The cube-root-of-two field in Alpöge's norm-prime estimate

Research checkpoint, 24 November 2026

The objective is RH for $K = \mathbb{Q}(\sqrt[3]{2})$. Its new factor is the degree-two Artin L-function of conductor 108. Write $k = \mathbb{Q}(\sqrt{-3})$ and $E = k(\sqrt[3]{2})$. We specialize one pinned source theorem by hand and determine how much stronger a prime estimate would have to be to give RH.

1. Replacing the large-discriminant hypothesis

For primes $q > 3$, three solutions of $z^3 = 2 \bmod q$ are equivalent to $q = a^2 + 27b^2$. This is the classical ring class field criterion. Choose the sign of a so $a = 1 \bmod 3$. Since a, b have opposite parity, $6 \mid a - 1 - 3b$. Then $A = 2a, B = 6b$ satisfy both divisibilities in `NormOne 3 6 q`. Conversely $6 \mid B$ forces A even in $4q = A^2 + 3B^2$, giving the representation. See Cox, §9, Proposition 9.5 and its corollaries.

Put $\omega = (-1+\sqrt{-3})/2$ and $\mathcal{O} = \mathbb{Z}[\omega]$. Each integral ideal prime to 6 has a unique generator congruent to 1 modulo $3\mathcal{O}$: the ring is norm-Euclidean and its six units have six distinct images in $(\mathcal{O}/3\mathcal{O})^\times$, a group of order six. Two such generators represent the same ray class modulo $6\mathcal{O}$ precisely when they agree modulo 2. Indeed, their ratio is already 1 modulo 3 locally, and any unit preserving this last condition is 1. Since $\mathcal{O}/2\mathcal{O} = \mathbb{F}_4$, CRT gives three classes. The coordinates of $a + b\omega$ modulo 6 can be represented by $(a, b) = (1, 0), (4, 3), (1, 3)$; their reductions modulo 2 are respectively $1, \omega, \omega^2$.

For any of these representatives, the norms in the class, with ideal multiplicity, are given by one polynomial on $(u, v) \in \mathbb{Z}^2$:

$$(a + 6u)^2 - (a + 6u)(b + 6v) + (b + 6v)^2 = 36\left(u + \frac{2a - b}{12} - \frac{v}{2}\right)^2 + 27\left(v + \frac{b}{6}\right)^2.$$

This is the source's `qForm` with $\alpha = 36, \gamma = 27, l = -1/2$; $\alpha\gamma = 972 = 3 \cdot 6^4/4$. Its values are positive integers. This gives the conclusion of the shifted-form input in our case. In particular the pinned count and theta estimate apply directly. If $a_g(n)$ counts ideals as above in class g of norm n, and $\kappa = \pi/(18\sqrt{3})$, they give

$$\left|\sum_{n \le X} a_g(n) - \kappa X\right| \le 10\sqrt{X} \qquad (X \ge 1),$$

$$\left|\sum_{n \ge 1} a_g(n) e^{-tn} - \kappa/t\right| \le \kappa(36^2 + 27^2 + 36^2 27^2 t^2)t \le 432^{10} t \qquad (0 < t \le 1).$$

As a finite check, we independently formed the ideal Euler products through norm 10,000: a rational prime $q > 3$ inert in k gives one trivial class at norm q^2; a split prime gives either two trivial classes or the two opposite nontrivial classes, by the cubic residue test. Every coefficient matched the lattice enumeration. The three cumulative ideal counts were $1013, 1007, 1007$.

2. Transfer through the prime-counting lemma

The outer proof uses $100 \le d$ to obtain a ray family at line 106. In the constructor, lines 82–83 request its two arithmetic inputs. Section 1 supplies the lattice estimates. The prime-power input discards $100 \le d$ when introducing its variables at line 136. Here a prime-norm ideal of trivial ray class has a generator congruent to 1 modulo 6, which also verifies its norm condition directly.

More explicitly, $\lambda_g(n)$ sums ideal von Mangoldt weights at norm n in ray class g, omitting ideals over 2 and 3. These weights are nonnegative and sum over classes to at most $2\Lambda(n)$, by the quadratic Euler factors. Unique ideal factorization gives the convolution of λ with a equal to $a_g(n)\log n$. The `LFam.sq` field only tests characters whose square is trivial. On the ray group of order three only the trivial character qualifies. With $A(n) = \sum_g a_g(n)$, $(A * A)(n)$ is nonnegative and $(A * A)(n^2) \ge A(n)^2 \ge A(n)$ for $n \ge 1$, using the pair (n, n). At zero both sides vanish. The family parameter is $B_0 = 4 \cdot 3 \cdot 6^2 = 432$; $1/B_0 \le \kappa \le 4$, the group order is at most B_0, and the unique norm-one ideal is trivial. This checks the remaining fields.

Applying the abstract short-interval lower bound and removing higher prime powers now gives constants $c, C > 0$ such that for all sufficiently large X

$$\#\{X < q \le (1+h)X : q \text{ prime splitting completely in } E\} \ \ge ChX/\log X, \qquad e^{-c\sqrt{\log X}} \le h \le 1.$$

Since B_0 is fixed, the source condition on $\log B_0$ holds eventually. This removes the field restriction in this application.

Comparison with existing work. Write $\Theta(X) = \sum_{q \le X,\ q \text{ split completely in } E} \log q$, excluding ramified primes, and let Ψ_E count prime ideal powers with their von Mangoldt weights. Then

$$0 \le \Psi_E(X) - 6\Theta(X) \ll_E \sqrt{X}.$$

In this Galois extension, unramified prime ideals of rational prime norm occur only over completely split primes. The remaining unramified terms contribute at most $6\log q$ per rational prime power q^j, $j \ge 2$. Chebyshev's bound gives $\sum_{j\ge 2} \sum_{q \le X^{1/j}} \log q \ll \sqrt{X}$; the two ramified primes cost $O(\log X)$.

For the standard representation ρ of S_3, Artin factorization gives $\zeta_E = \zeta L(\chi_{-3})L(\rho)^2$ and $\zeta_K = \zeta L(\rho)$. The public 7/8 zero-free theorem covers all three factors. The fixed-field truncated explicit formula then gives $\Psi_E(X) = X + O_E(X^{7/8}\log^2 X)$. Indeed take a good height of order X at a half-integer endpoint and bound the zero sum using $\sum_{|\Im\rho'| \le T} 1/|\rho'| \ll_E \log^2 T$; changing the endpoint by at most one costs $O_E(\log(2X))$. See the prime ideal explicit formula. In particular intervals of length $X^{9/10}$ already have $(1/6 + o(1))X^{9/10}/\log X$ completely split primes. These intervals are eventually shorter than the shortest ones in the source specialization.

3. The precision a one-sided estimate would need

Suppose for every $\epsilon > 0$ that $6\Theta(X) \geq X - O_\epsilon(X^{1/2+\epsilon})$ for all sufficiently large X. Fix $1/2 < \beta < 1$. For suitable C the function $g(X) = \Psi_E(X) - X + CX^\beta$ is eventually nonnegative. Its Mellin transform $\int_1^\infty g(x)x^{-s-1}\,dx$ on $\Re s > 1$ is

$$-\frac{\zeta_E'(s)}{s\zeta_E(s)} - \frac{1}{s-1} + \frac{C}{s-\beta}.$$

The apparent pole at 1 cancels. A zero with $\Re\rho' > \beta$ would force the abscissa of convergence σ_0 of the integral to be at least $\Re\rho'$. Landau's theorem for Mellin integrals of one sign requires a real singularity at σ_0. The only possible one is a real zero of ζ_E, producing a simple pole of residue $-\operatorname{ord}_{\sigma_0}(\zeta_E)/\sigma_0 < 0$. This would send the transform to $-\infty$ from the right. Its tail is nonnegative and its initial integral stays bounded, so this is impossible. Let $\beta \downarrow 1/2$ and use the functional equation. This proves RH for E, hence for K. Conversely RH for E gives the stated lower bound by the explicit formula. Given Dirichlet GRH, RH for K and for E are equivalent by the displayed factorizations.

Where the geometric comparison must change. Alpöge's `ch_core` uses characters of an abelian group. Over $\mathbb{Q}$, every one-dimensional character of S_3 agrees on the identity and a three-cycle. The cubic trace takes 2 and -1 there. Passing to arbitrary rational congruences cannot give an exact selector either: for every fixed modulus m, put $D = \mathbb{Q}(\zeta_{\operatorname{lcm}(m,3)})$. Since the maximal abelian subfield of E is k, $D \cap E = k$. In the compositum, the elements restricting to the identity on D restrict on E to all three elements of $\mathrm{Gal}(E/k)$. Chebotarev gives both splitting types even among the primes congruent to 1 modulo $\operatorname{lcm}(m, 3)$.

The local data also prevent using $E/\mathbb{Q}$ as the host with $d = 3$: the pinned `HostFactsS.inertia_d` requires inertia of order two. At 3 the ramification index in E is divisible by three from K (the shift $(t-1)^3 - 2$ is Eisenstein) and by two from k. It is therefore six. Omitting the Euler factor at 3 does not change the inertia group in the geometric hypothesis.

Over k, define $\Psi_j(X) = \sum_{n \leq X} \lambda_j(n)$ for the three ray classes from section 1, with $j = 0$ the principal class. Conjugation interchanges the two nontrivial classes, so $\Psi_1(X) = \Psi_2(X)$ identically. Either cubic character has the same weighted sum $\Psi_0(X) - \Psi_1(X)$. Moreover $\Psi_0(X) = 2\Theta(X) + O(\sqrt{X})$ by separating rational prime norms from higher prime powers. Under Dirichlet GRH, $\sum_j \Psi_j(X) = X + O(\sqrt{X}\log^2 X)$ from $\zeta_k = \zeta L(\chi_{-3})$ and removing the two Euler places. Hence a geometric upper bound $\Psi_1(X) - \Psi_0(X) \ll_\epsilon X^{1/2+\epsilon}$ would suffice. The lattice estimate of section 1 concerns $a_j(n)$, whereas this bound requires the weights $\lambda_j(n)$. We obtained no such bound.

Priority and verification. In addition to the public 7/8 theorem, a Hecke-family extension reports 10499/12000. The Masullo formalization records an open step in its critical-line claim. This search did not establish priority or turn up a complete proof for the fixed field. The specialization and implications here are hand deductions from the linked sources; the upstream Lean builds were not replayed.