A geometric test for the cubic prime discrepancy

Research checkpoint for $\mathbb{Q}(\sqrt[3]{2})$, 24 November 2026

Let $\mathcal{B}$ be the primes $q > 3$ for which $x^3 = 2 \bmod q$ has no root, and put $\vartheta_{\mathcal{B}}(X) = \sum_{q \in \mathcal{B},\ q \le X} \log q$. We construct one rational formal series whose denominator primes through degree N are exactly $\mathcal{B} \cap [5, N]$, omitting 2 and 3. Its ordinary common denominator grows too fast to supply the desired upper bound on the product of the distinct primes. All deductions here are by hand.

Why look at an elliptic curve with extra structure? The one-dimensional characters used by Alpöge's `ch_core` cannot distinguish the identity from a three-cycle in S_3. More generally, let $F/\mathbb{Q}$ be any fixed Galois CM field and let $S = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. Complex conjugation is central in $\mathrm{Gal}(F/\mathbb{Q})$, but its image in $\mathrm{Gal}(S/\mathbb{Q}) = S_3$ is a transposition, which is not central. Thus S is not contained in F. The normal subfield $F \cap S$ lies in $\mathbb{Q}(\sqrt{-3})$. Even among primes splitting completely in F, Chebotarev applied to FS produces both identity and three-cycle Frobenius in S. This argument concerns a fixed host. Finite level structures on a CM elliptic curve can carry the missing action: the three nonzero 2-torsion points of $y^2 = x^3 - 2$ have x-coordinates the three roots. Alpöge's local comparison gives valuations of jets at selected inert primes. The following test uses two cubic twists and computes their local integrality directly. Geometric gain in the original construction, pp. 49–50; Honda on formal groups and zeta functions.

Formal comparison. For $D = 1, 4$ let $C_D : y^2 = x^3 + D$. At infinity write $x = t^{-2}$, $y = -t^{-3}\sqrt{1 + Dt^6}$. The usual parameter $-x/y$ is $t/\sqrt{1 + Dt^6}$, an invertible integral change of parameter at every $q > 3$. The invariant differential is $dt/\sqrt{1 + Dt^6}$. Its integral with constant term zero is the formal logarithm

$$\ell_D(t) = \sum_{j \ge 0} \frac{(-1)^j \binom{2j}{j} D^j}{4^j (6j + 1)}\, t^{6j+1}.$$

Let $h(t) = \ell_4^{-1}(\ell_1(t)) = \sum h_n t^n$, where the inverse is for composition. For $\alpha^3 = 2$ one has

$$h(t) = \alpha^{-1}[\alpha](t), \qquad [z](t) := \ell_1^{-1}(z\ell_1(t)).$$

Indeed $\ell_4(t) = \ell_1(\alpha t)/\alpha$ because $\alpha^6 = 4$. The coefficients h_n are rational by the definition over $\mathbb{Q}$.

If $x^3 = 2 \bmod q$ has a root, it lifts by Hensel to a unit $\alpha \in \mathbb{Z}_q$. For $m \ge 0$ an integer, $[m]$ is multiplication by m on the integral formal group of C_1. In each degree its coefficient is a polynomial in m over $\mathbb{Q}_q$. Taking integers converging q-adically to α shows $h_n \in \mathbb{Z}_q$ for every n. This includes the primes with exactly one cube root.

First bad degree and exact support. At every $q > 3$, ℓ_D and its compositional inverse are integral through degree $q-1$. In degree q, the equation $\ell_4(h) = \ell_1$ therefore gives

$$qh_q \equiv q[t^q](\ell_1 - \ell_4) \pmod{q}.$$

For $q \in \mathcal{B}$ we have $q \equiv 1 \bmod 6$. Put $j = (q-1)/6$. The right side is $(-1)^j 4^{-j}\binom{2j}{j}(1-4^j)$, nonzero: $2j < q$ and $4^j = 2^{(q-1)/3} \not\equiv 1 \bmod q$. Thus $v_q(h_q) = -1$. Set D_N equal to the prime-to-6 part of the least common multiple of the reduced denominators of $h_1, \ldots, h_N$, and $R_N = \mathrm{rad}(D_N)$. We have proved, for every $N \geq 1$,

$$\log R_N = \vartheta_{\mathcal{B}}(N).$$

All prime factors here are detected by the same formal map; one can compute it without prescribing prime signs or factoring $x^3 - 2$ at the primes.

What ordinary denominator estimates measure. For each $q \in \mathcal{B}$ and every $k \geq 1$ we obtain the exact value

$$-v_q(h_{q^k}) = v_q((q^k)!) = (q^k - 1)/(q-1).$$

Here are the details. In degree n, the coefficient of $[z]$ is a polynomial in z of degree at most n, integer-valued on the nonnegative integers over $\mathbb{Z}_q$. Its finite differences at 0 are integral, so its binomial polynomial expansion has integral coefficients. Multiplication by $n!$ clears all polynomial denominators. Evaluation at the algebraic integer α, a unit at q, gives $v_q(h_n) \geq -v_q(n!)$.

For equality, the case $k = 1$ was established above. At $n = q^k$, $k \geq 2$, use $\ell_4(h) = \ell_1$ and put $c_m = [t^m]\ell_4$; $v_q(c_m) \geq -v_q(m)$. In a product $c_m h_{n_1} \cdots h_{n_m}$ with $m \geq 2$, $\sum n_i = n$, the excess of $v_q(n!)$ over $\sum_i v_q(n_i!)$ is $(\sum_i s_q(n_i) - 1)/(q-1)$, with s_q the base-q digit sum. This positive integer is at least $(m-1)/(q-1)$. It exceeds $v_q(m)$ unless $m = q$: for $q \mid m$ with valuation one and $m > q$ this follows at once, and $(q^a - 1)/(q-1) > a$ for $a \geq 2$. At $m = q$ equality requires all digit sums to be one, hence all $n_i = q^{k-1}$, since these powers are at most q^{k-1} and have this average. The single term $c_q h_{q^{k-1}}^q$ has the extremal valuation by induction and $v_q(c_q) = -1$. The right-hand coefficient $[t^n]\ell_1$ has valuation at least $-k > -v_q(n!)$. There is no other term with which the extremal one can cancel.

Consequence for the size of D_N. Fix an integer J. For $1 \leq k \leq J$, use the disjoint ranges $N^{1/(k+1)} < q \leq N^{1/k}$. Each $q \in \mathcal{B}$ there contributes at least $q^{k-1} \log q$ to $\log D_N$. The three-cycles have density $1/3$, so partial summation of the fixed-field prime number theorem gives $(1/(3k) + o_k(1))N$ from the kth range. Consequently $\liminf_{N\to\infty} \log D_N/N \geq \frac{1}{3}\sum_{k\leq J} 1/k$. Letting J grow shows $\log D_N/N \longrightarrow +\infty$. In particular no ordinary common-denominator bound of the form $D_N \leq e^{CN}$ with fixed C can prove the required radical estimate.

Quantitative version using the existing zero-free region. The public 7/8 Hecke theorem and the fixed-field explicit formula give $\vartheta_{\mathcal{B}}(T) = T/3 + O(T^{7/8}\log^2(2T))$. Indeed $\vartheta_{\mathcal{B}}$ is the difference between the primes 1 mod 3 and the completely split primes, apart from ramification. For the latter use $6\Theta(T) = \Psi_S(T) + O(\sqrt{T})$ and the Artin factorization as in the first checkpoint. Partial summation, with $\theta = 7/8$, gives uniformly in $k \geq 1$ and $T \geq 2$

$$\sum_{q \leq T,\ q \in \mathcal{B}} q^{k-1}\log q = \frac{T^k}{3k} + O(T^{k-1+\theta}\log^2(2T)).$$

The integral error has factor $(k-1)/(k-1+\theta) \leq 1$. Set $J = \lfloor \log N/(16\log\log N)\rfloor$. For $k \leq J$ both endpoints in the disjoint ranges are at least $(\log N)^{15}$ for large N, so $kT^{-1/8}\log^2(2T) = o(1)$ uniformly there. This uses eventual decrease of $T^{-1/8}\log^2(2T)$. The lower-endpoint main term is at most $N^{-1/(k+1)}$ times the upper one. Summing yields

$$\log D_N \ \geq\ (1/3 - o(1))\, N\log\log N.$$

Consequence for the research question. Assuming Dirichlet GRH, the weighted count of primes 1 mod 3 is $N/2 + O(\sqrt{N}\log^2(2N))$. Such a prime $q > 3$ either splits completely or has no cube root of 2, giving

$$\Theta(N) = N/2 - \log R_N + O(\sqrt{N}\log^2(2N)).$$

Hence $\log R_N \leq N/3 + O_\epsilon(N^{1/2+\epsilon})$ for every $\epsilon > 0$ would imply RH for $\mathbb{Q}(\sqrt[3]{2})$ by the one-sided criterion from the first checkpoint. The existing 7/8 theorem gives $\log R_N = N/3 + O(N^{7/8}\log^2(2N))$. The new local computation separates the prime types exactly, but supplies no saving in that exponent. A comparison that already deducts or normalizes away higher local multiplicities is outside the obstruction for D_N.

Reproducible arithmetic and scope. The companion script `check_twist_denominators.py` computes $h = t\,g(t^6)$ from the independent recursion $(1+s)(g+6sg')^2 = 1 + 4sg^6$ with $g(0) = 1$, using rational arithmetic. Through degree 500 it checks every denominator against cube roots found by direct enumeration: all 30 rootless primes first occur in their own degree. The observed exponents at degrees $49, 343, 169, 361$ were respectively $8, 57, 14, 20$ at primes $7, 7, 13, 19$. Classical formal-group theory already relates local integrality to Frobenius; the priority of this particular calculation has not been established. The formal comparisons are mathematical proofs on paper, without a Lean replay.