hexagon:2611.00895v1

Small roots of split quadratic congruences and fundamental units in a quartic family

Brice Pouly*

Abstract

We study two questions about square classes associated with the forms n, $n+1$, $3n+1$ and $3n+2$. For the least positive integer $k \neq 3$ for which $(kn+1)/(3n+1)$ is a rational square, we prove $\log(n^2/K_*(n)) = 2(\log 2)\omega(n) + O(\log\log\log n)$ on a set of natural density one. The proof combines an exact second moment for dilated congruence roots with a weighted sieve that includes every rational denominator. The same estimates give $\log(n/(r_n+2)) = (\log 2)\omega(n) + O(\log\log\log n)$ on a density-one set for the least nonnegative root of $(r+1)(r+3) \equiv 0 \pmod{n}$. This establishes its normal-order exponent $\log 2$ predicted by Crişan and Pollack for this polynomial. Both Gaussian limit laws follow from Erdős–Kac. Second, write $D(n) = n(n+1)(3n+1)(3n+2) = d_n s_n^2$ with d_n squarefree. The unit $9n(n+1)+1+3s_n\sqrt{d_n}$ is fundamental in the full ring of integers of $\mathbb{Q}(\sqrt{d_n})$ except for at most $\exp(O((\log X)^{2/3}))$ indices $n \leq X$; there are at least a constant multiple of $\log X$ exceptions. The upper bound specializes Alpöge's integral-point descent using the splitting fields of a Chebyshev family. A final change of index retains the Liouville sign in a series over fundamental regulators. It transports local holomorphic continuation at $s=1$ equivalently between the two signed series, yielding a conditional cancellation criterion.

Contents

1 Two questions about square classes **2**

Part I. Small roots and square copies **5**

2 Small representatives of a square class **5**

Part II. Fundamental units and regulators **12**

3 A quartic family of quadratic units **12**

4 Uniform control of the exceptional powers **14**

5 An explicit Richaud–Degert sector **17**

6 A signed series over fundamental regulators **18**

A Computational checks and reproducibility **22**

AI assistance **22**

*Research and manuscript preparation with AI assistance. The computational appendix describes the checks and the use of AI.

1 Two questions about square classes

If two positive integers have a rational square as their quotient, every completely multiplicative function taking values in $\{-1, 1\}$ assigns them the same sign. This observation leads to a concrete size question. Given n, how small can an integer slope $k \neq 3$ be if $kn + 1$ is to have the same square class as $3n + 1$? There is always a quadratic-size choice:

$$(3n^2 + 7n + 5)n + 1 = (3n + 1)(n + 1)^2. \tag{1.1}$$

The first part of this article determines the logarithmic saving available for almost every n and the fluctuations of that saving.

The second question concerns the product

$$D(n) = n(n + 1)(3n + 1)(3n + 2), \qquad A_n = 9n(n + 1) + 1. \tag{1.2}$$

The identity

$$A_n^2 - 9D(n) = 1 \tag{1.3}$$

produces an explicit norm-one unit in the quadratic field defined by the squarefree part of $D(n)$. A solution of Pell's equation may be a large power of a smaller unit, so (1.3) alone does not identify the regulator. We show that this obstruction occurs on a set much smaller than any positive power of the parameter range.

The two parts use different counting arguments. Their common object is the square class of the indicated affine forms: the first varies one form to preserve its class, while the second encodes the class of their product by a unit. No cancellation estimate for the Liouville function is used in either argument.

1.1 The size of the first square copy

Let $\omega(n)$ count distinct prime divisors, and define

$$K_*(n) = \min\{k \in \mathbb{N} : k \geq 1,\ k \neq 3,\ (kn + 1)/(3n + 1) \in \mathbb{Q}^2\}. \tag{1.4}$$

Equation (1.1) makes this a finite minimum. Theorem 2.1 proves that, on a set of natural density one,

$$\log \frac{n^2}{K_*(n)} = 2(\log 2)\omega(n) + O(\log\log\log n). \tag{1.5}$$

All logarithms in this article are natural. In particular,

$$K_*(n) = \frac{n^2}{(\log n)^{2\log 2 + o(1)}}$$

on a density-one set. Corollary 2.2 combines (1.5) with the Erdős–Kac theorem to give

$$\frac{\log(n^2/K_*(n)) - 2(\log 2)\log\log N}{2(\log 2)\sqrt{\log\log N}} \implies \mathcal{N}(0, 1), \qquad n \text{ uniform on } \{1, \dots, N\}. \tag{1.6}$$

These are statements for natural counting measure. They assert neither a uniform bound for every modulus nor a limit law on arbitrarily chosen short or harmonic windows.

The factor $2\log 2$ has a local explanation. Each odd prime power dividing a modulus has two roots of $u^2 \equiv 1$. Thus a typical modulus has about $2^{\omega(n)}$ global candidates. A first useful root at scale $n/2^{\omega(n)}$ produces a slope at its squared scale. Making that reasoning valid requires two estimates. An exact second moment detects a small nontrivial root after averaging

over a rough cofactor; a weighted count rules out substantially smaller roots even when the square quotient has a denominator.

That last qualification matters already at $n = 5$:

$$\frac{7 \cdot 5 + 1}{3 \cdot 5 + 1} = \frac{36}{16} = \left(\frac{3}{2}\right)^2.$$

Here $K_*(5) = 7$, whereas requiring an integer square multiplier first gives $u = 4$ and $k = 51$. The upper bound can use integer square multipliers, but a lower bound for (1.4) must retain rational ones.

For the least nonnegative root

$$r_n = \min\{r \geq 0 : (r+1)(r+3) \equiv 0 \pmod{n}\},$$

the substitution $u = r + 2$ gives $u^2 \equiv 1 \pmod{n}$. Corollary 2.3 yields the more precise relation

$$\log \frac{n}{r_n + 2} = (\log 2)\omega(n) + O(\log\log\log n) \tag{1.7}$$

on a density-one set, and hence

$$r_n = \frac{n}{(\log n)^{\log 2 + o(1)}} \quad \text{on a set of natural density one.} \tag{1.8}$$

It also gives a Gaussian limit for $\log(n/(r_n + 2))$, with centring $(\log 2)\log\log N$ and scale $(\log 2)\sqrt{\log\log N}$ when n is uniform up to N. After their respective normalisations, the two statistics jointly converge to (G, G), where G is standard normal. Indeed, both differ from the same normalised $\omega(n)$ by a quantity tending to zero in probability. The polynomial is soluble for every modulus and has no nonnegative integer root; its two integer roots are -1 and -3.

1.2 Fundamental units in the full ring of integers

Write $D(n) = d_n s_n^2$, where $d_n > 1$ is squarefree and $s_n > 0$, and put

$$U_n = A_n + 3s_n\sqrt{d_n} = A_n + \sqrt{A_n^2 - 1}. \tag{1.9}$$

Theorem 1.1 (Exceptional nonfundamental units)**.** *Let $E(X)$ be the number of integers $1 \leq n \leq X$ for which U_n is not fundamental in $\mathcal{O}_{\mathbb{Q}(\sqrt{d_n})}$. There are absolute constants $c, C > 0$ such that, for $X \geq 3$,*

$$c\log(2X) \leq E(X) \leq \exp\bigl(C(\log X)^{2/3}\bigr). \tag{1.10}$$

Fundamental means the positive generator greater than one of the full unit group modulo $\{\pm 1\}$. It does not mean merely the smallest unit of norm $+1$, nor the generator of the order $\mathbb{Z}[U_n]$. In particular, the field at a nonexceptional index has no unit of norm -1, and its regulator is $\log U_n$.

Proper powers really occur. For example, $U_1 = 19 + 6\sqrt{10} = (3 + \sqrt{10})^2$. The square cases reduce to two fixed Pell equations. An odd prime exponent ℓ instead gives an integral point on

$$y^2 = 2D_\ell(x) + 5, \qquad D_\ell(v + v^{-1}) = v^\ell + v^{-\ell},$$

where D_ℓ is a Dickson–Chebyshev polynomial and $y = 3(2n + 1)$. The splitting field has degree at most $\ell(\ell - 1)$. The field-degree dependence is already explicit in Alpöge's descent [4, Section 3, pp. 3–5]; using this particular field gives an $\exp(O(\ell^2))$ bound for the relevant integral points. Balancing small exponents against the height bound for large ones produces the power $2/3$ in (1.10).

The exceptional cube case is also explicit: U_n is a cube in its full unit group exactly for $n = 2$ and $n = 8$. Its proof uses the complete integral-point data for the elliptic curve $y^2 = x^3 - 12x + 20$, with the data source identified at the point of use.

1.3 Prior work and the scope of the results

The least nontrivial roots of $u^k \equiv 1 \pmod{n}$ and related sequences were studied by Andrica and Crişan [12]; see also [1, Section 5, Theorem 5.1]. The identity $r_n + 2 = s_2(n)$ identifies our shifted root with their least-root object. Our estimates concern its typical size and the minimum over all rational square copies.

Crişan and Pollack [1] prove logarithmic upper and lower bounds for the least root of a general soluble polynomial congruence. Their Theorem 1.2, together with the end of its proof, permits every upper-bound exponent $c_f < \kappa_f/2$; their introduction predicts the exponent κ_f. For $f(r) = (r+1)(r+3)$ one has $\kappa_f = \log 2$. Thus (1.8) proves this particular case of their prediction. The more precise relation (1.5) concerns the minimum over rational square copies and leads to the fluctuations in (1.6).

Martin and Sitar [13, Theorem 1.4] study global equidistribution of roots of reducible quadratics; Dartyge and Martin [3, Theorem 1] give aggregated exponential-sum formulas at fixed frequencies. Kowalski and Soundararajan [2, Theorem 1.2 and Remark 1.3(2)] relate discrepancy to small roots for almost all moduli, including prime powers. Their subsequent work [14, Theorem 1.5 and Remark 1.6] develops Fourier moments for Chinese-remainder constructions with twisted multiplicativity. Here the local probabilities for equal and unequal frequencies, the uniform return to integer moduli, and the lower-bound weight $2^{-\omega(n)}$ together give the individual $\omega(n)$ estimate, including rational denominators.

For quadratic units, Louboutin [8, Theorem 4] describes when a unit is fundamental in the order it generates. The question in (1.10) is in the full ring of integers, where a smaller unit can lie outside that order. Gras [15, Theorem 4.2, Corollary 4.3 and Section 5.2] studies first occurrences of squarefree kernels in trace families and explains the limitation introduced by nonlinear substitutions of the trace. Our trace $2A_n = 18n(n+1)+2$ gives such a specialization. The bound in Theorem 1.1 controls the exceptional powers in this restricted family and concerns the full unit group. Diao [20] counts discriminants with small fundamental Pell solutions in a study of class numbers. Here the parameter is the index n, and the exceptional event is that the prescribed unit U_n is a proper power.

Alpöge [4, Theorem 1.1 and Section 3, pp. 3–5] supplies the integral-point descent behind our count. His proof retains the degree of a field containing three roots before applying a general cubic bound in the polynomial degree. We specialize that dependence using the explicit splitting field of our Chebyshev family. The resulting quadratic exponential cost gives (1.10). The elementary sector $s_n = 2$ in Section 5 is a Richaud–Degert subfamily: its fundamental unit is classical [17, Lemma 2], while its density is computed separately here.

There is also a connection with arithmetic reconstruction from quadratic traces [9, Theorem 1.3 and Sections 4–5]. That work constructs repeated signs uniformly in a prescribed target prime. Here we estimate square copies and determine the regulator for almost all indices of the quartic family. Pell equations also provide a classical link between quadratic values and Liouville signs; see Borwein, Choi and Ganguli [19, Theorem 2.2].

Finally, Section 6 uses $\lambda(D(n)) = \mu(d_n)$ to index a signed series by fundamental units. The resulting holomorphic comparison is unconditional. Holomorphic continuation of the signed regulator series near $s = 1$ is a sufficient condition for cancellation on every harmonic window of divergent mass when all indices in the window are included, by a local Tauberian boundedness principle [16, Theorem 3.1]. The comparison makes this continuation equivalent to that of the original signed Dirichlet series near 1. Establishing it remains an additional analytic problem. The comparison already follows from $E(X) \ll_\varepsilon X^\varepsilon$ for every $\varepsilon > 0$; its proof does not require the quantitative exponent $2/3$.

1.4 Conventions and route through the proof

An assertion holds on a set of natural density one if the number of exceptions up to X is $o(X)$. For a varying asymptotic expression, we use this phrase when the asymptotic holds as n tends to infinity through one such set. All implied constants are absolute unless a subscript or the surrounding statement specifies their dependence. We use $\mathbb{N} = \{1, 2, \dots\}$.

Part I proves the root and slope results. The averaging over residues is first kept separate from the sieve that returns to integer moduli, so that the required uniformity in the modulus is visible. Part II proves the unit count, then gives the regulator series and its analytic criterion. The computational appendix records finite checks; the asymptotic claims rest on the proofs.

Part I. Small roots and square copies

2 Small representatives of a square class

The rational square class of $3n+1$ can always be represented by another positive affine value $kn+1$. Indeed,

$$(3n^2 + 7n + 5)n + 1 = (3n + 1)(n + 1)^2.$$

The question is how much smaller the first such slope usually is. Define

$$K_*(n) = \min\{k \in \mathbb{N} : k \geq 1,\ k \neq 3,\ (kn+1)/(3n+1) \in \mathbb{Q}^2\}, \qquad n \geq 1. \tag{2.1}$$

Here $\mathbb{Q}^2$ denotes the set of rational squares, and $\omega(n)$ counts distinct prime divisors. All logarithms are natural. A statement holds in natural density one if the number of exceptions up to N is $o(N)$.

Theorem 2.1. *There is an absolute constant $B > 0$ such that, on a set of natural density one,*

$$n^2 4^{-\omega(n)} (\log\log n)^{-B} \leq K_*(n) \leq n^2 4^{-\omega(n)} (\log\log n)^{B}. \tag{2.2}$$

Consequently,

$$K_*(n) = \frac{n^2}{(\log n)^{2\log 2 + o(1)}} \tag{2.3}$$

on a set of natural density one.

Corollary 2.2. *If n is uniform on $\{1, \dots, N\}$, then*

$$\frac{\log(n^2/K_*(n)) - 2(\log 2)\log\log N}{2(\log 2)\sqrt{\log\log N}} \implies \mathcal{N}(0,1). \tag{2.4}$$

Corollary 2.3. *Let r_n be the least nonnegative integer satisfying $(r_n+1)(r_n+3) \equiv 0 \pmod{n}$. For every $n \geq 1$,*

$$r_n + 2 = s_2(n) := \min\{u \in \mathbb{N} : u \geq 2,\ u^2 \equiv 1 \pmod{n}\}.$$

On a set of natural density one,

$$\log \frac{n}{r_n + 2} = (\log 2)\omega(n) + O(\log\log\log n). \tag{2.5}$$

In particular,

$$r_n = \frac{n}{(\log n)^{\log 2 + o(1)}} \tag{2.6}$$

on a set of natural density one. If n is uniform on $\{1, \dots, N\}$, then

$$\frac{\log(n/(r_n+2)) - (\log 2)\log\log N}{(\log 2)\sqrt{\log\log N}} \implies \mathcal{N}(0,1). \tag{2.7}$$

The two sides of (2.2) require different arguments. For an upper bound it suffices to use integer square multipliers: if $u > 1$ and $u^2 \equiv 1 \pmod{n}$, then

$$k = \frac{(3n+1)u^2 - 1}{n} \in \mathbb{N}, \qquad 3 < k \le 4u^2. \tag{2.8}$$

For a lower bound we must also allow rational square multipliers. Writing $3n+1 = st^2$ with s squarefree, every admissible slope gives $kn+1 = su^2$ for an integer $u \ge 1$: if the rational square root is a/b in lowest terms, then $b^2 \mid 3n+1$, hence $b \mid t$ and $u = ta/b \in \mathbb{N}$. We obtain $n \mid (u-t)(u+t)$. A weighted count of this factorisation controls every possible denominator t.

The upper bound uses a feature of the split congruence that is absent for a general irreducible polynomial. Split $n = dm$, where d contains the small prime powers of n. We can impose $u \equiv 1 \pmod{m}$ first. The roots modulo d then move by multiplication by $m^{-1} \pmod{d}$. An exact second-moment calculation controls these dilations; a sieve bound shows that the rough cofactors m cannot concentrate in the bad residue classes.

2.1 A sieve bound with the progression kept uniform

Put $w(a) = 2^{-\omega(a)}$ for $a \ge 1$. We first record the elementary upper-bound sieve used in both directions of the argument. Its uniformity includes the starting point of the progression.

Lemma 2.4. *Let a_0, b be integers with $b \ge 1$ and $(a_0, b) = 1$. Let $\mathcal{I}$ be an interval of length H in the integer parameter v, on which $a_0 + bv > 0$. For sufficiently large H, set $R = \lceil 6 \log\log(10H) \rceil$. Uniformly for $2 \le z \le H^{1/(8R)}$ and $0 \le \theta \le 1$,*

$$\sum_{v \in \mathcal{I}} \prod_{\substack{p \le z,\ p \nmid b \\ p \mid a_0 + bv}} (1-\theta) \le H \prod_{\substack{p \le z \\ p \nmid b}} (1 - \theta/p) + O\Big(\frac{H}{(\log H)^2} + H^{1/4} \Big). \tag{2.9}$$

In particular, if $1 \le b \le 2X$ and $1/2 \le H \le 2X$, then

$$\sum_{v \in \mathcal{I}} w(a_0 + bv) \ll \frac{(1+H)(\log\log(20X))^2}{\sqrt{\log(2+H)}}. \tag{2.10}$$

All implied constants are absolute.

Proof. Retain each prime $p \le z$, $p \nmid b$, independently with probability θ. For a fixed integer a, the product on the left of (2.9) is the probability that no retained prime divides a. The even Bonferroni truncation through order $2R$ is an upper bound for this probability. Each squarefree modulus q that occurs satisfies $q \le z^{2R} \le H^{1/4}$ and $(q, b) = 1$. The condition $q \mid a_0 + bv$ specifies one class of v modulo q, with count $H/q + O(1)$. The total counting error is therefore $O(H^{1/4})$.

To complete the truncated main term to its Euler product, put $S = \sum_{p \le z} \theta/p \le \log\log H + O(1)$. The absolute tail is at most $H \sum_{j > 2R} S^j/j! \ll H/(\log H)^2$, since $j! \ge (j/e)^j$. This proves (2.9).

Take $\theta = 1/2$ and $z = H^{1/(8R)}$. Ignoring prime divisors above z only increases $w(a)$. Mertens' estimates give

$$\prod_{\substack{p \le z \\ p \nmid b}} (1 - 1/(2p)) \ll (\log z)^{-1/2} \frac{b}{\varphi(b)}.$$

For $b \le 2X$, $b/\varphi(b) \ll \log\log(20X)$. One can see this directly by splitting the product over $p \mid b$ at $\log(6X)$: Mertens' product bounds the small primes, and $\omega(b) \le \log(2X)/\log 2$ bounds the remaining product. Since $R \ll \log\log(20X)$, the stated power two in (2.10) absorbs the factor $R^{1/2}$ and the error in (2.9). Bounded H is covered by the elementary bound $O(1+H)$. The forms of Mertens' estimates used here are the prime reciprocal sum and its logarithmically weighted counterpart [11]. □

2.2 Counting abnormally small square-class representatives

The next estimate is uniform in the size cutoff L. This allows us later to choose a different cutoff on each level set of $\omega(n)$.

Lemma 2.5. *Fix positive integers A, J. For $X < n \le 2X$, write $3n+1 = st^2$ with s squarefree. Let $\mathcal{B}(X, L; A, J)$ consist of the integers in this interval such that $t \le A$, $v_2(n) \le J$, and there is an integer $u \ne t$ with $1 \le u \le X/L$ and $n \mid u^2 - t^2$. Then, uniformly for $L \ge 1$,*

$$\sum_{n \in \mathcal{B}(X,L;A,J)} 2^{-\omega(n)} \ll_{A,J} \frac{X(\log\log(20X))^4}{L}. \tag{2.11}$$

Moreover, the integers with $t > A$ or $v_2(n) > J$ number

$$O\Big(X/A + X/2^J + \sqrt{X}\Big). \tag{2.12}$$

Proof. The bound for $t > A$ follows by summing $\#\{X < n \le 2X : q^2 \mid 3n+1\} \ll X/q^2 + 1$ over $A < q \le \sqrt{6X+1}$; moduli divisible by 3 contribute nothing. The bound for $v_2(n) > J$ is immediate.

Fix $t \le A$ and $j = v_2(n) \le J$. We may assume $X > A^2$. Then $u \ne t$ and $n \mid u^2 - t^2$ force $u > t$. Also $(n, t) = 1$, because $t^2 \mid 3n+1$. Every odd prime power in n therefore divides exactly one of $u - t$ and $u + t$. Allocate these prime powers to obtain coprime odd integers a, b with

$$n = 2^j ab, \quad a \ge b, \quad a \mid u + \sigma t, \quad b \mid u - \sigma t$$

for one of the signs $\sigma \in \{-1, 1\}$.

The positive integer $v = (u + \sigma t)/a$ satisfies $v \ll_{A,J} b/L$. Indeed, $u > t$ and $u \le X/L$ imply $u + t \le 2X/L$, while $a > X/(2^j b)$. The congruence

$$av \equiv 2\sigma t \pmod{b}$$

has a solution only if $(v, b) = 1$, and then it specifies one invertible class of a modulo b. There are $O_{A,J}(b/L)$ possible positive integers v; this remains true when there are none. For each such class the interval for a has length $X/(2^j b)$, so the progression parameter has length $H = X/(2^j b^2)$. The condition $a \ge b$ implies $b \le \sqrt{2X/2^j}$ and hence $H \ge 1/2$.

Since $w(n) \le w(a)w(b)$, applying (2.10) to a gives an upper bound

$$\ll_{A,J} \frac{XD_X^2}{L} \sum_{b \le \sqrt{2X/2^j}} \frac{w(b)}{b\sqrt{\log(2 + X/(2^j b^2))}}, \qquad D_X = \log\log(20X). \tag{2.13}$$

Repeated representations can only increase this upper bound. For $2^i \le b < 2^{i+1}$, (2.10) with modulus one gives $\sum_b w(b)/b \ll D_X^2/\sqrt{1+i}$. If $M = \lfloor \log_2 \sqrt{2X/2^j} \rfloor$, the other denominator in (2.13) is $\gg \sqrt{1 + M - i}$ on that block. Finally,

$$\sum_{i=0}^{M} \frac{1}{\sqrt{(1+i)(1+M-i)}} \ll 1.$$

Sum over the finitely many t, j, σ to obtain (2.11). □

2.3 Separating the small prime powers

For the upper bound put

$$T = \log\log X, \qquad Z = X^{1/T^2}, \qquad n = dm, \tag{2.14}$$

where d is the product of all prime powers in n whose prime is at most Z. Thus $(d, m) = 1$ and every prime divisor of m exceeds Z.

Lemma 2.6. *For all but $o(X)$ integers $X < n \le 2X$,*

$$d \le X^{1/3}, \qquad T/2 \le W := \omega(d) \le 2T, \qquad \omega(m) \le 3\log T + 5. \tag{2.15}$$

Proof. The average of $\log d$ is $O(\log Z)$, by summing prime powers and using $\sum_{p\le Z} \log p/(p-1) \ll \log Z$. Markov's inequality therefore makes $d > X^{1/3}$ an event of probability $O(T^{-2})$.

For a set of primes at most $X^{1/4}$, the mean of the number dividing a uniform integer in $(X, 2X]$ is its reciprocal sum plus $o(1)$. Its variance is at most that reciprocal sum plus $o(1)$: count the multiples of p and pq, with total normalised error $O(\pi(X^{1/4})^2/X) = O(X^{-1/2})$. In particular, the counts for $p \le Z$ and for $Z < p \le X^{1/4}$ have means

$$T - 2\log T + O(1), \qquad 2\log T + O(1),$$

respectively. Their variances are $O(T)$ and $O(\log T)$. Chebyshev's inequality gives the claimed bounds for these counts. At most four prime divisors of $n \le 2X$ exceed $X^{1/4}$, once X is sufficiently large. This proves the last assertion as well. □

2.4 An exact second moment for the roots

Let

$$\mathcal{R}_d = \{r \bmod d : r^2 \equiv 1 \pmod d\}, \qquad \rho_d = |\mathcal{R}_d|, \qquad G_d(h) = \rho_d^{-1} \sum_{r\in\mathcal{R}_d} \exp(2\pi i h(r-1)/d).$$

We average over all dilations $a \bmod d$ first. Restriction to invertible a will be made only after the second moment is estimated. For integers h, l, orthogonality gives the exact identity

$$\begin{aligned} M_d(h,l) &:= \frac{1}{d} \sum_{a \bmod d} G_d(ha)\overline{G_d(la)} \\ &= \rho_d^{-2} \#\{(r,s) \in \mathcal{R}_d^2 : h(r-1) \equiv l(s-1) \pmod d\}. \end{aligned} \tag{2.16}$$

The last expression is nonnegative and factors over prime powers. For an odd prime $p \mid d$ with $p \nmid hl(h-l)$, the only permitted pair among $(1,1), (1,-1), (-1,1), (-1,-1)$ is $(1,1)$, already modulo p. Its local probability is $1/4$. If $h = l \ne 0$ and $p \nmid h$, exactly the two equal pairs are permitted, with probability $1/2$. The factor at 2, and the remaining local factors, are at most one. Consequently, with $W = \omega(d)$ and $\omega(v) := \omega(|v|)$ for nonzero negative v,

$$\begin{aligned} M_d(h,h) &\ll 2^{-W} 2^{\omega(h)} && (h \ne 0), \\ M_d(h,l) &\ll 4^{-W} 4^{\omega(h)+\omega(l)+\omega(h-l)} && (hl(h-l) \ne 0). \end{aligned} \tag{2.17}$$

These estimates include arbitrary prime powers in d.

Fix a nonnegative smooth function G supported in $(1,2)$, with $\int G = 1$. For d satisfying (2.15), put

$$\delta = T^{100} 2^{-W}, \qquad g(x) = \sum_{j\in\mathbb{Z}} G((x+j)/\delta). \tag{2.18}$$

Here $\delta \to 0$ uniformly over the prescribed range of W. If c_h are the Fourier coefficients of g, then

$$c_0 = \delta, \qquad |c_h| \ll \nu_h := \delta(1+\delta|h|)^{-2}, \qquad \sum_{h\in\mathbb{Z}} \nu_h \ll 1. \tag{2.19}$$

The Fourier series converges absolutely. In particular, no truncation with a growing frequency cutoff is needed below.

Lemma 2.7. *Uniformly for the above d and δ,*

$$V_d := \frac{1}{d}\sum_{a \bmod d} \left| \frac{1}{\rho_d} \sum_{r\in\mathcal{R}_d} g(a(r-1)/d) - \delta \right|^2 \ll 2^{-W}\delta T + 4^{-W}T^{63}. \tag{2.20}$$

It follows that the dilations for which the average of g is zero occupy at most $O(dT^{-99})$ residue classes modulo d.

Proof. Expand the absolutely convergent Fourier series and apply (2.17). The diagonal contributes at most

$$2^{-W}\sum_{h\neq 0} |c_h|^2 2^{\omega(h)},$$

and the off-diagonal contribution is at most

$$4^{-W}\sum_{\substack{h,l\neq 0\\ h\neq l}} \nu_h\nu_l\, 4^{\omega(h)+\omega(l)+\omega(h-l)}.$$

For each positive integer q, $q^{\omega(v)} \le \tau_q(v)$, where τ_q counts ordered factorisations into q positive factors. Summing over the first $q-1$ factors gives

$$\sum_{v\le Y} \tau_q(v) \le Y(1+\log Y)^{q-1}.$$

Split the weighted sum at $1/\delta$ and then into dyadic blocks. For $q = 2, 64$ this yields

$$\sum_{v\neq 0} \nu_v q^{\omega(v)} \ll_q (1+\log(1/\delta))^{q-1} \ll_q T^{q-1}. \tag{2.21}$$

Since $|c_h|^2 \ll \delta\nu_h$, the diagonal is $O(2^{-W}\delta T)$.

The discrete convolution satisfies $(\nu * \nu)_v \ll \nu_v$. To check this, in each term of the convolution at least one of the two distances from zero is at least $|v|/2$; bound that factor by $4\nu_v$ and sum the other using (2.19). Apply Hölder's inequality with exponent three to the factors $4^{\omega(h)}, 4^{\omega(l)}, 4^{\omega(h-l)}$, with measure $\nu_h\nu_l$. The first two resulting sums use (2.21) with $q = 64$; the third uses the same estimate after the convolution bound. Each is $O(T^{63})$, so the off-diagonal term is $O(4^{-W}T^{63})$. This proves (2.20). Finally,

$$\frac{V_d}{\delta^2} \ll T^{-99} + T^{-137} \ll T^{-99}.$$

If the average of g vanishes, the absolute value in (2.20) is δ, which proves the last assertion. □

The root $r = 1$ is included in this calculation. Its contribution is at the origin and cannot hit the support of g. The scale $\delta = T^{100}2^{-W}$ is larger than its mass by a growing polylogarithmic factor; the second moment accounts for this atom without subtracting it.

2.5 Returning from dilations to integer moduli

For a fixed $d \le X^{1/3}$ and an invertible class $b \pmod d$, Lemma 2.4, with $\theta = 1$ and $z = Z$, gives

$$\#\{X/d < m \le 2X/d : m \equiv b \pmod d,\ p \mid m \Rightarrow p > Z\} \ll \frac{X}{d\varphi(d)\log Z}. \tag{2.22}$$

Indeed, the progression parameter has length $H = X/d^2 \ge X^{1/3}$, and $Z \le H^{1/(8\lceil 6\log\log(10H)\rceil)}$ for all sufficiently large X, uniformly in d. The sieve product is $O(d/(\varphi(d)\log Z))$. Both errors in (2.9) are absorbed by its asserted main bound.

Inversion permutes the invertible residue classes modulo d. By Lemma 2.7, the number of bad classes for m^{-1} is at most $O(dT^{-99})$. Sum (2.22) over these classes, and then over the possible d. Since $d/\varphi(d) \ll T$ for $d \le X^{1/3}$,

$$\begin{aligned}\#\{\text{bad } n\} &\ll \frac{XT^{-99}}{\log Z}\sum_{d\le X^{1/3}}\frac{1}{\varphi(d)} \\ &\ll XT^{-98}\frac{\log X}{\log Z} = O(XT^{-96}) = o(X).\end{aligned} \tag{2.23}$$

Extending the last sum to all d only increases it.

For every remaining n, a root $r \in \mathcal{R}_d$ gives an integer j with

$$j \equiv (r-1)m^{-1} \pmod d, \qquad \delta d < j < 2\delta d.$$

Then $u = 1 + mj > 1$ satisfies $u^2 \equiv 1 \pmod n$, and $u \ll n\delta$. The slope in (2.8) therefore obeys

$$\begin{aligned}K_*(n) &\ll n^2\delta^2 = n^2 4^{-\omega(n)}T^{200}4^{\omega(m)} \\ &\ll n^2 4^{-\omega(n)}T^{200+3\log 4} \le n^2 4^{-\omega(n)}T^{220}\end{aligned} \tag{2.24}$$

for all sufficiently large X, outside $o(X)$ integers. Here the final exponent leaves a fixed margin to absorb constants.

2.6 The lower bound at each prime-factor count

Fix A, J before letting X tend to infinity. The normal order of $\omega(n)$ gives $\omega(n) \le 2T$ outside $o(X)$ integers [10]. For each integer $0 \le b \le 2T$, apply Lemma 2.5 with

$$L_b = 2^b T^{100}.$$

On the set $\omega(n) = b$, its weight is exactly 2^{-b}. Thus

$$\begin{aligned}\#\{n \in \mathcal{B}(X, L_b; A, J) : \omega(n) = b\} &\le 2^b \sum_{n\in\mathcal{B}(X,L_b;A,J)} 2^{-\omega(n)} \\ &\ll_{A,J} XT^{-96}.\end{aligned} \tag{2.25}$$

The sum over all these levels is $O_{A,J}(XT^{-95})$.

Suppose an admissible slope satisfies $k \le n^2 4^{-b}T^{-220}$ and that $t \le A$, $v_2(n) \le J$. Writing $kn + 1 = su^2$ as above gives

$$u = t\sqrt{\frac{kn+1}{3n+1}} \le A\sqrt{k} \le 2AX2^{-b}T^{-110} \le X/L_b$$

for sufficiently large X depending on A. Hence such an n is counted in (2.25). Combining this with (2.12), the upper limit of the exceptional proportion is $O(A^{-1} + 2^{-J})$. Letting A, J tend to infinity proves the lower bound with the same absolute exponent 220 on each dyadic interval. The constants depending on A, J affect only the vanishing exceptional proportion and the starting scale; they do not enter this exponent.

Together with (2.24), this proves (2.2), after a harmless enlargement of the absolute exponent to replace $\log\log X$ by $\log\log n$. Summing dyadic intervals gives natural density one. The normal order $\omega(n) = (1 + o(1)) \log\log n$ then gives (2.3).

Proof of Corollary 2.2. Theorem 2.1 says

$$\log(n^2/K_*(n)) = 2(\log 2)\omega(n) + O(\log\log\log n)$$

outside a set of density zero. For uniform $n \le N$, the exceptional set has probability $o(1)$, and $\log\log\log N = o(\sqrt{\log\log N})$. The Erdős–Kac theorem for $\omega(n)$ now implies (2.4) [10]. □

Proof of Corollary 2.3. The substitution $u = r + 2$ is an order-preserving bijection between nonnegative solutions of the shifted congruence and integers $u \ge 2$ satisfying $u^2 \equiv 1 \pmod{n}$. This proves the identity with $s_2(n)$, including the small indices for which $r_n = 0$.

The root $u = 1 + mj$ constructed above satisfies, for all but $o(X)$ integers $X < n \le 2X$,

$$r_n + 2 \le u \ll n\delta \ll n2^{-\omega(n)}T^{100+3\log 2}, \qquad T = \log\log X.$$

Conversely, (2.8) applied to $u = r_n + 2$ gives $K_*(n) \le 4(r_n + 2)^2$. The lower bound in Theorem 2.1 therefore yields

$$r_n + 2 \ge \frac{1}{2}\sqrt{K_*(n)} \ge \frac{1}{2}n2^{-\omega(n)}(\log\log n)^{-B/2}$$

on a set of natural density one. Taking logarithms in these two bounds, replacing $\log\log X$ by $\log\log n$, and summing the dyadic exceptional counts proves (2.5).

The normal order of $\omega(n)$ gives $r_n + 2 = n/(\log n)^{\log 2 + o(1)}$ on a density-one set. This tends to infinity there, so subtracting 2 gives (2.6). For uniform $n \le N$, the exceptional set has probability $o(1)$ and the error in (2.5) is $O(\log\log\log N) = o(\sqrt{\log\log N})$, after discarding finitely many small indices. The Erdős–Kac theorem [10] now gives (2.7). □

The least nontrivial roots $s_k(n)$ and related sequences were studied by Andrica and Crişan [12]; the relation to shifted polynomials is also recorded in [1, Section 5, Theorem 5.1]. Crişan and Pollack formulate the prediction $r_n = n/(\log n)^{\kappa_f + o(1)}$ for the least nonnegative root of a polynomial congruence on its soluble moduli [1, p. 2]. For $f(x) = (x+1)(x+3)$ every modulus is soluble, the two integer roots are negative, and f has two roots modulo every odd prime. Their constant is therefore $\kappa_f = \log 2$ [1, Lemma 3.3]. Corollary 2.3 establishes this predicted exponent for this polynomial. The Chinese remainder theorem, root equidistribution, and their Fourier moments have earlier treatments [13, 2, 3, 14]. The estimates above concern a shrinking interval and retain the individual fluctuation $\omega(n)$ needed for (2.4) and (2.7). Both Gaussian laws are consequences of the classical Erdős–Kac theorem applied to these arithmetic estimates.

Part II. Fundamental units and regulators

3 A quartic family of quadratic units

The same four linear factors that enter the square-class problem also produce a Pell equation. The identity is elementary; the main issue is to decide whether its solution generates the full unit group.

Write

$$D(n) = n(n+1)(3n+1)(3n+2) = d_n s_n^2, \qquad A_n = 9n(n+1)+1, \tag{3.1}$$

where d_n is squarefree and $s_n > 0$. Put

$$U_n = A_n + 3s_n\sqrt{d_n}. \tag{3.2}$$

For a real quadratic field, its fundamental unit will mean the generator $\eta > 1$ of the group of units modulo $\{\pm 1\}$, in the chosen real embedding. Its norm may be -1. Thus asking whether U_n is fundamental is stronger than asking whether it generates the subgroup of units of norm 1.

Lemma 3.1. *For every $n \geq 1$, the integer d_n is greater than 1, the integer s_n is even, and U_n is a unit of norm 1 in the full ring of integers of $\mathbb{Q}(\sqrt{d_n})$. Moreover,*

$$A_n^2 - 9D(n) = 1, \qquad 2A_n - 1 < U_n < 2A_n. \tag{3.3}$$

If $m < n$ and $d_m = d_n$, then $n > 6m$.

Proof. Set $t = n(n+1)$. Then $D(n) = t(9t+2)$, so $(9t+1)^2 - 9D(n) = 1$. If $d_n = 1$, the two positive integral squares A_n^2 and $(3s_n)^2$ would differ by 1, which is impossible. Since t is even,

$$D(n) = 4\left(\frac{t}{2}\right)\left(\frac{9t}{2}+1\right),$$

and s_n is even. Formula (3.3) proves the unit assertion and the displayed estimates.

Suppose that $d_m = d_n = d$. The quotient $U_n/U_m = a + b\sqrt{d}$ belongs to $\mathbb{Z}[\sqrt{d}]$, has norm 1, and is greater than 1. Its rational coefficient is

$$a = A_nA_m - 9s_ns_md \equiv 1 \pmod{18},$$

because $A_j \equiv 1 \pmod{18}$ and s_j is even. Thus $a \geq 19$ and

$$\frac{U_n}{U_m} \geq 19 + 6\sqrt{10} > 36.$$

On the other hand,

$$\frac{U_{6m}}{U_m} < \frac{2A_{6m}}{2A_m - 1} < 36.$$

The strict increase of U_n in n gives $n > 6m$. □

In particular, $n \mapsto d_n$ is injective on every dyadic interval $[X, 2X)$. This is the kernel injectivity used in the catalogue of quadratic probes in [22]. At an odd prime $p \nmid D(n)$, the product of the four Legendre symbols observed there is $\left(\frac{d_n}{p}\right)$.

Let

$$E(X) = \#\{1 \leq n \leq X : U_n \neq \eta_{d_n}\}, \tag{3.4}$$

where η_{d_n} denotes the fundamental unit of the full ring of integers. If an index is not counted by $E(X)$, then the field has no unit of norm -1, and its regulator is $\log U_n$. Also, the map $n \mapsto d_n$ is injective on the set of these indices: two occurrences would give two different positive fundamental units in the same field.

3.1 Proper powers and integral traces

It is useful to express the exceptional condition through the trace, rather than through the coefficients of a unit. The trace is integral even when the full ring of integers contains half-integral coefficients.

Lemma 3.2. *If U_n is a proper power of a unit, then at least one of the following holds.*

1. *There are integers $x \geq 1$ and $\sigma \in \{1, -1\}$ such that*
$$2x^2 - 9(2n+1)^2 = -5 + 4\sigma. \tag{3.5}$$
2. *There are an odd prime ℓ and an integer $x \geq 3$ such that*
$$y^2 = 2D_\ell(x) + 5, \qquad y = 3(2n+1), \tag{3.6}$$
where $D_0(X) = 2$, $D_1(X) = X$, and
$$D_{j+1}(X) = XD_j(X) - D_{j-1}(X).$$
In the second case, uniformly for $n \leq X$,
$$\ell \ll \log(2X), \qquad 3 \leq x \ll 1 + X^{2/\ell}. \tag{3.7}$$

All implied constants are absolute.

Proof. Write $U_n = \eta_{d_n}^k$ with $k \geq 2$. If k is even, let $\xi = \eta_{d_n}^{k/2}$, $\sigma = \mathrm{Norm}(\xi)$, and $x = \mathrm{Tr}(\xi)$. The identity $\mathrm{Tr}(\xi^2) = x^2 - 2\sigma$ gives $x^2 = 2A_n + 2\sigma$, which is equivalent to (3.5).

If k is odd, choose a prime $\ell \mid k$ and put $\xi = \eta_{d_n}^{k/\ell}$. Its norm is 1, since $\xi^\ell = U_n$ and ℓ is odd. Consequently $x = \xi + \xi^{-1}$ is an integer at least 3, and
$$D_\ell(x) = \xi^\ell + \xi^{-\ell} = 2A_n.$$
The identity $4A_n + 5 = 9(2n+1)^2$ yields (3.6). Finally,
$$\xi \geq \frac{3+\sqrt{5}}{2} > 1, \qquad \xi^\ell = U_n \ll X^2,$$
which proves (3.7). □

Proposition 3.3. *The number of indices $n \leq X$ for which U_n is a square of a unit is $O(\log(2X))$. There are $\gg \log(2X)$ such indices.*

Proof. For $\sigma = 1$, equation (3.5) becomes
$$\big(3(2n+1)\big)^2 - 2x^2 = 1.$$
For $\sigma = -1$, it first implies $3 \mid x$ and then becomes
$$(2n+1)^2 - 2(x/3)^2 = 1.$$
The positive solutions of either Pell equation form a subsequence of the powers of $3 + 2\sqrt{2}$. Their first coordinates grow geometrically, so at most $O(\log(2X))$ have $n \leq X$.

For the lower bound, write
$$(2n_j + 1) + z_j\sqrt{8} = (3+\sqrt{8})^j, \qquad j \geq 1.$$
The first coordinate is odd and $n_j(n_j+1) = 2z_j^2$. Therefore
$$U_{n_j} = 18z_j^2 + 1 + 6z_j\sqrt{9z_j^2+1} = \big(3z_j + \sqrt{9z_j^2+1}\big)^2.$$
The square root on the right is an algebraic integer of norm -1 in $\mathbb{Q}(\sqrt{d_{n_j}})$. The indices n_j grow geometrically, proving the lower bound. □

There is already a qualitative conclusion before any uniform estimate in ℓ. The polynomial D_ℓ equals $2T_\ell(X/2)$, with T_ℓ the Chebyshev polynomial. Its critical points are $2\cos(j\pi/\ell)$, $1 \le j < \ell$, and its critical values are 2 and -2. Thus $2D_\ell + 5$ has no repeated root. For each fixed odd prime ℓ, the curve (3.6) has genus $(\ell-1)/2 \ge 1$, and Siegel's theorem gives finitely many integral points [4, Section 1].

Fix $L > 0$. The primes $\ell \le L$ consequently contribute a finite number depending on L, while (3.7) bounds the contribution of the others by

$$O\big((1 + X^{2/L})\log(2X)\big).$$

Together with Proposition 3.3, this proves

$$E(X) \ll_\epsilon X^\epsilon \qquad (\epsilon > 0). \tag{3.8}$$

This qualitative estimate already suffices for the holomorphic comparison of regulator series in Section 6. It does not provide uniform control of the finite contribution as L grows. The next section supplies that control and the exponent $2/3$.

4 Uniform control of the exceptional powers

4.1 The discriminant and the splitting field

For an odd prime ℓ, put

$$f_\ell(X) = 2D_\ell(X) + 5, \qquad F_\ell(Z) = 2^{\ell-1} f_\ell(Z/2). \tag{4.1}$$

The change of variables

$$Z = 2x, \qquad Y = 2^{(\ell-1)/2} y \tag{4.2}$$

embeds the integral solutions of (3.6) into $Y^2 = F_\ell(Z)$.

Lemma 4.1. *The polynomial F_ℓ is monic, integral, irreducible, and has degree ℓ. Its discriminant satisfies*

$$|\operatorname{disc} f_\ell| = \frac{(2\ell)^\ell 3^{\ell-1}}{2}, \qquad |\operatorname{disc} F_\ell| = 2^{(\ell-1)^2} 3^{\ell-1} \ell^\ell. \tag{4.3}$$

It has a root field $K_\ell = \mathbb{Q}(z)$, where $z^\ell = -2$, and a splitting field contained in

$$L_\ell = \mathbb{Q}(z, \zeta_\ell), \qquad [L_\ell : \mathbb{Q}] \le \ell(\ell-1).$$

Moreover,

$$|\operatorname{Cl}(\mathcal{O}_{K_\ell,S})[2]| \le \exp\big(C\ell\log(2\ell)\big), \qquad S = \{\infty, 2, 3, \ell\}, \tag{4.4}$$

for an absolute constant C.

Proof. Since D_ℓ is monic and integral, multiplying $2D_\ell(Z/2) + 5$ by $2^{\ell-1}$ gives a monic integral polynomial. At the $\ell - 1$ critical points of f_ℓ, its values are 1 and 9, each occurring $(\ell-1)/2$ times. The derivative has leading coefficient 2ℓ. The resultant formula for the discriminant gives the first identity in (4.3). Scaling the argument and the polynomial gives the second.

The identity $D_\ell(w + w^{-1}) = w^\ell + w^{-\ell}$ shows that the roots of F_ℓ are

$$2(z\zeta_\ell^j + z^{-1}\zeta_\ell^{-j}), \qquad 0 \le j < \ell.$$

They are distinct by (4.3). The polynomial $X^\ell + 2$ is Eisenstein at 2, so $[\mathbb{Q}(z) : \mathbb{Q}] = \ell$. Also,

$$[\mathbb{Q}(z) : \mathbb{Q}(z + z^{-1})] \le 2.$$

This index divides the odd prime ℓ and hence is 1. Thus F_ℓ is irreducible with the stated root field and splitting field.

The field discriminant Δ_{K_ℓ} divides the discriminant of $X^\ell + 2$, so

$$|\Delta_{K_\ell}| \le 2^{\ell-1}\ell^\ell.$$

Minkowski's theorem gives an integral ideal of norm at most $\sqrt{|\Delta_{K_\ell}|}$ in each ideal class. Consequently

$$h_{K_\ell} \le |\Delta_{K_\ell}|\zeta_{K_\ell}(2) \le |\Delta_{K_\ell}|\zeta(2)^\ell \le \exp(C\ell\log(2\ell)).$$

Localizing the class group and then taking its 2-torsion cannot increase this bound. □

4.2 Keeping the field degree in the descent

Alpöge's theorem gives a uniform bound for the integral points of a monic hyperelliptic equation in terms of a 2-torsion class group and an exponential cost cubic in the degree [4, Theorem 1.1]. His proof already retains the degree of a field containing three roots before replacing it by the general cubic bound [4, Section 3, pp. 3–5]. We record this dependence for the present family. The specialization below uses its explicit splitting field; the descent mechanism is Alpöge's.

Lemma 4.2 (Alpöge's descent with the field degree retained)**.** *Let $\ell \ge 5$ be prime, set $K = K_\ell$ and $S = \{\infty, 2, 3, \ell\}$, and let $L/\mathbb{Q}$ be a number field containing three distinct roots of F_ℓ. Put $M = [L : \mathbb{Q}]$. There is an absolute constant C such that*

$$\#\{(Z, Y) \in \mathbb{Z}^2 : Y^2 = F_\ell(Z)\} \le |\operatorname{Cl}(\mathcal{O}_{K,S})[2]| \exp\big(C(\ell + M)\big). \tag{4.5}$$

Proof. We give the count, following the second descent argument in [4, Section 3, pp. 3–5]. Let ρ be a root of F_ℓ in K. All primes dividing its discriminant belong to S. Write $h_{K,S}[2] = |\operatorname{Cl}(\mathcal{O}_{K,S})[2]|$.

For an S-integral point (Z, Y), the ideal $(Z - \rho)$ in $\mathcal{O}_{K,S}$ is a square. Indeed, away from S, its prime divisors are coprime to the remaining factors of $F_\ell(Z)$, and the product is Y^2. The ideal square root has class in $\operatorname{Cl}(\mathcal{O}_{K,S})[2]$. For each such class choose a prime ideal representative $\mathfrak{p}$, as in Alpöge's proof, and invert that prime. There are at most $h_{K,S}[2]$ choices of class. Once the class is fixed,

$$Z - \rho = \gamma\beta^2, \qquad \beta \in \mathcal{O}_{K,S\cup\{\mathfrak{p}\}}, \quad \gamma \in \mathcal{O}^\times_{K,S\cup\{\mathfrak{p}\}}. \tag{4.6}$$

Modulo squares there are $\exp(O(\ell))$ choices for γ, by the unit theorem: at most $4\ell + 1$ places have been inverted, including the archimedean places. The norm of $\mathfrak{p}$ is irrelevant for this count.

Fix three distinct roots ρ_1, ρ_2, ρ_3 in L and the corresponding embeddings $\sigma_i : K \hookrightarrow L$. For fixed class and γ, equation (4.6) gives

$$Z - \rho_i = \gamma_i\beta_i^2, \qquad \gamma_i = \sigma_i(\gamma), \quad \beta_i = \sigma_i(\beta) \qquad (1 \le i \le 3).$$

The three γ_i are conjugates of this single choice of γ; they introduce no additional class-group choices. Adjoin $\sqrt{\gamma_1}, \sqrt{\gamma_2}, \sqrt{\gamma_3}$ to L, obtaining a field L' of degree at most $8M$. Enlarge the set of places to contain those above S and the three conjugate auxiliary prime ideals. The resulting set S' has $O(M)$ places, with an absolute constant. Put $a_i = \sqrt{\gamma_i}\beta_i$. Then

$$(a_i - a_j)(a_i + a_j) = \rho_j - \rho_i.$$

The right-hand side is an S'-unit, and both factors are S'-integral. Hence all six factors $a_i \pm a_j$ are S'-units.

The quotient of the S'-unit group by cubes has $\exp(O(M))$ elements. Choose cube-class representatives for

$$a_1 + a_2, \quad a_1 - a_2, \quad a_2 + a_3, \quad a_2 - a_3, \quad a_1 - a_3.$$

The total number of choices remains $\exp(O(M))$. The two identities

$$(a_1 + a_2) - (a_2 + a_3) = a_1 - a_3, \qquad (a_1 - a_2) + (a_2 - a_3) = a_1 - a_3$$

then become two nonsingular binary cubic equations after division by the cube expression for $a_1 - a_3$. Evertse's bound, in the form used in [4, Section 3], gives

$$\exp(O([L' : \mathbb{Q}] + |S'|)) = \exp(O(M))$$

solutions for each equation [5]. The constants do not depend on the coefficients or on the norms of the inverted primes.

These two solutions determine the ratios

$$\frac{a_1 + a_2}{a_1 - a_3}, \qquad \frac{a_1 - a_2}{a_1 - a_3}.$$

Their product equals $(\rho_2 - \rho_1)/(a_1 - a_3)^2$. Since the roots are distinct, it determines $(a_1 - a_3)^2$, then a_1 up to at most two choices, and finally $Z = a_1^2 + \rho_1$. There are at most two choices of Y for each Z.

Combining the counts gives

$$\begin{aligned} \#\{(Z, Y) \in \mathbb{Z}^2 : Y^2 = F_\ell(Z)\} &\le h_{K,S}[2] \exp(O(\ell)) \exp(O(M)) \exp(O(M)) \\ &= h_{K,S}[2] \exp(O(\ell + M)). \end{aligned}$$

The factors respectively account for the ideal class, the square class, the five cube classes, and the two cubic equations. Reconstruction has bounded multiplicity. The three roots were fixed throughout; allowing them to vary would add only a factor $O(\ell^3)$, which is absorbed in the displayed exponential. □

Corollary 4.3. *There is an absolute constant C such that for every prime $\ell \ge 5$,*

$$\#\{(Z, Y) \in \mathbb{Z}^2 : Y^2 = F_\ell(Z)\} \le \exp(C\ell^2). \tag{4.7}$$

Proof. Take $L = L_\ell = \mathbb{Q}(z, \zeta_\ell)$ in Lemma 4.2. Lemma 4.1 gives $M \le \ell(\ell - 1)$ and $h_{K,S}[2] \le \exp(C\ell \log(2\ell))$, proving the bound. □

Thus the quadratic exponential cost follows by inserting this family's splitting field into a dependence already present in Alpöge's proof.

4.3 Cubes and the final cutoff

Proposition 4.4. *The unit U_n is a cube in the full unit group of $\mathbb{Q}(\sqrt{d_n})$ if and only if $n = 2$ or $n = 8$.*

Proof. For $\ell = 3$, one has $D_3(x) = x^3 - 3x$. Equations (3.6) and (4.2) give

$$Y^2 = Z^3 - 12Z + 20, \quad Z = 2x \ge 6, \quad Y = 6(2n + 1) > 0. \tag{4.8}$$

This is the displayed integral model of the elliptic curve with LMFDB label 216.a1 (Cremona label 216a1). Its complete list of integral points, up to the involution $Y \mapsto -Y$, is [6]

Z	-4	-2	1	2	4	10	22	89
$\lvert Y\rvert$	2	6	3	2	6	30	102	$839.$

Here we use the published complete integral-point computation; the database's account of its rigorous integral-point calculations is given in [7]. Of the listed points, the conditions in (4.8) retain only $(10, 30)$ and $(22, 102)$. They yield $n = 2$ and $n = 8$, respectively. Conversely, the units

$$\frac{5+\sqrt{21}}{2}, \qquad \frac{11+3\sqrt{13}}{2}$$

have norm 1 and cubes U_2 and U_8. Both belong to the full ring of integers of the indicated field. □

Proof of the exceptional-set bound in Theorem 1.1. The lower bound follows from Proposition 3.3. For the upper bound, take

$$L_0 = \max\{5, (\log X)^{1/3}\}.$$

Even powers contribute $O(\log(2X))$ indices. Cubes contribute only two. The odd primes $5 \le \ell \le L_0$ contribute at most

$$L_0 \exp(CL_0^2)$$

by Corollary 4.3. For $\ell > L_0$, the trace bound (3.7) gives a total of

$$O\big((1 + X^{2/L_0}) \log(2X)\big),$$

because each pair (ℓ, x) determines at most one positive n. Both terms are at most $\exp(C'(\log X)^{2/3})$, after increasing the absolute constant to include bounded X. This proves the asserted bound for $E(X)$. The statements about fundamental units and regulators follow from their definition and the fact that U_n has norm 1. □

For comparison, the general exponential cost $\exp(O(\ell^3))$ would require $L_0 = (\log X)^{1/4}$ and give the exponent $3/4$. The quadratic bound for the splitting-field degree, used in Corollary 4.3, is exactly what changes the cutoff and produces $2/3$.

5 An explicit Richaud–Degert sector

The subfamily with the smallest possible square factor, $s_n = 2$, is a Richaud–Degert subfamily. Its fundamental units are given by the classical formula recorded in [17, Lemma 2, p. 142]; see also [18]. We compute its density and include an elementary proof of the fundamental-unit assertion.

Proposition 5.1. *The set $\{n \ge 1 : s_n = 2\}$ has natural density, and logarithmic density, equal to*

$$\frac{7}{18} \prod_{p \ge 5} \left(1 - \frac{4}{p^2}\right) > 0. \tag{5.1}$$

For every index in this set except $n = 1$, the unit U_n is fundamental in the full ring of integers. At $n = 1$,

$$d_1 = 10, \qquad U_1 = (3 + \sqrt{10})^2.$$

To identify the classical formula, put $q = n(n+1)/2$. On this sector,

$$d_n = D(n)/4 = 9q^2 + q = (3q)^2 + q.$$

The Richaud–Degert parameters are $a = 3q$ and $r = q$, with $-a < r \le a$ and $r \mid 4a$. For $q \ne 1, 4$, that formula gives

$$\eta_{d_n} = \frac{2a^2 + r + 2a\sqrt{d_n}}{r} = 18q + 1 + 6\sqrt{d_n} = U_n.$$

The case $q = 1$ is $n = 1$, when $\eta_{10} = 3 + \sqrt{10}$; $q = 4$ is not a value of $n(n+1)/2$ for an integer n. This classical identification is separate from the density calculation.

Proof. The condition $s_n = 2$ means exactly that $D(n)/4$ is squarefree. At 2, one has $v_2(D(n)) \geq 3$ for every n, and $v_2(D(n)) = 3$ in the four residue classes $1, 3, 4, 6$ modulo 8. These classes have density $1/2$. At 3, the condition excludes the two classes $0, -1$ modulo 9, giving a factor $7/9$. For $p \geq 5$, the four roots of the four linear factors are distinct modulo p, so the forbidden classes modulo p^2 have density $4/p^2$.

The Chinese remainder theorem gives the finite products of these local densities. To pass to all primes, note that a prime square dividing $D(n)$ for $p \geq 5$ divides one of the individual linear factors. For $n \leq X$, the contribution of primes $p > z$ is therefore at most

$$O\left(\sum_{z<p\leq\sqrt{3X+2}}\left(\frac{X}{p^2}+1\right)\right) = O\left(\frac{X}{z}+\sqrt{X}\right).$$

Letting first $X \to \infty$ and then $z \to \infty$ proves the natural density. Partial summation proves the logarithmic density with the same value.

For completeness, the following size comparison proves the fundamental-unit assertion directly. On this sector, $d_n = D(n)/4$ is even, so the full ring of integers is $\mathbb{Z}[\sqrt{d_n}]$. Every unit $\xi > 1$ in it has positive integral coefficients in the chosen embedding, and hence $\xi > \sqrt{d_n}$. For $n \geq 3$, we have $d_n \geq 330$ and

$$U_n = A_n + 6\sqrt{d_n} < 12\sqrt{d_n} + 1 < d_n.$$

It cannot be a power ξ^k with $k \geq 2$. The index $n = 2$ does not belong to the sector, while the displayed identity deals with $n = 1$. □

6 A signed series over fundamental regulators

The qualitative estimate (3.8), $E(X) \ll_\varepsilon X^\varepsilon$ for every $\varepsilon > 0$, makes the series over exceptional indices absolutely convergent at every positive real abscissa. This permits a change of index from integers to quadratic fields while retaining the Liouville sign. The quantitative exponent $2/3$ in Theorem 1.1 is not needed here. The resulting Dirichlet series identifies an analytic condition for cancellation; the condition itself is not established here.

6.1 The field family and the change of variable

For squarefree $d > 1$, let $\eta_d > 1$ be the fundamental unit of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, with respect to the embedding in which $\sqrt{d} > 0$. We choose the positive generator of the unit group modulo $\{\pm 1\}$, so its norm may initially be either sign. Define

$$\mathcal{F} = \left\{ d > 1 : \begin{array}{l} d \text{ is squarefree}, \quad \mathrm{N}(\eta_d) = 1, \\ 2\,\mathrm{Tr}(\eta_d) + 5 = m^2 \text{ for some } m \geq 9, \quad m \equiv 3 \pmod 6 \end{array} \right\}. \tag{6.1}$$

Here the trace and norm are from $\mathbb{Q}(\sqrt{d})$ to $\mathbb{Q}$.

Proposition 6.1 (A one-to-one parametrisation)**.** *The map $n \mapsto d_n$ is a bijection from $\{n \geq 1 : U_n$ is fundamental in $\mathcal{O}_{\mathbb{Q}(\sqrt{d_n})}\}$ onto $\mathcal{F}$. Its inverse is $n = (m-3)/6$, where m is the positive integer in (6.1).*

Proof. For a fundamental index, $\eta_{d_n} = U_n$ and

$$2\,\mathrm{Tr}(U_n) + 5 = 4A_n + 5 = 36n(n+1) + 9 = (6n+3)^2.$$

Conversely, let $d \in \mathcal{F}$ and put $n = (m-3)/6 \geq 1$. Then $\mathrm{Tr}(\eta_d) = 2A_n$ and $\mathrm{N}(\eta_d) = 1$. Thus η_d is the root greater than one of $z^2 - 2A_n z + 1$, namely U_n. The discriminant of this quadratic is

$$(2A_n)^2 - 4 = 36D(n),$$

so its quadratic field has squarefree radicand $d_n = d$. Finally A_n is strictly increasing for $n \geq 1$, which proves injectivity. No assertion about all repetitions of d_n is needed. □

Write $\lambda(n) = (-1)^{\Omega(n)}$ for the Liouville function and μ for the Möbius function. For our squarefree decomposition,

$$C(n) := \lambda\big(D(n)\big) = \lambda(n)\lambda(n+1)\lambda(3n+1)\lambda(3n+2) = \mu(d_n). \tag{6.2}$$

The last equality is exact: the factor s_n^2 makes no contribution to the parity of $\Omega(D(n))$. For $\Re s > 1$, set

$$\mathcal{D}_C(s) = \sum_{n\geq 1} \frac{C(n)}{n^s}, \qquad Z_\mu(s) = \sum_{d\in\mathcal{F}} \mu(d)\eta_d^{-s/2}, \qquad Z_+(s) = \sum_{d\in\mathcal{F}} \eta_d^{-s/2}. \tag{6.3}$$

The real logarithm is used to define each complex power.

Theorem 6.2 (Holomorphic comparison)**.** *Both differences*

$$\mathcal{D}_C(s) - 18^{s/2} Z_\mu(s), \qquad \zeta(s) - 18^{s/2} Z_+(s) \tag{6.4}$$

extend holomorphically from $\Re s > 1$ to $\Re s > 0$. Consequently, Z_+ has a meromorphic continuation to that half-plane, with a unique pole there: a simple pole at $s = 1$ of residue $18^{-1/2}$.

Proof. Since $U_n = A_n + \sqrt{A_n^2 - 1}$, we have

$$U_n = 18n^2\big(1 + O(n^{-1})\big). \tag{6.5}$$

For s in a fixed compact subset K of $\Re s > 0$, it follows that

$$n^{-s} - 18^{s/2} U_n^{-s/2} = O_K\big(n^{-\Re s - 1}\big).$$

Thus the sum of these differences over fundamental indices converges absolutely and locally uniformly on $\Re s > 0$, with or without the coefficient $C(n)$.

For the nonfundamental indices, (3.8) gives $E(X) \ll_\varepsilon X^\varepsilon$ for every fixed $\varepsilon > 0$. Partial summation therefore shows that

$$\sum_{\substack{n\geq 1 \\ U_n \text{ nonfundamental}}} n^{-\sigma} < \infty \qquad (\sigma > 0).$$

The corresponding Dirichlet series is holomorphic in the same half-plane. Proposition 6.1 now identifies the remaining sums with Z_μ and Z_+, proving (6.4). The assertion about Z_+ follows from the meromorphic continuation and residue of ζ. □

Corollary 6.3 (Equivalent local continuations)**.** *The series Z_μ admits a holomorphic continuation to a neighbourhood of $s = 1$ if and only if $\mathcal{D}_C$ does.*

Proof. Write $H(s) = \mathcal{D}_C(s) - 18^{s/2} Z_\mu(s)$ for the holomorphic function on $\Re s > 0$ given by Theorem 6.2. The factor $18^{s/2}$ is entire and never vanishes. Either local continuation therefore defines the other by $\mathcal{D}_C = 18^{s/2} Z_\mu + H$ or $Z_\mu = 18^{-s/2}(\mathcal{D}_C - H)$. □

Thus the change of index transports the local analytic condition exactly. It provides an arithmetic formulation in terms of fundamental regulators; proving the continuation requires further information about the signed series.

6.2 A local continuation criterion for harmonic windows

For real $1 \le U < V$, put

$$H(U, V) = \sum_{U < n \le V} \frac{1}{n}.$$

The sums in this subsection range over all integer indices in $(U, V]$. Their starting points may vary arbitrarily.

Theorem 6.4 (A sufficient analytic condition)**.** *If Z_μ admits a holomorphic continuation to a neighbourhood of $s = 1$, then*

$$\sup_{1 \le U < V} \left| \sum_{U < n \le V} \frac{C(n)}{n} \right| < \infty. \tag{6.6}$$

In particular,

$$\frac{1}{H(U, V)} \sum_{U < n \le V} \frac{C(n)}{n} \longrightarrow 0 \qquad \text{whenever } H(U, V) \longrightarrow \infty.$$

The boundedness principle below is a special case of the local complex Tauberian theorem of Debruyne and Vindas [16, Theorem 3.1]. We include a direct smoothing proof adapted to logarithmic sums. A uniform $O(1)$ bound for initial harmonic sums is equivalent to a uniform $O(1)$ bound over all windows, by taking differences of two initial sums. Either bound is stronger than the sole assertion that the initial sum is $o(\log X)$.

Lemma 6.5 (A bounded primitive from local analyticity)**.** *Let $(a_n)_{n \ge 1}$ be a bounded complex sequence and let $F(s) = \sum_{n \ge 1} a_n n^{-s}$ for $\Re s > 1$. If F continues holomorphically across $s = 1$, then $\sup_{1 \le U < V} |\sum_{U < n \le V} a_n/n| < \infty$.*

Proof. Consider the measure on $\mathbb{R}$

$$\nu = \sum_{n \ge 1} \frac{a_n}{n} \, \delta_{\log n}.$$

It is translation bounded: the total variation on every interval of length one is bounded by a constant depending only on $\sup_n |a_n|$. In particular, it defines a tempered distribution. We use the Fourier convention $\widehat{K}(t) = \int_{\mathbb{R}} K(x) e^{-itx} \, dx$. For $\sigma > 0$, the Fourier transform of $e^{-\sigma x} \nu$ is $F(1 + \sigma + it)$. Since ν is supported on $[0, \infty)$, domination against Schwartz functions gives $e^{-\sigma x} \nu \to \nu$ in tempered distributions. Passing to the limit $\sigma \downarrow 0$ shows that $\widehat{\nu}$ agrees, near $t = 0$, with the smooth function supplied by the continuation of $F(1 + it)$.

Choose $\widehat{K} \in C_c^\infty(\mathbb{R})$ with support in that neighbourhood and $\widehat{K}(0) = 1$. Its inverse Fourier transform K is a Schwartz function and $\int_{\mathbb{R}} K = 1$. Moreover

$$\widehat{K * \nu}(t) = \widehat{K}(t) F(1 + it)$$

is smooth and compactly supported, so $K * \nu$ is itself Schwartz. For any bounded interval I, Fubini's theorem gives

$$\int_I (K * \nu)(x)\, dx = \int_{\mathbb{R}} K(t) \nu(I - t)\, dt.$$

Translation boundedness implies $|\nu(I) - \nu(I - t)| \ll 1 + |t|$, uniformly in I: translating an interval changes only two boundary intervals. Consequently

$$\left| \nu(I) - \int_I (K * \nu)(x)\, dx \right| \ll \int_{\mathbb{R}} (1 + |t|) |K(t)|\, dt.$$

The integral of $K * \nu$ over I is bounded by its L^1 norm. Taking $I = (\log U, \log V]$ proves the assertion. □

For the relation to [16, Theorem 3.1], put $S(t) = \sum_{n \le e^t} a_n/n$ and $\tau(t) = S(t) - F(1)$ for $t \ge 0$, where $F(1)$ is the value of the continuation, and extend τ by zero to $t < 0$. Bounded coefficients give $|S(t + h) - S(t)| \ll 1 + h$ for $h \ge 0$, so the real and imaginary parts of τ are boundedly decreasing. Its Laplace transform is

$$\int_0^\infty \tau(t) e^{-zt}\, dt = \frac{F(1 + z) - F(1)}{z}, \qquad \Re z > 0.$$

Local holomorphy of F makes the singularity at $z = 0$ removable, which implies the local boundary condition of that theorem. Its conclusion $\tau(t) = O(1)$ gives the same bounded primitive.

Proof of Theorem 6.4. Corollary 6.3 transfers the assumed continuation of Z_μ to $\mathcal{D}_C$. Apply Lemma 6.5 to $a_n = C(n)$ and divide (6.6) by $H(U, V)$. □

Congruence restrictions. For a fixed $q \ge 1$ and $a \in \mathbb{Z}$, the corresponding field series is obtained by restricting (6.3) to $(m - 3)/6 \equiv a \pmod q$, with m as in (6.1). The proof of Theorem 6.2 applies term by term on that class, and local holomorphic continuation of its signed field series would give a bounded harmonic primitive on the class. The assumption of Theorem 6.4 concerns only the unrestricted series. Its local continuation at 1 remains open.

An unconditional bound on the real axis. For the same $C(n)$, Pouly [21] proves that on every fixed residue class the limsup of the absolute normalised harmonic average on windows of divergent mass is at most $B = 196567331/402653184$. In particular, taking $q = 1$, for every $\varepsilon > 0$ the initial sums $S(x) = \sum_{n \le x} C(n)/n$ satisfy $|S(x)| \le (B + \varepsilon) \log x + O_\varepsilon(1)$. For $t > 0$, Abel summation gives

$$t\, \mathcal{D}_C(1 + t) = t^2 \int_1^\infty S(x) x^{-1-t}\, dx.$$

Since $t^2 \int_1^\infty (\log x) x^{-1-t}\, dx = 1$, this bounds the limsup of the left-hand side in absolute value by B. The two comparisons in Theorem 6.2, together with $t\zeta(1 + t) \to 1$, now give

$$\limsup_{\sigma \downarrow 1} \frac{|Z_\mu(\sigma)|}{Z_+(\sigma)} \le B.$$

This estimate uses only values at real $\sigma > 1$.

If Z_μ admits a meromorphic continuation near 1, then $|Z_\mu(\sigma)| \le Z_+(\sigma)$ for real $\sigma > 1$ bounds any pole at 1 to order one. Writing $r = \operatorname{Res}_{s=1} Z_\mu(s)$, we obtain $|\sqrt{18}\, r| \le B$. The function $\mathcal{D}_C(s) - \sqrt{18}\, r\, \zeta(s)$ is then holomorphic near 1. Lemma 6.5 applied to $a_n = C(n) - \sqrt{18}\, r$ gives, uniformly for $1 \le U < V$,

$$\sum_{U < n \le V} \frac{C(n)}{n} = \sqrt{18}\, r\, H(U, V) + O(1).$$

A Computational checks and reproducibility

The source archive for this article is available on Zenodo at https://doi.org/10.5281/zenodo.24443299. It contains the LaTeX source, bibliography, exact-arithmetic programs, their recorded outputs and instructions for reproducing them. The computations check the following finite instances of the proofs.

The program `checks/gram.py` checks the factorisation of (2.16) on five composite moduli, including prime powers, for all frequencies $-7 \le h, l \le 7$. It also verifies the local probabilities $1/2$ and $1/4$ and the Chinese remainder lifting formula used to construct $u = 1 + mj$. The program `checks/roots.py` compares the exact minimum $K_*(n)$ obtained by root enumeration with a direct search over slopes for $1 \le n < 240$. It checks the corresponding small roots and the universal identity (1.1).

The program `checks/pell.py`, run with bound 20 000, checks the Pell identity, the evenness of s_n, and the local spacing of repeated squarefree kernels. It enumerates proper powers by the integral trace recurrence for both possible norms. It returns the ten exceptional indices

$$1,\ 2,\ 8,\ 16,\ 49,\ 288,\ 560,\ 1681,\ 9800,\ 19040.$$

This finite list is not used to prove the upper bound for $E(X)$. The discriminant formulas are also checked symbolically for each odd prime $\ell \le 31$ by `checks/discriminants.py`.

The classification of all cube indices in Proposition 4.4 imports the complete integral-point list of the specified elliptic curve from LMFDB. The complete integral-point computation has not been rerun for this article. Its source and the database's account of the computation are cited in the proof. The quantitative exceptional-set theorem needs only the finiteness of the fixed cubic case; its growing-degree argument is proved in Section 4.

AI assistance

OpenAI language models assisted with the mathematical arguments, bibliographic research, exact-arithmetic programs and manuscript preparation. The programs and their recorded outputs accompany the proofs.

References

[1] V. Crişan and P. Pollack, *The smallest root of a polynomial congruence*, Math. Res. Lett. **27** (2020), no. 1, 43–66. https://doi.org/10.4310/MRL.2020.v27.n1.a4. Author manuscript: https://www.pollack-math.net/smallroots5.pdf.

[2] E. Kowalski and K. Soundararajan, *Equidistribution from the Chinese Remainder Theorem*, Adv. Math. **385** (2021), article 107776. https://doi.org/10.1016/j.aim.2021.107776. Preprint version consulted: https://arxiv.org/abs/2003.12965v2.

[3] C. Dartyge and G. Martin, *Exponential sums with reducible polynomials*, Discrete Anal. (2019), paper no. 15, 31 pp. https://doi.org/10.19086/da.10793. Preprint version consulted: https://arxiv.org/abs/1802.09090v2.

[4] L. Alpöge, *Note on a theorem of Professor X.*, preprint (2021), arXiv:2109.14328v1. https://arxiv.org/abs/2109.14328v1.

[5] J.-H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. **75** (1984), no. 3, 561–584. https://doi.org/10.1007/BF01388644.

[6] The LMFDB Collaboration, *Elliptic curve with LMFDB label 216.a1 (Cremona label 216a1)*, The L-functions and Modular Forms Database, https://www.lmfdb.org/EllipticCurve/Q/216a1/, accessed 21 November 2026.

[7] J. Cremona and A. Sutherland, *Elliptic curves over $\mathbb{Q}$: Reliability*, The L-functions and Modular Forms Database, https://www.lmfdb.org/knowledge/show/rcs.rigor.ec.q, accessed 21 November 2026.

[8] S. R. Louboutin, *Fundamental units for orders generated by a unit*, Publ. Math. Besançon Algèbre Théorie Nr. (2015), 41–68. https://doi.org/10.5802/pmb.12.

[9] B. Pouly, *Arithmetic reconstruction and error recovery from three quadratic traces*, Hexagon preprint 2610.00353v1 (2026). https://hexagonmath.org/2610.00353v1. Archived deposit: https://doi.org/10.5281/zenodo.23317860.

[10] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940), 738–742. https://doi.org/10.2307/2371483. Author archive: https://users.renyi.hu/~p_erdos/1940-12.pdf.

[11] NIST Digital Library of Mathematical Functions, *Functions of number theory*, §27.11, equations 27.11.8 and 27.11.10, https://dlmf.nist.gov/27.11, accessed 21 November 2026.

[12] D. Andrica and V. Crişan, *The smallest nontrivial solution to $x^k \equiv 1 \pmod{n}$ and related sequences*, Amer. Math. Monthly **126** (2019), no. 2, 173–178. https://doi.org/10.1080/00029890.2019.1538402.

[13] G. Martin and S. Sitar, *Erdős–Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples*, Mathematika **57** (2011), no. 1, 1–29. https://doi.org/10.1112/S0025579310001580. Preprint version consulted: https://arxiv.org/abs/0903.1834v1, Theorem 1.4.

[14] E. Kowalski and K. Soundararajan, *Exponential sums, twisted multiplicativity, and moments*, in *Analysis at Large: Dedicated to the Life and Work of Jean Bourgain*, A. Avila, M. Th. Rassias and Y. Sinai (eds.), Springer, Cham, 2022, 299–332. https://doi.org/10.1007/978-3-031-05331-3_13. Author manuscript: https://people.math.ethz.ch/~kowalski/exp-sums.pdf, Theorem 1.5 and Remark 1.6.

[15] G. Gras, *Unlimited lists of quadratic integers of given norm—application to some arithmetic properties*, Commun. Adv. Math. Sci. **6** (2023), no. 3, 148–176. https://doi.org/10.33434/cams.1327372. Theorem 4.2, Corollary 4.3 and §5.2.

[16] G. Debruyne and J. Vindas, *Complex Tauberian theorems for Laplace transforms with local pseudofunction boundary behavior*, J. Anal. Math. **138** (2019), no. 2, 799–833. https://doi.org/10.1007/s11854-019-0045-3. Preprint version consulted: https://arxiv.org/abs/1604.05069v2, Theorem 3.1.

[17] H. Yokoi, *On real quadratic fields containing units with norm -1*, Nagoya Math. J. **33** (1968), 139–152. https://doi.org/10.1017/S0027763000012939. Lemma 2, p. 142.

[18] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97. https://doi.org/10.1007/BF02941943.

[19] P. Borwein, S. K. K. Choi and H. Ganguli, *Sign changes of the Liouville function on quadratics*, Canad. Math. Bull. **56** (2013), no. 2, 251–257. https://doi.org/10.4153/CMB-2011-166-9.

[20] Y. Diao, *On the average of class numbers of indefinite binary quadratic forms*, preprint (2026), arXiv:2610.28001. https://arxiv.org/abs/2610.28001.

[21] B. Pouly, *An explicit bound below one half for a quartic Liouville correlation*, preprint (2026). https://doi.org/10.5281/zenodo.24443184.

[22] B. Pouly, *Simultaneous quadratic probes: reconstruction thresholds and marked Poisson limits*, preprint (2026). https://doi.org/10.5281/zenodo.24443281.