

Unconditional implications of the Quasi-Riemann Hypothesis

Written by GPT 6 Astra

9 October 2026

Abstract

This record identifies published conclusions formerly obtained under RH or GRH whose proofs require only a fixed zero-free half-plane for Dirichlet L -functions, with further applications of finite-order Hecke L -functions over $\mathbb{Q}(\sqrt{-3})$. The input is the 7/8 theorem stated in the recent OpenAI manuscript claiming to prove the quasi-Riemann Hypothesis. We give the uniform analytic deductions explicitly and distinguish them from previously established algebraic and combinatorial results used in the proofs. An accompanying audit records the source verification and rejected candidates. No theorem about all number-field or automorphic L -functions is inferred from the Dirichlet statement; the pure cubic and cubic-nonresidue applications separately identify the precise fixed-field Hecke input.

Principal conclusions. The following guide distinguishes complete published conclusions from published orders of magnitude whose sharp GRH constants are not recovered. The proofs specify every imported algebraic and computational input.

Source	Conclusion recovered here
Montgomery–Vaughan	Character sums $\ll \sqrt{q} \log \log(3q)$; Theorem 2.1.
Granville–Soundararajan	Uniform cancellation when $\log x / \log \log q \rightarrow \infty$; Theorem 3.1.
Klurman–Mangerel–Teräväinen	All four published uniform short-progression conclusions for bounded multiplicative functions, including the hybrid short-interval theorem, with the stated typicality conditions; and $\mathcal{L}_3(q) \ll_\delta q^{2+\delta}$ for every modulus; Theorem 4.1 and Corollary 4.2.
Walsh	The complete linear Fourier-cancellation conclusion for Möbius and Liouville in intervals with $\log H / \log \log X \rightarrow \infty$; Theorem 5.1.
Green–Tao	The full published power-saving improvement for Möbius correlations with polynomial nilsequences, $O_{m,d}(Q^{C_{m,d}}(1 + \ F\ _{\text{Lip}})N^{-C_{m,d}})$, with $C_{m,d} > 0$ and effective constants; Theorem 6.1.
Mangerel	Quadratic Gauss-sum rigidity from approximate prime dilations up to N^c , for every fixed $c > 0$, with the full published sparse-prime allowance; Theorem 7.1.
Sofos; Montgomery	Infinitely many primes with both the first prime nonresidue and the next gap $\gg \log p \log \log p$; the published Paley clique lower order follows from the same argument; Theorem 8.1 and Corollary 8.2.
Mourtada–Murty	Both quadratic Euler–Kronecker extreme-value bounds, with leading terms $\log \log x + \log \log \log x$ and $\gg \sqrt{x}$ prime conductors below x for each sign; Theorem 9.1.
Badzyan; Ford–Luca–Moree	The full all-conductor bound $ \gamma_{\mathbb{Q}(\zeta_m)} \ll \log m \log \log(3m)$ and the published GRH error for the second coefficient in counting n with $q \nmid \varphi(n)$; Theorem 10.1 and Corollary 10.3.
Hough	Exact maximum bias for products of two primes, $(\log \log \log x) / \log \log x$; Theorem 11.1.
Littlewood	Two-sided $L(1, \chi)$ bounds and the orders of magnitude for ζ , $1/\zeta$, and ζ'/ζ on the line 1.
Darbar–David–Lalín–Lumley	Both extreme-value distribution formulas for cubic $L(1, \chi)$, throughout the full published GRH ranges with endpoint constant -37 ; Theorem 13.1.
Granville–Soundararajan	Both quadratic $L(1, \chi_d)$ tail asymptotics with error $O(A^{-1} + t^{-1})$, throughout the full published larger range with endpoint constant -20 ; Theorem 14.1.
Hoffstein–Lockhart	Effective bounds $L(1, \text{Ad } f)^{-1}$, $ \rho_f(1) ^2 \ll \log(1 + \lambda N)$ for every Maass newform, including the dihedral case; Theorem 15.1.
Boyd–Kisilevsky	Effective growth of the imaginary quadratic class-group exponent; Theorem 16.2.
Ellenberg–Venkatesh	The exact GRH exponents for torsion in every quadratic and every cubic ideal class group, with effective constants and no exceptional fields, and the specified further families in every fixed degree; Theorem 17.1 and Corollary 17.3.
Lamzouri	The full sharper odd-class-number average $\frac{15}{4}H^2 / \log H + O(H^2(\log \log H)^3 / (\log H)^2)$; Theorem 18.1.
Louboutin	Effective exponent growth in the specified family of simplest cyclic cubic fields; Theorem 24.2.
Daileda	The class-number bound $h_F \ll \sqrt{D_F} \ell(D_F) / \log D_F$ for all pure cubic fields; Theorem 25.2.

Pollack	The exact limiting mean of the least completely split prime in cyclic fields of every fixed odd prime degree; Theorem 26.1.
Elsenhans–Klüners–Nicolae; Euler–Kani	Complete 1046-field classification for exponent dividing 8, and the exact 65 idoneal integers; Theorems 19.3 and 19.5.
Chang–Kwon; Miyada	Complete lists of 489 imaginary abelian fields, and 301 multiquadratic fields, with one class per genus.
Ahn–Kwon	Exactly 650 imaginary multiquadratic fields with class-group exponent dividing 2, with independently verified finite computations; Theorem 21.1.
Mollin; Louboutin	Exactly 107 real quadratic fields of extended Richaud–Degert type with ordinary class number two, and exactly 43 with class number one, using the same fresh complete finite computation; Theorem 22.1 and Corollary 22.4.
Louboutin	The complete 19-value exceptional-case classification for $\omega(d + x^2) \leq 2$, and hence the full 42-value list for odd d ; Theorem 23.1.
Bourdon–Pollack	CM torsion in odd degree has upper order $(d \log \log d)^{2/3}$; Theorem 27.1.
Clark–Genao–Pollack–Saia	The exact typical degrees $d_{\text{CM}}(X_0(N)) = (\log N)^{(\log 2)/2 + o(1)}$ and $d_{\text{CM}}(X_1(N)) = N(\log N)^{(\log 2)/2 + o(1)}$; the least nonsquare which is a square modulo N has typical size $(\log N)^{\log 2 + o(1)}$; Theorem 28.1 and Corollary 28.2.
Banwait	An unconditional algorithm bounding every prime-degree isogeny over each eligible quadratic field; Theorem 29.1.
Rasmussen–Tamagawa	The full uniform finiteness theorem for all dimensions and all fixed odd degrees; Theorem 30.1.
Schütt; Elkies–Schütt	Finitely many rational CM newforms per weight up to the specified twists; every rational weight-3 newform has a singular K3 realization over $\mathbb{Q}$.
Kani	The exact 21 exceptional types of non-CM elliptic products which are not genus-2 Jacobians; Theorem 32.2.
Pasten; Wei	The all-Heegner-point height error of order $\log \log d_K$ and the root-discriminant height bound for adjacent CM types; Theorems 33.1 and 34.1.
Binyamini–Kowalski	Fully effective André–Oort bounds and enumeration for arbitrary subvarieties of $Y(1)^n$; Theorem 35.2; effective polynomial bounds in Theorem 35.3.
Edixhoven–Richard	The André–Oort statement for reductions of full CM orbits modulo any prime; Theorem 36.1.
Habegger	Weakly bounded height on every nonspecial modular-plane curve with unequal projection degrees; Theorem 37.1.
Balestrieri–Johnson–Newton	Effective computation of the Brauer–Manin set for every singular K3 surface and every geometric Kummer surface of a product of CM elliptic curves; Theorem 38.1.
Khayutin	Joint equidistribution of CM packets and Galois orbits in the published two-fixed-split-prime setting, including bounded order conductors; Theorem 39.1.
Duke–Schulze-Pillot; Duke	Effective primitive-spinor representation thresholds, and effective $n > CD^{337}$ squarefree representation; Theorems 41.1 and 41.2.
Kane; Elkies–Ono–Yang	Effective CM lifting to every supersingular class, with multiplicity bounds and the polynomial congruence; Theorem 42.1.
Campagna	Effective enumeration of singular S_ℓ -units for $S_\ell = \{p : p \equiv 1 \pmod{3}\} \cup \{\ell\}$, $\ell \geq 5$; Theorem 40.1.
Achter–Howe; Arul et al.	The published GRH orders for split abelian surfaces and for pairs of D_4 -curves with isogenous Jacobians.

Jeřábek; Adleman–Manders–Miller Miller	The stated total-search complexity memberships for factoring, and deterministic extraction of fixed-degree roots in prime fields. Deterministic polynomial-time equivalence of factoring, φ , λ , and λ' , with one supplied value; the period-oracle equivalence and graph-recognition conclusions; Theorem 46.1.
Gao; Rónyai	Polynomial-time balance decomposition and proper factoring of squarefree completely split polynomials of even degree; Theorem 48.1.
Rónyai; Ivanyos et al.	Deterministic proper factoring when three divides the degree of a completely split polynomial; Theorem 49.1.
Pollack–Schorn	The exact expected bit complexity for three-square representations without a supplied factorization; Theorem 50.1.
Balaji–Nosan– Shirmohammadi–Worrell	Square-root circuit identity testing in coRP; Theorem 51.1.
Balaji–Perifel– Shirmohammadi–Worrell	General cyclotomic identity testing in BPP and the deterministic restricted diagonal theorem; Theorems 52.1 and 52.2.
Castel; Kutas	A randomized polynomial-time isotropic-vector algorithm in dimension at least five without a factorization oracle; Theorem 53.1.
Wesolowski	Polynomial-time prime sampling for every primitive positive definite integral quadratic form of rank at least two, with the published interval and input-size dependence; Theorem 54.1.
Herlédan Le Merdy–Wesolowski	The full worst-case to average-case reduction to supersingular maximal orders for every prime $p > 3$, including the formerly conditional $p \equiv 1 \pmod{8}$ case; Theorem 55.1.

Contents

1	The analytic input and uniform consequences	7
2	The Montgomery–Vaughan character-sum bound	10
3	Cancellation in the Granville–Soundararajan range	14
4	Multiplicative functions in short arithmetic progressions	15
5	Fourier uniformity in intervals longer than every fixed logarithmic power	20
6	Power decay in Möbius correlations with polynomial nilsequences	24
7	Rigidity from approximate quadratic Gauss-sum symmetries	28
8	Large first prime nonresidues and gaps between them	31
9	Extreme Euler–Kronecker constants of quadratic fields	33
10	Cyclotomic Euler–Kronecker constants and a second asymptotic coefficient	35
11	The maximum quadratic-character bias for products of two primes	39
12	Littlewood’s orders of magnitude on the line $\Re s = 1$	41
13	The asymmetric tails of cubic L-values	43
14	The larger quadratic L-value tail range	49
15	The first Fourier coefficient of a Maass newform	52
16	The exponent of imaginary quadratic class groups	54
17	Pointwise torsion bounds for every quadratic and cubic class group	56
17.1	Further field families with the same published torsion exponent	59
18	The sharper average for odd imaginary-quadratic class numbers	61
18.1	Complex moments over prime discriminants	62
18.2	From the moments to the class-number count	64
19	Small class-group exponents and Euler’s idoneal numbers	66
19.1	The eighteen exceptions to $xy + yz + zx = d$	68
20	The complete abelian one-class-per-genus classifications	69
21	The complete multiquadratic exponent-two classification	70
22	The complete Richaud–Degert class-number-two classification	73
22.1	The complete class-number-one list in the same family	76
23	A complete polynomial-factorization classification	77
24	Class-group exponents of simplest cyclic cubic fields	79
25	Daileda’s class-number bound for pure cubic fields	81
26	The mean least completely split prime in cyclic fields	83
27	The upper order of CM torsion in odd degrees	85
28	The typical least degree of a CM point on a modular curve	86

29	Effective bounds for prime-degree isogenies over quadratic fields	91
30	Uniform Rasmussen–Tamagawa finiteness in every odd degree	93
31	Rational CM newforms of every fixed weight	96
32	Geometric consequences of the complete exponent-two classification	97
32.1	The Elkies–Schütt realization theorem	97
32.2	Products of non-CM elliptic curves that are not Jacobians	98
33	Pasten’s height estimate for all Heegner points	99
34	Wei’s height bound for adjacent CM types	100
34.1	Individual heights for every abelian CM field	102
35	Fully effective André–Oort for powers of the modular curve	103
35.1	Effectivity of Binyamini’s polynomial bounds	105
36	Edixhoven–Richard’s André–Oort theorem modulo a prime	106
37	Weakly bounded height on curves in the modular plane	109
38	Effective Brauer–Manin sets for singular and CM Kummer surfaces	111
39	Joint equidistribution of CM points	114
40	Effective bounds for Campagna’s singular S -units	116
41	Effective representation by positive ternary quadratic forms	118
42	Effective CM lifting to every supersingular elliptic curve	121
43	The Achter–Howe bounds for split abelian surfaces	124
43.1	Class numbers and the arithmetic estimate	124
43.2	Upper bound for surfaces	126
43.3	Lower bound for surfaces	127
44	Isogenous genus-two curves with a dihedral action	128
45	Integer factoring in parity and pigeonhole search classes	129
46	Miller’s equivalences between factoring and arithmetic functions	131
47	Deterministic extraction of roots	133
48	Deterministic splitting in even degree and Gao’s balance test	135
49	Rónyai’s splitting theorem when three divides the number of factors	137
50	The Pollack–Schorn algorithm for three squares	140
51	Randomized identity testing for square-root circuits	142
52	Two cyclotomic identity-testing theorems	145
53	Castel’s polynomial-time isotropic-vector algorithm	148
54	Finding prime values of positive definite quadratic forms	151
55	Worst-case to average-case reductions to supersingular maximal orders	154

1 The analytic input and uniform consequences

Throughout, $\log$ is the natural logarithm, Λ is the von Mangoldt function, and sums indexed by $n \leq x$ run over positive integers unless an interval or a different index set is explicitly specified. Put

$$\vartheta = \frac{7}{8}, \quad \delta = 1 - \vartheta = \frac{1}{8}, \quad \ell(x) = \log \log(e^e x) \quad (x \geq 1).$$

The harmless modification in ℓ makes bounds meaningful also for small arguments. All constants below are absolute and effective unless a dependence is specified.

Theorem 1.1 (Imported zero-free theorem). *For every Dirichlet character χ modulo a positive integer q , its Dirichlet L -function has no zero in $\Re s > 7/8$. The pole at $s = 1$ for a principal character is excepted.*

This is the Dirichlet part of [58, Theorem 1.1]. We use it as a cited unconditional theorem. We do not claim to have supplied a new proof of it. The companion [59] gives the weaker boundary $11/12$; that boundary would suffice for all qualitative conclusions in this record, with larger fixed logarithmic exponents in the intermediate estimates.

For a primitive nonprincipal character, the functional equation relates $L(s, \chi)$ to $L(1 - s, \bar{\chi})$. Since Theorem 1.1 also applies to $\bar{\chi}$, every nontrivial zero $\rho = \beta + i\gamma$ satisfies

$$\delta \leq \beta \leq \vartheta. \tag{1}$$

The same assertion holds for the nontrivial zeros of ζ . Uniformity in q below is derived from this zero location and the ordinary explicit formula. It is not inferred from uniformity of the fixed-character estimates in the proof of [58].

Lemma 1.2 (Uniform prime sum). *For a primitive nonprincipal character χ modulo $q \geq 3$ and $x \geq 2$,*

$$\psi(x, \chi) := \sum_{n \leq x} \Lambda(n) \chi(n) \ll x^{7/8} \log^2(qx).$$

Also $\psi(x) = x + O(x^{7/8} \log^2(2x))$.

Proof. We use the classical uniform truncated explicit formula and zero count [60, Chapters 16 and 19]; these analytic identities and bounds are unconditional. At a half-integer x , choose a permissible height $T \asymp x$. For a primitive nonprincipal character the formula is

$$\psi(x, \chi) = - \sum_{|\gamma| \leq T} \frac{x^\rho}{\rho} + O(\log^2(qx)),$$

where, after (1), the terms from trivial zeros and the logarithmic derivative at zero are included in the error. To justify this last uniformity explicitly, subtract the completed logarithmic derivatives at 1 and 2. The zero contribution has terms $((1 - \rho)(2 - \rho))^{-1}$, whose absolute sum is $O_\delta(\log(3q))$. The absolutely convergent Dirichlet series bounds $L'/L(2, \chi)$, and the gamma factors and functional equation then bound the finite Laurent coefficient at zero by $O_\delta(\log(3q))$.

The usual zero count is

$$N_\chi(U) := \#\{\rho : |\Im \rho| \leq U\} \ll (U + 1) \log(q(U + 2)),$$

with multiplicities. The zeros with $|\gamma| \leq 1$ contribute $O_\delta(\log(3q))$ to $\sum 1/|\rho|$; partial summation for the remaining zeros gives

$$\sum_{|\gamma| \leq T} \frac{1}{|\rho|} \ll_\delta \log^2(q(T+2)).$$

Now $|x^\rho| \leq x^{7/8}$ gives the assertion at half-integers. Moving an arbitrary x to a neighboring half-integer changes the sum by $O(\log(2x))$, which is absorbed. The argument for ζ is the same, with the residue x of its pole included. $\square$

Lemma 1.3 (A short logarithmic expansion). *For every primitive nonprincipal character modulo $q \geq 3$ and $y \geq 2$,*

$$\log L(1, \chi) = \sum_{n \leq y} \frac{\Lambda(n)\chi(n)}{n \log n} + O\left(\frac{y^{-1/8} \log^2(qy)}{\log y}\right). \quad (2)$$

The logarithm is the branch obtained by continuation of the Euler-product logarithm from the real interval $s > 1$.

Proof. For $\Re s > 1$ the Euler product gives

$$\log L(s, \chi) = \sum_{n \geq 2} \frac{\Lambda(n)\chi(n)}{n^s \log n}.$$

Lemma 1.2 and summation by parts give locally uniform convergence of the series on $\Re s > 7/8$. Its exponential agrees with L initially on $\Re s > 1$, hence throughout this zero-free half-plane by analytic continuation. At $s = 1$, the tail is

$$-\frac{\psi(y, \chi)}{y \log y} + \int_y^\infty \psi(u, \chi) \frac{\log u + 1}{u^2 (\log u)^2} du.$$

Its absolute value has the asserted bound. For example, put $u = yv$, use $\log(qyv) \leq \log(qy) + \log v$ and $\log(yv) \geq \log y$, and integrate $v^{-9/8}(1 + \log v)^2$. This also proves the claimed uniformity and effectivity. $\square$

Theorem 1.4 (Littlewood bounds in order of magnitude). *For all primitive nonprincipal Dirichlet characters χ modulo q ,*

$$\frac{c}{\ell(q)} \leq |L(1, \chi)| \leq C\ell(q)$$

for fixed effective $c, C > 0$.

Proof. In Lemma 1.3 take $y = (\log(3q))^{24}$. The error is bounded absolutely, since $y^{-1/8} = (\log(3q))^{-3}$ and $\log(qy) \ll \log(3q)$. The elementary Mertens estimate gives

$$\sum_{n \leq y} \frac{\Lambda(n)}{n \log n} = \log \log y + O(1).$$

Consequently $|\Re \log L(1, \chi)| \leq \log \log y + O(1)$. Exponentiating gives $c/\log y \leq |L(1, \chi)| \leq C \log y$; $\log y = 24 \log \log(3q) \asymp \ell(q)$ proves the result. $\square$

These are the previously GRH-conditional orders of magnitude of Littlewood's bounds; see [61] and [62, (1.1)]. The sharper leading constants obtained under GRH are not asserted here. For real primitive nonprincipal characters, $L(1, \chi) > 0$, so the absolute values may be omitted. The effective imaginary-quadratic class-number consequence below is already explicitly announced in [59, Introduction]; its proof is included to establish the common input of the later applications.

Corollary 1.5 (Quadratic class numbers). *For a negative fundamental discriminant D ,*

$$\frac{c\sqrt{|D|}}{\ell(|D|)} \leq h(D) \leq C\sqrt{|D|\ell(|D|)}.$$

For every negative quadratic-order discriminant Δ ,

$$h(\Delta) \ll \sqrt{|\Delta|\ell(|\Delta|)^2}, \quad H(\Delta) \ll \sqrt{|\Delta|\ell(|\Delta|)^3}, \quad (3)$$

where $h(\Delta)$ is the proper ideal class number and $H(f^2D) = \sum_{d|f} h(d^2D)$.

Proof. The analytic class-number formula is $h(D) = w_D \sqrt{|D|} L(1, \chi_D) / (2\pi)$, with $w_D \in \{2, 4, 6\}$. Apply Theorem 1.4. If $\Delta = f^2D$, the order class-number formula gives

$$h(f^2D) = \frac{fh(D)}{[\mathcal{O}_D^\times : \mathcal{O}_{f^2D}^\times]} \prod_{p|f} \left(1 - \frac{\chi_D(p)}{p}\right) \leq h(D)\sigma(f).$$

Here $\sigma(f) = \sum_{d|f} d \ll f\ell(f)$. Thus $h(f^2D) \ll f\sqrt{|D|\ell(f^2|D|)^2}$. Summing this bound over $d | f$ gives

$$H(f^2D) \ll \sqrt{|D|\ell(f^2|D|)^2}\sigma(f) \ll f\sqrt{|D|\ell(f^2|D|)^3}.$$

The unit index is retained; dropping it as an equality would be incorrect for certain nonmaximal orders in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. $\square$

The upper bounds (3) are precisely the GRH-conditional orders in [65, Lemma 4.4]. Their uniformity in both D and f is needed in the geometric applications below.

Lemma 1.6 (Small character witnesses). *There is an effective absolute constant C_0 such that, for every nonprincipal character χ modulo $q \geq 3$, there is a prime p with*

$$p \leq C_0(\log(3q))^8, \quad p \nmid q, \quad \chi(p) \neq 1.$$

In particular the primes up to this bound which are coprime to q generate $(\mathbb{Z}/q\mathbb{Z})^\times$.

Proof. First let χ be primitive nonprincipal, with conductor f . Perron's formula with kernel $1/(s(s+1))$, followed by a contour shift, gives

$$\sum_{n \leq x} \Lambda(n) \chi(n) (1 - n/x) = - \sum_{\rho} \frac{x^\rho}{\rho(\rho+1)} + O(\log(fx)). \quad (4)$$

For completeness, the integral on the initial line $\Re s = 2$ is $-(2\pi i)^{-1} \int (L'/L)(s, \chi) x^s / (s(s+1)) ds$. The residues at the nontrivial zeros give the displayed sum. The poles of the kernel at 0, -1 , and coincident trivial zeros in the relevant parity, give $O(\log(fx))$; the uniform finite Laurent coefficients are bounded by the logarithmic-derivative argument in the proof of Lemma 1.2. The further trivial-zero residues are absolutely convergent and $O(1 + \log x)$, and the remaining integrals tend to zero along admissible heights. This is also the usual integrated explicit formula of [60, Chapter 19]. By (1) and the zero count,

$$\sum_{\rho} \frac{1}{|\rho(\rho+1)|} \ll \log(3f).$$

Thus the left side of (4) is $O(x^{7/8} \log(3f) + \log(fx))$.

If χ modulo q is induced from χ^* of conductor $f \mid q$, the omitted prime powers contribute at most

$$\sum_{p \mid q} \sum_{p^a \leq x} \log p \leq \omega(q) \log x \ll \log(3q) \log x.$$

Suppose now that $\chi(p) = 1$ for every $p \leq x$ coprime to q . The smoothed sum would equal

$$\sum_{n \leq x} \Lambda(n)(1 - n/x) - \sum_{\substack{p^a \leq x \\ p \mid q}} \log p(1 - p^a/x).$$

The first term is $x/2 + O(x^{7/8} \log^2(2x))$ by Lemma 1.2 and integration; the second is $O(\log(3q) \log x)$. Compare this with (4) and take $x = C_0(\log(3q))^8$. The ratio of the character-zero bound to x is $O(C_0^{-1/8})$; the other errors are $o(x)$ uniformly as $q \rightarrow \infty$. Choose C_0 sufficiently large, then enlarge it effectively for the finitely many remaining moduli. This contradicts the main term $x/2$.

Finally, if the indicated primes generated a proper subgroup of the finite abelian unit group, a nontrivial character of the quotient would be 1 on every one of them. Lifting it gives a nonprincipal Dirichlet character, contradicting the assertion just proved. $\square$

The lemma strengthens the conservative logarithmic exponent used in [58, Corollary 1.2]. We use it as an intermediate estimate, without claiming that the exact GRH exponent 2 in Ankeny's theorem has been recovered.

2 The Montgomery–Vaughan character-sum bound

The following is the classical GRH-conditional order of magnitude of Montgomery and Vaughan [69]; see also [68, (1.2)]. The proof below replaces the GRH input and keeps this order of magnitude.

Theorem 2.1. *For every nonprincipal Dirichlet character χ modulo $q \geq 3$ and every real $u < v$,*

$$\left| \sum_{u < n \leq v} \chi(n) \right| \ll \sqrt{q} \ell(q),$$

with an effective absolute constant.

Proof. We first prove the assertion for primitive characters and sums beginning at 1. Write $e(t) = \exp(2\pi it)$.

Let $\vartheta = 7/8$ and $\delta = 1 - \vartheta = 1/8$. We use the zero-free theorem for every Dirichlet L -function, including all products of the characters below. All constants in this argument are effective and absolute.

The uniform explicit formula and partial summation imply that, for every nonprincipal Dirichlet character η modulo Q and $t \geq 2$,

$$\sum_{p \leq t} \eta(p) \ll t^\vartheta \log^2(Qt). \quad (\text{P})$$

For primitive characters this follows from the zero bound $\beta \leq \vartheta$; prime powers cost $O(\sqrt{t} \log^2 t)$, which is absorbed since $\vartheta > 1/2$. If η is imprimitive, replacing it by its primitive inducing character removes at most the primes dividing Q , a contribution at most $\omega(Q) \ll \log(2Q)$, also absorbed in (P). The modest logarithmic exponent in (P) is sufficient; no optimized version is needed.

We first record a consequence without an additive phase. Let $\mathcal{S}(y)$ denote the positive integers whose prime factors are all at most y , including 1. Set $P^+(1) = 1$. For $2 \leq y \leq X$, write each

integer $n \leq X$ outside $\mathcal{S}(y)$ uniquely as $n = pm$, where $p = P^+(n)$ is its largest prime factor. Then $m \leq X/y$ and $p \geq P^+(m)$. Thus

$$\sum_{\substack{n \leq X \\ n \notin \mathcal{S}(y)}} \eta(n) = \sum_{m \leq X/y} \eta(m) \sum_{\substack{y < p \leq X/m \\ p \geq P^+(m)}} \eta(p).$$

The inner sum is a difference of two prime sums covered by (P), including the possible lower-endpoint prime. Consequently

$$\left| \sum_{\substack{n \leq X \\ n \notin \mathcal{S}(y)}} \eta(n) \right| \ll \log^2(QX) X^\vartheta \sum_{m \leq X/y} m^{-\vartheta} \ll X y^{-\delta} \log^2(QX). \quad (\text{U})$$

If $X < y$, the sum is zero. Partial summation therefore gives, uniformly for $1 \leq Z \leq q$ and $Q \leq q(\log q)^4$,

$$\sum_{\substack{n \leq Z \\ n \notin \mathcal{S}(y)}} \frac{\eta(n)}{n} \ll y^{-\delta} (\log q)^3. \quad (\text{H})$$

Here and below it suffices to take q larger than an absolute effective threshold. Explicitly, if $A(t)$ denotes the sum in (U), its weighted version is $A(Z)/Z + \int_1^Z A(t)t^{-2} dt$; inserting (U) and $\log(Qt) \ll \log q$ proves (H).

Put $L = \log q$ and

$$s = L^4, \quad S = L^8, \quad y = L^{64}.$$

We may assume q is large enough that $S < q$, $y < q$, and $s < q$. All smaller conductors are absorbed into the absolute constant by the classical Polya–Vinogradov inequality (or the trivial bound); this is an effective finite range.

We next show that, for every primitive nonprincipal $\chi \pmod{q}$, every $r \leq s$, every $(b, r) = 1$, and every $1 \leq Z \leq q$,

$$\sum_{n \leq Z} \frac{\chi(n) e(bn/r)}{n} \ll \log \log q. \quad (\text{R})$$

Split the sum according to $d = (n, r)$ and put $v = r/d$, $n = dm$. The condition $(n, r) = d$ is exactly $(m, v) = 1$. Because every prime factor of d is at most $r \leq s < y$, the integer n is y -smooth if and only if m is y -smooth. Define $\tau(\psi) = \sum_{a \bmod v} \psi(a) e(a/v)$. On the reduced residue classes modulo v , finite character orthogonality gives

$$e(bm/v) = \frac{1}{\varphi(v)} \sum_{\psi \bmod v} \tau(\bar{\psi}) \psi(b) \psi(m), \quad (m, v) = 1.$$

Thus the difference between the left side of (R) and its restriction to $\mathcal{S}(y)$ is

$$\sum_{d|r} \frac{\chi(d)}{d} \frac{1}{\varphi(v)} \sum_{\psi \bmod v} \tau(\bar{\psi}) \psi(b) \sum_{\substack{m \leq Z/d \\ m \notin \mathcal{S}(y)}} \frac{(\chi\psi)(m)}{m}, \quad v = r/d.$$

Every product $\chi\psi$ is nonprincipal. Indeed, if it were principal on the units modulo $\text{lcm}(q, v)$, the primitive inducing characters of χ and $\bar{\psi}$ would coincide, forcing $q \mid v$, whereas $v \leq r < q$. Its

modulus may be taken to be $qv \leq qL^4$, so (H) applies. The standard Gauss-sum bound $|\tau(\psi)| \leq \sqrt{v}$, valid also for imprimitive characters, yields the error bound

$$\ll y^{-1/8} L^3 \sum_{d|r} \frac{\sqrt{r/d}}{d} \leq y^{-1/8} L^3 \sqrt{r} \sum_{d \geq 1} d^{-3/2} \ll L^{-8} L^3 L^2 = L^{-3}.$$

Notice that the divisor sum actually converges; a crude harmonic divisor bound is unnecessary. The restricted sum has absolute value at most

$$\sum_{n \in \mathcal{S}(y)} \frac{1}{n} = \prod_{p \leq y} (1 - p^{-1})^{-1} \ll \log y \ll \log \log q$$

by Mertens' product estimate. This proves (R).

It remains to reduce an arbitrary phase to (R). We use the following unconditional Montgomery–Vaughan bound, recorded as Lemma 4.2 in Granville–Soundararajan: if f is completely multiplicative with $|f(n)| \leq 1$, $|\alpha - b/r| \leq r^{-2}$ and $(b, r) = 1$, then, for $2 \leq R \leq r$ and $T \geq Rr$,

$$\left| \sum_{Rr \leq n \leq T} \frac{f(n)e(n\alpha)}{n} \right| \ll \log \log(3T) + \frac{(\log R)^{3/2}}{\sqrt{R}} \log(3T). \quad (\text{MV})$$

Its implied constant is absolute.

Choose a reduced rational approximation b/r with $r \leq S$ and

$$|\alpha - b/r| \leq \frac{1}{rS}.$$

Integer roundings in Dirichlet approximation can be avoided by replacing S by $\lceil S \rceil$ throughout; this changes only absolute constants and none of the following estimates.

If $s < r \leq S$, split the harmonic exponential sum at r^2 . The part $n \leq r^2$ is $O(\log(2r)) = O(\log L)$. Apply (MV) to the remaining part with $R = r$. Since $r > L^4$ and $\log r \ll \log L$, its bound is

$$O\left(\log L + \frac{(\log r)^{3/2}}{\sqrt{r}} L\right) = O(\log L).$$

If $r^2 > q$, the initial segment is the entire sum and the same bound holds (for the assumed large q one has $r^2 < q$ anyway).

Now suppose $r \leq s$, and write $\beta = \alpha - b/r$ and

$$N = \min\{q, (r|\beta|)^{-1}\},$$

with the second quantity infinite when $\beta = 0$. For $n \leq N$,

$$\sum_{n \leq N} \frac{|e(n\alpha) - e(bn/r)|}{n} \ll |\beta|N \leq r^{-1} \leq 1. \quad (\text{A})$$

If $N = q$, (R) and (A) finish the proof. Otherwise $N = (r|\beta|)^{-1} \geq S$.

For completeness, a distinct second rational approximation can be chosen without a boundary ambiguity. Let $Q_1 = \lceil 2N \rceil$. Dirichlet's theorem gives a reduced b_1/r_1 with $r_1 \leq Q_1$ and $|\alpha - b_1/r_1| \leq 1/(r_1 Q_1)$. This rational differs from b/r , because the error of b/r is exactly $1/(rN) > 1/(rQ_1)$. Therefore

$$\frac{1}{rr_1} \leq \left| \frac{b}{r} - \frac{b_1}{r_1} \right| \leq \frac{1}{rN} + \frac{1}{r_1 Q_1},$$

which implies $r_1 \geq N - Nr/Q_1 \geq N - r/2 \geq N/2$. Also $r_1 \leq Q_1 \leq 3N$, and the new approximation satisfies $|\alpha - b_1/r_1| \leq r_1^{-2}$.

Put $R = L^5$. For large q , $R \leq r_1$ because $r_1 \geq S/2 = L^8/2$. The interval $N < n \leq \min(q, Rr_1)$ contributes at most

$$\sum_{N < n \leq 3RN} \frac{1}{n} \ll \log(3R) \ll \log L.$$

If $q > Rr_1$, apply (MV) with the new approximation to the remaining interval. Its contribution is

$$\ll \log L + \frac{(\log R)^{3/2}}{\sqrt{R}} L \ll \log L.$$

Together with (A), this proves

$$\sum_{n \leq q} \frac{\chi(n)e(n\alpha)}{n} = \sum_{n \leq N} \frac{\chi(n)e(bn/r)}{n} + O(\log \log q) \ll \log \log q, \quad (\text{F})$$

uniformly for every real α .

Finally, Pólya's truncated Fourier expansion for a primitive nonprincipal character gives, uniformly for $0 \leq t \leq q$,

$$\sum_{n \leq t} \chi(n) = \frac{\tau(\chi)}{2\pi i} \sum_{1 \leq |h| \leq q} \frac{\bar{\chi}(h)}{h} (1 - e(-ht/q)) + O(\log(2q)).$$

At jump points the choice of endpoint convention changes the formula by at most one, absorbed in the error. Separate positive and negative h and use (F) for $\bar{\chi}$ at phases $0, t/q, -t/q$. Since $|\tau(\chi)| = \sqrt{q}$, we obtain

$$M(\chi) := \max_{1 \leq t \leq q} \left| \sum_{n \leq t} \chi(n) \right| \ll \sqrt{q} \log \log q.$$

Replacing $\log \log q$ by $\log \log(3q)$ gives a positive uniform expression for all $q \geq 3$.

It remains to treat imprimitive characters and arbitrary intervals. Let χ modulo q be induced by the primitive nonprincipal character χ^* modulo f , and put $R = \prod_{p|q, p \nmid f} p$. Inclusion–exclusion gives, for every $x \geq 0$,

$$\sum_{n \leq x} \chi(n) = \sum_{d|R} \mu(d) \chi^*(d) \sum_{m \leq x/d} \chi^*(m).$$

The inner sum is bounded by the primitive maximum, at every endpoint, by periodicity and the zero sum over a complete period. Moreover

$$\frac{2^{\omega(R)}}{\sqrt{R}} = \prod_{p|R} \frac{2}{\sqrt{p}} \leq \frac{4}{\sqrt{6}} < 2, \quad fR \mid q.$$

Indeed, only $p = 2, 3$ can make a factor exceed 1. Thus the imprimitive maximum is at most $2C\sqrt{q}\ell(q)$. Differences of two initial sums prove the assertion for intervals, including negative endpoints by periodicity. $\square$

What the proof changes. The direct alteration of [68, Lemma 5.1] would give an exponent $7/8 + 1/3 > 1$, and is insufficient. Here the unconditional Montgomery–Vaughan estimate reduces the problem to additive characters of denominator at most $(\log q)^4$. Smooth truncation on these rational phases then needs only prime sums without an additive phase. Neither the sharp GRH leading constants nor the refinements for characters of small odd order are asserted by this theorem.

3 Cancellation in the Granville–Soundararajan range

The first assertion of Granville–Soundararajan’s [49, Corollary A] states, under GRH, that a nonprincipal character sum is $o(x)$ whenever $q \rightarrow \infty$ and $\log x / \log \log q \rightarrow \infty$. This range is much shorter than the range in which the Pólya–Vinogradov estimate alone gives cancellation. We recover the whole qualitative assertion, by an argument using Halász’s theorem instead of the source’s sharper smooth-number approximation.

Theorem 3.1 (Granville–Soundararajan’s cancellation conclusion). *There is an effective absolute constant C such that, for every nonprincipal character χ modulo $q \geq 3$ and $3 \leq x \leq q$,*

$$\left| \sum_{n \leq x} \chi(n) \right| \leq Cx \frac{\log(2u)}{u}, \quad u = \max \left\{ 1, \frac{\log x}{\log \log(3q)} \right\}.$$

In particular, uniformly over nonprincipal characters,

$$\sum_{n \leq x} \chi(n) = o(x) \quad \text{if } q \rightarrow \infty, \quad \frac{\log x}{\log \log q} \rightarrow \infty.$$

The last statement permits $x > q$ as well.

Proof. We first extend the prime-sum bound to imprimitive characters. If χ is induced by the primitive nonprincipal character χ^* of conductor $f \mid q$, then

$$|\psi(v, \chi) - \psi(v, \chi^*)| \leq \sum_{p \mid q} \sum_{p^k \leq v} \log p \leq \omega(q) \log v \ll \log(3q) \log(2v).$$

Consequently Lemma 1.2 implies, uniformly for all these characters and $v \geq 2$,

$$\psi(v, \chi) \ll v^{7/8} \log^2(qv). \quad (5)$$

Put $L = \log(3q)$ and $y = L^{32}$. For $0 \leq \sigma \leq 1$, $|t| \leq L$, and $s = 1 + \sigma + it$, summation by parts in the Euler-product logarithm gives

$$\log L(s, \chi) = \sum_{n \leq y} \frac{\Lambda(n) \chi(n)}{n^s \log n} + O\left((1 + |t|) y^{-1/8} \log^2(qy)\right). \quad (6)$$

Here the logarithm is continued from $\Re s > 1$; for $\sigma = 0$ the identity follows by locally uniform convergence. For precision, the omitted tail equals

$$-\frac{\psi(y, \chi)}{y^s \log y} + \int_y^\infty \psi(v, \chi) v^{-s-1} \left(\frac{s}{\log v} + \frac{1}{(\log v)^2} \right) dv.$$

Using (5), its modulus is bounded by the error in (6), uniformly in the stated rectangle. The integral estimate follows upon writing $v = yw$ and integrating $w^{-9/8}(1 + \log w)^2$. Since $\log(qy) \ll L$ and $y^{-1/8} = L^{-4}$, that error is $O(L^{-1})$. The elementary Mertens estimate therefore gives

$$\log |L(1 + \sigma + it, \chi)| \leq \sum_{n \leq y} \frac{\Lambda(n)}{n \log n} + O(1) = \log \log y + O(1).$$

Together with the absolutely convergent Euler product for $\sigma > 0$, this proves

$$|L(1 + \sigma + it, \chi)| \ll \min\{\log y, \sigma^{-1}\} \quad (0 < \sigma \leq 1, |t| \leq L). \quad (7)$$

We use the following precise unconditional form of Halász's theorem: [50, Theorem 1.1, $\kappa = 1$]. If a multiplicative function a has Dirichlet series $F(s)$ whose logarithmic derivative has coefficients $\Lambda_a(n)$ satisfying $|\Lambda_a(n)| \leq \Lambda(n)$, then, for x sufficiently large,

$$\left| \sum_{n \leq x} a(n) \right| \ll \frac{x}{\log x} \int_{1/\log x}^1 \left(\max_{|t| \leq \log x} \left| \frac{F(1 + \sigma + it)}{1 + \sigma + it} \right| \right) \frac{d\sigma}{\sigma} + \frac{x \log \log x}{\log x}.$$

The absolute implied constant is effective. For $a(n) = \chi(n)$, one has $F = L(\cdot, \chi)$ and $\Lambda_a(n) = \chi(n)\Lambda(n)$, so its hypotheses hold, including for imprimitive characters.

Suppose first that $x \geq y$, so $u = \log x / \log L \geq 32$. Set $a = \log y = 32 \log L$ and $v = \log x$, so $v \geq a > 1$. Since $\log x \leq \log q < L$, estimate (7) applies throughout Halász's integral. Moreover $|1 + \sigma + it| \geq 1$. Splitting at $\sigma = 1/a$ yields

$$\int_{1/v}^1 \min\{a, \sigma^{-1}\} \frac{d\sigma}{\sigma} = a \log(v/a) + a - 1.$$

It follows that

$$\frac{1}{x} \left| \sum_{n \leq x} \chi(n) \right| \ll \frac{32}{u} \left(1 + \log \frac{u}{32} \right) + \frac{\log \log x}{\log x} \ll \frac{\log(2u)}{u}.$$

For the last inequality, write $\log \log x = \log u + \log \log L$ and use $\log L \geq \log \log 9 > 0$; both $1/\log L$ and $|\log \log L|/\log L$ are bounded in this range. When $x < y$, one has $1 \leq u < 32$, and the trivial bound $|\sum_{n \leq x} \chi(n)| \leq x$ proves the claim after increasing the absolute constant. This also absorbs the bounded values of x omitted from the stated form of Halász's theorem.

The asserted limit for $x \leq q$ follows since $\log(2u)/u \rightarrow 0$. For $x \geq q$, periodicity and the vanishing of one complete nonprincipal character sum give $\sum_{n \leq x} \chi(n) = \sum_{n \leq r} \chi(n)$ for some $0 \leq r < q$. Theorem 2.1 bounds the last expression by $O(\sqrt{q} \ell(q)) = o(q)$, which is also $o(x)$. $\square$

Only the cancellation conclusion of [49, Corollary A] is claimed here. The quantitative decay proved above is weaker than the paper's GRH smooth-number estimates. Its unconditional examples with large character sums at lengths $(\log q)^A$, for each fixed A , already show why the condition $u \rightarrow \infty$ is necessary for this uniform qualitative conclusion.

4 Multiplicative functions in short arithmetic progressions

The following removes the GRH qualifications from Corollary 1.1 and Theorems 1.2, 1.4, and 1.5 of Klurman–Mangerel–Teräväinen [20]. These are estimates for arbitrary bounded multiplicative functions, with a single character correction. The conditions concerning typical moduli are part of the published statements and are retained.

Write $\mathbb{U} = \{z \in \mathbb{C} : |z| \leq 1\}$ and set

$$\mathbb{D}_q(f, g; x)^2 = \sum_{\substack{p \leq x \\ p \nmid q}} \frac{1 - \operatorname{Re}(f(p)\overline{g(p)})}{p}.$$

An integer q is y -typical if, for every real $z \geq y$,

$$\#\{p \leq z : p \mid q\} \leq \frac{1}{100} \pi(z).$$

For a character $\chi \pmod{q}$ and $(a, q) = 1$, put

$$E_f(x; q, a; \chi) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} f(n) - \frac{\chi(a)}{\varphi(q)} \sum_{n \leq x} f(n) \overline{\chi(n)}.$$

For modulus 1, the unique character and the unique residue class are understood in the usual way. A star on a residue-class sum means that only invertible classes are summed.

Theorem 4.1 (The full published short-progression conclusions). *Let $f : \mathbb{N} \rightarrow \mathbb{U}$ be multiplicative.*

1. Suppose $1 \leq Q \leq x/10$ and $(\log(x/Q))^{-1/200} \leq \varepsilon \leq 1$. For every prime $p \leq Q$, choose $\chi_1 \pmod{p}$ minimizing

$$\inf_{|t| \leq \log x} \mathbb{D}_p(f, \chi(n)n^{it}; x).$$

Then

$$\sum_{a \pmod{p}}^* |E_f(x; p, a; \chi_1)|^2 \ll \varepsilon \frac{x^2}{p}.$$

2. Fix $\eta > 0$. Suppose $x \geq 10$, $(\log x)^{-1/200} \leq \varepsilon \leq 1$, and $Q \leq x^{1/2-100\eta}$. If f vanishes outside the x^η -smooth positive integers, then for every $q \leq Q$, with χ_1 chosen by the same minimization with modulus q ,

$$\max_{(a,q)=1} |E_f(x; q, a; \chi_1)| \ll_\eta \varepsilon \frac{x}{q}.$$

3. Under the parameter assumptions in part 1, for every $(x/Q)^{\varepsilon^2}$ -typical $q \leq Q$, and with χ_1 again chosen by that minimization,

$$\sum_{a \pmod{q}}^* |E_f(x; q, a; \chi_1)|^2 \ll \varepsilon \varphi(q) \left(\frac{x}{q}\right)^2.$$

4. Suppose $X \geq h \geq 10$, $1 \leq Q \leq h/10$, and $(\log(h/Q))^{-1/200} \leq \varepsilon \leq 1$. For every $(h/Q)^{\varepsilon^2}$ -typical $q \leq Q$, choose (χ_1, t_1) to minimize $\mathbb{D}_q(f, \chi(n)n^{it}; X)$ over characters modulo q and real $|t| \leq X$. Put

$$B_f(x, h; q, a) = \frac{\chi_1(a)}{\varphi(q)} \left(\int_x^{x+h} v^{it_1} dv \right) \frac{1}{3X} \sum_{n \leq 3X} f(n) \overline{\chi_1(n)} n^{-it_1}.$$

Then

$$\int_X^{2X} \sum_{a \pmod{q}}^* \left| \sum_{\substack{x < n \leq x+h \\ n \equiv a \pmod{q}}} f(n) - B_f(x, h; q, a) \right|^2 dx \ll \varepsilon \varphi(q) X \left(\frac{h}{q}\right)^2.$$

All implied constants are uniform in the displayed parameters and in f ; only that in part 2 may depend on the fixed η . Any minimizing character or minimizing pair may be used.

Proof. We state explicitly the unconditional analytic input from [20]; this distinguishes the imported mean-value estimates from the new removal of the zero hypothesis. Section 3.2 of that paper identifies sufficient sets of good moduli by

$$\mathcal{G}(u, \varepsilon) = \left\{ q \leq u : \begin{array}{l} L(s, \chi) \neq 0 \text{ for every } \chi \pmod{q} \text{ with } \text{cond}(\chi) > u^{\varepsilon^{200}}, \\ \text{Re } s \geq 1 - \varepsilon^{-100} \frac{\log \log u}{\log u}, \quad |\text{Im } s| \leq 3u \end{array} \right\}. \quad (8)$$

The four conclusions above hold unconditionally when the modulus is restricted to this set, with $u = x$ in parts 1–3 and $u = X$ in part 4. No zero-density estimate is required when membership in this set is known for every modulus.

For clarity, the published proof of this input uses Lemma 8.2 to bound prime character sums in the prescribed zero-free region, then Propositions 8.3 and 8.5 to control, respectively, the size and the number of large twisted multiplicative sums. Proposition 9.2 and character orthogonality give the variance conclusions; the exact identity used here is

$$\sum_{a(q)}^* |E_f(x; q, a; \chi_1)|^2 = \frac{1}{\varphi(q)} \sum_{\substack{\chi(q) \\ \chi \neq \chi_1}} \left| \sum_{n \leq x} f(n) \overline{\chi(n)} \right|^2.$$

Proposition 9.4 and the Parseval reduction in §9.2, equation (50), give the hybrid conclusion with the displayed integral main term. Section 11, especially §11.3.2, gives the smooth-supported pointwise conclusion. The only character sums omitted from the zero-free condition have small conductor; their treatment is unconditional in Lemma 7.9 and Lemma 8.2. The large-conductor conditions appearing in these arguments are precisely those recorded in (8): in the variance and hybrid proofs their width is at most $\varepsilon^{-88} \log \log u / \log u$ after the $\varepsilon^{1.1}$ substitution in §9.2, while in §11.3.2 the width is $\varepsilon^{-100} \log \log u / \log u$. The conductor cutoffs used there are larger than $u^{\varepsilon^{200}}$. Lemma 8.1 estimates the number of excluded moduli by a zero-density theorem; that counting step is the step which becomes unnecessary here.

There is a parameter detail in applying these published arguments at the smallest permitted ε , which we verify rather than suppress. In §9.2 the substitution $\varepsilon \mapsto \varepsilon^{1.1}$ can fall below the stated lower range in Propositions 9.2 and 9.4. In their proofs, however, the separation inequalities (52) and the sieve-error estimates use $\log R > \varepsilon^{-100}$, where $R = x/Q$ or h/Q . The original assumption gives $\log R \geq \varepsilon^{-200}$, and therefore, after substitution, still gives $\log R \geq (\varepsilon^{1.1})^{-100}$. All the power inequalities used in those separation estimates have this margin. The upper-range requirement on M in Lemma 8.1 estimates the number of bad moduli only; it is not needed for the analytic estimates on a specified good modulus.

There are also calls to Proposition 8.3 and Corollary 8.4 with parameter $\kappa = \varepsilon^{6.6}$ in §9 and $\kappa = \varepsilon^{9.5}$ in §11.3.2. These can fall below their displayed bound $\kappa \geq (\log u)^{-1/50}$. Under our fixed strip the versions needed here remain valid in the larger range

$$(\log u)^{-1/20} \leq \kappa \leq c, \tag{9}$$

where $c > 0$ is a fixed sufficiently small constant. Here are the required checks. The truncated Perron formula used in the proof of Lemma 8.2, equation (34), can now be shifted to $\operatorname{Re} s = 15/16$. The fixed distance from all nontrivial zeros bounds the logarithmic derivative there by $O((\log u)^2)$ for $q \leq u$ and $|\operatorname{Im} s| \leq 3u$. With height of order $(\log u)^{1000}$, shifted if necessary to avoid the zeta pole on a horizontal side, this gives, uniformly for $|t| \leq 2.1u$,

$$\sum_{n \leq P} \Lambda(n) \chi(n) n^{-it} = \mathbf{1}_{\chi=\chi_0} \frac{P^{1-it}}{1-it} + O\left(P^{15/16} (\log u)^3 + \frac{P}{(\log P)^{100}}\right) \tag{10}$$

for $u^{\kappa^{5.5}} \leq P \leq u$. The Perron truncation error follows by absolute values from $|\Lambda(n) \chi(n) n^{-it}| \leq \log n$, exactly as in that equation. When the pole at $s = 1 - it$ is outside the truncated rectangle, its displayed term is $O(P/(\log u)^{1000})$ and is absorbed by the error. Removing Euler factors at primes dividing q contributes at most $O((\log u)^2)$, also absorbed. The same argument treats zeta after its pole is subtracted.

In (9), $\log P \geq (\log u)^{29/40}$; hence the error in (10) is $o(\kappa^{10}P)$. This proves Lemma 8.2(i) in this larger range for every nonprincipal character, and for the principal character when $|t| \geq \kappa^{-10}$, as required. For a nonprincipal character, partial summation and Mertens' theorem now give

$$\mathbb{D}_q(\chi(n)n^{it}, 1; u)^2 \geq 5.5 \log(1/\kappa) + O(1).$$

The omission of primes dividing q costs $O(1)$ here, since the omitted primes under consideration exceed $u^{\kappa^{5.5}}$. For the principal character, the unconditional estimate (35) in the source gives $(1/3 - o(1)) \log \log u$ when $(\log u)^{-1/2} \leq |t| \leq 2.1u$. This is larger than $5.5 \log(1/\kappa) + O(1)$ because $5.5/20 = 11/40 < 1/3$. Thus Lemma 8.2(ii) also extends.

The proof of Proposition 8.3 now applies: its first part uses this distance lower bound against the upper bound $5.48 \log(1/\kappa) + O(1)$, and the remainder $(\log u)^{-1/4}$ in the unconditional Halász estimate of Lemma 7.4 is $o(\kappa)$. For the second part we use only $|t| \leq u/2$ and $Z \leq u$. Then every auxiliary $|v| \leq Z/2$ satisfies $|t + v| \leq u$, so the minimizing property of $t_1 \in [-u, u]$ is applicable; also $|t + v - t_1| \leq 2u$. This restriction avoids extending the minimizing property outside its defining interval. The damping of primes in $[P, Q]$ costs at most $\frac{1}{6} \log(1/\kappa)$ in squared distance. The remaining coefficient of $\log \log u$ is at least $1/12 - 1/120 - o(1) = 3/40 - o(1) > 1/15$. The claimed $(\log u)^{-1/15}$ saving therefore survives, including the Halász prefactor. Integrating the weights $r^{\omega_{[P,Q]}(n)}$ over $0 \leq r \leq 1$ proves Corollary 8.4 in the same enlarged range and for this restricted t -range, as in its published proof. This suffices for the hybrid application, because its relevant upper frequency is

$$T = \frac{X}{h} \left(\frac{h}{Q} \right)^{0.01\varepsilon^{1.1}} \leq Xh^{-0.99} < X/2.$$

The part of the Parseval reduction with larger frequencies uses the unconditional mean-value estimate of Lemma 6.2 instead. In the progression-only application the twist is $t = 0$; in the logarithmic-range version of Remark 8.1 the $\frac{1}{2} \log u$ ranges for both t and the auxiliary Halász twist keep their sum inside $[-\log u, \log u]$. The uses of Proposition 8.5 require parameters $\varepsilon^{2.2}$ in §9 and ε^3 in §11; these already satisfy its stated lower bound $(\log u)^{-1/30}$ and need no enlargement. Finally $6.6/200 < 1/20$ and $9.5/200 < 1/20$, so (9) covers both applications above. These checks justify the published deductions throughout the exact endpoint ranges in the theorem.

In every one of the four parameter ranges we have

$$\varepsilon \geq (\log u)^{-1/200}.$$

Indeed $\log(x/Q) \leq \log x$ and $\log(h/Q) \leq \log X$. Consequently

$$0 < \varepsilon^{-100} \frac{\log \log u}{\log u} \leq \frac{\log \log u}{\sqrt{\log u}}. \quad (11)$$

Choose an absolute effectively computable u_0 so large that the right side is strictly less than $1/8$ for $u \geq u_0$. The entire rectangle in (8) then lies in $\operatorname{Re} s > 7/8$. By the imported Dirichlet QRH theorem, all primitive nonprincipal Dirichlet L -functions are nonzero there. If χ is induced by χ^* , then

$$L(s, \chi) = L(s, \chi^*) \prod_{\substack{p|q \\ p \nmid \operatorname{cond}(\chi)}} (1 - \chi^*(p)p^{-s}).$$

The additional factors have no zero when $\operatorname{Re} s > 0$. The cutoff in (8) is greater than 1, so it excludes the principal character. Therefore

$$\mathcal{G}(u, \varepsilon) = [1, u] \cap \mathbb{Z} \quad (u \geq u_0)$$

uniformly throughout the required range of ε . Applying the unconditional analytic input proves all four claims for these u .

It remains to verify uniformity for the bounded range $10 \leq u < u_0$. Here $\varepsilon \geq (\log u_0)^{-1/200}$ and $q \leq u_0$. In parts 1–3, each progression contains at most $x/q + 1$ terms, and the character main term has modulus at most $x/\varphi(q)$. These bounds, with $q \leq u_0$ and $x/q \geq 1$, imply the stated pointwise and variance estimates after increasing an absolute constant. In part 4, each short progression contains at most $h/q + 1$ terms and $|B_f| \leq h/\varphi(q)$. Integrating the squared trivial bound over an interval of length X similarly gives the asserted result, with a constant depending only on u_0 . This completes the proof for all the stated parameters. $\square$

Corollary 4.2 (The published GRH bound for the least product of three primes). *For every fixed $\delta > 0$ there is an effective C_δ such that every reduced residue class $a \pmod{q}$ contains an integer $n = p_1 p_2 p_3 \leq C_\delta q^{2+\delta}$ with exactly three prime factors counted with multiplicity. Equivalently,*

$$\mathcal{L}_3(q) := \max_{(a,q)=1} \min\{n \geq 1 : n \equiv a \pmod{q}, \Omega(n) = 3\} \ll_\delta q^{2+\delta}.$$

For q sufficiently large in terms of δ the three primes may additionally be required to be at most q .

Proof. The bound for $\mathcal{L}_3$ is explicitly recorded under GRH in [20, §2]. We use the positive lower-bound consequence of its Proposition 12.2, whose proof in §12.2 applies to all moduli despite its caption mentioning primes. Choose a fixed sufficiently small $\alpha > 0$ with $1000\alpha < \min(\delta, 1)$, and set

$$P_1 = q^{1000\alpha}, \quad P_2 = P_3 = q.$$

That proposition gives a positive weighted count of triples

$$P_j^{1-\alpha} \leq p_j \leq P_j \quad (1 \leq j \leq 3), \quad p_1 p_2 p_3 \equiv a \pmod{q},$$

provided all Dirichlet L -functions modulo q have no zero in

$$\operatorname{Re} s \geq 1 - \frac{M(\alpha)}{\log q}, \quad |\operatorname{Im} s| \leq (\log q)^3,$$

for an effective $M(\alpha)$. The principal character is included here: its L -function has a pole at 1, which is not a zero. For $q > \exp(8M(\alpha))$ the zero-free requirement follows from the fixed strip for zeta and Dirichlet L -functions, and the extra imprimitive Euler factors have no zeros in this rectangle.

To see positivity without depending on a multiplicity convention, take the ordered triples produced by the character expansion in the proof of Proposition 12.2. Their reciprocal-product mass has a positive main term proportional to

$$\frac{1}{\varphi(q)} \prod_{j=1}^3 \sum_{\substack{P_j^{1-\alpha} \leq p \leq P_j \\ p \nmid q}} \frac{1}{p},$$

with relative error $O(\alpha)$ in that proof. Each prime sum tends to $-\log(1-\alpha) > 0$ by the prime number theorem. Deleting primes dividing q costs $O(\log q/P_j^{1-\alpha}) = o(1)$. Thus the mass is positive for fixed sufficiently small α and large q . Counting an integer once instead of with its representation multiplicity changes this mass by a factor between 1 and 6, so positivity is unchanged. A detected product is at most $P_1 P_2 P_3 = q^{2+1000\alpha} \leq q^{2+\delta}$ and all its prime factors are at most q . For the finitely many smaller q , the unconditional theorem on primes in arithmetic progressions supplies a product of exactly three primes in each reduced class: fix a prime $r \nmid q$ and take a prime $p \equiv ar^{-2} \pmod{q}$. An effective bound for this finite range is absorbed into C_δ . $\square$

Scope. The conclusion for typical moduli is uniform for every such modulus, rather than outside a small exceptional set. The character correction remains necessary for general f ; for example $f = \chi$ itself has a large correlation with that character. The smooth-support assumption in part 2 is retained. The zero-free input has been used only in a rectangle whose width tends uniformly to zero, so the fixed strip suffices without square-root error terms for primes.

5 Fourier uniformity in intervals longer than every fixed logarithmic power

Walsh's published Fourier-cancellation conclusion [92] assumes GRH and allows intervals longer than every fixed power of $\log X$. Its analytic input is a twisted prime estimate with some positive power saving. The value of that saving is not part of the conclusion. We prove that estimate, including its uniformity in the real twist, and use the published inverse argument only in the short-interval range needed here. The remaining interval lengths are covered by a previous unconditional theorem. References to intermediate numbered results are to the full author version linked from Walsh's publication page.

For a complex multiplicative function g with $|g(n)| \leq 1$, put

$$\mathcal{D}(g; T, Q) = \inf_{\substack{\chi \pmod{q}, q \leq Q \\ |t| \leq T}} \left(\sum_{p \leq T} \frac{1 - \Re(g(p)p^{it}\chi(p))}{p} \right)^{1/2}.$$

Characters in this definition need not be primitive. Write $e(u) = \exp(2\pi i u)$.

Theorem 5.1 (Walsh's Fourier-cancellation conclusion). *If $H = H(X) \leq X$ and $\log H / \log \log X \rightarrow \infty$, then, for $g = \mu$ or $g = \lambda$,*

$$\int_X^{2X} \sup_{\alpha \in \mathbb{R}/\mathbb{Z}} \left| \sum_{x \leq n \leq x+H} g(n)e(\alpha n) \right| dx = o(HX).$$

Here μ and λ are respectively the Möbius and Liouville functions. The frequency inside the supremum may vary with x . Equivalently, for every $\eta > 0$ there are $K > 1$ and X_0 such that the integral is less than ηHX whenever $X \geq X_0$ and $(\log X)^K \leq H \leq X$.

Lemma 5.2 (The precise twisted prime input). *There are absolute constants $c > 0$ and $A > 1$ such that, for every Dirichlet character χ modulo q , every real t , and $P \gg (\log(3q(2 + |t|)))^A$,*

$$\frac{1}{P} \left| \sum_{n \leq P} \Lambda(n) \chi(n) n^{it} \right| \ll \frac{\delta_\chi}{1 + |t|} + P^{-c},$$

where $\delta_\chi = 1$ for a principal character and is zero otherwise. More precisely, uniformly for $P \geq 2$,

$$\sum_{n \leq P} \Lambda(n) \chi(n) n^{it} = \delta_\chi \frac{P^{1+it}}{1+it} + O\left(P^{15/16} \log^2(3qP(2 + |t|))\right). \quad (12)$$

The same constants, after alteration, give

$$\left| \sum_{P \leq p \leq 2P} \chi(p) p^{it} \right| \ll \frac{P}{\log P} \left(\frac{\delta_\chi}{1 + |t|} + P^{-c} \right) \quad (13)$$

in the stated logarithmic range.

Proof. We may assume $P \geq 3$, since the bounded range $2 \leq P < 3$ is absorbed by the error in (12). Let $a = 15/16$ and $b = 1 + 1/\log P \leq 2$. The zero-free theorem and the classical local partial-fraction expansion of L'/L imply

$$-\frac{L'}{L}(s, \chi) = \frac{\delta_\chi}{s-1} + O(\log(3q(2 + |\Im s|))) \quad (a \leq \Re s \leq 2). \quad (14)$$

Indeed, there are $O(\log(3q(2 + |\Im s|)))$ zeros with ordinate within one of $\Im s$; each is horizontally separated from this strip by at least $1/16$. The remaining terms in the local expansion obey the same logarithmic bound. For an induced character the additional terms are bounded by

$$\sum_{p|q} \frac{\log p}{p^a - 1} \ll \log(3q).$$

Thus the assertion includes principal and imprimitive characters.

First take P to be a half-integer and put $U = P^2(2 + |t|)$. Truncated Perron's formula for $-L'/L(s - it, \chi)$ gives

$$\sum_{n \leq P} \Lambda(n) \chi(n) n^{it} = \frac{1}{2\pi i} \int_{b-iU}^{b+iU} -\frac{L'}{L}(s - it, \chi) \frac{P^s}{s} ds + O\left(\frac{P \log^2(2P)}{U} + \log^2(2P)\right).$$

The absolute values of the coefficients are at most $\Lambda(n)$, so the truncation error has no factor depending on t . Shift the contour to $\Re s = a$. The only pole crossed is $s = 1 + it$ when χ is principal; it lies strictly between the horizontal sides and contributes the displayed main term. On the left side, $|s - 1 - it| \geq 1/16$ and (14) bounds the integral by

$$\ll P^a \log(3q(P + U + |t|)) \log(2U) \ll P^a \log^2(3qP(2 + |t|)).$$

Each horizontal side contributes $O(P \log(3q(P + U + |t|))/U)$. This proves (12) at half-integers. Changing the cutoff by at most one changes the sum by $O(\log(2P))$ and its main term by $O(1)$, since the derivative of $v^{1+it}/(1+it)$ has modulus one. Thus arbitrary real P is allowed.

For example, choosing $A = 128$ and then a sufficiently large absolute lower-range constant absorbs the logarithmic factor into a power of P , giving the assertion with a smaller fixed c , such as $1/64$. To obtain (13), subtract prime powers from (12) and apply partial summation with the weight $1/\log v$ on $[P, 2P]$. Prime powers contribute at most $O(P^{1/2} \log^2(2P))$ before that partial summation. The principal main term becomes

$$\int_P^{2P} \frac{v^{it}}{\log v} dv \ll \frac{P}{(1 + |t|) \log P},$$

by integration by parts using $v^{1+it}/(1+it)$. All error terms are absorbed by a smaller fixed $c > 0$. $\square$

Proof of Theorem 5.1. We shall use the following inverse implication only for $(\log X)^K \leq H \leq X^{1/2}$: if a complex multiplicative g with $|g| \leq 1$ has the displayed Fourier integral at least $\eta H X$, then $\mathcal{D}(g; CX^2/H^2, C) \leq C$, for suitable constants C, K depending on η . This is the part of the proof of the published Theorem 1.1 whose full parameter range we verify below.

First verify the complete analytic interface to that combinatorial proof. Let $\mathcal{P}$ be the primes in $[P, 2P]$, let $P \leq \tilde{H} \leq Y/(\log Y)^2$, and let A_1, A_2 be $\tilde{H}$ -separated sets in $[Y/10, 10Y]$. For $Q \geq 1$ with

$$\log(3Q) \leq \log(3Y) \leq P^\varepsilon,$$

choose a sufficiently small fixed $\varepsilon > 0$, depending only on the absolute constants in Lemma 5.2. The lemma applies to every character modulo Q and every $|t| \ll Y$.

A labelled path of length k has successive points x_j in $A_1 \cup A_2$ and prime labels $p_j, q_j \in \mathcal{P}$ such that $|x_j/p_j - x_{j+1}/q_j| \ll \tilde{H}/P$. For $k \leq \varepsilon_0 \log(Y/\tilde{H})$, Walsh's unconditional path estimate (Lemma 2.6) gives

$$\left| x_1 \prod_{j=1}^k (q_j/p_j) - x_{k+1} \right| \ll k\tilde{H}.$$

For given endpoints and prime labels, separation gives at most $O(1)^k$ paths. Majorize the condition above by a nonnegative Schwartz function φ with Fourier transform supported in $[-1, 1]$ and $\varphi \geq 1$ on $[-1, 1]$. Fourier inversion reduces the number of paths from A_1 to A_2 satisfying

$$\prod_{j=1}^k p_j \equiv u \prod_{j=1}^k q_j \pmod{Q}, \quad (u, Q) = 1,$$

with all labels coprime to Q , to at most

$$\frac{C^k k \tilde{H}}{Y} \int_{|\xi| \leq Y/(C_1 k \tilde{H})} |S_1(\xi) S_2(\xi) T(\xi)| d\xi, \quad S_j(\xi) = \sum_{x \in A_j} e(\xi \log x).$$

Character orthogonality expresses T as

$$T(\xi) = \frac{1}{\phi(Q)} \sum_{\chi \pmod{Q}} \overline{\chi(u)} \left| \sum_{p \in \mathcal{P}} \chi(p) p^{2\pi i \xi} \right|^{2k}.$$

Hence, by (13) and $|\mathcal{P}| \asymp P/\log P$,

$$|T(\xi)| \leq C^{2k} |\mathcal{P}|^{2k} \left(\frac{1}{\phi(Q)(1 + |\xi|)^{2k}} + P^{-2ck} \right).$$

For the first term use $|S_j| \leq |A_j|$ and integrate $(1 + |\xi|)^{-2k}$. For the second use Cauchy-Schwarz and the continuous large sieve: since the numbers $\log x$, $x \in A_j$, are separated by $\gg \tilde{H}/Y$,

$$\int_{|\xi| \leq Y/(C_1 k \tilde{H})} |S_j(\xi)|^2 d\xi \ll (Y/\tilde{H}) |A_j|.$$

Absorbing k into C^k proves the path bound

$$\ll \frac{C^k \tilde{H}}{\phi(Q)Y} |\mathcal{P}|^{2k} |A_1| |A_2| + C^k |A_1|^{1/2} |A_2|^{1/2} |\mathcal{P}|^{2k} P^{-ck}. \quad (15)$$

This is at least as strong as the source's Lemma 2.8, whose second term has the additional factor $\phi(Q)$. In particular its $k = Q = 1$ consequence, Corollary 2.9, follows with some fixed positive c_0 :

$$\#\{(x, y, p, q) \in A_1 \times A_2 \times \mathcal{P}^2 : |x/p - y/q| \ll \tilde{H}/P\} \ll \frac{\tilde{H}}{Y} |A_1| |A_2| |\mathcal{P}|^2 + |A_1|^{1/2} |A_2|^{1/2} P^{2-c_0}. \quad (16)$$

For clarity, the remaining imported result is the combinatorial implication proved in [92, Sections 2–8]: estimates of the forms (15) and (16), with any fixed positive saving, imply the inverse assertion just stated. Its hypotheses do not prescribe a numerical saving. The full dependency chain

is as follows. Suppose, for a contradiction, that the asserted inverse conclusion fails while the Fourier correlation hypothesis holds. The unconditional reduction in Section 2.1, using Elliott's inequality and the large sieve, then supplies an H -separated configuration $\mathcal{J} = \{(x, \alpha_x)\}$ of cardinality $\gg_\eta X/H$, and $P \in [H^{\epsilon^2}, H^\epsilon]$, with $\gg_\eta (X/H)|\mathcal{P}|^2$ relations

$$|x/p - y/q| < \delta H/P, \quad \|p\alpha_x - q\alpha_y\| \leq C_0/(PH).$$

Sections 3–4 prove the unconditional phase and fixed-prime lifting lemmas. Section 5 uses (16) to keep configuration sizes and relation densities bounded through the successive lifts (Proposition 5.8). The same estimate yields the downward expansion of Lemma 6.5. Here only $c_0 > 0$ is used: the adjustable loss exponent $\tilde{c}$ is chosen smaller than a fixed multiple of c_0 by increasing K . Section 7 constructs a global frequency, and its Lemma 7.3 uses (15) to bound its rational denominator. In that application the path length is a sufficiently large constant multiple of $\log b / \log P$; increasing that constant absorbs any fixed decrease in c . Finally Section 8 removes the temporary logarithmic losses in the frequency and phase approximation, again using (16). The resulting conclusion is

$$|T_0| \ll_\eta X^2/H^2, \quad b \ll_\eta 1, \quad \left\| \alpha_x - \frac{a_x}{b} - \frac{T_0}{x} \right\| \ll_\eta H^{-1}$$

for $\gg_\eta X/H$ points in $\mathcal{J}$. The unconditional short-interval multiplicative-function step described in Section 2.1 then gives $\mathcal{D}(g; CX^2/H^2, C) \leq C$.

This chain is the published proof with its sole GRH input, Lemma 2.7, replaced by Lemma 5.2. All parameters may still be chosen in the order prescribed in Section 2.3: the prime input constants are absolute, then the configuration constants depend on η , and finally K is sufficiently large in terms of these. In the construction in Section 7 the lifted scales satisfy $\log Y \ll_\eta \log X$. Moreover $Y/\tilde{H} = X/H \geq X^{1/2}$, so $\tilde{H} \leq Y/(\log Y)^2$ holds at every such scale. Consequently $P \geq H^{\epsilon^2} \geq (\log X)^{K\epsilon^2}$ makes the prime input valid at every scale, after increasing K .

We finish by spelling out the consequence for μ and λ . For a fixed Q , uniformly for $q \leq Q$, $|t| \leq Z$, and $Z \rightarrow \infty$, the prime version of (12) and partial summation give

$$\Re \sum_{p \leq Z} \frac{\chi(p)p^{it}}{p} \geq -\log \log \log Z - O_Q(1). \quad (17)$$

Here is a direct verification. Put $y = (\log Z)^{128}$. The primes $p \leq y$ contribute at worst $-\log \log y - O(1)$. On $[y, Z]$ the error term in the prime counting formula contributes $O(y^{-1/16} \log^2(3QZ)) = O(1)$ after partial summation with $1/v$. For a principal character the remaining real main term is

$$\int_y^Z \frac{\cos(t \log v)}{v \log v} dv = \int_{\log y}^{\log Z} \frac{\cos(tw)}{w} dw \geq -O(1)$$

uniformly in t : the part with $|tw| \leq 1$ is nonnegative, and integration by parts bounds every subinterval of $|tw| \geq 1$ by an absolute constant. For a nonprincipal character that main term is absent. This proves (17). Since $\mu(p) = \lambda(p) = -1$, Mertens' estimate now implies

$$\mathcal{D}(g; Z, Q)^2 \geq \log \log Z - \log \log \log Z - O_Q(1) \rightarrow \infty.$$

For $H \leq X^{1/2}$, the inverse theorem would contradict this bound along any sequence with normalized Fourier average at least a fixed positive η , since $Z = CX^2/H^2 \geq CX$. For $X^{1/2} \leq H \leq X$, partition each interval into pieces of length $h = X^{1/4}$ and one remainder of length at most h . The triangle inequality bounds its maximal Fourier sum by the sum of the corresponding maxima on the pieces,

plus $O(h)$. Integrating, each translated starting-point interval lies in $[X, 3X]$. The unconditional power-length result of Matomäki–Radziwiłł–Tao [93], applied on a fixed finite covering by intervals of the form $[Y, 2Y]$ with $Y \asymp X$, bounds each integrated piece by $o(Xh)$. There are $O(H/h)$ pieces and the remainder is $O(Xh) = o(XH)$. This proves $o(XH)$ throughout the remaining range. The two ranges together prove the full published Fourier-cancellation conclusion. $\square$

Range of the imported inverse argument. The printed inverse theorem itself is formulated without an upper restriction on H . Its mixing lemma has the upper restriction $\tilde{H} \leq Y/(\log Y)^2$, and the fixed-power predecessors do not explicitly settle the general-function inverse statement for H very close to X . We therefore do not assert that larger inverse range. The theorem proved here is the complete Fourier-cancellation conclusion stated in the published abstract and introduction; the unconditional long-interval argument above supplies its full range.

The transferred conclusion concerns linear phases. The author’s discussion of higher-step nilsequences and almost exponential growth of Liouville sign patterns is a proposed extension, not a theorem proved in that paper, and is not asserted here. The recent improvement of the unconditional interval range by Pilatte, arXiv:2604.26564, still explicitly distinguishes Walsh’s GRH conclusion; its range $H \geq \exp((\log X)^{2/5+\varepsilon})$ does not include the range established above.

6 Power decay in Möbius correlations with polynomial nilsequences

Green–Tao’s unconditional nilsequence theorem has decay faster than every fixed negative power of $\log N$. Their published remarks immediately after Theorem 1.1 explicitly assert a stronger conclusion under GRH: decay N^{-c} , with $c > 0$ depending only on dimension and filtration degree [110, p. 543]. We prove that complete power-decay conclusion. The logarithmic theorem and its mere effectivity are not the assertion being counted here.

We specify the terminology. A nilmanifold is G/Γ , where G is a connected, simply connected nilpotent Lie group and Γ is a discrete cocompact subgroup. A degree- d filtration $G_\bullet$ is a descending sequence of closed connected subgroups $G = G_0 = G_1 \supseteq \cdots \supseteq G_{d+1} = \{1\}$ with $[G_i, G_j] \subseteq G_{i+j}$. A sequence $g : \mathbb{Z} \rightarrow G$ is polynomial relative to this filtration if every iterated multiplicative difference $\partial_{h_i} \cdots \partial_{h_1} g$ takes values in G_i , where $\partial_h g(n) = g(n+h)g(n)^{-1}$. A Mal’cev basis $\mathcal{X} = (X_1, \dots, X_m)$ identifies G with $\mathbb{R}^m$ by $\exp(t_1 X_1) \cdots \exp(t_m X_m)$, identifies Γ with integer coordinates, and satisfies that $\text{span}(X_{j+1}, \dots, X_m)$ is a Lie algebra ideal for each $0 \leq j < m$. It is adapted to $G_\bullet$ if each filtration subgroup is spanned by an appropriate final segment of the basis, and Q -rational if all its Lie-bracket structure constants are rational of height at most Q , where the height of a reduced fraction a/b is $\max\{|a|, |b|\}$. We use the right-invariant coordinate metric and induced quotient metric $d_{\mathcal{X}}$ of [111, Definitions 2.1–2.4]. For a function F on this quotient, write

$$\|F\|_{\text{Lip}} = \|F\|_{\infty} + \sup_{x \neq y} \frac{|F(x) - F(y)|}{d_{\mathcal{X}}(x, y)}.$$

Theorem 6.1 (Green–Tao’s published GRH improvement). *For every pair of positive integers m, d there are effective constants $c = c(m, d) > 0$ and $C = C(m, d) > 0$ such that the following holds. Suppose G/Γ has dimension m , a degree- d filtration, and an adapted Q -rational Mal’cev basis, $Q \geq 2$. For every $g \in \text{poly}(\mathbb{Z}, G_\bullet)$, every Lipschitz function $F : G/\Gamma \rightarrow [-1, 1]$, and every integer $N \geq 2$,*

$$\left| \frac{1}{N} \sum_{n \leq N} \mu(n) F(g(n)\Gamma) \right| \leq C Q^C (1 + \|F\|_{\text{Lip}}) N^{-c}.$$

The constants are uniform in g , the nilmanifold, its stated rationality parameter, F , and N .

Proof. We first establish the required analytic estimate, including arithmetic progressions which are not coprime to their modulus.

A uniform Möbius estimate with polynomial modulus loss. There are effective absolute constants $B \geq 1$ and $\delta > 0$ such that, for every Dirichlet character modulo q , including a principal or induced character,

$$\left| \sum_{n \leq t} \mu(n) \chi(n) \right| \ll q^B t^{1-\delta} \quad (t \geq 1). \quad (18)$$

Here a small unspecified positive saving is sufficient. We give a proof which avoids any Lindelöf estimate.

Put $a = 15/16$. The zero-free input implies the effective polynomial-growth bound

$$|L(s, \chi)^{-1}| \ll \{q(3 + |\Im s|)\}^{B_0} \quad (a \leq \Re s \leq 2) \quad (19)$$

for an effective absolute integer $B_0 \geq 1$. To verify this, first take a primitive nonprincipal character. On the disc centered at $2 + it$ of radius $35/32$, one has $\Re s \geq 29/32$. The character partial sums $A(u) = \sum_{n \leq u} \chi(n)$ satisfy $|A(u)| \leq q$, so partial summation gives

$$L(s, \chi) = s \int_1^\infty A(u) u^{-s-1} du, \quad |L(s, \chi)| \leq q|s|/(\Re s).$$

Consequently $\log |L| \ll \log(q(3 + |t|))$ on the disc. The whole disc lies in $\Re s > 7/8$ and is zero-free. Choose the logarithm at its center by the absolutely convergent Euler product, so its value there is $O(1)$. Borel–Carathéodory on the concentric disc of radius $17/16$ therefore gives $|\log L| \ll \log(q(3 + |t|))$. This proves (19) for primitive nonprincipal characters. For the primitive principal character, apply the same argument to the holomorphic, nonvanishing function $(s-1)\zeta(s)$ on these discs. Its logarithm at the center is $O(\log(3 + |t|))$. The elementary summation formula

$$(s-1)\zeta(s) = s - s(s-1) \int_1^\infty \{u\} u^{-s-1} du$$

bounds its absolute value on the disc by $O((3 + |t|)^2)$. The zero of $1/\zeta$ at 1 is harmless. For an induced character, the extra reciprocal Euler factors are bounded, uniformly on the strip, by

$$\prod_{p|q} (1 - p^{-a})^{-1} \leq (1 - 2^{-a})^{-\omega(q)} \leq q^{C_0}.$$

Enlarge B_0 to obtain (19) in all cases.

Choose an integer $k > B_0 + 1$ and define the k th Riesz sum

$$R_k(t) = \frac{1}{k!} \sum_{n \leq t} \mu(n) \chi(n) (t - n)^k.$$

Its Mellin formula and a contour shift from $\Re s = 2$ to $\Re s = a$ give

$$R_k(t) = \frac{1}{2\pi i} \int_{(a)} \frac{t^{s+k}}{L(s, \chi) s(s+1) \cdots (s+k)} ds \ll q^{B_0} t^{k+a}.$$

There is no pole in the intervening strip. Absolute convergence on the new line and vanishing of the horizontal integrals follow from $k > B_0 + 1$ and (19). Set $\delta = (1 - a)/(k + 1)$ and $h = t^{1-\delta}/k$. If Δ_h denotes the forward difference with step h , repeated integration of the k th derivative gives

$$h^{-k} \Delta_h^k R_k(t) = \int_{[0,1]^k} \sum_{n \leq t+h(u_1+\dots+u_k)} \mu(n) \chi(n) d\mathbf{u}.$$

The right side differs from $\sum_{n \leq t} \mu(n) \chi(n)$ by at most $kh + 1$. On the left, the Riesz bound and $t + kh \leq 2t$ give $O(q^{B_0} t^{a+k\delta})$. Since $a + k\delta = 1 - \delta$, this proves (18), after enlarging constants for bounded t .

For any q -periodic function f of absolute value at most one, the same estimate implies, for an effective absolute D ,

$$\left| \sum_{n \leq t} \mu(n) f(n) \right| \ll q^D t^{1-\delta}. \quad (20)$$

First suppose f vanishes outside the units modulo q . Expand in the characters of $(\mathbb{Z}/q\mathbb{Z})^\times$. Parseval and Cauchy–Schwarz bound the sum of the absolute Fourier coefficients by $\sqrt{\phi(q)}$, proving the claim with modulus factor $q^{B+1/2}$. In general, when $\mu(n) \neq 0$, the integer $d = (n, q)$ is squarefree and $n = du$ with $(u, q) = 1$. Thus the sum is

$$\sum_{d|\text{rad}(q)} \mu(d) \sum_{u \leq t/d} \mu(u) f(du) \mathbf{1}_{(u,q)=1}.$$

For every d the function in the inner sum is still q -periodic and vanishes off the units. Keeping this modulus q retains all the necessary coprimality restrictions. There are at most q choices of d , and $(t/d)^{1-\delta} \leq t^{1-\delta}$, so $D = B + 2$ suffices. Taking a difference of two initial sums now shows that for every arithmetic progression $P \subseteq [1, N]$ of common difference q ,

$$\left| \frac{1}{N} \sum_{n \in P} \mu(n) \right| \ll q^D N^{-\delta}. \quad (21)$$

The unconditional nilsequence inputs. We use two published quantitative theorems. First, the one-variable factorization theorem [111, Theorem 1.19] states that for each $B_1 > 0$ and $M_0 \geq 2$, an M_0 -rational input has a factorization

$$g = \varepsilon g' \gamma, \quad M_0 \leq M \ll_{m,d,B_1} M_0^{A_1},$$

where $A_1 = A_1(m, d, B_1)$ is effective. Here ε is (M, N) -smooth, meaning $d_{\mathcal{X}}(\varepsilon(n), 1) \leq M$ and $d_{\mathcal{X}}(\varepsilon(n), \varepsilon(n-1)) \leq M/N$; g' takes values in a rational subgroup G' and its orbit is totally M^{-B_1} -equidistributed in G'/Γ' ; and γ is M -rational, with $\gamma(n)\Gamma$ periodic of some period $q \leq M$. Totally ρ -equidistributed means that every mean-zero Lipschitz test function H has average of magnitude at most $\rho \|H\|_{\text{Lip}}$ on every progression of length at least ρN . The 2014 correction to the companion paper explicitly leaves this one-variable theorem unchanged.

Second, [110, Proposition 2.1] gives effective constants $c_1 = c_1(m, d) > 0$ such that an orbit which is totally ρ -equidistributed in a nilmanifold with an adapted Q_1 -rational basis satisfies

$$\left| \frac{1}{N} \sum_{n \in P} \mu(n) H(g(n)\Gamma) \right| \ll_{m,d} \rho^{c_1} Q_1 \|H\|_{\text{Lip}} \log N \quad (22)$$

when H has integral zero and $|P| \geq N/Q_1$. This is the unconditional Type I/II theorem, valid for all $0 < \rho < 1/2$, not just logarithmic values of ρ . We take constants uniformly over dimensions at most m .

We also record the precise coordinate consequences used to join these two inputs. They are the unconditional claim and its proof on p. 547 of [110], using [111, Appendix A, Propositions A.9 and Lemmas A.3–A.5, A.12–A.14, A.17]. Choose representatives γ_j of $\gamma(j)\Gamma$ in the coordinate fundamental domain. They have rational coordinates of height $M^{O_{m,d}(1)}$. Put $H_j = \gamma_j^{-1}G'\gamma_j$, $\Lambda_j = H_j \cap \Gamma$, and $g_j(n) = \gamma_j^{-1}g'(n)\gamma_j$. For any $a_0 \in G$ with $d_{\mathcal{X}}(a_0, 1) \leq M$, the function

$$F_{j,a_0}(u\Lambda_j) = F(a_0\gamma_j u\Gamma)$$

is well-defined. There are effective $b > 0$ and $C_1 > 0$, depending only on m, d , such that these quotients have M^{C_1} -rational adapted bases, the transformed functions have Lipschitz norm at most M^{C_1} when the original norm is at most one, and the transformed orbit is totally $M^{-bB_1+C_1}$ -equidistributed. Enlarging C_1 absorbs the fixed multiplicative constants. In particular, neither b nor C_1 depends on B_1 .

Choice of parameters and the full correlation. Normalize F by $1 + \|F\|_{\text{Lip}}$; restoring this factor at the end is harmless. Thus we may suppose both its absolute value and Lipschitz norm are at most one. We first choose B_1 , depending only on m, d , sufficiently large as specified below. This fixes the factorization exponent $A_1 \geq 1$. Then choose $\eta > 0$ so small that

$$\eta A_1(D+3) < \delta/2, \quad 3\eta A_1 < 1/2. \quad (23)$$

Assume $Q \leq N^\eta$ and apply factorization with $M_0 = N^\eta$; finitely many bounded N are absorbed in the effective constant. Then $M \ll N^{\eta A_1}$ and $M \geq N^\eta$.

Split the residue classes modulo q into progressions P whose diameters are at most $2N/M^2$ and whose sizes are at least $N/(2qM^2)$. Such a partition exists for all sufficiently large N , because (23) ensures $N \gg M^3$. It has $O(M^3)$ members, each of size at least $N/(2M^3)$. On a progression in the residue class j , freeze $\varepsilon(n)$ at any point $n_P \in P$, putting $a_P = \varepsilon(n_P)$. Right invariance of the coordinate metric gives

$$|F(\varepsilon(n)g'(n)\gamma_j\Gamma) - F(a_P g'(n)\gamma_j\Gamma)| \ll M^{-1}.$$

After summing over the partition and normalizing by N , the total freezing error is $O(M^{-1})$. The remaining contribution on P equals

$$\frac{1}{N} \sum_{n \in P} \mu(n) F_{j,a_P}(g_j(n)\Lambda_j).$$

Subtract the Haar mean of F_{j,a_P} . Its constant part is $O(M^D N^{-\delta})$ by (21), since the progression has common difference $q \leq M$ and the mean has absolute value at most one. Over all the pieces these parts total

$$O(M^{D+3} N^{-\delta}) \ll N^{-\delta/2}. \quad (24)$$

For the mean-zero part apply (22), taking Q_1 to be a sufficiently large fixed power of M to control both the rational basis and $N/|P|$. The preceding coordinate bounds give, after summing over the $O(M^3)$ pieces,

$$O(M^{-bc_1 B_1 + C_2} \log N),$$

where $C_2 = C_2(m, d)$ is independent of B_1 . Choose B_1 so large that $bc_1 B_1 \geq C_2 + 3$. This is the earlier choice, made before A_1 and η . The displayed bound is then $O(M^{-3} \log N) \ll N^{-\eta}$. A zero-dimensional subgroup has no mean-zero part and requires no application of (22).

Together with the freezing error and (24), this proves an effective $O_{m,d}(N^{-c})$ bound when $Q \leq N^\eta$, where $c = \min\{\eta, \delta/2\} > 0$. If $Q > N^\eta$, the theorem follows from the trivial bound by choosing its exponent C so that $C\eta \geq c$. Restoring $1 + \|F\|_{\text{Lip}}$ finishes the proof. $\square$

The proof uses the published unconditional factorization, coordinate and Type I/II results with all parameter losses made explicit above. It does not assume an inverse theorem with polynomial bounds for Gowers norms.

7 Rigidity from approximate quadratic Gauss-sum symmetries

Mangerel's Theorem 1.3(b) in [97] extends a rigidity statement to arbitrarily small fixed powers of the prime modulus, assuming a specified zero-free region for its Dirichlet L -functions. Theorem 1.1 supplies that region for all sufficiently large moduli. We prove its entire conditional conclusion below. The author's unconditional Theorem 1.1 and the converse in Theorem 1.3(a) are not counted as additional transfers.

Write $e(t) = \exp(2\pi it)$. If N is an odd prime and $f : \mathbb{N} \rightarrow \{-1, 1\}$, define

$$S_f(a) = \sum_{1 \leq n < N} f(n)e(an/N), \quad a \in \mathbb{Z}/N\mathbb{Z}.$$

Here “multiplicative” means multiplicative on coprime arguments; complete multiplicativity of f is not required.

Theorem 7.1 (Mangerel's conditional rigidity conclusion). *Fix $0 < c < 1$ and constants $B_1, B_2 > 0$. There are constants $M_0, N_0, C > 0$, depending only on c, B_1, B_2 , with the following property. Let $N \geq N_0$ be prime, let $M_0 \leq M \leq N$, and let $f : \mathbb{N} \rightarrow \{-1, 1\}$ be multiplicative. Suppose that $\mathcal{A}$ is a set of primes less than N and that signs $g(p) \in \{-1, 1\}$ are specified for the primes $p \leq N^c$, with*

$$\frac{1}{N} \sum_{a \bmod N} |S_f(ap) - g(p)S_f(a)|^2 \leq B_1 \frac{N}{M} \quad (p \in \mathcal{A}, p \leq N^c), \quad (25)$$

$$\sum_{\substack{p < N \\ p \notin \mathcal{A}}} \frac{1}{p} \leq \frac{B_2}{\sqrt{\min\{M, \log N\}}}. \quad (26)$$

Then a real Dirichlet character ψ modulo N satisfies

$$\#\{1 \leq n < N : f(n) \neq \psi(n)\} \leq C \frac{N}{\sqrt{M}}.$$

The principal character and the Legendre symbol are the two possibilities for ψ .

Proof. We first state the two published inputs and check the analytic hypothesis of the one that was conditional. Mangerel calls a prime N of A -Littlewood type when every nonprincipal character modulo N has a nonvanishing L -function throughout

$$\Re s > 1 - A \frac{\log \log N}{\log N}, \quad |\Im s| \leq N. \quad (27)$$

For each fixed A , choose N so large that $A \log \log N / \log N < 1/8$. The region in (27) is then contained in $\Re s > 7/8$. Thus Theorem 1.1 establishes its nonvanishing for every such N .

We derive the needed good-prime representation statement directly from [97, Proposition 2.7], keeping its constant parameters independent. Put $G = (\mathbb{Z}/N\mathbb{Z})^\times$, fix $0 < d < \min\{c, 1/2\}$, and put

$C_0 = 1/d$. Choose a constant U sufficiently large for that proposition, allowing dependence on C_0 , with $dU > 2$. Set

$$L = dU, \quad a_0 = \frac{d}{2(\log(2U))^2}, \quad x = N^L, \quad y = N^d, \quad z = N^{a_0}.$$

The source parameters then satisfy

$$u = \frac{\log x}{\log y} = U, \quad v = \frac{\log x}{\log z} = \frac{L}{a_0}, \quad \frac{v}{u} = 2(\log(2U))^2, \quad y \leq N \leq y^{C_0}.$$

Choose a sufficiently small fixed $0 < \eta < (U \log U)^{-2}$, and choose A sufficiently large in terms of η, C_0 . This order of choices ensures all the proposition's parameter conditions. The rough-and-smooth range in its proof also holds for large N : $y \leq \sqrt{x}$, $y \geq z^2$, $y \leq z^{\log \log x}$, and $z \geq \exp(\sqrt{\log x})$.

Choose $M_0 \geq (B_2/\eta)^2$ and $\log N_0 \geq (B_2/\eta)^2$, so that (26) is at most η . Apply the proposition to $\mathcal{A} \cup \{N\}$; adjoining N only accommodates its convention that the missing-prime sum is taken over $p \leq N$, and $N > y$ cannot occur in a represented integer. Its conclusion is that, for each $u_0 \in G$, the number of integers $v_{u_0} \leq x$ representing u_0 modulo N whose prime factors belong to $\mathcal{A} \cap (z, y]$ is at least a constant multiple of

$$\frac{xU^{-2U}}{vN \log x} = \frac{U^{-2U}}{vL} \frac{N^{L-1}}{\log N}.$$

This tends to infinity because $L > 2$. In particular, for all sufficiently large N such a representative exists. Since all of its prime factors exceed N^{a_0} , it has at most $K = \lceil L/a_0 \rceil$ prime factors, counted with multiplicity. We have therefore proved that every $u_0 \in G$ has a representative satisfying

$$v_{u_0} \equiv u_0 \pmod{N}, \quad v_{u_0} \leq N^L, \quad \Omega(v_{u_0}) \leq K, \quad p \mid v_{u_0} \implies p \in \mathcal{A} \cap [2, N^d]. \quad (28)$$

Here Ω counts prime factors with multiplicity. The only analytic condition on N in the imported proposition is (27); it was verified above. Increasing N_0 accounts for all the fixed thresholds. All primes occurring in the representative are covered by (25).

The second input is the uniform real mean-value lower bound of Granville–Soundararajan [98, Theorem 1 and the extension to merely multiplicative functions in the introduction]: there is an absolute $\delta_1 > -2/3$ such that

$$\frac{1}{x} \sum_{n \leq x} h(n) \geq \delta_1 + o(1) \quad (29)$$

uniformly over real multiplicative h with $|h(n)| \leq 1$. In particular, for all sufficiently large x the left-hand side exceeds $-2/3$. The uniformity allows h to depend on N . Mangerel also records this as Lemma 3.2.

We give the remaining finite-group argument explicitly. Put $G = (\mathbb{Z}/N\mathbb{Z})^\times$ and let $Q \subset G$ be its subgroup of squares. On functions on $\mathbb{Z}/N\mathbb{Z}$ use the norm

$$\|V\|_{\text{Fourier}}^2 = \frac{1}{N} \sum_{a \bmod N} |V(a)|^2$$

and the unitary dilation operators $U_r V(a) = V(ar)$ for $r \in G$. Extend the given prime signs completely multiplicatively on integers whose prime factors belong to $\mathcal{A} \cap [2, N^d]$; this is an auxiliary extension of g , not an extra hypothesis on f . For any product $v = p_1 \cdots p_k$ of such primes, a telescoping of the commuting unitary operators gives

$$\|U_v S_f - g(v) S_f\|_{\text{Fourier}} \leq \sum_{j=1}^k \|U_{p_j} S_f - g(p_j) S_f\|_{\text{Fourier}} \leq k \sqrt{B_1 N/M}. \quad (30)$$

For example, the first inequality follows by expanding $U_{p_1} \cdots U_{p_k} - \prod_j g(p_j)$ as the sum of k terms, each containing a single factor $U_{p_j} - g(p_j)$, and applying the triangle inequality. The other factors preserve the norm.

For every $b \in Q$, choose $u \in G$ with $u^2 = b$ and use the representative v_u in (28). Then $v_u^2 \equiv b \pmod{N}$, $\Omega(v_u^2) \leq 2K$, and $g(v_u^2) = 1$. Therefore (30) implies

$$\|U_b S_f - S_f\|_{\text{Fourier}}^2 \leq 4K^2 B_1 N/M \quad (b \in Q). \quad (31)$$

Define $F(0) = 0$ and $F(n) = f(n)$ for the representatives $1 \leq n < N$. Its additive Fourier transform is S_f . With $R_b F(n) = F(b^{-1}n)$, Parseval's identity converts (31) exactly into

$$\sum_{n \bmod N} |R_b F(n) - F(n)|^2 \leq 4K^2 B_1 N/M.$$

Let $P_Q F = |Q|^{-1} \sum_{b \in Q} R_b F$. Averaging a finite unitary group action is an orthogonal projection; directly, expanding the squares and using $P_Q^2 = P_Q = P_Q^*$ gives

$$\frac{1}{|Q|} \sum_{b \in Q} \|R_b F - F\|_2^2 = 2\|F - P_Q F\|_2^2.$$

Consequently

$$\|F - P_Q F\|_2^2 \leq 2K^2 B_1 N/M. \quad (32)$$

The projection is constant on each of the two cosets of Q in G . Let these constants be $r, s \in [-1, 1]$, and put $m = (N - 1)/2$. Since F takes only the values ± 1 on G ,

$$\|F - P_Q F\|_2^2 = m(1 - r^2) + m(1 - s^2).$$

Round r, s separately to their nearer signs, making any choice in a tie, and call the resulting function on G F_0 . The number J of disagreements between F and F_0 is

$$J = \frac{m}{2}(1 - |r|) + \frac{m}{2}(1 - |s|) \leq \frac{1}{2}\|F - P_Q F\|_2^2 \leq K^2 B_1 \frac{N}{M}.$$

There are just four possible rounded functions: $1, -1, \chi_N, -\chi_N$, where χ_N is the Legendre symbol.

The two negative choices are impossible once M_0, N_0 have been increased. Indeed, if $F_0 = -\psi$ for $\psi = 1$ or $\psi = \chi_N$, then $h(n) = f(n)$ or $h(n) = f(n)\chi_N(n)$, respectively, is a real multiplicative function bounded by one, and

$$\frac{1}{N-1} \sum_{n < N} h(n) = -1 + \frac{2J}{N-1} \leq -1 + \frac{2K^2 B_1 N}{M(N-1)}.$$

For instance $M_0 > 12K^2 B_1$ makes this less than $-2/3$ for all sufficiently large N , contradicting (29) at $x = N - 1$. Thus $F_0 = \psi$ is a real character on G . The displayed bound for J proves, in fact, $J \ll_{c, B_1, B_2} N/M$, which implies the asserted published bound $J \ll_{c, B_1, B_2} N/\sqrt{M}$. $\square$

The analytic transfer uses only the finite-height region explicitly required in the published theorem. No complete multiplicativity assumption, density condition stronger than (26), or lower restriction such as $c > 1/4$ has been added. The square-subgroup averaging above is a direct replacement for the source's final Fourier analysis; the sharper intermediate estimate is not counted as a separate published-result transfer.

8 Large first prime nonresidues and gaps between them

For a prime p , write $n_1(p) < n_2(p) < \dots$ for the primes that are quadratic nonresidues modulo p . In particular, p itself is not in this list. Sofos's Theorem 4 in [99] proves a lower bound of order $\log p$ unconditionally, and a lower bound of order $\log p \log \log p$ under GRH, for the simultaneous largeness of $n_1(p)$ and $n_2(p) - n_1(p)$. Its entire conditional conclusion follows here.

Theorem 8.1 (Sofos's conditional large-gap conclusion). *There is an absolute constant $c_0 > 0$ such that*

$$\min\{n_1(p), n_2(p) - n_1(p)\} > c_0(\log p)(\log \log p)$$

for infinitely many primes p .

Proof. We prove the prime sign-pattern estimate used in the argument, including its conductor and uniformity details. All logarithms in this proof are natural. Fix

$$\kappa = \frac{1}{32 \log 2}, \quad y = \kappa(\log x)(\log \log x), \quad k = \pi(y),$$

where x tends to infinity. Assign any signs $\varepsilon_\ell \in \{-1, 1\}$ to the primes $\ell \leq y$. We will count primes $p \in (x, 2x]$ with all $\left(\frac{\ell}{p}\right) = \varepsilon_\ell$, and, for later use, also impose $p \equiv 1 \pmod{4}$.

Put

$$Q = 8 \prod_{\substack{3 \leq \ell \leq y \\ \ell \text{ prime}}} \ell.$$

The quadratic symbol $\left(\frac{\ell}{p}\right)$ on primes $p > y$ is the value at p of a real Dirichlet character modulo Q . Indeed, one can first take the primitive character of fundamental discriminant 8 for $\ell = 2$, and of fundamental discriminant ℓ or 4ℓ for an odd prime ℓ , and then induce it modulo Q . Denote this character by χ_ℓ . Also write χ_{-4} for the character giving the sign of -1 , induced modulo Q .

For a subset S of the primes at most y , set $d_S = \prod_{\ell \in S} \ell$, $\chi_S = \prod_{\ell \in S} \chi_\ell$, and $\varepsilon_S = \prod_{\ell \in S} \varepsilon_\ell$. The empty products are the principal character modulo Q and 1, respectively. On primes coprime to Q , χ_S is the quadratic character of the positive squarefree integer d_S . It is principal precisely when S is empty. Moreover, $\chi_{-4}\chi_S$ is always nonprincipal: its quadratic squareclass is $-d_S$. The corresponding fundamental discriminants all divide Q . This verifies that exactly one of the 2^{k+1} characters in the following expansion is principal.

For x large enough that $x > y$, the weighted number of the desired primes is exactly

$$\begin{aligned} W(x) &= \sum_{x < p \leq 2x} (\log p) \frac{1 + \chi_{-4}(p)}{2} \prod_{\ell \leq y} \frac{1 + \varepsilon_\ell \chi_\ell(p)}{2} \\ &= \frac{1}{2^{k+1}} \sum_{S \subseteq \{\ell \leq y: \ell \text{ prime}\}} \varepsilon_S \sum_{x < p \leq 2x} (\chi_S(p) + \chi_{-4}(p) \chi_S(p)) \log p. \end{aligned} \tag{33}$$

The prime-power contribution to a von Mangoldt sum up to $2x$ is $O(\sqrt{x} \log^2(2x))$, uniformly in its character. Thus Lemma 1.2 gives, for every character ξ in this expansion,

$$\sum_{x < p \leq 2x} \xi(p) \log p = \delta_\xi x + O(x^{7/8} \log^2(3Qx)),$$

where δ_ξ is 1 for the principal character and 0 otherwise. This estimate is valid for the induced characters as well; alternatively the omitted prime factors all divide Q and lie below $y < x$, so they

do not change the displayed prime sum. Every coefficient ε_S has absolute value one. Consequently (33) is

$$W(x) = \frac{x}{2^{k+1}} + O(x^{7/8} \log^2(3Qx)), \quad (34)$$

uniformly over all the choices of signs.

Chebyshev's estimate gives $\log Q \ll y$. The prime number theorem gives

$$k = (\kappa + o(1)) \log x, \quad 2^{k+1} = x^{1/32+o(1)}.$$

The ratio of the error in (34) to its main term is therefore

$$\ll 2^{k+1} x^{-1/8} (\log x + y)^2 = x^{-3/32+o(1)} \longrightarrow 0.$$

In particular every prescribed sign pattern occurs at some prime $p \in (x, 2x]$ with $p \equiv 1 \pmod{4}$, for all sufficiently large x .

Now let r be the largest prime at most $y/2$. Prescribe $\varepsilon_r = -1$ and $\varepsilon_\ell = 1$ at every other prime $\ell \leq y$. For a prime p supplied by the preceding argument, $n_1(p) = r$ and $n_2(p) > y$. The prime number theorem ensures $r = (1 + o(1))y/2$, whence

$$\min\{n_1(p), n_2(p) - n_1(p)\} \geq \min\{r, y - r\} = (1 + o(1))y/2.$$

Since $x < p \leq 2x$, both $\log p / \log x$ and $\log \log p / \log \log x$ tend to one uniformly. Any fixed $c_0 < \kappa/2$, for example $c_0 = \kappa/4$, therefore satisfies the stated strict inequality for every sufficiently large x and the chosen prime p . Taking x through an unbounded sequence proves infinitude. $\square$

The same argument recovers the classical GRH lower order for large cliques in prime Paley graphs, recorded in the published abstract and introduction of [100] and attributed there to [101, Chapter 13]. This is a consequence of the same prime-pattern calculation, not a different analytic input. We specify both common graph conventions.

Corollary 8.2 (The published Paley clique lower order). *For infinitely many primes $p \equiv 1 \pmod{4}$, the Paley graph on $\mathbb{F}_p$, in which distinct vertices a, b are adjacent when $a - b$ is a nonzero square, has a clique of size $\gg \log p \log \log p$. The same lower order holds for the Paley sum graph, in which adjacency means that $a + b$ is a nonzero square.*

Proof. In the sign-pattern construction above choose every $\varepsilon_\ell = 1$. Then every integer $1 \leq n \leq y$ is a square modulo p , since each prime in its factorization is a square modulo p . The set $\{0, 1, \dots, \lfloor y \rfloor\}$ is a clique in the difference graph: each nonzero difference has absolute value at most y , and -1 is a square because $p \equiv 1 \pmod{4}$. For the sum graph, use $\{1, 2, \dots, \lfloor y/2 \rfloor\}$ instead; distinct vertices have sums between 1 and y , and these sums are nonzero modulo p . Both sets have size $\gg \log p \log \log p$. $\square$

The quantified conclusion of Sofos's theorem asserts the existence of some positive constant c_0 ; that entire conclusion has been preserved. This argument does not assert a particular optimal leading constant for Montgomery's least-nonresidue bound, nor the square-logarithm upper bound that requires the sharper GRH error term.

9 Extreme Euler–Kronecker constants of quadratic fields

For a number field K , its Euler–Kronecker constant is

$$\gamma_K = \lim_{s \rightarrow 1} \left(\frac{\zeta'_K}{\zeta_K}(s) + \frac{1}{s-1} \right).$$

For a fundamental discriminant D , the factorization $\zeta_{\mathbb{Q}(\sqrt{D})}(s) = \zeta(s)L(s, \chi_D)$ gives

$$\gamma_{\mathbb{Q}(\sqrt{D})} = \gamma + \frac{L'}{L}(1, \chi_D),$$

where γ is Euler’s constant. Mourtada–Murty [105] proved unconditionally that both signs attain the lower order $\log \log |D| + O(1)$ infinitely often. Their GRH result adds the term $\log \log \log |D|$. We recover that complete conditional lower bound, including the coefficient one on both logarithms and the published $\gg \sqrt{x}$ abundance. For the full statement and proof in an accessible author source, see [106, Chapter 4, Theorem 17]; that chapter is explicitly identified as the work published in [105].

Theorem 9.1 (Mourtada–Murty’s conditional omega conclusions). *There are absolute constants C_+, C_- such that, for every sufficiently large x , there are $\gg \sqrt{x}$ primes $p \leq x$, $p \equiv 1 \pmod{4}$, separately for each sign, such that*

$$\frac{L'}{L}(1, \chi_p) \geq \log \log x + \log \log \log x - C_+,$$

and $\gg \sqrt{x}$ such primes for which

$$-\frac{L'}{L}(1, \chi_p) \geq \log \log x + \log \log \log x - C_-.$$

Consequently the same two lower bounds hold for $\gamma_{\mathbb{Q}(\sqrt{p})}$ and $-\gamma_{\mathbb{Q}(\sqrt{p})}$, after altering the constants.

Proof. We give the full averaging argument. Let X tend to infinity, and put

$$\kappa = \frac{1}{32 \log 2}, \quad y = \kappa(\log X)(\log \log X), \quad Z = (\log X)^{32}, \quad k = \pi(y).$$

For sufficiently large X one has $2 < y < Z < X$. For $\epsilon \in \{-1, 1\}$ let $\mathcal{P}_\epsilon$ consist of the primes $p \in (X, 2X]$ satisfying $p \equiv 1 \pmod{4}$ and

$$\left(\frac{\ell}{p} \right) = \epsilon \quad \text{for every prime } \ell \leq y.$$

Write $W_\epsilon = \sum_{p \in \mathcal{P}_\epsilon} \log p$. The prime-pattern computation (33)–(34) gives

$$W_\epsilon = \frac{X}{2^{k+1}} + O\left(X^{7/8} \log^2(3QX)\right), \quad Q = 8 \prod_{\substack{3 \leq \ell \leq y \\ \ell \text{ prime}}} \ell. \quad (35)$$

Indeed, the characters in the projector are the quadratic characters of the squareclasses d_S and $-d_S$, where $d_S = \prod_{\ell \in S} \ell$ and S runs through subsets of the primes at most y . Exactly the empty positive squareclass is principal. Their primitive conductors divide Q . The prime number theorem and Chebyshev’s bound give

$$2^{k+1} = X^{1/32+o(1)}, \quad \log Q \ll y.$$

In particular $W_\epsilon \geq X/2^{k+2} > 0$ for all sufficiently large X .

We first justify a sufficiently short expansion of the logarithmic derivative. For every $p \in (X, 2X]$, Lemma 1.2 and partial summation imply

$$-\frac{L'}{L}(1, \chi_p) = \sum_{n \leq Z} \frac{\Lambda(n) \chi_p(n)}{n} + O\left(Z^{-1/8} \log^2(3pZ)\right) = \sum_{n \leq Z} \frac{\Lambda(n) \chi_p(n)}{n} + o(1), \quad (36)$$

uniformly in these primes. To check the first identity directly, the same estimate for $\psi(t, \chi_p)$ shows that the series $\sum_n \Lambda(n) \chi_p(n)/n$ converges. Its tail beyond Z is

$$-\frac{\psi(Z, \chi_p)}{Z} + \int_Z^\infty \frac{\psi(t, \chi_p)}{t^2} dt \ll Z^{-1/8} \log^2(3pZ).$$

Abel's theorem identifies the convergent series with $-L'/L(1, \chi_p)$, by taking real $s \downarrow 1$ in the absolutely convergent Dirichlet series at $s > 1$. The error in (36) is $O((\log X)^{-2})$ with our choice of Z .

For every prime ℓ with $y < \ell \leq Z$, the same projector, now multiplied by the character $p \mapsto (\ell/p)$, gives

$$\sum_{p \in \mathcal{P}_\epsilon} (\log p) \chi_p(\ell) \ll X^{7/8} \log^2(12Q\ell X). \quad (37)$$

There is no principal term: all the resulting squareclasses are ℓd_S or $-\ell d_S$, and the new prime $\ell > y$ occurs to an odd exponent. Their primitive conductors divide $4Q\ell$. All primes dividing these moduli lie below X , so inducing the characters introduces no change in the displayed prime sums. In the normalized projector the sum of the absolute values of the coefficients is one. This proves the claimed uniform bound without a loss of 2^k .

Average (36) over $\mathcal{P}_\epsilon$ with positive weights $(\log p)/W_\epsilon$. Only prime powers occur. For $\ell \leq y$, their character values are exactly ϵ^a at ℓ^a . For $\ell > y$ and even a , their character values are exactly one, since $p > Z$. The total contribution of these even powers is bounded by

$$\sum_{\ell > y} \frac{\log \ell}{\ell^2 - 1} \leq \sum_{n > y} \frac{\log n}{n^2 - 1} \ll \frac{\log y}{y} = o(1).$$

For odd powers of primes $\ell > y$, apply (37). Their combined contribution in absolute value is at most

$$\begin{aligned} & \frac{X^{7/8}}{W_\epsilon} \log^2(12QZX) \sum_{n \leq Z} \frac{\Lambda(n)}{n} \\ & \ll 2^{k+2} X^{-1/8} \log^2(12QZX) \log Z = X^{-3/32+o(1)} = o(1). \end{aligned}$$

Here $\sum_{n \leq Z} \Lambda(n)/n \ll \log Z$ follows by partial summation from Chebyshev's estimate.

Extending the prescribed prime powers from $\ell^a \leq Z$ to all $a \geq 1$ changes the sum by at most

$$\frac{2}{Z} \sum_{\ell \leq y} \log \ell \ll \frac{y}{Z} = o(1).$$

Consequently the exact weighted averages satisfy

$$\frac{1}{W_\epsilon} \sum_{p \in \mathcal{P}_\epsilon} (\log p) \left(-\frac{L'}{L}(1, \chi_p) \right) = \sum_{\ell \leq y} \frac{\epsilon \log \ell}{\ell - \epsilon} + o(1). \quad (38)$$

The classical Mertens estimate $\sum_{\ell \leq y} (\log \ell)/\ell = \log y + O(1)$ and convergence of $\sum_{\ell} (\log \ell)/(\ell(\ell - 1))$ show that the right side of (38) is $\log y + O(1)$ when $\epsilon = 1$, and $-\log y + O(1)$ when $\epsilon = -1$. We retain the abundance assertion in the published conclusion. For either desired sign, let V_p denote that signed value of $L'/L(1, \chi_p)$ and choose the corresponding pattern ϵ . There is an absolute C such that its weighted mean is at least $\log y - C$. The truncation (36) gives the pointwise bound $|V_p| \leq B \log \log X$ for an absolute B and all sufficiently large X . If α is the total normalized weight of primes with $V_p \geq \log y - C - 1$, then

$$\log y - C \leq \alpha B \log \log X + (1 - \alpha)(\log y - C - 1).$$

Thus $\alpha \gg 1/\log \log X$. Since each prime weight before normalization is at most $\log(2X)$, the number of these primes is

$$\gg \frac{W_{\epsilon}}{(\log X)(\log \log X)} \gg \frac{X}{2^{k+2}(\log X)(\log \log X)} = X^{31/32 - o(1)} \gg \sqrt{X}.$$

Finally

$$\log y = \log \log X + \log \log \log X + \log \kappa,$$

Set $X = x/2$. Replacing X by x changes the two iterated logarithms by $o(1)$, and the primes just counted lie below x . This proves both abundance statements and, in particular, infinitude for each sign. The formula for $\gamma_{\mathbb{Q}(\sqrt{p})}$ proves the final assertion. $\square$

The theorem is an omega statement, not an upper bound for all quadratic fields. The full leading terms of the published GRH conclusion have been retained. No particular optimized numerical value of the bounded remainder is asserted.

10 Cyclotomic Euler–Kronecker constants and a second asymptotic coefficient

Write $K_m = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m th root of unity, and define

$$\gamma_m = \lim_{s \rightarrow 1} \left(\frac{\zeta'_{K_m}(s)}{\zeta_{K_m}(s)} + \frac{1}{s-1} \right).$$

Badzayan’s published conditional conclusion [107, Section 2] concerns every positive integer m , including composite conductors. We retain that scope and its full order of magnitude. The second conclusion below is the GRH clause of Ford–Luca–Moree’s Theorem 2 [108].

Theorem 10.1 (Badzayan’s bound). *There is an effective absolute constant C such that, for every integer $m \geq 3$,*

$$|\gamma_m| \leq C \log m \log \log(3m).$$

We prove the sieve estimate needed for the prime-power terms explicitly. This also avoids applying a prime-only Brun–Titchmarsh estimate to a sum containing higher powers.

Lemma 10.2. *For $m \geq 3$, put*

$$\mathcal{M}_m = \{j \in \mathbb{N} : mj + 1 \leq m^{32}, \quad mj + 1 \text{ is a prime power}\}.$$

Uniformly for $1 \leq T \leq m^{31}$,

$$A_m(T) := \#\{j \in \mathcal{M}_m : j \leq T\} \ll \frac{m}{\varphi(m)} \frac{T}{\log(2T)}.$$

Consequently

$$\sum_{j \in \mathcal{M}_m} \frac{1}{j} \ll \frac{m}{\varphi(m)} \log \log(3m).$$

All implied constants are effective and absolute.

Proof. It suffices first to treat large T ; bounded T follows by enlarging the absolute constant. Put $z = T^{1/8}$ and

$$G_m(z) = \sum_{\substack{d \leq z \\ (d, m) = 1}} \frac{\mu^2(d)}{\varphi(d)}.$$

Here μ is the Möbius function. For a squarefree d , the sum of $1/n$ over all positive integers with radical d is $1/\varphi(d)$. Therefore

$$G_m(z) \geq H_m(z) := \sum_{\substack{n \leq z \\ (n, m) = 1}} \frac{1}{n}.$$

Every positive integer factors uniquely as ab , where every prime factor of a divides m and $(b, m) = 1$. Writing $a \mid m^\infty$ for the first condition, we obtain

$$\sum_{n \leq z} \frac{1}{n} = \sum_{a \mid m^\infty} \frac{1}{a} H_m(z/a) \leq H_m(z) \prod_{p \mid m} (1 - p^{-1})^{-1}.$$

In particular

$$G_m(z) \geq \frac{\varphi(m)}{m} \log z. \tag{39}$$

For completeness, the required upper sieve follows by minimizing a finite quadratic form. Use real weights λ_d supported on squarefree $d \leq z$ with $(d, m) = 1$ and $\lambda_1 = 1$. The number of $j \leq T$ for which no prime $p \leq z$, $p \nmid m$, divides $mj + 1$ is at most

$$\sum_{j \leq T} \left(\sum_{d \mid mj+1} \lambda_d \right)^2 = T \sum_{d, e} \frac{\lambda_d \lambda_e}{[d, e]} + O \left(\left(\sum_d |\lambda_d| \right)^2 \right).$$

The progression modulo $[d, e]$ has exactly one allowed residue, since $([d, e], m) = 1$. Using $(d, e) = \sum_{r \mid (d, e)} \varphi(r)$, put $v_r = \sum_{r \mid d} \lambda_d / d$. Then

$$\sum_{d, e} \frac{\lambda_d \lambda_e}{[d, e]} = \sum_r \varphi(r) v_r^2, \quad \lambda_1 = \sum_r \mu(r) v_r.$$

Choose $v_r = \mu(r) / (\varphi(r) G_m(z))$ on the same support. Möbius inversion yields

$$\lambda_d = \frac{\mu(d) d}{\varphi(d) G_m(z)} \sum_{\substack{s \leq z/d \\ (s, dm) = 1}} \frac{\mu^2(s)}{\varphi(s)}.$$

These weights satisfy $\lambda_1 = 1$, have quadratic form $G_m(z)^{-1}$, and obey $|\lambda_d| \leq d/\varphi(d) \leq d$. Thus $\sum |\lambda_d| \ll z^2$, and the sifted count is

$$\ll \frac{m}{\varphi(m)} \frac{T}{\log z} + z^4.$$

If $mj + 1 = p^a$ with $p > z$, it is among these sifted integers. For a fixed prime $p \leq z$ occurring in such a power, one has $p \nmid m$. Let f be its multiplicative order modulo m . Every admissible exponent a is a multiple of f , and $p^f \geq m + 1$. Hence there are at most 32 admissible powers $p^a \leq m^{32}$ for this fixed base p . This bounds the number of small-base contributions by $32\pi(z) \leq 32z$. It is the number of admissible exponents that is bounded here; the exponents themselves need not be at most 32. We conclude that

$$A_m(T) \ll \frac{m}{\varphi(m)} \frac{T}{\log T} + T^{1/2} + T^{1/8} \ll \frac{m}{\varphi(m)} \frac{T}{\log(2T)}.$$

Finally, partial summation, with $V = m^{31}$, gives

$$\sum_{j \in \mathcal{M}_m} \frac{1}{j} = \frac{A_m(V)}{V} + \int_1^V \frac{A_m(t)}{t^2} dt \ll \frac{m}{\varphi(m)} \left(1 + \int_1^V \frac{dt}{t \log(2t)} \right),$$

which is the asserted bound. $\square$

Proof of Theorem 10.1. Define nonnegative coefficients $\Lambda_{K_m}(n)$ by

$$-\frac{\zeta'_{K_m}(s)}{\zeta_{K_m}(s)} = \sum_{n \geq 1} \frac{\Lambda_{K_m}(n)}{n^s} \quad (\Re s > 1).$$

The abelian factorization uses the primitive characters inducing all characters modulo m : $\zeta_{K_m}(s) = \prod_{\chi \bmod m} L(s, \chi^*)$. Exactly one factor is $\zeta(s)$. Summing Lemma 1.2 over these $\varphi(m)$ factors gives

$$\sum_{n \leq t} \Lambda_{K_m}(n) = t + E_m(t), \quad E_m(t) \ll \varphi(m) t^{7/8} \log^2(3mt).$$

Partial summation and the Laurent expansion at 1 now give, for every $Y \geq 2$,

$$\begin{aligned} \gamma_m &= \log Y - \sum_{n \leq Y} \frac{\Lambda_{K_m}(n)}{n} + \frac{E_m(Y)}{Y} - \int_Y^\infty \frac{E_m(t)}{t^2} dt \\ &= \log Y - \sum_{n \leq Y} \frac{\Lambda_{K_m}(n)}{n} + O\left(\varphi(m) Y^{-1/8} \log^2(3mY)\right). \end{aligned} \tag{40}$$

For example, the constant in the first identity is identified by taking real $s \downarrow 1$ in the logarithmic-derivative series; the integrable bound on $E_m(t)/t^2$ justifies that passage. Take $Y = m^{32}$, so the error is $O(1)$. Positivity already gives $\gamma_m \leq 32 \log m + O(1)$.

We bound the positive sum in (40). If $p \nmid m$ has order f modulo m , it splits into $\varphi(m)/f$ prime ideals of norm p^f . Thus its contributions are exactly $\varphi(m) \log p/p^a$ for the exponents with $p^a \equiv 1 \pmod{m}$. By Lemma 10.2, their total is at most

$$\varphi(m) \sum_{j \in \mathcal{M}_m} \frac{\log(mj + 1)}{mj + 1} \leq 32 \log m \frac{\varphi(m)}{m} \sum_{j \in \mathcal{M}_m} \frac{1}{j} \ll \log m \log \log(3m).$$

For a prime dividing m , write $m = p^a u$ with $p \nmid u$. Its ramification index is $\varphi(p^a)$, its residue degree is $f = \text{ord}_u(p)$, with $f = 1$ when $u = 1$, and there are $\varphi(u)/f$ prime ideals above it. Even the sum over all their powers, without the truncation, is

$$\frac{\varphi(u) \log p}{p^f - 1} \leq \log p,$$

because $u \mid p^f - 1$ and $\varphi(u) \leq u$. The contribution of primes dividing m is therefore at most $\sum_{p|m} \log p \leq \log m$. These bounds in (40) prove the claimed two-sided estimate, with an effective absolute constant. $\square$

Corollary 10.3 (Ford–Luca–Moree’s GRH error term). *For an odd prime q , define $e_0(q), e_1(q)$ by the classical asymptotic expansion, with q fixed,*

$$\#\{n \leq x : q \nmid \varphi(n)\} = \frac{x}{(\log x)^{1/(q-1)}} \left(e_0(q) + \frac{e_1(q)}{\log x} + O_q((\log x)^{-2}) \right).$$

Then, as q varies through odd primes,

$$\frac{e_1(q)}{e_0(q)} = \frac{1 - \gamma}{q - 1} + O\left(\frac{\log q \log \log(3q)}{q^2}\right),$$

with an effective absolute implied constant.

Proof. We record the unconditional coefficient identity and its derivation to specify both normalizations. Put $f_p = \text{ord}_q(p)$,

$$S(q) = \sum_{\substack{p \neq q \\ f_p \geq 2}} \frac{\log p}{p^{f_p} - 1}, \quad C(q, s) = \prod_{\substack{p \neq q \\ f_p \geq 2}} (1 - p^{-f_p s})^{(q-1)/f_p}.$$

The Dirichlet series of the counting function is

$$H_q(s) = (1 - q^{-2s}) \zeta(s) (C(q, s) (1 - q^{-s}) \zeta_{K_q}(s))^{-1/(q-1)}.$$

This follows by checking the Euler factors: $q \nmid \varphi(n)$ allows the exponent of q to be at most one and excludes primes $p \equiv 1 \pmod{q}$ from n . Set $\alpha = (q - 2)/(q - 1)$ and $F_q(s) = H_q(s)(s - 1)^\alpha/s$. The unconditional Selberg–Delange coefficient calculation [108, Propositions 1–2] gives $e_0 = F_q(1)/\Gamma(\alpha) > 0$ and $e_1 = F'_q(1)/\Gamma(\alpha - 1)$. Consequently

$$(q - 1) \frac{e_1(q)}{e_0(q)} = -\frac{F'_q(1)}{F_q(1)}.$$

Since $C'(q, 1)/C(q, 1) = (q - 1)S(q)$, logarithmic differentiation of the displayed formula for H_q yields

$$(q - 1) \frac{e_1(q)}{e_0(q)} = 1 - \gamma + \frac{(3 - q) \log q}{(q - 1)^2(q + 1)} + S(q) + \frac{\gamma_q}{q - 1}. \quad (41)$$

Theorem 10.1 bounds the last term. It remains to bound $S(q)$, for which the preceding sieve suffices. Expand $1/(p^{f_p} - 1)$ as a geometric series and split the resulting powers at $Y = q^{32}$. Below Y , the sum is at most

$$\sum_{\substack{n \leq Y \\ n \equiv 1 \pmod{q}}} \frac{\Lambda(n)}{n} \ll \frac{\log q \log \log(3q)}{q}.$$

All terms above Y have exponent at least two. Their contribution is bounded by

$$\sum_{\substack{p^a > Y \\ a \geq 2}} \frac{\log p}{p^a} \ll \frac{\log Y}{\sqrt{Y}}.$$

Indeed, bases $p \leq \sqrt{Y}$ contribute at most $(2/Y) \sum_{p \leq \sqrt{Y}} \log p \ll Y^{-1/2}$ by summing each geometric tail, while bases $p > \sqrt{Y}$ contribute at most $2 \sum_{n > \sqrt{Y}} (\log n)/n^2 \ll (\log Y)/\sqrt{Y}$. It follows that $S(q) \ll q^{-1} \log q \log \log(3q)$. Substitution into (41) proves exactly the stated error term. $\square$

The leading-order existence of the asymptotic expansion is already unconditional. The recovered Ford–Luca–Moree conclusion is its specific uniform error as the prime q varies. No Elliott–Halberstam or prime-tuple conclusions from that paper are asserted here.

11 The maximum quadratic-character bias for products of two primes

Hough proved the following precise asymptotic under GRH [37, Theorem 1.4]. The lower bound was already unconditional; the conditional part was the uniform upper bound when the conductor is allowed to be as large as the counting parameter. We prove that the fixed zero-free strip suffices for the same asymptotic, including its leading constant.

Let $\mathcal{X}(x)$ denote the nonprincipal primitive quadratic Dirichlet characters of conductor at most x . For $\chi \in \mathcal{X}(x)$ of conductor d , and $\eta \in \{-1, 1\}$, put

$$N_d(x) = \#\{(p, q) : p, q \text{ prime}, pq \leq x, (pq, d) = 1\},$$

$$N_{\chi, \eta}(x) = \#\{(p, q) : p, q \text{ prime}, pq \leq x, \chi(p) = \chi(q) = \eta\}, \quad R_{\chi, \eta}(x) = \frac{4N_{\chi, \eta}(x)}{N_d(x)}.$$

Here pairs are ordered, as in the sums in the published proof. The asymptotic below is unchanged if products are counted without ordering.

Theorem 11.1 (Hough’s maximum-bias asymptotic, unconditionally). *For either fixed $\eta \in \{-1, 1\}$,*

$$\max_{\chi \in \mathcal{X}(x)} |R_{\chi, \eta}(x) - 1| \sim \frac{\log \log \log x}{\log \log x} \quad (x \rightarrow \infty).$$

In fact the maximum equals $\{\log \log \log x + O(1)\}/\log \log x$.

Proof. We give the uniform counting argument; this is the point where GRH was used in [37, Section 3]. Write

$$L_2 = \log \log x, \quad L_3 = \log \log \log x, \quad A_\chi(t) = \sum_{p \leq t} \chi(p).$$

All estimates below are for sufficiently large x , uniformly in $d \leq x$. Removing prime powers from Lemma 1.2 and partially summing gives

$$|A_\chi(t)| \ll t^{7/8} \log^2(dt) \quad (t \geq 2). \quad (42)$$

The same argument for ζ gives $\pi(t) = \text{Li}(t) + O(t^{7/8} \log^2(2t))$. We deliberately retain the harmless extra logarithms.

The prime reciprocal series

$$B_\chi = \sum_p \frac{\chi(p)}{p}$$

converges by (42). The Euler product and the absolutely convergent contribution of higher prime powers give

$$B_\chi = \log L(1, \chi) + O(1), \quad |B_\chi| \leq L_3 + O(1),$$

where the latter estimate follows from the two-sided bound in Theorem 1.4. The constants are uniform, including the finitely many small conductors. Partial summation also gives

$$\sum_{p > \sqrt{x}} \frac{\chi(p)}{p} \ll x^{-1/16} \log^2 x = o(1). \quad (43)$$

To see the uniformity in the infinite tail, bound $\log(dt) \leq \log x + \log t$ and integrate $t^{-9/8}(\log x + \log t)^2$ from $\sqrt{x}$ to infinity.

First control the denominator without discarding ramified primes. The hyperbola decomposition and the above prime-number theorem yield

$$N_1(x) = 2 \sum_{p \leq \sqrt{x}} \pi(x/p) - \pi(\sqrt{x})^2 = \frac{2x}{\log x} (L_2 + O(1)).$$

For completeness, the aggregate prime-number-theorem error here is at most

$$x^{7/8} \log^2 x \sum_{n \leq \sqrt{x}} n^{-7/8} \ll x^{15/16} \log^2 x = o(x/\log x).$$

In the main term, replacing $\text{Li}(x/p)$ by $x/\{p \log(x/p)\}$ costs $O(xL_2/\log^2 x)$, and replacing $\log(x/p)$ by $\log x$ costs $O(x/\log x)$ since $\sum_{p \leq \sqrt{x}} \log p/p \ll \log x$. Mertens' estimate then gives the displayed formula for N_1 .

We have the uniform elementary bound

$$\sum_{p|d} \frac{1}{p} \leq \log \log \log(8d) + O(1).$$

Indeed, for d large split at $z = \log d$. Mertens' estimate controls the primes up to z , while there are at most $\log d/\log z$ prime divisors larger than z , whose total reciprocal contribution is at most $1/\log z$. Small d is absorbed in the constant. Every excluded pair contains a prime dividing d . For such primes $p \leq \sqrt{x}$, use $\pi(x/p) \ll x/(p \log x)$; for larger $p \mid d$, use $\pi(x/p) \leq \sqrt{x}$ and $\omega(d) \ll \log x$. Hence

$$N_d(x) = \frac{2x}{\log x} (L_2 + O(1 + L_3)). \quad (44)$$

In particular this denominator is positive for all sufficiently large x , uniformly over the conductors in question.

Let

$$T_\chi(x) = \sum_{\substack{pq \leq x \\ (pq, d)=1}} \chi(p), \quad U_\chi(x) = \sum_{pq \leq x} \chi(p)\chi(q),$$

with all variables prime. Put $\pi_d(t) = \#\{p \leq t : p \nmid d\}$. The exact hyperbola identity is

$$T_\chi(x) = \sum_{p \leq \sqrt{x}} \chi(p) \pi_d(x/p) + \sum_{\substack{q \leq \sqrt{x} \\ q \nmid d}} A_\chi(x/q) - A_\chi(\sqrt{x}) \pi_d(\sqrt{x}).$$

By (42), the last two terms are $O(x^{15/16} \log^2 x)$. Replacing π_d by π in the first sum costs at most $\omega(d)\pi(\sqrt{x})$, which is $O(\sqrt{x} \log x)$. Applying the prime-number theorem to that sum and using the same aggregate error as above, we obtain

$$T_\chi(x) = \sum_{p \leq \sqrt{x}} \chi(p) \operatorname{Li}(x/p) + O(x^{15/16} \log^2 x).$$

The same two main-term replacements as for N_1 , now with $|\chi(p)| \leq 1$, and (43), give

$$T_\chi(x) = \frac{x}{\log x} (B_\chi + O(1)). \quad (45)$$

Similarly,

$$U_\chi(x) = 2 \sum_{p \leq \sqrt{x}} \chi(p) A_\chi(x/p) - A_\chi(\sqrt{x})^2 \ll x^{15/16} \log^2 x + x^{7/8} \log^4 x = o(x/\log x).$$

On pairs coprime to d , expanding $(1 + \eta\chi(p))(1 + \eta\chi(q))$ gives the exact identity

$$4N_{\chi,\eta}(x) = N_d(x) + 2\eta T_\chi(x) + U_\chi(x).$$

Using (44) and (45) yields

$$R_{\chi,\eta}(x) - 1 = \frac{\eta B_\chi + O(1)}{L_2 + O(1 + L_3)} = \frac{\eta B_\chi + O(1)}{L_2}.$$

The last error is uniform because $|B_\chi| \ll 1 + L_3$ and $(1 + L_3)^2/L_2 = o(1)$. Thus the maximum in the theorem is at most $(L_3 + O(1))/L_2$.

For the reverse bound, the unconditional Corollary 2.2 of [37], derived there from the large-value theorem of Granville and Soundararajan, supplies primitive quadratic characters of conductor at most x with $B_\chi \geq \log \log \log x - O(1)$. Applying the uniform formula just proved gives the matching lower bound for either fixed sign η . No GRH input is used in that large-value statement.

Finally, passing from ordered pairs to unordered prime products changes each count by half its diagonal contribution, of size at most $\pi(\sqrt{x})$. Since $N_d(x) \asymp xL_2/\log x$, the resulting change in the normalized ratio is $O(x^{-1/2}/L_2)$, which is negligible. $\square$

Scope of the transfer. The assertion is Hough's published maximum-bias asymptotic. The uniform formula in the proof is included to verify its dependence on the conductor and on primes dividing it. It does not establish the usual GRH-based limiting distributions for ordinary prime-number races, which depend on zeros on the critical line and often on additional independence hypotheses.

12 Littlewood's orders of magnitude on the line $\Re s = 1$

The assertions below are the qualitative orders of magnitude in the classical RH-conditional bounds of Littlewood. For the reciprocal, see J. E. Littlewood, *Mathematical Notes (5): On the Function $1/\zeta(1+ti)$* , *Proc. London Math. Soc.* (2) **27** (1928), 349–357, [doi:10.1112/plms/s2-27.1.349](https://doi.org/10.1112/plms/s2-27.1.349). The logarithmic-derivative assertion and its historical RH dependence are recorded in the introduction to A. Chirre, M. Valås Hagen and A. Simonič, *Conditional estimates for the logarithmic derivative of Dirichlet L -functions*, *Indag. Math.* **35** (2024), 14–27, [doi:10.1016/j.indag.2023.07.005](https://doi.org/10.1016/j.indag.2023.07.005). We recover the orders of magnitude, not the sharper numerical leading constants available under RH.

Theorem 12.1. *There is an effective absolute constant C such that, for $|t| \geq 3$,*

$$|\zeta(1+it)| \leq C\ell(|t|), \quad \frac{1}{|\zeta(1+it)|} \leq C\ell(|t|), \quad \left| \frac{\zeta'}{\zeta}(1+it) \right| \leq C\ell(|t|).$$

Here ℓ is the positive modified iterated logarithm defined in Section 1.

Proof. Complex conjugation reduces the problem to positive t . It suffices to work with large t , since on any remaining compact segment of $\Re s = 1$ bounded away from its pole the functions in question are continuous and nonzero where appropriate, by Theorem 1.1. Put

$$\kappa = \frac{1}{32}, \quad y = (\log t)^{64}, \quad s = 1 + it.$$

We first justify two bounds on a horizontal strip at height comparable to t :

$$|\log \zeta(\sigma + i\tau)| + \left| \frac{\zeta'}{\zeta}(\sigma + i\tau) \right| \ll \log t \quad \left(\frac{31}{32} \leq \sigma \leq 2, \quad \frac{t}{2} \leq \tau \leq \frac{3t}{2} \right). \quad (46)$$

The logarithm is continued from its Euler-product value on $\Re s > 1$. For large t , disks of radius $35/32$ centered at $2 + i\tau$ lie in $\Re s > 7/8$, avoid the pole, and have imaginary parts comparable to t . The classical polynomial growth bound for ζ gives $\Re \log \zeta = \log |\zeta| \ll \log t$ on these disks, while the Euler series gives $|\log \zeta(2 + i\tau)| \ll 1$ at their centers. Borel–Carathéodory bounds the logarithm on the concentric disks of radius $17/16$ by $O(\log t)$. These inner disks contain the needed horizontal segments together with a fixed neighborhood. Cauchy’s estimate on circles of radius $1/64$ then gives the derivative bound in (46). All radii are fixed and all constants effective.

For $F = \log \zeta$ and $F = -\zeta'/\zeta$, Mellin inversion and absolute convergence on $\Re w = 1$ give, respectively,

$$\sum_{n \geq 2} \frac{\Lambda(n)e^{-n/y}}{n^s \log n} = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \log \zeta(s+w) \Gamma(w) y^w dw, \quad (47)$$

$$\sum_{n \geq 2} \frac{\Lambda(n)e^{-n/y}}{n^s} = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} -\frac{\zeta'}{\zeta}(s+w) \Gamma(w) y^w dw. \quad (48)$$

Truncate the integrals at $|\Im w| = t/2$ and shift the finite contour to $\Re w = -\kappa$. Throughout the shifted rectangle, $s+w$ has imaginary part between $t/2$ and $3t/2$. Thus the pole of ζ at $s+w = 1$, which would occur at $w = -it$, is outside the rectangle; no singularity of $\log \zeta$ is crossed. Theorem 1.1 also excludes all zeros there. The only crossed pole is the simple pole of $\Gamma(w)$ at $w = 0$, with residue 1.

Stirling’s formula bounds the two omitted tails on $\Re w = 1$, and the two horizontal sides, by $O(yt^2 e^{-\pi t/4} \log t)$. The precise power of t is immaterial here. The new vertical side is, by (46),

$$\ll y^{-\kappa} \log t \int_{-\infty}^{\infty} |\Gamma(-\kappa + iv)| dv \ll \frac{1}{\log t},$$

since $y^{-\kappa} = (\log t)^{-2}$ and $-\kappa$ is not a pole of Γ . Consequently

$$\log \zeta(1+it) = \sum_{n \geq 2} \frac{\Lambda(n)e^{-n/y}}{n^{1+it} \log n} + O(1), \quad (49)$$

$$-\frac{\zeta'}{\zeta}(1+it) = \sum_{n \geq 2} \frac{\Lambda(n)e^{-n/y}}{n^{1+it}} + O(1). \quad (50)$$

The unconditional Mertens estimate and the Chebyshev bound $\sum_{n \leq u} \Lambda(n) \ll u$, followed by summation by parts, imply

$$\sum_{n \geq 2} \frac{\Lambda(n)e^{-n/y}}{n \log n} \leq \log \log y + O(1), \quad \sum_{n \geq 2} \frac{\Lambda(n)e^{-n/y}}{n} \ll \log y.$$

For the first bound, the portion $n \leq y$ is bounded by the unsmoothed Mertens sum; the remaining portion is $O(1)$ by the same partial summation. For the second bound, the initial portion is $O(\log y)$ and the exponentially weighted tail is $O(1)$. Taking real parts in (49), with both signs, and then exponentiating proves the first two assertions, because $\log y = 64 \log \log t$. The triangle inequality in (50) proves the third assertion. $\square$

Corollary 12.2. *For every primitive nonprincipal Dirichlet character modulo q ,*

$$\left| \frac{L'}{L}(1, \chi) \right| \ll \ell(q).$$

Proof. Lemma 1.2 and partial summation give the convergent expansion

$$-\frac{L'}{L}(1, \chi) = \sum_{n \leq y} \frac{\Lambda(n)\chi(n)}{n} + O(y^{-1/8} \log^2(qy)).$$

Take $y = (\log(3q))^{24}$. The error is bounded, while the absolute value of the finite sum is at most $\sum_{n \leq y} \Lambda(n)/n \ll \log y$. This is $O(\ell(q))$. The order of magnitude is the one previously obtained under GRH in the logarithmic-derivative literature just cited. $\square$

13 The asymmetric tails of cubic L -values

Put $K = \mathbb{Q}(\omega)$, where $\omega^2 + \omega + 1 = 0$. In this section $\mathcal{F}_3(X)$ is the family of primitive Dirichlet characters of exact order three, conductor at most X , and conductor *coprime to three*. This is precisely the family defined in [10, Section 2, (2.1)]. In particular it does not include characters whose conductors are divisible by nine. Write $\log_j$ for the j -fold iterated logarithm. Define

$$\phi_X(t) = \frac{\#\{\chi \in \mathcal{F}_3(X) : |L(1, \chi)| > e^\gamma t\}}{|\mathcal{F}_3(X)|}, \quad \psi_X(t) = \frac{\#\{\chi \in \mathcal{F}_3(X) : |L(1, \chi)| < (\zeta(3)e^{-\gamma})^{1/2}/t\}}{|\mathcal{F}_3(X)|}.$$

The constants in the following theorem are

$$2C_+ = \int_0^1 \frac{2e^{2u} - 2e^{-u}}{u(e^{2u} + 2e^{-u})} du - \int_1^\infty \frac{6}{u(e^{3u} + 2)} du,$$

$$C_- = \int_0^1 \frac{2e^u - 2e^{-2u}}{u(e^{-2u} + 2e^u)} du - \int_1^\infty \frac{3e^{-2u}}{u(e^{-2u} + 2e^u)} du.$$

They are the source's $C_{\max}$ and $C_{\min}$, respectively.

Theorem 13.1 (Darbar–David–Lalín–Lumley, Theorem 1.4). *Fix $C > 0$. For sufficiently large X and $e^{10} \leq A \leq (\log_2 X)^C$, uniformly in the source's range*

$$1 \leq t \leq \log_2 X + \log_3 X - \log_2 A - 37 + C_+ + o(1),$$

one has

$$\phi_X(t) = \exp \left\{ -\frac{2e^{t-C_+}}{t} \left(1 + O_C(t^{-1/2} + A^{-1}) \right) \right\}.$$

Similarly, uniformly for

$$1 \leq t \leq (\log_2 X + \log_3 X - \log_2 A - 37 + C_- + o(1))^{1/2},$$

one has

$$\psi_X(t) = \exp \left\{ -\frac{e^{t^2-C_-}}{t^2} \left(1 + O_C(t^{-1/2} + A^{-1}) \right) \right\}.$$

These conclusions require no GRH assumption. The $o(1)$ in the ranges may be taken to be zero; allowing the usual vanishing endpoint adjustment gives exactly the published formulation.

The proof uses the finite-order Hecke part of the supplied theorem over K , in addition to its Dirichlet part. We replace the conditional character averages and moment comparisons in [10, Section 6]. Their numerical auxiliary error exponents are not asserted here.

Lemma 13.2 (Uniform finite-order Hecke sums). *For positive integers m that are not cubes,*

$$S(X; m) := \sum_{\chi \in \mathcal{F}_3(X)} \chi(m) \ll X^{15/16} \exp\{c(\log(3mX))^{3/4}\}.$$

The constant c and the implied constant are absolute and effective.

Proof. First let η be any nonprincipal finite-order Hecke character of K with a chosen modulus of norm Q . (For a primitive character this is its conductor; for an induced character the omitted Euler factors are included in this modulus.) On $\sigma \geq 15/16$, uniformly in v , we have

$$|\log L(\sigma + iv, \eta)| \ll (\log(3Q(3 + |v|)))^{3/4}. \quad (51)$$

Here the logarithm is the branch continued horizontally from the absolutely convergent Euler product. To verify the assertion, the zero-free half-plane $\Re s > 7/8$, the usual polynomial growth of this fixed-degree L -function, and Borel–Carathéodory on discs centered at $2 + iv$ give $|\log L(s, \eta)| \ll \log(3Q(3 + |\Im s|))$ on $\Re s \geq 57/64$. This bound also follows for an induced character by including its omitted Euler factors. Set $H = \log(3Q(3 + |v|))$ and $Y = H^{10}$. Mellin inversion and a shift to $\Re w = -3/64$ give

$$\log L(s, \eta) = \sum_{\mathfrak{p}, k \geq 1} \frac{\eta(\mathfrak{p})^k}{k(N\mathfrak{p})^{ks}} e^{-(N\mathfrak{p})^k/Y} + O(Y^{-3/64}H).$$

The exponential decay of $\Gamma(w)$ justifies the shift and its tails; only its pole at zero is crossed. The absolute value of the displayed sum is $O(1 + Y^{1/16})$: the number of ideals of K of norm at most u is $O(u)$, and the prime-power coefficients are at most one. Thus the two bounds are $O(H^{5/8})$ and $O(H^{17/32})$. This proves (51), with room to spare.

For the cubic residue character $\eta_m(\mathfrak{a}) = (m/\mathfrak{a})_3$, the conductor divides $(9m)$, so $Q \ll m^2$. This character is nonprincipal if m is not a cube: a rational number that is a cube in the quadratic field K is already a rational cube. The standard cubic reciprocity construction, including primes over three, is the construction used in [10, Section 3 and Lemma 6.2].

Let d be a positive rational integer. Truncated Perron inversion for

$$L(s, \eta_m) \prod_{\mathfrak{p}|d} (1 - \eta_m(\mathfrak{p})(N\mathfrak{p})^{-s})$$

and a shift to 15/16 show that its coefficients satisfy

$$\left| \sum_{\substack{Na \leq Z \\ (a,d)=1}} \eta_m(\mathfrak{a}) \right| \ll 4^{\omega(d)} Z^{15/16} \exp\{c(\log(3mX))^{3/4}\}, \quad 1 \leq Z \leq X.$$

For completeness, take the Perron endpoint to be a half-integer with the same floor as Z and a height of order $(3mX)^4$. The coefficients in absolute value are bounded by the ideal-counting coefficients, which are at most the ordinary divisor function. The truncation error is therefore $O(1)$ after a harmless fixed enlargement of the height. Equation (51) bounds the shifted vertical integral, and the horizontal integrals are smaller. At most two prime ideals lie over each rational prime, accounting for $4^{\omega(d)}$. These details avoid any inference of a Lindelöf bound on the critical line.

The unconditional Möbius decomposition in [10, (3.3), equivalently (6.1)] removes square factors and rational prime divisors from the primary Eisenstein integers that parameterize the family. In absolute value it bounds $S(X; m)$ by a constant times the sum of the preceding estimate with $Z = X/(d^2(N\mathfrak{l})^2)$, over $d \geq 1$ and ideals $\mathfrak{l}$. Both majorants converge:

$$\sum_{d \geq 1} \frac{4^{\omega(d)}}{d^{15/8}} < \infty, \quad \sum_{\mathfrak{l}} (N\mathfrak{l})^{-15/8} < \infty.$$

The coprimality restrictions can be discarded in this upper bound. This proves the lemma. $\square$

The exact random model. Let $\mathbb{X}(p)$ be independent, taking $1, \omega, \omega^2$ with equal probabilities if $p = 3$ or $p \equiv 2 \pmod{3}$. For $p \equiv 1 \pmod{3}$, put

$$\mathbb{P}(\mathbb{X}(p) = 0) = \frac{2}{p+2}, \quad \mathbb{P}(\mathbb{X}(p) = \omega^j) = \frac{p}{3(p+2)} \quad (0 \leq j < 3).$$

Write $\alpha_p = 1$ in the first case and $p/(p+2)$ in the second, and $L_y(\chi) = \prod_{p \leq y} (1 - \chi(p)/p)^{-1}$, with the analogous random product $L_y(\mathbb{X})$. The unconditional counting formula [10, Proposition 2.1] says

$$\frac{S(X; m)}{|\mathcal{F}_3(X)|} = \prod_{p|m} \alpha_p + O_\epsilon(3^{\omega(m)} X^{-3/8+\epsilon}) \quad (m \text{ a cube}), \quad |\mathcal{F}_3(X)| \asymp X. \quad (52)$$

We use its unconditional exponent 5/8 before normalization, not its separate conditional improvement.

Lemma 13.3 (Moments with room at the published endpoint). *Put $L = \log X$, $\ell = \log_2 X$, $y = A^4 L \ell$, and $r_0 = e^{-37} L \ell / \log A$. Uniformly for $|r| \leq 4r_0$,*

$$\frac{1}{|\mathcal{F}_3(X)|} \sum_{\chi} |L_y(\chi)|^{2r} = \mathbb{E} |L_y(\mathbb{X})|^{2r} (1 + O_C(X^{-1/32})).$$

Proof. An exact four-point interpolation makes all supports finite. For a fixed prime put

$$a = (1 - 1/p)^{-2r}, \quad b = (1 + 1/p + 1/p^2)^{-r}, \quad c_0 = (a + 2b)/3.$$

On $w \in \{0, 1, \omega, \omega^2\}$ one has

$$|1 - w/p|^{-2r} = 1 + \frac{a-b}{3}(w + w^2) + (c_0 - 1)w^3.$$

Expanding the product produces coefficients c_m , with each prime exponent at most three. Thus every m in its support has $\log m \leq 3\vartheta(y) \ll y$. Its random expectation is exactly the sum over cube m , weighted by $\prod_{p|m} \alpha_p$.

Here is a uniform bound on the total absolute coefficient mass, including the factors $3^{\omega(m)}$ in (52). Let

$$E_p = 1 - \alpha_p + \alpha_p c_0, \quad B_p = 1 + 2|a - b| + 3|c_0 - 1|, \quad R = |r| + 1.$$

Then $c_0 \geq 1/3$ (use $a \geq 1$ for $r \geq 0$ and $b \geq 1$ for $r \leq 0$), and $\alpha_p \geq 7/9$. Consequently $B_p/E_p \leq 32$. If $p > 4R$, elementary exponential inequalities give $|a - 1| \leq 6R/p$, $|b - 1| \leq 4R/p$, and $E_p \geq e^{-3R/p}$. Hence $B_p/E_p \leq e^{40R/p}$. It follows, uniformly when $4R < y$, that

$$\log \frac{\sum_m 3^{\omega(m)} |c_m|}{\mathbb{E}|L_y(\mathbb{X})|^{2r}} \leq \pi(4R) \log 32 + 40R \sum_{4R < p \leq y} \frac{1}{p}.$$

This is $o(L)$ if $R \leq \sqrt{L}$. Otherwise the effective prime number theorem bounds it, for sufficiently large X , by

$$\frac{200R}{\log(4R)} + 40R \log \frac{\log y}{\log(4R)}.$$

Both terms increase over the relevant interval up to $R = 4r_0 + 1$; for the second the derivative is $\log(\log y / \log(4R)) - 1/\log(4R) > 0$, using the actual margin $y/(4R) > e^2$ and $\log(4R) > 1$. At that endpoint $\log y - \log(4R) \leq 8 \log A$ and $\log(4R) \geq \ell/2$. Substitution gives an upper bound $(3000e^{-37} + o(1))L < L/1000$. All these estimates hold uniformly for the stated range of A ; C is fixed.

Lemma 13.2 bounds every noncube term by $X^{15/16+o_C(1)}$, since $y = L\ell^{O_C(1)}$ and $(\log(3mX))^{3/4} = o_C(L)$. The cube terms use (52). Dividing by the positive random moment, the two relative errors are at most $X^{-1/16+1/1000+o_C(1)}$ and $X^{-3/8+\epsilon+1/1000}$, respectively. This proves the assertion. $\square$

Lemma 13.4 (Discarding a small set in the Euler-product truncation). *For all but $O_C(X^{1-1/2000})$ members of $\mathcal{F}_3(X)$,*

$$L(1, \chi) = L_y(\chi) \left(1 + O_C \left(\frac{1}{A\ell} \right) \right).$$

Proof. The Dirichlet prime-sum estimate already proved in this record gives, by partial summation, the uniform truncation $L(1, \chi) = L_z(\chi)(1 + O(L^{-2}))$ at $z = L^{32}$. For large X , $y < z$ and $L^{-2} = o_C((A\ell)^{-1})$. Split $(y, z]$ into intervals $(u, 2u]$, truncated at z if necessary, where $u = 2^j y$ and $0 \leq j \ll \ell$.

For each integer $k \geq 1$, expansion of an even moment and Lemma 13.2 give

$$\begin{aligned} \sum_{\chi \in \mathcal{F}_3(X)} \left| \sum_{u < p \leq \min(2u, z)} \frac{\chi(p)}{p} \right|^{2k} &\ll X \left(\frac{32k}{u \log u} \right)^k \\ &+ X^{15/16} e^{c(\log X + 3k \log z)^{3/4}} \left(\sum_{u < p \leq 2u} \frac{1}{p} \right)^{2k}. \end{aligned}$$

To justify the cube part without a combinatorial estimate on multinomial coefficients, take independent uniform cubic roots ξ_p . Its sum is exactly the moment of $\sum \xi_p/p$. The real and imaginary parts are centered bounded independent sums. The elementary exponential bound for such sums gives $\mathbb{P}(|\sum \xi_p/p| > v) \leq 4 \exp(-v^2/(4 \sum p^{-2}))$. Integrating this bound yields at most

$4 \cdot 4^k k! (\sum p^{-2})^k \leq (16k \sum p^{-2})^k$. Use $\sum_{u < p \leq 2u} p^{-2} \leq 2/(u \log u)$ for large u . The noncube part has $m \leq z^{3k}$, which proves its displayed bound.

Set $D_j = 5A2^{j/3}$ and $k = \lfloor L/(1000 \log D_j) \rfloor$. Markov's inequality, with threshold $2^{-j/6}/(A\ell)$, bounds the cube contribution to the exceptional count by

$$X \left(\frac{32kA^2 2^{j/3} \ell^2}{u \log u} \right)^k \leq XD_j^{-k} \leq X^{1-1/1100}$$

for sufficiently large X . For the other contribution, $\sum_{u < p \leq 2u} p^{-1} \leq 2 \log 2 / \log u$ and $\log u \geq \ell/2$. Thus its Markov factor is at most $D_j^{2k} \leq X^{2/1000}$, while the exponential in the preceding display is $X^{oc(1)}$. This contribution is $O(X^{19/20})$. Summing over $O_C(\ell)$ intervals leaves $O_C(X^{1-1/2000})$ exceptions. Outside them, the geometric sum of the thresholds is less than $10/(A\ell)$. For sufficiently large X , the prime-power error and the initial truncation error are each at most $1/(A\ell)$. Thus, on compatible logarithm branches, $|\log L(1, \chi) - \log L_y(\chi)| \leq 12/(A\ell)$. Exponentiation proves the lemma, with for example the explicit relative-error constant 30 for sufficiently large X . $\square$

Proof of Theorem 13.1. We give the remaining distribution argument to specify exactly the precision needed from the moments. The unconditional random-product calculation [10, Proposition 4.5 and Proposition 6.6] gives, for $1 \ll r < y/4$,

$$\begin{aligned} \log \mathbb{E}(e^{-\gamma} |L_y(\mathbb{X})|)^{2r} &= 2r \log \log r + \frac{2r(C_+ - 1)}{\log r} + O\left(\frac{r}{(\log r)^2} + \frac{r^2}{y \log r}\right), \\ \log \mathbb{E}(\zeta(3)e^{-\gamma} |L_y(\mathbb{X})|^{-2})^r &= r \log \log r + \frac{r(C_- - 1)}{\log r} + O\left(\frac{r}{(\log r)^2} + \frac{r^2}{y \log r}\right). \end{aligned}$$

For either normalized variable W , write $a = 2, C_* = C_+$ in the first case and $a = 1, C_* = C_-$ in the second, and $m_y(r) = \log \mathbb{E}W^{ar}$. The same calculation gives

$$\frac{m'_y(r)}{a} = \log \log r + \frac{C_*}{\log r} + O\left((\log r)^{-2} + \frac{r}{y \log y}\right), \quad 0 \leq m''_y(r) \ll \frac{1}{r \log r}.$$

These derivative assertions do not require differentiating an unspecified error term. They follow from the full-product derivative estimates in [10, Proposition 4.5], then deleting primes above y : their first-derivative contribution is $O(r/(y \log y) + 1/(y^2 \log y))$ by the local Taylor expansion for $p > y > 4r$. An explicit bound, useful at the endpoint, is

$$|m'_\infty(r) - m'_y(r)| \leq \frac{100r}{y \log y} + \frac{100}{y^2 \log y}.$$

Indeed $U_p = \log |1 - \mathbb{X}(p)/p|^{-2}$ satisfies $|U_p| \leq 3/p$ and $|\mathbb{E}U_p| \leq 2/p^3$ for $p > y$. The derivative of its tilted mean is its tilted variance, at most $9/p^2$. Integrate this bound from zero to r (or to $-r$) and sum over $p > y$, using the effective prime number theorem. Each second derivative is a nonnegative variance, so deletion only decreases it. In particular, with $t_r = \exp(m'_y(r)/a)$,

$$t_r = \log r + C_* + O((\log r)^{-1} + r/y).$$

Apply Lemma 13.3 to the corresponding empirical variable on the finite family. Its moments at r and at $r \pm cr/\sqrt{\log r}$ differ from the random moments by relative $O_C(X^{-1/32})$. Tilt its probability

measure by W^{ar} . Taylor's theorem and the displayed second-derivative bound show that, for a sufficiently large fixed B , the tilted probability of

$$|W - t_r| > B/\sqrt{\log r}$$

is $O(\exp(-c_1 r/(\log r)^2)) + O_C(X^{-1/32})$. Indeed apply Markov with increments $\pm c_2 r/\sqrt{\log r}$; the linear term cancels by the definition of t_r , and choosing B relative to the second-derivative constant makes the remaining exponent negative. For large r the interval therefore has tilted probability at least $1/2$.

Here are the inequalities behind this step and the return to the original measure. Put $M_X(r) = \mathbb{E}_X W^{ar}$, where $\mathbb{E}_X$ denotes the uniform empirical average, and let $\mathbb{P}_{X,r}$ have density $W^{ar}/M_X(r)$ with respect to it. For $h > 0$ and $u > 0$,

$$\mathbb{P}_{X,r}(\log W > m'_y(r)/a + u) \leq \frac{M_X(r+h)}{M_X(r)} \exp\{-hm'_y(r) - ah u\}.$$

The lower-tail inequality uses $r-h$ in the numerator and changes the sign of the linear term. For $h \asymp r/\sqrt{\log r}$ and $u \asymp B/(\log r)^{3/2}$, the logarithm of the right side is at most

$$O\left(\frac{h^2}{r \log r}\right) - ah u + O_C(X^{-1/32}),$$

which is negative of order $r/(\log r)^2$ when B is large enough. This proves the asserted concentration, since $t_r \asymp \log r$. If $\delta = B/\sqrt{\log r}$ and $t < t_r - \delta$, it also gives

$$\mathbb{P}_X(W > t) \geq \frac{M_X(r)}{2(t_r + \delta)^{ar}}, \quad \mathbb{P}_X(W > t) \leq \frac{M_X(r)}{t^{ar}}.$$

For the lower bound we choose r with t_r just above $t + \delta$; for the upper bound we choose r with t_r at t to within the same error. The estimates for t_r place both choices at $r = e^{t-C_*}(1 + O(t^{-1/2} + e^t/y))$.

Substituting the formula for $m_y(r)$ in these two bounds gives, uniformly in the required range,

$$\mathbb{P}(W > t) = \exp\left\{-\frac{ae^{t-C_*}}{t} \left(1 + O(t^{-1/2} + e^t/y)\right)\right\}.$$

One can obtain the value at any prescribed t by taking parameters on the two sides of $r = e^{t-C_*}$, with relative changes $O(t^{-1/2} + r/y)$. The range $|r| \leq 4r_0$ in Lemma 13.3 provides room for these changes even at $t = \log r_0 + C_*$. More explicitly, the preceding bound with constant 100 and $r_0/y = e^{-37}/(A^4 \log A)$ show that $t_{2r_0} > \log r_0 + C_* + 0.6$ for sufficiently large X uniformly in A . The remaining shifts tend to zero, so they still lie below $4r_0$. Thus no loss of $\log 4$ in the endpoint is necessary. Bounded t is included by the source's unconditional Theorem 1.3, or by increasing the absolute constants in the stated error terms.

For the second normalized variable the parameter here is t^2 in the notation of the theorem. It gives a relative error $O(t^{-1} + e^{t^2}/y)$, which is stronger than the asserted $O(t^{-1/2} + A^{-1})$. In both cases the extra truncation error e^t/y (respectively e^{t^2}/y) is $O(A^{-4}/\log A)$ at the published endpoint.

Finally Lemma 13.4 changes the tail arguments by a relative $O((A\ell)^{-1})$. Since t (respectively t^2) is $O_C(\ell)$, this changes the exponent by relative $O_C(A^{-1})$. Quantitatively, the logarithm bound $12/(A\ell)$ above changes the large-value argument by at most $30/A$ and the squared small-value argument by at most $60/A$, for sufficiently large X . The discarded proportion is $O_C(X^{-1/2000})$. The modeled tails throughout the stated ranges are at least $X^{-1/10000}$ for large X : at the endpoint their negative logarithms are at most $(3e^{-37}/\log A + o(1)) \log X$. Hence the discarded proportion is negligible even relatively to the tail probability. This proves both assertions. $\square$

Scope of the transfer. The whole published Theorem 1.4 is recovered, including its constants $C_{\pm}$ and its endpoint -37 . The unconditional smaller-range Theorem 1.3 is not counted as a new result. The prime-conductor extreme values in Theorem 1.5 have a different sharp constant and are not asserted here. The proof replaces the source's conditional auxiliary exponents by smaller fixed savings and uses its already-unconditional random-product calculations. In particular it assumes neither a critical-line Lindelöf estimate nor GRH over another number field.

14 The larger quadratic L -value tail range

Let $\mathcal{D}(X)$ consist of the nontrivial fundamental discriminants d with $|d| \leq X$, of either sign, and let χ_d be the associated primitive quadratic character. The trivial discriminant 1, at which the L -function would have a pole, is omitted throughout. Define

$$\Phi_X(t) = \frac{\#\{d \in \mathcal{D}(X) : L(1, \chi_d) > e^{\gamma}t\}}{|\mathcal{D}(X)|}, \quad \Psi_X(t) = \frac{\#\{d \in \mathcal{D}(X) : L(1, \chi_d) \leq \zeta(2)e^{-\gamma}/t\}}{|\mathcal{D}(X)|},$$

and put

$$C_1 = \int_0^1 \frac{\tanh u}{u} du + \int_1^\infty \frac{\tanh u - 1}{u} du.$$

Theorem 14.1 (Granville–Soundararajan, Theorem 4). *For sufficiently large X , uniformly for*

$$e \leq A \leq \log_2 X, \quad 1 \leq t \leq \log_2 X + \log_3 X - \log_2 A - 20,$$

both $F_X = \Phi_X$ and $F_X = \Psi_X$ satisfy

$$F_X(t) = \exp \left\{ -\frac{e^{t-C_1}}{t} \left(1 + O \left(A^{-1} + t^{-1} \right) \right) \right\}.$$

This is the complete larger-range conclusion stated under GRH in [7, Theorem 4], now without that assumption.

We include the uniform estimates and the final concentration argument, in particular the sharper t^{-1} error. The smaller unconditional range in the source is not being counted again.

Proof. Write $L = \log X$, $\ell = \log_2 X$, $K = e^{10}$, and set

$$y = (KA)^4 L\ell, \quad r_0 = e^{-20} L\ell / \log A.$$

The fixed enlargement K makes the Euler-product approximation quantitatively harmless even at the lower endpoint $A = e$.

Averages of quadratic characters. The Dirichlet version of the logarithm and Perron argument in Lemma 13.2 gives, for every nonprincipal character ξ of a chosen modulus q ,

$$\sum_{n \leq Z} \xi(n) \ll Z^{15/16} \exp\{c(\log(3qZ))^{3/4}\}.$$

Indeed the same smoothed logarithm contour at $57/64$, with cutoff $(\log(3q(3 + |v|)))^{10}$, proves $|\log L(\sigma + iv, \xi)| \ll (\log(3q(3 + |v|)))^{3/4}$ on $\sigma \geq 15/16$; the ordinary Dirichlet coefficients are even simpler than the ideal coefficients in that lemma. A modulus, rather than just a primitive conductor, controls the omitted Euler factors.

If n is not a square, expand the squarefree condition in the usual description of fundamental discriminants $d = m$ with squarefree $m \equiv 1 \pmod{4}$, or $d = 4m$ with squarefree $m \equiv 2, 3 \pmod{4}$, allowing both signs. Characters modulo four detect the congruences. The resulting nonzero sums involve nonprincipal quadratic characters of modulus at most $8n$, evaluated on intervals of length at most X/a^2 . They are nonprincipal because the squarefree kernel of n is not one: an odd prime in that kernel cannot be removed by a twist modulo four; if the kernel is two, the character modulo eight cannot be canceled by such a twist. When n is even the even-discriminant terms vanish. Summing over the squarefree-sieve variable a , using $\sum a^{-15/8} < \infty$, proves

$$\sum_{d \in \mathcal{D}(X)} \chi_d(n) \ll X^{15/16} \exp\{c(\log(3nX))^{3/4}\} \quad (n \text{ nonsquare}). \quad (53)$$

For square n , elementary squarefree counting instead gives

$$\frac{1}{|\mathcal{D}(X)|} \sum_d \chi_d(n) = \prod_{p|n} \frac{p}{p+1} + O_\epsilon(3^{\omega(n)} X^{-1/2+\epsilon}), \quad |\mathcal{D}(X)| = \frac{6}{\pi^2} X + O(\sqrt{X}). \quad (54)$$

This is the unconditional square-term formula used in [7, Sections 5–6]; it follows directly by Möbius inversion and inclusion–exclusion at the primes dividing n . Only squarefree $\sqrt{n}$ will be needed below, so its divisor-function error is bounded by the displayed $3^{\omega(n)}$.

Real moments of the short product. Let the independent variables $\mathbb{Y}(p)$ take values $0, 1, -1$ with probabilities $1/(p+1), p/(2p+2), p/(2p+2)$, respectively. Use $L_y(\chi)$ and $L_y(\mathbb{Y})$ for the products up to y . For a real r , put

$$a = (1 - 1/p)^{-r}, \quad b = (1 + 1/p)^{-r}, \quad c_0 = (a + b)/2.$$

The identity

$$(1 - w/p)^{-r} = 1 + \frac{a-b}{2}w + (c_0 - 1)w^2 \quad (w = 0, 1, -1)$$

expands the full product into a finite sum $\sum_n c_n \chi(n)$. Every prime exponent is at most two, hence $\log n \leq 2\vartheta(y)$. Its random expectation is precisely the sum of its square terms, weighted by $\prod_{p|n} p/(p+1)$.

Set $R = |r| + 1$, $\alpha_p = p/(p+1)$, $E_p = 1 - \alpha_p + \alpha_p c_0$, and $B_p = 1 + 3(|a-b|/2 + |c_0 - 1|)$. As $c_0 \geq 1/2$ and $\alpha_p \geq 2/3$, one has $B_p/E_p \leq 32$. For $p > 4R$, the elementary exponential bounds give $|a-1| \leq 3R/p$, $|b-1| \leq 2R/p$, and $E_p \geq e^{-2R/p}$, so $B_p/E_p \leq e^{40R/p}$. As in Lemma 13.3,

$$\log \frac{\sum_n 3^{\omega(n)} |c_n|}{\mathbb{E} L_y(\mathbb{Y})^r} \leq \pi(4R) \log 32 + 40R \sum_{4R < p \leq y} \frac{1}{p}.$$

For $R \leq \sqrt{L}$ this is $o(L)$. For larger $R \leq 4r_0 + 1$, the preceding prime-number-theorem argument bounds it by

$$\frac{200R}{\log(4R)} + 40R \log \frac{\log y}{\log(4R)} \leq (30000e^{-20} + o(1))L < L/1000.$$

For clarity, at the upper endpoint $\log y - \log(4R) \leq 64 \log A$ and $\log(4R) \geq \ell/2$. The two functions of R increase in this interval, since $\log y - \log(4R) > 2$. Substitution yields the last displayed bound. Equations (53) and (54) now prove, uniformly for $|r| \leq 4r_0$,

$$\frac{1}{|\mathcal{D}(X)|} \sum_d L_y(\chi_d)^r = \mathbb{E} L_y(\mathbb{Y})^r (1 + O(X^{-1/32})). \quad (55)$$

Here $y = L\ell^{O(1)}$, so the exponential in (53) is $X^{o(1)}$ throughout the finite support. Both signs of r are covered by the local ratios; no lower bound of one for the negative random moment is assumed.

Removing the long prime tail. The same high-moment argument as in Lemma 13.4, with independent signs in place of cubic roots and $\tilde{A} = KA$, proves

$$|\log L(1, \chi_d) - \log L_y(\chi_d)| \leq \frac{12}{KA\ell} \quad \text{outside } O(X^{1-1/2000}) \text{ discriminants.} \quad (56)$$

Here are the estimates needed for that substitution. Initially truncate uniformly at $z = L^{32}$ using the Dirichlet prime-sum estimate. On an interval $(u, 2u]$ with $u = 2^j y$, expansion and (53) give

$$\sum_d \left| \sum_{u < p \leq \min(2u, z)} \frac{\chi_d(p)}{p} \right|^{2k} \ll X \left(\frac{32k}{u \log u} \right)^k + X^{15/16} e^{c(\log X + 2k \log z)^{3/4}} \left(\sum_{u < p \leq 2u} \frac{1}{p} \right)^{2k}.$$

The square terms are bounded by the moments of independent signs, using the same exponential tail estimate. Take $k = \lfloor L/(1000 \log(5\tilde{A}2^{j/3})) \rfloor$ and threshold $2^{-j/6}/(\tilde{A}\ell)$. The two exceptional counts are at most $X^{1-1/1100}$ and $X^{19/20}$, respectively, for sufficiently large X . Summing the $O(\ell)$ intervals gives the claimed exceptional set. The thresholds sum to less than $10/(\tilde{A}\ell)$; the initial truncation and prime-power errors are each eventually at most $1/(\tilde{A}\ell)$. This proves (56) with its explicit constant.

The tail asymptotic and its t^{-1} error. For the upper and lower tails, respectively, define random variables

$$W_+ = e^{-\gamma} L_y(\mathbb{Y}), \quad W_- = \zeta(2) e^{-\gamma} L_y(\mathbb{Y})^{-1},$$

and the same variables on the finite discriminant family. The unconditional random-product calculations in [7, Section 3, (3.1)–(3.5), (3.10)] give for either sign, writing $m_y(r) = \log \mathbb{E} W_{\pm}^r$,

$$\begin{aligned} m_y(r) &= r \log \log r + \frac{r(C_1 - 1)}{\log r} + O\left(\frac{r}{(\log r)^2} + \frac{r^2}{y \log r}\right), \\ m'_y(r) &= \log \log r + \frac{C_1}{\log r} + O\left((\log r)^{-2} + \frac{r+1}{y \log y}\right), \quad 0 \leq m''_y(r) \ll \frac{1}{r \log r}. \end{aligned}$$

The derivative statements follow from the differentiated local factors, not by formal differentiation of the first error term. For example, the local tilted variance is $O(p^{-2} e^{-r/(2p)})$, since the winning sign has probability bounded away from zero and its logarithm is separated from the other two values by at least $1/(2p)$. Summation proves the second-derivative bound. For the first derivative the source's prime-sum expression $I(r; y)$ gives the stated constant C_1 . To check explicitly the negative normalization, let $E_p^+(r) = \mathbb{E}(1 - \mathbb{Y}(p)/p)^{-r}$. Symmetry of $\mathbb{Y}(p)$ gives the exact local identity

$$(1 - p^{-2})^{-r} \mathbb{E}(1 - \mathbb{Y}(p)/p)^r = E_p^+(r) + \frac{1}{p+1} ((1 - p^{-2})^{-r} - 1).$$

For $p \leq \sqrt{r}$, the added term and its logarithmic derivative are exponentially suppressed relative to the winning sign, since $\log(1 + 1/p) \geq 1/(2p)$. For $p > \sqrt{r}$, differentiating the relative added term bounds its contribution by $O(p^{-3} + rp^{-4})$. Summation is $O(r^{-1/2})$, hence $o((\log r)^{-2})$. The full normalized negative moment therefore has the same first-derivative constant C_1 as the positive moment. Deleting primes above y changes that derivative by at most $100(r+1)/(y \log y)$: use $|\log(1 - \mathbb{Y}(p)/p)^{-1}| \leq 2/p$, its mean $O(p^{-2})$, and tilted variance at most $4/p^2$.

Let $t_r = e^{m'_y(r)} = \log r + C_1 + O((\log r)^{-1} + r/y)$. Tilt the empirical measure by $W_\pm^r$, and apply (55) at r and at $r \pm cr/\log r$. The second-derivative bound and Markov's inequality give, for a sufficiently large fixed B ,

$$\mathbb{P}_r \left(|W_\pm - t_r| > \frac{B}{\log r} \right) \ll \exp \left(-\frac{c_1 r}{(\log r)^3} \right) + X^{-1/32}.$$

In fact, Taylor expansion cancels the linear term at $m'_y(r)$; the increment is $cr/\log r$, and the deviation in $\log W_\pm$ is of order $(\log r)^{-2}$. Both the quadratic term and the favorable linear deviation are therefore of order $r/(\log r)^3$, with the latter larger by the choice of B . More explicitly, write $M_X(s)$ for the empirical moment and put $h = cr/\log r$. If $d > 0$, the upper tilted tail is at most

$$\frac{M_X(r+h)}{M_X(r)} e^{-h(m'_y(r)+d)} \leq (1 + O(X^{-1/32})) \exp \left(\frac{C_0 h^2}{r \log r} - hd \right).$$

The lower tilted tail uses $r - h$ and satisfies the same bound. With $\delta = B/\log r$, both logarithmic distances from t_r to $t_r \pm \delta$ are at least $B/(3(\log r)^2)$ for large r . Choosing $B > 6C_0 c$ makes the exponent negative as asserted. The probability of the complementary interval is at least $1/2$.

Undoing the tilt there, and using ordinary Markov for the other bound, uses the concrete inequalities

$$\mathbb{P}(W_\pm \geq t_r - \delta) \geq \frac{M_X(r)}{2(t_r + \delta)^r}, \quad \mathbb{P}(W_\pm \geq t) \leq \frac{M_X(r)}{t^r}.$$

Inserting the moment expansion and bracketing a prescribed t by the two choices of r gives

$$\mathbb{P}(W_\pm > t) = \exp \left\{ -\frac{e^{t-C_1}}{t} \left(1 + O(t^{-1} + e^t/y) \right) \right\}.$$

The same estimate holds with $\geq$; the interval argument provides both versions without any assumption concerning atoms. The two bracketing parameters differ from e^{t-C_1} by relative $O(t^{-1} + e^t/y)$; all of them lie in $[1, 4r_0]$ in the stated range. In particular at the upper endpoint $e^{t-C_1} = e^{-C_1} r_0$, and the explicit derivative truncation bound above leaves ample room. Bounded t follows from the source's unconditional smaller-range theorem, after increasing the error constant if necessary.

Finally (56) changes the argument by at most $30/(KA)$ for sufficiently large X , which changes the negative logarithm of the modeled tail by relative $O(A^{-1})$. Also $e^t/y \ll e^{-20}/((KA)^4 \log A) \ll A^{-1}$. The modeled tails at the largest permitted t have negative logarithm at most $2e^{-20}L/\log A$ for large X ; here the explicit enlargement $K = e^{10}$ controls the argument shift even when $A = e$. Thus they are at least $X^{-1/10000}$. The discarded proportion $O(X^{-1/2000})$ is negligible relatively to these tails. Substitution proves both conclusions, with exactly the published range and the published error $O(A^{-1} + t^{-1})$. $\square$

Published scope and later work. The 2004 errata [8] correct notation and do not alter this theorem. Darbar–Maiti's 2025 paper [9] on large quadratic L -values still explicitly distinguishes the smaller unconditional range from this larger GRH range. Their extreme-value statements do not replace the present two tail asymptotics. No sharp prime-conductor constant from Granville–Soundararajan's Theorem 5a is inferred here.

15 The first Fourier coefficient of a Maass newform

Hoffstein–Lockhart's Theorem 0.1 [18] gives the bounds below subject to a real zero-free interval for the adjoint L -function. Goldfeld–Hoffstein–Lieman [19] removed that condition for non-dihedral

forms, but retained a weaker level bound for dihedral forms because of possible quadratic Dirichlet exceptional zeros. We recover the entire original conclusion, uniformly over both kinds of forms and over the level and Laplace eigenvalue.

Theorem 15.1 (The full Hoffstein–Lockhart bound). *Let f be a weight-zero Maass newform for $\Gamma_0(N)$ with even Dirichlet nebentype, Laplace eigenvalue $\lambda = 1/4 + t^2$, and normalization*

$$\frac{1}{\text{vol}(\Gamma_0(N)\backslash\mathbb{H})} \int_{\Gamma_0(N)\backslash\mathbb{H}} |f(z)|^2 \frac{dx dy}{y^2} = 1.$$

Define its Fourier coefficients by

$$f(z) = \sum_{n \neq 0} \rho_f(n) |n|^{-1/2} W_t(nz), \quad W_t(x + iy) = (|y| \cosh \pi t)^{1/2} K_{it}(2\pi|y|) e^{2\pi i x}.$$

Let $F = \text{Ad } f$ denote its adjoint lift, with the standard L -function normalized to have first Dirichlet coefficient 1. There are absolute effectively computable constants $c, C > 0$ such that

$$L(1, F) \geq \frac{c}{\log(1 + \lambda N)}, \quad |\rho_f(1)|^2 \leq C \log(1 + \lambda N).$$

Proof. We first isolate the exceptional-zero classification needed here. The proof in [19, pp. 180–181] establishes an absolute effective $c_0 > 0$ such that any real zero of $L(s, F)$ in

$$1 - \frac{c_0}{\log(1 + \lambda N)} < s < 1 \tag{57}$$

must be a zero of a nonprincipal quadratic Dirichlet L -function of conductor at most N . This is an unconditional structural input, not an assertion of GRH for a higher-degree L -function.

Here is the distinction between its two cases. For a non-dihedral f , the positive-coefficient product $\zeta(s)L(s, F)^2 L(s, F \times F)$ has a pole of order two at 1, while a zero of $L(s, F)$ would have multiplicity at least three in it. The positive-coefficient zero-count lemma in [19, p. 178] rules this out in (57). For a dihedral form $\pi = \text{AI}_{K/\mathbb{Q}} \theta$, with K quadratic and nontrivial automorphism σ , the factorization is

$$L(s, F) = L(s, \chi_K) L_K(s, \theta/\theta^\sigma).$$

The second character is inverted by σ . If its square is nontrivial, the usual complex-character zero-free argument rules out a real exceptional zero, with the uniform constants in the cited proof. If its square is trivial, its automorphic induction splits into quadratic Dirichlet characters. The quotient structure is essential here: writing $\psi = \theta/\theta^\sigma$, and taking a lift τ of σ in the global Weil group, one has $\psi(\tau^2) = 1$, since τ commutes with τ^2 . Thus the two extensions of ψ may take τ to $+1$ and -1 , and both have order at most two. These characters have conductor at most N . This is precisely the remaining alternative described on p. 181 of that appendix. The Dirichlet QRH input excludes zeros of all these factors for $s > 7/8$. Since $\lambda \geq 3/16$, decreasing c_0 if necessary puts the interval (57) inside $(7/8, 1)$. Consequently this interval is zero-free for every f .

For completeness we give the positive-coefficient residue argument that converts this zero-free interval into both bounds, including the bad local factors. Put $Q = 1 + \lambda N$, let $a_f(n) = \rho_f(n)/\rho_f(1)$ for $n > 0$, and consider

$$H_1(s) = \zeta(s)L(s, F), \quad H_2(s) = \zeta(2s) \sum_{n \geq 1} \frac{|a_f(n)|^2}{n^s}.$$

The unconditional local and Rankin–Selberg facts recorded in [18, §1, especially Lemma 1.2] are as follows. Each H_j is a Dirichlet series $\sum b_j(n)n^{-s}$ with $b_j(n) \geq 0$ and $b_j(1) = 1$, absolutely convergent for $\operatorname{Re} s > 1$. Each has a meromorphic continuation to $\operatorname{Re} s > 0$ with only a simple pole at 1. For absolute effective A, B, C_0 ,

$$|H_j(1/2 + iv)| \leq C_0 Q^A (1 + |v|)^B.$$

Moreover $H_2(s) = L_N(s)H_1(s)$, where the finite local factor L_N has neither zeros nor poles in the real interval under consideration. Their residues are exactly

$$R_1 = L(1, F), \quad R_2 = \frac{2\pi}{3} |\rho_f(1)|^{-2}. \quad (58)$$

These are the source normalization and its equation (0.5). Both residues are positive, since a Dirichlet series with nonnegative coefficients is positive to the right of its simple real pole.

Choose an absolute A_1 sufficiently large and put $M = Q^{A_1}$, $\delta = 1/\log M$, and $\beta = 1 - \delta$. We may ensure $\beta > 3/4$, $C_0 Q^A \leq M$, and that $[\beta, 1)$ lies in the zero-free interval already obtained. Both H_j are negative on $[\beta, 1)$: this is true just to the left of their pole, and the sign cannot change without a real zero.

Fix an integer $r > B + 2$ and $Y \geq 2$. Mellin inversion gives

$$\frac{1}{2\pi i} \int_{(2)} \frac{H_j(s + \beta) Y^s}{s(s+1) \cdots (s+r)} ds = \frac{1}{r!} \sum_{n \leq Y} b_j(n) n^{-\beta} (1 - n/Y)^r \geq \frac{2^{-r}}{r!}.$$

Shift to $\operatorname{Re} s = 1/2 - \beta$. The crossed poles are $s = \delta$ and $s = 0$. The growth bound and $r > B + 2$ give

$$\frac{2^{-r}}{r!} \leq \frac{R_j Y^\delta}{\delta(1+\delta) \cdots (r+\delta)} + \frac{H_j(\beta)}{r!} + O(MY^{1/2-\beta}).$$

The middle term is negative. Taking $Y = M^{C_1}$ with an absolute sufficiently large C_1 makes the final error less than half the left side, since $1/2 - \beta < -1/4$. Also $Y^\delta = e^{C_1}$. It follows that $R_j \gg \delta \asymp 1/\log Q$, with absolute effective constants. Substituting (58) gives both assertions. $\square$

Scope. The non-dihedral conclusion was already unconditional in 1994 and is included here solely because the published original theorem quantified over all Maass newforms. The removed obstruction is the uniform level dependence for dihedral forms. No zero-free fixed strip for a general adjoint or Rankin–Selberg L -function is claimed.

16 The exponent of imaginary quadratic class groups

For a negative fundamental discriminant D , let $E(D)$ be the exponent of the ideal class group of $K = \mathbb{Q}(\sqrt{D})$: the least positive integer annihilating every ideal class. Boyd and Kisilevsky [70] proved under ERH that $E(D) \rightarrow \infty$. The following recovers that exact qualitative conclusion, and the published order of magnitude recorded in [71, Introduction]. The sharper asymptotic coefficient $1/2$ obtained under ERH is not asserted.

Lemma 16.1 (A small split prime). *There is an effective absolute constant C_1 such that for every negative fundamental discriminant D , some rational prime p satisfies*

$$p \nmid D, \quad \left(\frac{D}{p}\right) = 1, \quad p \leq C_1 (\log(3|D|))^8.$$

Here the symbol is the Kronecker symbol, including at $p = 2$.

Proof. Put $Q = |D|$ and $\chi = \chi_D$. This is a real primitive nonprincipal Dirichlet character modulo Q . Add the principal smoothed sum to (4). The estimates proved there give

$$\sum_{n \leq x} \Lambda(n)(1 + \chi(n))(1 - n/x) = \frac{x}{2} + O(x^{7/8} \log(3Q) + x^{7/8} \log^2(2x) + \log(Qx)).$$

If there were no split prime at most x , all contributions with $n = p$ and $p \nmid D$ would vanish. The terms supported on prime powers with $p \mid D$ are $O(\log(3Q) \log x)$: each such prime contributes at most $2 \log x$, and there are at most $\log Q / \log 2$ such primes. The remaining prime-power terms with exponent at least two have total absolute value $O(\sqrt{x} \log^2(2x))$. Indeed, there are at most $\sqrt{x}$ possible underlying primes, at most $\log x / \log 2$ exponents per prime, and each von Mangoldt weight is at most $\log x$; the slightly sharper stated bound also follows by summing $\sum_{a \geq 2} \psi(x^{1/a})$ and the elementary bound $\psi(t) \ll t$. Consequently the entire left side would be bounded by these two errors.

Take $x = C_1(\log(3Q))^8$. The ratio of the character-zero error to x is $O(C_1^{-1/8})$, while each other displayed error is $o(x)$ as $Q \rightarrow \infty$. Choosing C_1 large gives a contradiction for all sufficiently large Q . The effective estimates determine the threshold; increase C_1 effectively over the finite remaining set. A split prime for each such field can be found by exhaustive search, whose termination follows from the ordinary prime number theorem for arithmetic progressions. This proves the lemma. $\square$

Theorem 16.2 (Boyd–Kisilevsky qualitative conclusion). *As D runs through negative fundamental discriminants,*

$$E(D) \gg \frac{\log |D|}{\log \log |D|} \quad (|D| \geq 16),$$

with an effective absolute implied constant. In particular $E(D) \rightarrow \infty$, and for every fixed positive integer M there are only finitely many imaginary quadratic fields with $E(D) \leq M$. They lie in an effectively computable finite interval of discriminants.

Proof. Choose the split prime p from Lemma 16.1, and write $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ with distinct prime ideals. If e is the order of $[\mathfrak{p}]$ in the class group, then $\mathfrak{p}^e = (\alpha)$ for an algebraic integer α . We have $e \mid E(D)$ and

$$p^e = |N_{K/\mathbb{Q}}(\alpha)|.$$

The element α is not rational. If it were rational, it would be an integer and its valuations at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ would be equal, whereas those of $\mathfrak{p}^e$ are e and 0 . Every algebraic integer of this quadratic field can be written $\alpha = (a + b\sqrt{D})/2$ with $a, b \in \mathbb{Z}$, and $b \neq 0$ here. Therefore

$$p^e = \frac{a^2 + |D|b^2}{4} \geq \frac{|D|}{4}, \quad E(D) \geq e \geq \frac{\log(|D|/4)}{\log C_1 + 8 \log \log(3|D|)}.$$

This proves the stated order and its effectivity after adjusting the absolute constant over a finite initial interval. The displayed explicit function tends to infinity, so solving its inequality with right side M gives an effective upper bound for all discriminants with $E(D) \leq M$. $\square$

This argument applies to every fixed exponent, including exponent 7. It does not identify the complete numerical lists for exponents 3, 5, 6 or 7: a new effective discriminant cutoff need not be below the range of an existing computation.

17 Pointwise torsion bounds for every quadratic and cubic class group

Ellenberg–Venkatesh [88, Proposition 3.1] prove under GRH that, for a degree- n number field K and fixed positive integer m ,

$$|\mathrm{Cl}_K[m]| \ll_{n,m,\varepsilon} D_K^{1/2-1/(2m(n-1))+\varepsilon}, \quad D_K = |\mathrm{disc}(K)|.$$

Here $\mathrm{Cl}_K[m]$ is the subgroup of the ordinary ideal class group annihilated by m . We recover this exact published conclusion for every quadratic and every cubic field. The cases of prime torsion $m \geq 5$ are the principal new cases: the corresponding claims for $m = 2, 3$ were already unconditional, with stronger bounds available in several cases. This is a pointwise assertion about every field, without an exceptional family.

Theorem 17.1 (The quadratic and cubic cases of Ellenberg–Venkatesh). *For each integer $m \geq 2$ and each $\varepsilon > 0$,*

$$|\mathrm{Cl}_K[m]| \ll_{m,\varepsilon} \begin{cases} D_K^{1/2-1/(2m)+\varepsilon}, & [K:\mathbb{Q}] = 2, \\ D_K^{1/2-1/(4m)+\varepsilon}, & [K:\mathbb{Q}] = 3. \end{cases}$$

The constants are effective and uniform over the indicated fields. In the quadratic case the proof gives the more precise bound

$$|\mathrm{Cl}_K[m]| \ll_m D_K^{1/2-1/(2m)} \log(3D_K) \ell(D_K), \quad \ell(x) = \log \log(e^e x). \quad (59)$$

Uniform supplies of degree-one primes. For a quadratic field of signed fundamental discriminant Δ , put $D = |\Delta|$ and let χ_Δ be its primitive quadratic Dirichlet character. Lemma 1.2, its principal-character version, and removal of prime powers give

$$\sum_{\substack{p \leq x \\ \chi_\Delta(p)=1}} \log p = \frac{x}{2} + O(x^{7/8} \log^2(Dx) + \sqrt{x} \log^2(2x) + \log(3D) \log(2x)). \quad (60)$$

Indeed the indicator is $(1 + \chi_\Delta(p))/2$ away from primes dividing D . The higher prime powers contribute $O(\sqrt{x} \log^2(2x))$, and the omitted ramified prime powers contribute $O(\log(3D) \log(2x))$. The same argument with a minus sign counts the primes with $\chi_\Delta(p) = -1$. Thus for every fixed $a, c > 0$, at $x = cD^a$ there are $\gg_{a,c} D^a / \log(3D)$ primes of either sign, once D exceeds an effective threshold. Each prime of sign $+1$ supplies a degree-one unramified prime ideal of the quadratic field.

If K is cyclic cubic, its two nontrivial Artin characters are primitive Dirichlet characters $\chi, \bar{\chi}$ of order three. Their conductor f satisfies $D_K = f^2$. Character orthogonality gives

$$1_{\{\chi(p)=1\}} = \frac{1 + \chi(p) + \bar{\chi}(p)}{3} \quad (p \nmid f).$$

The same explicit-formula argument consequently counts $\gg_a D_K^a / \log(3D_K)$ completely split primes below D_K^a .

If K is non-Galois cubic, the Galois group of its normal closure is S_3 . Its quadratic resolvent is $\mathbb{Q}(\sqrt{\Delta_K})$, where Δ_K is the signed field discriminant. The primitive character χ_d of this resolvent has fundamental discriminant d with $|d| \leq D_K$, since Δ_K/d is an integer square. For $p \nmid D_K$, the condition $\chi_d(p) = -1$ says that Frobenius is an odd permutation. In S_3 this is necessarily a transposition, so p has splitting type $(1, 2)$ in K and supplies one degree-one unramified prime ideal.

Formula (60) with the minus sign, conductor $|d| \leq D_K$, and removal of the primes dividing D_K , again supplies

$$M \gg_a D_K^a / \log(3D_K) \quad (61)$$

such ideals of norm at most D_K^a . Its error is uniform even when the resolvent discriminant stays small. No prime theorem for the nonabelian normal closure has been assumed.

A complete quadratic argument, including the regulator. We give a direct version of the mechanism behind [88, Lemma 2.3 and Remark 2.4], so that the infinite unit group in a real quadratic field causes no hidden gap. Set $D = D_K$, $h = |\text{Cl}_K|$, $h_m = |\text{Cl}_K[m]|$, and

$$Y = 4^{-1/m} D^{1/(2m)}.$$

Select all rational split primes $p \leq Y$ and one prime ideal $\mathfrak{p}$ over each. Their number M satisfies

$$M \gg_m D^{1/(2m)} / \log(3D) \quad (62)$$

for effectively large D , by (60). These are distinct rational primes, and every one is unramified.

Partition these ideals according to their classes in $\text{Cl}_K / \text{Cl}_K[m]$, a group of size h/h_m . If $\mathfrak{p}, \mathfrak{q}$ lie in the same part, then

$$(\mathfrak{p}\mathfrak{q}^{-1})^m = (\alpha)$$

for some $\alpha \in K^\times$. Multiplying by the rational integer q^m gives an algebraic integer $\gamma = q^m \alpha$ with

$$(\gamma) = \mathfrak{p}^m \bar{\mathfrak{q}}^m, \quad |N_{K/\mathbb{Q}} \gamma| = (pq)^m. \quad (63)$$

For $p \neq q$, this ideal is not fixed by the nontrivial automorphism of K , so $\gamma \notin \mathbb{Q}$. Every nonrational algebraic integer of a quadratic field satisfies

$$|\sigma_1 \gamma - \sigma_2 \gamma| \geq \sqrt{D}. \quad (64)$$

To verify this directly, write $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ with $\omega - \bar{\omega} = \sqrt{\Delta_K}$. The difference of the two conjugates of $a + b\omega$, for $b \neq 0$, has absolute value $|b|\sqrt{D}$.

For imaginary quadratic K , the two conjugates of γ have equal absolute value. Equations (63) and (64) would imply

$$\sqrt{D} \leq 2(pq)^{m/2} \leq 2Y^m = \frac{\sqrt{D}}{2},$$

which is impossible. Every part therefore has at most one member, and $h_m \leq h/M$.

For real quadratic K , fix the first embedding σ_1 and choose a fundamental unit ϵ_K with $|\sigma_1 \epsilon_K| > 1$. Put $R = \log |\sigma_1 \epsilon_K|$; units of norm -1 are included. For each nonempty part choose a reference prime p_0 . For every prime p in that part choose α_p with $(\alpha_p) = (\mathfrak{p}\mathfrak{p}_0^{-1})^m$, and define the point

$$u_p = \log |\sigma_1 \alpha_p| - \frac{m}{2} \log(p/p_0) \pmod{R\mathbb{Z}}$$

on the circle of length R . Changing the generator multiplies it by a unit, and hence does not change this point.

For two distinct primes p, q in the part, multiply α_p/α_q by a unit so that the balanced first logarithm is the shortest signed difference t between u_p and u_q . The resulting $\gamma = q^m(\alpha_p/\alpha_q)\epsilon_K^j$ is still an algebraic integer with the ideal and norm in (63). Its two real absolute values are

$$|\sigma_1 \gamma| = (pq)^{m/2} e^t, \quad |\sigma_2 \gamma| = (pq)^{m/2} e^{-t}.$$

This remains true when their signs differ. Therefore

$$\sqrt{D} \leq |\sigma_1 \gamma - \sigma_2 \gamma| \leq 2Y^m e^{|t|} = \frac{\sqrt{D}}{2} e^{|t|}, \quad |t| \geq \log 2.$$

The points in each part are thus pairwise separated by at least $\log 2$ in circular distance. There are at most $1 + R/\log 2$ of them: if there are at least two, add the successive gaps around the circle. Also $R \geq \log((1 + \sqrt{5})/2)$, as follows at once from the integer trace and norm ± 1 of a fundamental unit. Consequently

$$M \leq \frac{h}{h_m} \left(1 + \frac{R}{\log 2}\right) \ll \frac{hR}{h_m}, \quad h_m \ll \frac{hR}{M}.$$

This is the required regulator factor; replacing hR by h in this argument would be unjustified.

The quadratic class number formulas and Theorem 1.4 give, effectively,

$$h \ll \sqrt{D}\ell(D) \quad (K \text{ imaginary quadratic}), \quad hR \ll \sqrt{D}\ell(D) \quad (K \text{ real quadratic}).$$

For example the exact real formula is $2hR = \sqrt{D}L(1, \chi_D)$. Combining these estimates with (62) proves (59) for effectively large D . For bounded D the effective elementary upper bound $h \ll \sqrt{D} \log(3D)$ absorbs the remaining cases. The stated quadratic exponent follows by absorbing the logarithmic factors in D^ε .

The published small-prime lemma and the cubic deduction. We use the following unconditional result with its full hypotheses. Ellenberg–Venkatesh [88, Lemma 2.3] state: if K/K_0 has degree $d > 1$, m is a positive integer, $0 < a < 1/(2m(d-1))$, and there are M unramified prime ideals of K of norm at most $N_{K_0/\mathbb{Q}}(\mathfrak{D}_{K/K_0})^a$ which are not extensions of prime ideals of any proper intermediate field, then, for every $v > 0$,

$$|\text{Cl}_K[m]| \ll_{[K:\mathbb{Q}], m, a, v} D_K^{1/2+v}/M. \quad (65)$$

Here $\mathfrak{D}_{K/K_0}$ denotes the relative discriminant ideal. Dependence on the strict margin in a is included explicitly. This is an imported unconditional lemma, not a consequence of GRH. Its proof uses small neighborhoods in the Arakelov class group. Writing $\mathcal{D} = N_{K_0/\mathbb{Q}}(\mathfrak{D}_{K/K_0})$, collisions between their m th powers give a generator of height $O(\mathcal{D}^{ma})$, while their Lemma 2.2 bounds the height of a primitive generator below by a constant times $\mathcal{D}^{1/(2(d-1))}$. The nonextension hypothesis rules out the remaining collisions from proper subfields, except for a bounded unit multiplicity. The volume upper bound needed is only $h_K R_K \ll_n \sqrt{D_K} (\log(3D_K))^{n-1}$, which follows effectively from the residue upper bound and the class number formula. No ineffective lower half of Brauer–Siegel is needed. The bounded-degree height and unit estimates are effective, so (65) has an effective implied constant.

Apply this lemma with $K_0 = \mathbb{Q}$, $d = 3$, and the ideals in (61). A cubic field has no proper intermediate field besides $\mathbb{Q}$, and a degree-one prime ideal cannot be $p\mathcal{O}_K$, whose norm is p^3 . Thus all hypotheses are satisfied. It is enough to treat $0 < \varepsilon < 1/(4m)$; larger ε follows from such a smaller choice. Put

$$a = \frac{1}{4m} - \frac{\varepsilon}{3}, \quad v = \frac{\varepsilon}{3}.$$

Then (65) and (61) give

$$|\text{Cl}_K[m]| \ll_{m, \varepsilon} D_K^{1/2-1/(4m)+2\varepsilon/3} \log(3D_K) \ll_{m, \varepsilon} D_K^{1/2-1/(4m)+\varepsilon}.$$

All thresholds and constants are effective. This completes the proof of Theorem 17.1.

Published scope and later results. The exponents asserted in the theorem are exactly the degree-two and degree-three specializations of the published GRH proposition. The more precise quadratic logarithmic estimate is a consequence of the proof, not a separate published theorem being counted. Heath-Brown’s later work [89, Theorems 1, 5, and 10] already gives the cubic exponent for pure cubic fields, gives a conditional version for arbitrary cubics using only a weak zero-free disk for the same quadratic or cubic Dirichlet character, and gives the quadratic exponent when all prime divisors of the discriminant are sufficiently small. Those existing special cases are not new admissions. Neither those results nor averaged torsion estimates supply the unrestricted pointwise assertions here. We use the exponent $1/(4m)$ in the cubic saving, as in Ellenberg–Venkatesh and Heath-Brown’s Theorem 5; no stronger exponent inferred from the later paper’s printed Corollary 7 or Theorem 11 is claimed.

For prime $m = 2$, genus theory settles the quadratic case and the known cubic bounds are stronger. For prime $m = 3$, the quadratic bound was already unconditional in Ellenberg–Venkatesh and is improved by Chan–Koymans [90]; the cubic bound $D_K^{1/3+\varepsilon}$ was already unconditional as well. Lemke Oliver–Zaman’s general unconditional improvement [91] over the trivial estimate gives a logarithmic saving, rather than the power savings asserted here. The current-literature check records these overlaps explicitly; it does not assert a global priority determination.

17.1 Further field families with the same published torsion exponent

The same published proposition has additional full-family specializations within the precise scope of the available zero-free theorems. The following criterion records the group-theoretic reason; it is used to identify those specializations, not to assert the proposition for arbitrary number fields.

Lemma 17.2 (An abelian quotient detecting degree-one primes). *Fix $n \geq 2$. Let $K/\mathbb{Q}$ have degree n , normal closure N , and transitive Galois group $G \leq S_n$. Suppose that there is a nonempty subset C of the abelianization $A = G/[G, G]$ such that every element of G mapping to C fixes at least one of the n embeddings of K . Then, for each fixed $a > 0$, the number of degree-one unramified prime ideals of K of norm at most D_K^a is*

$$\gg_{n,a} D_K^a / \log(3D_K)$$

for effectively large D_K . All constants are uniform in K and the indicated Galois group.

Proof. Let $F = N^{[G,G]}$. It is abelian over $\mathbb{Q}$, with group A . Its characters are primitive Dirichlet characters after passage to their individual conductors. By the conductor–discriminant formula, each such conductor divides D_F , and their least common multiple is at most D_F . Also

$$D_F \leq D_N \leq D_K^{n!}.$$

For the second inequality, write N as a compositum of at most n conjugates of K and use the standard discriminant inequality $D_N \leq \prod_i D_{K_i}^{[N:K_i]}$. The exponent of D_K is at most $[N:\mathbb{Q}] \leq n!$. A weaker fixed-degree power would suffice.

For an unramified rational prime p , character orthogonality in A expresses $1_C(\text{Frob}_p|_F)$ as a linear combination of at most $|A| \leq n!$ Dirichlet characters. Its trivial-character coefficient is $|C|/|A| \geq 1/n!$, and every coefficient has absolute value at most one. Lemma 1.2 and removal of prime powers therefore give, uniformly for $x \geq 2$,

$$\sum_{\substack{p \leq x, p \nmid D_N \\ \text{Frob}_p|_F \in C}} \log p = \frac{|C|}{|A|} x + O_n(x^{7/8} \log^2(D_K x) + \sqrt{x} \log^2(2x) + \log(3D_K) \log(2x)).$$

At $x = D_K^a$ the error is smaller than half the main term beyond an effective threshold. Each prime counted has a Frobenius fixed point in the action on the embeddings of K , and hence has a degree-one unramified prime ideal in K . Dividing the weighted count by $\log x$ proves the assertion. $\square$

Corollary 17.3 (Further specializations of Ellenberg–Venkatesh). *Fix $n \geq 2$, an integer $m \geq 2$, and $\varepsilon > 0$. Then*

$$|\mathrm{Cl}_K[m]| \ll_{n,m,\varepsilon} D_K^{1/2-1/(2m(n-1))+\varepsilon} \quad (66)$$

holds effectively and uniformly for degree- n fields in any of the following classes:

1. *abelian extensions of $\mathbb{Q}$;*
2. *fields of prime degree whose normal closure has solvable Galois group;*
3. *quartic fields whose normal-closure Galois group is not S_4 ;*
4. *fields containing $E = \mathbb{Q}(\sqrt{-3})$ which are abelian over E .*

The fourth assertion uses the imported finite-order Hecke zero-free theorem over E ; the first three use only the Dirichlet theorem. These are stated restrictions of the published GRH proposition, with the same exponent, rather than a claim covering all degree- n fields. Existing unconditional subcases are not counted again.

Proof. First apply Lemma 17.2 to the first three classes. For an abelian transitive faithful action the action is regular, so $C = \{1\}$ works.

For a solvable transitive group G of prime degree p , the action is primitive. A minimal nontrivial normal subgroup is elementary abelian; its orbits form a block system, so it is transitive. An abelian transitive subgroup in a faithful primitive permutation action is regular: a point stabilizer fixes every point. Hence this normal subgroup has order p . Identifying it with the translations of $\mathbb{F}_p$, its normalizer is the affine group, and

$$G = C_p \rtimes C_s \leq \mathrm{AGL}_1(\mathbb{F}_p), \quad s \mid p-1.$$

If $s = 1$, use the abelian case. If $s > 1$, the commutator subgroup is C_p and the abelianization is C_s . Every affine map $x \mapsto ax + b$ with $a \neq 1$ has the unique fixed point $b/(1-a)$. Thus $C = C_s \setminus \{1\}$ satisfies the criterion.

The transitive subgroups of S_4 other than S_4 are C_4, V_4, D_4, A_4 , where D_4 has order eight. The first two are abelian. For A_4 the commutator subgroup is V_4 , and both nontrivial cosets in A_4/V_4 consist of three-cycles, each fixing one point. For D_4 , use

$$r = (1234), \quad s = (24), \quad [D_4, D_4] = \{1, r^2\}.$$

The coset $s[D_4, D_4] = \{(24), (13)\}$ consists of permutations with two fixed points. This supplies the required C . For comparison, neither coset of $[S_4, S_4] = A_4$ has this property: one contains double transpositions and the other contains four-cycles. No conclusion for general S_4 -quartics is drawn.

In all these cases select one of the degree-one prime ideals above each counted rational prime. Such an ideal is never the extension of a prime ideal from a proper intermediate field K_0 : an extended ideal has norm $N_{K_0/\mathbb{Q}}(\mathfrak{p})^{[K:K_0]}$, which cannot be the rational prime p when $[K:K_0] > 1$. The unconditional lemma (65), with base $\mathbb{Q}$ and any $a < 1/(2m(n-1))$, therefore applies. Choose $a = 1/(2m(n-1)) - \varepsilon/3$ and $v = \varepsilon/3$ when ε is small, and absorb $\log(3D_K)$ into the remaining $D_K^{\varepsilon/3}$. Larger ε follows by weakening a smaller positive value. This proves (66) in the first three classes.

For the fourth class, write $[K : E] = r$, so $n = 2r$, and let $N = K\overline{K}$. Because K/E and $\overline{K}/E$ are abelian, N/E is abelian of degree $g \leq r^2$. The field N is stable under complex conjugation and normal over E , hence is normal over $\mathbb{Q}$. It contains the normal closure of K and indeed is that closure. The discriminant bound for a compositum gives

$$D_N \leq D_K^{[N:K]} D_{\overline{K}}^{[N:\overline{K}]} \leq D_K^{2r}.$$

By the conductor–discriminant formula over E , every finite-order Hecke character ψ associated with N/E has conductor $\mathfrak{f}_\psi$ satisfying

$$N_{E/\mathbb{Q}} \mathfrak{f}_\psi \leq N_{E/\mathbb{Q}} \mathfrak{D}_{N/E} \leq D_N.$$

The character of conductor one is interpreted through ζ_E . The imported fixed-field theorem and the explicit formula proved in (76) apply to every other character, with degree two and uniform conductor dependence. Orthogonality in $\text{Gal}(N/E)$ therefore gives

$$\sum_{\substack{\mathfrak{p} \text{ prime of } E, N\mathfrak{p} \leq x \\ \mathfrak{p} \text{ splits completely in } N/E}} \log N\mathfrak{p} = \frac{x}{g} + O_n(x^{7/8} \log^2(D_K x) + \sqrt{x} \log^2(2x) + \log(3D_K) \log(2x)),$$

where primes ramified in N/E are omitted. The principal term uses $\zeta_E(s) = \zeta(s)L(s, \chi_{-3})$; both factors are within the Dirichlet input. Higher powers and the omitted conductor primes have been bounded exactly as in the rational explicit formula.

Prime ideals of E of residue degree two have norm p^2 and contribute $O(\sqrt{x} \log(2x))$. After deleting them and the prime above three, every remaining prime ideal lies above a rational prime split in E . If one such prime splits completely in N/E , so does its conjugate, since $N/\mathbb{Q}$ is Galois. The rational prime consequently splits completely in N and in K . Each rational prime is counted at most twice. At $x = D_K^a$ this again supplies $\gg_{n,a} D_K^a / \log(3D_K)$ rational primes and degree-one ideals of K . The preceding application of (65) finishes the proof. $\square$

The inclusion of fixed-degree abelian extensions does not label every subcase as previously open. Genus theory, the known 2- and 3-torsion results, and stronger bounds for some elementary abelian extensions overlap this corollary. Its purpose is to give the exact uniform domain on which the published GRH exponent follows from the stated analytic input, while retaining the unrestricted quadratic and cubic prime- $m \geq 5$ cases as the main applications.

18 The sharper average for odd imaginary-quadratic class numbers

For a positive integer h , let $\mathcal{F}(h)$ be the number of imaginary quadratic fields with ideal class number h . Lamzouri’s published GRH theorem [11, Theorem 1.2] is the following estimate, including its error term. The leading asymptotic was already made unconditional in [12, Theorem 1.1], with the weaker denominator $(\log H)^{3/2}$ in the error. The conclusion recovered here is the sharper error term.

Theorem 18.1 (Lamzouri’s odd-class-number average). *As $H \rightarrow \infty$,*

$$\sum_{\substack{h \leq H \\ h \text{ odd}}} \mathcal{F}(h) = \frac{15}{4} \frac{H^2}{\log H} + O\left(\frac{H^2 (\log \log H)^3}{(\log H)^2}\right).$$

The implied constant and the threshold are effective and absolute.

We prove the required complex-moment estimate rather than importing its GRH version. All logarithms in the proof are natural; parameters are sufficiently large whenever iterated logarithms are used.

18.1 Complex moments over prime discriminants

Let $Y(p)$, indexed by the rational primes, be independent random variables with values $1, -1$, each of probability $1/2$, and put

$$\mathcal{L} = \prod_p (1 - Y(p)/p)^{-1}.$$

The product converges almost surely to a positive number. Indeed, $\log \mathcal{L} = \sum_p Y(p)/p + O(\sum_p p^{-2})$, and the independent mean-zero series converges almost surely by the finite variance sum. All real moments exist. For each complex z , define the multiplicative function d_z by

$$d_z(p^j) = \frac{z(z+1) \cdots (z+j-1)}{j!}, \quad d_z(1) = 1.$$

Expanding the local factors and taking expectations gives

$$\mathbb{E} \mathcal{L}^z = \sum_{m \geq 1} \frac{d_z(m^2)}{m^2}. \quad (67)$$

Here and below powers of a positive number use its real logarithm. To justify absolute convergence and passage from finite products, take an integer $k \geq \max(1, |z|)$. Then $|d_z(n)| \leq d_k(n)$. For integers $j \geq 0$,

$$d_k(p^{2j}) \leq d_{k(k+1)/2}(p^j).$$

One elementary proof pairs an ordered nondecreasing list of $2j$ members of $\{1, \dots, k\}$ consecutively. The resulting multiset of j unordered pairs determines the original multiset, giving an injection into multisets of j of the $k(k+1)/2$ pair types. Consequently, for $\sigma > 1/2$,

$$\sum_{m \geq 1} \frac{d_k(m^2)}{m^{2\sigma}} \leq \zeta(2\sigma)^{k(k+1)/2}. \quad (68)$$

The same argument bounds all finite-product moments uniformly; using a higher real moment gives uniform integrability and proves (67) for the limiting random product.

Lemma 18.2. *Uniformly for*

$$|z| \leq \frac{\log x}{100(\log \log x)^2},$$

one has

$$\sum_{\substack{p \leq x \\ p \equiv 3 \pmod{4}}} L(1, \chi_{-p})^z = \frac{\text{Li}(x)}{2} \mathbb{E} \mathcal{L}^z + O(x^{15/16}), \quad \text{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

The constants and the lower threshold for x are absolute and effective.

Proof. Put $Z = \exp((\log x)^2)$ and $k = \max(1, \lceil |z| \rceil)$. We first establish, uniformly for primitive nonprincipal χ of conductor $q \leq x$,

$$L(1, \chi)^z = \sum_{n \geq 1} \frac{d_z(n) \chi(n)}{n} e^{-n/Z} + O\left(e^{-(\log x)^2/64}\right). \quad (69)$$

Use the holomorphic Euler-product branch of $\log L(s, \chi)$ on $\Re s > 7/8$. On $\Re s \geq 31/32$ with real part bounded above,

$$|\log L(s, \chi)| \ll \log(q(|\Im s| + 3)).$$

For clarity, this follows from Borel–Carathéodory on fixed-radius discs centered at $2 + i\Im s$: the outer disc stays in $\Re s > 7/8$, the Euler product bounds its central logarithm, and the usual uniform polynomial bound for L bounds the real part of that logarithm. The distances from the inner disc to the outer boundary are fixed positive constants.

Mellin inversion of e^{-u} gives the sum in (69) as

$$\frac{1}{2\pi i} \int_{(1)} L(1+w, \chi)^z \Gamma(w) Z^w dw.$$

Shift to $\Re w = -1/32$. Only the pole of Γ at 0 is crossed. The logarithm bound and Stirling’s formula bound the new integral by

$$Z^{-1/32} \exp\{Ck \log x + Ck \log(k+2) + C\}.$$

This is at most the error in (69) for all sufficiently large effective x , since $k \ll \log x / (\log \log x)^2$. The same estimates make the horizontal contour integrals tend to zero. For real quadratic χ , the branch at 1 is the real logarithm since $L(1, \chi) > 0$.

Next, quadratic reciprocity gives $\chi_{-p}(n) = (n/p)$ for $p \equiv 3 \pmod{4}$. If $n > 0$ is nonsquare, the primitive quadratic character attached to its positive squarefree part is nonprincipal and even. Its product with χ_{-4} is odd and is also nonprincipal. Their conductors are at most $4n$. Lemma 1.2, the removal of prime powers, and partial summation therefore give

$$\sum_{\substack{p \leq x \\ p \equiv 3 \pmod{4}}} \chi_{-p}(n) = \frac{\text{Li}(x)}{2} \mathbf{1}_{n=\square} + O\left(x^{7/8} \log^2(4nx) + \log(2n)\right). \quad (70)$$

When replacing a Kronecker symbol by its primitive character, primes dividing the removed square part of n contribute at most $\omega(n)$. This is covered by the final term. The same term accounts for the primes dividing n in the square case. The prime number theorem in the two classes modulo 4 follows from the same lemma, including its principal term.

The smoothed sum of the errors is small enough even though Z is much larger than a power of x . Specifically, with $a = 1/\log Z$, the inequality $e^{-n/Z} \leq en^{-a}$ and two derivatives of $\zeta(1+a)^k$ give

$$\sum_{n \geq 1} \frac{d_k(n)}{n} e^{-n/Z} \log^2(4nx) \ll (k+1)^2 (\log Z)^2 \{C \log Z\}^k = x^{o(1)}. \quad (71)$$

The $o(1)$ is uniform in the displayed range for z and is effective: the logarithm of the right side is $O(k \log \log Z + \log(k+2) + \log \log Z) = o(\log x)$. In particular it is at most $x^{1/32}$ for sufficiently large x . This all-integer bound also controls the removed ramified primes; using the much larger bound (68) for that error would be insufficient.

Finally, $|1 - e^{-u}| \leq u^{1/4}$ and (68) with $\sigma = 3/4$ imply

$$\sum_{m \geq 1} \frac{|d_z(m^2)|}{m^2} |e^{-m^2/Z} - 1| \leq Z^{-1/4} \zeta(3/2)^{k(k+1)/2} \ll e^{-(\log x)^2/8}.$$

Average (69) over the primes, insert (70), and use (71) and this last estimate. The total error is $O(x^{29/32} + 1)$, which is within the stated $O(x^{15/16})$. Equation (67) gives the main term. $\square$

18.2 From the moments to the class-number count

Proof of Theorem 18.1. Set $l = \log \log H$ and $X = H^2(\log H)^4$. The effective lower bound in Corollary 1.5 shows that every negative fundamental discriminant with $h(D) \leq 2H$ has $|D| \leq X$ for sufficiently large effective H . To justify the inversion, the inequality $\sqrt{|D|} \ll H \log \log(e^e |D|)$ first gives $|D| \ll H^3$ for large H , and then gives $|D| \ll H^2 l^2 < X$. Thus no exceptional discriminant or ineffective cutoff is needed.

Genus theory says that an imaginary quadratic field has odd class number exactly when its fundamental discriminant has one prime discriminant factor. These fields have discriminant $-p$ with $p \equiv 3 \pmod{4}$, together with -4 and -8 . Except for $p = 3$, the class-number formula is

$$h(-p) = \frac{\sqrt{p}}{\pi} L(1, \chi_{-p}).$$

The finitely many stated exceptions affect all counts below by $O(1)$.

Put

$$c = \frac{1}{\log H}, \quad T = \frac{\log X}{1000(\log \log X)^2}.$$

For $s = c + it$, $|t| \leq T$, Lemma 18.2 applies with $z = -s$ uniformly to every endpoint $\sqrt{X} \leq y \leq X$, after increasing the absolute threshold. Partial summation, the class-number formula, and the omission of the initial range up to $\sqrt{X}$ give

$$\sum_{\substack{p \leq X \\ p \equiv 3 \pmod{4}}} h(-p)^{-s} = \frac{\pi^s}{2} \mathbb{E} \mathcal{L}^{-s} \int_2^X \frac{u^{-s/2}}{\log u} du + O((1 + |s|)X^{15/16}). \quad (72)$$

For the omitted range, the actual sum has modulus at most $\sqrt{X}$ because $h(-p) \geq 1$, and the model integral has that size because $|\mathbb{E} \mathcal{L}^{-s}| \leq \mathbb{E} \mathcal{L}^{-c} \ll 1$. In particular the sign in the random moment is $-s$, as required by the class-number formula.

We give the smoothing argument explicitly. Take

$$N = \lceil 100 \log \log H \rceil, \quad \lambda = 10/T, \quad \Delta = \lambda N \ll \frac{(\log \log H)^3}{\log H}.$$

The letter N in this paragraph is a smoothing parameter. Define

$$I(y) = \frac{1}{2\pi i} \int_{(c)} y^s \left(\frac{e^{\lambda s} - 1}{\lambda s} \right)^N \frac{ds}{s}.$$

This is the average of $\mathbf{1}_{ye^U > 1}$ over $U = t_1 + \dots + t_N$, with the t_i independent uniform variables on $[0, \lambda]$. This identity follows by integrating Perron's formula; its boundary sets have measure zero. Hence $0 \leq I \leq 1$, $I(y) = 1$ for $y \geq 1$, and $I(y) = 0$ for $y \leq e^{-\Delta}$.

Let $A(H) = \sum_{h \leq H, h \text{ odd}} \mathcal{F}(h)$ and

$$S(H) = \sum_{\substack{p \leq X \\ p \equiv 3 \pmod{4}}} I(H/h(-p)).$$

The cutoff already proved and the support properties give

$$S(He^{-\Delta}) + O(1) \leq A(H) \leq S(H) + O(1), \quad (73)$$

where the same parameters X, c, T, N, λ are used in both sums. Since $\Delta = o(1)$, these cutoffs also include every field needed for the two smoothed sums.

The part $|t| > T$ of the Mellin integral for $S(H)$ is bounded by

$$\ll \frac{X}{N} \left(\frac{3}{\lambda T} \right)^N \ll \frac{H^2}{(\log H)^{20}}.$$

Here $H^c = e$ and $h^{-c} \leq 1$. On the remaining part, the smoothing factor has modulus at most $e^{\lambda c N} \ll 1$. Insert (72); its contribution to the error is at most $O(X^{15/16}(T + \log(T/c) + 1))$, again $O(H^2/(\log H)^{20})$. Extending the model integral back to the whole line costs the same tail bound, since $\mathbb{E}\mathcal{L}^{-c} \ll 1$. Fubini and the uniform-average description of I now give

$$S(H) = \frac{1}{2} \mathbb{E}_{U,Y} J \left(\min \left(X, \frac{\pi^2 H^2 e^{2U}}{\mathcal{L}^2} \right) \right) + O \left(\frac{H^2}{(\log H)^{20}} \right), \quad (74)$$

where $J(v) = \int_2^v du / \log u$ for $v \geq 2$ and $J(v) = 0$ for $v < 2$. The powers in the model have therefore been used with the correct reciprocal of $\mathcal{L}$.

We justify the two final estimates for this model. All fixed negative moments of $\mathcal{L}$ were established above. Thus

$$\mathbb{E}(\mathcal{L}^{-2} \mathbf{1}_{\mathcal{L} < 2\pi/(\log H)^2}) \leq \left(\frac{2\pi}{(\log H)^2} \right)^{12} \mathbb{E}\mathcal{L}^{-14} \ll (\log H)^{-24}.$$

Since $U \leq \Delta = o(1)$, $J(v) \ll v$, and $X = H^2(\log H)^4$, this removes the truncation by X in (74) with an error of the same negligible size.

Uniformly for $0 \leq u \leq \Delta$, the estimate $J(v) = v/\log v + O(v/(\log v)^2)$ gives

$$\mathbb{E}J(\pi^2 H^2 e^{2u} \mathcal{L}^{-2}) = \frac{\pi^2 H^2 e^{2u}}{2 \log H} \mathbb{E}\mathcal{L}^{-2} + O(H^2/(\log H)^2). \quad (75)$$

Here is a direct bound for the expectation error. On $H \leq v = \pi^2 H^2 e^{2u} \mathcal{L}^{-2} \leq H^3$,

$$\left| \frac{1}{\log v} - \frac{1}{2 \log H} \right| \ll \frac{1 + |\log \mathcal{L}|}{(\log H)^2},$$

and $\mathbb{E}[\mathcal{L}^{-2}(1 + |\log \mathcal{L}|)] < \infty$ by fixed positive and negative moments. The portions $v > H^3$ and $v < H$ are $O(H^{-1})$, using, for example, the fixed moments $\mathbb{E}\mathcal{L}^{-12}$ and $\mathbb{E}\mathcal{L}^{12}$ and the bound $J(v) \ll v$. Thus (75) holds with an effective constant.

Finally,

$$\mathbb{E}\mathcal{L}^{-2} = \prod_p (1 + p^{-2}) = \frac{\zeta(2)}{\zeta(4)} = \frac{15}{\pi^2}, \quad \mathbb{E}e^{2U} = 1 + O(\Delta).$$

Equations (74) and (75) give

$$S(H) = \frac{15}{4} \frac{H^2}{\log H} + O \left(\frac{H^2}{(\log H)^2} + \frac{H^2 \Delta}{\log H} \right).$$

The same formula with H replaced by $He^{-\Delta}$ holds with the fixed smoothing parameters. Its main term changes by $O(H^2 \Delta / \log H)$. The sandwich (73) and the bound for Δ prove the theorem. Every cutoff and constant in this argument is effective. $\square$

Scope and source comparison. The asymptotic for the cumulative count, rather than a formula for each individual $\mathcal{F}(h)$, is the published conclusion. The moment error in Lemma 18.2 is weaker than the square-root error available under GRH, but it is a fixed power saving and gives the exact published counting error after smoothing. No new conclusion for individual prescribed class numbers is inferred.

19 Small class-group exponents and Euler’s idoneal numbers

The numerical classifications in this section use published finite computations. We give the complete removal of their analytic hypotheses; we do not claim to have rerun their large searches. The precise zero-free interval needed is much smaller than the critical strip. The October 5 companion paper [59, Introduction] already announces the exponent-dividing-2 consequence and completeness of Euler’s 65 idoneal numbers. We record their full deduction here with that attribution; these two applications are not newly identified in this investigation. The extension to the published exponent-4 and exponent-8 lists is checked separately below.

Lemma 19.1 (Tatuzawa’s alternative, imported). *Let $D < 0$ be a fundamental discriminant, $Q = |D|$, and $0 < \epsilon < 1/2$. If*

$$Q \geq \max(e^{1/\epsilon}, e^{11.2}) \quad \text{and} \quad L(1, \chi_D) \leq 0.655\epsilon Q^{-\epsilon},$$

then $L(s, \chi_D)$ has a real zero in $(1 - \epsilon/4, 1)$.

This is the unconditional implication used in [71, Lemma 2], with attribution there to Tatuzawa’s Lemma 9 and Theorem 2. Its usual companion assertion, that there is at most one exceptional discriminant for a fixed ϵ , is not needed here.

Lemma 19.2 (The explicit class-number bound needed by the classification). *For every negative fundamental discriminant with $Q = |D| > e^{11.2}$,*

$$h(D) > \frac{0.655}{\pi e} \frac{\sqrt{Q}}{\log Q}.$$

Proof. Take $\epsilon = 1/\log Q$ in Lemma 19.1. Its numerical hypotheses hold. Moreover

$$1 - \frac{\epsilon}{4} = 1 - \frac{1}{4 \log Q} > 1 - \frac{1}{44.8} > \frac{7}{8}.$$

Theorem 1.1 excludes the real zero in Tatuzawa’s alternative, so $L(1, \chi_D) > 0.655/(e \log Q)$. As $D < -4$, the analytic class-number formula is $h(D) = \sqrt{Q} L(1, \chi_D)/\pi$, giving the claim. $\square$

Theorem 19.3 (Elsenhans–Klüners–Nicolae classification). *There are exactly 1046 imaginary quadratic fields whose ideal class group has exponent dividing 8. The counts by exact exponent, and largest absolute fundamental discriminants, are*

<i>exact exponent</i>	<i>number of fields</i>	<i>max D</i>
1	9	163
2	56	5460
4	203	435435
8	778	430950520.

Their discriminants and class-group structures are precisely the lists in [72].

Proof. The published computation [71, Theorems 1 and 2, Sections 4–6] establishes the following implication: if the lower bound

$$h(D) > \frac{0.655}{\pi e} \frac{\sqrt{|D|}}{\log |D|} \quad (|D| > e^{11.2})$$

holds for negative fundamental discriminants, then its lists of exact exponents 2, 4, 8 are complete. This is the precise mathematical content of the no-Siegel-zero assumption used for that part of their Theorem 2; see their Lemma 3 and the discussion preceding Algorithm 4. The small-discriminant class groups are included in their computation. Lemma 19.2 supplies this lower bound without a conjectural assumption. Their computed counts and maxima consequently apply to all negative fundamental discriminants. The exponent-1 list of nine fields was already unconditional. Adding the four counts gives $9 + 56 + 203 + 778 = 1046$. $\square$

Extent of the imported computation. The unconditional finite search in [71, Theorem 1] treats every field with $|D| \leq 3.1 \cdot 10^{20}$ and $E(D) \leq 8$. For exponents 4 and 8, their complete search under the displayed class-number bound goes further: genus theory and their Theorem 4 reduce the problem to $|D| < d_{24} < 2.38 \cdot 10^{34}$ and $|D| < d_{58} < 3.17 \cdot 10^{110}$, respectively, where d_j is the product of the first j primes. Their enumeration uses bounds on the 4-rank to avoid scanning all discriminants in these intervals. Thus one must not justify completeness merely by comparing the two large cutoffs with $3.1 \cdot 10^{20}$: the additional enumeration in their Section 5 is an essential published computational input.

For clarity, we also give an independent analytic exclusion that underlies the exponent-2 case.

Proposition 19.4 (No elementary 2-class group above the known list). *There are precisely 65 imaginary quadratic fields with class group of exponent dividing 2, and none has $|D| > 5460$.*

Proof. Put $d_{11} = 2 \cdot 3 \cdot 5 \cdots 31 = 200560490130$ and $a_0 = 0.655/(\pi e)$. Direct bounds give

$$a_0 \frac{\sqrt{d_{11}}}{\log d_{11}} > 2^{10}, \quad \frac{\log 31}{2} - \log 2 - \frac{\log 31}{\log d_{11}} > 0.$$

Suppose that $Q = |D| \geq d_{11}$ and the class-group exponent divides 2. Genus theory gives $h(D) = 2^{k-1}$, where k is the number of distinct prime factors of D . The function $\sqrt{t}/\log t$ is increasing for $t > e^2$. If $k \leq 11$, Lemma 19.2 therefore gives $h(D) > 2^{10} \geq 2^{k-1}$, a contradiction.

If $k > 11$, then $Q \geq d_{11} 31^{k-11}$. For real $u \geq 0$ define

$$F(u) = \frac{(\sqrt{31}/2)^u}{\log d_{11} + u \log 31}.$$

Its logarithmic derivative is

$$\frac{F'(u)}{F(u)} = \frac{\log 31}{2} - \log 2 - \frac{\log 31}{\log d_{11} + u \log 31} > 0.$$

Consequently

$$\frac{a_0 \sqrt{Q}}{2^{k-1} \log Q} \geq \frac{a_0 \sqrt{d_{11}}}{2^{10}} F(k-11) \geq \frac{a_0 \sqrt{d_{11}}}{2^{10} \log d_{11}} > 1,$$

again contradicting $h(D) = 2^{k-1}$ and Lemma 19.2. This excludes all $Q \geq d_{11}$. Since $d_{11} < 3.1 \cdot 10^{20}$, the unconditional finite computation in [71, Theorem 1] supplies exactly the $9 + 56$ fields below it, with largest absolute discriminant 5460. $\square$

The positive numbers $|D|$ for these 65 fields are

3, 4, 7, 8, 11, 15, 19, 20, 24, 35, 40, 43, 51, 52, 67, 84, 88, 91, 115, 120, 123, 132,
148, 163, 168, 187, 195, 228, 232, 235, 267, 280, 312, 340, 372, 403, 408, 420, 427,
435, 483, 520, 532, 555, 595, 627, 660, 708, 715, 760, 795, 840, 1012, 1092, 1155,
1320, 1380, 1428, 1435, 1540, 1848, 1995, 3003, 3315, 5460.

They are fundamental discriminants; this list is different from the list of idoneal integers below.

Theorem 19.5 (Completeness of Euler’s idoneal list). *The idoneal positive integers are exactly*

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37,
40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133,
165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408,
462, 520, 760, 840, 1320, 1365, 1848.

Here an integer $n \geq 1$ is called idoneal when every odd integer $m > 1$ coprime to n is prime if $m = x^2 + ny^2$ has exactly one solution with $x, y \geq 0$ and that solution is proper; “proper” means $\gcd(x, y) = 1$. Uniqueness counts all nonnegative solutions, not only the proper ones.

Proof. We use three established results about positive definite binary quadratic forms, in the precise form recorded by Kani [73]. First, Grube’s criterion (Theorem 6 there) says that n is idoneal if and only if the proper class group of primitive forms of discriminant $-4n$ has exponent dividing 2. Second, Corollary 14 there says that if an idoneal integer $n > 288$ is congruent to 1 or 2 modulo 4, then it is squarefree; if it is divisible by 4, then $n/4$ is a squarefree idoneal integer congruent to 2 modulo 4; and it is never congruent to 3 modulo 4. Third, Theorem 1 there gives precisely the displayed 65 idoneal integers up to 10000.

Suppose an additional idoneal integer exists. The finite theorem gives $n > 10000$. If $n \equiv 1, 2 \pmod{4}$, it is squarefree, so $D = -4n$ is fundamental. Grube’s criterion contradicts Proposition 19.4, since $|D| = 4n > 5460$. Otherwise $4 \mid n$, and $m = n/4 > 2500$ is squarefree, idoneal, and congruent to 2 modulo 4. Now $D = -4m$ is fundamental and $|D| = 4m > 10000 > 5460$, giving the same contradiction. These cases exhaust all possibilities, proving completeness. $\square$

Independent finite checks and provenance. We downloaded the author-maintained lists [72], checked their counts and largest discriminants, and independently enumerated reduced primitive binary quadratic forms to verify the class numbers of all 65 fields in Proposition 19.4. The same elementary enumeration verifies the displayed idoneal list through $n = 10000$: a reduced class has order dividing 2 precisely when its representative (a, b, c) has $b = 0$, $|b| = a$, or $a = c$. We additionally recomputed all 1046 listed class-group structures with PARI/GP 2.17.3, using `bnfinit` followed in every case by the full unconditional verification routine `bnfcertify` with default flag. The field discriminant, cyclic factors, and class number agreed for every entry. The saved verification log records all 1046 successful checks. These checks verify transcription and the small finite claims. The larger completeness computations in [71] remain imported published results. This avoids relying on the undocumented historical Lehmer computation discussed in [73, Remark 24(b)].

19.1 The eighteen exceptions to $xy + yz + zx = d$

Theorem 19.6 (Louboutin–Newman’s exact exceptional set). *For a positive integer d , the equation*

$$xy + yz + zx = d, \quad x, y, z \in \mathbb{Z}_{>0},$$

has no solution if and only if

$$d \in \{1, 2, 4, 6, 10, 18, 22, 30, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462\}.$$

Proof. We use the unconditional characterization in [87, Theorem 1, first assertion]: failure of a positive solution is equivalent to

$$d \in \{1, 4, 18\} \quad \text{or} \quad \begin{cases} d \text{ is squarefree, } d \equiv 2 \pmod{4}, \\ \text{Cl}(\mathbb{Q}(\sqrt{-d})) \text{ has exponent dividing 2.} \end{cases}$$

For such squarefree $d \equiv 2 \pmod{4}$, the field discriminant is $-4d$. Filtering the fundamental discriminants of Proposition 19.4 by this condition gives

$$d \in \{2, 6, 10, 22, 30, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462\}.$$

These 15 values are disjoint from $\{1, 4, 18\}$, and their union is exactly the stated set. The characterization proves both nonexistence for these values and existence for every other positive d . It also covers $d = 1$ directly, since $xy + yz + zx \geq 3$.

The structural characterization is an unconditional published input; its proof uses reduction of positive binary quadratic forms of discriminant $-4d$. The GRH hypothesis in the final assertion of [87, Theorem 1] was used solely for completeness of the quadratic-field list, now supplied by Proposition 19.4. $\square$

20 The complete abelian one-class-per-genus classifications

For an imaginary abelian extension $N/\mathbb{Q}$, write H_N for its Hilbert class field, and G_N for its genus field: the maximal abelian extension of $\mathbb{Q}$ containing N which is unramified over N at all finite primes. Put

$$h_N = [H_N : N], \quad g_N = [G_N : N].$$

There are no real places of N , so the finite-prime qualification causes no distinction between ordinary and narrow class fields here. The property *one class in each genus* is $h_N = g_N$.

Lemma 20.1. *For imaginary abelian $N/\mathbb{Q}$, the following are equivalent: $h_N = g_N$, $H_N = G_N$, and $H_N/\mathbb{Q}$ is abelian. If N is quadratic, these are also equivalent to $\text{Cl}(N)$ having exponent dividing 2.*

Proof. By definition G_N/N is unramified and abelian, so $G_N \subseteq H_N$. Thus equality of the degrees over N is equivalent to equality of the fields, and equality implies that $H_N/\mathbb{Q}$ is abelian. Conversely, if $H_N/\mathbb{Q}$ is abelian, its maximality property in the definition of G_N gives $H_N \subseteq G_N$.

For an imaginary quadratic field N , the Hilbert class field is Galois over $\mathbb{Q}$: conjugation sends every unramified abelian extension of N to another one, and hence preserves the maximal such extension. Its Galois group is

$$\text{Gal}(H_N/\mathbb{Q}) \simeq \text{Cl}(N) \rtimes \langle c \rangle, \quad c^2 = 1,$$

where c is complex conjugation and acts by inversion. Indeed $\mathfrak{a}\bar{\mathfrak{a}}$ is principal for every ideal $\mathfrak{a}$ of N , and the Artin isomorphism is equivariant for conjugation. This semidirect product is abelian exactly when every class equals its inverse, proving the last assertion. $\square$

Theorem 20.2 (The completed Chang–Kwon classification). *There are exactly 489 imaginary abelian number fields N with $h_N = g_N$, or equivalently with $H_N/\mathbb{Q}$ abelian. They consist of the 65 quadratic fields of Proposition 19.4 and the 424 nonquadratic fields in Chang–Kwon’s tables [83]. Among the latter, 77 are cyclic and 347 are noncyclic. All 489 fields have degree at most 24 and conductor at most 65689.*

Proof. For the quadratic fields, Lemma 20.1 reduces the classification exactly to Proposition 19.4. The largest absolute fundamental discriminant in that list is 5460; it is also the largest conductor in the quadratic part.

For the nonquadratic fields, we invoke the unconditional published [83, Theorem 1]. It gives precisely the stated 424 fields, their cyclic/noncyclic counts, and their degree and conductor bounds. The two classes are disjoint because their degrees differ. Their union therefore has size $65 + 424 = 489$ and satisfies the stated bounds. Chang–Kwon explicitly left only the completeness of the quadratic list dependent on GRH; that is the step supplied here. $\square$

Theorem 20.3 (Miyada’s multiquadratic classification, completed). *There are exactly 301 imaginary multiquadratic fields N with $h_N = g_N$: 65 have degree 2, 219 have degree 4, and 17 have degree 8. None has larger degree.*

Proof. Miyada’s unconditional structural theorem, restated in [83, Theorem 2], proves that an imaginary multiquadratic field with $h_N = g_N$ has degree at most 8. The unconditional enumerations [83, Proposition 3(2) and Proposition 4] give respectively 219 fields of degree 4 and 17 of degree 8. The quadratic case is exactly the 65 fields already proved complete above. Hence the total is $65 + 219 + 17 = 301$. This is the formerly GRH-dependent classification of [84], using the corrected nonquadratic tables in [83]. $\square$

The genus condition here is not interchangeable with the condition that the ideal class group have exponent dividing 2 once the degree is larger than 2. Also, the 424 nonquadratic fields were already classified unconditionally: the new deduction is completeness of the full 489-field classification and its 301-field multiquadratic subclassification. The finite computations supporting Chang–Kwon’s published theorem are imported established results and have not been rerun in this investigation.

21 The complete multiquadratic exponent-two classification

This section removes the GRH assumption from Ahn–Kwon’s published classification [44, Theorem 1]. Its finite arithmetic has been independently recomputed here. An imaginary multiquadratic field is a number field N without real embeddings such that $\text{Gal}(N/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$. Throughout this section, exponent dividing 2 includes the trivial class group. This condition concerns the ordinary ideal class group; it is different from equality of the class number and genus number.

Theorem 21.1 (Ahn–Kwon, unconditionally). *There are exactly 650 imaginary multiquadratic fields whose ideal class groups have exponent dividing 2. Their numbers by degree are*

$[N : \mathbb{Q}]$	2	4	8	16
number of fields	65	483	99	3.

There are no examples of larger degree. All have conductor at most 233905 and class number at most 32. The fields of degrees at least 4 are exactly those in Ahn–Kwon’s published Tables 4–6.

Proof. We give the mathematical reduction, the exact finite computation, and its unconditional verification. The complete list is supplied separately in text and JSON formats. The accompanying verification archive contains the arithmetic and exclusion records.

Norm descent. Let L/F be quadratic, with F imaginary. Class field theory gives

$$[\mathrm{Cl}(F) : N_{L/F} \mathrm{Cl}(L)] = [L \cap H_F : F] \leq 2,$$

where H_F is the ordinary Hilbert class field. If L/F ramifies at a finite prime, the index equals 1. Consequently, if $\mathrm{Cl}(L)$ has exponent dividing 2, then $\mathrm{Cl}(F)$ has exponent dividing 4 and at most one cyclic factor of order 4. In the ramified case its exponent divides 2. These are precisely the unconditional norm assertions of [44, Proposition 2].

We shall also use their elementary refinement. If an abelian 2-group G has exponent dividing 4 and at most one cyclic factor of order 4, then $|2G| \leq 2$. If G maps onto a subgroup H of an abelian group C with $[C : H] \leq 2$, then C is a 2-group and

$$|2C| \leq [C : H] |2H| \leq 4.$$

In particular, C has exponent dividing 8. If the map is surjective onto C , then C itself has exponent dividing 4 and at most one cyclic factor of order 4.

Existence of subfields to which ramified descent applies. Suppose N is imaginary multiquadratic of degree 2^n , $n \geq 2$. Write $G = \mathrm{Gal}(N/\mathbb{Q})$ additively and let $c \neq 0$ be complex conjugation. The inertia subgroups at finite primes generate G : their common fixed field would otherwise be a nontrivial extension of $\mathbb{Q}$ unramified at all finite primes, contrary to Minkowski's theorem. A nonzero inertia element $h \neq c$ gives an imaginary index-two subfield $N^{(h)}$ over which N ramifies. If no such h existed, the inertia subgroups would generate at most $\langle c \rangle$. If only one existed, they would generate at most $\langle c, h \rangle$. Thus there is at least one such subfield for $n \geq 2$, and at least two distinct ones for $n \geq 3$. In the latter case their compositum is N , and their intersection has degree 2^{n-2} .

The complete quadratic inputs. Proposition 19.4 supplies the 65 imaginary quadratic fields of exponent dividing 2. Among the 203 fields of exact exponent 4 in Theorem 19.3, exactly 161 have precisely one cyclic factor of order 4. The latter count is obtained by filtering the published group structures [72]; all these quadratic class-group structures have been independently verified as described above. Their largest absolute discriminant is 40755. The exponent-dividing-8 lists in the same theorem supply the additional quadratic obstructions used below.

An eligible quartic field has two distinct imaginary quadratic subfields. At least one belongs to the 65-field list, and the other belongs either to that list or to the 161-field list, by norm descent. Therefore exactly

$$\binom{65}{2} + 65 \cdot 161 = 12545$$

quartic candidates suffice. There is no duplication: the two imaginary quadratic subfields determine their quartic compositum.

Exact representation and arithmetic verification. Represent a multiquadratic field by the finite subgroup $V \subset \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$ of its quadratic characters, recording each squareclass by its signed squarefree integer representative. Thus $|V| = [N : \mathbb{Q}]$, the identity is 1, and multiplication of representatives is

$$a * b = \frac{ab}{\gcd(|a|, |b|)^2}.$$

The span of two such subgroups represents the compositum and their intersection represents the common subfield. All distinct index-two subgroups of V are enumerated; those containing a negative

representative give the imaginary index-two subfields. For a nonidentity representative a , put

$$d(a) = \begin{cases} a, & a \equiv 1 \pmod{4}, \\ 4a, & a \not\equiv 1 \pmod{4}. \end{cases}$$

The conductor–discriminant formula gives the exact integers

$$|\text{disc } N| = \left| \prod_{a \in V \setminus \{1\}} d(a) \right|, \quad f_N = \text{lcm}_{a \in V \setminus \{1\}} |d(a)|.$$

For a quadratic extension N/F between the imaginary fields under consideration, finite ramification is equivalent to $|\text{disc } N| \neq |\text{disc } F|^2$.

For every directly tested field, a basis of its squareclass subgroup produces a defining polynomial by successive linearly disjoint quadratic composita. PARI/GP 2.17.3 computes the class group with `bnfinit(P,1)` and then verifies its correctness with `bnfcertify(B)` using the default flag 0. This last step removes the GRH assumption from the class-group computation. Only a return value of 1 is accepted. Each resulting field discriminant is compared with the independent product formula above; the order of the displayed group is also checked against the computed class number. No unverified class group is used as an arithmetic input or a reason to exclude a field.

Quartic computation. All 12545 quartic candidates, including every negative case, were directly computed and verified in this manner. Exactly 483 have exponent dividing 2. Their class-number distribution is

h_N	1	2	4	8	16	32
$\#N$	47	160	112	132	26	6.

Their largest conductor is 233905.

Octic computation and explicit exclusions. Among unordered pairs of the 483 quartic survivors, exactly 12922 have quadratic intersection. Their composita give 8686 distinct octic candidates. Every candidate is decided as follows.

1. Ramified norm descent excludes 6848 candidates with an imaginary quartic subfield absent from the complete 483-field list. Another 623 are excluded by already verified class groups of unramified quartic subfields whose exponent or 4-rank violates norm descent. These give 7471 exclusions at the first stage.
2. For a quartic subfield F over which N/F is unramified, norm descent requires exponent dividing 4 and at most one cyclic factor of order 4. Applying the preceding refinement to its imaginary quadratic subfields excludes another 817 octics, using the complete quadratic lists and exact ramification tests.
3. The remaining quartic-subfield questions were resolved by 735 direct, unconditionally verified quartic computations. Their class-group exponent or 4-rank excludes another 237 octics.
4. The remaining 161 octic candidates were all directly computed and verified. Exactly 99 have exponent dividing 2.

The three exclusion sets are disjoint and, together with the 161 directly tested candidates, exhaust all 8686 candidates, since $7471 + 817 + 237 + 161 = 8686$. Each excluded field has an explicit obstructing subfield in the supplied data. The surviving class-number distribution is

h_N	1	2	4	8	16	32
$\#N$	17	27	19	32	1	3.

Their largest conductor is 6460.

Degrees sixteen and thirty-two. The 99 octic survivors give 674 unordered pairs with quartic intersection and 278 distinct composita of degree 16. Ramified norm descent to the complete octic list excludes 261. For the remaining 17, the unramified norm restriction is tested on 122 additional imaginary octic subfields, whose class groups are all directly computed and unconditionally verified. These exclude 14 more candidates. The three remaining fields are directly verified to have groups C_2, C_2^2, C_2^2 , and are

$$\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}, \sqrt{-5}), \quad \mathbb{Q}(\sqrt{-1}, \sqrt{-3}, \sqrt{-5}, \sqrt{-7}), \quad \mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \sqrt{-7}, \sqrt{-10}).$$

Their conductors are respectively 120, 420, 840.

The three pairwise composita of these fields all equal

$$N_{32} = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}, \sqrt{-5}, \sqrt{-7}).$$

Its subfield $M = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-5}, \sqrt{-7})$ has class group C_4 , again checked with `bnfinit` and `bnfcertify`. The exact discriminants give

$$\frac{|\text{disc } N_{32}|}{|\text{disc } M|^2} = 3^{16} > 1.$$

Thus N_{32}/M ramifies and norm surjectivity excludes N_{32} . The earlier descent proves that every possible higher-degree example would contain an eligible degree-32 subfield. None therefore exist.

Finally, the 483, 99, and 3 computed squareclass subgroups have been compared individually with the published Tables 4, 5, and 6 of [44]; their sets agree exactly. The 99 and 3 class numbers also agree entry by entry. The table transcriptions, visually checked corrections of the scanned text, and comparison program are included with the computations. A second enumeration, written independently using binary vectors of prime squareclasses and importing none of the first enumeration's functions, checks all candidate sets, intersection counts, exclusion partitions, discriminants, group orders, and the final conductor and class-number maxima. It gives $65 + 483 + 99 + 3 = 650$, as asserted. $\square$

Scope of the computation. The analytic completeness of the quadratic inputs comes from the preceding unconditional theorems. The remaining proof is finite arithmetic, verified without GRH-dependent bounds for class-group generators. The attached archive contains the executable inputs, complete PARI outputs for all computations used in the proof, explicit subfield exclusions, the independently written enumeration check, and the complete 650-field list. A preliminary slow computation of a degree-16 negative case was stopped after its exclusion had been proved from an octic subfield; its partial log is retained and is not used in the proof.

22 The complete Richaud–Degert class-number-two classification

For this section, a squarefree integer $D > 1$ is of *extended Richaud–Degert type* if there are integers $m \geq 1$ and $r \neq 0$ such that

$$D = m^2 + r, \quad r \mid 4m.$$

This is the divisibility definition in [94, Introduction]; no additional normalization of r is imposed. We use D for the squarefree radicand and $\Delta = D$ if $D \equiv 1 \pmod{4}$, and $\Delta = 4D$ otherwise, for the fundamental discriminant. The class number is the ordinary ideal class number, without a positivity condition on generators.

Theorem 22.1 (Mollin’s complete list). *There are exactly 107 real quadratic fields of extended Richaud–Degert type with ordinary class number two. Their squarefree radicands are precisely the following:*

10	15	26	30	34	35	39
42	51	65	66	78	85	87
95	102	105	110	119	122	123
138	143	146	165	182	194	203
205	215	221	222	230	258	285
287	318	327	357	362	365	395
402	429	447	482	485	527	533
623	629	635	645	678	741	782
843	885	902	957	965	1022	1085
1157	1173	1205	1245	1298	1469	1517
1533	1605	1685	1853	1965	2013	2037
2045	2085	2093	2117	2301	2373	2397
2613	2717	2813	3005	3237	3365	3597
3605	3813	4245	4277	4773	4893	5645
5757	5885	5957	6573	7157	7733	8333
9005	14405					

The list is the one in [94, Theorems 3.1–3.13 and Remark 3.1]; its completeness now requires no GRH.

Lemma 22.2 (A regulator bound for the full divisibility family). *If $D \geq 3$ is of extended Richaud–Degert type and R_D denotes the logarithm of its fundamental unit greater than one, then*

$$R_D \leq \log(16D).$$

Proof. Fix a representation $D = m^2 + r$ as above and put

$$\eta = \frac{(m + \sqrt{D})^2}{|r|}.$$

Its norm is one, and its trace is

$$\frac{4m^2}{|r|} + 2 \operatorname{sgn}(r) \in \mathbb{Z},$$

because $|r| \mid 4m$. Thus η is an algebraic integer unit. It is greater than one: equivalently, $(m + \sqrt{D})^2 > |m^2 - D|$, which holds for $m, D > 0$. Consequently $R_D \leq \log \eta$, regardless of whether the fundamental unit has norm 1 or -1 .

The divisibility condition implies $|r| \leq 4m$, and hence $(m - 2)^2 \leq D + 4$ and $m \leq 2 + \sqrt{D + 4}$. Since $|r| \geq 1$,

$$\eta \leq (2 + \sqrt{D + 4} + \sqrt{D})^2 \leq 16D \quad (D \geq 3).$$

For the last inequality, $\sqrt{D + 4} \leq 3\sqrt{D} - 2$ follows by squaring, since it is equivalent to $8D \geq 12\sqrt{D}$. This proves the bound. $\square$

Lemma 22.3 (An explicit cutoff). *If an extended Richaud–Degert field has class number two, then $D < 10^8$.*

Proof. Tatuzawa's original real-character lemma [95, Lemma 9, with the hypotheses on p. 170] applies to every primitive real Dirichlet character, of either parity. It states that, for $0 < \epsilon < 1/2$ and $\Delta \geq \max(e^{11.2}, e^{1/\epsilon})$, the inequality

$$L(1, \chi_\Delta) \leq 0.655\epsilon\Delta^{-\epsilon}$$

forces a real zero in $(1 - \epsilon/4, 1)$. This entire interval lies to the right of $7/8$, so Theorem 1.1 excludes that alternative. Taking $\epsilon = 1/\log \Delta$, for $\Delta \geq e^{11.2}$ we obtain

$$L(1, \chi_\Delta) > \frac{0.655}{e \log \Delta}.$$

The real quadratic class-number formula, with the ordinary class number and the fundamental unit of either norm, is

$$2h_D R_D = \sqrt{\Delta} L(1, \chi_\Delta).$$

If $h_D = 2$ and $D \geq 10^8$, Lemma 22.2 would therefore imply

$$4 \log(16D) \geq 4R_D > \frac{0.655\sqrt{\Delta}}{e \log \Delta} \geq \frac{0.655\sqrt{D}}{e \log(4D)}.$$

This is impossible. Indeed, at $D = 10^8$,

$$\frac{\sqrt{D}}{\log(4D) \log(16D)} > \frac{10000}{20 \cdot 22} = \frac{250}{11} > \frac{4e}{0.655},$$

using $\log(4 \cdot 10^8) < 20$, $\log(16 \cdot 10^8) < 22$, and $4e/0.655 < 16.61$. The expression on the left increases for $D \geq 10^8$, since its logarithmic derivative with respect to $\log D$ is

$$\frac{1}{2} - \frac{1}{\log(4D)} - \frac{1}{\log(16D)} > 0.$$

The contradiction proves the cutoff. □

Proof of Theorem 22.1. The preceding lemma reduces the problem to squarefree $D < 10^8$. The finite search is exhaustive with the following explicit bounds: for $1 \leq m \leq 10002$, enumerate every positive divisor s of $4m$ and form $D = m^2 + s$ and $D = m^2 - s$. Keep $1 < D < 10^8$ that are squarefree, and remove duplicates. Every possible field occurs because

$$m \leq 2 + \sqrt{D+4} < 2 + \sqrt{10^8+4} < 10003.$$

Conversely, every retained radicand satisfies the defining condition. This gives exactly 149024 distinct squarefree radicands. An independent enumeration, reversing the divisor loops and testing squarefreeness with an integer sieve, gives the identical candidate set.

For each retained radicand, compute the full ideal class group and verify the computation with PARI/GP's unconditional `bnfcertify` routine. Select the fields whose class number is two. The resulting set is exactly the displayed set of 107 radicands. The program, complete enumeration record, and comparison with the independently transcribed published list accompany the computational supplement. In particular, completeness uses the full finite enumeration, not merely verification of the 107 positive entries. Together with the analytic cutoff, this proves the theorem. □

Source conventions and scope. The theorem recovers the global classification in [94, Introduction and Remark 3.7]. Several displayed lists in that source are labeled Δ even though their entries are the radicands $D = \Delta/4$; its worked examples make the intended convention clear. The table here consistently lists radicands. We do not import the source’s separate continued-fraction and prime-producing-polynomial equivalences, some of which have additional typographical defects. The complete search and the regulator argument above provide an independent route to the stated global classification.

22.1 The complete class-number-one list in the same family

The same finite enumeration also settles the earlier conditional class-number-one list. Louboutin [102, pp. 315–316] records the following 43 radicands, attributing the classification under the extended Riemann hypothesis to his work and to Mollin–Williams. That source normalizes r by $-m < r \leq m$ or permits $r = \pm 4m/3$. Here we prove the identical list for the full divisibility definition of extended Richaud–Degert type from the beginning of this section, which contains that family.

Corollary 22.4 (The complete extended Richaud–Degert class-number-one list). *There are exactly 43 real quadratic fields of extended Richaud–Degert type with ordinary class number one. Their squarefree radicands are precisely*

2	3	5	6	7	11	13
14	17	21	23	29	33	37
38	47	53	62	69	77	83
93	101	141	167	173	197	213
227	237	293	398	413	437	453
573	677	717	1077	1133	1253	1293
1757						

Proof. The cutoff proof for Lemma 22.3 actually excludes every field with $h_D \leq 2$ and $D \geq 10^8$. Indeed, its only use of the class-number value is

$$\sqrt{\Delta}L(1, \chi_\Delta) = 2h_DR_D \leq 4R_D \leq 4\log(16D),$$

which holds for all such h_D . The same Tatzuwa lower bound contradicts this inequality for $D \geq 10^8$. Thus every field in this corollary is among the 149024 candidates already enumerated and unconditionally verified in the proof of Theorem 22.1.

Selecting the records with class number one gives exactly the 43 displayed radicands. This selected list has been compared, entry by entry, with the published list on pp. 315–316 of [102]; the two lists agree. All positive entries and all exclusions use the same complete arithmetic verification as the class-number-two classification. This proves both directions without a further hypothesis or a new enumeration. $\square$

This corollary concerns the complete divisibility family. Several subfamilies already have unconditional classifications: Lee’s Theorem 1.1 [104] treats the wide types not congruent to 5 modulo 8, and Biró–Lapkova’s Theorem 1.1 [103] treats $D = (an)^2 + 4a$ with a, n odd and positive. Those earlier conclusions are not counted again here. The new use of the imported zero-free strip is the completeness of the full published 43-field list; its proof shares the regulator bound, cutoff, and complete computation above.

23 A complete polynomial-factorization classification

For a positive integer n , let $\omega(n)$ denote its number of distinct prime divisors. For odd $d \geq 1$, put

$$M_{\text{odd}}(d) = \max_{\substack{1 \leq x \leq \sqrt{d} \\ x \text{ odd}}} \omega(d + x^2).$$

The following is the complete classification in [96, Theorem 1.3]. The published statement allows one exceptional value without its restricted Riemann hypothesis.

Theorem 23.1. *Let $d \equiv 7 \pmod{8}$ be prime or a product of two distinct primes. Then $M_{\text{odd}}(d) \leq 2$ if and only if*

$$d \in \{7, 15, 23, 31, 39, 47, 55, 79, 103, 127, 151, 223, 247, \\ 463, 487, 583, 823, 1087, 1423\}.$$

For each such d , the ideal class group of $\mathbb{Q}(\sqrt{-d})$ is cyclic and is generated by the class of either prime ideal above 2. Its class number satisfies $h(-d) \leq \log(2d)/\log 2$.

Lemma 23.2. *For a squarefree $d \equiv 7 \pmod{8}$ with $M_{\text{odd}}(d) \leq 2$, the class group is generated by a prime above 2. If d is prime or the product of two distinct primes, then*

$$h(-d) \leq \frac{\log(3d)}{\log 2}.$$

Proof. Write $K = \mathbb{Q}(\sqrt{-d})$ and $(2) = \mathfrak{p}_2 \bar{\mathfrak{p}}_2$. The ideal classes of prime ideals of norm at most $\sqrt{d}$ generate $\text{Cl}(K)$: the usual imaginary quadratic Minkowski bound is $2\sqrt{d}/\pi < \sqrt{d}$, and factoring the resulting integral ideal gives this assertion. Inert prime ideals are principal.

Let $\ell \leq \sqrt{d}$ be an odd noninert prime. There is an odd x with $1 \leq x \leq \ell$ and $x^2 \equiv -d \pmod{\ell}$; use the two opposite roots and choose the odd representative, with $x = \ell$ when the root is zero. Since $8 \mid d + x^2$ and $M_{\text{odd}}(d) \leq 2$, we have

$$d + x^2 = 2^a \ell^b, \quad a \geq 3, \quad b \geq 1.$$

If $b \geq 2$, squarefreeness implies $\ell \nmid x$. Set $x' = 2\ell - x$. Then x' is positive and odd, and

$$(x')^2 \leq 4\ell^2 \leq \frac{1}{2} 2^a \ell^b = \frac{1}{2} (d + x^2) \leq d.$$

Furthermore, ℓ divides $d + (x')^2$ exactly once, because $d + (x')^2 = d + x^2 + 4\ell^2 - 4\ell x$. The defining polynomial condition therefore gives $d + (x')^2 = 2^{a'} \ell$. Thus, in either case, there is an odd u such that

$$d + u^2 = 2^v \ell, \quad v \geq 3.$$

The integer $\alpha = (u + \sqrt{-d})/2$ has norm $2^{v-2}\ell$. Its principal ideal is primitive: if a rational integer greater than one divided α in $\mathcal{O}_K$, it would divide the coefficient 1 of $(1 + \sqrt{-d})/2$. Consequently $(\alpha) = \mathfrak{q}_2^{v-2} \mathfrak{q}_\ell$ for primes above 2 and ℓ . The class of either prime above ℓ is therefore in $\langle [\mathfrak{p}_2] \rangle$. This proves the cyclicity assertion.

Suppose first that $d = pq$ with odd primes $p < q$. Taking $x = p$ shows that $p + q = 2^a$ with $a \geq 3$. Also $q < 9p$. Otherwise both $x = p$ and $x = 3p$ are permitted, and the same condition gives $q + p = 2^a$ and $q + 9p = 2^b$ with $b > a$. Subtracting gives $8p = 2^a(2^{b-a} - 1)$, whence $a = 3$ and $p + q = 8$, contrary to $q \geq 9p$. Now put

$$\alpha = \frac{(q - p)/2 + \sqrt{-pq}}{2}.$$

Since $(q - p)/2$ is odd, this is an algebraic integer, and

$$N\alpha = \frac{(p + q)^2}{16} = 2^{2a-4}.$$

Its ideal is again primitive, so the order of $[\mathfrak{p}_2]$ divides $2a - 4$. Since $1 < q/p < 9$,

$$2^{2a-4} = \frac{(p + q)^2}{16} < \frac{25}{36}pq < d.$$

It follows that $h(-d) \leq 2a - 4 < \log d / \log 2$.

Suppose next that $d = p$ is prime. The prime $p \equiv 7 \pmod{8}$ splits in $\mathbb{Z}[\sqrt{2}]$, a principal ideal domain with unit $1 + \sqrt{2}$ of norm -1 . Hence there is an element of norm $-p$. Multiplying it by a power of $3 + 2\sqrt{2}$, and changing its sign, puts its positive real embedding z_0 in

$$(\sqrt{2} - 1)\sqrt{p} \leq z_0 < (\sqrt{2} + 1)\sqrt{p}.$$

The other embedding is $-p/z_0$. Writing the element as $x + y\sqrt{2}$, and replacing it by the negative of its conjugate if necessary, gives integers $0 < x < \sqrt{p}$, $0 < y < \sqrt{p}$ with $p + x^2 = 2y^2$. The bounds follow from $|x| = |z_0 - p/z_0|/2$ and $y = (z_0 + p/z_0)/(2\sqrt{2})$; their endpoints cannot be attained by integers since p is not a square. Congruences modulo 8 show that x is odd and $y = 2z$, so

$$p + x^2 = 8z^2.$$

If $z = 2^u$, the primitive integer $(x + \sqrt{-p})/2$ has norm 2^{2u+1} , and thus $h(-p) \leq 2u + 1 \leq \log(p/2)/\log 2$.

If z is not a power of 2, observe that $0 < 2z - x \leq \sqrt{p}$ and

$$p + (2z - x)^2 = 4z(3z - x), \quad \gcd(z, 3z - x) = 1.$$

The gcd assertion follows from $p + x^2 = 8z^2$: a prime common to z and x would have its square divide p . The polynomial condition and the presence of an odd prime in z force $3z - x = 2^u$. Then

$$p + (-3x + 8z)^2 = 8(3z - x)^2 = 2^{2u+3}.$$

The primitive integer $(-3x + 8z + \sqrt{-p})/2$ therefore has norm 2^{2u+1} and $h(-p) \leq 2u + 1$. For $0 \leq x \leq \sqrt{p}$, the function $\sqrt{8p + 8x^2} - 3x$ is positive and decreasing, so

$$0 < -3x + 8z \leq \sqrt{8p}, \quad 2^{2u+1} \leq \frac{9p}{4} < 3p.$$

This proves the stated bound in every case. □

Proof of Theorem 23.1. For $d \geq e^{11.2}$, Tatuzawa's Lemma 9 and the 7/8 strip give

$$L(1, \chi_{-d}) > \frac{0.655}{e \log d}.$$

Indeed, its contrary inequality with $\epsilon = 1/\log d$ forces a real zero in $(1 - \epsilon/4, 1)$, as in the proof of Lemma 22.3. Here the imaginary quadratic class-number formula is $\pi h(-d) = \sqrt{d}L(1, \chi_{-d})$. Lemma 23.2 consequently implies

$$\frac{\sqrt{d}}{\log d \log(3d)} < \frac{\pi e}{0.655 \log 2} < 19.$$

This is impossible for $d \geq 10^8$: at that endpoint the left side exceeds $10000/(19 \cdot 20) > 26$, and its logarithmic derivative is $1/2 - 1/\log d - 1/\log(3d) > 0$ thereafter. Thus $d < 10^8$.

The remaining verification is an exhaustive computation with integers. Initialize $\omega(n) = 0$ for $1 \leq n \leq 2 \cdot 10^8$. For $p = 2, 3, \dots, 2 \cdot 10^8$, if its current entry is zero, increment the entry of every positive multiple of p . Such p are exactly the primes: a composite already has a smaller prime divisor, while a prime has none. The final entries are therefore exactly the numbers of distinct prime divisors.

For every one of the 12500000 integers $7 \leq d < 10^8$ with $d \equiv 7 \pmod{8}$, test successive positive odd x while $x^2 \leq d$, rejecting the value as soon as $\omega(d + x^2) > 2$. Every array access satisfies $d + x^2 < 2 \cdot 10^8$. This examines 14416679 polynomial values in total and leaves the displayed nineteen values together with 63, 135, 175, 207, 343. The latter five are not squarefree. Exact trial division of the survivors confirms that each of the nineteen retained values is prime or a product of two distinct primes. The program and its complete output are included in the computational supplement.

An independent sieve, marking numbers whose odd part is one or a power of a single odd prime, gives exactly the same test outcomes and survivor lists. Thus the finite classification was reproduced without using the distinct-prime-divisor counting sieve.

Cyclicity and the generator assertion follow from Lemma 23.2. For the precise remaining numerical bound in the published statement, enumerate the reduced positive definite integral binary quadratic forms of discriminant $-d$ for the nineteen values. The class numbers, in the displayed increasing order, are

$$1, 2, 3, 3, 4, 5, 4, 5, 5, 5, 7, 7, 6, 7, 7, 8, 9, 9, 9.$$

This enumeration takes $1 \leq a \leq \sqrt{d/3}$, $-a \leq b \leq a$, $c = (b^2 + d)/(4a) \in \mathbb{Z}$, $a \leq c$, $\gcd(a, b, c) = 1$, with $b \geq 0$ when $|b| = a$ or $a = c$. These are exactly the usual reduced-form representatives. The integer inequalities $2^{h(-d)} \leq 2d$ hold for every entry, and prove the stated bound without rounding logarithms. $\square$

The full odd-parameter list. Combining this theorem with the already unconditional [96, Theorems 1.1–1.2] gives the exact classification for all odd positive d : besides the nineteen values above, the values are

$$\{1, 9, 25, 27, 49, 63, 135, 175, 207, 343\} \quad \text{and} \quad \{3, 5, 11, 13, 17, 19, 37, 43, 67, 73, 97, 163, 193\}.$$

Thus there are 42 odd positive parameters in total. The new unconditional part is the formerly exceptional nineteen-value case; the other two parts are cited published unconditional results.

Source and verification scope. The generator argument follows [96, Section 5], with its unit normalization supplied explicitly and its semiprime generator and numerical estimates corrected above. These repairs yield a safe preliminary bound $h(-d) \leq \log(3d)/\log 2$; the exact published bound follows after the complete enumeration. The cutoff uses the original real-zero alternative of Tatzuza, rather than assuming the source's restricted Riemann hypothesis. No conclusion is asserted for the separate even-parameter conjectures in that paper.

24 Class-group exponents of simplest cyclic cubic fields

We use the precise convention of Louboutin [85]. For an integer $m \geq -1$, put

$$P_m(X) = X^3 - mX^2 - (m+3)X - 1, \quad f_m = m^2 + 3m + 9, \quad K_m = \mathbb{Q}(\rho_m), \quad P_m(\rho_m) = 0.$$

Restrict to the values of m for which $\mathcal{O}_{K_m} = \mathbb{Z}[\rho_m]$. Equivalently, either $3 \nmid m$ and f_m is squarefree, or $m \equiv 0, 6 \pmod{9}$ and $f_m/9$ is squarefree. For these parameters $K_m/\mathbb{Q}$ is cyclic of degree 3, has conductor f_m , and has discriminant f_m^2 . This restriction is part of the term “simplest cubic field” in that paper; it must not be silently dropped.

Lemma 24.1 (A small prime splitting in a cyclic cubic field). *There is an effective absolute constant C_2 such that every cyclic cubic field of conductor f has a rational prime $p \nmid f$ which splits completely and satisfies $p \leq C_2(\log(3f))^8$.*

Proof. Let χ be a primitive cubic Dirichlet character associated with the field; the other nontrivial character is $\bar{\chi}$. For $p \nmid f$, complete splitting is equivalent to $\chi(p) = 1$. Adding the two instances of (4) and the principal smoothed sum gives

$$\sum_{n \leq x} \Lambda(n)(1 + \chi(n) + \bar{\chi}(n))(1 - n/x) = \frac{x}{2} + O(x^{7/8} \log(3f) + x^{7/8} \log^2(2x) + \log(fx)).$$

For an unramified prime p , the coefficient in parentheses is 3 when p splits completely and 0 otherwise. If no such split prime lies below x , only ramified prime powers and higher prime powers can contribute. Their total is

$$O(\log(3f) \log x + \sqrt{x} \log^2(2x)),$$

by exactly the elementary prime-power estimates used in Lemma 16.1. At $x = C_2(\log(3f))^8$ this contradicts the main term when C_2 is sufficiently large. The estimates are effective; a further finite enlargement handles the remaining conductors. This proves the assertion. $\square$

Theorem 24.2 (Louboutin’s exponent-growth conclusion). *Let e_m be the exponent of $\text{Cl}(K_m)$ in the family just defined. For every permitted $m \geq 1$,*

$$e_m \geq \frac{\log(2m+3)}{\log C_2 + 8 \log \log(3f_m)}.$$

In particular, effectively,

$$e_m \gg \frac{\log m}{\log \log m} \quad (m \geq 3),$$

so the exponents tend to infinity and only finitely many fields in this family have any fixed bounded class-group exponent.

Proof. The unconditional arithmetic input is [85, Proposition 9(1)]: the least absolute norm of a nonzero principal integral ideal of K_m which is not (n) for a rational integer $n \geq 1$ equals $2m+3$ (we use it only for $m \geq 1$). Louboutin derives this from the minimum-norm theorem of Lemmermeyer–Pethő [86, Theorem 1].

Choose p as in Lemma 24.1. Its factorization is $(p) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$, with three distinct prime ideals of norm p . Since e_m annihilates the class group, $\mathfrak{p}_1^{e_m}$ is a principal integral ideal. It cannot equal (n) for a positive rational integer n : a rational integer has equal valuations at the three primes above p , whereas this ideal has valuations $(e_m, 0, 0)$. Its norm is therefore at least $2m+3$, so

$$2m+3 \leq p^{e_m} \leq (C_2(\log(3f_m))^8)^{e_m}.$$

Taking logarithms gives the displayed bound. Since $f_m \asymp m^2$, the claimed order of magnitude and divergence follow. For fixed E , the inequality $2m+3 \leq (C_2(\log(3f_m))^8)^E$ places m in an effective finite interval; the two excluded small parameters $-1, 0$ cause no issue. $\square$

This is the full order-of-magnitude conclusion of the formerly GRH-dependent [85, Proposition 9(4)]. The paper's separate exact five-field classification for exponent 2 used a stronger numerical cutoff; its completeness does not follow just by replacing that cutoff by a qualitative logarithmic bound. Also, the paper's exponent-3 classification was already unconditional and is not counted as a new consequence here.

25 Daileda's class-number bound for pure cubic fields

This application uses the full finite-order Hecke statement of [58, Theorem 1.1], rather than only its Dirichlet consequence: for $K_0 = \mathbb{Q}(\sqrt{-3})$, every finite-order Hecke L -function over K_0 has no zero in $\Re s > 7/8$. The primitive characters used below have order three. Their conductors vary, while their base field is always K_0 .

Lemma 25.1 (The $L(1)$ upper bound over the Eisenstein field). *Let η be a nonprincipal primitive finite-order Hecke character of K_0 , of conductor $\mathfrak{f}$, and put $Q = 3N\mathfrak{f}$. Then*

$$|L_{K_0}(1, \eta)| \ll \ell(Q),$$

with an absolute effective implied constant.

Proof. Extend η by zero on ideals not coprime to $\mathfrak{f}$. For a nonzero integral ideal $\mathfrak{a}$, put $\Lambda_{K_0}(\mathfrak{a}) = \log N\mathfrak{p}$ if $\mathfrak{a} = \mathfrak{p}^j$ for a prime ideal $\mathfrak{p}$ and $j \geq 1$, and put it equal to zero otherwise. Define

$$\Psi_\eta(x) = \sum_{N\mathfrak{a} \leq x} \Lambda_{K_0}(\mathfrak{a}) \eta(\mathfrak{a}).$$

The completed Hecke L -function has degree two, conductor Q , and a fixed complex gamma factor, because a finite-order character has trivial archimedean type. Its functional equation relates η and $\bar{\eta}$. Thus its nontrivial zeros lie in $1/8 \leq \Re \rho \leq 7/8$, and its ordinary zero count is

$$\#\{\rho : |\Im \rho| \leq T\} \ll (T+1) \log(Q(T+2)).$$

The unconditional truncated explicit formula consequently gives

$$\Psi_\eta(x) \ll x^{7/8} \log^2(Qx) \quad (x \geq 2). \quad (76)$$

Here is the uniformity argument. At a half-integer x , take a permissible height $T \asymp x$ in the explicit formula. Its zero sum is $-\sum_{|\Im \rho| \leq T} x^\rho / \rho$; the error and the contributions at zero are $O(\log^2(Qx))$. The zero count and $\Re \rho \geq 1/8$ bound $\sum_{|\Im \rho| \leq T} |\rho|^{-1}$ by $O(\log^2(Q(T+2)))$. The constant term at zero is $O(\log Q)$: subtract the completed logarithmic derivatives at 1 and 2, whose zero contributions are bounded absolutely by $\sum_\rho |(1-\rho)(2-\rho)|^{-1} \ll \log Q$, and then use the functional equation and the absolutely convergent series at 2. Finally, the coefficient of a rational prime power p^j in $-L'_{K_0}/L_{K_0}$ has absolute value at most $2 \log p$. Moving to a neighboring half-integer therefore costs only $O(\log(2x))$. These are precisely the explicit-formula arguments of Lemma 1.2, with fixed degree two in place of degree one.

The Euler-product logarithm and summation by parts, using (76), now give

$$\log L_{K_0}(1, \eta) = \sum_{N\mathfrak{a} \leq y} \frac{\Lambda_{K_0}(\mathfrak{a}) \eta(\mathfrak{a})}{N\mathfrak{a} \log N\mathfrak{a}} + O\left(\frac{y^{-1/8} \log^2(Qy)}{\log y}\right). \quad (77)$$

As in Lemma 1.3, the logarithm is continued from the Euler product on the positive real interval $s > 1$. The same tail integral proves convergence and the stated error; there is no pole because η is nonprincipal.

The untwisted positive sum on the right has coefficient one:

$$\sum_{\mathbf{N}\mathbf{a} \leq y} \frac{\Lambda_{K_0}(\mathbf{a})}{\mathbf{N}\mathbf{a} \log \mathbf{N}\mathbf{a}} = \log \log y + O(1). \quad (78)$$

Indeed, higher powers contribute $O(1)$; rational primes $p \equiv 1 \pmod{3}$ give two prime ideals of norm p , rational primes $p \equiv 2 \pmod{3}$ give one prime ideal of norm p^2 , and the only ramified rational prime is 3. Hence the sum is $2 \sum_{p \leq y, p \equiv 1 \pmod{3}} p^{-1} + O(1) = \log \log y + O(1)$, by the unconditional Mertens estimate for the fixed progression $1 \pmod{3}$.

Take $y = (\log(3Q))^{24}$ in (77). Its error is bounded absolutely. Taking real parts, using $\Re \eta(\mathbf{a}) \leq 1$, and applying (78) gives $\log |L_{K_0}(1, \eta)| \leq \log \log y + O(1)$. Exponentiation proves the lemma. $\square$

Theorem 25.2 (Daleda's pure cubic bound, without GRH). *There is an effective absolute constant C such that every pure cubic number field $F = \mathbb{Q}(\sqrt[3]{m})$ of degree three, with absolute discriminant D_F and ideal class number h_F , satisfies*

$$h_F \leq C \frac{\sqrt{D_F} \ell(D_F)}{\log D_F}.$$

For $D_F \rightarrow \infty$ this is the exact order of magnitude of the GRH-conditional pure cubic conclusion of [38, Proposition 3, p. 243].

Proof. Replacing m by a rationally equivalent radicand, take m to be a positive cube-free integer. The splitting field $N = F(\zeta_3)$ has group S_3 over $\mathbb{Q}$ and is cyclic of degree three over K_0 . If η is either nontrivial character of $\text{Gal}(N/K_0)$, viewed by class field theory as a primitive finite-order Hecke character, Artin induction gives

$$\zeta_F(s) = \zeta(s) L_{K_0}(s, \eta). \quad (79)$$

Explicitly, the degree-three permutation representation of S_3 is the sum of the trivial representation and the irreducible representation $\text{Ind}_{A_3}^{S_3} \eta$. Induction of Artin L -functions therefore proves (79) at every prime, including ramified primes. The conductor-discriminant formula for this permutation representation gives

$$D_F = 3\mathbf{N}\mathfrak{f}_\eta.$$

Equivalently, the degree-two Artin L -function in [38, Lemma 7] has conductor D_F and is the finite-order Hecke L -function over K_0 just described. This identification requires neither the Artin conjecture nor GRH.

The signature of F is $(1, 1)$ and its only roots of unity are $\{1, -1\}$. Taking residues at 1 in (79), the analytic class-number formula yields

$$h_F = \frac{\sqrt{D_F}}{2\pi R_F} L_{K_0}(1, \eta), \quad (80)$$

where R_F is the regulator. The value on the right is positive, as is also immediate from the positive residue of ζ_F .

For completeness, the required regulator lower bound has a direct proof. Choose the fundamental unit ϵ positive and greater than 1 in the unique real embedding; then $R_F = \log \epsilon$ and $\mathbf{N}_{F/\mathbb{Q}} \epsilon = 1$.

Its other conjugates are $z, \bar{z}$, with $|z| = \epsilon^{-1/2}$. The unit is not rational, so it has degree three and $\mathbb{Z}[\epsilon]$ is an order in F . Consequently

$$D_F \leq |\text{disc}(\epsilon)| = |\epsilon - z|^4 |z - \bar{z}|^2 \leq 4\epsilon^{-1}(\epsilon + \epsilon^{-1/2})^4 \leq 64\epsilon^3.$$

Moreover, the nonzero integer $N_{F/\mathbb{Q}}(1 - \epsilon)$ has absolute value $(\epsilon - 1)|1 - z|^2 \leq 4(\epsilon - 1)$, so $\epsilon \geq 5/4$. It follows that

$$\log D_F \leq \log 64 + 3R_F \leq \left(3 + \frac{\log 64}{\log(5/4)}\right) R_F.$$

Thus $R_F \gg \log D_F$ with an explicit positive constant. Apply Lemma 25.1 with $Q = D_F$ to (80) to finish the proof. $\square$

The distinction between one and two powers of $\log \log D_F$ matters. A crude degree-two Euler-product majorant would lose this distinction. Here the fixed quadratic resolvent K_0 gives (78), which supplies the single power needed in Daileda's published pure cubic bound. The more general assertions in his Proposition 3 for arbitrary cubic fields have varying quadratic resolvent fields and are not asserted here.

26 The mean least completely split prime in cyclic fields

Fix an odd prime l , and let $\mathcal{K}_l(X)$ be the set of cyclic extensions $K/\mathbb{Q}$ of degree l with conductor $f_K \leq X$. Write $N_l(X) = \#\mathcal{K}_l(X)$, and let r_K be the least rational prime that splits completely in K . In particular, a ramified prime does not qualify. Define, for rational primes q ,

$$c_l(q) = \begin{cases} (l^2 - 1)/(l^2 + l - 1), & q = l, \\ \frac{l-1}{l} \frac{q+l}{q+l-1}, & q \equiv 1 \pmod{l}, \\ (l-1)/l, & q \neq l, q \not\equiv 1 \pmod{l}. \end{cases}$$

These numbers include the contribution of ramification in the probability of failing to split completely.

Theorem 26.1 (Pollack's mean-value theorem). *For every fixed odd prime l ,*

$$\lim_{X \rightarrow \infty} \frac{1}{N_l(X)} \sum_{K \in \mathcal{K}_l(X)} r_K = \Delta_l := \sum_{p \text{ prime}} p(1 - c_l(p)) \prod_{q < p} c_l(q).$$

The series converges. The same mean results when the fields are ordered by discriminant. This is the conclusion of [43, Theorem 1.2], with its RH assumptions removed. The case $l = 3$ was already unconditional in that paper, so the new cases of this transfer are $l \geq 5$.

Proof. We first prove the uniform estimate replacing the sole RH input in Pollack's argument. A field K as above corresponds to $l - 1$ primitive Dirichlet characters of order l and conductor f_K . Choose one, χ . Every χ^j , $1 \leq j < l$, is primitive of the same conductor: its kernel is the kernel of χ . For $p \nmid f_K$, character orthogonality gives

$$\mathbf{1}_{\{p \text{ splits completely in } K\}} = \frac{1}{l} \sum_{j=0}^{l-1} \chi(p)^j.$$

In the term $j = 0$ we use the principal character modulo f_K , so that the average is zero at integers not coprime to f_K . Apply (4) to the $l - 1$ nonprincipal characters, and Lemma 1.2 followed by integration to the principal term. After removing powers p^a with $a \geq 2$, this yields

$$\begin{aligned} & \sum_{\substack{p \leq y \\ p \text{ splits completely in } K}} \log p(1 - p/y) \\ &= \frac{y}{2l} + O_l(y^{7/8} \log(3f_K) + y^{7/8} \log^2(2y) + \log(3f_K) \log(2y) + \sqrt{y} \log^2(2y)). \end{aligned}$$

Here powers of primes dividing f_K contribute at most $O(\log(3f_K) \log(2y))$, while all powers with exponent at least two contribute $O(\sqrt{y} \log^2(2y))$. Put $y = C_l(\log(3f_K))^8$. The ratio of the first error term to y is $O_l(C_l^{-1/8})$; the remaining ratios tend effectively to zero as $f_K \rightarrow \infty$. Choose C_l large enough, and enlarge it effectively for the finitely many remaining conductors. The displayed sum is positive, proving

$$r_K \leq C_l(\log(3f_K))^8. \quad (81)$$

The finite enlargement can, for example, be made by enumerating the primitive order- l characters of the bounded conductors and testing successive primes; Dirichlet's theorem guarantees termination.

We next state exactly the unconditional counting results imported from [43]. Its Lemma 2.1 gives $N_l(X) \sim a_l X$ with $a_l > 0$. Its Lemma 3.1 gives, for every fixed finite set Q of rational primes,

$$\frac{\#\{K \in \mathcal{K}_l(X) : \text{no } q \in Q \text{ splits completely in } K\}}{N_l(X)} \longrightarrow \prod_{q \in Q} c_l(q). \quad (82)$$

Finally its Lemma 3.2, together with the $(l-1)$ -to-one character-field correspondence, gives constants $b_l, c'_l > 0$ such that, for $2 \leq u \leq (10l^2)^{-1} \log X$,

$$\#\{K \in \mathcal{K}_l(X) : r_K \geq u\} \leq b_l X \exp(-c'_l u / \log u). \quad (83)$$

These lemmas are unconditional. The higher reciprocity and Chebotarev arguments used to prove them are qualitative equidistribution statements for each fixed auxiliary field; they do not invoke an RH bound for those fields. In particular no zero-free theorem for general Kummer extensions is being assumed.

Fix $z \geq 2$. By applying (82) first to all primes below p , and then to all primes at most p , subtraction gives

$$\lim_{X \rightarrow \infty} \frac{\#\{K \in \mathcal{K}_l(X) : r_K = p\}}{N_l(X)} = (1 - c_l(p)) \prod_{q < p} c_l(q).$$

There are only finitely many primes $p \leq z$, so their contribution to the mean tends to the corresponding partial sum defining Δ_l .

To justify passage from partial sums to the full mean, set $u_X = (10l^2)^{-1} \log X$. For X large enough that $u_X > z$, (83) bounds the first part of the remaining sum by

$$\frac{1}{N_l(X)} \sum_{\substack{K \in \mathcal{K}_l(X) \\ z < r_K \leq u_X}} r_K \ll_l \sum_{\substack{p > z \\ p \text{ prime}}} p \exp(-c'_l p / \log p).$$

The series on the right converges, as is seen by comparison with $\sum_{m \geq 2} m \exp(-c'_l m / \log m)$, and its tail tends to zero as $z \rightarrow \infty$. For the second part, use (81) for every $f_K \leq X$ and (83) at u_X :

$$\frac{1}{N_l(X)} \sum_{\substack{K \in \mathcal{K}_l(X) \\ r_K > u_X}} r_K \ll_l (\log(3X))^8 \exp(-c'_l u_X / \log u_X) = o(1).$$

Consequently the tails of the finite means vanish uniformly after taking $\limsup_{X \rightarrow \infty}$ and then $z \rightarrow \infty$.

For completeness, $c_l(q) \leq \rho_l < 1$ for every sufficiently large prime q . Thus the p th summand in Δ_l is at most $O_l(p\rho_l^{\pi(p)})$. The elementary lower bound $\pi(t) \gg t/\log t$ proves convergence directly. Combining this convergence with the preceding tail estimates proves the asserted limit. Finally the conductor–discriminant formula is $|D_K| = f_K^{l-1}$, so changing from a discriminant cutoff to a conductor cutoff only replaces X by $X^{1/(l-1)}$. $\square$

27 The upper order of CM torsion in odd degrees

For a positive integer d , let $T_{\text{CM}}(d)$ be the largest cardinality of $E(F)_{\text{tors}}$, where F ranges over number fields of degree d and E/F ranges over elliptic curves with complex multiplication. The order of complex multiplication is allowed to be nonmaximal. Bourdon and Pollack [74, Theorem 1.3] determined, under GRH, the upper order of this function on odd degrees. We recover that order of magnitude; the numerical constant in their GRH upper bound is not claimed.

Theorem 27.1. *There is an effective absolute constant C such that, for every odd positive integer d ,*

$$T_{\text{CM}}(d) \leq C(d\ell(d))^{2/3}.$$

Moreover,

$$0 < \limsup_{\substack{d \rightarrow \infty \\ d \text{ odd}}} \frac{T_{\text{CM}}(d)}{(d \log \log d)^{2/3}} < \infty.$$

Proof. We state precisely the unconditional algebraic input. The Strong Odd Degree Theorem [74, Theorems 1.1–1.2] implies that the torsion group has order at most 4, or is cyclic of order p^n or $2p^n$, where $p \equiv 3 \pmod{4}$ is prime and $n \geq 1$. Write $h_p = h(\mathbb{Q}(\sqrt{-p}))$. If $p > 3$, then in either cyclic case

$$h_p \frac{p-1}{2} p^{\lfloor 3n/2 \rfloor - 1} \mid d. \quad (84)$$

The source gives an additional factor 3 in some cases; omitting that factor only weakens the necessary divisibility used here. If $p = 3$ and $n \geq 2$, it gives

$$3^{\lfloor 3n/2 \rfloor - 2} \mid d. \quad (85)$$

For $p = 3, n = 1$, the torsion order is at most 6. These statements hold for every CM order, including the nonmaximal orders that can achieve the smallest degrees.

Suppose first that $p > 3$. Since $-p$ is a negative fundamental discriminant, Corollary 1.5 yields the effective bound

$$h_p \gg \frac{\sqrt{p}}{\ell(p)}.$$

Using $(p-1)/2 \geq p/3$ and $\lfloor 3n/2 \rfloor + 1/2 \geq 3n/2$ for integral n , we obtain from (84)

$$d \geq h_p \frac{p-1}{2} p^{\lfloor 3n/2 \rfloor - 1} \gg \frac{p^{\lfloor 3n/2 \rfloor + 1/2}}{\ell(p)} \geq \frac{p^{3n/2}}{\ell(p)}.$$

Also, $h_p \geq 1$ and $\lfloor 3n/2 \rfloor - 1 \geq 0$ show that $p \leq 2d + 1$. The function ℓ is increasing and satisfies $\ell(2d+1) \ll \ell(d)$ for $d \geq 1$. Consequently

$$p^{3n/2} \ll d\ell(d), \quad \#E(F)_{\text{tors}} \leq 2p^n \ll (d\ell(d))^{2/3}.$$

For $p = 3, n \geq 2$, (85) and $\lfloor 3n/2 \rfloor \geq 3n/2 - 1/2$ imply

$$d \geq 3^{3n/2-5/2}, \quad \#E(F)_{\text{tors}} \leq 2 \cdot 3^n \leq 2 \cdot 3^{5/3} d^{2/3}.$$

The bounded torsion cases are absorbed into the absolute constant. This proves the asserted uniform upper bound, and hence the finiteness of the limsup.

For completeness, the positivity of the limsup was already unconditional in [74, Theorem 1.3(1)]. Its mechanism is as follows. Joshi's theorem [75, Theorem 1], in the form recorded in [74, Proposition 3.1], supplies infinitely many primes $p \equiv 3 \pmod{4}$, tending to infinity, such that

$$L(1, \chi_{-p}) \ll \frac{1}{\log \log p}.$$

Set $d_p = h_p(p-1)/2$. Genus theory gives h_p odd, since $-p$ has one prime discriminant factor; thus d_p is odd. Dirichlet's class number formula, for $p > 3$, gives

$$d_p = \frac{\sqrt{p}}{\pi} L(1, \chi_{-p}) \frac{p-1}{2} \ll \frac{p^{3/2}}{\log \log p}.$$

The Strong Odd Degree Theorem shows that a cyclic group of order p is realized in degree d_p when $p \equiv 3 \pmod{8}$, and one of order $2p$ is realized in degree d_p when $p \equiv 7 \pmod{8}$. In particular $T_{\text{CM}}(d_p) \geq p$. Since $d_p \geq (p-1)/2$, the degrees d_p tend to infinity. The preceding two inequalities give $\log \log d_p = \log \log p + O(1)$, and therefore

$$d_p \log \log d_p \ll p^{3/2}, \quad T_{\text{CM}}(d_p) \gg (d_p \log \log d_p)^{2/3}.$$

This proves positivity. □

Comparison with the published statement. Theorem 27.1 proves the qualitative upper-order conclusion of [74, Theorem 1.3]. The already unconditional lower bound there gives the more precise lower limsup constant $(12e^\gamma/\pi)^{2/3}$. Its upper limsup constant $(24e^\gamma/\pi)^{2/3}$ uses Littlewood's numerical GRH constant, which is not supplied by the fixed zero-free strip. The previously unconditional all-odd-degree estimate in that paper was $T_{\text{CM}}(d) \ll_\epsilon d^{2/3+\epsilon}$; the proof above replaces it by the published GRH order of magnitude.

28 The typical least degree of a CM point on a modular curve

For a modular curve $X/\mathbb{Q}$, let $d_{\text{CM}}(X)$ be the least residue-field degree over $\mathbb{Q}$ of a noncuspidal closed point represented by an elliptic curve with complex multiplication. For a negative quadratic-order discriminant Δ , let $d_{\Delta, \text{CM}}(X)$ denote the corresponding minimum with endomorphism order of discriminant Δ . The curves $X_0(N)$ and $X_1(N)$ classify, respectively, elliptic curves with a cyclic subgroup of order N and with a point of order N . All orders, including nonmaximal orders, are permitted.

Clark–Genao–Pollack–Saia proved the following two assertions under GRH [109, Theorem 1.7]. The proof below preserves their exact typical exponent. Their sharper maximal-order estimates in Theorems 1.3 and 1.5 are separate assertions and are not being transferred here.

Theorem 28.1 (The published typical-degree conclusions). *For every $\epsilon > 0$, all but $o(x)$ positive integers $N \leq x$ satisfy both*

$$2^{(1/2-\epsilon) \log \log x} \leq d_{\text{CM}}(X_0(N)) \leq 2^{(1/2+\epsilon) \log \log x}$$

and

$$N 2^{(1/2-\epsilon) \log \log x} \leq d_{\text{CM}}(X_1(N)) \leq N 2^{(1/2+\epsilon) \log \log x}.$$

Proof. We reproduce the counting argument of [109, §5.6], with the analytic estimates replaced explicitly. All logarithms in this proof are natural. It suffices by monotonicity to prove the assertions for $0 < \epsilon < 1/4$.

The algebraic inputs. Write h_Δ for the proper class number of the order. For squarefree B , put $B_- = \prod_{p|B, (\Delta/p)=-1} p$, where the symbols are Kronecker symbols, and put $\psi_0(B) = B \prod_{p|B} (1 + 1/p)$. The unconditional algebraic results [109, Lemma 4.4 and Proposition 4.6] give

$$d_{\Delta, \text{CM}}(X_0(B)) \asymp h_\Delta \psi_0(B_-), \quad B \text{ squarefree}, \quad (86)$$

$$\frac{\phi(N)}{6} d_{\text{CM}}(X_0(N)) \leq d_{\text{CM}}(X_1(N)) \leq \frac{\phi(N)}{2} d_{\text{CM}}(X_0(N)), \quad N \geq 3. \quad (87)$$

The constants in the first line are absolute and uniform in Δ and B . Also, if Δ is fundamental and $(\Delta/p) = 1$ for every $p \mid N$, then

$$d_{\text{CM}}(X_0(N)) \leq 2h_\Delta. \quad (88)$$

Indeed, over the Hilbert class field H of $K = \mathbb{Q}(\sqrt{\Delta})$, an elliptic curve with CM by $\mathcal{O}_K$ has a cyclic N -isogeny: choose at each $p^a \parallel N$ one of the two split prime ideals, to the power a , and multiply them. The resulting ideal I satisfies $\mathcal{O}_K/I \cong \mathbb{Z}/N\mathbb{Z}$, and its ideal isogeny is defined over H . Since $[H : \mathbb{Q}] = 2h_\Delta$, this proves (88), the fundamental-discriminant case of [109, Proposition 4.7]. For $B \mid N$, forgetting part of the level structure gives $d_{\Delta, \text{CM}}(X_0(B)) \leq d_{\Delta, \text{CM}}(X_0(N))$.

Theorem 1.4 and the order class-number formula give, with $b(t) = \log \log(3t)$,

$$\frac{c\sqrt{|\Delta|}}{b(|\Delta|)^2} \leq h_\Delta \leq C\sqrt{|\Delta|} b(|\Delta|)^2 \quad (89)$$

for every negative order discriminant. To check the lower bound as well as the upper bound, write $\Delta = f^2 D$ with D fundamental and use

$$h_\Delta = \frac{fh_D}{[\mathcal{O}_D^\times : \mathcal{O}_\Delta^\times]} \prod_{p|f} \left(1 - \frac{\chi_D(p)}{p}\right), \quad 1 \leq [\mathcal{O}_D^\times : \mathcal{O}_\Delta^\times] \leq 3.$$

The product lies between $\phi(f)/f$ and $f/\phi(f)$; $f/\phi(f) \ll b(f)$ proves (89). This includes the unit correction recorded in the authors' May 2026 errata.

The prime estimates. For every nonprincipal Dirichlet character modulo m , including an imprimitive one, Lemma 1.2 implies

$$\sum_{p \leq t} \chi(p) \ll t^{7/8} \log^2(3mt). \quad (90)$$

Pass first to the primitive character, remove prime powers, and then apply partial summation; the primes dividing m contribute at most $O(\log(3m))$ and are absorbed. Consequently $\sum_p \chi(p)/p$ converges and, uniformly for $T \geq Z \geq 2$,

$$\left| \sum_{Z < p \leq T} \frac{\chi(p)}{p} \right| \ll Z^{-1/8} \log^2(3mZ). \quad (91)$$

This follows by bounding the tail to infinity using (90). In particular its full sum has absolute value at most

$$\log \log \log(3m) + O(1), \quad (92)$$

after changing the absolute constant for bounded m : split at $Z = (\log(3m))^{32}$, bound the initial segment by $\sum_{p \leq Z} 1/p$, and apply (91). These are the replacements for the GRH estimates in [109, Lemma 5.7].

The lower typical bound. Fix $0 < \epsilon < 1/4$, let $L = \log \log x$, and restrict to

$$|\omega(N) - L| \leq \sqrt{L} \log L. \quad (93)$$

The Hardy–Ramanujan theorem excludes only $o(x)$ integers. Suppose $d_{\text{CM}}(X_0(N)) < 2^{(1/2-\epsilon)L}$ and choose the discriminant of a point achieving that degree. Apply (86) to $B = \text{rad}(N)$. Since $h_\Delta \geq 1$, (86) and (89) show, for sufficiently large x , that

$$|\Delta| < 2^{(1-\epsilon)L}, \quad (\Delta/p) \neq -1 \quad \text{if } p \mid N, \ p > 2^{L/2}. \quad (94)$$

For the first conclusion one may first invert $\sqrt{t}/b(t)^2 \ll 2^{(1/2-\epsilon)L}$ to get $t \leq \exp(O(L))$; its logarithmic denominator is then $\exp(o(L))$, which gives the asserted margin ϵL . For the second, a single such inert prime would make the degree $\gg p > 2^{L/2}$, a contradiction.

For each Δ in this range let $\mathcal{P}_\Delta$ be the primes $p \leq x$ for which either $p \leq 2^{L/2}$ or $(\Delta/p) \neq -1$. Equations (91) and (92), Mertens' estimate, and $\sum_{p \mid \Delta} 1/p \ll \log \log(3|\Delta|)$ give

$$\sum_{p \in \mathcal{P}_\Delta} \frac{1}{p} \leq \frac{L}{2} + O(\log L). \quad (95)$$

For clarity, use $\mathbf{1}_{(\Delta/p) \neq -1} = (1 + \chi_\Delta(p))/2 + \mathbf{1}_{p \mid \Delta}/2$, and enlarge the set by all the small primes.

We use the unconditional restricted Hardy–Ramanujan inequality [109, Lemma 5.8]: there are absolute $A, B > 0$ such that for any prime set $\mathcal{P} \subseteq [2, x]$ and $k \geq 1$,

$$\#\{n \leq x : \omega(n) = k, \ p \mid n \Rightarrow p \in \mathcal{P}\} \leq \frac{Ax}{\log x} \frac{(\sum_{p \in \mathcal{P}} p^{-1} + B)^{k-1}}{(k-1)!}.$$

For $k = L + O(\sqrt{L} \log L)$, Stirling's formula and (95) bound the right side by $x \exp(-(\log 2 + o(1))L)$, uniformly in Δ . Indeed the logarithm of its factor after x is $-L + k(1 + \log((L/2 + O(\log L))/k)) + O(\log L) = -(\log 2)L + o(L)$. There are at most $2^{(1-\epsilon)L}$ choices of Δ and $\exp(o(L))$ choices of k . The total is $x \exp(-(\epsilon \log 2 + o(1))L) = o(x)$. This proves the lower bound.

Preparation for the upper bound. Keep $0 < \epsilon < 1/4$ and put

$$\theta = (1 + \epsilon) \log 2, \quad U = (\log x)^\theta, \quad z = \exp(\sqrt{L}).$$

In addition to (93), restrict to integers $N \leq x$ for which the largest squarefull divisor is at most L , the largest divisor composed of primes at most z is at most $z^{\log L}$, and $P^+(N) > x^{1/L}$. Here P^+ and P^- denote largest and least prime factors, with $P^+(1) = 1$ and $P^-(1) = \infty$. Each restriction removes $o(x)$ integers, as follows. The squarefull restriction removes at most $x \sum_{s > L, \ s \text{ squarefull}} s^{-1} \ll x/\sqrt{L}$. For the second, the average logarithm of the z -smooth part is at most $\sum_{p \leq z} \sum_{a \geq 1} (\log p)/p^a \ll \log z$, so Markov's inequality gives $O(x/\log L)$ exceptions. Finally set $y = x^{1/L}$ and $\sigma = 1 - 1/\log y$. Rankin's bound gives

$$\#\{N \leq x : P^+(N) \leq y\} \leq x^\sigma \prod_{p \leq y} (1 - p^{-\sigma})^{-1} \ll x e^{-L} \log y = x/L.$$

The product bound follows from Mertens' theorem at $\sigma = 1$: its logarithm changes by $O(1)$ when σ moves to $1 - 1/\log y$, because $\sum_{p \leq y} (\log p)/p \ll \log y$ and $p^{1/\log y} \leq e$.

Let $\mathcal{D}$ be the negative fundamental discriminants with $U/2 < |\Delta| < U$. We will prove that, except for $o(x)$ of these admissible N , some $\Delta \in \mathcal{D}$ satisfies $(\Delta/p) = 1$ for every $p \mid N$. Equations (88) and (89) then give

$$d_{\text{CM}}(X_0(N)) \ll U^{1/2}(\log L)^2 < 2^{(1/2+\epsilon)L}$$

for sufficiently large x .

Write $N = p_0 p_1 \cdots p_k$, where p_0 is its entire z -smooth part and $z < p_1 < \cdots < p_k$ are primes. The squarefull restriction ensures that these large primes occur only once. The largest-prime restriction ensures $k \geq 1$, and (93) gives $k \leq L + o(L)$. For $0 \leq i \leq k$, let $\mathcal{D}_i$ contain those $\Delta \in \mathcal{D}$ splitting all primes dividing $p_0 p_1 \cdots p_i$. Uniformly in $p_0 \leq z^{\log L} = (\log x)^{o(1)}$,

$$|\mathcal{D}_0| \geq (\log x)^{\theta-o(1)}. \quad (96)$$

To see this, count the negative squarefree integers $\Delta \equiv 1 \pmod{8p_0}$ in the interval in question. They are fundamental and split 2 and every odd prime dividing p_0 . For $M_0 = 8p_0$, elementary Möbius inversion gives their number as

$$\frac{U}{2M_0} \prod_{p \nmid M_0} (1 - p^{-2}) + O(\sqrt{U}).$$

Indeed, only square divisors coprime to M_0 can occur; each such divisor d^2 leaves one residue class modulo M_0 , giving $U/(2M_0 d^2) + O(1)$, and the omitted tail of the main sum is $O(\sqrt{U}/M_0)$. Since $M_0 = U^{o(1)}$, the main term proves (96).

Choose $\delta > 0$ so small that $\theta + \log(1/2 - \delta) > 0$, and fix $0 < \theta' < \min\{1, \theta + \log(1/2 - \delta)\}$. If $\mathcal{D}_k$ is empty, let i be the first index with $|\mathcal{D}_{i+1}| \leq (1/2 - \delta)|\mathcal{D}_i|$. Then $|\mathcal{D}_i| \geq (1/2 - \delta)^i |\mathcal{D}_0| \geq (\log x)^{\theta'}$. Writing

$$M = p_0 p_1 \cdots p_i, \quad q = p_{i+1}, \quad r = p_{i+2} \cdots p_k,$$

we have

$$N = Mqr, \quad q > z, \quad P^-(r) > q > P^+(M), \quad T := x/M > x^{1/L}. \quad (97)$$

The set $\mathcal{D}(M) = \{\Delta \in \mathcal{D} : (\Delta/p) = 1 \text{ for all } p \mid M\}$ has size $J \geq (\log x)^{\theta'}$, and at least $(1/2 + \delta)J$ of its members fail to split q . The inequality for T follows because qr contains the largest prime factor of N . We now count such factorizations.

The case $r = 1$. Fix M and choose a prime $q \leq T$ uniformly. For $\Delta \in \mathcal{D}(M)$ define

$$X_\Delta(q) = \mathbf{1}_{(\Delta/q) \neq 1} = \frac{1 - \chi_\Delta(q)}{2} + \frac{\mathbf{1}_{q \mid \Delta}}{2}, \quad X(q) = \sum_{\Delta \in \mathcal{D}(M)} X_\Delta(q).$$

Because $T > x^{1/L}$ and $|\Delta\Delta'| \leq U^2$, (90) and $\pi(T) \gg T/\log T$ give

$$\mathbb{E}X_\Delta = \frac{1}{2} + O((\log x)^{-10}), \quad \mathbb{E}(X_\Delta X_{\Delta'}) = \frac{1}{4} + O((\log x)^{-10}) \quad (\Delta \neq \Delta').$$

For the second estimate, expand the product. Its character terms are $\chi_\Delta, \chi_{\Delta'}$ and $\chi_\Delta \chi_{\Delta'}$; the last is nonprincipal since distinct fundamental discriminants have distinct squareclasses. The primes dividing $\Delta\Delta'$ contribute $O(\log(U)/\pi(T))$, also absorbed in the stated error. Thus

$$\mathbb{E}(X - J/2)^2 \ll J + J^2(\log x)^{-10}.$$

Chebyshev's inequality bounds the fraction of bad primes by $O(J^{-1} + (\log x)^{-10}) \ll (\log x)^{-\theta'}$. Their number is at most

$$\ll \frac{xL}{M \log x} (\log x)^{-\theta'}.$$

Summing over $M \leq x$ gives $O(xL(\log x)^{-\theta'}) = o(x)$.

The case $r > 1$. For fixed M, q , the elementary upper-bound sieve gives

$$\#\{r \leq x/(Mq) : P^-(r) > P^+(M)\} \ll \frac{x}{Mq \log(2P^+(M))}. \quad (98)$$

We use this bound only when a factorization (97) exists, so $x/(Mq) > P^+(M)$, which is the required sieve range. It is also valid for $M = 1$ with the displayed normalization. This is the unconditional upper-bound sieve used in [109, §5.6, equation (18)].

For fixed M , give the primes $z < q \leq T$ probability $1/(qW)$, where $W = \sum_{z < q \leq T} q^{-1} = L + O(\log L)$. Define X_Δ and X as before. By (91), uniformly for each character of modulus at most U^2 involved in the expansion,

$$\left| \frac{1}{W} \sum_{z < q \leq T} \frac{\chi(q)}{q} \right| \ll z^{-1/8} L.$$

The primes dividing a discriminant contribute $O(z^{-1} \log U/W) = O(z^{-1})$. It follows that

$$\mathbb{E}(X - J/2)^2 \ll J + J^2 z^{-1/8} L.$$

Consequently the weighted fraction of bad primes is $O(J^{-1} + z^{-1/8} L)$. Since $J^{-1} \leq \exp(-\theta' L)$ and $z = \exp(\sqrt{L})$, we conclude, for large x , that

$$\sum_{\substack{z < q \leq T \\ X(q) \geq (1/2 + \delta)J}} \frac{1}{q} \ll W((\log x)^{-\theta'} + z^{-1/8} L) \ll z^{-1/10}. \quad (99)$$

Combine (98) and (99), and sum over M . The elementary estimate

$$\sum_{M \leq x} \frac{1}{M \log(2P^+(M))} \ll L$$

follows by taking $M = 1$ separately and grouping the other integers by their largest prime factor:

$$\sum_{\substack{M \geq 1 \\ P^+(M) = p}} \frac{1}{M} = \frac{1}{p} \prod_{\ell \leq p} (1 - 1/\ell)^{-1} \ll \frac{\log(2p)}{p}.$$

Therefore the number in the case $r > 1$ is $O(xLz^{-1/10}) = o(x)$. Both cases together prove that $\mathcal{D}_k \neq \emptyset$ except for $o(x)$ integers, completing the upper bound for $X_0(N)$.

Finally apply the two bounds just proved with $\epsilon/2$ in place of ϵ . Since $\phi(N)/N$ lies between $c/\log \log(3N)$ and 1, equation (87) absorbs this factor and the absolute constants into the available margin $2^{(\epsilon/2)L}$, uniformly for $3 \leq N \leq x$. The finitely many smaller levels have no effect. This proves the full assertion for $X_1(N)$ and finishes the theorem. $\square$

The same paper records the following GRH consequence immediately after Theorem 1.7 [109, p. 830]. We include the details because passing from prime moduli to arbitrary N requires accounting for prime powers and for nonsquares having a nontrivial square factor.

Corollary 28.2 (The published normal order of the least nonsquare that is a square modulo N). *Let $R(N)$ be the least positive integer which is not a square in $\mathbb{Z}$ but is congruent to a square modulo N . For every $\epsilon > 0$, all but $o(x)$ integers $N \leq x$ satisfy*

$$2^{(1-\epsilon) \log \log x} \leq R(N) \leq 2^{(1+\epsilon) \log \log x}.$$

In particular $R(N) = (\log N)^{\log 2 + o(1)}$ as N tends to infinity along a set of asymptotic density one.

Proof. For the upper bound repeat the discriminant-sieving portion of the preceding proof, again reducing to $0 < \epsilon < 1/4$ by monotonicity of the asserted bounds, with positive fundamental discriminants $U/2 < \Delta < U$, where $U = 2^{(1+\epsilon)\log\log x}$. Every estimate remains valid: the initial set contains the positive squarefree integers $\Delta \equiv 1 \pmod{8p_0}$, and distinct positive fundamental discriminants have nonprincipal product character. Thus for all but $o(x)$ integers $N \leq x$ there is such a Δ with $(\Delta/p) = 1$ at every $p \mid N$. For each odd $p^a \parallel N$, a root modulo p lifts to a root modulo p^a because Δ is coprime to p . If $2 \mid N$, then $(\Delta/2) = 1$ means $\Delta \equiv 1 \pmod{8}$, so it is a square modulo every power of 2. The Chinese remainder theorem gives a square root modulo N . The positive fundamental discriminant $\Delta > 1$ is not an integer square, so $R(N) \leq \Delta < U$.

For the lower bound set $A = 2^{(1-\epsilon)L}$, where $L = \log\log x$, and suppose that a positive nonsquare $a < A$ is a square modulo N . Write $a = bc^2$ with $b > 1$ squarefree. Every prime $p \mid N$ with $p > A$ is coprime to $2a$, and hence $(b/p) = 1$. The nonprincipal quadratic character associated with $\mathbb{Q}(\sqrt{b})$ has conductor at most $4b$. For each $b \leq A$, enlarge the permitted prime set by all primes $p \leq A$ and by the ramified primes. Its reciprocal sum is at most $L/2 + O(\log L)$ by (92). Restrict again to $\omega(N) = L + O(\sqrt{L}\log L)$ and apply the same restricted Hardy–Ramanujan inequality. For each b it gives at most $x \exp(-(\log 2 + o(1))L)$ integers N . There are at most A choices of b , so their union has size at most $x \exp(-(\epsilon \log 2 + o(1))L) = o(x)$. This permits arbitrary square factors c^2 without summing over them. The inequalities follow.

To obtain the stated density-one formulation with $\log N$, discard $N \leq \sqrt{x}$, for which there are $o(x)$ choices, and absorb the bounded difference between $\log\log N$ and $\log\log x$ into an arbitrarily small exponent margin. For every fixed margin the resulting exceptional set has density zero. A diagonal choice of margins tending to zero yields a single density-one set along which the displayed $o(1)$ tends to zero. $\square$

29 Effective bounds for prime-degree isogenies over quadratic fields

For a number field K , let $\text{IsogPrimeDeg}(K)$ be the set of rational primes p for which some elliptic curve over K admits a K -rational isogeny of degree p . Banwait’s published Algorithm 1.6 asserts, under GRH, the existence of an algorithm computing an upper bound for this set for every quadratic field other than an imaginary quadratic field of class number one [39, Algorithm 1.6]. We recover this entire algorithmic statement. Momose had already proved finiteness for these quadratic fields; effectivity is the conclusion at issue here.

Theorem 29.1 (Banwait’s effective quadratic-field isogeny bound). *There is an unconditional algorithm which, given a quadratic field K that is not an imaginary quadratic field of class number one, outputs an integer B_K such that*

$$p \in \text{IsogPrimeDeg}(K) \implies p \leq B_K.$$

In particular it computes a finite superset of $\text{IsogPrimeDeg}(K)$.

We first give the analytic step with all uniformity needed for this algorithm. For an abelian extension $F/\mathbb{Q}$, its conductor means an integer m_F such that $F \subseteq \mathbb{Q}(\zeta_{m_F})$; choosing the least such integer is unnecessary.

Lemma 29.2. *Fix a positive integer n . There is an effective constant C_n with the following property. If $L/\mathbb{Q}$ is abelian, $[L:\mathbb{Q}] \leq n$, and $L \subseteq \mathbb{Q}(\zeta_m)$, there is a prime q such that*

$$q \nmid m, \quad q \text{ splits completely in } L, \quad q \leq C_n(\log(3m))^8.$$

Proof. Let X be the group of Dirichlet characters corresponding to L , viewed as characters modulo m , and put $h = |X| \leq n$. For a prime $q \nmid m$, character orthogonality gives

$$\mathbf{1}_{q \text{ splits in } L} = \frac{1}{h} \sum_{\chi \in X} \chi(q).$$

Apply the smoothed explicit formula (4) to the primitive character inducing each nonprincipal $\chi \in X$. Its contribution is

$$O(x^{7/8} \log(3m) + \log(3m) \log(2x)),$$

where the second term also accounts for Euler factors removed at primes dividing m . The principal character contributes $x/2 + O(x^{7/8} \log^2(2x) + \log(3m) \log(2x))$ by Lemma 1.2. Prime powers of exponent at least two have total weight $O(\sqrt{x} \log^2(2x))$. Consequently

$$\begin{aligned} & \sum_{\substack{q \leq x \text{ prime} \\ q \nmid m \\ q \text{ splits in } L}} \log q (1 - q/x) \\ &= \frac{x}{2h} + O(x^{7/8} \log(3m) + x^{7/8} \log^2(2x) + \log(3m) \log(2x) + \sqrt{x} \log^2(2x)). \end{aligned}$$

The implied constant is absolute: the average over X cancels its cardinality. Set $x = C_n(\log(3m))^8$. The first error divided by x is $O(C_n^{-1/8})$; the other errors divided by x tend effectively to zero with m . Choose C_n large enough in terms of n , and enlarge it effectively for the finitely many remaining moduli. For those moduli one can enumerate primes until a completely split prime is found; Dirichlet's theorem ensures termination. The sum is positive, which proves the assertion. $\square$

We use the following previously published unconditional algebraic inputs. If $\lambda : G_K \rightarrow \mathbb{F}_p^\times$ is the character through which G_K acts on the kernel of a rational p -isogeny, and χ_p is the mod- p cyclotomic character, the isogeny is of *Momose type 2* when $\lambda^{12} = \chi_p^6$. Banwait–Derickx prove the following statements:

- (i) There are algorithms computing nonzero integers M_K and T_K such that an isogeny prime not of Momose type 1, 2 or 3 divides M_K , and a Momose type 1 isogeny prime divides T_K [40, Theorems 1.4 and 1.5].
- (ii) A Momose type 3 isogeny requires K to contain the Hilbert class field of an imaginary quadratic field [40, Definition 3.20].
- (iii) If p is of Momose type 2, q is a rational prime, and $\mathfrak{q} \mid q$ is a prime of K of residue degree f , then

$$q^f < p/4, \quad f \text{ odd}, \quad q^{2f} + q^f + 1 \not\equiv 0 \pmod{p} \implies q \text{ does not split in } \mathbb{Q}(\sqrt{-p})$$

[40, Proposition 6.1].

These are unconditional theorems, including the algorithmic effectivity in (i). The proof of (iii) distinguishes potentially good reduction, where Momose's local lemma makes q inert, from potentially multiplicative reduction, where splitting forces q^f to be a nontrivial cube root of unity modulo p . We import these established local and algebraic results; the conditional least-prime estimate in [40, Proposition 6.3] is not used.

Proof of Theorem 29.1. Write D for the fundamental discriminant of K . For any prime p , the compositum $L = K\mathbb{Q}(\sqrt{-p})$ is abelian of degree at most four and is contained in $\mathbb{Q}(\zeta_m)$ for $m = \text{lcm}(|D|, |D_{-p}|) \leq 4|D|p$, where D_{-p} is the fundamental discriminant of $\mathbb{Q}(\sqrt{-p})$. Lemma 29.2 supplies a prime q split in both fields with

$$q \leq Q_D(p) := C_4(\log(12|D|p))^8.$$

There is a prime of K above q with residue degree one. If $p > 3Q_D(p)^2$, then, since $q \geq 2$,

$$4q \leq 3q^2 < p, \quad 0 < q^2 + q + 1 \leq 3q^2 < p.$$

Input (iii), applied with $f = 1$, now contradicts the splitting of q in $\mathbb{Q}(\sqrt{-p})$. Thus every Momose type 2 prime satisfies

$$p \leq 3C_4^2(\log(12|D|p))^{16}. \quad (100)$$

An integer $B_2(D)$ above all positive solutions of this inequality is computable. Indeed the function

$$t \mapsto \frac{t}{(\log(12|D|t))^{16}}$$

is increasing once $\log(12|D|t) > 16$, and tends to infinity. Starting in that range, double t until the strict reverse of (100) holds. This gives a terminating algorithm for such a bound.

The hypotheses on K exclude Momose type 3: if the Hilbert class field H_A of an imaginary quadratic field A is contained in the quadratic field K , then $A = K$ and $[H_A : A] = 1$. Compute the nonzero integers M_K, T_K from (i), factor them, and output the maximum of $B_2(D)$ and their prime divisors. Every isogeny prime is bounded by this maximum, by (i)–(iii). All computations terminate. This proves the exact existence-of-an-algorithm assertion in [39, Algorithm 1.6] without GRH. $\square$

Precisely what is recovered. The new conclusion is the full qualitative algorithmic statement of Banwait’s Algorithm 1.6, with no restrictions on the eligible quadratic input field. We have not recovered the numerical GRH bounds in its tables, the particular computed candidate lists, or their subsequent exact classifications. The local filtering in the published algorithms can still be applied after replacing their conditional cutoff by the cutoff proved here. Deciding which members of a finite candidate list actually occur is a separate rational-point problem and is not asserted to be solved by this argument.

30 Uniform Rasmussen–Tamagawa finiteness in every odd degree

Let K be a number field and ℓ a prime. Write $\mu_{\ell^\infty} = \bigcup_{a \geq 1} \mu_{\ell^a}$, and let $\Omega_{K,\ell}$ be the maximal pro- ℓ extension of $K(\mu_{\ell^\infty})$ unramified away from primes above ℓ , inside a fixed algebraic closure of K . Let

$$\mathcal{A}(K, g, \ell) = \{[A]_K : \dim A = g, K(A[\ell^\infty]) \subseteq \Omega_{K,\ell}\}.$$

Here $[A]_K$ denotes K -isomorphism class, and the torsion field is generated by the coordinates of all ℓ -power torsion points. The condition says that, after adjoining the ℓ -power roots of unity, this torsion field lies in a pro- ℓ extension unramified away from ℓ . In particular A has good reduction at every finite prime not above ℓ .

Rasmussen–Tamagawa proved the following full uniform statement under GRH in [35, Theorem 5.2]. The argument below replaces its analytic input and retains all dimensions and all odd degrees in that theorem.

Theorem 30.1 (Uniform Rasmussen–Tamagawa theorem in odd degree). *For every positive integer g and every positive odd integer n , there is an effectively computable bound $B(g, n)$ such that*

$$[K : \mathbb{Q}] = n, \quad \ell > B(g, n) \implies \mathcal{A}(K, g, \ell) = \emptyset.$$

The bound is independent of the number field K and of the abelian variety. In particular, for every fixed number field of odd degree, the Rasmussen–Tamagawa finiteness assertion holds in every dimension.

Proof. We explain the unconditional algebraic input and reproduce the local contradiction, so that both the uniformity and the precise use of the zero-free strip are explicit. Put

$$M_g = |\mathrm{GL}_{2g}(\mathbb{F}_3)|, \quad C_{\mathrm{alg}}(g, n) = \max\{5, 2^{2g+1+2gM_g n^2}\}.$$

This deliberately generous bound avoids any need to optimize the indices of semistable reduction.

Suppose $[A] \in \mathcal{A}(K, g, \ell)$ and $\ell > C_{\mathrm{alg}}(g, n)$. Let $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^{\times}$ be the mod- ℓ cyclotomic character. By [35, Lemma 3.3], the semisimplification of the representation on $A[\ell]$ is

$$\overline{\rho}_{A, \ell}^{\mathrm{ss}} = \bigoplus_{r=1}^{2g} \chi^{i_r}|_{G_K} \quad (101)$$

for integers i_r . The group-theoretic reason is that the normal pro- ℓ subgroup acts trivially on simple modules in characteristic ℓ , and the remaining quotient is a subgroup of $\mathbb{F}_{\ell}^{\times}$; its simple representations are therefore one-dimensional powers of the cyclotomic character.

For a prime $\lambda \mid \ell$ of K , let a_{λ} be the minimal ramification index over the maximal unramified extension of K_{λ} needed for semistable reduction of A . Standard semistable-reduction theory gives $a_{\lambda} \mid M_g$ for $\ell > 3$: one may use the action on the 3-torsion, as in [35, Section 3.1]. Set

$$e_{\lambda} = a_{\lambda}e(\lambda/\ell), \quad 1 \leq e_{\lambda} \leq M_g n.$$

The finite-flat group-scheme calculation in [35, Section 3.3, equation (3.1)], an unconditional application of Tate–Oort theory after semistable base change, gives integers $j_{\lambda, r}$ satisfying

$$0 \leq j_{\lambda, r} \leq e_{\lambda}, \quad e_{\lambda} i_r \equiv j_{\lambda, r} \pmod{\ell - 1}. \quad (102)$$

These two structural facts are the established algebraic inputs.

Choose a prime $\mathfrak{p}_0$ of K above 2, and put $q_0 = N\mathfrak{p}_0 \leq 2^n$. It is a prime of good reduction because $\ell > 3$. Let $\alpha_1, \dots, \alpha_{2g}$ be the Frobenius eigenvalues there. The characteristic polynomial is integral, and the Weil bounds give $|\alpha_r| = \sqrt{q_0}$ in every complex embedding. For each λ , (101) and (102) imply the coefficientwise congruence

$$\prod_{r=1}^{2g} (T - \alpha_r^{e_{\lambda}}) \equiv \prod_{r=1}^{2g} (T - q_0^{j_{\lambda, r}}) \pmod{\ell}.$$

For $1 \leq k \leq 2g$, the absolute difference of the coefficients of T^{2g-k} is at most

$$\binom{2g}{k} (q_0^{e_{\lambda} k/2} + q_0^{e_{\lambda} k}) \leq 2^{2g+1+2gM_g n^2} < \ell.$$

Both polynomials are integral, so the congruence is an equality. Comparison of the absolute values of their roots then gives

$$j_{\lambda, r} = e_{\lambda}/2, \quad e_{\lambda} i_r \equiv e_{\lambda}/2 \pmod{\ell - 1} \quad (1 \leq r \leq 2g). \quad (103)$$

In particular e_λ is even.

Consider the characters of $G_{\mathbb{Q}}$

$$\varepsilon_{r,s} = \chi^{i_r+i_s-1}, \quad m = \text{lcm}_{1 \leq r,s \leq 2g} \text{ord}(\varepsilon_{r,s}).$$

They have finite order dividing $\ell - 1$. Fixing any λ and adding the congruences in (103) shows that $\varepsilon_{r,s}^{e_\lambda} = 1$ for all r, s . Hence

$$m \mid \ell - 1, \quad m \mid e_\lambda, \quad m \leq M_g n. \quad (104)$$

This weaker bound suffices here; the finer divisibility and parity properties of the corresponding $m_{\mathbb{Q}}$ in the published paper are not needed.

Let L be the unique degree- m subfield of $\mathbb{Q}(\zeta_\ell)$. A prime $p \neq \ell$ splits completely in L precisely when $p \bmod \ell$ is an m -th power in $\mathbb{F}_\ell^\times$. Applying Lemma 29.2 with degree bound $M_g n$ and modulus ℓ gives such a prime with

$$p \leq C_{M_g n}(\log(3\ell))^8. \quad (105)$$

Choose an effective bound $C_{\text{an}}(g, n)$ so that for every real $t > C_{\text{an}}(g, n)$,

$$C_{M_g n}^n (\log(3t))^{8n} < \frac{t}{4g}.$$

Such a bound is computable: $t/(\log(3t))^{8n}$ is increasing for $\log(3t) > 8n$ and tends to infinity, so a doubling search beyond that point terminates. Set $B(g, n) = \max\{C_{\text{alg}}(g, n), C_{\text{an}}(g, n)\}$.

Assume now $\ell > B(g, n)$. Factor the ideal $p\mathcal{O}_K$. Since $\sum_{\mathfrak{p}|p} e(\mathfrak{p}/p)f(\mathfrak{p}/p) = n$ is odd, at least one prime $\mathfrak{p} \mid p$ has odd residue degree $f = f(\mathfrak{p}/p) \leq n$. Put $q = p^f$. Then

$$q \leq p^n < \ell/(4g). \quad (106)$$

This does not require p to be unramified in K . The abelian variety has good reduction at $\mathfrak{p}$, because $p \neq \ell$. As p is an m -th power modulo ℓ , so is q , and (104) implies

$$q^{i_r+i_s-1} = 1 \pmod{\ell} \quad \text{for all } r, s.$$

We reproduce the contradiction of [35, Proposition 4.2]. Let $\beta_1, \dots, \beta_{2g}$ be the eigenvalues of Frobenius at $\mathfrak{p}$, and write $a_k = \sum_r \beta_r^k \in \mathbb{Z}$. Then

$$a_2 \equiv \sum_r q^{2i_r} = 2gq \pmod{\ell}, \quad |a_2| \leq 2gq.$$

Because $4gq < \ell$, this forces $a_2 = 2gq$. Each β_r^2 has complex absolute value q , so equality in the triangle inequality forces $\beta_r^2 = q$ for every r . Thus every β_r equals $\sqrt{q}$ or $-\sqrt{q}$. Since f is odd, $\sqrt{q} = p^{(f-1)/2} \sqrt{p}$ is irrational. The integer a_1 must therefore be zero. But reduction modulo ℓ gives

$$0 = a_1^2 \equiv \sum_{r,s} q^{i_r+i_s} = 4g^2 q \pmod{\ell}.$$

This is impossible: $\ell > 2g$ and $p \neq \ell$. The contradiction proves $\mathcal{A}(K, g, \ell) = \emptyset$, with all constants depending only on g, n .

For a fixed K , only finitely many ℓ remain. For each such ℓ , finiteness of $\mathcal{A}(K, g, \ell)$ is the established Shafarevich finiteness theorem, since the varieties have good reduction away from ℓ . This proves the stated fixed-field consequence. $\square$

Scope and algebraic dependencies. This is the entire formerly GRH-conditional statement of [35, Theorem 5.2], including $n = 1$ and arbitrary g . The local finite-flat and semistable-reduction facts are unconditional; they were stated explicitly before their use, and the remaining character and Frobenius arguments were given in full. The theorem places a uniform bound on the allowed primes ℓ ; it does not enumerate all isomorphism classes or assert that their union over all degree- n fields is finite. No corresponding theorem for every even degree, or the general varying-base-field assertion of the source's Theorem 5.3, is claimed here.

31 Rational CM newforms of every fixed weight

Schütt's published finiteness theorem [76, Theorem 2.1] assumes ERH for odd real Dirichlet characters. It is an application of the preceding class-group exponent theorem; it does not require a zero-free theorem for the varying infinite-order Hecke characters that define the modular forms.

We use Schütt's convention for twisting. Ordinarily a quadratic Dirichlet character φ acts on a newform by taking the newform associated to $\sum_{n \geq 1} \varphi(n) a_n q^n$. On the corresponding Hecke character ψ of K , this is multiplication by $\varphi \circ N_{K/\mathbb{Q}}$. For $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{-3})$, the convention additionally permits the quartic and sextic twists, respectively, of the Hecke character that preserve rational coefficients, as in [76, Section 1]. These exceptional twists must be included in the statement below.

Theorem 31.1 (Schütt's finiteness conclusion). *For every fixed integer weight $k \geq 2$, there are only finitely many normalized cuspidal CM newforms with rational Fourier coefficients, of arbitrary level, up to twisting in the preceding sense. Equivalently, for each positive infinity type l , only finitely many Hecke characters of imaginary quadratic fields with rational associated newforms occur up to this twisting equivalence.*

Proof. Put $l = k - 1$. The unconditional Hecke–Shimura construction and Ribet's converse, recalled in [76, Theorems 1.1 and 1.4], associate a CM newform of weight k to a Hecke character ψ of its unique imaginary quadratic CM field K , of infinity type l . Rationality of the Fourier coefficients implies that ψ takes integral ideals coprime to its conductor to $\mathcal{O}_K$ [76, Lemma 2.2].

We detail the resulting class-group restriction. Let $\mathfrak{m}$ be the conductor. For α prime to $\mathfrak{m}$,

$$\eta(\alpha) = \frac{\psi((\alpha))}{\alpha^l}$$

factors through the finite group $(\mathcal{O}_K/\mathfrak{m})^\times$. It has values in K by the rationality statement, hence its values are roots of unity in K and are units in $\mathcal{O}_K$. Thus $(\psi((\alpha))) = (\alpha)^l$ as ideals. Take any ideal class and choose an integral representative $\mathfrak{a}$ coprime to $\mathfrak{m}$. If its order is j , write $\mathfrak{a}^j = (\alpha)$. Multiplicativity gives

$$(\psi(\mathfrak{a}))^j = (\psi((\alpha))) = (\alpha)^l = \mathfrak{a}^{jl}.$$

The group of fractional ideals is free abelian on the prime ideals, so equality of j th powers implies $(\psi(\mathfrak{a})) = \mathfrak{a}^l$. Therefore $\mathfrak{a}^l$ is principal and $j \mid l$. Since the original ideal class was arbitrary, $E(D_K) \mid l$.

Theorem 16.2 leaves only finitely many possible fields K . Schütt's unconditional classification [76, Theorem 2.4] states that, for fixed l , sending a rational-coefficient Hecke character to its CM field is a bijection between the twisting classes and the imaginary quadratic fields with $E(D_K) \mid l$. In particular there is just one such twisting class for each of the finitely many admissible fields. The Hecke–Shimura correspondence gives the claimed finiteness for newforms. $\square$

The newly unrestricted part is the statement for every fixed weight. Schütt already established unconditional finiteness for weights 2, 3, 4, 5, 6, and for weights $2^r + 1$ and $3 \cdot 2^r + 1$ in his theorem. We do not count those special cases again. At weight 3, his explicit table has precisely the 65 CM fields from Proposition 19.4; that table is now complete, by the same unconditional correspondence. Its formerly possible extra field is excluded by Proposition 19.4.

32 Geometric consequences of the complete exponent-two classification

32.1 The Elkies–Schütt realization theorem

A singular K3 surface means a smooth projective K3 surface whose geometric Picard number is 20. Thus its transcendental part $T_\ell(X)$ in second ℓ -adic cohomology has dimension 2. Here a normalized cuspidal Hecke eigenform is associated to X when its two-dimensional Galois representation is the transcendental representation of X ; in particular their characteristic polynomials of Frobenius agree at all common good primes. This is the notion of association in [78].

Theorem 32.1 (Elkies–Schütt, with the ERH hypothesis removed). *Let $f = \sum_{n \geq 1} a_n q^n$ be a normalized cuspidal newform of weight 3 with rational Fourier coefficients, of arbitrary level and nebentypus ε . Then f is associated to a singular K3 surface X defined over $\mathbb{Q}$. At all but finitely many rational primes p , the Frobenius polynomial on $T_\ell(X)$ is*

$$1 - a_p T + \varepsilon(p) p^2 T^2.$$

Proof. Ribet’s theorem, as stated in [76, Corollary 1.2], says that an odd-weight newform with real coefficients has CM by its quadratic nebentypus; the corresponding quadratic field K is imaginary. These are unconditional facts also recalled in [78, Section 3 and Theorem 4]. Schütt’s classification identifies its twisting class with K , and the exponent of $\text{Cl}(K)$ divides $3 - 1 = 2$. Proposition 19.4 proves that K is one of the 65 fields in the table on page 5 of [78].

The following geometric input is the unconditional construction in [78, Lemma 7, Sections 5, 7–9]: each one of these 65 fields is realized by a singular K3 surface over $\mathbb{Q}$; the associated newforms account for one representative of every twisting class, and all required twists are geometrically realized. We spell out the twisting step to distinguish this from realizing only 65 individual newforms. Their modularity uses Livné’s theorem, stated as [78, Theorem 3]. It identifies the transcendental factor of second cohomology, not the entire 22-dimensional cohomology group.

For fields other than $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, the constructed surface has an elliptic fibration with section over $\mathbb{Q}$, of Weierstrass form

$$y^2 = x^3 + A(t)x + B(t), \quad A, B \in \mathbb{Q}[t].$$

For a quadratic character χ_d , replace it by

$$dy^2 = x^3 + A(t)x + B(t), \quad d \in \mathbb{Q}^\times.$$

The smooth minimal surface is geometrically isomorphic to the original surface, so it is again a singular K3 surface. Over $\mathbb{Q}(\sqrt{d})$, the two equations are identified by scaling y . The nontrivial Galois descent action is the fiberwise involution $y \mapsto -y$. It acts by -1 on the holomorphic 2-form $dt \wedge dx/y$, hence also on its complex conjugate. Since the transcendental Betti space has rank 2 for a singular K3 surface, the involution acts by -1 on that entire space, and therefore on $T_\ell(X)$ by comparison. The new Galois representation is precisely $T_\ell(X) \otimes \chi_d$, as required.

The exceptional fields require additional twists. Lemma 7 of [78] explicitly supplies them: for $K = \mathbb{Q}(\sqrt{-3})$, the relevant Kummer surface has an isotrivial fibration with $A(t) = 0$, permitting cubic twists fiberwise; combined with quadratic twists these give the sextic twisting convention. For $K = \mathbb{Q}(i)$, the order-4 automorphisms of the corresponding Kummer realization (equivalently the Fermat-quartic realization discussed there) provide the biquadratic twists. These are precisely the extra Hecke-character twists in Schütt’s classification. Their realization is part of that unconditional lemma.

Thus every twist belonging to every one of the 65 CM fields is realized over $\mathbb{Q}$. These exhaust the weight-3 rational newforms, proving the theorem. In the published proof of [78, Theorem 1], ERH was used only to assert that this field list is complete; the present argument replaces exactly that step. $\square$

The explicit equations and proofs of their Picard numbers in [78] are imported established geometric results. The argument here does not claim a fresh verification of every equation in their tables.

32.2 Products of non-CM elliptic curves that are not Jacobians

Let F be an algebraically closed field, and let E_1, E_2 be elliptic curves over F with $\text{Hom}(E_1, E_2) = \mathbb{Z}h$ for an isogeny h . Put $n = \deg h$. This is Kani’s notion of a pair of type n ; in particular the curves are isogenous and have endomorphism ring $\mathbb{Z}$. An isomorphism of their product with a Jacobian below is an isomorphism of abelian varieties; it does not require the product principal polarization to become the Jacobian polarization.

Theorem 32.2 (Kani’s exact exceptional list). *The abelian surface $E_1 \times E_2$ is not isomorphic to the Jacobian of a smooth genus-2 curve if and only if*

$$n \in \{1, 2, 4, 6, 10, 12, 18, 22, 28, 30, 42, 58, 60, 70, 78, \\ 102, 130, 190, 210, 330, 462\}.$$

Equivalently, these are exactly the types of such products which contain no smooth irreducible curve of genus 2.

Proof. Kani’s unconditional structural theorem [73, Theorem 38] states that a product of type n contains no smooth genus-2 curve if and only if

$$n = 1 \quad \text{or} \quad (n \text{ is even and idoneal, and } 8 \nmid n).$$

It is the criterion underlying the formerly GRH-conditional completeness of the exceptional list in [79, Theorem 5]. Theorem 19.5 supplies all idoneal integers. Filtering its 65 values by the displayed criterion gives exactly the 21 integers listed above, including 28.

For completeness, the equivalence of the two geometric formulations is the standard genus-2 polarization fact used in Kani’s theorem. A smooth genus-2 curve embedded in an abelian surface has self-intersection 2 by adjunction and defines an irreducible principal polarization; the resulting principally polarized surface is its Jacobian. Conversely a genus-2 Jacobian contains its Abel–Jacobi image as a smooth genus-2 curve, and an isomorphism of abelian varieties transports this curve to $E_1 \times E_2$. Thus the absence of such a curve is exactly the stated failure to be a Jacobian. $\square$

33 Pasten's height estimate for all Heegner points

The following recovers the order of the error term in [77, Proposition 13.3]. We specify the metric because changing the height normalization changes the exact formula used in the proof.

Let $D \geq 1$ be squarefree with an even number of prime divisors, and let $B/\mathbb{Q}$ be the indefinite quaternion algebra ramified exactly at the primes dividing D . Fix a maximal order $\mathcal{O}_B$. For compact open subgroups U of $(B \otimes \mathbb{A}_f)^\times$, let X_U be the compactified Shimura curves and let $X = \varprojlim_U X_U$ be their tower. A quadratic imaginary field K satisfies the *Heegner hypothesis for D* when every prime dividing D is inert in K . An optimal embedding $\mathcal{O}_K \hookrightarrow \mathcal{O}_B$ determines a Heegner point $P_K = [\tau_K, 1] \in X(\mathbb{Q})$, where τ_K is the fixed point in the upper half-plane for $K^\times$.

Use the Arakelov height h_{Ar} defined in [77, §13.3–13.4]: the integral line bundle is the relative dualizing sheaf on the sufficiently small-level integral models, and its metric under the complex uniformization is

$$\|f(z) dz\| = 2|f(z)| \operatorname{Im} z.$$

Pulling back along the integral extensions of the point and gluing at auxiliary levels gives a metrized rank-one $\mathcal{O}_F$ -module $\widehat{M}$, for a number field F defining the chosen finite-level point. The height is the normalized degree

$$h_{\text{Ar}}(P_K) = \frac{1}{[F:\mathbb{Q}]} \left(\log \#(M/\mathcal{O}_F \eta) - \sum_{\sigma:F \hookrightarrow \mathbb{C}} \log \|\eta\|_\sigma \right), \quad 0 \neq \eta \in M.$$

The compatibility of the integral models makes this independent of the auxiliary levels, F , and η . This is Pasten's source normalization; it is a height relative to the displayed hyperbolic metric, rather than to an unspecified metric on a canonical bundle.

Theorem 33.1. *Let $d_K = |\operatorname{disc}(K)|$. Uniformly for the preceding D and every imaginary quadratic field K satisfying the Heegner hypothesis for D ,*

$$h_{\text{Ar}}(P_K) = \frac{1}{2} \log(d_K D) + O(\ell(d_K)),$$

with an effective absolute implied constant.

Proof. Write χ_K for the primitive quadratic Dirichlet character of conductor d_K . The unconditional geometric input is Pasten's height formula [77, Theorem 13.2]:

$$h_{\text{Ar}}(P_K) = -\frac{L'}{L}(0, \chi_K) + \frac{1}{2} \log(D/d_K).$$

For $D > 1$ this follows from the Chowla–Selberg height formula and the integral-model comparison in that theorem; the same displayed formula for $D = 1$ is the classical Chowla–Selberg case. Its geometric hypotheses require the inertness condition stated above, and no Riemann hypothesis is used in this input.

Because K is imaginary quadratic, χ_K is odd. Its completed L -function

$$\xi_K(s) = \left(\frac{d_K}{\pi} \right)^{(s+1)/2} \Gamma\left(\frac{s+1}{2} \right) L(s, \chi_K)$$

satisfies $\xi_K(s) = \xi_K(1-s)$. Taking logarithmic derivatives at $s = 0$ and $s = 1$ gives

$$-\frac{L'}{L}(0, \chi_K) = \frac{L'}{L}(1, \chi_K) + \log(d_K/\pi) + \frac{1}{2} \left(\frac{\Gamma'}{\Gamma}(1/2) + \frac{\Gamma'}{\Gamma}(1) \right).$$

Since $\Gamma'/\Gamma(1) = -\gamma$ and $\Gamma'/\Gamma(1/2) = -\gamma - 2\log 2$, substitution yields the exact identity

$$h_{\text{Ar}}(P_K) = \frac{1}{2} \log(d_K D) + \frac{L'}{L}(1, \chi_K) - (\gamma + \log(2\pi)).$$

This also verifies the signs and normalizations in [77, Section 13.7]. Apply Corollary 12.2 with conductor d_K . Its effective constant is absolute and independent of D , proving the asserted uniform estimate. $\square$

The conclusion applies to every eligible K . Pasten's paper also obtains sufficient height bounds unconditionally for suitably chosen K by zero-density arguments; that already unconditional selection result is different from Proposition 13.3, which is the all- K estimate recovered here. The more precise $2 + \varepsilon$ error constant stated under GRH in that proposition is not asserted here.

34 Wei's height bound for adjacent CM types

Wei's published Theorem 1.4 [80] assumes the absence of certain Siegel zeros for relative L -functions of CM fields, a consequence of GRH. Its hypothesis can be removed even though the imported zero-free theorem does not cover these relative L -functions: Stark's theorem reduces the particular exceptional zeros in question to imaginary quadratic Dirichlet L -functions. The argument uses the proved averaged Colmez formula, not the full Colmez conjecture.

For a number field F , set $d_F = |\text{disc}(F)|$ and $r_F = [F : \mathbb{Q}]^{-1} \log d_F$, the logarithm of its root discriminant. A CM field E of degree $2g$ is a totally imaginary quadratic extension of its maximal totally real subfield E^+ . A CM type Φ chooses one embedding from each complex-conjugate pair of embeddings $E \hookrightarrow \mathbb{C}$. Write $h(E, \Phi)$ for the stable Faltings height of an abelian variety with multiplication by the full ring $\mathcal{O}_E$ and type Φ , using Wei's normalization. It depends only on (E, Φ) .

Theorem 34.1. *For each positive integer g , there are effective constants $C_1(g) > 0$ and $C_2(g)$ with the following property. Let E be any CM field of degree $2g$. Let A_i/K_i , for $i = 1, 2$, be abelian varieties of dimension g with embeddings*

$$\mathcal{O}_E \hookrightarrow \text{End}_{K_i}(A_i),$$

and let their CM types be Φ_i . If $|\Phi_1 \cap \Phi_2| = g - 1$, then

$$\frac{h_{\text{Falt}}^{\text{st}}(A_1) + h_{\text{Falt}}^{\text{st}}(A_2)}{2} \leq C_1(g) \frac{r_{K_1} + r_{K_2}}{2} + C_2(g).$$

Proof. We first remove the exceptional-zero hypothesis, then reconstruct the height and discriminant comparisons.

Exceptional zeros. Put $F = E^+$ and $\chi = \chi_{E/F}$, so that $L(s, \chi) = \zeta_E(s)/\zeta_F(s)$ is the entire quadratic Hecke L -function attached to E/F . The usual Dedekind zero-free-region theorem, in the form used by Wei, states that this function has at most one zero in

$$\text{Re } s \geq 1 - \frac{1}{4 \log d_E}, \quad |\text{Im } s| \leq \frac{1}{4 \log d_E},$$

and a zero there is real and simple. This follows also from Stark's Lemma 3 applied to ζ_E , since the entire factor $L(s, \chi)$ divides ζ_E .

Stark's Lemma 9 [82], stated for a totally real field of degree g and its totally complex quadratic extension, says that a real zero β of $L(s, \chi)$ in the range

$$1 - \frac{1}{16g! \log d_E} \leq \beta < 1 \tag{107}$$

is also a zero of the Dedekind zeta function of an imaginary quadratic subfield $k \subset E$. Since $\zeta(s)$ has no real zero in $(0, 1)$, the factorization $\zeta_k(s) = \zeta(s)L(s, \chi_k)$ forces $L(\beta, \chi_k) = 0$. But $d_E \geq 3$ and $g! \geq 1$ give

$$\beta \geq 1 - \frac{1}{16 \log 3} > \frac{7}{8},$$

contradicting Theorem 1.1. Thus there is no zero in (107). Combining this with the preceding reality statement proves Wei's generalized no-Siegel-zero hypothesis, with the effective choice $C_{\text{zero}}(g) = 16g!$. This argument makes no assertion of a fixed zero-free strip for general Dedekind or Hecke L -functions.

A uniform height bound in terms of d_E . The unconditional analytic estimate used in the proof of [81, Proposition 5.3], isolating the possible exceptional zero β_0 in the wider region of width $1/(4 \log d_E)$, is

$$-\frac{L'}{L}(0, \chi) - \frac{\delta}{1 - \beta_0} \leq \frac{75}{2} \log d_E + \frac{1}{2} \log \frac{d_E}{d_F} + \frac{g}{2} \left(\frac{\Gamma'}{\Gamma}(1/2) - \log \pi \right).$$

Here $\delta = 1$ if such a zero exists and $\delta = 0$ otherwise; the fraction involving β_0 is defined as zero in the latter case. This is the explicit zero estimate preceding the invocation of the no-Siegel-zero hypothesis in that proof. Since a possible β_0 lies outside (107),

$$\frac{\delta}{1 - \beta_0} \leq 16g! \log d_E.$$

Therefore

$$-\frac{1}{2} \frac{L'}{L}(0, \chi) - \frac{1}{4} \log \frac{d_E}{d_F} \leq \left(\frac{75}{4} + 8g! \right) \log d_E + O(g), \quad (108)$$

with an effective absolute constant in $O(g)$.

The proved averaged Colmez formula, in the source normalization, is

$$\frac{1}{2^g} \sum_{\Phi} h(E, \Phi) = -\frac{1}{2} \frac{L'}{L}(0, \chi) - \frac{1}{4} \log \frac{d_E}{d_F},$$

where the sum runs over all 2^g CM types, with no quotient by isomorphism. Also, stable Faltings heights satisfy the effective universal lower bound $h(E, \Phi) \geq -gC_0$ for an absolute constant C_0 . These are the unconditional inputs recorded in [81, Theorems 2.1 and 5.2]. For any chosen Φ_0 , isolating its term and applying (108) gives

$$\begin{aligned} h(E, \Phi_0) &= 2^g \left(-\frac{1}{2} \frac{L'}{L}(0, \chi) - \frac{1}{4} \log \frac{d_E}{d_F} \right) - \sum_{\Phi \neq \Phi_0} h(E, \Phi) \\ &\leq A_g \log d_E + B_g, \end{aligned}$$

for effective $A_g > 0, B_g$ depending only on g . For example, the coefficient $A_g = 2^g(75/4 + 8g!)$ suffices after increasing B_g .

Adjacent types and reflex fields. Let E_i^* be the reflex field of (E, Φ_i) , and put $M = E_1^* E_2^*$. We prove that M contains a conjugate of E , following the elementary argument of Wei's Lemma 5.5. The reflex field of a type Φ is generated by the type traces $\sum_{\varphi \in \Phi} \varphi(x)$ for $x \in E$. Write $E = F(\sqrt{-a})$ with $a \in F$ totally positive. The two types differ at exactly one real embedding $\sigma_0 : F \hookrightarrow \mathbb{R}$. Let φ_1, φ_2 be their respective extensions at that embedding; these extensions are complex conjugates. Subtracting the two type traces of $\sqrt{-a}$ gives

$$2\varphi_1(\sqrt{-a}) \in M.$$

Choose $b \in F$ with $F = \mathbb{Q}(b)$. Subtracting the type traces of $b\sqrt{-a}$ gives $2\sigma_0(b)\varphi_1(\sqrt{-a}) \in M$. Division shows that $\sigma_0(b) \in M$, and therefore $\varphi_1(E) \subset M$.

Root discriminants are nondecreasing under field extensions, and the discriminant inequality for a compositum gives $r_{E_1^*E_2^*} \leq r_{E_1^*} + r_{E_2^*}$. Hence

$$\frac{\log d_E}{2g} = r_E \leq r_M \leq r_{E_1^*} + r_{E_2^*}.$$

Because the full $\mathcal{O}_E$ -actions are defined over K_i , the field K_i contains the corresponding reflex field E_i^* , after the fixed compatible embeddings into $\mathbb{C}$. Consequently

$$\log d_E \leq 2g(r_{K_1} + r_{K_2}).$$

Apply the preceding individual height bound to Φ_1 and Φ_2 and average. The required inequality follows with $C_1(g) = 4gA_g$ and $C_2(g) = B_g$. $\square$

Source scope and a typographical correction. The journal's Theorem 1.4 is Theorem 1.7 in the arXiv version [81]. Both printed displays repeat $[K_1 : \mathbb{Q}]$ in the denominator of the d_{K_2} term. The symmetric expression with $[K_2 : \mathbb{Q}]$ in that denominator is what their root-discriminant proof establishes, and it has been proved explicitly above. The published special case where E has no imaginary quadratic subfield was already unconditional; the present argument includes CM fields with such subfields. Wei's separate theorem for individual heights relative to the root discriminant of the field of definition assumes the full Colmez conjecture in general, and is not asserted here.

34.1 Individual heights for every abelian CM field

The abelian-CM-field specialization of [80, Theorem 1.3] has no remaining Colmez assumption, because the Colmez formula for abelian CM fields is a theorem of Colmez and Obus. The published unconditional special case [80, Theorem 4.10] excludes imaginary quadratic subfields. The next result removes that restriction. We give a direct proof to display exactly which L -functions are required.

Corollary 34.2. *For each $g \geq 1$, there are effective constants $C_3(g) > 0, C_4(g)$ such that*

$$h_{\text{Falt}}^{\text{st}}(A) \leq C_3(g)r_K + C_4(g)$$

whenever A/K has dimension g and admits an embedding $\mathcal{O}_E \hookrightarrow \text{End}_K(A)$ for a CM field E of degree $2g$ that is Galois and abelian over $\mathbb{Q}$.

Proof. Let $G = \text{Gal}(E/\mathbb{Q})$, identify its embeddings with G , and let $\Phi \subset G$ be the CM type of A . Its stabilizer $H = \{h \in G : h\Phi = \Phi\}$ has fixed field the reflex field $R = E^H$. The $\mathcal{O}_E$ -action being defined over K implies $R \subset K$.

In the abelian case, the class function entering the Colmez formula is simply $A_\Phi(\sigma) = |\Phi \cap \sigma\Phi|$. Its character expansion has coefficients

$$m_\chi = \frac{1}{2g} \left| \sum_{\varphi \in \Phi} \chi(\varphi) \right|^2 \geq 0, \quad A_\Phi = \sum_{\chi \in \widehat{G}} m_\chi \chi.$$

This identity follows by expanding the square and applying finite character orthogonality. In particular $m_1 = g/2$ and, evaluating at the identity, $\sum_\chi m_\chi = g$. Let $c \in G$ be complex conjugation.

The disjoint union $G = \Phi \sqcup c\Phi$ shows that $m_\chi = 0$ for every nontrivial even character χ . Therefore the nontrivial terms are odd and their coefficients sum to $g/2$. Moreover, if $m_\chi \neq 0$, invariance $h\Phi = \Phi$ forces $\chi(h) = 1$ for every $h \in H$. Hence every character that occurs factors through $\text{Gal}(R/\mathbb{Q})$.

Write q_χ for the conductor of the primitive Dirichlet character corresponding to χ . The conductor–discriminant formula for the abelian extension $R/\mathbb{Q}$ gives

$$d_R = \prod_{\psi \in \widehat{\text{Gal}(R/\mathbb{Q})}} q_\psi, \quad q_\chi \leq d_R \text{ if } m_\chi \neq 0.$$

The proved abelian Colmez formula, in Wei’s normalization [81, Theorem 4.8], is

$$h(E, \Phi) = -Z_\Phi - \frac{1}{2}\mu_\Phi,$$

where

$$Z_\Phi = -\frac{g}{2} \log(2\pi) + \sum_{\chi} m_\chi \frac{L'}{L}(0, \chi), \quad \mu_\Phi = \sum_{\chi} m_\chi \log q_\chi.$$

The trivial-character contribution to Z_Φ cancels its first term, since $\zeta'(0)/\zeta(0) = \log(2\pi)$ and $m_1 = g/2$. For each remaining, odd character, its functional equation gives

$$-\frac{L'}{L}(0, \chi) = \log q_\chi - (\gamma + \log(2\pi)) + \frac{L'}{L}(1, \bar{\chi}).$$

The constant root number disappears under logarithmic differentiation. Substitution yields the exact real identity

$$h(E, \Phi) = \frac{1}{2} \sum_{\chi \neq 1} m_\chi \log q_\chi + \sum_{\chi \neq 1} m_\chi \frac{L'}{L}(1, \bar{\chi}) - \frac{g}{2}(\gamma + \log(2\pi)).$$

The terms of conjugate characters pair to real values. Corollary 12.2, positivity of the m_χ , and their sum $g/2$ now give

$$h(E, \Phi) \leq \frac{g}{4} \log d_R + O(g\ell(d_R) + g),$$

with an effective absolute constant in the O term. Since $[R : \mathbb{Q}] \leq 2g$, the discriminant formula in a tower implies

$$\log d_R = [R : \mathbb{Q}]r_R \leq 2gr_K.$$

Finally $\ell(x) \ll 1 + \log x$ for $x \geq 1$. This proves the corollary with effective constants depending only on g . $\square$

The corollary retains the hypothesis that $E/\mathbb{Q}$ is abelian. It makes no claim to the individual-height theorem for arbitrary CM fields, where the full Colmez formula remains a separate input.

35 Fully effective André–Oort for powers of the modular curve

Identify $Y(1)$ with the affine j -line. A *special point* is a singular modulus, the j -invariant of an elliptic curve with complex multiplication. Its discriminant is the negative discriminant of its endomorphism order, which need not be maximal.

A special subvariety of $Y(1)^n$ is an irreducible component of a locus defined by fixing some coordinates to singular moduli and imposing modular equations $\Phi_N(x_i, x_j) = 0$ among the remaining

coordinates. Here Φ_N is the classical modular polynomial for cyclic N -isogenies, and $\Phi_1(X, Y) = X - Y$. Equivalently, partition the nonconstant coordinates into blocks, choose one distinguished coordinate per block, and impose such a modular relation between it and each other coordinate of the block. For a special subvariety V , let $D(V)$ be the largest absolute discriminant of its constant coordinates, with $D(V) = 0$ if there are none. A special subvariety of X is *maximal* if it is not contained in a larger special subvariety of X .

The result below is the fully effective conclusion described in [51, Section 1.2 and Theorem 1] under GRH for imaginary quadratic fields. It is stronger than the unconditional assertion that there are finitely many maximal special subvarieties: the bound and a terminating enumeration are computable from the input.

Lemma 35.1 (Effective class numbers for every imaginary quadratic order). *For every rational $0 < \eta < 1/2$, an effectively computable positive constant c_η satisfies*

$$h(\Delta) \geq c_\eta |\Delta|^{1/2-\eta}$$

for every negative quadratic-order discriminant Δ .

Proof. Write $\Delta = f^2 D$, where D is fundamental. Corollary 1.5 gives an effective positive constant c with $h(D) \geq c\sqrt{|D|}/\ell(|D|)$. Since $t^\eta/\ell(t)$ has an effectively computable positive lower bound for $t \geq 3$, this implies $h(D) \geq c'_\eta |D|^{1/2-\eta}$ effectively. The order class-number formula gives

$$h(f^2 D) = \frac{fh(D)}{[\mathcal{O}_K^\times : \mathcal{O}_f^\times]} \prod_{p|f} \left(1 - \frac{\chi_D(p)}{p}\right) \geq \frac{h(D)}{3} \varphi(f).$$

The unit index is at most 3. For any $\eta > 0$, one can effectively choose P_η such that $1 - p^{-1} \geq p^{-2\eta}$ for all primes $p > P_\eta$. The finite product over smaller primes then proves $\varphi(f) \geq c''_\eta f^{1-2\eta}$, with an effective positive constant. Multiplying the two inequalities proves the assertion. $\square$

Theorem 35.2 (Binyamini's fully effective Andr e–Oort conclusion). *For positive integers n, d, r , there is an effectively computable constant $B(n, d, r)$ with the following property. If an algebraic subvariety $X \subseteq Y(1)^n$ is defined over a number field F , $\deg X \leq d$, and $[F : \mathbb{Q}] \leq r$, then every maximal special subvariety $V \subseteq X$ satisfies*

$$\deg V \leq B(n, d, r), \quad D(V) \leq B(n, d, r).$$

The degree is taken in the standard projective compactification $\mathbb{A}^n \subset \mathbb{P}^n$, with the degrees of irreducible components summed for reducible X . All maximal special subvarieties of an explicitly given X can be computed by a terminating algorithm. In particular, the bound is independent of the heights of the coefficients defining X .

Proof. We state exactly the established input being used. In [51, Section 2.2], a fixed Siegel–Tatuzawa exceptional field K_* is introduced to account for the possible failure of an effective class-number lower bound with exponent $1/2 - \eta$. Theorem 1 of that paper bounds $\deg V$ and the discriminants of all constant coordinates whose CM fields differ from K_* , effectively in terms of $\deg X$ and $[F : \mathbb{Q}]$ (with n fixed). The other discriminants have a bound that additionally depends on the unknown discriminant of K_* . Section 1.2 explicitly includes the case where the same effective lower bound holds without an exception: in that case one takes $K_* = \emptyset$ and obtains the fully effective result for every coordinate.

Lemma 35.1, for example with the paper's fixed choice $\eta = 1/100$, supplies exactly this effective class-number input for every order. Thus $K_* = \emptyset$ is now permitted. All remaining inputs in that

theorem are unconditional: its effective point-counting estimates, its algebraic reduction to isolated special points, and the effective version of Duke's equidistribution theorem in the appendix by Kowalski. The last effectivity depends on the same class-number lower bound, so it introduces no second exceptional field or additional GRH assumption. Applying the theorem gives the two stated bounds. Replacing the actual degree and field degree by their finitely many possible values at most d, r , and taking their maximum, gives $B(n, d, r)$ as stated.

We give the finite enumeration argument. Put $B = \lceil B(n, d, r) \rceil$. There are finitely many quadratic-order discriminants Δ with $|\Delta| \leq B$, and their singular moduli can be computed by enumerating reduced primitive positive binary quadratic forms and computing the corresponding class polynomials. These are terminating unconditional algorithms; complex approximations can be made rigorous with error bounds for the j -expansion.

Every modular relation needed in a block description of V may be chosen with $N \leq \deg V \leq B$. Indeed, project V onto the two coordinates of that relation. Its image is the irreducible modular curve $\Phi_N = 0$. Linear projection cannot increase the degree, and this curve has degree at least $\deg_X \Phi_N = N \prod_{p|N} (1 + 1/p) \geq N$. Consequently one enumerates finitely many partitions of the coordinate set, finitely many constant singular moduli from the preceding list, and finitely many choices $1 \leq N \leq B$ for the modular relations. Compute the irreducible components of the resulting loci over $\overline{\mathbb{Q}}$, retain those contained in X , and retain only the maximal ones under inclusion. Factorization and containment of explicitly given algebraic varieties over number fields are effective. Every maximal special subvariety occurs in this list by the proved bounds, and discarding contained entries introduces no loss. Thus the algorithm terminates with precisely the required collection. $\square$

The effective differential-algebraic and point-counting theorems of [51] are imported published inputs. Their proofs are not reproduced here. The deduction above removes their sole exceptional-field obstruction and records the complete enumeration argument. It does not claim that the constants are small enough for practical computation.

35.1 Effectivity of Binyamini's polynomial bounds

There is a useful quantitative refinement of Theorem 35.2. In this refinement the bound is polynomial in the degree and logarithmic height of the input variety. The corresponding polynomial bound, with an ineffective constant, was already unconditional; the additional conclusion is that its constants, and hence the algorithm using them, can be specified effectively.

For a variety $X \subseteq \mathbb{A}^n$ defined over a number field F , let $h(X)$ be the absolute logarithmic Weil height of its Chow coordinates in the standard projective embedding, and set

$$\delta_X = \max\{1, [F : \mathbb{Q}], \deg X, h(X)\}.$$

This is the complexity convention used in [45, Section 1.1.4]; we do not identify it with the bit length of an arbitrary representation of the input.

Theorem 35.3 (Effective constants in the polynomial André–Oort bound). *For each n , one can compute a polynomial P_n such that every maximal special subvariety V of an algebraic $X \subseteq Y(1)^n$ satisfies*

$$\deg V \leq P_n(\delta_X), \quad D(V) \leq P_n(\delta_X).$$

The algorithm of [45, Theorem 7 and Section 9.4] for computing all such V has an effective polynomial bound in δ_X for fixed n , in the arithmetic presentation used there.

Proof. We specify the input and the dependence being removed. Binyamini’s Theorem 7 gives precisely these polynomial degree and discriminant bounds, and the corresponding polynomial-step algorithm, but with an ineffective constant. The paragraph following that theorem identifies the sole source of ineffectivity as Siegel’s lower bound for quadratic class numbers. In the proof, the class-number input supplies the Galois-orbit lower bound in equation (126). Section 9.2 reduces the positive-dimensional problem to special points by effective algebraic constructions with polynomial bounds. The point-counting estimates used in Section 9.3 are effective, and Section 9.4 uses effective algebraic separation and the j -expansion to turn the bound into the asserted algorithm.

Lemma 35.1 now supplies the needed uniform effective estimate for every imaginary quadratic order. For example $h(\Delta) \geq c|\Delta|^{1/4}$ has an effectively computable absolute $c > 0$. Consequently the orbit constants in the cited argument are effective. Explicitly, if a special point $p = (j_1, \dots, j_n)$ has coordinate discriminants Δ_i and $\Delta(p) = \prod_i |\Delta_i|$, then

$$[\mathbb{Q}(p) : \mathbb{Q}] \geq \max_i h(\Delta_i) \geq c\Delta(p)^{1/(4n)}.$$

Over the defining field F , the orbit size is at least this quantity divided by $[F : \mathbb{Q}]$. This supplies an explicit effective polynomial lower bound of the form needed in equation (126).

One may also check separately the height input in equation (121) of [45]. If j has order discriminant $\Delta = f^2 D$, the height identity [46, Lemma 4.1] and the nonnegativity of every conductor correction give

$$h_F(E) \leq \frac{1}{4} \log |\Delta| + \frac{1}{2} \frac{L'}{L} (1, \chi_D) + C \leq C' \log(3|\Delta|)$$

with effective constants, by Corollary 12.2. The effective height comparison in equation (3.1) of [46] is

$$h(j) - c_0 \log(3 + h(j)) \leq 12h_F(E).$$

Since $c_0 \log(3 + t) \leq t/2 + C_0$ effectively for $t \geq 0$, it follows that $h(j) \leq C_1 \log(3|\Delta|)$ effectively. In particular the weaker bound $h(j) \ll_\varepsilon |\Delta|^\varepsilon$ used in the point-counting proof has an effective constant for every positive rational ε . Thus no hidden ineffective height constant remains.

For the remaining passage to the point-counting region, use the alternative in [45, Remark 41]. It uses the height estimate (121) and logarithmic subdivision in place of equidistribution to cover the relevant Galois conjugates by $O_\varepsilon(\Delta(p)^\varepsilon)$ many foliation balls, after adjusting ε . The height estimate just proved makes these constants effective. This route preserves the polynomial bounds and requires no separate equidistribution rate.

All formerly ineffective parameters in the published proof of Theorem 7 have now been supplied effectively. Its finite sequence of algebraic operations and polynomial point-counting bounds therefore computes the coefficients and exponents of a valid P_n , and supplies the asserted effective bound for its algorithm. The polynomial-time existence assertion itself is not being claimed as new: it is already part of Binyamini’s unconditional theorem. $\square$

36 Edixhoven–Richard’s André–Oort theorem modulo a prime

Fix a rational prime p . A *CM point over $\mathbb{Q}$* in $\mathbb{A}_{\mathbb{Q}}^2$ means a closed point both of whose coordinates are singular moduli. Its closure in $\mathbb{A}_{\mathbb{Z}}^2$ is finite over $\mathbb{Z}$. Its *reduction at p* means the underlying reduced finite closed subset of its fibre over p . Thus the reduction includes the reductions of the entire $G_{\mathbb{Q}}$ -orbit, rather than one chosen pair of singular moduli. This distinction is essential.

Theorem 36.1 (Edixhoven–Richard). *Let Σ be any collection of reductions at p of CM points over $\mathbb{Q}$, and let $Z \subseteq \mathbb{A}_{\mathbb{F}_p}^2$ be the Zariski closure of their union. Every one-dimensional irreducible*

component of Z is either a fibre of one of the coordinate projections or an irreducible component of the image of $Y_0(n)_{\mathbb{F}_p} \rightarrow \mathbb{A}_{\mathbb{F}_p}^2$ for some integer $n \geq 1$.

This is the complete statement of [32, Theorem 1.2], originally proved under GRH for quadratic fields. The proof below replaces its only conditional input and includes the passage from individual CM reductions to every curve component. The special curves here include Frobenius transforms of modular curves; the integer n need not be prime to p .

Proof. We use the unconditional CM reduction facts established in [32, Sections 2–3]. For an imaginary quadratic order $\mathcal{O}_{K,f} = \mathbb{Z} + f\mathcal{O}_K$ with $p \nmid f$, if p splits in K , reduction gives a bijection between its CM j -invariants and its ordinary j -invariants over $\mathbb{F}_p$. The resulting set $J_{K,f}$ has cardinality $h(f^2 D_K)$ and is a torsor under $\text{Pic}(\mathcal{O}_{K,f})$. Every ordinary j -invariant belongs to exactly one such set. If a conductor is divisible by p , its prime-to- p part gives the same reduced set. If p does not split in the CM field, all reductions are supersingular, and the set of all supersingular j -invariants in characteristic p is finite.

In particular, each coordinate projection of an $s \in \Sigma$ is entirely ordinary or entirely supersingular. In the ordinary case its image is exactly one $J_{K,f}$. For an ordinary pair in s , its canonical lifts have the same endomorphism orders as the reductions; the reductions of the full Galois orbit of that pair of canonical lifts are again exactly s . These assertions remain true for the original CM points with conductor divisible by p : removing the p -primary conductor is the quotient by inertia in the CM class-group action.

Suppose first that Z is a reduced curve with no component a fibre of a coordinate projection, and that the union of the $s \in \Sigma$ is dense in Z . Write d_1, d_2 for the degrees of the two projections of Z , summed over components. Only finitely many points of Z have a supersingular coordinate. We may discard all s with such a coordinate and retain density: their union is contained in the intersection of Z with finitely many fibres.

For any remaining s , put

$$N_s = \#s(\mathbb{F}_p), \quad \Delta_i = f_i^2 D_i \quad (i = 1, 2), \quad D = \max\{|\Delta_1|, |\Delta_2|\},$$

where $\mathcal{O}_{K_i, f_i}$ is its i -th coordinate endomorphism order and D_i is the fundamental discriminant of K_i . The projections are surjective onto the corresponding CM torsors, so

$$\max_i h(\Delta_i) \leq N_s \leq h(\Delta_1)h(\Delta_2). \quad (109)$$

Lemma 35.1, with exponent $1/4$, and the elementary upper bound $h(\Delta) \ll \sqrt{|\Delta|} \log(3|\Delta|)$ therefore give effective absolute constants with

$$N_s \geq cD^{1/4}, \quad \log N_s \ll \log(3D).$$

There are only finitely many such sets s for bounded D , because there are only finitely many pairs of endomorphism orders and finitely many points in each product $J_{K_1, f_1} \times J_{K_2, f_2}$.

We now replace the GRH step in the published Theorem 4.1. Define

$$m = pf_1 f_2 |D_1 D_2| \prod_{\substack{r \leq \log N_s \\ r \text{ prime}}} r.$$

The empty product is 1. The field $L = K_1 K_2$ is abelian over $\mathbb{Q}$, has degree at most 4, and is contained in $\mathbb{Q}(\zeta_m)$. The elementary bound $\sum_{r \leq t} \log r \ll t$, together with (109) and $f_1 f_2 \leq D$, gives

$$\log(3m) \ll_p \log(3D).$$

Lemma 29.2 supplies a prime ℓ with

$$\ell \nmid p f_1 f_2 D_1 D_2, \quad \ell \text{ splits in both } K_1, K_2, \quad \log N_s < \ell \ll_p (\log(3D))^8. \quad (110)$$

It is thus split in both orders. Since a positive power of D eventually exceeds every fixed power of its logarithm, all but finitely many s satisfy

$$N_s > 2d_1 d_2 (\ell + 1)^2. \quad (111)$$

As D tends to infinity, $\log N_s$ does too, so the primes obtained in (110) range over an infinite set.

Let T_ℓ be the Hecke correspondence on the j -line which sends an elliptic curve to its $\ell + 1$ quotients by subgroups of order ℓ . We verify

$$s \subseteq (T_\ell \times T_\ell)(s). \quad (112)$$

Choose an ordinary pair (E_1, E_2) in s and their canonical CM lifts, with the CM fields embedded compatibly with their actions on tangent spaces. Since ℓ splits in both fields and is prime to both conductors, choose a prime of $K_1 K_2$ above ℓ ; its intersections $\mathfrak{l}_i$ with the two orders have index ℓ . CM reciprocity identifies simultaneous Frobenius action on the pair of lifts with the inverse ideal-class actions $[\mathfrak{l}_i]^{-1}$. The corresponding ideal actions give ℓ -isogenies in both coordinates. Both the original pair and its simultaneous conjugate reduce to s , so the original pair lies in the Hecke image of s . This proves (112) for every pair in s .

Consequently $s \subseteq Z \cap (T_\ell \times T_\ell)Z$. In $\mathbb{P}^1 \times \mathbb{P}^1$, the two projection degrees of $(T_\ell \times T_\ell)Z$, with its correspondence multiplicities, are $(\ell + 1)^2 d_1$ and $(\ell + 1)^2 d_2$. If the two curves had no common component, their intersection would have at most $2d_1 d_2 (\ell + 1)^2$ geometric points by the intersection pairing on $\mathbb{P}^1 \times \mathbb{P}^1$. This contradicts (111). Thus for infinitely many ℓ the intersection has a curve component.

We state precisely the unconditional geometric input used next: [32, Theorem 5.1] says that if an irreducible curve $C \subseteq \mathbb{A}_{\mathbb{F}_p}^2$ is not a coordinate fibre and $(T_\ell \times T_\ell)C$ is reducible for infinitely many primes ℓ , then C is a component of a modular correspondence. No GRH is assumed in this criterion. Its inputs are the large mod- ℓ monodromy of non-isotrivial elliptic curves over function fields, Goursat's lemma for the two monodromy groups, and Zarhin's isogeny theorem. More explicitly, reducibility forces the two representations to be isomorphic up to a quadratic character for infinitely many ℓ . The characters range over a finite set: outside the bad-reduction set they are unramified, and in characteristic 2 the common semistable extension obtained from the two 3-torsion representations bounds their conductors. One twist therefore occurs infinitely often, and Zarhin's theorem gives an isogeny of the generic elliptic curves. The minimal isogeny gives the asserted modular component. This explains both the unconditional nature of the criterion and its validity at $p = 2$.

Write $Z = \bigcup_{i \in I} Z_i$ for its irreducible components. For each of the infinitely many primes just obtained, some Z_i is contained in $(T_\ell \times T_\ell)Z_j$. When $\ell > 12d_1$, this image must be reducible. Indeed, if irreducible it equals Z_i . For any ordinary (x, y) in Z_j , the set $T_\ell(y)$ has at least $(\ell + 1)/12$ distinct points, by the elementary ordinary-isogeny multiplicity bound used in [32, Section 6]. Fixing any $x' \in T_\ell(x)$ would then give more than d_1 points in one projection fibre of Z_i , which is impossible. Since I is finite, one Z_j has reducible Hecke image for infinitely many ℓ . The unconditional criterion shows that this Z_j is special.

It remains to justify that this argument proves the assertion for *every* component, and for the original Z . This point needs the full-orbit hypothesis. For an integer $n \geq 1$, let $T(n)$ denote the reduced integral correspondence of pairs admitting an isogeny of degree n . It is a finite union of

modular correspondences (in characteristic zero one factors out multiplication by an integer from the kernel). In the ordinary locus, if s meets $T(n)_{\mathbb{F}_p}$, it is wholly contained there. To see this, canonically lift the isogeny at the meeting point. Every Galois conjugate of the lifted pair still admits an isogeny of degree n , and all their reductions comprise s .

Choose n for the special component just found, and remove all components of Z contained in $T(n)_{\mathbb{F}_p}$. Their complement Z' meets that correspondence in only finitely many points. The sets s meeting $T(n)_{\mathbb{F}_p}$ contribute only those finitely many points to Z' . The remaining full sets s are contained in Z' and have dense union there. Induction on the number of components proves the assertion for every component of a curve Z without coordinate fibres.

Finally, for a general Z , the assertions are empty if its dimension is 0 or 2. Otherwise remove its isolated points and its coordinate fibre components. This removal can also be performed using whole sets s . Let B_1 be the finite first-coordinate image of the vertical components and isolated points, and B_2 the analogous second-coordinate image of the horizontal components and isolated points. If a projection of s meets B_i , then that entire projection is either supersingular or the unique ordinary CM torsor $J_{K,f}$ containing the meeting point. Hence the union of all such projections is finite. All discarded s therefore lie on a finite union of coordinate fibres; this union meets the remaining non-fibre components in a finite set. The undiscarded s are contained in those remaining components and are still dense there. The preceding induction applies, and proves the theorem. $\square$

Scope. The theorem concerns reductions of full CM orbits over $\mathbb{Q}$, not arbitrary individual points over $\overline{\mathbb{F}_p}$. It is distinct from characteristic-zero André–Oort and from positive-characteristic formulations in terms of dense families of positive-dimensional special subvarieties. We do not assert the conjectural extensions to other orbit fields or higher dimensions.

37 Weakly bounded height on curves in the modular plane

Write $h(x)$ for the absolute logarithmic Weil height and $h(x, y) = \max\{h(x), h(y)\}$. In the modular plane $\mathbb{A}_{\mathbb{Q}}^2$, a special curve is a modular curve $Y_0(N)$ or a coordinate fibre whose fixed coordinate is a singular modulus. A special point is a pair of singular moduli. The plane itself is also special. Every point P lies in a unique smallest special subvariety $S(P)$. Define $S_{\mathbb{Q}}(P)$ to be the union of the distinct Galois conjugates of $S(P)$ over $\mathbb{Q}$, and take degrees in the compactification $\mathbb{P}^1 \times \mathbb{P}^1$ with respect to $\mathcal{O}(1, 1)$; the degree of a finite reduced set is its cardinality.

Theorem 37.1 (Habegger’s weakly bounded height theorem). *Let $C \subset \mathbb{A}_{\mathbb{Q}}^2$ be an irreducible algebraic curve which is not special. Let d_1, d_2 be the degrees of its two coordinate functions on the smooth projective model of C , with degree zero for a constant function. Suppose $d_1 \neq d_2$. There exists a constant $c(C) > 0$ such that every $P \in C(\overline{\mathbb{Q}})$ with $\dim S(P) \leq 1$ satisfies*

$$h(P) \leq c(C) \log(1 + \deg S_{\mathbb{Q}}(P)).$$

This is the complete conclusion of [31, Corollary 1.2(ii)], whose hypothesis was GRH for all odd real Dirichlet L -functions. The logarithmic bound is uniform over the infinitely many special curves meeting C . It is not a claim of bounded height independent of the special subvariety, which would be false in general.

Proof. We first prove the uniform CM estimate needed for the coordinate fibres. Let j be a singular modulus and let its endomorphism order have discriminant $\Delta = f^2 D$, where $D < 0$ is fundamental.

Let E have j -invariant j , and write $h_F(E)$ for the stable Faltings height in Deligne's normalization. The unconditional Chowla–Selberg and conductor formula [31, Lemma 4.1] is

$$2h_F(E) = \frac{1}{2} \log |\Delta| + \frac{L'}{L} (1, \chi_D) - \sum_{r|f} e_f(r) \log r - \gamma - \log(2\pi), \quad (113)$$

where, for $r^a \| f$,

$$e_f(r) = \frac{1 - \chi_D(r)}{r - \chi_D(r)} \frac{1 - r^{-a}}{1 - r^{-1}} \geq 0.$$

The logarithmic derivative estimate Corollary 12.2 therefore gives $h_F(E) \ll \log |\Delta|$, with an absolute constant. The unconditional comparison between the two heights [31, equation (3.1)] gives an absolute $A > 0$ with

$$h(j) - A \log(3 + h(j)) \leq 12h_F(E) \leq h(j) + A.$$

Since $A \log(3 + t) \leq t/2 + B_A$ for $t \geq 0$ and a suitable absolute B_A , the left inequality implies $h(j) \ll \log |\Delta|$.

The class polynomial of this order is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(j) : \mathbb{Q}] = h(\Delta)$. Applying Lemma 35.1 with exponent $1/4$ yields $h(\Delta) \geq c_0 |\Delta|^{1/4}$ for an absolute $c_0 > 0$. Consequently

$$\log |\Delta| \leq 4 \log h(\Delta) + 4 |\log c_0| \ll \log(1 + h(\Delta)).$$

We have proved, for every singular modulus and every conductor,

$$h(j) \ll \log(1 + [\mathbb{Q}(j) : \mathbb{Q}]). \quad (114)$$

All constants in this auxiliary estimate can be chosen effectively.

We recall two unconditional height comparisons and give the argument for the non-CM modular case as well. The coordinate-height relation on a fixed curve, obtained from the height pairing for divisors on its smooth projective model, is

$$|d_2 h(x) - d_1 h(y)| \leq A_C \sqrt{1 + h(x)} \quad ((x, y) \in C(\overline{\mathbb{Q}})), \quad (115)$$

provided $d_1 > 0$, after enlarging A_C to include the finitely many points over singularities. This is the unconditional relation [31, equation (3.2)]. It follows from the fact that the divisor $d_2(x)_\infty - d_1(y)_\infty$ has degree zero; its height is bounded by a constant times the square root of a height associated with the positive-degree divisor $(x)_\infty$. In particular $h(y) \ll_C 1 + h(x)$. The same assertion holds with the two coordinates interchanged whenever $d_2 > 0$.

Suppose first that neither coordinate of $P = (x, y)$ is a singular modulus. Then $S(P) = Y_0(N)$ for a unique $N \geq 1$. Indeed, a cyclic isogeny between two elliptic curves without CM generates their rank-one group of homomorphisms: if it were an integer multiple of a generator by an integer of absolute value greater than one, its kernel would contain the noncyclic full torsion subgroup for that integer. Thus two cyclic isogenies between the same pair have the same degree. In this case

$$\deg S_{\mathbb{Q}}(P) = 2\Psi(N), \quad \Psi(N) = N \prod_{r|N} (1 + r^{-1}) \geq N.$$

Choose elliptic curves E_x, E_y with these j -invariants. Their cyclic degree- N isogeny gives the unconditional Faltings estimate $|h_F(E_x) - h_F(E_y)| \leq \frac{1}{2} \log N$. Combining this with the height comparison above gives

$$|h(x) - h(y)| \leq A \log(3 + h(x) + h(y)) + 6 \log N \quad (116)$$

for an absolute A . At least one projection degree is positive; interchange the coordinates if necessary so that $d_1 > 0$. By (115), $h(y) \ll_C 1 + h(x)$. Since the nonzero integer $d_2 - d_1$ has absolute value at least one,

$$h(x) \leq |d_2 h(x) - d_1 h(y)| + d_1 |h(y) - h(x)| \leq B_C \sqrt{1 + h(x)} + 6d_1 \log N.$$

The logarithm in (116) is absorbed into the square-root term. The inequality $B_C \sqrt{1 + t} \leq t/2 + B'_C$ implies $h(x) \ll_C \log(1 + N)$, and the same follows for $h(y)$. As $2\Psi(N) \geq N$, this proves the desired inequality in this case. This reproduces the unconditional part of Habegger's argument.

Suppose next that x is a singular modulus. If y is also a singular modulus, then $S(P) = \{P\}$ and

$$\deg S_{\mathbb{Q}}(P) = [\mathbb{Q}(x, y) : \mathbb{Q}] \geq [\mathbb{Q}(x) : \mathbb{Q}].$$

If y is not a singular modulus, then $S(P) = \{x\} \times \mathbb{A}^1$ and $\deg S_{\mathbb{Q}}(P) = [\mathbb{Q}(x) : \mathbb{Q}]$. Thus (114) bounds $h(x)$ by an absolute constant times $\log(1 + \deg S_{\mathbb{Q}}(P))$ in both cases. Moreover $d_1 > 0$: otherwise $C = \{x\} \times \mathbb{A}^1$ would be special, contrary to the hypothesis. Equation (115) bounds $h(y)$ by $O_C(1 + h(x))$; the additive constant is absorbed because $\log(1 + \deg S_{\mathbb{Q}}(P)) \geq \log 2$. The case where only y is singular follows by interchanging the coordinates. These cases exhaust $\dim S(P) \leq 1$. $\square$

The condition $d_1 \neq d_2$ remains essential to this proof's non-CM modular branch. The argument does not establish weakly bounded height for all nonspecial plane curves. Nor does it identify bounded-degree finiteness as new: that conclusion was already unconditional in [31, Corollary 1.1 and p. 46].

38 Effective Brauer–Manin sets for singular and CM Kummer surfaces

For a smooth projective variety X over a number field k , put $\mathrm{Br} X = H_{\mathrm{\acute{e}t}}^2(X, \mathbb{G}_m)$, $\mathrm{Br}_0 X = \mathrm{im}(\mathrm{Br} k \rightarrow \mathrm{Br} X)$, and $\mathrm{Br}_1 X = \ker(\mathrm{Br} X \rightarrow \mathrm{Br} X_{\bar{k}})$. Its Brauer–Manin set is

$$X(\mathbb{A}_k)^{\mathrm{Br}} = \left\{ (P_v)_v : \sum_v \mathrm{inv}_v \alpha(P_v) = 0 \text{ for every } \alpha \in \mathrm{Br} X \right\}.$$

A singular K3 surface means a smooth K3 surface whose geometric Néron–Severi group has rank 20. The Kummer surface of an abelian surface is the minimal resolution of its quotient by $[-1]$.

Theorem 38.1 (Balestrieri–Johnson–Newton's effectivity theorem). *Let k be a number field and let X/k be either a singular K3 surface or a surface geometrically isomorphic to $\mathrm{Kum}(E_1 \times E_2)$, where both elliptic curves $E_i/\mathbb{C}$ have complex multiplication by imaginary quadratic orders. Then $X(\mathbb{A}_k)^{\mathrm{Br}}$ is effectively computable from equations for X and k .*

This is the full conclusion of [24, Theorem 7.8], stated there under GRH. The orders may be nonmaximal, the two CM fields may differ, and X need not be a Kummer surface over k . Effective computability is in the sense of [26, Theorem 1]: an effective description of the indicated adelic subset, with a computable bound on the algorithm's running time in terms of the input. It does not decide the existence of a rational point whenever that subset is nonempty.

Proof. We replace the analytic input and then verify all the geometric and algorithmic hypotheses. Throughout, implied constants are absolute and effectively computable.

Let E/F be a CM elliptic curve, where $d = [F : \mathbb{Q}]$, and let $\Delta = f^2 D < 0$ be the discriminant of its endomorphism order. The class polynomial gives $h(\Delta) = [\mathbb{Q}(j(E)) : \mathbb{Q}] \leq d$. Lemma 35.1, with exponent $1/4$, implies

$$|\Delta| \ll d^4. \quad (117)$$

The CM height formula (113), its nonnegative conductor correction, and Corollary 12.2 also give

$$h_F(E) \ll \log(2|\Delta|) \ll \log(2d). \quad (118)$$

Here h_F is the stable Faltings height. Changing between the normalizations used in the cited isogeny theorems adds a fixed constant, which is harmless in this inequality.

We next bound the transcendental Brauer group of a product $A = E_1 \times E_2$ over F , uniformly in its CM orders. If the two curves are geometrically isogenous, their CM field is the same imaginary quadratic field K . Write $\Delta_i = f_i^2 D_K$ for their order discriminants. The unconditional statement [24, Theorem 6.4] supplies an extension M/FK of degree dividing $\#\mathcal{O}_K^\times \leq 6$ over which all homomorphisms between the two curves are defined, and gives

$$\# \frac{\text{Br } A}{\text{Br}_1 A} \leq \frac{4}{\pi^2} f_1^2 f_2^2 |D_K| [M : \mathbb{Q}]^4.$$

Since $[M : \mathbb{Q}] \leq 12d$ and $f_1^2 f_2^2 |D_K| = |\Delta_1 \Delta_2| / |D_K|$, equation (117) proves

$$\# \frac{\text{Br } A}{\text{Br}_1 A} \ll d^{12}. \quad (119)$$

If the curves are geometrically non-isogenous, put $F' = FK_1 K_2$, so $[F' : \mathbb{Q}] \leq 4d$. All endomorphisms of $A_{\overline{F}}$ are defined over F' . The unconditional isogeny and Brauer estimates of [25, Theorems 1.5(3) and 1.8], applied to the product as in [24, equation (6.6)], give a positive integer b such that the exponent of $\text{Br}(A_{\overline{F}})^{\text{Gal}(\overline{F}/F')}$ is at most $2b^{3/2}$ and

$$b \leq 241^4 2^{60} [F' : \mathbb{Q}]^4 \max\{1, \log[F' : \mathbb{Q}], h_F(E_1) + h_F(E_2) + 3\}^4.$$

For clarity, in the notation of Gaudron–R  mond this specialization has $n = 2$ and $b \leq \Upsilon^4$. Their bound for Υ is $241 \cdot 2^9 \exp(4) [F' : \mathbb{Q}]$ times the displayed maximum, and $\exp(4) < 2^6$ gives the stated estimate. Here the e in their formula $(en)^{2n}$ is Euler’s number; we use this formula directly rather than the smaller numerical constant printed in (6.6). Equation (118) therefore yields $b \ll d^4 \log(2d)^4$. The geometric N  ron–Severi rank of this product is 2; accordingly $\text{Br}(A_{\overline{F}}) \simeq (\mathbb{Q}/\mathbb{Z})^4$. A finite subgroup of this group with exponent at most $2b^{3/2}$ has at most $16b^6$ elements. The natural injection of the transcendental quotient into these Galois invariants proves

$$\# \frac{\text{Br } A}{\text{Br}_1 A} \ll d^{24} \log(2d)^{24}. \quad (120)$$

The injections used here, and below, do not require a rational point: for every extension L/F , the map $\text{Br } A / \text{Br}_1 A \rightarrow \text{Br } A_L / \text{Br}_1 A_L$ is injective because both map to the same geometric Brauer group.

We pass from products to surfaces. Let $M(r)$ be the least common multiple of the orders of finite subgroups of $\text{GL}_r(\mathbb{Z})$. Minkowski’s theorem makes this an effectively computable integer. If X is geometrically a Kummer surface of a product, the unconditional geometric results [24, Remark 3.7, Theorem 3.5, and Corollary 3.10] give an extension L/k with

$$[L : k] \leq 2^9 3M(20)$$

and CM elliptic curves $E_1, E_2/L$ such that

$$\frac{\mathrm{Br} X}{\mathrm{Br}_1 X} \hookrightarrow \frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)}.$$

These results include the possible 2-covering of the abelian surface: an extension of degree at most 16 trivializes it. Thus they apply to every geometric Kummer surface in the statement, not only to a product construction already given over k . Equations (119) and (120) give, for $d = [k : \mathbb{Q}]$,

$$\# \frac{\mathrm{Br} X}{\mathrm{Br}_1 X} \leq C d^{24} \log(2d)^{24} \quad (121)$$

for an effective absolute C .

For an arbitrary singular K3 surface, the unconditional Shioda–Inose construction, with its descent as used in [24, proof of Theorem 7.5], gives an extension k'/k of degree at most $2M(20)$ and a dominant rational map $Y \dashrightarrow X_{k'}$ of degree two, where Y/k' is a Kummer surface with geometric Néron–Severi rank 20. Its elliptic factors are isogenous CM curves. Pullback on Brauer groups induces a map on transcendental quotients whose kernel is killed by two; this follows from the restriction–corestriction identity for the degree-two extension of function fields. The kernel injects into $\mathrm{Br}(X_{\bar{k}})[2]$, which has order 4 because $\mathrm{Br}(X_{\bar{k}}) \simeq (\mathbb{Q}/\mathbb{Z})^2$. Hence

$$\# \frac{\mathrm{Br} X}{\mathrm{Br}_1 X} \leq 4 \# \frac{\mathrm{Br} Y}{\mathrm{Br}_1 Y}.$$

The preceding effective uniform bound applies to Y and again gives (121), after enlarging C . Resolution of the rational map causes no change in these Brauer groups, by birational invariance for smooth projective surfaces.

It remains to include the algebraic Brauer group and construct the adelic set. The group $\mathrm{Pic}(X_{\bar{k}})$ is torsion free of rank $r \leq 20$. The unconditional bound [24, Remark 1.4] is

$$\# \frac{\mathrm{Br}_1 X}{\mathrm{Br}_0 X} \leq M(r)^r \leq M(20)^{20}.$$

We have therefore produced a computable bound for $\#(\mathrm{Br} X / \mathrm{Br}_0 X)$, depending only on $[k : \mathbb{Q}]$. The unconditional algorithm [27, Theorem 8.38] computes the geometric Néron–Severi group with its Galois action and divisor representatives. Its applicability to K3 surfaces in characteristic zero uses the established Tate theorem for K3 surfaces, not an additional conjecture. Since $\mathrm{Pic}^0(X_{\bar{k}}) = 0$, these divisors generate the geometric Picard group. The hypotheses of [26, Theorem 1] are now all satisfied: equations for a smooth projective surface, generators for its torsion-free geometric Picard group, and an effective bound for the Brauer group modulo constants. That theorem computes $X(\mathbb{A}_{\bar{k}})^{\mathrm{Br}}$, as required. $\square$

The numerical constants of the original GRH bounds in [24, Theorems 7.4–7.6] are not claimed here; the complete published algorithmic statement in Theorem 7.8 is the admitted conclusion. The rank-20 Kummer subcase was already unconditional in their Theorem 7.7. The full statement also includes non-Kummer singular K3 surfaces and products of non-isogenous CM elliptic curves. Algorithms for principal CM K3 surfaces, including Valloni’s algorithm and Monnet’s later explicit bounds, impose maximal-order CM and do not by themselves give this entire statement.

39 Joint equidistribution of CM points

Khayutin's published Theorems 1.3 and 3.10 [30] assume the absence of exceptional Landau–Siegel zeros of the quadratic CM fields. We remove this analytic assumption. The two fixed splitting primes, the stated restrictions on the orders, and the genericity conditions are retained. The maximal-order case of the second statement is the published Theorem 1.4.

Theorem 39.1 (Khayutin's joint-packet and Galois-orbit conclusions). *The following statements hold without an RH or GRH assumption.*

1. Let G be a $\mathbb{Q}$ -form of PGL_2 , let $K_f \subset G(\mathbb{A}_f)$ be compact open, and fix a compact real torus $K_\infty \subset G(\mathbb{R})$. Put

$$Y = G(\mathbb{Q}) \backslash G(\mathbb{A}) / (K_\infty K_f).$$

Let P_i be K_∞ -invariant toral packets with negative fundamental discriminants D_i , and also write P_i for their finite images in Y . Here a toral packet is the image of an adelic orbit of an anisotropic rational torus, as in [30, §§2.4.1–2.4.2]. The finite packet is a principal homogeneous space for a finite abelian group C_i , with a canonical surjection $C_i \rightarrow \mathrm{Pic}(\mathcal{O}_{E_i})$, where $E_i = \mathbb{Q}(\sqrt{D_i})$. Choose $\sigma_i \in C_i$ and put

$$N_i = \min\{N\mathfrak{a} : 0 \neq \mathfrak{a} \subseteq \mathcal{O}_{E_i}, [\mathfrak{a}] = [\sigma_i]\}, \quad \mu_i = \frac{1}{|P_i|} \sum_{z \in P_i} \delta_{(z, \sigma_i z)}.$$

Assume $N_i \rightarrow \infty$ and that two fixed distinct primes p_1, p_2 split in every E_i . Every weak-* limit point of (μ_i) is a convex combination of the uniform probability measures on the connected components of $Y \times Y$.

2. Let G be a $\mathbb{Q}$ -form of PGL_2 split over $\mathbb{R}$, and let X be a finite product of indefinite Shimura curves relative to this same G , at fixed levels. Let $x_i \in X$ be special points such that all coordinates of x_i have CM by the same imaginary quadratic order $\mathcal{O}_i \subset E_i$. Assume that its conductor $f_i = [\mathcal{O}_{E_i} : \mathcal{O}_i]$ is bounded independently of i . Let ν_i be the normalized counting measure on the finite Galois orbit of x_i . Assume that two fixed distinct primes p_1, p_2 split in every E_i , and that, for every proper special subvariety $Z \subsetneq X$, the set $\{i : x_i \in Z\}$ is finite. Every weak-* limit point of (ν_i) is a convex combination of the uniform probability measures on the connected components of X .

Here uniform measure means the normalized invariant measure on the indicated locally homogeneous component. In a connected product the conclusion is convergence to its uniform probability measure.

Proof. We first give the exact analytic replacement, and then spell out the published unconditional geometric and sieve inputs that it makes applicable. For an imaginary quadratic field E of fundamental discriminant D , write χ_D for its primitive quadratic Dirichlet character. We have

$$\zeta_E(s) = \zeta(s)L(s, \chi_D), \quad \left| \frac{L'}{L}(1, \chi_D) \right| \ll \log \log(e^e |D|), \quad L(1, \chi_D) \gg \frac{1}{\log \log(e^e |D|)}. \quad (122)$$

The last two assertions follow from Corollary 12.2 and Theorem 1.4. In particular, for a single absolute constant C , uniformly in all these fields,

$$\frac{L'}{L}(1, \chi_D) \leq C \log |D|.$$

This is exactly the analytic inequality assumed in [30, Proposition 10.15] and deduced there from the no-exceptional-zero hypothesis in §10.4. Alternatively, the zero-free half-plane for both factors of ζ_E directly excludes every exceptional zero in its usual region $\beta > 1 - c/\log |D|$ once $|D|$ is large. The fixed constant c in the definition of that region is immaterial here.

We record the proof mechanism to identify the full dependency on this inequality. In the notation of [30, Theorem 3.2], joint packets lift to homogeneous toral sets

$$H_i = [T_i(\mathbb{A})^\Delta(g_i, s_i g_i)] \subset [G \times G], \quad [G] = G(\mathbb{Q}) \backslash G(\mathbb{A}).$$

In the following adelic argument write μ_i for their invariant probability measures, whose finite projections are the packet measures in the statement. The superscript $+$ on $G(\mathbb{A})^+$ denotes the image of the adelic points of the simply connected cover of G . The unconditional reduction in [30, Proposition 3.4 and Corollary 3.5] makes the split tori at p_1, p_2 fixed by bounded right translations. Duke's theorem gives tightness and the correct one-coordinate marginals. The unconditional joining classification used in [30, Theorem 4.4 and Corollary 4.5] then says that a limit is a mixture of $(G \times G)(\mathbb{A})^+$ -invariant measures and the intermediate measures supported on translates of homogeneous Hecke correspondences.

For a general joint lift, let $\mathcal{O}_i$ be its associated order and define N_i as the minimum norm of an integral invertible $\mathcal{O}_i$ -ideal in the class of s_i , as in [30, Lemma 10.4]. This agrees with the notation of part (1). The following two ranges exhaust the possible twists. Let $\theta < 1/2$ be an available unconditional bound towards Ramanujan in the normalization of [30, §10.4, equation (56)]. For an admissible ellipse-counting exponent $\theta_l > 2/3$ sufficiently close to $2/3$, put

$$a = \frac{2 - \theta_l^{-1}}{3}, \quad b = \frac{1}{2 + 2/(1 - \theta)}.$$

Since $a \rightarrow 1/6$ as $\theta_l \downarrow 2/3$ and $b > 1/6$, we can fix $a < c < b$. Separate the indices into $N_i \geq |D_i|^c$ and $N_i < |D_i|^c$.

In the first range, [30, Lemma 10.4, Theorem 8.7, Proposition 10.15, and §10.4] give, for the published Bowen test neighborhoods $B^{(-n,n)}$, for each fixed n and translated Hecke measure λ_ξ , and all sufficiently large i ,

$$\text{Cor}[\mu_i, \lambda_\xi](B^{(-n,n)}) \ll F(\text{ctr}(\xi)) p_1^{-4n} \left(1 + \frac{|D_i|^{-2/3+o(1)}}{L(1, \chi_{D_i})} \right).$$

Here the cross-correlation is the integral of the nonnegative automorphic kernel, as in [30, Definitions 8.1–8.2]:

$$\text{Cor}[\alpha, \beta](B) = \int_{[G \times G]} \int_{[G \times G]} \sum_{\gamma \in (G \times G)(\mathbb{Q})} \mathbf{1}_{B \times B}(x^{-1} \gamma y) d\alpha(x) d\beta(y).$$

Also $\text{ctr}(\xi_1, \xi_2) = \xi_1^{-1} \xi_2$, and F is a positive continuous function independent of i, n . These are unconditional estimates with the explicit displayed logarithmic-derivative inequality as input; the class-number formula cancels the factor $\sqrt{|D_i|} L(1, \chi_{D_i})$ against the toral volume. Equation (122) makes the parenthesis bounded. The unconditional entropy comparison [30, Lemma 10.1], with $\rho = 1$, excludes all intermediate Hecke measures. Its continuity requirement on F is established in the cited §10.4.

In the second range the unconditional Ellenberg–Michel–Venkatesh argument, with the adaptations proved in [30, §10.4, equations (56)–(59)], applies with the fixed gap $b - c > 0$. It uses a

Hecke norm gap and Linnik's basic lemma; both are unconditional. The otherwise ineffective use of Siegel's lower bound in that basic lemma can also be replaced by (122), although effectivity is not needed for the qualitative conclusion. The resulting maximal-entropy statement again implies $(G \times G)(\mathbb{A})^+$ -invariance. Passing to subsequences in the two ranges therefore proves the conclusion of the published Theorem 3.2 whenever its non-analytic hypotheses hold. This argument imports the proved joining, geometric, and sieve lemmas just identified; it assumes no unproved automorphic bound.

For part (1), the fundamental-discriminant condition means that the conductor is 1. Minkowski's bound gives $N_i \ll \sqrt{|D_i|}$, so $N_i \rightarrow \infty$ forces $|D_i| \rightarrow \infty$. The condition $N_i \rightarrow \infty$ is the escape from every fixed Hecke correspondence used in the passage from the published Theorem 3.2 to Theorem 1.3. All the hypotheses of that passage are now satisfied. The projection from $[G \times G]$ to $Y \times Y$ sends the invariant limit measures to the stated combinations of component measures. The residual spectrum may prescribe unequal component weights, as explained in [30, Proposition 3.6]; no equality of these weights is asserted.

For part (2), now writing $D_i = \text{disc}(\mathcal{O}_i)$, bounded $|D_i|$ would allow only finitely many CM points at the fixed levels. Since a special point is a proper special subvariety, the hypothesis implies $|D_i| \rightarrow \infty$. Since $D_i = f_i^2 \text{disc}(E_i)$ and f_i is bounded, the field discriminants also tend to infinity. The geometric and sieve estimates above are uniform after partitioning the sequence into the finitely many possible conductors: their allowed dependence on f_i causes no loss. The logarithmic-derivative inequality uses the field character, exactly as required by the published Proposition 10.15. The passage to many factors is [30, Theorem 3.9]: the same unconditional joining classification reduces it to the two-coordinate case, because a connected reductive subgroup of G^r projecting onto $G \times G$ in every pair of coordinates is all of G^r . The special-subvariety hypothesis implies escape from every fixed pairwise Hecke correspondence. Shimura reciprocity identifies the finite Galois-orbit measure with the push-forward of the homogeneous toral measure, as in [30, §3.5, Theorem 3.10]. If the coordinates belong to different CM orbits of the same order, the bounded compact translations appearing there admit convergent subsequences. Right translation preserves the required invariance because $G^r(\mathbb{A})^+$ is normal. Pushing forward therefore gives exactly the conclusion in part (2). Tightness, supplied by the marginal equidistribution, also proves the asserted convergence when the product is connected. $\square$

The published targets are Theorems 1.3 and 3.10 of [30], including Theorem 1.4 as its maximal-order specialization, with their no-exceptional-zero assumption removed. No varying splitting-prime substitution is made. Results for products of pairwise distinct quaternion algebras do not by themselves imply this repeated-factor mixing statement. Nor does this argument remove the fixed splitting-prime condition from the more general mixing conjecture.

40 Effective bounds for Campagna's singular S -units

A *singular modulus* is the j -invariant of a complex elliptic curve with complex multiplication. It is an algebraic integer. For a set S of rational primes, a nonzero algebraic integer α is an S -unit if every prime divisor of $|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)|$ belongs to S . The set S is allowed to be infinite.

Theorem 40.1 (Campagna's effective singular- S -unit conclusion). *Let $\ell \geq 5$ be a rational prime, and put*

$$S_0 = \{p \text{ prime} : p \equiv 1 \pmod{3}\}, \quad S_\ell = S_0 \cup \{\ell\}.$$

There is an effectively computable $B(\ell)$ such that every singular modulus j which is an S_ℓ -unit has order discriminant Δ satisfying $|\Delta| \leq B(\ell)$. All these singular moduli can consequently be

determined by a finite algorithm.

This is the precise effective conclusion of [47, Theorem 1.4], published under GRH for the Dirichlet L -functions of imaginary quadratic fields. Mere finiteness was already unconditional. The point here is the computability of a bound valid for every discriminant.

Proof. We first verify the analytic hypothesis isolated in [47, Definition 5.1 and Theorem 5.5]. That hypothesis asks for one effective $k \geq 0$ such that, for every negative fundamental discriminant D ,

$$\frac{L'}{L}(1, \chi_D) \geq -0.2485 \log |D| - k. \quad (123)$$

Corollary 12.2 gives an effective absolute A with $|L'/L(1, \chi_D)| \leq A\ell(|D|)$. Because $A\ell(t) - 0.2485 \log t$ tends to $-\infty$ effectively, its positive part has an effectively bounded supremum for $t \geq 3$. Any effective upper bound for that supremum is a valid k . Thus the hypothesis in Campagna's stronger Theorem 5.5 is satisfied.

We spell out the remaining transfer, including why its height comparison has a strict positive margin. Write $d = |\Delta|$ and $\Delta = f^2 D$. In the normalization used in [47, Proposition 5.4], the unconditional Chowla–Selberg and Nakajima–Taguchi formulas give

$$h_F(E) = \frac{1}{4} \log d + \frac{1}{2} \frac{L'}{L}(1, \chi_D) - \frac{1}{2} \sum_{p|f} e_f(p) \log p - \frac{1}{2} (\gamma + \log(2\pi)), \quad e_f(p) = \frac{1 - \chi_D(p)}{p - \chi_D(p)} \frac{1 - p^{-v_p(f)}}{1 - p^{-1}}.$$

Here h_F is the stable Faltings height with Deligne's normalization. The unconditional height comparison used in that proposition is $h(j) \geq 12h_F(E) + 8.64$, where h is the absolute logarithmic Weil height. These geometric formulas are established inputs, and involve no Riemann hypothesis.

For completeness the conductor correction cannot spoil the coefficient in the height lower bound. Since $e_f(p) \leq 2(1 - p^{-v_p(f)})/((p+1)(1 - p^{-1}))$, define the additive function

$$\delta(m) = 0.2485 \log m - \sum_{p|m} \frac{\log p}{p+1} \frac{1 - p^{-v_p(m)}}{1 - p^{-1}}.$$

For $r \geq 1$ its increment at a prime power is

$$\delta(p^{r+1}) - \delta(p^r) = \left(0.2485 - \frac{p^{-r}}{p+1} \right) \log p > 0.$$

Also $\delta(p) > 0$ for $p \geq 5$, whereas $\delta(2), \delta(3) < 0$. Hence

$$0.2485 \log f - \frac{1}{2} \sum_{p|f} e_f(p) \log p \geq \delta(f) \geq \delta(2) + \delta(3) > -0.0605.$$

Substituting (123) and $|D| = d/f^2$ into the height formula proves

$$h(j) \geq 1.509 \log d - C_k, \quad (124)$$

with an effective absolute constant C_k depending on k .

Next an S_ℓ -unit in the theorem must in fact be an $\{\ell\}$ -unit. We give the reduction used in [47, Theorem 5.5], based on [48, Theorem 1.2 and Claim 3.1]. Suppose a prime $p \equiv 1 \pmod{3}$ divides the norm of j . At a prime above p , its CM elliptic curve and the curve with j -invariant 0 have the same reduction. The latter reduction is ordinary because p splits in $\mathbb{Q}(\sqrt{-3})$. Deuring's reduction

theorem then identifies the CM field of j with $\mathbb{Q}(\sqrt{-3})$. For every order in this field, reduction at 2 and at 3 is supersingular. In each of these characteristics the only supersingular j -invariant is 0. Consequently both 2 and 3 divide the norm of every nonzero such j . Neither belongs to S_ℓ , a contradiction. Thus no prime in S_0 divides the norm. If $\ell \equiv 1 \pmod{3}$, there are no such moduli, by the unconditional theorem that no singular modulus is an algebraic unit. It remains to consider $\ell \equiv 2 \pmod{3}$.

Let $H = h(\Delta)$ denote the order class number, to distinguish it from the Weil height. Since $h(j) = h(j^{-1})$, write

$$h(j) = A_\infty + N_\ell,$$

where the two terms are respectively the archimedean and the ℓ -adic contributions to the height of j^{-1} . The two unconditional estimates in [47, proof of Theorem 5.5, equations (42)–(44)] are, for $d \geq 10^{14}$,

$$A_\infty \leq \frac{12F(d) \log d}{H} + 3 \log \left(\frac{F(d) \sqrt{d} \log d}{H} \right) - 3.77, \quad F(d) = \max_{1 \leq a \leq \sqrt{d}} 2^{\omega(a)},$$

$$N_\ell \leq \max \left\{ \frac{3}{2}(\log(9d) + \log \ell), 3 \log \ell \right\}.$$

The first estimate comes from the archimedean analysis of Bilu, Habegger and Kühne quoted there; the second is Campagna's deformation-theoretic valuation bound, his Theorem 3.1 applied to $y^2 = x^3 + 1$. The automorphism count is 6 because $\ell \geq 5$, which is the reason for retaining this restriction on ℓ .

Here the new effective class-number lower bound makes the final comparison particularly direct. Put $\eta = 1/10000$. Lemma 35.1 gives $H \geq c_\eta d^{1/2-\eta}$ effectively. Also $F(d) \leq C_\eta d^\eta$ effectively: choose a prime threshold above which $2 \leq p^{2\eta}$, bound the product of the factors 2 at smaller primes by a fixed constant, and use $a \leq \sqrt{d}$. The preceding archimedean estimate therefore implies

$$A_\infty \leq C_1 d^{-1/2+2\eta} \log d + 6\eta \log d + 3 \log \log d + C_2,$$

with effective constants. For $d \geq \ell/9$, the other estimate is $N_\ell \leq \frac{3}{2} \log d + C_\ell$, with effective C_ℓ . Combining with (124) gives

$$(0.009 - 6\eta) \log d \leq C_1 d^{-1/2+2\eta} \log d + 3 \log \log d + C_3(\ell, k).$$

The left coefficient is $0.0084 > 0$; the right side is $o(\log d)$ with an effective rate. Choose an effective threshold $B(\ell)$, enlarged to exceed 10^{14} and $\ell/9$, beyond which this inequality fails. This proves the discriminant bound.

Finally enumerate the negative quadratic-order discriminants $|\Delta| \leq B(\ell)$ and compute their class polynomials exactly. Each such polynomial is irreducible over $\mathbb{Q}$ and its constant coefficient, up to sign, is the norm of any of its roots. Omit the polynomial X , and test whether the remaining constant coefficients are powers of ℓ up to sign. The reduction above shows that exactly the roots of the retained polynomials are the required S_ℓ -units. Thus this is a terminating exact algorithm. $\square$

41 Effective representation by positive ternary quadratic forms

The existence theorem of Duke–Schulze-Pillot was already unconditional. Its *effective* version is the published GRH consequence recovered here: Kane [52, Introduction, p. 128] explicitly identifies Dirichlet GRH as sufficient to make the representation threshold computable. The further GRH

assumptions on weight-2 modular L -functions in Kane's practical bounds and numerical tables are not available from Theorem 1.1, and those conclusions are not asserted here.

An integral ternary quadratic form means a homogeneous quadratic polynomial Q in three variables with integer coefficients. It is positive definite if $Q(x) > 0$ for nonzero $x \in \mathbb{R}^3$. A representation by an integral vector is *primitive* when the greatest common divisor of its coordinates is 1. The genus of Q consists of the integral forms equivalent to Q over every $\mathbb{Z}_p$; its spinor genus is the usual finer equivalence class obtained by imposing the local spinor-norm condition. Both contain finitely many integral equivalence classes.

Theorem 41.1 (Effective Duke–Schulze–Pillot theorem). *For every positive definite integral ternary form Q , one can compute an integer B_Q with the following property: if $n > B_Q$ is represented primitively by a form in the spinor genus of Q , then Q represents n . Consequently, an algorithm computes the complete finite set*

$$\{n \geq 1 : n \text{ is represented primitively by the spinor genus of } Q, \quad n \text{ is not represented by } Q\}.$$

Proof. Write $r_Q(n)$ for the number of representations of n by Q , and write $r_{\text{spn}}(n)$ for the average over its spinor genus, weighted by the reciprocals of the automorphism-group orders and divided by the total weight. We use two precise unconditional inputs from Duke–Schulze–Pillot [53]. Their Theorem 3(i), with no imposed congruence condition on the representing vectors, gives, for every $\eta > 0$,

$$|r_Q(n) - r_{\text{spn}}(n)| \leq A_{Q,\eta} n^{1/2-1/28+\eta}, \quad (125)$$

where $A_{Q,\eta}$ is effective. This is the half-integral-weight cusp-form estimate; its proof does not use Siegel's ineffective class-number lower bound.

The arithmetic part of their Lemma 5(ii), before the application of Siegel's bound, has the following form on integers represented primitively by the spinor genus:

$$r_{\text{spn}}(n) \geq b_{Q,\eta} n^{1/2-\eta} L(1, \chi_{\Delta_n}), \quad |\Delta_n| \leq c_Q n. \quad (126)$$

Here $\Delta_n < 0$ is the fundamental discriminant of $\mathbb{Q}(\sqrt{-2n \det A})$, where $A = (\partial^2 Q / \partial x_i \partial x_j)$, and $b_{Q,\eta} > 0$ and c_Q are effective. We specify the arithmetic content of this input to locate the issue of effectivity. The Siegel mass formula and its spinor-genus refinement express the averages in local densities and quadratic class numbers. At primes dividing the fixed level, primitive representability gives an effective uniform positive lower bound for the primitive local density. Indeed, if x is a primitive local vector, the identity $\text{adj}(A)Ax = (\det A)x$ bounds the minimum valuation of the coordinates of the gradient Ax by $v_p(\det A)$; Hensel lifting from an effectively bounded congruence depth then gives such a lower bound. At anisotropic primes primitivity also bounds the valuation of n . The remaining factors are the elementary Euler factors in the quadratic-order class-number formula and divisor sums. Their losses can be bounded by $C_{Q,\eta} n^\eta$ with effective constants. For instance, for every fixed $\eta > 0$,

$$\prod_{p|m} (1 - p^{-1}) \geq c_\eta m^{-\eta}$$

follows by choosing an effective threshold beyond which $1 - p^{-1} \geq p^{-\eta}$ and treating the finitely many smaller primes separately. The spinor correction is computed by the local densities in [53, Theorem 2(ii)]. More explicitly, Schulze–Pillot [55, Korollar 2 and its proof, pp. 130–131] compares the positive primitive mass of an exceptional half-genus with the primitive genus mass. The relevant local density ratios take only finitely many values: at good primes one of the two local contributions is zero, and at bad primes their recurrences stabilize, possibly interchanging the contributions, after

finitely many steps. The resulting positive comparison constant is therefore computable from the fixed lattice and the finitely many exceptional square classes. The primitive-spinor condition is exactly the positivity condition used in [53, Lemma 5(ii)]. Thus the constants in (126) preceding $L(1, \chi_{\Delta_n})$ are effective. It is the replacement of this last factor by Siegel's $|\Delta_n|^{-\eta}$ bound that made the original representation threshold ineffective.

Theorem 1.4 now gives $L(1, \chi_{\Delta_n}) \geq c/\ell(|\Delta_n|)$. For fixed Q and η , the elementary inequality $\ell(c_Q n) \leq C_{Q,\eta} n^\eta$ has an effective constant. Therefore (126) implies

$$r_{\text{spn}}(n) \geq b'_{Q,\eta} n^{1/2-2\eta}$$

effectively. Set $\eta = 1/112$. The exponent of the error in (125) is then $1/2 - 3\eta$. It follows that $r_Q(n) > 0$ whenever

$$n^\eta > 2A_{Q,\eta}/b'_{Q,\eta}.$$

For example, any effectively chosen integer larger than $\max\{1, (2A_{Q,\eta}/b'_{Q,\eta})^{112}\}$ can serve as B_Q .

To obtain the asserted finite set, enumerate the finitely many integral classes in the genus using positive-definite reduction, and select the spinor genus by the computable local spinor-norm conditions. For each $1 \leq n \leq B_Q$, test primitive representation by these finitely many forms and representation by Q . Each test is finite: a computable positive lower bound λ for the least eigenvalue of the Gram matrix bounds the coordinates of a representing vector by $\sqrt{n/\lambda}$, after adjusting for the convention $Q(x) = x^t A x / 2$. The preceding proof excludes every larger exception. No assertion about a practical running time is required or made. $\square$

Why the primitive-spinor hypothesis is retained. Local representability alone does not give this theorem: spinor exceptions may occupy infinite square classes. Moreover, repeated division by a prime at which Q is anisotropic can leave the number of representations bounded while n grows. These are the explicit obstructions discussed after [53, Lemma 5]; neither is removed by a zero-free region for Dirichlet L -functions.

There is also a uniform version for squarefree integers, with the same determinant exponent as Duke's published theorem.

Theorem 41.2 (Effective form of Duke's determinant bound). *There is an effective absolute constant $C > 0$ such that the following holds for every positive definite integral ternary form Q . Put*

$$D = \det \left(\frac{\partial^2 Q}{\partial x_i \partial x_j} \right).$$

If n is positive and squarefree, $n > CD^{337}$, and $Q(x) \equiv n \pmod{8D^3}$ has a solution, then Q represents n over $\mathbb{Z}$. In particular, all squarefree integers which are locally represented by Q but not represented integrally can be listed by a finite algorithm.

Proof. We retain Duke's published exponent 337 [54, Theorem 1], while making its constant effective. Let $r_{\text{gen}}(n)$ denote the automorphism-weighted average over the genus. Duke's unconditional Theorem 2 gives

$$|r_Q(n) - r_{\text{gen}}(n)| \leq A_\varepsilon D^{11/2} n^{1/2-1/28} (Dn)^\varepsilon \quad (127)$$

for squarefree n , with an effective constant depending only on $\varepsilon > 0$.

Equations (3)–(4) of that paper express $r_{\text{gen}}(n)$ as a positive absolute normalization factor times

$$L(1, \chi) \mathcal{N}(n; Q) \sqrt{n/D}, \quad \mathcal{N}(n; Q) = m^{-2} \#\{x \in (\mathbb{Z}/m\mathbb{Z})^3 : Q(x) \equiv n \pmod{m}\}, \quad m = (2D)^3.$$

The quadratic character χ here may be imprimitive; its modulus M is at most an absolute constant times Dn . Its primitive inducing character χ^* has conductor at most M , and

$$L(1, \chi) = L(1, \chi^*) \prod_{p|M} \left(1 - \frac{\chi^*(p)}{p}\right) \geq L(1, \chi^*) \frac{\varphi(M)}{M} \gg \frac{1}{\ell(M)^2}.$$

The last inequality uses Theorem 1.4 and the elementary effective bound $M/\varphi(M) \ll \ell(M)$. The character is nonprincipal, since the associated quadratic field is imaginary. The assumed congruence solution gives $\mathcal{N}(n; Q) \geq m^{-2}$. Consequently, with an effective absolute $c > 0$,

$$r_{\text{gen}}(n) \geq c n^{1/2} D^{-13/2} \ell(Dn)^{-2}. \quad (128)$$

This also verifies directly the effectivity of the lower bound in equation (5) of Duke's proof.

The ratio of the right side of (127) to the lower bound (128) is at most

$$C_\varepsilon D^{12+\varepsilon} n^{-1/28+\varepsilon} \ell(Dn)^2 \leq C'_\varepsilon D^{12+2\varepsilon} n^{-1/28+2\varepsilon},$$

where $\ell(u)^2 \ll_\varepsilon u^\varepsilon$ is effective. Take $\varepsilon = 1/(56 \cdot 676)$ and write $a = 1/28 - 2\varepsilon > 0$. If $n > CD^{337}$, this ratio is at most

$$C'_\varepsilon C^{-a} D^{12+2\varepsilon-337a} = C'_\varepsilon C^{-a} D^{-1/56}.$$

An effective absolute choice of C makes this less than $1/2$. Thus $r_Q(n) \geq r_{\text{gen}}(n)/2 > 0$.

For the final algorithm, test the finitely many squarefree $n \leq CD^{337}$. Local representability is decided by the same finite congruence test, as in Duke's theorem, and integral representability is a finite search in a positive-definite ellipsoid. The bound excludes all further exceptions. $\square$

Scope of the new effectivity. The numerical value of C has not been optimized or evaluated in this record. It is an effectively computable absolute constant, which is exactly what the algorithmic conclusion needs. The existence of a constant with exponent 337 was already proved unconditionally by Duke; the conclusion newly justified by the imported zero-free theorem is its effectivity. Kane's much smaller practical thresholds, the exact Ramanujan-form exception list, and his uniform bound of order $p^{14+\varepsilon}$ for supersingular CM lifting require further weight-2 information and are excluded.

42 Effective CM lifting to every supersingular elliptic curve

Kane's published Theorems 1.1 and 1.4 [56] give effective thresholds for surjectivity and multiplicity of CM reduction under GRH. We recover those qualitative effective conclusions. The existence of thresholds without effectivity was already unconditional, by Elkies–Ono–Yang [57]. The numerical cutoffs and exceptional discriminant lists in Kane's Theorems 1.2–1.3 are not claimed here.

Let $\mathcal{S}_p$ be the finite set of geometric isomorphism classes of supersingular elliptic curves in characteristic p . For $E \in \mathcal{S}_p$, put

$$w_E = \# \text{Aut}_{\overline{\mathbb{F}}_p}(E), \quad W_p = \sum_{E \in \mathcal{S}_p} \frac{1}{w_E}, \quad \mu(E) = \frac{1/w_E}{W_p}, \quad \mu_p = \min_{E \in \mathcal{S}_p} \mu(E) > 0.$$

For a negative fundamental discriminant D , let $H_D(X) \in \mathbb{Z}[X]$ be the monic Hilbert class polynomial of degree $h(D)$. Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ to define reduction of its roots. When p does not split in $\mathbb{Q}(\sqrt{D})$, every root reduces to a supersingular invariant. Let $m_E(D)$ be the number of these

roots reducing to $j(E)$, counted before reduction. Equivalently, it is the multiplicity of $j(E)$ in $H_D(X) \bmod p$. Thus

$$\sum_{E \in \mathcal{S}_p} m_E(D) = h(D).$$

Finally, let $S_p(X) = \prod_{E \in \mathcal{S}_p} (X - j(E)) \in \mathbb{F}_p[X]$; the product has distinct roots.

Theorem 42.1 (Effective form of Kane’s CM lifting theorems). *For every prime p and every $0 < c < 1$, there is an effectively computable $D_{p,c}$ such that, for every negative fundamental discriminant D satisfying $|D| \geq D_{p,c}$ and $\left(\frac{D}{p}\right) \neq 1$, one has*

$$m_E(D) \geq c \mu(E) h(D) \quad \text{for every } E \in \mathcal{S}_p.$$

In particular,

$$S_p(X)^{\lceil c \mu_p h(D) \rceil} \mid H_D(X) \bmod p.$$

Consequently, an algorithm computes the complete finite set of negative fundamental discriminants for which p is nonsplit and the CM reduction map fails to be onto $\mathcal{S}_p$.

Proof. If $p = 2$ or 3 , there is only one geometric supersingular class. Deuring’s reduction theorem then gives $m_E(D) = h(D)$ whenever p is nonsplit, proving the assertion. Assume henceforth $p \geq 5$. Increasing the threshold allows us to assume $D < -4$, so that $\#\mathcal{O}_D^\times = 2$.

We first specify the algebraic comparison, including the inert and ramified cases. For $E \in \mathcal{S}_p$, its endomorphism ring R_E is a maximal order in the definite quaternion algebra ramified exactly at p and infinity. Its Gross lattice and theta series are

$$L_E = \{x \in \mathbb{Z} + 2R_E : \text{tr}(x) = 0\}, \quad \theta_E(z) = \sum_{x \in L_E} e^{2\pi i \text{nr}(x)z} = 1 + \sum_{n \geq 1} a_E(n) e^{2\pi i n z}.$$

Each vector of norm $|D|$ determines an embedding $\mathcal{O}_D \hookrightarrow R_E$, by sending $\sqrt{D}$ to that vector, and conversely. The embedding is optimal because $\mathcal{O}_D$ is the maximal quadratic order. Conjugation by $R_E^\times$ has stabilizer $\mathcal{O}_D^\times$ of order 2, so the number of conjugacy classes of these embeddings is $2a_E(|D|)/w_E$.

Under the CM lifting correspondence, the fraction of these embedding classes that are normalized at p is $1/2$ when p is inert and 1 when p is ramified. A normalized embedding corresponds to one CM invariant reducing to $j(E)$; these are the Deuring–Gross–Zagier facts proved in the form needed here in [57, Section 3, especially Lemma 3.2]. It follows that

$$m_E(D) = \frac{k_p(D)}{w_E} a_E(|D|), \quad k_p(D) = \begin{cases} 1, & \left(\frac{D}{p}\right) = -1, \\ 2, & p \mid D. \end{cases} \quad (129)$$

The important feature is that $k_p(D)$ is independent of E . This orbit calculation fixes the convention that w_E is the full automorphism-group order.

We next use the unconditional effective cusp-form estimate. All the lattices L_E lie in one genus: maximal quaternion orders are conjugate locally, and conjugation preserves both reduced norm and trace. Their theta series therefore have the same Eisenstein part. Fix $E_0 \in \mathcal{S}_p$. The differences $\theta_E - \theta_{E_0}$ are weight- $3/2$ cusp forms of fixed level $4p$. Duke’s bound, as used in [57, Section 3] and [53], gives effectively, for every $\eta > 0$,

$$|a_E(|D|) - a_{E_0}(|D|)| \leq A_{p,\eta} |D|^{1/2-1/28+\eta} \quad (130)$$

for fundamental D outside an effectively computable finite set, uniformly over the finite set $\mathcal{S}_p$. To make explicit a possible half-integral-weight qualification, first remove the unary-theta component and apply the estimate to its orthogonal complement. Unary theta series have support in finitely many computable square classes tm^2 at this fixed level. A fundamental discriminant has square part at most 4, so those supports contain only finitely many fundamental D . They can all be placed below the threshold. Thus no assertion about unary-theta coefficients at arbitrary integers is needed. The constants in this cusp-form bound are effective; Siegel's class-number lower bound does not enter its proof.

Set $c_E(D) = a_E(|D|) - a_{E_0}(|D|)$ and $\bar{c}(D) = W_p^{-1} \sum_E c_E(D)/w_E$. Summing (129) and using $\sum_E m_E(D) = h(D)$ yields the exact identity

$$m_E(D) - \mu(E)h(D) = \frac{k_p(D)}{w_E} (c_E(D) - \bar{c}(D)). \quad (131)$$

In particular, the normalization of the common Eisenstein series has canceled. Since $k_p(D) \leq 2$ and $w_E \geq 2$, equations (130)–(131) give

$$|m_E(D) - \mu(E)h(D)| \leq 2A_{p,\eta}|D|^{1/2-1/28+\eta}.$$

The class-number formula and Theorem 1.4 supply an effective absolute $b > 0$ with

$$h(D) \geq b \frac{\sqrt{|D|}}{\ell(|D|)}.$$

Take $\eta = 1/56$. Dividing the preceding discrepancy estimate by $h(D)$ gives, with effective B_p ,

$$\left| \frac{m_E(D)}{h(D)} - \mu(E) \right| \leq B_p |D|^{-1/56} \ell(|D|).$$

The right side tends effectively to zero. Choose $D_{p,c}$ above the finite exceptional set so that it is at most $(1-c)\mu_p$ for every $|D| \geq D_{p,c}$. Such a choice is effective, for example by bounding $\ell(t) \leq Ct^{1/112}$ with an effective absolute C . Then

$$\frac{m_E(D)}{h(D)} \geq \mu(E) - (1-c)\mu_p \geq c\mu(E).$$

Since the multiplicities are integers, the claimed divisibility with the ceiling follows. Every multiplicity is positive, so the reduction map is surjective.

For the algorithmic conclusion, take, for example, $c = 1/2$. The set $\mathcal{S}_p$, its automorphism orders, and its Gross lattices are computable by the finite elliptic-curve and quaternion procedures described in [56, Sections 2 and 4]. Their modular forms and the effective constants just used therefore give a computable threshold. Enumerate the finitely many negative fundamental D below that threshold for which p is nonsplit. Compute $H_D(X) \bmod p$ and test whether it is divisible by $S_p(X)$. Hilbert class polynomials are computable exactly, for example by reduced quadratic forms and rigorous precision bounds for their complex roots. This finite test determines every exception, and the proved threshold excludes every larger one. $\square$

Corollary 42.2 (Effective fixed multiplicity and modular congruence). *Given a prime p and a positive integer t , one can compute a threshold $D_{p,t}$ such that every negative fundamental D with $|D| \geq D_{p,t}$ and p nonsplit satisfies $S_p(X)^t \mid H_D(X) \bmod p$. In particular, one can compute a threshold beyond which there exists $G_{D,p}(X) \in \mathbb{Z}[X]$ of degree at most $\lfloor h(D)/p \rfloor$ satisfying*

$$H_D(j(z)) \mid U(p) \equiv G_{D,p}(j(z)) \pmod{p}.$$

Here $U(p)$ sends $\sum_n a(n)q^n$ to $\sum_n a(pn)q^n$.

Proof. Take $c = 1/2$ in Theorem 42.1 and enlarge its threshold until $\mu_p h(D)/2 \geq t$, using the effective class-number lower bound in that proof. This proves the first assertion. For $t = 2$, apply the unconditional polynomial congruence criterion [57, Theorem 2.3(1)]. Its hypothesis only requires the square of the product of supersingular factors with $j \notin \{0, 1728\}$ to divide $H_D \bmod p$; our stronger divisibility supplies it. The degree bound is part of that criterion. The original existence statements were already unconditional; the recovered conclusion is a computable threshold, as discussed explicitly by Kane after his Theorem 1.4. $\square$

Scope of the transfer. The exponent in the effective discrepancy estimate is used only to prove termination of the finite procedure. No bound polynomial in p for the threshold is asserted. In particular, the $p^{14+\varepsilon}$ -type thresholds and the numerical exception tables requiring weight-2 GRH are not supplied by this argument.

43 The Achter–Howe bounds for split abelian surfaces

The result recovered here is the second assertion of Achter and Howe, *Split abelian surfaces over finite fields and reductions of genus-2 curves*, *Algebra & Number Theory* **11** (2017), 39–76, Theorem 1.2, doi:10.2140/ant.2017.11.39. It concerns varieties over a fixed finite field. It does not assert the conjectured asymptotic for the primes of split reduction of a fixed abelian surface over a number field.

Write $N(q)$ for the number of $\mathbb{F}_q$ -isomorphism classes of pairs (A, λ) , where A is a two-dimensional abelian variety, λ is a principal polarization defined over $\mathbb{F}_q$, and A is isogenous over $\mathbb{F}_q$ to a product of elliptic curves. This is an ordinary cardinality; it is not the sum of reciprocal automorphism orders. Put

$$L(q) = \log(3q), \quad \ell(q) = \log \log(e^e q).$$

These positive expressions avoid conventions for the finitely many small fields.

Theorem 43.1 (Achter–Howe’s bounds). *With absolute positive constants,*

$$\frac{q^{5/2}}{L(q)\ell(q)^6} \ll N(q) \ll q^{5/2} L(q)^2 \ell(q)^4$$

for every prime power q . These are the published GRH-conditional bounds, with exactly the same logarithmic exponents, now obtained using Theorem 1.1 without an additional hypothesis.

Theorem 1.4 gives the uniform estimate

$$L(1, \chi_D) \ll \log \log(e^e |D|) \quad (D < 0 \text{ a fundamental discriminant}), \quad (132)$$

which replaces the conditional analytic input in the original proof.

The use of (132) is confined to upper bounds for imaginary quadratic class numbers. A lower bound for $L(1, \chi_D)$ is not needed.

43.1 Class numbers and the arithmetic estimate

For a negative quadratic discriminant $\Delta = f^2 D$, with D fundamental, let $h(\Delta)$ denote the proper ideal class number of the order of discriminant Δ , and set

$$H(\Delta) = \sum_{d|f} h(d^2 D).$$

This convention is the unweighted Kronecker class number used by Achter–Howe. The analytic class number formula and (132) give

$$h(D) = \frac{w_D \sqrt{|D|}}{2\pi} L(1, \chi_D) \ll \sqrt{|D|} \log \log(e^e |D|), \quad (133)$$

where $w_D \in \{2, 4, 6\}$ is the number of units in the maximal order. The order class number formula, including its unit index, is

$$h(f^2 D) = \frac{f h(D)}{[\mathcal{O}_D^\times : \mathcal{O}_{f^2 D}^\times]} \prod_{r|f} \left(1 - \frac{\chi_D(r)}{r}\right).$$

Consequently,

$$h(f^2 D) \leq h(D) \sigma(f), \quad H(f^2 D) \leq \frac{h(D)}{f} \sigma(f)^2,$$

where $\sigma(f) = \sum_{d|f} d$. Indeed,

$$\sum_{d|f} d \prod_{r|d} (1 + 1/r) \leq \sigma(f) \prod_{r|f} (1 + 1/r) \leq \frac{\sigma(f)^2}{f}.$$

The elementary bound $\sigma(f) \ll f \log \log(e^e f)$ therefore implies

$$h(\Delta) \ll \sqrt{|\Delta|} (\log \log(e^e |\Delta|))^2, \quad H(\Delta) \ll \sqrt{|\Delta|} (\log \log(e^e |\Delta|))^3. \quad (134)$$

The unit index can only improve these upper bounds, including when $D = -3, -4$.

Let $q = p^r$. An ordinary elliptic curve $E/\mathbb{F}_q$ has Frobenius trace $a(E)$ with $|a(E)| < 2\sqrt{q}$ and $p \nmid a(E)$. Write

$$a^2 - 4q = f_{a,q}^2 D_{a,q}.$$

If $\text{End}_{\mathbb{F}_q}(E)$ has conductor d in the maximal order of $\mathbb{Q}(\sqrt{a^2 - 4q})$, define its relative conductor by $r(E) = f_{a,q}/d$. The ordinary elliptic curves of trace a and endomorphism order of conductor $d \mid f_{a,q}$ form a set of cardinality $h(d^2 D_{a,q})$. These are the classical Deuring–Waterhouse stratum facts recalled in Achter–Howe, Section 4; they are unconditional.

Define

$$\psi(n) = n \prod_{r|n} (1 + 1/r), \quad A(n) = \sum_{d|n} \frac{\psi(d)}{d}.$$

Using the order class number formula as an inequality gives

$$\begin{aligned} \sum_{\substack{E/\mathbb{F}_q \text{ ordinary} \\ a(E)=a}} r(E) &= \sum_{d|f_{a,q}} \frac{f_{a,q}}{d} h(d^2 D_{a,q}) \\ &\leq f_{a,q} h(D_{a,q}) A(f_{a,q}) \ll \sqrt{q} \ell(q) A(f_{a,q}). \end{aligned} \quad (135)$$

We next establish, uniformly in q ,

$$\sum_{\substack{1 \leq a < 2\sqrt{q} \\ p \nmid a}} A(f_{a,q}) \ll \sqrt{q} L(q). \quad (136)$$

If $d \mid f_{a,q}$ then $(d, q) = 1$ and $a^2 \equiv 4q \pmod{d^2}$. Let $B_q(d)$ be the number of solutions to this congruence modulo d^2 . For odd primes $r \nmid q$, $B_q(r^j) \leq 2$, while $B_q(2^j) \leq 8$ when $2 \nmid q$. The latter

bound follows by extracting a factor 4 when $j \geq 2$ and using the at most four square roots of an odd unit modulo a power of 2; $j = 1$ is immediate. Let C be the multiplicative function with $C(r^j) = 2(1 + 1/r)$ for $j \geq 1$. By the Chinese remainder theorem,

$$\frac{\psi(d)}{d} B_q(d) \leq 4C(d) \quad ((d, q) = 1).$$

Interchanging the divisor and trace sums, and counting each residue class in an interval of length $2\sqrt{q}$, gives

$$\begin{aligned} \sum_{\substack{1 \leq a < 2\sqrt{q} \\ p \nmid a}} A(f_{a,q}) &\leq \sum_{\substack{d \leq 2\sqrt{q} \\ (d,q)=1}} \frac{\psi(d)}{d} B_q(d) \left(\frac{2\sqrt{q}}{d^2} + 1 \right) \\ &\ll \sqrt{q} \sum_{d \geq 1} \frac{C(d)}{d^2} + \sum_{d \leq 2\sqrt{q}} C(d). \end{aligned}$$

The first series converges by its Euler product. For the second sum, let $D = C * \mu$ in the sense of Dirichlet convolution. Its prime-power values are $D(r) = 1 + 2/r$ and $D(r^j) = 0$ for $j \geq 2$, so $D \geq 0$ and

$$\sum_{n \leq x} C(n) \leq x \sum_{d \leq x} \frac{D(d)}{d} \leq x \prod_{r \leq x} (1 + 1/r + 2/r^2) \ll x \log(3x).$$

The final bound follows from $\sum_{r \leq x} 1/r \leq \log \log(3x) + O(1)$. This proves (136). Since the summands for a and $-a$ are the same, (135) now yields

$$R(q) := \sum_{E/\mathbb{F}_q \text{ ordinary}} r(E) \ll qL(q)\ell(q). \quad (137)$$

43.2 Upper bound for surfaces

Let $W(q)$ count those pairs (A, λ) in $N(q)$ whose two ordinary elliptic isogeny factors are nonisogenous. The unconditional gluing estimate of Achter–Howe, Lemma 6.1, is

$$W(q) \leq \sum_{\mathcal{S}} \sum_{\mathcal{T}: a(\mathcal{T}) \neq a(\mathcal{S})} h(\mathcal{O}_{\mathcal{S}}) h(\mathcal{O}_{\mathcal{T}}) r(\mathcal{S}) r(\mathcal{T}) \sum_{n|a(\mathcal{S})-a(\mathcal{T})} \psi(n). \quad (138)$$

Here $\mathcal{S}, \mathcal{T}$ run over ordinary strata and a divisor sum of a negative integer means the divisor sum of its absolute value. This estimate uses Frey–Kani gluing and the finite group-scheme automorphism bound in Achter–Howe, Proposition 4.3 and Lemma 6.4; none of these requires GRH.

For completeness, if $F(m) = \sum_{n|m} \psi(n)$, multiplicativity gives

$$\frac{F(m)}{m} \leq \prod_{r|m} \frac{1 + 1/r}{1 - 1/r} \leq \left(\frac{m}{\varphi(m)} \right)^2 \ll (\log \log(e^e m))^2.$$

Since $0 < |a(\mathcal{S}) - a(\mathcal{T})| < 4\sqrt{q}$, we may enlarge the sum in (138) to all pairs of strata and obtain

$$W(q) \ll \sqrt{q} \ell(q)^2 R(q)^2 \ll q^{5/2} L(q)^2 \ell(q)^4.$$

The other three disjoint types are ordinary isotypic, almost ordinary, and supersingular split surfaces. The *unconditional* parts of Achter–Howe, Propositions 3.2–3.4, bound their respective numbers by

$$O(q^2 L(q)^2 \ell(q)), \quad O(q^2 L(q) \ell(q)^2), \quad O(q^2).$$

Each is absorbed by the asserted upper bound for $N(q)$. Thus one need not use, or reprove, the conditional refinements of these three propositions.

43.3 Lower bound for surfaces

We give the count allowing explicitly for automorphisms of elliptic curves. There is an absolute $c_0 > 0$ such that the number $T(q)$ of ordinary elliptic $\mathbb{F}_q$ -isomorphism classes is at least $c_0 q$ for all sufficiently large q . For example, every $j \in \mathbb{F}_q$ occurs as the invariant of an elliptic curve defined over $\mathbb{F}_q$, and the number of supersingular geometric j -invariants is at most $p/12 + 2$. Hence $T(q) \geq q - p/12 - 2 \geq q/2$ for all sufficiently large q .

For an odd prime $r \neq p$, two elliptic curves have the same symplectic type modulo r if their r -torsion group schemes are isomorphic by a map preserving the Weil pairing. There are at most $r + 4$ such types: for each trace residue $a \pmod{r}$ with $a^2 \not\equiv 4q \pmod{r}$ there is one type, and for each of the at most two remaining residues there are at most three. This is the elementary Frobenius conjugacy classification in Achter–Howe, Lemma 10.1. If $t_1, \dots, t_s$ count the ordinary curves of the different types, then Cauchy–Schwarz gives

$$\sum_{i=1}^s t_i^2 \geq \frac{T(q)^2}{r+4} \geq c_1 \frac{q^2}{r} \quad (139)$$

for an absolute $c_1 > 0$, uniformly for $r \geq 5$ and sufficiently large q .

The number of ordered pairs of ordinary elliptic curves that are isogenous is

$$\sum_{\substack{|a| < 2\sqrt{q} \\ p \nmid a}} H(a^2 - 4q)^2 \ll q^{3/2} \ell(q)^6$$

by (134). Choose a fixed positive c_2 small enough that for every prime

$$5 \leq r \leq B(q) := c_2 \frac{\sqrt{q}}{\ell(q)^6}, \quad r \neq p,$$

the last expression is at most $(c_1/2)q^2/r$. Subtraction from (139) leaves at least $(c_1/2)q^2/r$ ordered nonisogenous ordinary pairs of the same symplectic type.

Restrict to $r \equiv 1 \pmod{4}$. Choose $b \pmod{r}$ with $b^2 = -1$. Composition of a symplectic isomorphism with multiplication by b is an anti-isometry. There are at least $r - 1$ anti-isometries for each such ordered pair: the centralizer of Frobenius in $\mathrm{GL}_2(\mathbb{F}_r)$ has order at least $(r - 1)^2$, and the multiplier map has image of size at most $r - 1$. This also proves directly the bound of Achter–Howe, Lemma 10.3. Thus, for each eligible r , there are $\gg q^2$ raw triples (E, F, η) with E, F nonisogenous and $\eta : E[r] \rightarrow F[r]$ an anti-isometry.

The graph of η is maximal isotropic in $(E \times F)[r]$. The quotient $(E \times F)/\mathrm{graph}(\eta)$ therefore carries a principal polarization. The uniqueness assertion in the nonisotypic case of Frey–Kani gluing, recalled in Achter–Howe, Section 5, says that the polarized surface determines the gluing data up to isomorphism and interchange of the two factors. An elliptic curve has at most 24 origin-preserving geometric automorphisms. Consequently a single polarized isomorphism class is counted by at most $2 \cdot 24^2$ of the raw triples just counted. Distinct primes r also give distinct classes by the same uniqueness assertion. It follows that

$$W(q) \gg q^2 \#\{r \leq B(q) : r \text{ prime}, r \equiv 1 \pmod{4}, r \neq p\}.$$

The unconditional prime number theorem for the fixed progression $1 \pmod{4}$ gives a prime count $\gg B(q)/\log B(q)$ as $q \rightarrow \infty$; omitting the one possible prime p does not change this estimate. Since $\log B(q) \asymp \log q$, we conclude

$$N(q) \geq W(q) \gg \frac{q^{5/2}}{L(q)\ell(q)^6}.$$

Finally, every finite field has an elliptic curve, and its self-product with the product principal polarization belongs to the set counted by $N(q)$. Enlarging the upper constant and decreasing the lower constant therefore handles the finitely many remaining q . This completes the proof of Theorem 43.1.

Dependency and scope audit. The finite-field algebraic inputs above are the unconditional stratum description, the gluing estimate and uniqueness assertion, the elementary symplectic-type classification, and the unconditional estimates for the three nondominant surface types. Every analytic use of GRH in the published proof of Theorem 1.2 has been replaced by (132). Neither GRH for higher-degree Dedekind zeta functions nor a statement about the primes of reduction of a fixed variety occurs in this argument. The displayed inequalities have the same powers of q , $\log q$, and $\log \log q$ as the published conditional theorem.

44 Isogenous genus-two curves with a dihedral action

Let q be an odd prime power. Let $\mathcal{Z}_q$ be the set of $\mathbb{F}_q$ -isomorphism classes of smooth projective geometrically connected genus-two curves whose group of $\mathbb{F}_q$ -rational automorphisms contains D_4 , the dihedral group of order eight. The embedding of D_4 is not part of the datum counted in $\mathcal{Z}_q$. Let $P(q)$ count unordered pairs of distinct members with Jacobians isogenous over $\mathbb{F}_q$.

Theorem 44.1 (The conditional bound in Arul et al.). *There is an absolute constant C such that, for every odd prime power $q > 7$,*

$$P(q) \leq Cq^{3/2}(\log \log q)^6.$$

Thus the GRH-conditional upper bound of [66, Theorem 4.6] holds unconditionally using Theorem 1.1.

We spell out the arithmetic input and the counting argument. The geometric classification used here is unconditional: it is [66, Lemma 2.4 and Propositions 2.8 and 4.2]. It gives the following facts. Every member of $\mathcal{Z}_q$ has a model

$$Z_{c,s} : y^2 = c(x^2 + 1)(x^4 + sx^2 + 1), \quad c \in \mathbb{F}_q^\times, \quad s \neq \pm 2.$$

There are two possible square classes of c , so $\#\mathcal{Z}_q \leq 2(q-2)$. Its Jacobian is isogenous to E^2 , for an elliptic curve E with a rational point of order two. Equipping Z with an embedding of D_4 gives an injective correspondence into pairs (E, T) , where T is such a point. The inverse recovers the displayed model from the model $y^2 = c(X+1)(X^2 + sX + 1)$ of E with $T = (-1, 0)$.

Lemma 44.2. *Let $N(q, t)$ be the number of $\mathbb{F}_q$ -isomorphism classes of elliptic curves with Frobenius trace t . Uniformly for odd q and $|t| \leq 2\sqrt{q}$,*

$$N(q, t) \ll \sqrt{q} \ell(q)^3.$$

Proof. Use the unconditional enumeration of elliptic curves in an isogeny class in [67, Theorem 4.6], the same input used in [66, Lemma 4.10]. In the ordinary case, the count is bounded by an absolute constant times $H(t^2 - 4q)$, hence by $C\sqrt{q} \ell(q)^3$ using (3). In the supersingular cases, Schoof's formulas consist of bounded terms, class numbers of orders with discriminants of size at most $4p$, and, when present, terms of size $O(p)$, where $p = \text{char } \mathbb{F}_q$. If $q = p$, the unbounded terms are the class-number terms, which the same bound controls. If $q = p^a$ with $a \geq 2$, then $p \leq \sqrt{q}$, so the $O(p)$ terms also satisfy the desired estimate. This covers the boundary cases $t = \pm 2\sqrt{q}$ when q is a square. $\square$

Proof of Theorem 44.1. The Frobenius polynomial of $\text{Jac}(Z)$ is $(X^2 - tX + q)^2$, with t even because E has a rational point of order two. Let $M(q, t)$ count the members with this polynomial. The injectivity just described gives

$$M(q, t) \leq 3N(q, t),$$

since an elliptic curve has at most three nonzero rational points of order two. Tate’s isogeny theorem over finite fields shows that two Jacobians here are isogenous if and only if their polynomials agree. Consequently

$$P(q) = \sum_{\substack{t^2 \leq 4q \\ t \text{ even}}} \binom{M(q, t)}{2} \leq \frac{1}{2} \left(\max_t M(q, t) \right) \sum_t M(q, t) \ll q^{3/2} \ell(q)^3.$$

For $q > 7$, $\ell(q) \asymp \log \log q$ and $(\log \log q)^3 \ll (\log \log q)^6$. This proves the stated published bound. The argument happens to give a smaller logarithmic factor; that observation is not used to claim priority for a new bound. $\square$

The theorem concerns pairs with isogenous Jacobians. It does not count “doubly isogenous” pairs involving the additional covers considered elsewhere in [66]; the title of that paper must not obscure this distinction.

45 Integer factoring in parity and pigeonhole search classes

Jeřábek [63], Theorem 3.8(ii–iii), proved under GRH for quadratic Dirichlet characters that

$$\text{Factoring}, \text{FullFac} \in \text{PPA}, \quad \text{Factoring} \in \text{PWPP}, \quad \text{FullFac} \in \text{FP}^{\text{PWPP}}.$$

These exact qualitative conclusions need only a uniform polylogarithmic bound for small quadratic-character witnesses. They do not assert a polynomial-time algorithm for factoring integers.

Here **Factoring** takes an integer $n > 1$ and asks for a proper nontrivial divisor if n is composite, or the answer “prime” if n is prime; the latter answer is checkable in deterministic polynomial time. The problem **FullFac** asks for the complete prime factorization. This total formulation agrees with the usual composite-input formulation after a polynomial-time primality test. All integers are supplied in binary. The class **PPA** consists of total polynomially verifiable search problems reducible to finding a second odd-degree vertex of a succinctly represented undirected graph, given one such vertex. The class **PWPP** consists of search problems reducible to finding a collision in a Boolean circuit

$$C : \{0, 1\}^{m+1} \longrightarrow \{0, 1\}^m.$$

A search reduction must work for every valid answer to its oracle queries. The notation FP^{PWPP} permits polynomially many adaptive oracle calls; we do not identify this class with **PWPP**.

Theorem 45.1 (Jeřábek’s factoring conclusions). *Unconditionally, using Theorem 1.1, one has*

$$\text{Factoring}, \text{FullFac} \in \text{PPA}, \quad \text{Factoring} \in \text{PWPP}, \quad \text{FullFac} \in \text{FP}^{\text{PWPP}}.$$

Proof. By Lemma 1.6, choose fixed effective constants C, A so that every nonprincipal quadratic Dirichlet character modulo m has an integer $t \leq C(\log(2m))^A$ with $\chi(t) \neq 1$. Enlarge

$$B(n) = \left\lceil C(\log(2n))^A \right\rceil$$

to be at least 2. First perform a deterministic polynomial-time primality test, returning immediately when n is prime. Handle even inputs and perfect powers by integer arithmetic. We can therefore assume n is odd, nonsquare, and has at least two distinct prime divisors. Trial division through $B(n)$ either finds a proper divisor, or ensures that every positive integer at most $B(n)$ is a unit modulo n . If $B(n) \geq n$, trial division already succeeds, so this range causes no problem.

We first prove that some integer $a \leq B(n)^2$ satisfies

$$\gcd(a, n) = 1, \quad \left(\frac{a}{n}\right) = 1, \quad a \text{ is not a square modulo } n. \quad (*)$$

Write $n = \prod_i p_i^{e_i}$. If any e_i is even, choose such a prime $p = p_i$; otherwise choose any p_i . Then n/p is not a square. In the first case its exponent at p is odd; in the second case another prime still occurs to an odd exponent. The Jacobi character modulo n/p is therefore nonprincipal. The character bound and the unit condition give $u \leq B(n)$ with $(u/(n/p)) = -1$. Consequently

$$\left(\frac{u}{n}\right) = -\left(\frac{u}{p}\right).$$

If $(u/n) = 1$, take $a = u$. Otherwise $(u/n) = -1$ and $(u/p) = 1$. Choose $v \leq B(n)$ with $(v/p) = -1$. If $(v/n) = 1$, take $a = v$; otherwise take $a = uv$. In each case $(a/n) = 1$ and $(a/p) = -1$, proving $(*)$. The factorization of n and the selected prime p are used only to prove existence; the algorithm does not know them.

The following two inputs are unconditional theorems from [63]: **FacRoot** $\in$ PPA (Theorem 3.4), and PPA is closed under polynomial-time Turing reductions (Theorem 2.1). The problem **FacRoot** takes odd n and a with $(a/n) = 1$ and returns either a proper divisor of n or a square root of a modulo n . Query it for every $a \leq B(n)^2$ with $\gcd(a, n) = 1$ and $(a/n) = 1$. The integer from $(*)$ has no square root, so every possible collection of valid oracle answers contains a proper factor of n . The list and all its arithmetic have polynomial size in $\log n$. Thus **Factoring** $\in$ PPA. Recursive splitting, with unconditional polynomial-time primality testing, uses at most $\log_2 n$ splits, proving **FullFac** $\in$ PPA as well.

For PWPP we must justify nonadaptive batching. Because n is not a square, the character bound finds $b \leq B(n)$ with $(b/n) = -1$. For each eligible a , consider the problem **FacRootMul**(n, a, b): find a proper divisor of n or a square root of one of a, b, ab . Neither b nor ab is a square, since their Jacobi symbols are -1 . For the a in $(*)$, every answer to this problem is therefore a proper factor. All of these queries are nonadaptive.

We reproduce the collision reduction underlying [63], Theorem 3.5. For units a, b modulo odd $n > 1$, put $a_0 = 1, a_1 = a, a_2 = b$ and define

$$F : \{0, 1, 2\} \times \{1, \dots, (n-1)/2\} \longrightarrow \{1, \dots, n-1\}, \quad F(i, x) = \begin{cases} a_i x^2 \bmod n, & \gcd(x, n) = 1, \\ x, & \gcd(x, n) > 1. \end{cases}$$

Given a collision $(i, x) \neq (j, y)$, a nonunit among x, y immediately gives a proper factor. Otherwise, if $i = j$, then $x \neq y$ and $x^2 \equiv y^2 \pmod{n}$. Our choice $1 \leq x, y < n/2$ excludes both $x \equiv y$ and $x \equiv -y \pmod{n}$, so $\gcd(x - y, n)$ is a proper nontrivial divisor. If $i < j$, then $(xy^{-1})^2 \equiv a_j/a_i \pmod{n}$. This gives a square root of a or b for $(i, j) = (0, 1), (0, 2)$; for $(i, j) = (1, 2)$, the element axy^{-1} is a square root of ab .

The domain of F has size $A_0 = 3(n-1)/2$, and the range has size $M_0 = n-1$. To reduce this to the stated binary definition, take $m = \lceil \log_2 A_0 \rceil$ and pad F to a function on $\{0, 1\}^m$ by sending the new arguments injectively to fresh values outside its old range. The new range has size

$$R = 2^m - (A_0 - M_0) \leq \frac{5}{6} 2^m,$$

because $2^m < 2A_0$. Apply this padded function separately to four m -bit blocks and encode the four outputs in radix R . As $(5/6)^4 < 1/2$, the resulting circuit has $4m$ input bits and at most $4m - 1$ output bits. A collision differs in some block but has the same value in that block. The added values were injective and disjoint from the old range, so it gives a collision of F . Thus $\text{FacRootMul} \in \text{PWPP}$.

Finally suppose there are k collision circuits $C_i : \{0, 1\}^{m_i+1} \rightarrow \{0, 1\}^{m_i}$. Pad them by copying extra bits until all output lengths equal $m = \max m_i$. For one such circuit C , compress a string of length $L > m$ by repeatedly applying C to its first $m + 1$ bits, leaving the remaining bits untouched, until its length is m . Denote this function by A_C . If $A_C(u) = A_C(v)$ with $u \neq v$, compare the two compression chains at the first stage where distinct strings become equal. Their equal tails and equal compressed prefixes give distinct inputs to C with equal outputs. Taking $L = km + 1$, the circuit

$$D(z) = (A_{C_1}(z), \dots, A_{C_k}(z))$$

has $km + 1$ input bits and km output bits. A collision gives a collision of every C_i , so all k queries can be answered by one PWPP call. This is the batching argument of [63], Lemma 3.6, with the compression step made explicit.

Apply it to the polynomial list of FacRootMul instances. At least one answer must split n , proving $\text{Factoring} \in \text{PWPP}$. Recursive splitting gives $\text{FullFac} \in \text{FP}^{\text{PWPP}}$, as asserted. $\square$

46 Miller's equivalences between factoring and arithmetic functions

Theorems 3–5 of Miller's published paper [13] concern deterministic reductions between arithmetic functions and recognition of their graphs. These are separate from the primality-testing conclusion of that paper, which has long had an unconditional replacement. We recover the full qualitative conclusions of those three theorems.

For $n \geq 1$, let $\lambda(n)$ be the exponent of the finite group $(\mathbb{Z}/n\mathbb{Z})^\times$, and put

$$\lambda'(n) = \text{lcm}_{p|n}(p-1), \quad \lambda'(1) = 1.$$

Write $\text{Fac}(n)$ for the complete prime factorization of n , including its exponents. All integers are supplied in binary.

Theorem 46.1 (Miller's functional-equivalence and recognition conclusions). *The functions Fac , φ , λ , and λ' are deterministically polynomial-time equivalent in the following strong sense: given n and the single value of any one of these functions at n , one can compute the values of all the others in time polynomial in $\log(2n)$.*

Moreover, complete integer factorization is deterministically polynomial-time Turing equivalent to computing the eventual period of the base- b expansion of $1/a$, for integers $a \geq 1$, $b \geq 2$. Finally, the graphs of φ , λ , λ' , and Fac are recognizable in deterministic polynomial time.

Proof. We first give a uniform version of Miller's splitting argument that also explains why a single supplied value suffices. Suppose that $n \geq 3$ is odd and that a positive integer M satisfying

$$\lambda'(n) \mid M \tag{140}$$

is supplied. There is a deterministic algorithm factoring n in time polynomial in $\log(2n) + \log(2M)$. It does not require the prime factorization of M .

Write $M = 2^s u$ with u odd, and set $B = \lceil C_0(\log(3n))^8 \rceil$, with C_0 from Lemma 1.6. For every composite factor $d \mid n$ encountered during recursion, first test whether d is a prime power. This takes polynomial time: test the integer roots for $1 \leq e \leq \lfloor \log_2 d \rfloor$, check the identity $r^e = d$, and test r for primality by an unconditional deterministic polynomial-time primality algorithm, for example Agrawal–Kayal–Saxena [14]. A prime-power factor is then completely factored. Otherwise, for each integer $2 \leq a \leq B$, compute $\gcd(a, d)$; if this is a proper nontrivial divisor, split d . If $\gcd(a, d) = 1$, compute

$$\gcd(a^{2^j u} - 1, d), \quad 0 \leq j \leq s, \quad (141)$$

using modular exponentiation, and split whenever a proper nontrivial divisor is found. The following argument proves that this search always succeeds when d has two distinct prime divisors.

Choose distinct primes $p, q \mid d$, and write $v_p = v_2(p-1)$ and $v_q = v_2(q-1)$. If $v_p > v_q$, apply Lemma 1.6 to the quadratic character modulo p . It supplies an integer $a \leq B$ with $(a/p) = -1$. If this a is not coprime to d , its gcd already splits d : it is not divisible by p , so that gcd is smaller than d . Otherwise the 2-part of the order of a modulo p is exactly 2^{v_p} , while the 2-part of its order modulo q is at most 2^{v_q} . These parts are different. The case $v_q > v_p$ is symmetric.

If $v_p = v_q = v$, apply the same lemma to the nonprincipal quadratic character

$$\chi(a) = (a/p)(a/q) \pmod{pq}.$$

It gives $a \leq B$ prime to pq for which the two Legendre symbols are opposite. Again, either its gcd splits d , or a is a unit modulo d . In the latter case the 2-part of its order is exactly 2^v at one of p, q and at most 2^{v-1} at the other.

Thus in every case there is a tested unit a such that the 2-parts of its orders at p and q differ. Condition (140) implies that the odd parts of both orders divide u . Write the orders of a^u modulo p and q as 2^i and 2^j , where $i \neq j$ and $0 \leq i, j \leq s$. At exponent $2^{\min(i,j)} u$, precisely one of these two prime divisors divides $a^{2^{\min(i,j)} u} - 1$. The corresponding gcd in (141) is therefore strictly between 1 and d . This argument does not assume that d is squarefree: a gcd containing one prime divisor and omitting another is a proper divisor regardless of their multiplicities.

For every recursive divisor $d \mid n$, we still have $\lambda'(d) \mid \lambda'(n) \mid M$. Hence the same original value M works at every stage. There are at most $\log_2 n$ prime factors counted with multiplicity, and therefore only $O(\log n)$ recursive nodes. Each node performs $O(B \log(2M))$ modular exponentiation or gcd operations on integers of polynomial bit length. This proves the claimed deterministic polynomial bound. For even n , first remove its power of 2 by division and apply the same procedure to the odd part; condition (140) remains valid there.

Now each of $\varphi(n)$, $\lambda(n)$, and $\lambda'(n)$ is a positive multiple of $\lambda'(n)$ and is at most n . The preceding algorithm therefore recovers $\text{Fac}(n)$ from the single value of any one of them, in time polynomial in $\log(2n)$. Conversely, from $n = \prod p^{e_p}$ one computes

$$\varphi(n) = \prod_{p \mid n} p^{e_p-1}(p-1), \quad \lambda'(n) = \text{lcm}_{p \mid n}(p-1),$$

and $\lambda(n) = \text{lcm}_{p \mid n} \lambda(p^{e_p})$, where $\lambda(p^e) = p^{e-1}(p-1)$ for odd p , $\lambda(2) = 1$, $\lambda(4) = 2$, and $\lambda(2^e) = 2^{e-2}$ for $e \geq 3$. Products, gcds, and lcms have polynomial bit complexity. This proves the first assertion, including $n = 1, 2$ by direct calculation.

For the period assertion the inputs $n \leq 2$ are immediate. For $n \geq 3$, first consider an oracle giving $\text{ord}_n(a)$ when $\gcd(a, n) = 1$. Enumerate the primes $a \leq B$ that are coprime to n , and call the oracle for their orders. By Lemma 1.6, their residue classes generate $(\mathbb{Z}/n\mathbb{Z})^\times$. In a finite abelian group the lcm of the orders of a generating set is its exponent: it annihilates every product of

generators, and is itself a multiple of each generator's order. Consequently the lcm of the returned values is exactly $\lambda(n)$. There are polynomially many oracle calls; each order and their lcm are at most n . Factoring now follows from the first assertion. This is a Turing reduction, rather than a reduction using one supplied order.

To identify this oracle with Miller's period function, remove from a all prime-power factors supported on primes dividing b . No factorization oracle is needed for that removal: repeatedly divide the current denominator by its gcd with b until the gcd is 1. If the resulting denominator is v , then

$$\text{period}(a, b) = \text{ord}_v(b),$$

with the convention that the eventual period is 1 when $v = 1$ (a terminating expansion has a constant zero tail). In particular, on coprime inputs the period oracle is exactly the order oracle just used. Conversely, a factoring oracle computes the factorization of v , hence $\lambda(v)$, and then factors $\lambda(v)$ as well. Starting with $t = \lambda(v)$, for each prime $r \mid t$ divide t by r whenever $b^{t/r} \equiv 1 \pmod{v}$, repeating until no such division is possible. The resulting t is the order: throughout, the true order divides t , and any proper multiple would permit one more prime division. All intermediate integers and queries have bit length polynomial in that of (a, b) . This proves the second assertion with exactly the oracle notion in Miller's Theorem 4.

Finally consider a proposed graph input (n, y) for one of $\varphi, \lambda, \lambda'$. Reject $y < 1$ or $y > n$ immediately. Run the bounded splitting procedure above with $M = y$, allowing it to report failure if its complete search at a node finds no split and no prime-power decomposition. Whether or not (140) holds, this computation terminates in polynomial time. Accept only if it returns a factorization whose prime factors and product have been verified, and the chosen arithmetic function computed from that factorization equals y . If y is correct, (140) holds and the procedure succeeds. If y is incorrect, a verified factorization cannot give an erroneous positive answer. The graph of Fac is itself already recognized unconditionally by primality tests and multiplication; its inclusion here records Miller's complete statement, not a new consequence. This proves the last assertion and also explains the distinction between recognizing a graph and computing an unknown function value. $\square$

Literature scope. Miller's Theorems 3–5 are the admission anchors; his sharp complexity bound for the particular primality test is not asserted. The later unconditional work of Morain–Renault–Smith [15] handles specified restrictions on prime-factor sizes, and Dąbrowski–Pomykała–Shparlinski [16] still distinguishes the general deterministic reduction under GRH from its unconditional randomized version. The very recent primary preprint [17] treats special Carmichael numbers and also retains this distinction. None of those restricted or randomized results supplies the general deterministic single-value reductions proved above.

47 Deterministic extraction of roots

Adleman, Manders, and Miller [64], Theorems I and III, proved under ERH that the least square root, and more generally the least n th root for every fixed positive integer n , can be found modulo a prime in deterministic polynomial time. Their Theorem II(a) gives deterministic polynomial-time square-root extraction modulo a supplied fully factored integer. These qualitative statements survive replacing ERH by a uniform effective polylogarithmic bound for the least power nonresidue. We give the algebraic argument, including the distinction between fixed n and n supplied in binary.

Theorem 47.1 (Adleman–Manders–Miller root-extraction conclusions). *There is a deterministic algorithm that, given a prime p , an integer a , and a positive integer n , finds all roots of $X^n - a$ in $\mathbb{F}_p$*

in time polynomial in n and $\log p + \log(2 + |a|)$. In particular, for each fixed n , the least nonnegative root can be found, or nonexistence decided, in deterministic polynomial time in the bit length of (p, a) . There is also a deterministic polynomial-time algorithm for finding a square root of a modulo an integer M whose complete prime factorization is supplied, or deciding that no such root exists.

Proof. Reduce a modulo p . If $a = 0$, its only root is 0; hence assume $a \neq 0$. The case $p = 2$ is immediate. Write $N = p - 1$, and factor n by trial division. This costs polynomial time in the numerical value n , as the theorem allows; it does not assert polynomial time in $\log n$.

For each prime $r \mid \gcd(n, N)$, compute $s_r = v_r(N)$ and put $R_r = r^{s_r}$. Put

$$U = N / \prod_{r \mid \gcd(n, N)} R_r.$$

Then $\gcd(n, U) = 1$. These calculations require no factorization of N outside the primes already dividing n .

For each such r , choose successively integers $z = 1, 2, \dots$ until $z \not\equiv 0 \pmod{p}$ and $z^{N/r} \neq 1$ in $\mathbb{F}_p$. A nontrivial character of order r has precisely the r th powers as its kernel. Lemma 1.6 therefore guarantees that this search stops after a fixed polynomial in $\log p$ trials. Put $c_r = z^{N/R_r}$. It has order exactly R_r : the condition $z^{N/r} \neq 1$ says that the r -part of the order of z is R_r , and exponentiation by N/R_r , which is prime to r , preserves this part while killing all other primary parts.

Let

$$e_r = \frac{N}{R_r} \left(\left(\frac{N}{R_r} \right)^{-1} \bmod R_r \right), \quad a_r = a^{e_r}.$$

Thus e_r is 1 modulo R_r and 0 modulo N/R_r ; exponentiation by e_r is the projection of the cyclic group $\mathbb{F}_p^\times$ onto its subgroup of order R_r . When $U > 1$, define similarly $e_U = (N/U)((N/U)^{-1} \bmod U)$ and $a_U = a^{e_U}$; when $U = 1$, set $a_U = 1$. These projections satisfy

$$a = a_U \prod_r a_r.$$

Compute $j_r \in \{0, \dots, R_r - 1\}$ with $a_r = c_r^{j_r}$ by successive base- r digits. Explicitly, set $j^{(0)} = 0$ and $\omega = c_r^{r^{s_r-1}}$. Suppose the first k digits have been found, so $j_r - j^{(k)}$ is divisible by r^k . Then

$$\left(a_r c_r^{-j^{(k)}} \right)^{r^{s_r-1-k}} = \omega^{d_k}, \quad 0 \leq d_k < r.$$

Test the r possible digits and put $j^{(k+1)} = j^{(k)} + d_k r^k$. The order of ω is r , so precisely one digit works. This determines j_r after s_r stages in time polynomial in r and $\log p$.

The equation on this primary component is the ordinary linear congruence

$$nt_r \equiv j_r \pmod{R_r}.$$

It is soluble exactly when $d_r := \gcd(n, R_r)$ divides j_r . If any component fails this test, there is no root. Otherwise extended Euclid supplies one solution t_r modulo R_r/d_r , and all solutions are $t_r + kR_r/d_r$, $0 \leq k < d_r$. On the U -component the unique root is $a_U^{n^{-1} \bmod U}$, interpreted as 1 when $U = 1$. Products of these component roots give all roots in $\mathbb{F}_p^\times$. Their number is

$$\prod_r d_r = \gcd(n, N) \leq n.$$

Consequently they can all be listed within the claimed time bound, and their least nonnegative integer representative can be selected. Every operation described is deterministic. The character-search constants are uniform in p and r , and $\sum_{r|n} r \leq n$ for $n \geq 2$, so the number of field operations is polynomial in n and $\log p$.

For the factored-modulus assertion, solve separately modulo each supplied prime power $\ell^e \parallel M$, then use the Chinese remainder theorem. Here are the local details, including nonunits. Reduce a modulo ℓ^e . If $a = 0$, take local root 0. Otherwise write $a = \ell^v u$ with $v < e$ and $\ell \nmid u$. A root exists only if v is even, because the valuation of a nonzero square below e is even. If $v = 2w$, it suffices to solve

$$y^2 \equiv u \pmod{\ell^{e-2w}},$$

then take $x = \ell^w y$ modulo ℓ^e . For odd ℓ , find a root modulo ℓ by the prime-field algorithm. Given $y_k^2 \equiv u \pmod{\ell^k}$ with $\ell \nmid y_k$, determine $t \pmod{\ell}$ from

$$2y_k t \equiv \frac{u - y_k^2}{\ell^k} \pmod{\ell},$$

and set $y_{k+1} = y_k + t\ell^k$. This produces a root at the next precision. For $\ell = 2$, the unit congruence is trivial modulo 2, soluble modulo 4 exactly when $u \equiv 1 \pmod{4}$, and soluble modulo 2^h , $h \geq 3$, exactly when $u \equiv 1 \pmod{8}$. In the latter case start with $y_3 = 1$. If $y_k^2 \equiv u \pmod{2^k}$ for $k \geq 3$, choose $t \in \{0, 1\}$ so that

$$y_{k+1} = y_k + t2^{k-1}, \quad y_{k+1}^2 \equiv u \pmod{2^{k+1}}.$$

Such a choice exists because the change in the square is $t2^k y_k$ modulo 2^{k+1} , and y_k is odd. There are at most $\log_2 M$ local lifting steps in total. The Chinese remainder theorem then gives one root modulo M in polynomial time. We make no claim here to find the least root modulo a composite M ; that is a different problem in the original paper. $\square$

48 Deterministic splitting in even degree and Gao's balance test

The input in this section is a prime p and a monic squarefree polynomial $f \in \mathbb{F}_p[X]$ of degree $n > 1$ which splits completely in $\mathbb{F}_p$. The distinct roots need not be known. These input promises can be checked in polynomial time by taking a gcd with the derivative and computing $X^p \bmod f$. A *proper factor* means a divisor with degree strictly between 0 and n .

Rónyai's published factoring theorem includes a deterministic polynomial-time algorithm under GRH to find a proper factor of every such f of even degree; see [42] and the explicit discussion in [41, Section 1]. Gao's [41, Theorems 3.1 and 3.3] gives a more general decomposition based on a balance condition on the roots. We prove these conclusions with a direct construction, replacing the GRH-dependent choice of a scalar root of unity by Lemma 1.6.

Suppose first that p is odd, and write $p - 1 = 2^s w$ with w odd. Fix an element $\eta \in \mathbb{F}_p^\times$ of order 2^s . Every $a \neq 0$ has a unique expression

$$a = \eta^u \theta, \quad 0 \leq u < 2^s, \quad \theta^w = 1.$$

Define $\epsilon_\eta(a) = 1$ if $u < 2^{s-1}$ and $\epsilon_\eta(a) = -1$ otherwise. In particular $\epsilon_\eta(-a) = -\epsilon_\eta(a)$. For the set F of roots of f , put

$$t_\alpha = \#\{\beta \in F \setminus \{\alpha\} : \epsilon_\eta(\alpha - \beta) = 1\}.$$

Gao calls F *square balanced with respect to η* when all t_α equal $(n - 1)/2$. This agrees with his definition using the scalar square-root choice σ_2 : $\sigma_2(a^2) = a$ exactly when $u < 2^{s-1}$ [41, Lemma 2.6(d) and Section 2.4]. When $p \equiv 3 \pmod{4}$, ϵ_η is the quadratic character.

Theorem 48.1 (Gao's balance decomposition and Rónyai's even-degree case). *There is a deterministic algorithm with bit complexity polynomial in n and $\log p$ which, for odd p , constructs η as above and computes all polynomials*

$$f_j(X) = \prod_{\substack{\alpha \in F \\ t_\alpha = j}} (X - \alpha), \quad 0 \leq j \leq n-1.$$

Their product is f , and the nonconstant members are pairwise coprime. The algorithm therefore finds a proper factor unless F is square balanced with respect to the constructed η . In particular, every squarefree completely split polynomial of even degree over a prime field admits a deterministic polynomial-time proper factor.

Proof. Lemma 1.6, applied to the quadratic character modulo p , permits an exhaustive search in polynomial time for a quadratic nonresidue z . Set $\eta = z^w$. Since $\eta^{2^{s-1}} = z^{(p-1)/2} = -1$, η has order 2^s . Only this scalar construction uses the new analytic input.

Form the explicitly presented commutative algebras

$$A = \mathbb{F}_p[X]/(f), \quad x = X \bmod f, \quad B = A[Y]/(g(Y)), \quad g(Y) = \frac{f(Y) - f(x)}{Y - x}, \quad y = Y \bmod g.$$

As $f(x) = 0$, g is a monic polynomial of degree $n-1$ over A . The algebra B is free of rank $n-1$ over A , with basis $1, y, \dots, y^{n-2}$. Abstractly, evaluation gives

$$A \simeq \prod_{\alpha \in F} \mathbb{F}_p, \quad B \simeq \prod_{\substack{\alpha, \beta \in F \\ \alpha \neq \beta}} \mathbb{F}_p.$$

These isomorphisms are used only to prove the algorithm correct; the unknown roots are not required to compute in A or B . The element $d = x - y$ has no zero coordinate in the second product.

We compute $\epsilon_\eta(d)$ simultaneously in all coordinates of B without finding the roots of f . Choose $0 \leq v < 2^s$ with $wv \equiv 1 \pmod{2^s}$, and put $E = wv$. Thus $E \equiv 1 \pmod{2^s}$ and $E \equiv 0 \pmod{w}$. Set $V_0 = d^E$. At a coordinate where $d = \eta^u \theta$, one has $V_0 = \eta^u$. For $i = 0, \dots, s-1$ compute in B

$$S_i = V_i^{2^{s-1-i}}, \quad b_i = \frac{1 - S_i}{2}, \quad V_{i+1} = V_i((1 - b_i) + b_i \eta^{-2^i}).$$

To verify the recurrence, write $u = \sum_{j=0}^{s-1} u_j 2^j$ with $u_j \in \{0, 1\}$. Induction on i gives, in this coordinate,

$$V_i = \eta^{\sum_{j=i}^{s-1} u_j 2^j}, \quad S_i = (-1)^{u_i}, \quad b_i = u_i.$$

Consequently $e = 1 - b_{s-1}$ is an idempotent of B , whose (α, β) coordinate is 1 exactly when $\epsilon_\eta(\alpha - \beta) = 1$. All divisions in the recurrence are divisions by the scalar 2, which is invertible. No division by a possible zero divisor occurs.

Compute the relative trace

$$T = \text{Tr}_{B/A}(e) \in A$$

as the trace of the matrix for multiplication by e in the displayed A -basis of B . Under the evaluation at α , that matrix is the multiplication matrix on $\prod_{\beta \in F \setminus \{\alpha\}} \mathbb{F}_p$, so $T(\alpha) = t_\alpha$ in $\mathbb{F}_p$. Since $n \leq p$ and $0 \leq t_\alpha \leq n-1$, these integers have distinct residues modulo p . Let $\tilde{T}(X)$ be the representative of T of degree less than n . Then ordinary polynomial gcd computations give exactly

$$\gcd(f(X), \tilde{T}(X) - j) = f_j(X) \quad (0 \leq j \leq n-1).$$

This proves the claimed output and the factorization of f .

Every unordered pair of roots contributes once to $\sum_{\alpha \in F} t_\alpha$, because $\epsilon_\eta(\alpha - \beta) = -\epsilon_\eta(\beta - \alpha)$. Hence, as an equality of integers,

$$\sum_{\alpha \in F} t_\alpha = \frac{n(n-1)}{2}.$$

All f_j are trivial except one precisely when all t_α coincide. Their common value must then be $(n-1)/2$. This is precisely the square-balanced case. When n is even the common value would not be an integer, so a proper factor must be produced.

Finally we verify the time bound. The algebra B has dimension $n(n-1)$ over $\mathbb{F}_p$ and an explicit multiplication table computable from f . All exponents above have $O(\log p)$ bits, and there are $s = O(\log p)$ iterations. Repeated squaring, construction of a multiplication matrix, its trace, and n polynomial gcd computations therefore use a number of field operations polynomial in $n, \log p$. Arithmetic in $\mathbb{F}_p$ has polynomial bit complexity, as does the initial search for z . For $p = 2$, the input promises and $n > 1$ force $f = X(X-1)$, which is factored immediately. $\square$

The result produces a proper factor in even degree; it does not assert complete polynomial-time factorization after an odd-degree factor has appeared. The stronger super-square-balance criterion in [41, Theorem 3.7] invokes further automorphism-splitting machinery and is not inferred from the argument here.

49 Rónyai's splitting theorem when three divides the number of factors

Rónyai's published deterministic factoring result under GRH has running time polynomial in n^r and $\log |k|$ when r is a prime divisor of the dimension of the relevant split algebra. See [42] and its precise algebraic formulation and unconditional reduction in [29, Section 5.2 and Theorem 5.6]. The case $r = 3$ uses the finite-order Hecke theorem over $\mathbb{Q}(\sqrt{-3})$ in an essential way. The following theorem retains the polynomial-time conclusion.

Theorem 49.1 (Rónyai's case $r = 3$). *There is a deterministic algorithm, polynomial in n and $\log p$, which finds a proper factor of every squarefree polynomial $f \in \mathbb{F}_p[X]$ that splits completely and whose degree n is divisible by three.*

We first supply the one finite-field ingredient that cannot be obtained from Dirichlet characters alone.

Lemma 49.2. *Let $p \equiv 2 \pmod{3}$ be prime, and put $k = \mathbb{F}_p[Z]/(Z^2 + Z + 1)$. A noncube in $k^\times$ can be found deterministically in time polynomial in $\log p$.*

Proof. The polynomial defining k is irreducible. Identify its image of Z with the reduction of $\omega = e^{2\pi i/3}$ from $\mathcal{O} = \mathbb{Z}[\omega]$, the ring of integers of $K_0 = \mathbb{Q}(\sqrt{-3})$. First test the six units of $\mathcal{O}$ by exponentiation to $(p^2 - 1)/3$. If one is a noncube, the algorithm has finished.

Otherwise fix, only for the proof of the search bound, an isomorphism between the third roots of unity in k and in $\mathbb{C}$. The nonprincipal cubic character $\chi : k^\times \rightarrow \{1, \omega, \omega^2\}$ obtained from $z \mapsto z^{(p^2-1)/3}$ is trivial on all units of $\mathcal{O}$. Since $\mathcal{O}$ has class number one, the formula

$$\eta((\alpha)) = \chi(\alpha \bmod p), \quad p \nmid \alpha,$$

therefore defines a finite-order Hecke character on the ideals prime to (p) . It is independent of the generator. It is trivial on every principal ideal generated by $\alpha \equiv 1 \pmod{p}$, so its conductor divides

(p) and its archimedean type is trivial. It is nonprincipal: every nonzero element of k has an integral lift, and some such lift has χ -value different from one.

The estimate (76), applied to the primitive character inducing η , gives

$$\sum_{\substack{N\mathfrak{a} \leq x \\ (\mathfrak{a}, (p))=1}} \Lambda_{K_0}(\mathfrak{a})\eta(\mathfrak{a}) \ll x^{7/8} \log^2(3p^2x).$$

Removing an Euler factor, if necessary, costs $O(\log(2x))$. On the other hand $\zeta_{K_0}(s) = \zeta(s)L(s, \chi_{-3})$, so the Dirichlet explicit formula gives

$$\sum_{\substack{N\mathfrak{a} \leq x \\ (\mathfrak{a}, (p))=1}} \Lambda_{K_0}(\mathfrak{a}) = x + O(x^{7/8} \log^2(3x) + \log(2x)).$$

All constants here are absolute and effective. If every integral α of norm at most x , prime to (p) , had $\chi(\alpha) = 1$, the two sums would coincide: every ideal of norm at most x is principal and has a generator of that same norm. For

$$x = C(\log(3p))^{32}$$

with an effective absolute constant C sufficiently large, the two estimates contradict each other. Consequently there is a noncube $a + b\omega$ with $a^2 - ab + b^2 \leq x$. Since this norm is at least $(a^2 + b^2)/2$, its two coordinates satisfy $|a|, |b| \leq \sqrt{2x}$.

The algorithm simply enumerates that integer box, reduces each entry in k , discards zero, and tests whether its $(p^2 - 1)/3$ power is one. The box has $O(x)$ entries, and every test has polynomial bit complexity in $\log p$. The analytic argument establishes termination within a polynomial number of tests; the algorithm never computes a Hecke character, a prime ideal, or a class field. $\square$

Lemma 49.3. *Let k be either $\mathbb{F}_p$ with $p \equiv 1 \pmod{3}$ or the field of Lemma 49.2. Given a split commutative k -algebra C , a nonidentity k -automorphism τ of order three, and a cubic nonresidue in k , one can find a nonzero zero divisor of C deterministically in time polynomial in $\dim_k C$ and $\log |k|$.*

Proof. All algebras in this argument have an identity, and are given by structure constants. Write $Q = |k|$ and $Q - 1 = 3^s w$, where $3 \nmid w$. If z is the supplied noncube, then $\zeta = z^w$ has order 3^s . In particular $\xi = \zeta^{3^{s-1}}$ is a primitive cube root of unity.

We record explicitly that this data permits taking cube roots in k . For a known cube $a \neq 0$, find the discrete logarithm of a^w to the base ζ in the group of order 3^s by successive ternary digits. If its first j digits give u_j , its next digit $d \in \{0, 1, 2\}$ is uniquely determined by

$$(a^w \zeta^{-u_j})^{3^{s-1-j}} = \xi^d.$$

This uses s steps and only three comparisons per step. If the resulting logarithm is v , take the least representative $u \equiv vw^{-1} \pmod{3^s}$. Then $a = \zeta^u \theta$ with $\theta^w = 1$. Since a is a cube, $3 \mid u$. For $3e \equiv 1 \pmod{w}$, $\zeta^{u/3} \theta^e$ is a cube root of a ; if $w = 1$, take $e = 0$. Multiplication by $1, \xi, \xi^2$ gives all three roots. Thus this step does not require factoring $Q - 1$ or a general discrete-logarithm oracle.

The algebra C is a product of copies of k . The automorphism τ permutes these factors and has at least one cycle of length three. The ξ -eigenspace of τ is therefore nonzero. Solve $(\tau - \xi I)h = 0$ by linear algebra and choose $h \neq 0$. If multiplication by h is singular, then h itself is a nonzero zero divisor and we finish. Otherwise h is a unit.

For $0 \leq j \leq s$, compute

$$v_j = h^{(Q-1)/3^j}.$$

The first member is $v_0 = 1$. The last is nonscalar, since $\tau(v_s) = \xi^w v_s \neq v_s$ and τ fixes every scalar. Let $j \geq 1$ be the first index for which v_j is nonscalar. Then $v_j^3 = v_{j-1} = a \in k^\times$. Because C is split, each coordinate of v_j belongs to k , so a is a cube in k . Compute its three distinct cube roots b_0, b_1, b_2 by the preceding routine. At least two occur among the coordinates of the nonscalar element v_j . Consequently at least one $v_j - b_i$ is a nonzero zero divisor. Testing the three multiplication matrices identifies one. Every algebraic operation, exponentiation, and linear-system solution has the asserted polynomial complexity. $\square$

Proof of Theorem 49.1. We state precisely the already unconditional algebraic theorem that we use from [29, Theorem 5.6]. For a finite-dimensional commutative semisimple algebra A over a finite field k , a unital subalgebra B , and a prime $r \neq \text{char } k$ dividing the free B -module rank m of A , its algorithm, in deterministic time polynomial in m^r and $\log |A|$, produces either a nonzero zero divisor of A , or a unital subalgebra $C \subseteq A$ and a semiregular automorphism of C of order r , with $C^r \supseteq B$. Here semiregular means that no nonidentity group element acts as the identity on a nonzero invariant ideal. This is an unconditional published algorithm, not an additional analytic hypothesis. Its construction uses the essential part of $A^{\otimes B^r}$, the kernel intersection of the coordinate multiplication maps. This part has B -rank $m(m-1) \cdots (m-r+1)$; the coordinate r -cycle acts semiregularly. When $r \mid m$, its rank over A is coprime to r , and the descent of [29, Proposition 5.2] produces the stated zero divisor or subalgebra with automorphism. For $r = 3$ all these dimensions and the published running time are polynomial in the input dimension.

Let f be as in the theorem. For $p > 3$ choose

$$k = \begin{cases} \mathbb{F}_p, & p \equiv 1 \pmod{3}, \\ \mathbb{F}_p[Z]/(Z^2 + Z + 1), & p \equiv 2 \pmod{3}. \end{cases}$$

In the first case Lemma 1.6, applied to a cubic Dirichlet character modulo p , finds a cubic nonresidue by enumeration; in the second use Lemma 49.2. Now $A = k[X]/(f)$ is split of dimension n . Apply the cited unconditional algebraic theorem with $B = k$ and $r = 3$. If it returns C, τ , apply Lemma 49.3. The resulting nonzero zero divisor of C is also a nonzero zero divisor of A , because the inclusion is an algebra embedding. Represent this element by $g \in k[X]$ of degree less than n . Then $\gcd(f, g)$ is a proper monic factor of f . Although computed over k , its roots are a subset of the roots of f in $\mathbb{F}_p$, so all its coefficients lie in $\mathbb{F}_p$. For $p = 2, 3$ exhaustive testing of the at most three possible roots already takes polynomial time. $\square$

The usual reduction to the prime-Frobenius fixed algebra also gives the following consequence. It is recorded separately from the published split-polynomial statement.

Corollary 49.4. *Suppose a finite field $\mathbb{F}_q$ is given in the usual polynomial representation over its prime field. A squarefree polynomial over $\mathbb{F}_q$ whose number of irreducible factors is divisible by three admits a proper factor in deterministic time polynomial in its degree and $\log q$. The number of irreducible factors need not be supplied.*

Proof. Put $q = p^e$, $d = \deg f$, and $R = \mathbb{F}_q[X]/(f)$. Compute the kernel

$$B_0 = \{a \in R : a^p = a\}$$

as an $\mathbb{F}_p$ -linear subspace of the ed -dimensional vector space R . The Frobenius map and this kernel are computed by exponentiation and linear algebra. Since f is squarefree, the Chinese remainder theorem gives $R \simeq \prod_{i=1}^t \mathbb{F}_{q^{d_i}}$ and $B_0 \simeq \mathbb{F}_p^t$, where t is the number of distinct irreducible factors. Thus $t = \dim_{\mathbb{F}_p} B_0$ is itself obtained without factoring f .

Apply the same split-algebra construction to $A = k \otimes_{\mathbb{F}_p} B_0$ when $3 \mid t$. If $k = \mathbb{F}_p$, the resulting nonzero zero divisor is already in B_0 . Otherwise write it as $z = z_0 + \omega z_1$ with $z_i \in B_0$. In the description $A \simeq k^t$, a zero coordinate of z forces both corresponding $\mathbb{F}_p$ -coordinates of z_0, z_1 to vanish. At least one z_i is nonzero, and that z_i is consequently a nonzero zero divisor in B_0 and in R . Taking its gcd with f over $\mathbb{F}_q$ gives a proper factor. If $p = 2, 3$, choose any nonscalar $b \in B_0$ and test $b - c$ for the at most three $c \in \mathbb{F}_p$ instead. The construction of B_0 , its structure constants, the extension of degree at most two, and every subsequent operation use time polynomial in d and $e \log p = \log q$. $\square$

The theorem provides a proper factor under the stated divisibility condition. Repeated application does not assert complete factorization in arbitrary degree, since a resulting factor may have a number of irreducible factors divisible by neither two nor three.

50 The Pollack–Schorn algorithm for three squares

The existence of a representation by three squares is classical. The previously conditional conclusion here concerns its computational cost when the integer is supplied without a factorization. We recover the exact expected complexity in [36, Theorem 3’], rather than just polynomial-time computability. As in that paper, $M(b)$ denotes a standard bit-complexity bound for multiplying two b -bit integers; one may use ordinary multiplication or either of the fast multiplication bounds specified there. In particular $M(b) \geq b$ and $M(cb) = O_c(M(b))$ for every fixed $c > 0$.

Theorem 50.1 (Pollack–Schorn’s three-square algorithm). *There is a randomized algorithm which, given a positive integer n not of the form $4^k(8m + 7)$, returns integers x, y, z with $n = x^2 + y^2 + z^2$, always correctly, and has expected bit complexity*

$$O\left(\frac{(\log n)^2}{\log \log n} M(\log n)\right) \quad (n \rightarrow \infty).$$

No factorization of n is an input.

Proof. First remove powers of 4 and at the end rescale the three coordinates by the corresponding power of 2. This costs $O(\log n)$ bit operations. It is therefore enough to treat $n \equiv 1, 2, 3, 5, 6 \pmod{8}$. Bounded values of n can be treated by exhaustive search. Throughout the proof let $b = \lceil \log_2(n + 1) \rceil$.

We first establish the replacement for the only ERH-dependent input in [36, Section 3.1]. There are effective absolute constants $C, c > 0$ such that, for $(a, q) = 1$, $q \geq 2$, and $X \geq Cq^{16}$,

$$\#\{p \leq X : p \text{ prime}, p \equiv a \pmod{q}\} \geq c \frac{X}{\varphi(q) \log X}. \quad (142)$$

Indeed, character orthogonality and Lemma 1.2, including the principal-character term, give

$$\sum_{\substack{m \leq X \\ m \equiv a \pmod{q}}} \Lambda(m) = \frac{X}{\varphi(q)} + O(X^{7/8} \log^2(qX)).$$

The contribution from proper prime powers is $O(X^{1/2} \log^2 X)$. Since $\varphi(q) \leq q$, taking the effective absolute constant C sufficiently large makes the two error terms at most $X/(2\varphi(q))$ for every $X \geq Cq^{16}$. Dividing the remaining sum over primes by $\log X$ proves (142). The exponent 16 is convenient; its numerical value will not enter the bit complexity.

We use the following four coprime residue classes from [36, Section 2.2]:

$n \bmod 8$	q	a	D	a_{22}
2, 6	$4n$	$2n - 1$	$(p+1)/n$	p
1	$8n$	$6n - 1$	$(p+1)/n$	p
3	$4n$	$(5n - 1)/2$	$(2p+1)/n$	$2p$
5	$4n$	$(3n - 1)/2$	$(2p+1)/n$	$2p$

Here $0 < a < q$, $p \equiv a \pmod{q}$, and always $a_{22} = Dn - 1$. In the first two rows respectively $D \equiv 2 \pmod{4}$, $p \equiv 3 \pmod{8}$, and $D \equiv 6 \pmod{8}$, $p \equiv 5 \pmod{8}$. In the last two rows $p \equiv 3 \pmod{4}$, and respectively $D \equiv 5 \pmod{8}$ and $D \equiv 3 \pmod{8}$.

When p is prime, $-D$ is a quadratic residue modulo p in all four rows. Here is a verification which does not presume D squarefree. In the first two rows put $d = D/2$. In the first row, quadratic reciprocity for Jacobi symbols gives

$$\left(\frac{-D}{p}\right) = \left(\frac{-2}{p}\right) \left(\frac{d}{p}\right) = \left(\frac{-1}{d}\right) (-1)^{(d-1)/2} = 1.$$

In the second row it gives $(-D/p) = -(p/d) = -(-1/d) = 1$, since $d \equiv 3 \pmod{4}$. In the third row $D \equiv 5 \pmod{8}$ gives

$$\left(\frac{-D}{p}\right) = -\left(\frac{p}{D}\right) = -\left(\frac{-1}{D}\right) \left(\frac{2}{D}\right) = 1;$$

in the fourth row $D \equiv 3 \pmod{8}$ gives instead $(-D/p) = (p/D) = (-1/D)(2/D) = 1$. We used $p \equiv -1 \pmod{d}$ in the first two rows and $2p \equiv -1 \pmod{D}$ in the last two.

For any candidate p in the indicated progression, we now attempt the following operation without testing primality. If $p \equiv 3 \pmod{4}$, compute $R = (-D)^{(p+1)/4} \bmod p$ and retain it only when $R^2 \equiv -D \pmod{p}$. If $p \equiv 5 \pmod{8}$, compute $R = (-D)^{(p+3)/8} \bmod p$. Retain it if its square is $-D$; if its square is D , replace it by $2^{(p-1)/4}R \bmod p$ and again retain it only if its square is $-D$. In every other case discard the candidate. For a prime candidate this procedure always succeeds: Euler's criterion proves the first formula; in the second case $R^2 = \pm D$ and $(2^{(p-1)/4})^2 = -1 \pmod{p}$. For the last two rows replace R by $R + p$, if needed, to make its parity agree with $-D$. We then have a verified integer a_{12} such that

$$a_{12}^2 \equiv -D \pmod{a_{22}}.$$

Successful verification has this meaning even if p is composite. The operation costs $O(bM(b))$ when $\log p = O(b)$.

To sample candidates efficiently, put

$$L = \prod_{\substack{\ell \leq \log n \\ \ell \text{ prime, } \ell \nmid q}} \ell, \quad K = \left\lceil \frac{Cq^{15}}{L} \right\rceil, \quad X = qLK.$$

Unconditional estimates for primes imply $\log L = O(\log n)$, and in fact $L \leq q^2$ for sufficiently large n . Consequently $Cq^{16} \leq X \leq Cq^{16} + q^3$, so $\log X = O(b)$. The list of primes, the divisibility tests, and their product can be computed in $O(b^{3/2}M(b))$ bit operations, by the unconditional precomputation in [36, Section 3.3].

For each prime $\ell \mid L$, choose a residue a_ℓ independently and uniformly in $\{1, \dots, \ell - 1\}$. Let a_0 be the unique integer in $(0, qL]$ satisfying

$$a_0 \equiv a \pmod{q}, \quad a_0 \equiv a_\ell \pmod{\ell} \quad (\ell \mid L).$$

Independently choose k uniformly in $\{0, \dots, K-1\}$ and put $p = a_0 + qLk$. This samples uniformly from the set S of integers in $(0, X]$ congruent to a modulo q with no prime factor at most $\log n$. The Chinese remainder theorem gives $\#S = K\varphi(L)$. Generation costs $O(b^2)$ bit operations in expectation, by the elementary CRT calculation in [36, Section 3.3]; rejection sampling implements each uniform choice with bounded expected overhead. The larger value of K here still has $O(b)$ bits.

Each prime in the progression up to X belongs to S : its least positive representative is at least $a > \log n$ for all sufficiently large n . Therefore (142) and Mertens' theorem show that the probability of a prime candidate is at least

$$c \frac{qLK}{\varphi(q) \log X} \frac{1}{K\varphi(L)} \gg \frac{1}{\log n} \frac{qL}{\varphi(q)\varphi(L)} = \frac{1}{\log n} \prod_{\ell|qL} (1 - 1/\ell)^{-1} \gg \frac{\log \log n}{\log n}.$$

All primes at most $\log n$ divide qL , which justifies the last inequality. Repeated independent sampling followed by the verified square-root operation thus terminates almost surely in $O(b/\log b)$ expected trials. Every prime trial succeeds; composite successes can only shorten the running time.

For a successful trial form the integral symmetric matrix

$$M_F = \begin{pmatrix} (D + a_{12}^2)/a_{22} & a_{12} & 1 \\ a_{12} & a_{22} & 0 \\ 1 & 0 & n \end{pmatrix}.$$

Its first two leading principal minors are positive and D , respectively, and its determinant is $Dn - a_{22} = 1$. Hence it is positive definite. All its entries have $O(b)$ bits. The unconditional ternary reduction algorithm in [36, Proposition 2] computes $A \in \text{SL}_3(\mathbb{Z})$ and a quasi-reduced form satisfying $M_{F_{\text{qred}}} = A^t M_F A$ in $O(b \log b M(b))$ bit operations. The unique positive definite integral quasi-reduced ternary form of determinant 1 is the sum of three squares [36, Lemma 1]. To recall the short argument, write $(c_{ij}) = M_{F_{\text{qred}}}$ and $(C_{ij}) = -\text{adj}((c_{ij}))$. Its quasi-reduction inequalities give $c_{11} < 2$, $|c_{12}| \leq c_{11}/2$, and $|C_{33}| < 2$. Thus $c_{11} = c_{22} = 1$, $c_{12} = 0$, and $C_{33} = -1$. The other two inequalities $|C_{13}|, |C_{23}| \leq |C_{33}|/2$ force $c_{13} = c_{23} = 0$, after which the determinant gives $c_{33} = 1$. It follows that $A^t M_F A = I_3$.

Output the third column $(x, y, z)^t = A^{-1}(0, 0, 1)^t$. Then $x^2 + y^2 + z^2 = n$. Its computation takes $O(M(b))$ operations: indeed if H is the maximum absolute entry of M_F , its largest eigenvalue is at most $3H$, and determinant 1 gives smallest eigenvalue at least $(3H)^{-2}$. Each column u of A satisfies $u^t M_F u = 1$, hence $\|u\|_2 \leq 3H$. Thus the entries of A have $O(b)$ bits, and A^{-1} is computed from its 2×2 minors. This elementary argument supplies the needed size bound independently of the displayed bound on $\|A\|$ in the cited proposition.

The expected bit complexity is consequently

$$O\left(b^{3/2}M(b) + \frac{b}{\log b}\{b^2 + bM(b)\} + b \log b M(b)\right) = O\left(\frac{b^2}{\log b}M(b)\right),$$

as asserted. Every output is verified by the integral construction; the analytic input controls termination and expected cost. $\square$

51 Randomized identity testing for square-root circuits

An arithmetic circuit here is a finite directed acyclic graph with integer constants and variables at its input gates, and addition, subtraction, or multiplication at its other gates. Its output represents

a polynomial $f \in \mathbb{Z}[X_1, \dots, X_k]$; the polynomial is not expanded. In the *2-Radical Identity Testing problem*, or 2-RIT, the input also specifies rational primes $a_1, \dots, a_k$ in binary, and asks whether

$$f(\sqrt{a_1}, \dots, \sqrt{a_k}) = 0,$$

where the square roots are positive real numbers. There is no bound on the circuit's formal degree beyond the exponential bound inherent in its size. Balaji–Nosan–Shirmohammadi–Worrell proved under GRH that this problem belongs to coRP [34, Theorem 2]. We recover precisely this assertion. Their unconditional coNP bound is a different, already established statement and is not counted as a new consequence here.

Theorem 51.1 (2-RIT in coRP). *There is a randomized algorithm with running time bounded by a polynomial in the input length on every random branch which always answers “zero” when the displayed expression is zero, and answers “nonzero” with probability at least 1/2 when it is nonzero.*

Proof. Repeated prime radicands can be identified by merging the corresponding variables, so assume they are distinct. Choose $s \geq 2$ at least the number of gates and input radicands and at least their bit lengths and the bit lengths of all integer constants. This is bounded by the ordinary encoded input length. The primality of the radicands is part of the input specification and may also be checked in deterministic polynomial time. The algorithm performs no integer factorization.

Put

$$K = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_k}), \quad R = \mathbb{Z}[\sqrt{a_1}, \dots, \sqrt{a_k}], \quad \alpha = f(\sqrt{a_1}, \dots, \sqrt{a_k}).$$

The distinct primes are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, by their valuations. Consequently $[K : \mathbb{Q}] = 2^k$, and each independent choice of signs for the square roots is an automorphism of K . One can see the degree assertion inductively: the quadratic subfields of an already constructed extension with group $(\mathbb{Z}/2\mathbb{Z})^j$ are the fields generated by square roots of the nonempty products of its j primes. A new prime cannot give one of these fields, by its valuation, so adjoining its square root doubles the degree. In particular the monomials $\prod_i \sqrt{a_i}^{e_i}$, $e_i \in \{0, 1\}$, form a basis, and

$$R \simeq \mathbb{Z}[Y_1, \dots, Y_k]/(Y_i^2 - a_i : 1 \leq i \leq k). \quad (143)$$

We need a bound on the number of primes that could erase a nonzero answer upon reduction. At every complex embedding of K , the input constants and square roots have absolute value at most 2^s . If the maximum of 1 and the absolute values computed up to some gate is H , after one more gate it is at most $2H^2$. Thus at the output, uniformly over all embeddings,

$$\log_2 \max\{1, |\sigma(\alpha)|\} \leq (s+1)2^s.$$

If $\alpha \neq 0$, its norm $N = N_{K/\mathbb{Q}}(\alpha)$ is a nonzero rational integer satisfying

$$\log_2 |N| \leq (s+1)2^{2s} =: B_s. \quad (144)$$

It therefore has at most B_s distinct prime divisors. Neither N nor α is computed by the algorithm; their potentially exponential bit lengths cause no computational cost.

We now arrange simultaneous finite-field square roots. Put

$$Q = 8 \prod_{a_i \neq 2} a_i,$$

and find by the Chinese remainder theorem the reduced residue $a \in \{1, \dots, Q-1\}$ satisfying

$$a \equiv 7 \pmod{8}, \quad a \equiv (-1)^{(a_i-1)/2} \pmod{a_i} \quad (a_i \neq 2). \quad (145)$$

Here $(a, Q) = 1$ and $\log_2 Q \leq s^2 + 3$. For every prime $p \equiv a \pmod{Q}$, the supplementary law gives $(2/p) = 1$. For each odd a_i , quadratic reciprocity gives

$$\left(\frac{a_i}{p}\right) = \left(\frac{p}{a_i}\right) (-1)^{(a_i-1)/2} = \left(\frac{(-1)^{(a_i-1)/2}}{a_i}\right) (-1)^{(a_i-1)/2} = 1.$$

We used $p \equiv 3 \pmod{4}$. Thus every a_i is a nonzero square modulo p , and

$$r_i = a_i^{(p+1)/4} \pmod{p} \quad (146)$$

is a square root. All roots are obtained deterministically by repeated squaring. This choice of progression treats the radicand 2 as well as every odd prime.

The prime-density estimate (142), already proved from the zero-free strip, supplies effective absolute constants $c, C > 0$. Choose a sufficiently large effective integer A , fixed independently of every input, and set

$$Y = 2^{A(s+1)^3}, \quad J = \lceil Y/Q \rceil, \quad X = QJ.$$

For this choice $X \geq CQ^{16}$, $\log X = O_A((s+1)^3)$, and the number P of primes $p \leq X$ in the progression satisfies

$$P \geq c \frac{X}{\varphi(Q) \log X} \geq 4B_s. \quad (147)$$

To justify the last inequality uniformly, use $\varphi(Q) \leq Q \leq 2^{s^2+3}$ and $\log X \leq (A(s+1)^3 + 1) \log 2$. The resulting lower bound is a fixed positive constant times $2^{A(s+1)^3 - s^2 - 3} / (A(s+1)^3 + 1)$, whereas $B_s = (s+1)2^{2s}$. Enlarging the effective integer A makes both required inequalities hold for all integers $s \geq 2$.

One trial uses $t = \lceil \log_2 J \rceil$ random bits to choose $u \in \{0, \dots, 2^t - 1\}$. If $u \geq J$, discard the trial. Otherwise set $p = a + Qu$ and test primality in deterministic polynomial time. Discard a composite candidate. For a prime candidate compute the roots (146) and evaluate the given circuit modulo p at them. If the answer is nonzero, return “nonzero”. If it is zero, start the next trial. The use of a fixed number of random bits, with unsuccessful draws counted as trials, avoids unbounded rejection sampling.

For correctness, (143) shows that any selection of roots r_i defines a ring homomorphism $\rho : R \rightarrow \mathbb{F}_p$. If $\alpha = 0$, therefore, $\rho(\alpha) = 0$ on every trial. If $\alpha \neq 0$ and $p \nmid N$, the identity

$$N = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\alpha)$$

and application of ρ show that every factor on the right has nonzero image; in particular $\rho(\alpha) \neq 0$. There are at most B_s primes dividing N . By (147), at least $3P/4$ primes in the progression are therefore successful when the answer is nonzero. Since $J \leq 2^t < 2J$, one trial succeeds with probability at least

$$\frac{3P}{4 \cdot 2^t} \geq \frac{3P}{8J} \geq \frac{3c}{8 \log X} \frac{Q}{\varphi(Q)} \geq \frac{c_0}{(s+1)^3}$$

for an effective absolute $c_0 > 0$. Perform $\lceil 2(s+1)^3/c_0 \rceil$ independent trials and, if none succeeds, return “zero”. A nonzero input is then missed with probability at most $e^{-2} < 1/2$, and a zero input is always accepted.

Finally, all CRT data and trial integers have $O(s^3)$ bits. Primality testing, the $k \leq s$ modular exponentiations, and evaluation of the s -gate circuit modulo p are polynomial-time operations on such integers. The number of trials is a fixed polynomial in s , on every random branch. We never expand the circuit polynomial or compute its value as a large algebraic number. This proves the claimed coRP bound. $\square$

The statement concerns equality to zero. It makes no assertion about the sign of a radical expression, about the Sum of Square Roots comparison problem, or about the source's general radical problem with arbitrary exponents, whose splitting fields need not be abelian.

52 Two cyclotomic identity-testing theorems

In *Cyclotomic Identity Testing* (CIT), the input is an arithmetic circuit over $\mathbb{Z}$ whose input monomials X^e have exponents written in binary, together with a positive integer n in binary. Writing f for its output polynomial and $\zeta_n = e^{2\pi i/n}$, the question is whether $f(\zeta_n) = 0$. Equivalently, a multivariate circuit is evaluated at specified powers of one root of unity. Balaji–Perifel–Shirmohammadi–Worrell give two GRH-conditional conclusions which follow from the present Dirichlet input [33, Theorems 1 and 4].

Theorem 52.1 (General cyclotomic circuits). *CIT belongs to BPP: it has a randomized algorithm, polynomial in the input length on every random branch, whose error probability on each input is at most $1/3$.*

Proof. Let $s \geq 2$ bound the number of binary arithmetic gates, all integer bit lengths, and the bit length of n . Gates with more than two inputs and integer weights can be replaced by binary gates with integer constants at polynomial cost. Set $\alpha = f(\zeta_n)$. At every embedding of $\mathbb{Q}(\zeta_n)$, each input monomial has absolute value 1. The gate-by-gate bound used in (144), now with $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \leq n \leq 2^s$, gives

$$\alpha \neq 0 \implies 0 < |N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\alpha)| \leq 2^{B_s}, \quad B_s = (s+1)2^{2s}.$$

Thus there are at most B_s primes dividing this norm. The algorithm does not compute the norm or expand the polynomial.

Put $Q = \max\{2, n\}$, and choose a fixed, sufficiently large effective integer A . Define

$$Y = 2^{A(s+1)}, \quad J = \lceil Y/Q \rceil, \quad X = QJ.$$

Increasing A once and for all makes $X \geq CQ^{16}$, and the prime-density estimate (142) gives

$$P := \#\{p \leq X : p \text{ prime, } p \equiv 1 \pmod{Q}\} \geq c \frac{X}{\varphi(Q) \log X} \geq 100B_s.$$

Indeed $Q \leq 2^s$ and $\log X = O_A(s)$, whereas $X/Q \geq 2^{A(s+1)-s}$. Consequently a uniformly sampled member of $\{1 + Qu : 0 \leq u < J\}$ is prime with probability at least $c_1/(s+1)$ for an effective absolute $c_1 > 0$. Using $\lceil \log_2 J \rceil$ random bits and discarding out-of-range indices loses a factor at most 2. Deterministic primality testing identifies a prime after $O(s)$ bounded trials, with probability at least 99/100. On failure we may return an arbitrary answer. Conditioned on success, the first prime obtained is uniform among the P primes in question. Thus, if $\alpha \neq 0$, it divides the norm with probability at most 1/100.

Next we construct a probable generator of $\mathbb{F}_p^\times$ without factoring $p - 1$. Put $b = \lceil \log_2 p \rceil$ and $T = 100b$. By trial division compute all primes $r \leq T$ dividing $p - 1$. Sample $h \in \mathbb{F}_p^\times$ and retain it when

$$h^{(p-1)/r} \not\equiv 1 \pmod{p} \quad \text{for every such } r. \quad (148)$$

For the proof of the probability estimates, fix a generator g and write $h = g^u$. The algorithm does not compute g or u . A uniform h makes u uniform modulo $p - 1$, and the tests say precisely that none of the indicated primes divides u . If t is the number of distinct primes dividing $p - 1$, then $t \leq b$. Listing those primes increasingly as $r_1, \dots, r_t$ gives $r_i \geq i + 1$, hence

$$\mathbb{P}(\text{all tests pass}) \geq \frac{\varphi(p-1)}{p-1} = \prod_{i=1}^t (1 - 1/r_i) \geq \prod_{i=1}^t \frac{i}{i+1} = \frac{1}{t+1} \geq \frac{1}{b+1}.$$

Conditioned on the tests, for every prime $r > T$ dividing $p - 1$ the probability that $r \mid u$ is exactly $1/r$. This follows from the Chinese remainder theorem, since the condition involves only different prime divisors. The union bound therefore gives

$$\mathbb{P}(h \text{ not a generator} \mid \text{tests pass}) \leq \sum_{\substack{r \mid p-1 \\ r > T \text{ prime}}} \frac{1}{r} \leq \frac{b}{T} = \frac{1}{100}.$$

Sampling by b random bits, and discarding 0 or a value at least p , gives a valid uniform member of $\mathbb{F}_p^\times$ with probability at least $1/2$. After $20(b+1)$ bounded trials the probability of obtaining no retained h is at most $e^{-10} < 1/100$. The first retained value is uniform among those satisfying (148). On failure we again return an arbitrary answer.

Set $\omega = h^{(p-1)/n} \bmod p$ and evaluate the circuit at ω modulo p , answering “zero” exactly when the result is zero. Conditional on h being a generator, ω has order exactly n . Therefore evaluation at ω defines a ring homomorphism

$$\mathbb{Z}[\zeta_n] \longrightarrow \mathbb{F}_p.$$

Indeed $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$, and the order of ω precludes its vanishing in any factor with $d < n$, so $\Phi_n(\omega) = 0$. A zero input remains zero under this map. If $\alpha \neq 0$ and p does not divide its norm, applying the map to the product of its Galois conjugates shows that its image is nonzero.

The four possible bad events are failure to find a prime, a norm-dividing prime for nonzero α , failure to retain h , and a retained h that is not primitive. Their total probability is less than $4/100 < 1/3$. All trial integers have $O(s)$ bits; there are $O(s)$ prime trials and $O(s)$ generator trials, and only $O(s)$ trial divisors in (148). Primality testing, modular powers (including the binary input exponents), and modular circuit evaluation take polynomial time. Every random branch has polynomial length, proving the theorem. $\square$

Theorem 52.2 (The restricted diagonal theorem). *There is a deterministic polynomial-time algorithm for CIT when*

$$f(X) = \sum_{i=1}^m g(X)^{d_i},$$

where $g \in \mathbb{Z}[X]$ is supplied in sparse representation, its exponents and n are in binary, and the nonnegative integers d_i are in unary.

Proof. The empty sum and the case $d := \max_i d_i = 0$ are immediate, so assume $m, d \geq 1$. Put $\gamma = g(\zeta_n)$ and $H(Y) = \sum_i Y^{d_i}$, a nonzero integer polynomial of degree d . For $n \leq 2$, direct integer evaluation suffices, so take $n \geq 3$.

Lemma 1.6 gives an effective constant C such that the units modulo n represented by integers at most $C(\log(3n))^8$ generate $(\mathbb{Z}/n\mathbb{Z})^\times$. Enumerate this polynomial-size set by gcd computations. Starting from γ , construct its orbit under these generators, stopping as soon as $d + 1$ distinct elements appear. Store an orbit element $g(\zeta_n^u)$ by its exponent $u \bmod n$. A successor under a generator v is $g(\zeta_n^{uv})$; all powers in its sparse presentation can be reduced modulo n .

The equality of two stored elements is a sparse cyclotomic identity test on $g(X^u) - g(X^v)$, which has at most twice the number of terms of g . We use the previously unconditional deterministic polynomial-time sparse-CIT algorithm, given in the stronger form NC in [33, Theorem 3]. This is the algorithmic input imported in this proof. There are only polynomially many comparisons before either the orbit closes or $d + 1$ elements are found.

The Galois action is $\sigma_v(\zeta_n) = \zeta_n^v$. Since the displayed units generate the full Galois group, closure under them is the full orbit: in a finite group, the semigroup generated by a set contains its inverses. Thus if $d + 1$ elements appear, the degree of γ exceeds d , so $H(\gamma) \neq 0$. Return “nonzero” in this case.

Otherwise the complete orbit has at most d elements, and $[\mathbb{Q}(\gamma) : \mathbb{Q}] \leq d$. Write $M = \sum_j |c_j|$ for the sum of the absolute coefficients in the sparse expression $g(X) = \sum_j c_j X^{e_j}$, and set

$$V = m \max\{1, M\}^d \geq 1.$$

Every Galois conjugate of $\beta := H(\gamma)$ has absolute value at most V . If $\beta \neq 0$, its norm in $\mathbb{Q}(\gamma)$ is a nonzero integer, because β is integral. If $r = [\mathbb{Q}(\gamma) : \mathbb{Q}] \leq d$, this gives

$$1 \leq |N_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\beta)| \leq |\beta| V^{r-1} \leq |\beta| V^{d-1}.$$

Consequently either $\beta = 0$ or $|\beta| \geq V^{-(d-1)}$. The logarithm of this positive lower bound’s reciprocal is polynomial in the input size, since d is supplied in unary.

For completeness, this gap can be used without an oracle for real arithmetic. Put $\epsilon = \frac{1}{4} V^{-(d-1)}$ and approximate each $\zeta_n^{e_j}$ by a rational complex number to absolute error less than

$$\delta = \min \left\{ \frac{1}{2 \max\{1, M\}}, \frac{\epsilon}{2md(M+1)^{d-1} \max\{1, M\}} \right\}.$$

The angles are $2\pi(e_j \bmod n)/n$. Rational approximations to π , sine, and cosine with the required accuracy are computable in polynomial time by their standard convergent series and range reduction; $\log(1/\delta)$ is polynomial in the input size. Form the resulting rational approximation $\tilde{\gamma}$ by exact rational arithmetic. It satisfies $|\tilde{\gamma} - \gamma| < \delta M \leq 1/2$ and $|\tilde{\gamma}| \leq M + 1$. The identity $z^e - w^e = (z - w) \sum_{j=0}^{e-1} z^j w^{e-1-j}$ gives

$$|H(\tilde{\gamma}) - H(\gamma)| \leq md(M+1)^{d-1} \delta M < \epsilon.$$

The exact rational computation of $H(\tilde{\gamma})$ has polynomial bit complexity, again because d is unary. Compare its squared complex absolute value with $(2\epsilon)^2$, a comparison of rational numbers. For zero β the magnitude is less than ϵ ; for nonzero β it exceeds 3ϵ . This decides correctly in deterministic polynomial time. $\square$

The analytic dependence in the first theorem is solely prime density in one arithmetic progression. In the second it is solely a polynomial-size generating set for the units modulo n . The sparse and bounded-degree cases which were already unconditional in the source are not counted again.

53 Castel's polynomial-time isotropic-vector algorithm

The precise published conditional conclusion used here is [2, Fact 2], attributed there to Castel: under GRH, a nonzero isotropic vector for an indefinite rational quadratic form in dimension at least five can be found in randomized polynomial time. Castel's published paper [1, Theorem 2.20 and Section 2F] supplies the algorithm and its correctness; it explicitly defers the complete complexity analysis to his thesis. We prove the qualitative polynomial-time conclusion, without asserting the original algorithm's more specific operation count or its particular prime-search range.

Theorem 53.1 (Castel's conclusion without GRH). *Given an indefinite symmetric rational matrix Q of dimension $n \geq 5$, there is a Las Vegas algorithm that returns a nonzero rational vector v with $v^T Q v = 0$, in expected time polynomial in the binary input length. The algorithm uses no integer-factorization oracle. Clearing denominators gives a nonzero integral solution when desired.*

We use three established algorithmic inputs with their precise scopes. Integer Hermite and Smith normal forms, including their transformation matrices, can be computed in polynomial time. Simon's indefinite LLL algorithm [4] either returns an isotropic vector or an integrally equivalent reduced matrix, in polynomial time. Finally, two unconditional randomized algorithms are used: the Adleman–Estes–McCurley algorithm [3] solves $x^2 + ay^2 = b \pmod{m}$ for odd m and $(ab, m) = 1$ without knowing the factorization of m (a returned answer is checked and failures are repeated); Simon's algorithm [5, Algorithms 5–7] finds a rational isotropic vector in fixed dimension at least four when one exists and the factorization of the determinant is supplied. The latter input is also recorded as [2, Fact 1]; its required factorization here will always be the already known factorization of $\pm 2p$. Simon's use of quadratic 2-class groups is through the unconditional randomized algorithm of Bosma–Stevenhagen [6]; see especially its Section 6, where the remaining random step is finding quadratic nonresidues modulo known primes. The Adleman–Estes–McCurley input is important: the older Pollard–Schnorr implementation cited by Castel was originally analyzed conditionally, and is not silently being treated as unconditional here.

Lemma 53.2 (Controlled minimization). *For an integral nondegenerate indefinite matrix Q of size five one can, in expected polynomial time, either find an isotropic vector or construct an integral matrix A rationally similar to Q such that*

$$\det A \neq 0, \quad \det A \text{ is odd}, \quad \text{SNF}(A) = \text{diag}(D, 1, 1, 1, 1), \quad D = |\det A|.$$

The matrix A and the accumulated similarity transformation have bit length polynomial in that of Q , and $D \leq |\det Q|$.

Proof. Write the positive Smith invariants in the order $d_5 \mid d_4 \mid \cdots \mid d_1$. If $d_2 > 1$, let $k \geq 2$ be the largest index with $d_k > 1$. The Smith transformation gives an integral unimodular change of variables after which the first k rows and columns of Q are divisible by any chosen divisor $m > 1$ of d_k . For $k \geq 3$ choose $m = d_k$, multiply the last $5 - k$ basis vectors by m , and divide the form by m . The resulting matrix is integral and its determinant is the previous determinant times m^{5-2k} , hence decreases in absolute value.

For $k = 2$, take $m = 2$ if d_2 is even and otherwise take $m = d_2$. The bottom 3×3 block is nonsingular modulo every prime dividing m . If $m = 2$, its associated quadratic function on $\mathbb{F}_2^3$ is linear, so a nonzero zero is found by linear algebra. For odd m , perform Gram–Schmidt over $\mathbb{Z}/m\mathbb{Z}$. A nonzero nonunit encountered in testing a pivot yields a proper divisor of m by a gcd; replace m by this divisor and restart. Each such replacement at least halves m . If all the tested norms vanish, testing sums of basis vectors and the invertibility of 2 supplies a nonzero pivot or a proper

divisor. Thus one obtains, after polynomially many operations, a diagonal ternary form with unit coefficients a, b, c modulo the current odd m . The Adleman–Estes–McCurley algorithm solves

$$x^2 + (b/a)y^2 = -c/a \pmod{m}.$$

Consequently the ternary block has a zero represented by a vector primitive modulo m . Lift it to an integral vector and divide by the gcd of its coordinates; that gcd is coprime to m , so the resulting primitive vector is still a zero modulo m . Complete it to an integral unimodular basis of the ternary block. In the resulting full matrix, the first two rows are divisible by m and the third diagonal entry is divisible by m . Multiplying the last two basis vectors by m and dividing the form by m therefore gives an integral matrix and divides its determinant by m . This is the minimization behind [1, Section 2B], with the unconditional bivariate-congruence routine specified explicitly.

After each minimization, apply indefinite LLL with a fixed parameter $1/4 < \delta < 1$, stopping if it finds an isotropic vector. Otherwise write the Gram–Schmidt diagonal entries as $B_1, \dots, B_5$. They satisfy $|B_i| \leq \gamma |B_{i+1}|$, where $\gamma = (\delta - 1/4)^{-1}$, and the size-reduction coefficients have absolute value at most $1/2$. Every leading principal minor is a nonzero integer. In particular

$$|B_5| = \frac{|\det Q|}{|\det Q_{[1,4]}|} \leq |\det Q|, \quad |B_i| \leq \gamma^{5-i} |\det Q|.$$

The entries of the reduced matrix are therefore at most $C|\det Q|$ in absolute value, with an absolute constant C . There are at most $\log_2 |\det Q|$ determinant-decreasing steps. Smith transformations, the modular operations, and the individual LLL transformations have polynomial bit complexity; multiplication of this polynomial number of transformation matrices preserves a polynomial bound on their accumulated bit length. We have thus reached $d_2 = 1$ with controlled size.

It remains to remove the even part. Let $v = v_2(\det Q)$ for the present matrix. A Smith change of basis makes the first row and column divisible by 2^v . Dividing the first basis vector by $2^{\lfloor v/2 \rfloor}$ keeps the matrix integral and leaves determinant valuation zero or one. The other four-dimensional block stays invertible modulo 2, and the rank modulo every odd prime is unchanged. If the valuation is one, write the matrix modulo the first row and column as a nonsingular symmetric bilinear form B on $\mathbb{F}_2^4$. Such a form has a two-dimensional totally isotropic subspace. For an alternating form this is a Lagrangian plane. Otherwise let w be the characteristic vector defined by $B(x, x) = B(x, w)$. Orthogonal decomposition into one-dimensional forms and alternating planes shows $B(w, w) = 0$ because the dimension is even; choose $v \in w^\perp$ outside $\langle w \rangle$, and use $\langle w, v \rangle$. A basis of this plane can be put in the first two positions of the four-dimensional block by an integral unimodular lift of a matrix in $\text{GL}_4(\mathbb{F}_2)$. Now multiply the entire form by 2 and divide its first three basis vectors by 2. The first row of the previous matrix was even, and the chosen 2×2 block was zero modulo 2, so all the resulting entries are integral. The determinant is divided by 2 and is odd. The rank at every odd prime is unchanged, hence the new matrix still has $d_2 = 1$. All these additional operations have polynomial bit complexity. $\square$

Lemma 53.3 (Prime completion). *Let A satisfy Lemma 53.2, with $D > 1$. For either specified sign $\sigma \in \{1, -1\}$, one can find, in expected polynomial time, an integral column u and an odd prime $p \nmid D$ such that*

$$u^\top \text{adj}(A)u \equiv 2\sigma p \pmod{D}, \quad p \leq C_0 D^{32},$$

where C_0 is an absolute effectively computable integer. The expected number of trials is $O(\log(2D))$; the algorithm does not factor D .

Proof. Put $G = (\mathbb{Z}/D\mathbb{Z})^\times$ and $H = G^2$. For each $\ell^e \parallel D$, local congruence diagonalization over $\mathbb{Z}/\ell^e\mathbb{Z}$ puts A in the form $\text{diag}(a_1, a_2, a_3, a_4, 0)$, with all a_i units. Here ℓ is odd and the Smith hypothesis gives rank four at ℓ . It follows that the adjugate quadratic form is a unit times the square of a primitive linear form. Its unit values constitute a single square coset locally; every such value has exactly $2\ell^{4e}$ preimages. Chinese remaindering shows that the unit values of $u^\top \text{adj}(A)u$ form one coset aH , and every one has exactly hD^4 preimages modulo D , where

$$h = [G : H] = 2^{\omega(D)} \leq D.$$

This factorization is used only to prove the distribution statement. The algorithm itself samples u directly modulo D .

Let $cH = (\sigma/2)aH$. Orthogonality on G/H and the prime-counting estimate from the 7/8 Dirichlet strip give, uniformly in this coset,

$$\pi_{cH}(X) = \frac{\text{Li}(X)}{h} + O(X^{7/8} \log^2(DX)).$$

Indeed all characters of G/H are quadratic Dirichlet characters modulo D ; the factor $1/h$ in the orthogonality formula cancels the number of error terms. Induced characters differ from their primitive characters only at primes dividing D , which is harmless in the stated error. The principal term uses the same zeta zero-free input. Taking $K = C_0 D^{31}$ and $X = DK = C_0 D^{32}$, with C_0 large enough, gives at least $X/(3h \log X)$ odd primes in cH . To see uniformity, the ratio of the error to $X/(h \log X)$ is at most $CDX^{-1/8} \log^3(DX)$; this is made uniformly small for $D \geq 3$ by one effective choice of C_0 .

One trial samples $u \in \{0, \dots, D-1\}^5$ uniformly, computes $b = u^\top \text{adj}(A)u \bmod D$, and discards the trial if $(b, D) > 1$. Otherwise let $r \in \{1, \dots, D\}$ represent $(\sigma/2)b \bmod D$, choose $j \in \{0, \dots, K-1\}$ uniformly, and test $p = r + jD$ for being an odd prime. An exact polynomial-time primality test makes this a Las Vegas procedure. Each admissible prime appears in a trial with probability exactly $h/(DK) = h/X$: its corresponding value b has hD^4 preimages among the D^5 possible columns, and j has K possibilities. Thus the success probability is at least $1/(3 \log X)$. All sampled numbers have $O(\log(2D))$ bits, and the adjugate and its value are computed with polynomially many bit operations. This proves the assertion. $\square$

Proof of the theorem. If Q is singular, a nonzero vector in its rational kernel already solves the problem and is found by linear algebra. Otherwise rational diagonalization first reduces the problem to a five-dimensional indefinite subform: choose five nonzero diagonal coefficients including both signs. Clear denominators, and apply Lemma 53.2. Unless a solution has already been found, let A be its output and write $\Delta = \det A$. Choose σ so that adding a one-dimensional form of sign $-\sigma/\Delta$ makes both signature indices at least two. Explicitly, if the negative index is one take $\sigma = \text{sign}(\Delta)$; if the positive index is one take the opposite sign; if both indices are already at least two either sign works.

Use Lemma 53.3 and set

$$z = \frac{u^\top \text{adj}(A)u - 2\sigma p}{\Delta}, \quad F = \begin{pmatrix} A & u \\ u^\top & z \end{pmatrix}.$$

This is integral, $\det F = -2\sigma p$, and its Schur complement is $-2\sigma p/\Delta$, so its two signature indices are at least two. If $D = 1$, simply use $u = 0$, $p = 3$ and the same formula for z . Every entry has polynomial bit length and the full factorization of $\det F$ is known. Meyer's theorem gives isotropy, and Simon's unconditional algorithm with this supplied factorization constructs a primitive isotropic vector t .

Complete t to a unimodular integral basis. If the gcd of the entries in its first Gram row is a , then $a^2 \mid \det F$: the top-left entry is zero, and each term in the determinant uses one further first-row entry and one further first-column entry. Since $\det F = \pm 2p$ is squarefree, $a = 1$. Euclidean operations on the remaining basis vectors therefore make the first row $(0, 1, 0, 0, 0, 0)$. Subtracting multiples of the first vector from the others and reducing the second diagonal entry modulo 2 splits off a block

$$\begin{pmatrix} 0 & 1 \\ 1 & \varepsilon \end{pmatrix}, \quad \varepsilon \in \{0, 1\}.$$

The complementary integral form F_4 has determinant $\pm 2p$ and is indefinite. It is locally isotropic at every odd prime not dividing $2p$: its nonsingular reduction in four variables has a nonzero zero, which lifts. At 2 and p its determinant is nonsquare because the valuation is one; an anisotropic four-dimensional quadratic form over a nonarchimedean local field of characteristic zero has square determinant. Thus it is isotropic at these places as well, and it is isotropic over $\mathbb{R}$. The Hasse–Minkowski theorem proves its rational isotropy. Simon’s algorithm, still with only the known factorization $2p$, constructs a second primitive isotropic vector. The same gcd and splitting argument gives a second hyperbolic plane. All these fixed-dimensional linear operations have polynomial bit complexity.

The two first vectors of these planes span a two-dimensional totally isotropic rational subspace W for F . Its intersection with the hyperplane having last coordinate zero is nonzero. Computing that intersection gives a nonzero isotropic vector for A . Undo the stored similarities and the initial restriction to obtain the required vector for Q . The only potentially unbounded repetitions were the unconditional bivariate-congruence calls and the prime-completion trials, both of expected polynomial length, so the total expected bit complexity is polynomial. $\square$

54 Finding prime values of positive definite quadratic forms

An integral quadratic form in r variables is a homogeneous polynomial $F \in \mathbb{Z}[X_1, \dots, X_r]$ of degree two. It is primitive when the gcd of its coefficients is one, equivalently the gcd of its values on $\mathbb{Z}^r$ is one. Write $F(X) = X^t G X$, with half-integral symmetric Gram matrix G , and use the discriminant convention

$$\text{disc}(F) = \begin{cases} (-1)^{r/2} \det(2G), & r \text{ even,} \\ \frac{1}{2}(-1)^{(r+1)/2} \det(2G), & r \text{ odd.} \end{cases}$$

The input length is the total binary length of the coefficients.

Theorem 54.1 (Wesolowski’s prime-value algorithm). *There is an effective absolute constant $c > 0$ and a Las Vegas algorithm with the following property. Given a primitive, positive definite, integral quadratic form F of rank $r \geq 2$, and an integer*

$$\rho > (2^{r^2} |\text{disc}(F)|)^c,$$

the algorithm returns $v \in \mathbb{Z}^r$ such that $F(v)$ is prime and $\rho < F(v) \leq \rho^2$. Its expected bit complexity is polynomial in the input length of F and $\log \rho$. It requires no integer factorization oracle.

This is the prime-value conclusion of [23, Proposition III.1], also stated as Proposition 3.6 in the full version. The constant c there is unspecified, so enlarging this absolute constant preserves the published conclusion. Rank at least two is the domain of the source’s binary-form reduction; rank one must be excluded, since the primitive form X^2 has no prime values. The sharper bounds $|\text{disc}(F)|^{1+\epsilon}$ in other propositions of that paper are not asserted here.

Proof. We first supply a uniform lower bound for primes represented by a binary quadratic form. This uses a published unconditional Chebotarev theorem, together with the present Dirichlet input only to remove its possible exceptional real zero.

Let $g(X, Y) = aX^2 + bXY + cY^2$ be a primitive positive definite integral binary form of discriminant $D = b^2 - 4ac < 0$, and write $D = f^2 D_K$, where D_K is the fundamental discriminant of $K = \mathbb{Q}(\sqrt{D})$. Let L be the ring class field of the order $\mathbb{Z} + f\mathcal{O}_K$. Class field theory identifies

$$H = \text{Gal}(L/K) \simeq \text{Pic}(\mathbb{Z} + f\mathcal{O}_K), \quad |H| = h(D).$$

Moreover $L/\mathbb{Q}$ is Galois, with generalized dihedral group: complex conjugation acts on H by inversion. The Artin element $\sigma \in H$ of the class corresponding to g has conjugacy class $C = \{\sigma, \sigma^{-1}\}$ in $\text{Gal}(L/\mathbb{Q})$, with repetitions removed. A rational prime $p \nmid D$ with Artin class C is represented by g . In particular $|C| \geq 1$ and $[L : \mathbb{Q}] = 2h(D)$.

For a Hecke character $\chi \in \hat{H}$, its conductor divides $f\mathcal{O}_K$. Thus the conductor parameter

$$Q_L = \max_{\chi \in \hat{H}} N_{K/\mathbb{Q}} f_{\chi} \quad \text{satisfies} \quad |D_K| Q_L \leq |D_K| f^2 = |D|.$$

This parameter, rather than the discriminant of the potentially large ring class field L , is essential.

We recall precisely the consequence of the unconditional [28, Theorem 1.4] that we use. There are effective absolute constants $c_2, c_3 > 0$ for which, when $x \geq (4|D_K|Q_L)^{c_2}$,

$$\begin{aligned} \pi_C(x) &= \frac{|C|}{2h(D)} (\text{Li}(x) - \theta_1 \text{Li}(x^{\beta_1})) (1 + O(E(x))), \\ E(x) &= \exp\left(-\frac{c_3 \log x}{\log(4|D_K|Q_L)}\right) + \exp\left(-\sqrt{c_3 \log x/2}\right). \end{aligned}$$

Here π_C counts unramified rational primes of class C , the implied constant is effective and absolute, and the term involving β_1 is omitted unless a real character of H has a real zero

$$\beta_1 = 1 - \frac{\lambda_1}{\log(4|D_K|Q_L)}, \quad 0 < \lambda_1 < \frac{1}{8}.$$

The field degree in the exponential error is $[K : \mathbb{Q}] = 2$; there is no dependence on $h(D)$ in that error.

Such an exceptional zero is absent here. For the trivial character, the Hecke L -function is $\zeta_K(s) = \zeta(s)L(s, \chi_{D_K})$. For a nontrivial real character χ of H , let $M = L^{\ker \chi}$. The inversion action becomes trivial on $H/\ker \chi \simeq C_2$, so $M/\mathbb{Q}$ is biquadratic. If its other two quadratic fields have primitive Dirichlet characters χ_1, χ_2 , the zeta factorizations give

$$L_K(s, \chi) = \frac{\zeta_M(s)}{\zeta_K(s)} = L(s, \chi_1)L(s, \chi_2).$$

Theorem 1.1 excludes zeros of these factors for $\Re s > 7/8$. The possible β_1 lies in this region, since $4|D_K|Q_L \geq 12$ and hence $\log(4|D_K|Q_L) > 1$. This removes the exceptional term without assuming a zero-free half-plane for arbitrary Hecke characters.

Choose an effective absolute A sufficiently large that the relative error above is at most $1/2$ for all $x \geq (4|D|)^A$. Increase A further to absorb the at most $\omega(|D|) \ll \log(3|D|)$ primes dividing D , using the class-number upper bound below. If $\pi_g(x)$ counts primes represented by g , we obtain

$$\pi_g(x) \geq \pi_C(x) - \omega(|D|) \geq \frac{\text{Li}(x)}{8h(D)} \gg \frac{x}{h(D) \log x} \quad (x \geq (4|D|)^A). \quad (149)$$

We also use the standard unconditional class-number upper bound

$$h(D) \ll \sqrt{|D|} \log(3|D|). \quad (150)$$

For clarity this is uniform for nonfundamental D : the order class number formula multiplies the maximal-order value by $f \prod_{p|f} (1 - \chi_{D_K}(p)/p)$, divided by the unit index. The usual upper bound for the imprimitive Dirichlet value $L(1, \chi_D)$ is $O(\log(3|D|))$; the order class-number formula then gives (150). It is also the unconditional estimate used in the source's prime-sampling proof.

We next turn the lower density into an exact discrete sampling algorithm. Apply Gauss reduction to g , recording its integral change of variables. We may assume $|b| \leq a \leq c$; hence

$$3ac \leq |D| \leq 4ac, \quad g(x, y) \geq \frac{1}{2}(ax^2 + cy^2), \quad c \leq |D|.$$

Set $R = \rho^2$ and sample integer pairs uniformly from the rectangle

$$|x| \leq \left\lceil \sqrt{2R/a} \right\rceil, \quad |y| \leq \left\lceil \sqrt{2R/c} \right\rceil.$$

Integer square-root computations determine the endpoints exactly. Uniform integer sampling by binary rejection has constant expected overhead. If $R \geq |D|$, this rectangle contains $O(R/\sqrt{|D|})$ lattice points and contains every integral pair with $g(x, y) \leq R$.

Choose an absolute A_1 sufficiently large, and suppose $\rho > (4|D|)^{A_1}$. Equation (149), with $x = \rho^2$, and the trivial bound of ρ for the number of primes at most ρ , imply

$$\#\{p : \rho < p \leq \rho^2, p \text{ prime and represented by } g\} \gg \frac{\rho^2}{h(D) \log \rho}.$$

Indeed the subtracted ρ is absorbed uniformly by this main term, by (150) and the choice of A_1 . Each such prime supplies at least one pair in the sampling rectangle. Therefore the probability that a trial gives a prime value in the desired interval is at least

$$\gg \frac{\sqrt{|D|}}{h(D) \log \rho} \gg \frac{1}{\log(3|D|) \log \rho}.$$

Evaluate $g(x, y)$, check the interval, and apply deterministic primality testing. Repeat until successful. Each trial has bit complexity polynomial in $\text{length}(g) + \log \rho$, and the expected number of trials is polynomial in these quantities. All outputs are checked; no continuous sampling or real-arithmetic oracle is used.

Finally we reduce arbitrary rank $r \geq 2$ to the binary case while controlling its discriminant. Put $\Delta = |\text{disc}(F)|$ and $B = 2^{r^2} \Delta$. The unconditional LLL algorithm supplies an integral basis $b_1, \dots, b_r$ with

$$\prod_{i=1}^r F(b_i) \leq 2^{r(r-1)/2} \det G \leq 2^{r(r-1)/2} \Delta =: U.$$

Every $F(b_i)$ is a positive integer, so each is at most U . Let $u = b_1$ and $m = F(u)$. If $m = 1$, set $v = b_2$; then $g(X, Y) = F(Xu + Yv)$ is positive definite and primitive.

Suppose $m > 1$. Sample $v = \sum_i v_i b_i$, with the v_i independent and uniform in $\{0, \dots, m-1\}$, until $\gcd(m, F(v)) = 1$. This uses gcd computations, not factorization. Here is a uniform bound for its success probability. For every odd prime $p \mid m$, primitivity of F implies that its reduction is a nonzero polynomial over $\mathbb{F}_p$ of degree two. At most $2p^{r-1}$ vectors are zeros, by the elementary polynomial root bound. For $p = 2$, its restriction to $\mathbb{F}_2^r$ is a nonzero multilinear polynomial of

degree at most two: diagonal terms become linear, and distinct cross terms remain distinct. Such a polynomial is nonzero on at least one quarter of the vectors. To see this, if a quadratic coefficient occurs, fix all other variables and examine its two variables; their product coefficient is nonzero, so at least one of the four values is nonzero. If no quadratic coefficient occurs, a nonzero linear or constant polynomial has the same lower bound. The Chinese remainder theorem makes the conditions for different $p \mid m$ independent.

If $p_1 < \dots < p_t$ are the odd prime divisors of m , then $p_i \geq i + 2$ and $t \leq \log_2 m$. Consequently

$$\mathbb{P}(\gcd(m, F(v)) = 1) \geq \frac{1}{4} \prod_{i=1}^t (1 - 2/p_i) \geq \frac{1}{4} \prod_{i=1}^t \frac{i}{i+2} = \frac{1}{2(t+1)(t+2)}.$$

The expected number of trials is thus $O((1 + \log m)^2)$. On success u, v are linearly independent: since u is a basis vector, an integral v in its rational span would be an integral multiple of u and would have $m \mid F(v)$. Moreover $\gcd(F(u), F(v)) = 1$ makes the binary restriction primitive.

The Cauchy–Schwarz inequality for the positive form gives

$$F(v) \leq \left(\sum_i |v_i| \sqrt{F(b_i)} \right)^2 \leq r^2 m^2 U.$$

For the binary discriminant D_g this yields

$$|D_g| \leq 4F(u)F(v) \leq 4r^2 U^4 \leq B^5.$$

The same bound holds in the case $m = 1$. All basis transformations and constructed vectors have polynomial bit length; LLL, gcd, evaluation, and reduction have polynomial bit complexity. Taking the absolute constant c in the theorem large enough ensures that $\rho > B^c$ implies $\rho > (4|D_g|)^{A_1}$. Apply the binary algorithm to g and return $xu + yv$ when it produces the pair (x, y) . The two successive random searches have polynomial expected running time, and primality and the required interval are checked exactly. This proves the theorem. $\square$

The ring class field is used only in the proof of prime density; the algorithm never constructs it, its class group, or the factorization of its discriminant. The full isogeny-path equivalence in [23] also uses class-group generation by small prime ideals over varying quadratic fields. That additional assertion is not proved by this argument and is not included in the theorem.

55 Worst-case to average-case reductions to supersingular maximal orders

For a prime $p > 3$, let $B_{p,\infty}$ be the rational quaternion algebra ramified precisely at p and at the real place. All endomorphisms below are geometric endomorphisms. The problem **MaxOrder** takes a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and asks for a maximal order in a presented copy of $B_{p,\infty}$ isomorphic to $\text{End}(E)$. The problem **MOER** additionally asks for an explicit isomorphism with $\text{End}(E)$, represented by four efficiently evaluable endomorphisms and their corresponding quaternions. An efficient representation of an isogeny permits its evaluation in time polynomial in the input length, the logarithm of its degree, and the degree of the field containing the evaluation point.

The stationary distribution on geometric supersingular isomorphism classes is

$$\mu_p(E) = \frac{24}{(p-1) \# \text{Aut}(E)}.$$

It has total variation distance $O(p^{-1})$ from the uniform distribution. As in the source, an average-case reduction permits a query distribution at negligible statistical distance from μ_p ; here p^{-1} is negligible in the bit length $\log p$.

Theorem 55.1 (Herlédan Le Merdy–Wesolowski’s maximal-order reduction). *For every prime $p > 3$, the worst-case MOER problem reduces to the average-case MaxOrder problem in probabilistic polynomial time. The query consists of one curve whose distribution is at total variation distance at most p^{-1} from μ_p . The reduction’s running time is polynomial in the input and oracle-output lengths. It applies to arbitrary valid maximal-order outputs, including outputs in different presented copies of $B_{p,\infty}$.*

This is the entire conclusion of [21, Section 7.3], Proposition 17 in the authors’ current minor revision of their TCC 2025 paper (Proposition 7.5 in the earlier version). The source assumes GRH when $p \equiv 1 \pmod{8}$. We give the missing uniform construction and then detail the unconditional remainder of the reduction.

Proof. We first construct, without an oracle, one curve E_0 with a known solution of MOER in time polynomial in $\log p$. For $p \not\equiv 1 \pmod{8}$, this is already unconditional in [22, Propositions 1 and 3]. Suppose therefore that $p \equiv 1 \pmod{8}$. Set $\chi_1 = \chi_{-4}$ and $\chi_2 = \chi_p$. For an odd prime $q \neq p$, the desired conditions are

$$q \equiv 3 \pmod{4}, \quad (p/q) = -1. \quad (151)$$

The three characters $\chi_1, \chi_2, \chi_1\chi_2$ are nonprincipal. Apply (4) to them, together with its principal-character version. The indicator of their simultaneous values $(-1, -1)$ is $\frac{1}{4}(1 - \chi_1)(1 - \chi_2)$ on integers coprime to $4p$. Consequently

$$\sum_{\substack{n \leq x, \\ \chi_1(n) = \chi_2(n) = -1}} \Lambda(n)(1 - n/x) = \frac{x}{8} + O(x^{7/8} \log(3p) + \log(3p) \log(2x) + x^{7/8} \log^2(2x)).$$

The contribution of prime powers of exponent at least two is $O(\sqrt{x} \log^2(2x))$. Choosing $x = C \log^8(3p)$ with a sufficiently large effective absolute C therefore proves the existence of a prime satisfying (151) and $q \leq C \log^8(3p)$. The finitely many small p are absorbed effectively, as in Lemma 1.6. Testing successive primes and Legendre symbols finds such a q in deterministic polynomial time in $\log p$.

We spell out why this weaker auxiliary-prime bound suffices for the special-curve construction of [22, Proposition 3]. Put $K = \mathbb{Q}(\sqrt{-q})$ and $R = \mathcal{O}_K$. Quadratic reciprocity gives $(-q/p) = -1$, so p is inert in K . Compute the Hilbert class polynomial H_{-q} by the classical complex CM algorithm. This is an unconditional computation in time polynomial in q : reduced forms can be enumerated in polynomial time, the degree is at most q , and the coefficient heights and the required precision are polynomially bounded in q . In particular, this cost is polynomial in $\log p$. CM reduction shows that its roots modulo p are supersingular and lie in $\mathbb{F}_{p^2}$. Genus theory gives $h(-q)$ odd, since $-q$ has just one prime discriminant. Frobenius acts on the roots, counted with multiplicity, in orbits of sizes one or two; there is therefore a root $j_0 \in \mathbb{F}_p$. This argument does not require the reductions of distinct complex singular moduli to remain distinct. Find such a root by finite-field polynomial factorization, and choose a curve $E_0/\mathbb{F}_p$ with invariant j_0 .

The geometric endomorphism ring of E_0 contains an element α with $\alpha^2 = [-q]$. We can find it as follows. Enumerate the $q + 1$ cyclic subgroups of $E_0[q]$, form their quotients by Vélú’s formulas, and, whenever the quotient is isomorphic to E_0 , enumerate the isomorphisms and test the identity $\alpha^2 = [-q]$. Every degree- q isogeny is separable and has such a kernel because $q \neq p$. Thus the

CM endomorphism occurs in this list. The torsion and the required isomorphisms are defined over extensions of degree polynomial in q (one may use the bound $\#\mathrm{GL}_2(\mathbb{F}_q)$ for the torsion and a further factor at most six). Rational maps of degree q and their compositions can be computed and compared in time polynomial in q and $\log p$. This gives α with the claimed running time.

Write π for the p -power Frobenius of E_0 . Since E_0 is supersingular over $\mathbb{F}_p$ and $p > 3$, $\pi^2 = [-p]$. Put $t = \mathrm{tr}(\alpha\pi)$. Both $\alpha\pi$ and its dual are inseparable, so their sum $[t]$ has zero differential and $p \mid t$. Moreover $\alpha\pi + \pi\alpha = [t]$. If $p > 4q$, the degree–trace inequality $|t| \leq 2\sqrt{pq} < p$ gives $t = 0$ immediately. If $p \leq 4q$, compute

$$t = 1 + pq - \deg(1 - \alpha\pi)$$

by rational-map arithmetic: the maps involved have degree $O(q^2)$, so this computation is polynomial in q and $\log p$. The quadratic fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\pi)$ are distinct because p and q are distinct primes. Hence α and π do not commute, and the strict degree–trace inequality gives $\delta := 4pq - t^2 > 0$. Consequently

$$S = \mathbb{Z}\langle 1, \alpha, \pi, \alpha\pi \rangle \subset \mathrm{End}(E_0)$$

is an order of discriminant δ^2 . The endomorphism ring is maximal, of discriminant p^2 , so its index over S is exactly

$$m = \frac{\delta}{p} = 4q - \frac{t^2}{p}, \quad 1 \leq m \leq 4q.$$

Since $p \mid t$ and $q \neq p$, we have $m \equiv 4q \pmod{p}$, and therefore $p \nmid m$. In particular,

$$S \subset \mathrm{End}(E_0) \subset m^{-1}S.$$

Enumerate the m^4 residue classes in $m^{-1}S/S$. For a representative γ/m , test whether γ kills $E_0[m]$. Since $p \nmid m$, this is equivalent to γ/m being an endomorphism. The same polynomial-degree torsion construction makes all these tests effective in time polynomial in q and $\log p$. Equivalently one can use the unconditional `ISOGENYDIVISION` algorithm of [21, Proposition 3]. Hermite normal form applied to the accepted representatives and S now gives a basis of the full endomorphism ring and its explicit quaternionic isomorphism. If a Hilbert-symbol presentation is desired, the elements α and $j' = 2q\pi + t\alpha$ satisfy

$$\alpha^2 = -q, \quad (j')^2 = -q\delta, \quad \alpha j' = -j' \alpha.$$

The unconditional `ISOGENYDIVISION` algorithm [21, Proposition 3] supplies efficient evaluators for the accepted fractions. Here division can also be implemented by lifting an evaluation point under $[m]$ and evaluating γ ; the result is independent of the lift and all necessary field degrees are polynomial in q . This proves the required special-curve construction.

We now follow the reduction in [21, Section 7.3]. Given the input curve E , choose a squarefree product N of successive primes at least 17, omitting p , until $N \geq p^8$, and take a random N -isogeny walk $\eta : E \rightarrow E'$. The prime number theorem shows that the largest prime used is $O(\log p)$, while $\log N = O(\log p)$. The normalized ℓ -walk operators have nonconstant eigenvalues of absolute value at most $2\sqrt{\ell}/(\ell + 1)$; this is the unconditional Ramanujan estimate, with stationary weights μ_p . For $\ell \geq 17$, this bound is at most $\ell^{-1/4}$. The weighted Cauchy–Schwarz inequality therefore bounds the total variation distance from μ_p after this walk by $\sqrt{p} N^{-1/4} \leq p^{-3/2} < p^{-1}$. This also gives a direct quantitative version of the source’s Proposition 5 and Corollary 1. The walk and its dual have efficient representations of polynomial length.

Query the average-case oracle on E' and let O' be a valid answer. The unconditional change-of-quaternion-model algorithm [21, Proposition 1] puts O' in the algebra containing the known order

$O_0 = \text{End}(E_0)$. Compute a connecting left O_0 -ideal I with right order O' , and scale it by a rational integer so that $I \subseteq O_0$. This is the unconditional lattice computation used in [21, Section 7.3], citing Kirschmer–Voight’s Algorithm 3.5. The unconditional IDEALTOISOGENY algorithm [21, Proposition 4] computes the associated isogeny $\psi : E_0 \rightarrow F$, and identifies the right order with $\text{End}(F)$. This algorithm allows arbitrary ideal norm; no powersmooth-ideal theorem is being invoked.

For completeness, the dictionary is transported explicitly as follows. Put $m = \deg \psi = \text{Nrd}(I)$. The inclusion $mO_0 \subseteq I$ and the identity $IO' \subseteq I$ imply $m\beta \in O_0$ for every $\beta \in O'$. Writing $\beta = \gamma/m$ with $\gamma \in O_0$, its corresponding endomorphism is

$$\frac{\psi \gamma \hat{\psi}}{m^2}.$$

Unconditional isogeny division computes these maps from a basis of O' . The Deuring correspondence says that isomorphic maximal orders correspond to supersingular curves up to Frobenius conjugation. Thus F is isomorphic to E' or to $(E')^{(p)}$. An isomorphism, and if necessary the Frobenius isogeny, transports the dictionary to E' ; division by p in the latter case is again covered by isogeny division. In particular, all four generators of $\text{End}(E')$ are now efficiently represented.

Finally recover the kernel ideal of $\hat{\eta} : E' \rightarrow E$. For each prime $\ell \mid N$, find its one-dimensional kernel inside $E'[\ell]$. Evaluating the known endomorphism basis on a generator of this kernel gives two linear equations modulo ℓ ; their solutions give precisely the ideal of endomorphisms killing the kernel. Coordinates in $E'[\ell]$ can be found by exhaustive search since $\ell = O(\log p)$. Intersect these ideals over $\ell \mid N$. Since N is squarefree, the intersection is exactly the kernel ideal of $\hat{\eta}$. Its right order and the same transport formula, applied once to $\hat{\eta}$, produce a solution of MOER for E . Computing the entire kernel ideal before transport avoids any growth from repeatedly rebuilding evaluation representations. Integer lattice operations, torsion computations, and the two isogeny-division steps have polynomial input and output lengths. This proves the stated reduction. $\square$

Combining Theorem 55.1 with the unconditional worst-case equivalences in [21, Theorem 1] removes the second exceptional case in their Theorem 2: the target may now be **MaxOrder**, or its prescribed-model variant **MaxOrder_Q**, for every p . As in the source, reductions involving the latter variant retain oracle access to the model-selection algorithm Q . The remaining exception, where the source problem is ℓ -**IsogenyPath**, is not removed by this argument: it prescribes a prime-power isogeny degree.

References

- [1] P. Castel, *Solving quadratic equations in dimension 5 or more without factoring*, The Open Book Series **1** (2013), 213–233. DOI:10.2140/obs.2013.1.213. Publisher full text.
- [2] P. Kutas, *Splitting quaternion algebras over quadratic number fields*, Journal of Symbolic Computation **94** (2019), 173–182. DOI:10.1016/j.jsc.2018.08.002. Accepted author manuscript.
- [3] L. M. Adleman, D. R. Estes and K. S. McCurley, *Solving bivariate quadratic congruences in random polynomial time*, Mathematics of Computation **48** (1987), no. 177, 17–28. DOI:10.1090/S0025-5718-1987-0866095-8.
- [4] D. Simon, *Solving quadratic equations using reduced unimodular quadratic forms*, Mathematics of Computation **74** (2005), no. 251, 1531–1543. DOI:10.1090/S0025-5718-05-01729-1.

- [5] D. Simon, *Quadratic equations in dimensions 4, 5 and more*, preprint, 4 July 2006. [Author's full text](#).
- [6] W. Bosma and P. Stevenhagen, *On the computation of quadratic 2-class groups*, *Journal de Théorie des Nombres de Bordeaux* **8** (1996), no. 2, 283–313; erratum, **9** (1997), no. 1, 249 (reference numbering). [Full text](#); [erratum](#).
- [7] A. Granville and K. Soundararajan, The distribution of values of $L(1, \chi_d)$, *Geom. Funct. Anal.* **13** (2003), 992–1028. [doi:10.1007/s00039-003-0438-3](#); [author's version](#).
- [8] A. Granville and K. Soundararajan, Errata to: The distribution of values of $L(1, \chi_d)$, *Geom. Funct. Anal.* **14** (2004), 245–246. [doi:10.1007/s00039-004-0456-9](#); [published errata](#).
- [9] P. Darbar and G. Maiti, Large values of quadratic Dirichlet L -functions, *Math. Ann.* **392** (2025), 4573–4605. [doi:10.1007/s00208-025-03187-6](#); [author's version](#).
- [10] P. Darbar, C. David, M. Lalín, and A. Lumley, Asymmetric distribution of extreme values of cubic L -functions at $s = 1$, *J. London Math. Soc.* **110** (2024), no. 4, e12996, 61 pp. [doi:10.1112/jlms.12996](#); [published version](#).
- [11] Y. Lamzouri, On the average of the number of imaginary quadratic fields with a given class number, *Ramanujan J.* **44** (2017), 411–416. [doi:10.1007/s11139-017-9910-9](#); [author's version](#).
- [12] Y. Lamzouri, The number of imaginary quadratic fields with prime discriminant and class number up to H , *Q. J. Math.* **68** (2017), 1379–1393. [doi:10.1093/qmath/hax026](#); [author's version](#).
- [13] G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.* **13** (1976), 300–317. [doi:10.1016/S0022-0000\(76\)80043-8](#); [author-hosted published scan](#).
- [14] M. Agrawal, N. Kayal, and N. Saxena, PRIMES is in P, *Ann. of Math. (2)* **160** (2004), 781–793. [doi:10.4007/annals.2004.160.781](#).
- [15] F. Morain, G. Renault, and B. Smith, Deterministic factoring with oracles, *Appl. Algebra Engrg. Comm. Comput.* **34** (2023), 663–690. [doi:10.1007/s00200-021-00521-8](#).
- [16] A. Dąbrowski, J. Pomykała, and I. E. Shparlinski, On oracle factoring of integers, *J. Complexity* **76** (2023), article 101741. [doi:10.1016/j.jco.2023.101741](#).
- [17] N. Gupta, A. Sikarov, and I. Volkovich, A computational perspective on Carmichael numbers, *ECCC Report TR26-212* (2026), preprint. [primary preprint](#).
- [18] J. Hoffstein and P. Lockhart, Coefficients of Maass forms and the Siegel zero, *Ann. of Math. (2)* **140** (1994), 161–176. [doi:10.2307/2118543](#).
- [19] D. Goldfeld, J. Hoffstein, and D. Lieman, Appendix: An effective zero-free region, *Ann. of Math. (2)* **140** (1994), 177–181. [doi:10.2307/2118544](#).
- [20] O. Klurman, A. P. Mangerel, and J. Teräväinen, Multiplicative functions in short arithmetic progressions, *Proc. London Math. Soc. (3)* **127** (2023), 366–446. [doi:10.1112/plms.12546](#); [published open-access copy](#).

- [21] A. Herlédan Le Merdy and B. Wesolowski, Unconditional foundations for supersingular isogeny-based cryptography, *Theory of Cryptography–TCC 2025*, LNCS **16270** (2026), 266–297; first online 3 December 2025. [doi:10.1007/978-3-032-12296-4_9](https://doi.org/10.1007/978-3-032-12296-4_9); [author’s minor revision, version 2, 2 February 2026](#).
- [22] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit, Supersingular isogeny graphs and endomorphism rings: reductions and solutions, *EUROCRYPT 2018*, LNCS **10822**, 329–368. [doi:10.1007/978-3-319-78372-7_11](https://doi.org/10.1007/978-3-319-78372-7_11).
- [23] B. Wesolowski, The supersingular isogeny path and endomorphism ring problems are equivalent, *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, 1100–1111. [doi:10.1109/FOCS52979.2021.00109](https://doi.org/10.1109/FOCS52979.2021.00109); [full version](#).
- [24] F. Balestrieri, A. Johnson, and R. Newton, Explicit uniform bounds for Brauer groups of singular K3 surfaces, *Ann. Inst. Fourier* **73** (2023), 567–607. [doi:10.5802/aif.3526](https://doi.org/10.5802/aif.3526).
- [25] É. Gaudron and G. Rémond, Nouveaux théorèmes d’isogénie, *Mém. Soc. Math. France (N.S.)* **176** (2023), 1–123. [doi:10.24033/msmf.484](https://doi.org/10.24033/msmf.484).
- [26] A. Kresch and Y. Tschinkel, Effectivity of Brauer–Manin obstructions on surfaces, *Adv. Math.* **226** (2011), 4131–4144. [doi:10.1016/j.aim.2010.11.012](https://doi.org/10.1016/j.aim.2010.11.012).
- [27] B. Poonen, D. Testa, and R. van Luijk, Computing Néron–Severi groups and cycle class groups, *Compos. Math.* **151** (2015), 713–734. [doi:10.1112/S0010437X14007878](https://doi.org/10.1112/S0010437X14007878).
- [28] J. Thorner and A. Zaman, A unified and improved Chebotarev density theorem, *Algebra Number Theory* **13** (2019), 1039–1068. [doi:10.2140/ant.2019.13.1039](https://doi.org/10.2140/ant.2019.13.1039).
- [29] G. Ivanyos, M. Karpinski, L. Rónyai, and N. Saxena, Trading GRH for algebra: algorithms for factoring polynomials and related structures, *Math. Comp.* **81** (2012), 493–531. [doi:10.1090/S0025-5718-2011-02505-6](https://doi.org/10.1090/S0025-5718-2011-02505-6); [published author copy](#).
- [30] I. Khayutin, Joint equidistribution of CM points, *Ann. of Math. (2)* **189** (2019), 145–276. [doi:10.4007/annals.2019.189.1.4](https://doi.org/10.4007/annals.2019.189.1.4).
- [31] P. Habegger, Weakly bounded height on modular curves, *Acta Math. Vietnam.* **35** (2010), no. 1, 43–69. [Published paper](#).
- [32] B. Edixhoven and R. Richard, A mod p variant of the André–Oort conjecture, *Rend. Circ. Mat. Palermo (2)* **69** (2020), 151–157. [doi:10.1007/s12215-018-00392-y](https://doi.org/10.1007/s12215-018-00392-y).
- [33] N. Balaji, S. Perifel, M. Shirmohammadi, and J. Worrell, Cyclotomic identity testing and applications, *Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation (ISSAC ’21)* (2021), 35–42. [doi:10.1145/3452143.3465530](https://doi.org/10.1145/3452143.3465530).
- [34] N. Balaji, K. Nosan, M. Shirmohammadi, and J. Worrell, Identity testing for radical expressions, *Proceedings of the 37th ACM/IEEE Symposium on Logic in Computer Science (LICS ’22)* (2022), article 8, 1–11. [doi:10.1145/3531130.3533331](https://doi.org/10.1145/3531130.3533331).
- [35] C. Rasmussen and A. Tamagawa, Arithmetic of abelian varieties with constrained torsion, *Trans. Amer. Math. Soc.* **369** (2017), no. 4, 2395–2424. [doi:10.1090/tran/6790](https://doi.org/10.1090/tran/6790).
- [36] P. Pollack and P. Schorn, Dirichlet’s proof of the three-square theorem: An algorithmic perspective, *Math. Comp.* **88** (2019), no. 316, 1007–1019. [doi:10.1090/mcom/3349](https://doi.org/10.1090/mcom/3349).

- [37] P. Hough, A lower bound for biases amongst products of two primes, *Res. Number Theory* **3** (2017), article 19. [doi:10.1007/s40993-017-0083-9](https://doi.org/10.1007/s40993-017-0083-9).
- [38] R. C. Daileda, Non-abelian number fields with very large class numbers, *Acta Arith.* **125** (2006), 215–255. [doi:10.4064/aa125-3-2](https://doi.org/10.4064/aa125-3-2).
- [39] B. S. Banwait, Explicit isogenies of prime degree over quadratic fields, *Int. Math. Res. Not.* **2023**, no. 14, 11829–11876. [doi:10.1093/imrn/rnac134](https://doi.org/10.1093/imrn/rnac134).
- [40] B. S. Banwait and M. Derickx, Explicit isogenies of prime degree over number fields, *Algebra Number Theory* **19** (2025), no. 6, 1147–1197. [doi:10.2140/ant.2025.19.1147](https://doi.org/10.2140/ant.2025.19.1147).
- [41] S. Gao, On the deterministic complexity of factoring polynomials, *J. Symbolic Comput.* **31** (2001), 19–36. [doi:10.1006/jsco.1999.1001](https://doi.org/10.1006/jsco.1999.1001).
- [42] L. Rónyai, Factoring polynomials over finite fields, *J. Algorithms* **9** (1988), 391–400. [doi:10.1016/0196-6774\(88\)90029-6](https://doi.org/10.1016/0196-6774(88)90029-6).
- [43] P. Pollack, The smallest inert prime in a cyclic number field of prime degree, *Math. Res. Lett.* **20** (2013), 163–179. [doi:10.4310/MRL.2013.v20.n1.a13](https://doi.org/10.4310/MRL.2013.v20.n1.a13); [Author’s copy](#).
- [44] J.-H. Ahn and S.-H. Kwon, The class groups of the imaginary Abelian number fields with Galois group $(\mathbb{Z}/2\mathbb{Z})^n$, *Bull. Austral. Math. Soc.* **70** (2004), 267–277. [doi:10.1017/S0004972700034481](https://doi.org/10.1017/S0004972700034481).
- [45] G. Binyamini, Point counting for foliations over number fields, *Forum Math. Pi* **10** (2022), e6, 1–39. [doi:10.1017/fmp.2021.20](https://doi.org/10.1017/fmp.2021.20).
- [46] P. Habegger, Weakly bounded height on modular curves, *Acta Math. Vietnam.* **35** (2010), 43–69. [Published paper](#).
- [47] F. Campagna, Effective bounds on differences of singular moduli that are S -units, *Math. Proc. Cambridge Philos. Soc.* **174** (2023), 415–450. [doi:10.1017/S0305004122000378](https://doi.org/10.1017/S0305004122000378); [Author preprint](#).
- [48] F. Campagna, On singular moduli that are S -units, *Manuscripta Math.* **166** (2021), 73–90. [doi:10.1007/s00229-020-01230-1](https://doi.org/10.1007/s00229-020-01230-1).
- [49] A. Granville and K. Soundararajan, Large character sums, *J. Amer. Math. Soc.* **14** (2001), 365–397. [doi:10.1090/S0894-0347-00-00357-X](https://doi.org/10.1090/S0894-0347-00-00357-X); [Author’s copy](#).
- [50] A. Granville, A. J. Harper, and K. Soundararajan, A new proof of Halász’s theorem, and its consequences, *Compos. Math.* **155** (2019), 126–163. [doi:10.1112/S0010437X18007522](https://doi.org/10.1112/S0010437X18007522); [Author preprint](#).
- [51] G. Binyamini, with an appendix by E. Kowalski, Some effective estimates for André–Oort in $Y(1)^n$, *J. Reine Angew. Math.* **767** (2020), 17–35. [doi:10.1515/crelle-2019-0028](https://doi.org/10.1515/crelle-2019-0028); [Author preprint](#).
- [52] B. Kane, Representations of integers by ternary quadratic forms, *Int. J. Number Theory* **6** (2010), 127–158. [doi:10.1142/S1793042110002831](https://doi.org/10.1142/S1793042110002831).
- [53] W. Duke and R. Schulze-Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids, *Invent. Math.* **99** (1990), 49–57. [doi:10.1007/BF01234411](https://doi.org/10.1007/BF01234411); [Author’s copy](#).

- [54] W. Duke, On ternary quadratic forms, *J. Number Theory* **110** (2005), 37–43. [doi:10.1016/j.jnt.2004.06.013](https://doi.org/10.1016/j.jnt.2004.06.013); [Author’s copy](#).
- [55] R. Schulze-Pillot, Darstellungsmaße von Spinorgeschlechtern ternärer quadratischer Formen, *J. Reine Angew. Math.* **352** (1984), 114–132. [Original published paper](#).
- [56] B. Kane, CM liftings of supersingular elliptic curves, *J. Théor. Nombres Bordeaux* **21** (2009), 635–663. [doi:10.5802/jtnb.692](https://doi.org/10.5802/jtnb.692).
- [57] N. D. Elkies, K. Ono, and T. Yang, Reduction of CM elliptic curves and modular function congruences, *Int. Math. Res. Not.* **2005** (2005), no. 44, 2695–2707. [Author preprint](#).
- [58] OpenAI, *The Quasi-Riemann Hypothesis: A Zero-Free Half-Plane $\Re s > 7/8$* , 30 September 2026, Theorem 1.1. [Official manuscript and source](#).
- [59] OpenAI, *The Quasi-Riemann Hypothesis*, 5 October 2026, companion proof of the 11/12 boundary. [Official manuscript and source](#).
- [60] H. Davenport, *Multiplicative Number Theory*, 3rd ed., revised by H. L. Montgomery, Springer, 2000.
- [61] J. E. Littlewood, On the class-number of the corpus $P(\sqrt{-k})$, *Proc. London Math. Soc.* (2) **27** (1928), 358–372.
- [62] J. B. Friedlander and H. Iwaniec, A note on Dirichlet L -functions, *Exposition. Math.* **36** (2018), 343–350. [doi:10.1016/j.exmath.2018.06.003](https://doi.org/10.1016/j.exmath.2018.06.003); [author preprint](#).
- [63] E. Jeřábek, Integer factoring and modular square roots, *J. Comput. Syst. Sci.* **82** (2016), 380–394. [doi:10.1016/j.jcss.2015.08.001](https://doi.org/10.1016/j.jcss.2015.08.001).
- [64] L. Adleman, K. Manders, and G. Miller, On taking roots in finite fields, *18th Annual Symposium on Foundations of Computer Science* (1977), 175–178. [Original paper](#).
- [65] J. D. Achter and E. W. Howe, Split abelian surfaces over finite fields and reductions of genus-2 curves, *Algebra Number Theory* **11** (2017), 39–76. [doi:10.2140/ant.2017.11.39](https://doi.org/10.2140/ant.2017.11.39).
- [66] V. Arul, J. Booher, S. R. Groen, E. W. Howe, W. Li, V. Matei, R. Pries, and C. Springer, Doubly isogenous genus-2 curves with D_4 -action, *Math. Comp.* **93** (2024), 347–381. [doi:10.1090/mcom/3891](https://doi.org/10.1090/mcom/3891).
- [67] R. Schoof, Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46** (1987), 183–211.
- [68] A. Granville and K. Soundararajan, Large character sums: pretentious characters and the Pólya–Vinogradov theorem, *J. Amer. Math. Soc.* **20** (2007), 357–384. [doi:10.1090/S0894-0347-06-00536-4](https://doi.org/10.1090/S0894-0347-06-00536-4).
- [69] H. L. Montgomery and R. C. Vaughan, Exponential sums with multiplicative coefficients, *Invent. Math.* **43** (1977), 69–82. [doi:10.1007/BF01390204](https://doi.org/10.1007/BF01390204).
- [70] D. W. Boyd and H. Kisilevsky, On the exponent of the ideal class groups of complex quadratic fields, *Proc. Amer. Math. Soc.* **31** (1972), 433–436. [doi:10.1090/S0002-9939-1972-0289454-4](https://doi.org/10.1090/S0002-9939-1972-0289454-4).

- [71] A.-S. Elsenhans, J. Klüners, and F. Nicolae, Imaginary quadratic number fields with class groups of small exponent, *Acta Arith.* **193** (2020), 217–233. [doi:10.4064/aa180220-20-3](https://doi.org/10.4064/aa180220-20-3); [author preprint](#).
- [72] A.-S. Elsenhans, J. Klüners, and F. Nicolae, *Imaginary quadratic fields with small exponent*, author-maintained tables, accessed 9 October 2026. [Complete tables](#).
- [73] E. Kani, Idoneal numbers and some generalizations, *Ann. Sci. Math. Québec* **35** (2011), 197–227. [Published paper](#).
- [74] A. Bourdon and P. Pollack, Torsion subgroups of CM elliptic curves over odd degree number fields, *Int. Math. Res. Not.* 2017 (2017), no. 16, 4923–4961. [doi:10.1093/imrn/rnw163](https://doi.org/10.1093/imrn/rnw163); [author preprint](#).
- [75] P. T. Joshi, The size of $L(1, \chi)$ for real nonprincipal residue characters χ with prime modulus, *J. Number Theory* **2** (1970), 58–73.
- [76] M. Schütt, CM newforms with rational coefficients, *Ramanujan J.* **19** (2009), 187–205. [doi:10.1007/s11139-008-9147-8](https://doi.org/10.1007/s11139-008-9147-8); [author preprint](#).
- [77] H. Pasten, Shimura curves and the abc conjecture, *J. Number Theory* **254** (2024), 214–335. [doi:10.1016/j.jnt.2023.07.002](https://doi.org/10.1016/j.jnt.2023.07.002); [author manuscript](#).
- [78] N. D. Elkies and M. Schütt, Modular forms and K3 surfaces, *Adv. Math.* **240** (2013), 106–131. [doi:10.1016/j.aim.2013.03.008](https://doi.org/10.1016/j.aim.2013.03.008); [author preprint](#).
- [79] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves, *Collect. Math.* **67** (2016), 21–54. [doi:10.1007/s13348-015-0148-9](https://doi.org/10.1007/s13348-015-0148-9).
- [80] X. Wei, Smallness of Faltings heights of CM abelian varieties, *J. Number Theory* **242** (2023), 73–101. [doi:10.1016/j.jnt.2022.07.007](https://doi.org/10.1016/j.jnt.2022.07.007).
- [81] X. Wei, *Smallness of Faltings heights of CM abelian varieties*, arXiv:2111.00617v1 (2021). [Preprint with the numbering used in the proof](#).
- [82] H. M. Stark, Some effective cases of the Brauer–Siegel theorem, *Invent. Math.* **23** (1974), 135–152. [doi:10.1007/BF01405166](https://doi.org/10.1007/BF01405166).
- [83] K.-Y. Chang and S.-H. Kwon, The imaginary abelian number fields with class numbers equal to their genus class numbers, *J. Théor. Nombres Bordeaux* **12** (2000), 349–365. [doi:10.5802/jtnb.283](https://doi.org/10.5802/jtnb.283).
- [84] I. Miyada, On imaginary abelian number fields of type $(2, 2, \dots, 2)$ with one class in each genus, *Manuscripta Math.* **88** (1995), 535–540. [doi:10.1007/BF02567840](https://doi.org/10.1007/BF02567840).
- [85] S. Louboutin, The exponent three class group problem for some real cyclic cubic number fields, *Proc. Amer. Math. Soc.* **130** (2002), 353–361. [doi:10.1090/S0002-9939-01-06168-8](https://doi.org/10.1090/S0002-9939-01-06168-8).
- [86] F. Lemmermeyer and A. Pethő, Simplest cubic fields, *Manuscripta Math.* **88** (1995), 53–58. [doi:10.1007/BF02567804](https://doi.org/10.1007/BF02567804); [author preprint](#).
- [87] S. Louboutin and M. F. Newman, On the diophantine equation $xy + yz + zx = d$, *Acta Math. Inform. Univ. Ostraviensis* **6** (1998), 155–158. [Published paper](#).

- [88] J. S. Ellenberg and A. Venkatesh, Reflection principles and bounds for class group torsion, *Int. Math. Res. Not.* 2007 (2007), article rnm002, 18 pp. [doi:10.1093/imrn/rnm002](https://doi.org/10.1093/imrn/rnm002).
- [89] D. R. Heath-Brown, ℓ -Torsion in class groups via Dirichlet L -functions, *Int. J. Number Theory* (2026). [doi:10.1142/S17930442126500168](https://doi.org/10.1142/S17930442126500168); [Author version](#).
- [90] S. Chan and P. Koymans, A new pointwise bound for 3-torsion of class groups, [arXiv:2505.00611](https://arxiv.org/abs/2505.00611) (2025). Prior-art comparison only. [Author preprint](#).
- [91] R. J. Lemke Oliver and A. Zaman, Improving the trivial bound for ℓ -torsion in class groups, [arXiv:2502.03464](https://arxiv.org/abs/2502.03464) (2025). Prior-art comparison only. [Author preprint](#).
- [92] M. N. Walsh, Stability under scaling in the local phases of multiplicative functions, *Invent. Math.* **241** (2025), 325–362. [doi:10.1007/s00222-025-01343-y](https://doi.org/10.1007/s00222-025-01343-y); [author-linked full version](#).
- [93] K. Matomäki, M. Radziwiłł, and T. Tao, Fourier uniformity of bounded multiplicative functions in short intervals on average, *Invent. Math.* **220** (2020), 1–58. [doi:10.1007/s00222-019-00926-w](https://doi.org/10.1007/s00222-019-00926-w).
- [94] R. A. Mollin, Class number two for real quadratic fields of Richaud–Dégert type, *Serdica Math. J.* **35** (2009), 287–300. [Published paper](#).
- [95] T. Tatzuza, On a theorem of Siegel, *Japanese J. Math.* **21** (1951), 163–178. [doi:10.4099/jjm1924.21.0_163](https://doi.org/10.4099/jjm1924.21.0_163).
- [96] S. R. Louboutin, Ideal class groups of some quadratic number fields and factorization of values of some quadratic polynomials, *Czechoslovak Math. J.* **76** (2026), 677–697. [Publisher record](#); [author version](#).
- [97] A. P. Mangerel, On a rigidity property for quadratic Gauss sums, *Mathematika* **72** (2026), no. 1, e70061, 30 pp. [doi:10.1112/mtk.70061](https://doi.org/10.1112/mtk.70061).
- [98] A. Granville and K. Soundararajan, The spectrum of multiplicative functions, *Ann. of Math.* (2) **153** (2001), 407–470. [doi:10.2307/2661346](https://doi.org/10.2307/2661346).
- [99] E. Sofos, Statistics of small prime quadratic non-residues, *Rend. Semin. Mat. Univ. Politec. Torino* **80** (2022), no. 1, 73–85. [Published paper](#).
- [100] R. Mrazović, A random model for the Paley graph, *Q. J. Math.* **68** (2017), 193–206. [doi:10.1093/qmath/haw037](https://doi.org/10.1093/qmath/haw037).
- [101] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics **227**, Springer, 1971.
- [102] S. Louboutin, Prime producing quadratic polynomials and class-numbers of real quadratic fields, *Canad. J. Math.* **42** (1990), no. 2, 315–341. [doi:10.4153/CJM-1990-018-3](https://doi.org/10.4153/CJM-1990-018-3).
- [103] A. Biró and K. Lapkova, The class number one problem for the real quadratic fields $\mathbb{Q}(\sqrt{(an)^2 + 4a})$, *Acta Arith.* **172** (2016), no. 2, 117–131. [doi:10.4064/aa7957-12-2015](https://doi.org/10.4064/aa7957-12-2015).
- [104] J. Lee, The complete determination of wide Richaud–Dégert types which are not 5 modulo 8 with class number one, *Acta Arith.* **140** (2009), no. 1, 1–29. [doi:10.4064/aa140-1-1](https://doi.org/10.4064/aa140-1-1).

- [105] M. Mourtada and V. Kumar Murty, Omega theorems for $\frac{L'}{L}(1, \chi_D)$, *Int. J. Number Theory* **9** (2013), no. 3, 561–581. [doi:10.1142/S1793042112501485](https://doi.org/10.1142/S1793042112501485).
- [106] M. Mourtada, *The distribution of values of logarithmic derivatives of real L-functions*, Ph.D. thesis, University of Toronto, 2013, Chapter 4, especially Theorem 17. [Author’s full thesis](#).
- [107] A. I. Badzyan, The Euler–Kronecker constant, *Math. Notes* **87** (2010), 31–42; Russian original, *Mat. Zametki* **87** (2010), 35–47. [English publication](#); [Russian original](#).
- [108] K. Ford, F. Luca, and P. Moree, Values of the Euler φ -function not divisible by a given odd prime, and the distribution of Euler–Kronecker constants for cyclotomic fields, *Math. Comp.* **83** (2014), 1447–1476. [doi:10.1090/S0025-5718-2013-02749-4](https://doi.org/10.1090/S0025-5718-2013-02749-4); [Revised author version, with the numbering used here](#).
- [109] P. L. Clark, T. Genao, P. Pollack, and F. Saia, The least degree of a CM point on a modular curve, *J. London Math. Soc.* (2) **105** (2022), 825–883. [doi:10.1112/jlms.12518](https://doi.org/10.1112/jlms.12518); [Author errata](#), 4 May 2026.
- [110] B. Green and T. Tao, The Möbius function is strongly orthogonal to nilsequences, *Ann. of Math.* (2) **175** (2012), 541–566. [doi:10.4007/annals.2012.175.2.3](https://doi.org/10.4007/annals.2012.175.2.3).
- [111] B. Green and T. Tao, The quantitative behaviour of polynomial orbits on nilmanifolds, *Ann. of Math.* (2) **175** (2012), 465–540. [doi:10.4007/annals.2012.175.2.2](https://doi.org/10.4007/annals.2012.175.2.2); correction, *Ann. of Math.* (2) **179** (2014), 1175–1183, [doi:10.4007/annals.2014.179.3.8](https://doi.org/10.4007/annals.2014.179.3.8).