under way and will be released separately.

The re-check, and what it does not see. Nothing in the source is edited and nothing is elaborated again. In a private copy of the compiled modules of the unmodified build, each constant of a set S is replaced by an axiom with the same name, universe parameters and type. The set S has 150 constants: `Parameters.E`, the development's E, our B; every other constant of `New.Data.Different` whose closure contains `E`, except four definitions whose values apply a construction that does not see the cyclotomic structure (`Parameters.Φ`, `bigOmega`, `c₀InE` and `sqrtNegDInE`); and `instUnramCMFieldE`, the embedding of E in $\mathbb{Q}(\mu)$. Every name still resolves and every stored type is unchanged; what is removed is the ability to unfold a member of S, among them the identity of E with `CyclotomicField`, the values of ζ, of `relDifferentGen`, of the group law `instCommGroupΦ`, of `placeOfInt`, `placeClass` and `placePerm`, and the stored proof that E is a cyclotomic extension of k_d.

The program, `KReplayAll.lean` in the data record of this paper [9], re-adds each constant of the closure of `New.grh` to Lean's kernel with `Environment.addDeclCore` (`KReplayAll.lean`, l. 194 and 510), under a fresh name, in this copy; this is the kernel check the replay tools apply. Of the 150 members of S, 138 lie in the closure, and of its other 37,419 constants the kernel accepts 37,395 and rejects 24; eight of the accepted were checked again at a higher memory limit, their first checks having exceeded the run's.

Each rejected constant needs one of seven removed values and lies in a row of Table 1 (the record lists each with its value and row [9]). A constant that only names a member of S is not rejected, as the kernel infers the type of a constant from its stored type and unfolds a constant only if it has a value, which an axiom has not.

The masking takes effect: the theorem $E =$ `CyclotomicField`… by `rfl`, and the stored proof that E is cyclotomic, are accepted unmasked and rejected masked. Each constant receives its own verdict, as importing compiled modules inserts their constants without a kernel check (`finalizeImport` in `Lean/Environment.lean`), the list of constants to check is fixed beforehand from the stored terms, and each check starts from the same environment.

What the re-check cannot see is a use through a type: a masked constant keeps its type, so `instCommGroupΦ` still supplies commutativity of the places, and the instance that E is cyclotomic still supplies that statement. These uses are the subject of rows 3 and 7 of Table 1 and of the third check, below.

The statements of the set-up. Masking keeps types, so a step may still use a statement of the set-up. Each member of S was read with E in place of the development's field, the statement of a definition being its type and a definition keeping its value wherever that value can be formed for E. Then 130 members are true for E, 20 are false for E or cannot be formed for it, and none is undecided; the record lists each member with its reading [9]. Two readings need a word. The value of `Parameters.placeOfInt`, the inverse of the bijection of the places of B onto $(\mathbb{Z}/N_1)^\times$, cannot be formed for E; we read `placeOfInt` as the homomorphic section $a \mapsto (\tau^{\epsilon(a)}, a)$, with τ a fixed transposition and $\epsilon(a) = 0$ or 1 as $(\frac{a}{37}) = 1$ or -1, extended by 1 off the units. This is a convention: the proof for E uses no

inverse of the class map (row 9). The generator ϖ of the different of the set-up keeps its value for B, so `different_eq_span_varpi`, one of its parts and `prod_varpi_eq_rootDiscr_pow` are false for E, while `infinitePlace_apply_varpi` is true; γ_E of Proposition 8.5 replaces ϖ (row 12). Every direct user, in the closure and outside `New.Data.Different`, of a member of S that is false for E or cannot be formed for it lies in a row of Table 1, and the list below names seven such users under rows 3 and 12.

The structure of the set-up. The commutative group law of the places, `instCommGroupΦ`, and the abelian-extension instances of the field are reached through instance resolution, which the re-check does not see. Every module that names them was compiled with them removed and three facts supplied in their place: that the field is Galois over $\mathbb{Q}$ and over k_d, and that it is a CM field. All three hold for our E, a compositum of Galois extensions of $\mathbb{Q}$ that is CM by Lemma 3.6, and as all three are propositions, a declaration can use only their statements. Eleven of these modules were compiled in this way one at a time against the unmodified build, and the sixteen others in a chain of 63 modules: the sixteen, eight of the eleven, and the 39 between them. As Lean compiles the development, every declaration of the sixteen compiles when the places are given only a group structure, and the sixteen still compile with the abelian-extension instances removed as well, none of their constants using those instances. In the eleven modules seven declarations fail, each in one of the seven groups described in the third column of row 7 of Table 1. The option `tactic.skipAssignedInstances false` makes `rw` and `simp` synthesize again the instances they use. With it set and the instances removed, twelve declarations fail in the eleven modules and 30 in the chain. Of the twelve, nine are in these seven groups, the seven above and two more, and the other three also fail with the option alone, with the instances in place. Of the 30, five are among those nine: four of them fail without the option too, and the fifth compiles without it, its log showing a use of the commutative group law [9]. Twenty-four others also fail with the option alone, with the instances in place, and the remaining one, `Data.descent_past_gridPathMap`, reports a missing equation lemma of `Data.legDescents`, which fails to elaborate.

Where the rows are used.

1: `Parameters.isTightFrame_zeta_pow` and `Parameters.exists_isTightFrame`, TightFrameExists 57–66 and 87–92.

2: `Data.exists_char_hasWeight`, IndexTypes 89–97; the Weil data, WeilDataOfE 222–243.

3: `Parameters.toCycloField`, Different 104, and `Data.algebraMap_mem_cycloField`, LevelPlacesChosen 20–21, used at FitTwistsExist 54, DenominatorBound 31 and 98 and RibetElement 37 and 135; `instUnramCMFieldE`, LevelPlacesChosen 16–18.

4: `fixes_emb_of_fixes_rootsOfUnity`, ThickSpacing 12–16, used at OnePlaceDefect 38 and 53.

5: The abelian instance, the indexing of the places and the CM type, Different 110, 116–123 and 144–146; `Parameters.exists_smul_eq_or_star`, WeilDataOfE 103–110.

6: The group law, Different 112 and 120–123.

7: The uses described after Lemma 9.6, in JetExponentBound and LocalStatement, at `Data.exists_isMarked`, `Data.IsMarked.notMem_thick`, `Data.IsMarked.sum_inducedPlace_sub_star_eq_zero`, `Data.jetExponent` with `couplingCount`, `Data.le_jetExponent`, `Data.IsMarked.sum_lowColumns_le`, `Data.IsGoodDatum.exists_hecke_transfer`, `Data.IsGoodDatum.mem_raises`, `Data.IsMarked.hasType_prod_markOperator_pow`, `Data.IsGoodDatum.gaugeLe_Bmu_of_isMarked`, `Data.IsGoodDatum.gaugeLe_collisionSum`, `Data.IsGoodDatum.gaugeLe_pow_jetCeil_smul` and `Data.exists_indexDvd_Bmu_divisible`.

8: `Parameters.placePerm`, Different 224–231; the Galois conjugates of the lift, AlgebraicPartConjugates 52–78; `Parameters.coe_trace_eq_sum`, TightFrameExists 12.

9: `Parameters.placeClass` and `Parameters.placeOfInt`, Different 127–139, 196 and 217–218; `placeClass_ratio`, ThickSpacing 27–39.

10: `Parameters.frob_ext`, WeilDataOfE 43–56, `Parameters.frob_iff_eq_frobElem_pow`, 59–69, and `Parameters.frobElem_eq_one`, 143–145, used at ThetaProducts 57–76 and MarkedPrimeType 39–51.

11: `Parameters.card_infinitePlace_E`, Different 168–169, used at Magnitudes 155–156, ConjugateGenerator 64–65, ConjugatesOfJets 216, GoodFormTransfer 79–80 and ShortAndEnough 105–111; `Parameters.card_placeClass_eq`, Different 174–175, used at ShortAndEnough 109 and New/Main 147–167.

12: `Parameters.relDifferent_spec` and `Parameters.relDifferentGen`, Different 299–301 and 317; the valuation identity, WeilDataOfE 189–211; `Parameters.herm_mem_quadInt`, TightFrameExists 15–23; the strong size control, `Data.hasLogBound_varpi`, IndexTypes 19. The integrality of $N_1\alpha_B$, WeilDataOfE 219, is used at CrudeRows 148, ThetaProducts 64, ConjugatesOfJets 207 and NaturalFormNear 135; that of α_B^{-1}, WeilDataOfE 207, at CrudeRows 148 and TightFrameExists 61; and $N_1 d \in \mathfrak{D}_{B/\mathbb{Q}}$, Different 330, at WeilDataOfE 95, SizeEstimates 71, CrudeRows 212, RowsReached 97, LineArithmetic 43, LineCoordinates 61, NaturalFormNear 136 and ChainValuation 255. The record lists the direct users of `Parameters.relDifferent_spec`, of `Parameters.relDifferentGen` and of the three integrality statements [9]. Users of members of S false for E: `Data.filling._proof_71`, FillingData 125–140; `Data.gradingY._proof_8`, GradingsOfY 191–196; `Data.valuation_shift_const_eq_ideleA_norm`, PairTensorData 195–202; `Data.hasLogBound_rootDisc._simp_1`, IndexTypes 29–33; `Data.instIsAdmissibleEFilling`, FillingAdmissible 39–81; and `Parameters.norm_gal_vacuumRoot`, PeriodDefs 17–30.

13: `Parameters.instWeilDataE`, WeilDataOfE 222–243; `Parameters.norm_iota_periodFactor`, TightFrameExists 36.

The declarations cited. The files are relative to `grh-compact/src`.

Declaration	File, line
`abs_log_mass_ratio_sub_le`	`Lib/SiegelWeil/Mass/MassRatio.lean`, l. 21
`classNumber_le`	`Lib/General/NumberTheory/ClassNumberBound.lean`, l. 10
`Columns.hasType_markOperator`	`New/Columns/TwistedHeckeType.lean`, l. 146
`couplingCount`	`New/Curve/LiveSum.lean`, l. 69
`Data.algebraMap_mem_cycloField`	`New/Selmer/LevelPlacesChosen.lean`, l. 20
`Data.budget`	`New/Data/AdmissibleData.lean`, l. 143
`Data.c_ge`	`New/Data/Magnitudes.lean`, l. 21
`Data.chosenGroupOrder`	`New/Data/ChosenPlaceLevels.lean`, l. 36
`Data.collisionSum`	`New/Curve/LiveSum.lean`, l. 65
`Data.depth_indicator_jet`	`New/Rows/GluedFormTheta.lean`, l. 33
`Data.dirCost`	`New/Data/AdmissibleData.lean`, l. 151
`Data.enough_forms`	`New/Endgame/ShortAndEnough.lean`, l. 173
`Data.exists_char_hasWeight`	`New/Seesaw/IndexTypes.lean`, l. 89
`Data.exists_family_covolumeSq_le`	`New/Endgame/LongForms.lean`, l. 78
`Data.exists_indexDvd_Bmu_divisible`	`New/Columns/LocalStatement.lean`, l. 285
`Data.exists_isFrobPacking`	`New/Curve/DepthPairs.lean`, l. 34
`Data.exists_isMarked`	`New/Columns/JetExponentBound.lean`, l. 57
`Data.exists_prime_window`	`New/Data/AdmissibleData.lean`, l. 44
`Data.finrank_rows_le_mass`	`New/Filling/RowDimension.lean`, l. 15
`Data.finrank_rows_ne_zero`	`New/Filling/FillingTheorem.lean`, l. 45
`Data.forcedPart`	`New/Curve/LiveSum.lean`, l. 24
`Data.gain`	`New/Curve/LiveSum.lean`, l. 28
`Data.HasLogBound`	`New/Data/Magnitudes.lean`, l. 18
`Data.hasLogBound_f`	`New/Data/Magnitudes.lean`, l. 155
`Data.hasLogBound_rootDisc`	`New/Seesaw/IndexTypes.lean`, l. 30
`Data.hasLogBound_varpi`	`New/Seesaw/IndexTypes.lean`, l. 19
`Data.heightPerRow_le`	`New/Endgame/ShortAndEnough.lean`, l. 48
`Data.IndexLe`	`New/Endgame/ShortAndEnough.lean`, l. 130
`Data.integral_forms_long`	`New/Endgame/LongForms.lean`, l. 63
`Data.IsCollision`	`New/Curve/LiveSum.lean`, l. 61

Declaration	File, line
Data.IsFullMark	New/Exchange/CrudeModularData.lean, l. 85
Data.IsGoodDatum.exists_hecke_transfer	New/Columns/LocalStatement.lean, l. 50
Data.IsGoodDatum.gaugeLe_Bmu_of_isMarked	New/Columns/LocalStatement.lean, l. 255
Data.IsGoodDatum.gaugeLe_collisionSum	New/Columns/LocalStatement.lean, l. 264
Data.IsGoodDatum.gaugeLe_pow_jetCeil_smul	New/Columns/LocalStatement.lean, l. 272
Data.IsGoodDatum.mem_raises	New/Columns/LocalStatement.lean, l. 106
Data.IsMarked	New/Exchange/CrudeModularData.lean, l. 77
Data.IsMarked.hasType_markOperator	New/Columns/MarkedPrimeType.lean, l. 15
Data.IsMarked.hasType_prod_markOperator_pow	New/Columns/LocalStatement.lean, l. 233
Data.IsMarked.notMem_thick	New/Columns/JetExponentBound.lean, l. 79
Data.IsMarked.sum_inducedPlace_sub_star_eq_zero	New/Columns/JetExponentBound.lean, l. 88
Data.IsMarked.sum_lowColumns_le	New/Columns/JetExponentBound.lean, l. 208
Data.IsServed.m_dvd_orderOf	New/Columns/JetExponentBound.lean, l. 21
Data.isSplitLevel_nonInducedPlaces	New/Seesaw/LiftCharacters.lean, l. 57
Data.jetExponent	New/Columns/JetExponentBound.lean, l. 115
Data.k	New/Data/AdmissibleData.lean, l. 82
Data.le_jetExponent	New/Columns/JetExponentBound.lean, l. 168
Data.localAsk	New/Curve/LiveSum.lean, l. 19
Data.loss	New/Curve/LiveSum.lean, l. 39
Data.mainHeight	New/Endgame/ShortAndEnough.lean, l. 32
Data.markExponent	New/Exchange/CrudeModularData.lean, l. 98
Data.N	New/Seesaw/IndexTypes.lean, l. 145
Data.ne_d_of_placeClass_eq	New/Curve/DepthPairs.lean, l. 18
Data.nominalWeight_add_le	New/Data/Weights.lean, l. 25
Data.o_0	New/Curve/LiveSum.lean, l. 53
Data.placeOfInt_mul_mem_tops_iff	New/Columns/JetExponentBound.lean, l. 34
Data.primeSum	New/Data/AdmissibleData.lean, l. 138
Data.primeSum_eq_sum_localAsk	New/Columns/SizeEstimates.lean, l. 29
Data.remainder	New/Endgame/ShortAndEnough.lean, l. 42
Data.remainder_eq	New/Endgame/ShortAndEnough.lean, l. 86
Data.s_le	New/Data/AdmissibleData.lean, l. 25
Data.scale	New/Data/AdmissibleData.lean, l. 29
Data.seesaw	New/Seesaw/SeesawTheorem.lean, l. 135
Data.short_forms	New/Endgame/ShortAndEnough.lean, l. 138
denominatorLe_rowBudget	New/Selmer/DenominatorBound.lean, l. 47
entireL_ne_zero_of_primeError_le	New/Endgame/OneSidedCriterion.lean, l. 28
eventually_primeError_le_rpow	New/Main.lean, l. 149
exists_cycChar_pow_sub_one_dvd	New/Selmer/DenominatorBound.lean, l. 26
exists_data	New/Data/DataExist.lean, l. 49
exists_detecting_points_cocycles	Lib/Cyclotomic/OddSha/OddShaBound.lean, l. 19
exists_detecting_points_hom	Lib/ClassField/Global/Avatars.lean, l. 213
exists_entireL_quadTwist_ne_zero	Lib/Analytic/QuadraticTwist/ZeroFreeTwist.lean, l. 193
exists_eq_principalIdele_mul_norm	Lib/ClassField/Global/CMNorms.lean, l. 35
exists_isFitFamily	New/Selmer/FitTwistsExist.lean, l. 24
exists_isLaw	New/Selmer/ReciprocityLaw.lean, l. 48
exists_isPrimeTriangle	New/Selmer/TrianglePrimes.lean, l. 24
exists_length_shaOdd_le	Lib/Cyclotomic/OddSha/OddShaBound.lean, l. 69
exists_prime_modEq_one_log_mem	Lib/Analytic/Primes/AuxiliaryPrimes.lean, l. 69
exists_three_term_free	New/Data/DataExist.lean, l. 20
fixes_emb_of_fixes_rootsOfUnity	New/Selmer/ThickSpacing.lean, l. 12
hasTriangleCost_tateTwist	New/Selmer/TateTwistSteps.lean, l. 28
HeckeSizes	New/TwistedHecke/Counting.lean, l. 163

Declaration	File, line
index_pow_at_places_le	Lib/ClassField/Global/Avatars.lean, l. 44
IndexDvd	New/Core/ModuleIndex.lean, l. 20
IsIntegralOnNullCone	New/Curve/FormalParameter.lean, l. 101
IsPolar	Lib/Analytic/Landau/PolarLandau.lean, l. 34
IsPolar.exists_window_sub_mul_le	New/Endgame/OneSidedCriterion.lean, l. 73
IsPolar.landau	Lib/Analytic/Landau/PolarLandau.lean, l. 88
isPolar_primeError	New/Endgame/PrimeError.lean, l. 69
IsTightFrame	Lib/Weil/Construction/ConjugateJetDefs.lean, l. 21
LFunction_eq_zero_re	Main.lean, l. 10
mellin_gaussianTheta_char	Lib/Analytic/DirichletTheta/MellinTheta.lean, l. 158
New.grh	New/Main.lean, l. 174
New.zeros_on_line	New/Main.lean, l. 194
New.zeta_zeros_on_line	New/Main.lean, l. 200
nonempty_splittingChar	Lib/ClassField/HeckeCharacter/SplittingCharExists.lean, l. 19
norm_gaussianTheta_functional_equation	Lib/Analytic/DirichletTheta/MellinTheta.lean, l. 139
Parameters	New/Data/Different.lean, l. 23
Parameters.c	New/Data/AdmissibleData.lean, l. 15
Parameters.card_infinitePlace_E	New/Data/Different.lean, l. 168
Parameters.card_placeClass_eq	New/Data/Different.lean, l. 174
Parameters.coe_trace_eq_sum	New/Curve/TightFrameExists.lean, l. 12
Parameters.different_eq_span_varpi	New/Data/Different.lean, l. 353
Parameters.exists_isJetConjugate_generator	New/Curve/ConjugateGenerator.lean, l. 26
Parameters.exists_isTightFrame	New/Curve/TightFrameExists.lean, l. 90
Parameters.exists_smul_eq_or_star	New/Data/WeilDataOfE.lean, l. 105
Parameters.frob_ext	New/Data/WeilDataOfE.lean, l. 46
Parameters.frob_iff_eq_frobElem_pow	New/Data/WeilDataOfE.lean, l. 59
Parameters.frobElem_eq_one	New/Data/WeilDataOfE.lean, l. 144
Parameters.herm_mem_quadInt	New/Curve/TightFrameExists.lean, l. 15
Parameters.infinitePlace_apply_varpi	New/Data/Different.lean, l. 364
Parameters.instWeilDataE	New/Data/WeilDataOfE.lean, l. 225
Parameters.isTightFrame_zeta_pow	New/Curve/TightFrameExists.lean, l. 59
Parameters.jetScale	New/Curve/PeriodDefs.lean, l. 51
Parameters.norm_iota_periodFactor	New/Curve/TightFrameExists.lean, l. 36
Parameters.norm_jetSeries_le	New/Curve/ConjugatesOfJets.lean, l. 55
Parameters.placeClass	New/Data/Different.lean, l. 139
Parameters.placeOfInt	New/Data/Different.lean, l. 135
Parameters.placePerm	New/Data/Different.lean, l. 224
Parameters.q_eq_inert	New/Data/WeilDataOfE.lean, l. 129
Parameters.q_eq_of_modEq_one	New/Data/WeilDataOfE.lean, l. 158
Parameters.relDifferent_spec	New/Data/Different.lean, l. 299
Parameters.relDifferentGen	New/Data/Different.lean, l. 317
Parameters.smul_eq_iff_inert	New/Data/WeilDataOfE.lean, l. 119
Parameters.smul_eq_star_iff_inert	New/Data/WeilDataOfE.lean, l. 124
Parameters.smul_ne_star	New/Data/WeilDataOfE.lean, l. 151
Parameters.thetaProducts_normal_form	New/Curve/ThetaProducts.lean, l. 86
Parameters.toCycloField	New/Data/Different.lean, l. 104
placeClass_ratio	New/Selmer/ThickSpacing.lean, l. 30
primeError	New/Endgame/PrimeError.lean, l. 38
ribet_columns	New/Selmer/RibetElement.lean, l. 122
riemannZeta_eq_zero_re	Main.lean, l. 6

Declaration	File, line
`rowBudget`	`New/Selmer/RibetElement.lean`, l. 36
`shaOdd`	`Lib/ClassField/Places/SelmerDefs.lean`, l. 96
`Space.finitePart`	`Lib/Weil/Construction/FinitePart.lean`, l. 18
`Space.jetSeries`	`Lib/Weil/Construction/DataProduct.lean`, l. 32
`star_inequality`	`New/Main.lean`, l. 121
`sum_sq_gaussianTheta_jacobiSym_le`	`Lib/Analytic/QuadraticTwist/ZeroFreeTwist.lean`, l. 91
`thetaTailIntegral_zero_le_two_mul`	`Lib/Analytic/DirichletTheta/MellinTheta.lean`, l. 168
`three_lines_bound_of_LFunction_eq_zero`	`Lib/Analytic/QuadraticTwist/ZeroFreeTwist.lean`, l. 25
`two_pow_dvd_or_of_pow_eq_one`	`Lib/General/NumberTheory/QuadFieldSplitting.lean`, l. 77
`two_pow_le_of_pow_eq_one`	`Lib/General/NumberTheory/QuadFieldSplitting.lean`, l. 86
`WeilData`	`Lib/General/NumberTheory/UpsilonValues.lean`, l. 30
`WeilData.norm_map_chiFin`	`Lib/ClassField/HeckeCharacter/SplittingCharOnU1.lean`, l. 79
`zero_density_quadTwist`	`Lib/Analytic/QuadraticTwist/ZeroFreeTwist.lean`, l. 147

Declarations

Use of AI. This paper and its results were produced by an AI research system that the author designed, built and directs, running on Anthropic's Claude Fable 5.2 in Claude Code and OpenAI's GPT-6.2 Astra in Codex. The author chooses the problems and prioritizes the work. Separate AI agents checked each result. The system also searched the literature and checked the citations against reliable sources. The author read the paper and takes full responsibility for all of the paper's contents.

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [9].

References

1. Levent Alpöge, Untitled note, November 20, 2026, https://alpo.ge/remark.pdf.
2. Dean Cureton and Jesse Thorner, *A quasi-Riemann hypothesis for Dedekind zeta functions*, 2026, Preprint, Hexagon 2610.00200v2, https://hexagonmath.org/2610.00200v2.
3. Samit Dasgupta, Mahesh Kakde, Jesse Silliman, and Jiuya Wang, *The Brumer–Stark conjecture over* $\mathbb{Z}$, 2023, Preprint, arXiv:2310.16399v1.
4. Leonardo de Moura and Sebastian Ullrich, *The Lean 4 theorem prover and programming language*, Automated Deduction – CADE 28, Lecture Notes in Comput. Sci., vol. 12699, Springer, Cham, 2021, doi:10.1007/978-3-030-79876-5_37, pp. 625–635.
5. Pierre Deligne and Kenneth A. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), no. 3, 227–286, doi:10.1007/BF01453237.
6. *NIST Digital Library of Mathematical Functions*, https://dlmf.nist.gov/, Release 1.2.8 of 2026-09-15, F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, B. V. Saunders, H. S. Cohl and M. A. McClain, eds.; read November 27, 2026.
7. David Rodney Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), no. 3, 235–275, doi:10.4064/aa-72-3-235-275.
8. Boyang Hu, *A seven-eighths zero-free half-plane for unitary Weil L-functions*, 2026, Preprint, Hexagon 2610.00216v2, https://hexagonmath.org/2610.00216v2.

9. Manvir Jaswal, *Programs and data for "The Riemann hypothesis for the Dedekind zeta function of a non-abelian cubic field"*, 2026, Zenodo, doi:10.5281/zenodo.24637246.
10. Matti Jutila, *On mean values of Dirichlet polynomials with real characters*, Acta Arith. **27** (1975), 191–198, doi:10.4064/aa-27-1-191-198.
11. Manfred Kolster, *Higher relative class number formulae*, Math. Ann. **323** (2002), no. 4, 667–692, doi:10.1007/s002080200321.
12. Baiying Liu, *Mixed character moments and a zero-free half-plane for unitary Hecke L-functions*, 2026, Preprint, Hexagon 2611.00741v1, https://hexagonmath.org/2611.00741v1.
13. Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, Berlin, 1999, doi:10.1007/978-3-662-03983-0.
14. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, Berlin, 2008, doi:10.1007/978-3-540-37889-1.
15. Alberto Perelli and Jacek Pomykała, *Averages of twisted elliptic L-functions*, Acta Arith. **80** (1997), no. 2, 149–163, doi:10.4064/aa-80-2-149-163.
16. Hans Rademacher, *On the Phragmén–Lindelöf theorem and some applications*, Math. Z. **72** (1959), no. 1, 192–204, doi:10.1007/BF01162949.
17. John Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), no. 1, 64–94, doi:10.1215/ijm/1255631807.
18. Michael Rubinstein, *An outline of the shortened proof of the Riemann Hypothesis*, 2026, Version 1.5, November 27, 2026, https://www.math.uwaterloo.ca/~mrubinst/alpoge_claude_grh/rh-outline.pdf.
19. Luke Sernau, *grh-lean*, https://github.com/lsernau/grh-lean, 2026, Lean 4 proof, compact edition, commit `72fead10`.
20. Jean-Pierre Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer, New York, 1977, doi:10.1007/978-1-4684-9458-7.
21. ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer, New York, 1979, doi:10.1007/978-1-4757-5673-9.
22. Harold M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. **23** (1974), 135–152, doi:10.1007/BF01405166.
23. Sergei A. Stepanov, *On the number of points of a hyperelliptic curve over a finite prime field*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1171–1181.
24. Daichi Tanaka, *Explicit construction of Maass wave forms and their Petersson inner products*, 2026, Preprint, arXiv:2601.21588v3.
25. The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, 2026, Records 3.3.148.1 and 2.2.37.1, and the totally real cubic fields of discriminant below 148, read November 28, 2026.
26. The mathlib Community, *The Lean mathematical library*, Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, New York, 2020, doi:10.1145/3372885.3373824, pp. 367–381.
27. Jesse Thorner and Asif Zaman, *A unified and improved Chebotarev density theorem*, Algebra Number Theory **13** (2019), no. 5, 1039–1068, doi:10.2140/ant.2019.13.1039.
28. Andrew Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), no. 3, 493–540, doi:10.2307/1971468.

Toronto, Canada
Email address: `manvirjaswal@icloud.com`
URL: `https://manvirjaswal.github.io`