Elliptic root numbers and a signed squarefree variance for a quartic Liouville correlation

Brice Pouly

Prepared with AI assistance

hexagon:2611.01201v1

Abstract

We compare the Liouville sign of $D(n) = n(n+1)(3n+1)(3n+2)$ with root numbers in a non-isotrivial family of elliptic curves. A local formula gives the exact density of agreement. One explicit prime parameter has 1276 digits. Under Dirichlet GRH a single prime below 10^{282} gives agreement above 99.9929039%. Unconditionally an explicit product of 417 curves, all with prime parameters at most 70 891, gives agreement above 99.9962654%. The signed masses of the positive even valuation strata can be recovered either from corrected twists at one fixed spectral point $0 < \Re s < 1/2$, using the full prime-indexed family of numerators, or from the logarithmic means of the uncorrected root numbers by averaging over primes. The latter also recovers the sum of the squared masses. The short-interval variance of the corrected twists has an explicit signed covariance form on the $\sqrt{H}$ scale. We determine its kernel, stability modulus and constrained minimum near bias 1/3. A bound of 0.01386 on the variance coefficient at index 29, or either of two tests on 512 signed means, would force the quartic bias below 1/3. Estimating these arithmetic means remains open. A joint law of marked valuations gives uniform comparison on short progressions.

1 The sign to be recovered

Let $\Omega(t)$ count the prime factors of t with multiplicity, and write

$$\lambda(t) = (-1)^{\Omega(t)}, \qquad D(n) = n(n+1)(3n+1)(3n+2), \qquad C(n) = \lambda(D(n)).$$

A multiplicative prime of an elliptic curve can contribute a minus sign to its functional equation. It contributes once, even when the specializing parameter is divisible by a high power of the prime. Removing a square factor leaves λ unchanged. A root number designed to follow $C(n)$ must therefore account for the primes at which one of the four linear factors has positive even valuation. Their rarity gives a good approximation. Their positions retain information about the signed mean that is lost when all n are averaged together.

There are two questions here. How often can the sign of one curve, chosen as a function of n, equal $C(n)$? And if one varies quadratic twists, which measurements suffice to recover the signed contributions separately? For the first question the error is a product of explicit local probabilities (Theorem 2.1). For the second the answer depends on how the twists are sampled. The entire prime-indexed family, evaluated at one fixed spectral point, determines the profile (Theorem 4.1). An additive interval of twists instead gives a quadratic form which loses exactly one coordinate (Theorems 5.1 and 7.1). That loss matters when using the form to bound a quartic mean.

We work with positive integer arguments. For $I = (U, V]$, $1 \le U < V$, let

$$\langle f \rangle_{I;a,q} = \frac{\sum_{n \in I,\, n \equiv a \ (q)} f(n)/n}{\sum_{n \in I,\, n \equiv a \ (q)} 1/n}.$$

An extraction is a subsequence of windows with $\log(V/U) \to \infty$ on which the bounded averages in use converge. A diagonal subsequence suffices for the countably many local conditions. Write $\langle f \rangle$ for the resulting limit with $q = 1$, and $c = \langle C \rangle$. Our arithmetic input is Theorem 1.1 of *An explicit bound below one half for a quartic Liouville correlation* (DOI `10.5281/zenodo.24443184`) [30]. For every fixed a, q it gives

$$\limsup_{\log(V/U)\to\infty} |\langle C \rangle_{I;a,q}| \;\le\; B, \qquad B = \frac{196567331}{402653184}. \tag{1}$$

There is no uniformity in a growing modulus in this use of the theorem. The agreement density in Theorem 2.1 does not use this bound. The estimate for the difference of signed means and the coordinate constraints in Section 3 do.

The relation between root numbers and Liouville signs, and the averaging of the remaining local corrections, have substantial precedents. Rizzo's treatment of a one-parameter family already confines the defect of modified local factors to square divisors and controls their tail [31, §5, Theorems 18–19 and Proposition 26]. Helfgott isolates the Liouville factor from multiplicative reduction in [18, Theorem 6.6] and gives a general local averaging argument in [18, Proposition 7.7]. The construction here specifies the family, computes its ramified correction, and obtains the exact product (3). Since D splits into four affine forms, the required large-square estimate is elementary and unconditional.

Bettin, David and Delaunay realize every rational number in $[-1, 1]$ as the integer-parameter average root number of a non-isotrivial family [5, Theorem 3]. Our agreement density averages the product of a root number with the prescribed sign $C(n)$. It therefore measures how accurately the first sign follows the second. Estimating either sign's mean still requires information about its signed distribution.

The following comparisons refer to the same quartic sign. A density of agreement controls how often two signs differ. Bounding the bias of either sign requires a signed mean.

Observation	Parameters	What is known
One explicit curve	one specified 1276-digit prime	Agreement $> 99.99246539\%$, by a primality certificate and local factors.
One curve under GRH	one prime $r < 10^{282}$	Existence with agreement $> 99.9929039\%$. The prime is unspecified.
Product of curves	417 specified primes $\le 70\,891$	Agreement $> 99.9962654\%$. The finite list and the guarantee are unconditional.
Means of individual curves	512 specified primes from 6043 to 46 171	Two sufficient inequalities for $\lvert c\rvert < 1/3$. Their quadrature errors are certified. Their arithmetic inputs are open.

Section 2 derives the local signs and constructs the short parameters. Section 3 recovers the signed strata from the corrected twists and from the root numbers themselves. Theorem 3.3 gives the finite tests. At a fixed complex point, Section 4 recovers the same masses even after a set of prime indices of relative density zero is removed. A nonzero profile gives poles of full multiplicity at half a nontrivial zeta zero on a positive proportion of the indices. Sections 5–8 turn instead to additive intervals. They determine the signed covariance form, identify the coordinate lost by centering and minimize the form at a prescribed bias. Appendix A treats the local information available when the progression varies with the interval.

2 Agreement of an elliptic root number with the quartic sign

For a prime $r \equiv 19 \bmod 24$, put $\chi_r(a) = (a/r)$. For $t \ge 1$ set

$$z = 144rt, \qquad V = 1 + z^2, \qquad U = r^3 + 48rt + 24t^3, \qquad u = -U.$$

Write $W_r(t)$ for the global root number of

$$E_{r,t}: \quad y^2 = x^3 - 27u^2Vx + 54u^3V^2. \tag{2}$$

The choice of $1+z^2$ restricts its prime factors to 1 mod 4. The cubic U fixes the splitting sign at each prime of t away from $6r$. The possible error at r itself then has only one difficult valuation.

Theorem 2.1. *The natural density of $W_r(D(n)) = C(n)$, and its logarithmic density on every sequence of growing logarithmic windows, equal $(1+\gamma_r)/2$, where*

$$\gamma_r = \left(1 - \frac{4(r+2)}{r^2(r+1)}\right) \prod_{\substack{p>3 \\ \chi_r(p)=1}} \left(1 - \frac{8}{p(p+1)}\right). \tag{3}$$

On every extraction, $|c - \langle W_r(D)\rangle| \le B(1-\gamma_r)$. For $r = 991027$ the density exceeds 0.993840 and the mean error is below 0.00602. The explicit prime r_* in Proposition 2.3 gives density greater than 0.99992465 and mean error less than 0.000073565.

2.1 The pointwise calculation

Let $k = v_r(t)$, $t_0 = t/r^k$, $j = v_r(U)$, and set $J = 1$ for odd j, $J = \chi_r(U/r^j)$ for even j. Then

$$\frac{W_r(t)}{\lambda(t)} = \underbrace{(-1)^k \chi_r(t_0) J}_{\epsilon_r(t)} \prod_{\substack{p>3,\ \chi_r(p)=1 \\ 0<v_p(t)\ \text{even}}} (-1). \tag{4}$$

Indeed $c_4 = 6^4u^2V$, $c_6 = -6^6u^3V^2$, $\Delta = -2^6 3^9 u^6 V^3 z^2$. The invariant $j(E_{r,t}) = -1728/z^2$ varies with t. At its poles the splitting character has squareclass $-c_6$, equivalently u. The standard local root-number formulas, in *Root numbers and parity phenomena* [8, Theorem 2.3 and Corollary 2.4], give the following contributions.

Place	Local sign or product of local signs
Real place	-1
$2, 3$	$+1$ at each place
$p > 3,\ p \mid t,\ p \neq r$	$-(-r^3/p) = -\chi_r(p)$
$p \mid V$	$(2/p)^{v_p(V)}$, with product 1
$p \mid U,\ p \nmid rV$	$(-1/p)^{v_p(U)}$, with product $-(-1)^j$
r	-1 for odd j, $\chi_r(U/r^j)$ for even j

At $2, 3$, the valuations of $j(E)$ are negative and $u \equiv 5 \bmod 8$, $u \equiv 2 \bmod 3$ give the nontrivial unramified quadratic classes. At $p \mid V$ the discriminant valuation modulo 12 is $3v_p(V)+6v_p(u)$. The four potentially good types give the entry in the table since $(-1/p) = 1$. Their product is the Jacobi symbol $(2/V) = 1$. At a remaining prime of U, good reduction acquires the sign $(-1/p)$ under a ramified twist. As $U \equiv 3 \bmod 4$, the product away from r is as stated. Finally, the ramified potentially multiplicative sign at r is $(-1/r) = -1$. In the unramified case it is the negative of the splitting character. Multiplying gives $J \prod_{p>3,\, p\neq r,\, p\mid t}[-\chi_r(p)]$. Using $\chi_r(2) = \chi_r(3) = -1$ gives (4) with multiplicities restored.

For example, take $r = 163$. The first split prime above three is 41. At $n = 560$ one has $3n + 1 = 41^2$, hence a reversal at 41. Up to this point the other three forms are smaller than 41^2, except for $3n + 2 = 1682$ at the endpoint, and all four are smaller than 163^2. Below 560 every form is smaller than 41^2. Thus 560 is the first disagreement.

2.2 Local means and conditioning

Write $\mathbb{P}_p$ for Haar probability on $\mathbb{Z}_p$. The four roots $0, -1, -1/3, -2/3$ of D are simple and distinct for every $p > 3$. At each positive valuation the unit part is uniform on the units. This follows by lifting a simple root one digit at a time. In particular

$$\mathbb{P}_p(v_p(D) = a) = 4(1 - p^{-1})p^{-a} \quad (a \geq 1), \qquad \delta_p = \mathbb{P}_p(0 < v_p(D) \text{ even}) = \frac{4}{p(p+1)}. \quad (5)$$

For $k = 0, 1$, reduction of U, respectively U/r^2, in (4) gives $\epsilon_r = 1$ pointwise. For $k \geq 3$, $j = 3$, and the unit average of ϵ_r is zero. For $k = 2$ put $P(t_0) = U/r^3 = 1 + 48t_0 + 24r^3t_0^3$. Its simple root modulo r is the square unit $-1/48$. Off that residue the contribution to the full unit mean is $-1/(r-1)$. On it P is uniform on $r\mathbb{Z}_r$. An odd positive $v_r(P)$ leaves a fair unit character in J. An even positive $v_r(P)$ gives $J = 1$ and contributes $1/(r^2-1)$ to the full unit mean. Thus the conditional mean at $k = 2$ is $-r/(r^2-1)$. In particular the loss in the ramified factor is

$$(1 + r/(r^2-1))\mathbb{P}_r(k = 2) + \mathbb{P}_r(k \geq 3) = \left(1 + \frac{r}{r^2-1}\right)\frac{4(r-1)}{r^3} + \frac{4}{r^3} = \frac{4(r+2)}{r^2(r+1)}.$$

At a split prime the factor in (4) has mean $1 - 2\delta_p$. Independence for finitely many primes follows from the Chinese remainder theorem after truncating p-adic precision. The measure-zero roots in the ramified factor introduce no boundary term. For $p > y \geq r$, disagreement requires p^2 to divide one of four injective affine forms taking values in $[1, 3X+2]$ on $1 \leq n \leq X$. The count is at most $4\sum_{p>y}\lfloor(3X+2)/p^2\rfloor \ll X/y$. Partial summation gives the same limiting tail on logarithmic windows.

This proves the product in Theorem 2.1. If E is the set of disagreement, its cylinder approximations and (1) give $|\langle C\mathbf{1}_E\rangle| \leq B\mathbb{P}(E)$. Since $C - W_r(D) = 2C\mathbf{1}_E$ and $2\mathbb{P}(E) = 1 - \gamma_r$, this also proves the mean estimate. The same argument on a specified class gives the following conditional version.

Proposition 2.2. *On a fixed progression $a \bmod q$, the agreement density is $(1 + \gamma_r(a;q))/2$ and the corresponding absolute logarithmic mean error is at most $B(1 - \gamma_r(a;q))$. Here $\gamma_r(a;q)$ is the product of the factors in (3), with each local expectation at $p \mid q$ replaced by its expectation on $x \in a + p^{v_p(q)}\mathbb{Z}_p$, with $t = D(x)$. For a fixed r, the infimum and supremum of these densities over fixed progressions are 0 and 1.*

Proof. On a split prime ball of precision $m = v_p(q) \geq 1$, if $p^m \nmid D(a)$ the valuation is fixed. Otherwise the conditional probability of a positive even valuation is $p/(p+1)$ for even m, and $1/(p+1)$ for odd m, by lifting the root. At r one integrates $\epsilon_r(D(x))$ from (4) on the indicated ball. The tail count above incurs at most the fixed factor q under conditioning, and (1) applies on all refinements. To see the two extremes, avoid the four roots at r and at all split primes up to y. This forces sign $+1$ at those places. To force sign -1, prescribe valuation exactly two at one fixed split prime instead. The Chinese remainder theorem gives a class in each case. The product of the untouched factors tends to one as $y \to \infty$. □

2.3 An explicit parameter

Dirichlet's theorem gives parameters with γ_r arbitrarily close to one by prescribing nonsplitting at all small primes and then taking r large. A numerical statement for a *specified* curve requires a prime representative and control of the remaining product.

Proposition 2.3. *Let $Y = 3000$, $F = 3\prod_{7\leq p\leq Y,\ p\equiv 3\ (4)} p$, and $M = 4\prod_{5\leq p\leq Y,\ p\equiv 1\ (4)} p$, with products over primes. For $p \mid M$, $p > 2$, let ν_p be the least positive quadratic nonresidue. Take the unique $0 \leq h < M$ satisfying*

$$(F/3)h \equiv 3 \pmod 4, \qquad 1 + 2Fh \equiv \nu_p \pmod p \quad (p \mid M,\ p > 2).$$

The prime $r_* = 1 + 2F(h + 14M)$ *has* 1276 *decimal digits. Its first split prime above three is* 3023*, and its agreement density lies between* 0.9999246539 *and* 0.9999266537*.*

Proof. The class gives $r_* \equiv 19 \bmod 24$. For primes $p \mid F,\ p > 3$ one has $(-r_*/p) = (-1/p) = -1$. At the odd primes of M the chosen nonresidue gives the same value. Reciprocity identifies this with $\chi_{r_*}(p)$ once primality is established. The certificate checks $F^2 > r_*$ and, for each of the 218 prime factors s of F, the single base $b = 2$ with

$$b^{r_*-1} \equiv 1 \bmod r_*, \qquad \gcd(b^{(r_*-1)/s} - 1, r_*) = 1.$$

For every prime divisor l of r_* the order of the relevant base modulo l forces $s \mid l - 1$. Hence $F \mid l - 1$, which rules out a prime divisor at most $\sqrt{r_*}$. This is the squarefree-factor case of Pocklington's criterion [29]. Directed integer products up to $P = 2 \cdot 10^6$, with mesh 10^{-25}, and $\prod_{p>P}(1 - 8/[p(p+1)]) \geq 1 - 8/(P+1)$ give the displayed interval. For 991027 the same computation with $P = 2 \cdot 10^7$ and mesh 10^{-22} proves Theorem 2.1's smaller-parameter figures. All quantities in these tests are integers or rationals. □

2.4 How small can one prime parameter be?

Let $d_r = (1 - \gamma_r)/2$. In Proposition 2.3 every local sign up to a cutoff was prescribed. For the next result we prescribe the first signs and average the remaining losses. The small-prime input goes back to Ankeny's GRH bound for a quadratic nonresidue [1] and Bach's explicit bounds for a prime outside a subgroup [2]. We use the estimates for primes in cosets of Lamzouri, Li and Soundararajan [21, 22]. The local cost assigned to the signs is given by (3).

Theorem 2.4. *Assume GRH for Dirichlet L-functions. There exists a prime* $r \equiv 19 \bmod 24$*,* $r < 10^{282}$*, for which* $d_r < 0.000070961$*. In particular the agreement exceeds* 99.9929039%*.*

Proof. Take $Y = 3163,\ Z = 20\,000\,000,\ x = 10^{282}$. Put $Q = 24\prod_{5\leq p\leq Y} p$, all products indexed by p here running over primes. The units $a \bmod Q$ with $a \equiv 19 \bmod 24$ and $(-a/p) = -1$ for every $5 \leq p \leq Y$ form one coset A of index $h = 8 \cdot 2^{445} = 2^{448}$. For $q = Q$ or Qp with $Y < p \leq Z$, write $S(x, \psi) = \sum_{m\leq x} \Lambda(m)\psi(m)\log(x/m)$. Uniformly for characters modulo these q,

$$|S(x, \psi) - \mathbf{1}_{\psi \text{ principal}} x| < 5000\sqrt{x}. \tag{6}$$

Here are the margins in the imported estimate. The products give $Q < 2^{4430}$, $QZ < 2^{4455}$, $\log q < 3150,\ \log x < 700,\ \omega(q) \leq 450$, and $2h \log q < \sqrt{x}$. For the principal character use (4.3) of [21], with error at most $\sqrt{x}/20 + \omega(q)(\log x)^2/2$. For the others use (4.8) and Lemma 2.4 there. The weighted sum of $\Lambda(n)/n$ occurring in (4.8) has absolute value at most $\log x$, by Lemma 2.4 applied to its positive majorant. The resulting first term is at most $(\sqrt{x} + 19/6)(3150 + 1400)$. The remaining logarithmic terms are less than 10^{10}, even on replacing $\log x$ by 700 and $\log \max(q/\pi, 2x)$ by 3151. This proves (6). Formula numbers refer to arXiv v3 of [21]. The authors identify the correction in [22] with Lemma 6.1 of the earlier version, concerning the asymptotic nonresidue estimates.

Give the primes $Z < r \leq x$ in A weights $\log r \log(x/r)$ of total mass M. The coset indicator is a sum of h characters with coefficients of modulus $1/h$. An even power of a unit is 1 mod 24, hence contributes nothing. There are fewer than 1400 possible exponents, and removing the other proper prime powers and the small primes costs at most $1400 \cdot 700^2 x^{1/3} + Z \cdot 700^2 < \sqrt{x}$. Thus $M \geq x/h - 5001\sqrt{x} > 0$. For a prime $Y < p \leq Z$, twisting the coset indicator by $(-r/p)$ leaves only nonprincipal characters modulo Qp. Its weighted sum has modulus at most $5001\sqrt{x}$, with the same exclusions. With $\alpha = 5001h/\sqrt{x} < 0.003635$, the probability of a plus sign is at most $1/(2(1 - \alpha))$.

Apply $1-\prod(1-a_i)\le\sum a_i$ to (3). The weighted mean of d_r is at most

$$\frac{2}{1-\alpha}\sum_{Y<p\le Z}\frac{1}{p(p+1)}+\frac{4}{Z+1}+\frac{4}{(Z+1)^2}.$$

The last two terms cover primes above Z and the ramified place r, respectively. With $D_0=10^{24}$, the sum of the ceilings $\lceil D_0/[p(p+1)]\rceil$ is 35251438649798916910. Substituting this upper sum divided by D_0 gives less than 0.000070961. At least one positive-weight prime satisfies the bound. Its value is unspecified. □

For comparison across accuracies, let $r(\xi)$ be the least eligible prime with $d_r\le\xi$. The same argument under GRH gives

$$\limsup_{\xi\downarrow0}\xi\log^2(1/\xi)\log r(\xi)\le 4\log 2.$$

Indeed, let $Y\to\infty$, $Z=Y^2$, $x=h^2Y^{10}$, $h=8\cdot2^{\pi(Y)-2}$. The smoothed character error divided by x/h is $O(h\log^2(QZx)/\sqrt{x})=o(1)$, as is the discarded prime-power mass on that scale. The prime number theorem gives $\sum_{p>Y}1/[p(p+1)]\sim1/(Y\log Y)$. The mean loss is thus at most $(2+o(1))/(Y\log Y)$. Take $Y\sim(2+\eta)/(\xi\log(1/\xi))$, use $\log x\sim(2\log2)Y/\log Y$, and then send $\eta\downarrow0$.

2.5 A product of curves with explicit small parameters

The price of requiring a single prime is that many prescribed signs must appear in one residue class. Under multiplication the signs of several primes can instead be assembled by linear algebra. For fixed $Y\ge13$ let S be a set of distinct primes $r>Y$, $r\equiv19\bmod24$, and put $U_S=\prod_{r\in S}r$. We require

$$|S|\text{ odd},\qquad(-U_S/p)=-1\quad(5\le p\le Y).\tag{7}$$

Write $R_S(n)=\prod_{r\in S}W_r(D(n))$. This is the root number of the product of the curves in (2).

Proposition 2.5. *Put $\sigma_p=\left(\frac{U_S/p}{p}\right)$ for $p\in S$, with integer numerator U_S/p. Under (7), the natural and logarithmic disagreement densities of R_S and C equal $d_S=(1-\Gamma_S)/2$, where*

$$\Gamma_S=\prod_{p\in S}\left(1-\frac{4}{p^2}-\frac{4\sigma_p}{p^2(p+1)}\right)\prod_{\substack{p>Y,\ p\notin S\\(-U_S/p)=1}}\left(1-\frac{8}{p(p+1)}\right).$$

There is an explicit set of 417 such primes at $Y=6000$, all at most 70 891, for which $d_S<0.000037345586$. On every fixed progression whose modulus has all prime factors at most Y, the same density holds and the difference of the logarithmic means has limit superior in absolute value at most $2Bd_S$. For this set the latter is less than 0.000036463.

Proof. Since $|S|$ is odd, (4) leaves a single factor C in R_S. If $p\notin S$ and $p>3$, the residual factor is $-(-U_S/p)$ at positive even valuations and 1 otherwise, by quadratic reciprocity. It is identically 1 up to Y. At $p\in S$, the other $|S|-1$ curves contribute σ_p at positive even valuations. The ramified factor has conditional mean $-p/(p^2-1)$ at valuation two and zero at each higher valuation, as computed above. Using (5), its product with the other curves therefore has mean $1-4/p^2-4\sigma_p/[p^2(p+1)]$. Approximation of the finitely many ramified factors by residue classes, CRT and the large-square tail in Section 2 give the product. Conditioning on a fixed Y-smooth modulus leaves all contributing local laws unchanged. Applying (1) on finite refinements to C times the disagreement indicator yields the stated bound for logarithmic means.

For the finite certificates use

$$d_S \le \sum_{p\in S} \frac{2(p+1+\sigma_p)}{p^2(p+1)} + 4 \sum_{\substack{p>Y,\ p\notin S\\ (-U_S/p)=1}} \frac{1}{p(p+1)}.$$

The source gives the prime lists. Sieving verifies primality, and modular exponentiation verifies every sign in (7). The summands through 2 000 000 are rounded up on the 10^{-24} grid. The remaining contribution is at most $4/2\,000\,001$. For the largest list the integer sums on that grid are 2223315117675981347 at the ramified primes and 33122271448209733569 elsewhere. This calculation gives the last row below without GRH.

Y	number of curves	largest prime	upper bound for d_S
3400	253	40 531	0.000063953722
4000	273	46 819	0.000055382659
6000	417	70 891	0.000037345586

□

There is also a general height bound for this construction under Dirichlet GRH. Write $m = \pi(Y) - 2$, $Q = 24\prod_{5\le p\le Y} p$. Attach to each eligible prime its vector

$$v(r) = \big(1, ((1-(-r/p))/2)_{5\le p\le Y}\big) \in \mathbb{F}_2^{m+1}.$$

If the span is proper, take a nonzero linear functional vanishing on it. Requiring the functional to be one, together with $r \equiv 19 \bmod 24$, selects a nonempty coset of index 16 if it uses any of the p-coordinates and index 8 otherwise. This follows from CRT and the independence of the local quadratic characters. Theorem 1.4 of [21] supplies a new prime at most $\max\{10^9, (15\log Q + 51 + \frac{5}{2}(\log\log Q)^2)^2\}$. It is coprime to Q, hence exceeds Y. Repeating gives a basis, and writing the all-ones vector in it gives (7) with at most $m+1$ primes. The height is $O(Y^2)$ per prime. Since disagreement requires a square at a prime $p > Y$, one has $d_S \ll 1/(Y\log Y)$. Accuracy ξ can thus be attained with $O(1/(\xi\log^2(1/\xi)))$ curves of individual height $O(1/(\xi^2\log^2(1/\xi)))$.

Corollary 2.6 (Agreement on moving progressions)**.** *Fix S, Y as in Proposition 2.5, and let $L(X) \to \infty$. In $X < n \le X + H$, $0 < H \le X$, the ordinary disagreement frequency tends uniformly to d_S over all classes modulo Y-smooth q satisfying*

$$\frac{H}{q} \;\ge\; L(X)\frac{X^{1/3}}{(\log X)^{2/3}}.$$

In particular, on $X < n \le 2X$ the conclusion holds simultaneously for all such $q \le X^{2/3}$.

Proof. Choose a precision at the finitely many primes of S so that the ramified signs are determined away from cylinders of total Haar measure less than ε. Such cylinders exist because the signs are locally constant off the finitely many roots involved in the unit computations. Split the progression modulo the product of these fixed prime powers. It is coprime to q, so the cylinder frequencies have error $O_{S,\varepsilon}(q/H)$. On each refined class the unramified signs are a bounded test of the square valuations away from S. Let m be the fixed refining modulus and $N' = H/(qm)$. Every refined class has $\omega(qm) \le \pi(Y) + |S|$. For large X one has $N' \ge X^{1/3}/\log X$, so estimate (48) in the proof of Theorem A.1, with $k = 2$, applies there. Its second term is $O_{S,Y,m}(1/L(X))$, and its first tends to zero. The product law at all contributing primes outside S is unchanged. Summing over the refinements, then letting $\varepsilon \downarrow 0$, proves the assertion. This controls the unsigned frequency of disagreements. For moving moduli the resulting comparison of ordinary signed means costs $2d_S + o(1)$. □

3 Valuation strata and their signed means

Let $\mathcal{E}$ consist of the positive squarefree integers coprime to six, including 1. For $t \geq 1$ put

$$K(t) = \prod_{\substack{p>3 \\ 0<v_p(t) \text{ even}}} p, \qquad g_e = \langle C(n)\mathbf{1}_{K(D(n))=e} \rangle.$$

The number g_e is a signed mass, so division by the density μ_e of the stratum gives its conditional mean. The local probabilities (5), the square-divisor estimate, and (1) give

$$\begin{aligned} c = \sum_{e \in \mathcal{E}} g_e, \qquad |g_e| \leq B\mu_e, \qquad \mu_e = \mu_1 \prod_{p|e} t_p, \\ \mu_1 = \prod_{p>3} (1-\delta_p), \qquad t_p = \frac{\delta_p}{1-\delta_p} = \frac{4}{p(p+1)-4}. \end{aligned} \tag{8}$$

Indeed both the stratum and a finite union of strata can be approximated in density by unions of fixed progressions. The unsigned masses sum to one by the Euler product. Since $t_p \ll p^{-2}$, $\sum_e |g_e| e^a < \infty$ for every $a < 1$. For instance, knowing g_1 leaves the explicit bound $|c| \leq |g_1| + B(1-\mu_1)$, attained in the abstract box by putting all remaining strata at their bounds with a common sign aligned with g_1 when $g_1 \neq 0$. The product for μ_1 gives $1/3 - B(1-\mu_1) > 0.19461753$. This singles out one signed mass whose control would already suffice for a bias below one third.

The ordinary sample $8 \leq n < 16$ illustrates the loss of information in c. Its eight signs have sum zero. The signed counts on $K = 1$ and $K = 5$ are 1 and -1. A twist that assigns opposite weights to these two strata has a nonzero average on the sample.

Let μ denote the Möbius function and $\mathcal{U} = \{u \geq 1 : \mu^2(u) = 1,\ u \equiv 1 \bmod 24\}$. We shall vary the splitting class at all odd primes independently. For $e \in \mathcal{E}$ define

$$\chi_e(n) = \left(\frac{n}{e}\right), \qquad \widetilde{\chi}_e(n) = \prod_{p|e} \left(\frac{n/p^{v_p(n)}}{p}\right), \qquad F_u(e) = \mu(e)\widetilde{\chi}_e(u).$$

The Jacobi symbol modulo one is one. Removing the full power of p in the unit part keeps the last sign defined also when $p \mid u$. The observable below is a root number multiplied by explicit parity and unit-character factors. These corrections make all valuation strata visible, including those ramified in the twist.

Proposition 3.1. *Put $V' = 1 + (12t)^4$. For the curve $y^2 = x^3 - 27u^2V'x + 54u^3(V')^2$, denote its root number by $W'_u(t)$. If $t^{[u]}$ denotes the largest divisor of t coprime to u, then*

$$\underbrace{W'_u(t)\,(-1)^{1+v_2(t)+v_3(t)+\sum_{p|u} v_p(t)} \left(\frac{t^{[u]}}{u}\right) \prod_{p|(u,K(t))} \left[-\left(\frac{u/p}{p}\right)\right]}_{A_u(t)} = \lambda(t) F_u(K(t)). \tag{9}$$

Consequently the limiting means $m_u = \langle A_u(D(n)) \rangle$ satisfy

$$m_u = \sum_e g_e F_u(e), \qquad g_e = \mathbb{E}_{\mathcal{U}}[F_u(e) m_u], \qquad \mathbb{E}_{\mathcal{U}}|m_u|^2 = \sum_e g_e^2, \tag{10}$$

where $\mathbb{E}_{\mathcal{U}}$ is the limit of the uniform averages on $\mathcal{U} \cap [1, T]$ as $T \to \infty$.

Proof. At a pole of the invariant the splitting class is u. At $2, 3$ it is a square, giving local sign -1 at both places. Each prime of V' is 1 mod 8 (the order of $12t$ modulo that prime is eight). Its potentially good sign is positive even if it divides u. At the primes of u the ramified sign

away from V' is $(-1/p)$, also when $p \mid t$. The product over $p \mid u$ is one. Including the real sign now gives

$$W'_u(t) = -\prod_{\substack{p>3,\, p\mid t\\ p\nmid u}} \left[-\left(\frac{u}{p}\right)\right].$$

For $p \mid t,\ p \nmid 6u$, multiplying by the Jacobi symbol in (9) contributes $(u/p)^{v_p(t)}$ by reciprocity. Thus an odd valuation contributes -1, and a positive even one contributes $-(u/p)$. At $p \mid u$ the explicit parity and unit-character factors in (9) do the same job. The powers of $2, 3$ supply their own parity. This proves the pointwise identity and the first equality in (10).

For a finite set of primes $p > 3$, the residue vectors of u modulo p^2 have the product law uniform on all $p^2 - 1$ classes other than 0 mod p^2, conditional on $u \in \mathcal{U}$. This includes the classes $p \parallel u$, not only the units. The assertion follows by CRT for a bounded squarefree sieve and then the tail $\sum_{p>y} p^{-2}$. On both the unit classes and the classes $p \parallel u$, the Legendre character of the unit part has mean zero. These independent fair signs give $\mathbb{E}_{\mathcal{U}} F_u(e)F_u(f) = \mathbf{1}_{e=f}$. The two remaining assertions are the usual orthogonal inversion and Parseval identities for products of independent fair signs; absolute convergence permits their application to the full profile. □

For later use set $\mathrm{sf}(n) = \prod_{v_p(n) \text{ odd}} p$. Products of the signs obey $F_u(d)F_u(e) = F_u(\mathrm{sf}(de))$. In particular multiplication by $F_u(d)$ makes the term g_d constant. Both measurements below start by subtracting that constant. For comparison with the product in Proposition 2.5, the corrected signs in (9) obey a simpler multiplication rule. For an odd number of distinct primes $u_j \equiv 1 \bmod 24$, multiplicativity of the unit parts gives $\prod_j A_{u_j}(t) = A_{\prod_j u_j}(t)$. Prescribing $\left(\frac{\prod_j u_j}{p}\right) = -1$ for $5 \le p \le Y$ removes these small primes. The supplied list of 215 primes at $Y = 3400$, all at most 42409, has disagreement below 0.000068505308. At a prime dividing $u = \prod_j u_j$ the relevant local symbol is $\left(\frac{u/p}{p}\right)$, and at the other primes it is $\left(\frac{u}{p}\right)$. Each plus sign costs at most $4/[p(p+1)]$ in the disagreement bound. This calculation applies to the corrected observable A_u.

3.1 Recovering the signed masses from the root numbers themselves

The identity (10) uses an observable with explicit corrections at the primes of the twist parameter. We can also observe the root number $W_r(D(n))$ itself. Define

$$\Phi_r(e) = \mu(e)\left(\frac{e}{r}\right), \qquad M_r = \langle W_r(D)\rangle, \qquad F_r^0 = \sum_{e\in\mathcal{E}} g_e \Phi_r(e) \quad (r \text{ prime},\ r \equiv 19 \bmod 24).$$

We use uppercase M_r for these means. The m_u in (10) belong to the corrected family $u \equiv 1 \bmod 24$. For example, at $e = r$ the test $\Phi_r(e)$ vanishes, while the root number is always a sign. Pointwise, writing $K = K(D(n))$, (4) gives

$$|W_r(D(n)) - C(n)\Phi_r(K)| \le 2\mathbf{1}_{r^2\mid D(n)}. \tag{11}$$

Outside this event the ramified factor equals one and the remaining factors multiply to $\Phi_r(K)$. On a common logarithmic extraction take the limits for all e, r. The error in (11) has the form C times a bounded local function. Approximation by fixed congruence classes, as in Proposition 2.2, bounds its signed mean by B times its mean absolute value. The same argument applies to W_r/C. Hence

$$|M_r - F_r^0| \le 8B/r^2, \qquad |M_r|, |F_r^0| \le B. \tag{12}$$

Fix a nonnegative, nonzero $w \in C_c^\infty((1,2))$. Denote the average over primes $r \equiv 19 \bmod 24$ with weights $(\log r)w(r/R)$ by $\mathcal{A}_R$, normalized by their sum $Z_R \sim R\int w/8$.

Theorem 3.2 (Inversion for raw prime parameters)**.** *On each common logarithmic extraction, for every fixed $d \in \mathcal{E}$,*

$$\lim_{R\to\infty} \mathcal{A}_R \Phi_r(d) M_r = g_d, \qquad \lim_{R\to\infty} \mathcal{A}_R M_r^2 = \sum_{e\in\mathcal{E}} g_e^2 =: \mathcal{P}(g). \tag{13}$$

Under Dirichlet GRH the respective errors are $O_w(B\log(2d)/\sqrt{R})$ and $O_w(B^2/\sqrt{R})$. The squares in (13) *are taken after the logarithmic average in n.*

Proof. For $d, e \in \mathcal{E}$, reciprocity expresses $\Phi_r(d)\Phi_r(e)$ as a constant sign times the Jacobi symbol (r/de). When $d \neq e$ some prime above three has odd exponent in de, so the character stays nonprincipal when twisted by any character modulo 24. When $d = e$, the test equals one except at primes dividing d. The prime number theorem on fixed progressions therefore gives $\mathcal{A}_R \Phi_r(d)\Phi_r(e) \to \mathbf{1}_{d=e}$.

For the quantitative form, the smoothed explicit formula under GRH gives, for any character $\psi \bmod l$,

$$\sum_m \Lambda(m)\psi(m)w(m/R) = \mathbf{1}_{\psi \text{ principal}} R \int w + O_w(\sqrt{R}\log(2l)).$$

Indeed the Mellin transform of w decays faster than any inverse power in fixed strips. The zeros in each unit interval of ordinates number $O(\log(2l(2+|t|)))$. The functional equation bounds the integral on the line $\Re s = -1/2$, and the possible contribution at zero is $O_w(\log(2l))$ [19, Chapter 5]. An imprimitive character deletes powers of primes dividing l, of total weight $O_w(\log(2l))$ on one dyadic band. Proper prime powers on the full band cost $O_w(\sqrt{R})$ by Chebyshev's bound. Expand the residue class in the eight characters modulo 24. In the diagonal case the weight of $r \mid d$ is $O_w(\log(2d)/R)$. Consequently

$$|\mathcal{A}_R \Phi_r(d)\Phi_r(e) - \mathbf{1}_{d=e}| \ll_w R^{-1/2}\log(2de). \tag{14}$$

Now replace M_r by F_r^0 using (12), at costs $O(B/R^2)$ and $O(B^2/R^2)$ respectively. The single and double expansions converge absolutely because $\sum |g_e| \le B$. Apply fixed-index orthogonality by dominated convergence. For the rates, $\sum_e \mu_e \log e = \sum_{p>3} \delta_p \log p < \infty$, which makes (14) summable in both expansions. □

Varying the progression and the prime interval together. There are two ways to use (14) before extracting limits. First, averaging (11) in r pointwise gives, under Dirichlet GRH,

$$|\mathcal{A}_R \Phi_r(d) W_r(D(n)) - C(n)\mathbf{1}_{K=d}| \ll_w \frac{\log(2dK)}{\sqrt{R}} + \frac{\log(2D(n))}{R}.$$

The exceptional primes satisfy $\sum_{r^2 \mid D(n)} \log r \le \frac{1}{2}\log D(n)$. Thus for $n \le 2X$, $d \le X^A$, $R = (\log X)^{2+\eta}$ the error is $O_{w,A,\eta}((\log X)^{-\eta/2})$. This estimate can be averaged over any probability distribution on these n.

Second, put $I = (X, X+H] \cap (a + q\mathbb{Z})$, $0 < H \le X$, $N = H/q$, and use its uniform probability. Fix any real weight $|b(n)| \le 1$ independent of r, and set

$$g_e(I) = \mathbb{E}_I[bC\mathbf{1}_{K=e}], \qquad M_r(I) = \mathbb{E}_I[bW_r(D)].$$

For fixed $Y \ge 3, \eta > 0$, suppose every prime divisor of q is at most Y and $N \ge X^{1/3+\eta}$. For $R > Y$ sufficiently large, (14) yields

$$|\mathcal{A}_R \Phi_r(d) M_r(I) - g_d(I)| \ll_{w,Y,\eta} \frac{\log(2d)}{\sqrt{R}} + \frac{1}{N}, \tag{15}$$

$$\left|\mathcal{A}_R M_r(I)^2 - \sum_e g_e(I)^2\right| \ll_{w,Y,\eta} \frac{1}{\sqrt{R}} + \frac{1}{N}. \tag{16}$$

To prove these estimates, the four roots modulo r^2 in (11) cost $O(r^{-2}+1/N)$, since $r \nmid q$. The logarithmic moment that must be summed in (14) is $\mathbb{E}_I \log K$. In the conditioned product law of Theorem A.1 with $k=2$, it is at most $\sum_{p\le Y}\log p + \sum_{p>Y}\delta_p \log p$. In the real sample $K^2 \mid D(n)$, so $\log K \le C_0 \log(2X)$ for an absolute C_0. Apply that theorem to the test $\min(\log K, C_0\log(2X))$, dividing first by its bound. The difference of expectations is $O_{Y,\eta}(\log(2X)X^{-c_\eta})$ for some $c_\eta>0$. Thus $\mathbb{E}_I \log K \ll_{Y,\eta} 1$. Sum (14) against $g_e(I)$ and against $g_e(I)g_f(I)$, using $\sum|g_e(I)|\le 1$. This proves (15)–(16). On dyadic intervals the range is $q \le X^{2/3-\eta}$. The constant B from the fixed-progression theorem is used only for logarithmic extractions at fixed modulus.

3.2 What a finite list of root numbers would have to measure

The additive-interval variance in Section 5 contains mixed covariances. The prime average in (13) gives the simpler energy $\mathcal{P}(g)$. For a prescribed bias its minimum in the box (8) can be computed before asking whether an arithmetic mean satisfies the resulting test. Set

$$S_2=\sum_e \mu_e^2=\prod_{p>3}((1-\delta_p)^2+\delta_p^2), \qquad T=\tfrac{1}{3}-B(1-\mu_1), \qquad P_*=T^2+B^2(S_2-\mu_1^2).$$

The directed product computations give $0.19461706 < T < 0.194618$, $B\mu_5 < 0.053764$ and $0.0417438 < P_* < 0.0417446$. Let $a_e = B\mu_e$. The largest a_e for $e>1$ is a_5. The vector $g_1^*=T,\ g_e^*=a_e\ (e>1)$ lies in the box and has sum $1/3$. Replacing g by $-g$ if necessary, assume its sum is nonnegative. For $h=g-g^*$,

$$\sum_e g_e^* h_e = T(|c|-1/3)+\sum_{e>1}(a_e-T)h_e \ge T(|c|-1/3).$$

Expansion of the squared norm gives the useful uniform bound

$$\mathcal{P}(g) \ \ge\ P_* + 2T(|c|-1/3)+\sum_e h_e^2. \tag{17}$$

It follows that P_* is the exact minimum of $\mathcal{P}$ for $|c|\ge 1/3$, attained only at $\pm g^*$ in the abstract box. Formula (17) also gives the bias margin for a strict energy estimate.

Theorem 3.3 (Two tests on 512 prime parameters)**.** *Let $\mathcal{S}$ consist of the first* 512 *primes congruent to* 19 mod 24 *above* 6000*, from* 6043 *to* 46171*. Write $\mathcal{A}$ for the uniform average on this fixed list. On every common logarithmic extraction,*

$$|\mathcal{A}M_r| \le 0.1911 \implies |c| < 0.333332,$$
$$\mathcal{A}M_r^2 \le 0.03754 \implies |c| < 0.33332637.$$

Each implication is unconditional. The two arithmetic premises are open. If on every relevant extraction at least one premise holds, the uniform conclusion is $|c|<1/3$.

Proof. For independent r,s sampled uniformly from the list write

$$H_{rs}=\sum_e \mu_e \Phi_r(e)\Phi_s(e)=\prod_{p>3}\left(1-\delta_p+\delta_p\left(\frac{p}{r}\right)\left(\frac{p}{s}\right)\right), \qquad J_r=\sum_e \mu_e^2\Phi_r(e)^2.$$

All Euler factors in H are in $(0,1]$, and $0\le S_2-J_r\le \delta_r^2$ because a missing term has $r\mid e$. Write $\mathcal{A}_{r,s}$ for the double average and let $r_0=\min\mathcal{S}$. Cauchy–Schwarz in the probability μ_e, followed by (12), yields

$$|\mathcal{A}M_r - g_1| \le B\sqrt{(1-\mu_1)(\mathcal{A}_{r,s}H_{rs}-\mu_1)}+8B/r_0^2, \tag{18}$$

$$|\mathcal{A}M_r^2-\mathcal{P}(g)| \le B^2\sqrt{\mathcal{A}_{r,s}H_{rs}^2-S_2+2\mathcal{A}(S_2-J_r)}+16B^2/r_0^2. \tag{19}$$

In the first line the squared norm is $\sum_{e>1}\mu_e(\mathcal{A}\Phi_r(e))^2 = \mathcal{A}_{r,s}H_{rs} - \mu_1$. In the second it is the squared norm of $\mathcal{A}\Phi_r(e)\Phi_r(f) - \mathbf{1}_{e=f}$ in $\mu_e\mu_f$. Expanding its three terms gives respectively $\mathcal{A}_{r,s}H_{rs}^2, -2\mathcal{A}J_r, S_2$.

For the certificate, truncate the products at $p \le 6000$ to obtain upper bounds. In this range no parameter ramifies. Each unequal pair of local signs contributes $1 - 8/[p(p+1)]$. Block products of twelve signs, rounded up after multiplication, give

$$\mathcal{A}_{r,s}H_{rs} < 0.716032813843, \qquad \mathcal{A}_{r,s}H_{rs}^2 < 0.528983569579.$$

Integer square roots rounded upwards and the directed bounds for μ_1, S_2 give errors below 0.003515697 and 0.004201088 in (18) and (19). The computation of P_* uses $P_* = (1/3-B)^2 + 2B(1/3-B)\mu_1 + B^2S_2$, retaining the sign of the middle coefficient when bounding the products. With $\mu_1 > 0.7158503030$, the first test gives $|c| \le 0.1911 + 0.003515697 + B(1-\mu_1) < 0.333332$. The second gives $\mathcal{P}(g) < 0.041741088$. Inserting this in (17) with $P_* > 0.0417438$ and $0 < T < 0.194618$ gives its stated margin. □

These computations use local probabilities and character signs. To evaluate M_r itself one still has to average $\lambda(D(n))$ against those local factors. Even the coordinate g_1, where all the unramified tests equal one, retains that sign.

4 Reconstruction at one fixed spectral point

Multiplying a twist by $F_u(\ell)$ makes the ℓ-th coefficient constant. Subtracting that constant removes the principal character from the ensuing Dirichlet series. The diagonal is observable by (10). For a prime $\ell \equiv 1 \bmod 24$ define, initially for $\Re s > 1$,

$$D_\ell(s) = \sum_{u\in\mathcal{U}} \frac{F_u(\ell)m_u - g_\ell}{u^s}, \qquad N_\ell(s) = 8\zeta(2s)(1-2^{-2s})(1-3^{-2s})D_\ell(s).$$

The series D_ℓ are formed from the corrected twist means, rather than from the Hasse–Weil coefficients of the elliptic curves. Each index ℓ supplies one auxiliary function. The data for reconstruction consist of all the values $N_\ell(s)$ at the same point s.

Determination by quadratic-twist values has several antecedents. Luo and Ramakrishnan [23, Theorem B] treat critical values of holomorphic newforms. Ni proves determination by prime quadratic twists at a fixed point [26, Theorem 3.2], and uniform density-one nonvanishing [27, Theorem 1.1], for a fixed finite-dimensional space of level-one cusp forms in the region of absolute convergence. Elliott [10] studies quadratic L-values in $\Re z > 1/2$, while Mishou and Nagoshi [25, Theorem 1.1 and Corollary 1.3] establish universality and positive-proportion nonvanishing for prime discriminants in a fixed progression. Their Lemma 3.1 reproduces Elliott's mean-square approximation by finite Euler products.

Here the unknown profile is infinite, the transformed point $z = 1 - s$ lies in $1/2 < \Re z < 1$, and the ramified factors vary with its coordinates. We prove the mixed prime averages and the conductor-dependent tail estimate required in this setting. One prime average isolates a combination of characters; a second separates their conductors and recovers the coefficients.

Theorem 4.1. *Each N_ℓ extends holomorphically to $\Re s > 0$. Fix any s with $0 < \sigma = \Re s < 1/2$. The values $N_\ell(s)$ determine every g_e, even if one deletes a set of indices of relative density tending to zero among primes $R < \ell \le 2R$, $\ell \equiv 1 \bmod 24$. If $g \neq 0$, there exist $b, \eta > 0$, depending on s, g, such that for every sufficiently large R at least a proportion η of these primes satisfy*

$$|\ell^{s-1/2}N_\ell(s)| \ge b.$$

In particular, if $g \neq 0$ and ρ is any fixed nontrivial zero of ζ of multiplicity m, then D_ℓ has a pole of order m at $\rho/2$ on such a positive proportion of indices. The proportion and the sufficiently large dyadic intervals may depend on ρ and g.

Let $\mathrm{sf}(b) = \prod_{v_p(b)\ \mathrm{odd}} p$. We have $F_u(e)F_u(\ell) = F_u(\mathrm{sf}(e\ell))$. Expanding the eight characters modulo 24 and using (10) gives

$$N_\ell(s) = \sum_{e\neq\ell} g_e \mu(k) \sum_{\psi \bmod 24} L(s, \chi_k\psi) \prod_{p\mid k} (1 - \widetilde{\chi}_k(p)\psi(p)p^{-s})^{-1}, \quad k = \mathrm{sf}(e\ell). \tag{20}$$

At $p \nmid 6k$ this uses $(1+a)/(1-a^2) = (1-a)^{-1}$. At $p \mid k$, the unit-part sign likewise gives a nonzero Euler term. Every k in (20) exceeds one. Thus the L-functions are entire, and on a compact subset of $\Re s > 0$ convexity and the finite products bound each summand without g_e by $O_\varepsilon(k^{1/2+\varepsilon})$, with the compact set fixed. Equation (8) gives normal convergence.

Write $z = 1 - s,\ \tau = \Re z > 1/2$, and let $\mathbb{E}_R$ denote the uniform average over the indicated dyadic primes. All characters modulo 24 are real. Let ψ^* be the primitive character of conductor f inducing ψ. For $\ell \nmid e$, the character $\theta\chi_\ell$, $\theta = \chi_e\psi^*$, is primitive quadratic of conductor $ef\ell$. Its parity j equals that of θ. Its completed functional equation has sign $+1$. Since $\chi_\ell(2) = \chi_\ell(3) = 1$, it gives

$$\ell^{s-1/2} L(s, \chi_{e\ell}\psi) = A_{e\psi} L(z, \theta\chi_\ell), \quad A_{e\psi} = (ef/\pi)^{1/2-s} \frac{\Gamma((z+j)/2)}{\Gamma((s+j)/2)} \prod_{p\mid 6} (1 - \theta(p)p^{-s}). \tag{21}$$

The factor at ℓ in (20) is $1 + O_s(\ell^{-\sigma})$. Each remaining ramified factor has numerator $1 + \widetilde{\chi}_e(p)\psi(p)\chi_\ell(p)p^{-s}$ and denominator $1 - p^{-2s}$, by reciprocity and $\ell \equiv 1 \bmod 4$.

The strict inequality $\Re z > 1/2$ is essential to the short Dirichlet-polynomial argument below. The central values of individual quadratic characters of prime conductor are studied, for instance, by Baluyot and Pratt in *Dirichlet L-functions of quadratic characters of prime conductor at the central point* [3].

Lemma 4.2. *For a fixed squarefree a prime to six, including $a = 1$,*

$$\lim_{R\to\infty} \mathbb{E}_R \mathbf{1}_{\ell\nmid e} \chi_\ell(a) L(z, \theta\chi_\ell) = a^{-z}\theta(a) H_{e\psi}, \tag{22}$$

$$H_{e\psi} = \prod_{p\mid 6} (1 - \theta(p)p^{-z})^{-1} \prod_{p\nmid 6e} (1 - p^{-2z})^{-1}.$$

Uniformly in e, for sufficiently small $\varepsilon > 0$,

$$\|\mathbf{1}_{\ell\nmid e} L(z, \theta\chi_\ell)\|_{L^2(\mathbb{E}_R)} \ll_{s,\varepsilon} 1 + e^{1/4+\varepsilon}. \tag{23}$$

Proof. Smooth the Dirichlet series with $\exp(-n/R^{1/8})$. Shift its Mellin contour to real part $1/2 - \tau$, taking the residue at zero. On the new line Heath-Brown's fourth-moment estimate [17, Theorem 2], restricted to the distinct primitive real characters of conductors $ef\ell \le 48eR$, gives

$$\|\mathbf{1}_{\ell\nmid e} L(1/2 + it, \theta\chi_\ell)\|_{L^2(\mathbb{E}_R)} \ll_\varepsilon e^{1/4+\varepsilon} R^\varepsilon (1 + |t|)^{1/4+\varepsilon}.$$

Here the number of primes in the band is $\asymp R/\log R$ and the L^2 norm is bounded by the L^4 norm. Minkowski's inequality and the decay of the gamma factor bound the smoothing error in L^2 by $O_{s,\varepsilon}(e^{1/4+\varepsilon} R^{-(\tau-1/2)/8+\varepsilon})$. Truncate the smoothed series at $R^{1/6}$ with exponentially small error.

For its second moment, include all dyadic primes to bound the mean of its squared modulus. After pairing $m, n \le R^{1/6}$, group their product by its squarefree part h away from six. The coefficient of $\chi_\ell(h)$ has absolute value $O_{\tau,\varepsilon}(h^{-\tau+\varepsilon})$, by the divisor bound and the convergent sum over $mn = 2^i 3^j h b^2$, $(b, 6) = 1$. In particular the diagonal $h = 1$ is bounded. For $1 < h \le (\log R)^A$, quadratic reciprocity and Siegel–Walfisz give a total $o(1)$. Indeed (ℓ/h) is nonprincipal even after restriction to 1 mod 24. For the larger h the multiplicative large sieve, applied to the prime indicator on the band and the primitive characters $(\cdot/h)$, gives

$$\sum_{\substack{h\in\mathcal{E} \\ h\le R^{1/3}}} |\mathbb{E}_R \chi_\ell(h)|^2 \ll \log R.$$

The conductor square $R^{2/3}$ is shorter than the prime interval. By Cauchy–Schwarz the large-h contribution is $o(1)$ for A sufficiently large in terms of τ. This proves (23). The prime number theorem in progressions, the multiplicative large sieve and the functional equation used here may be found in [19].

For the first moment with fixed a the same argument groups the squarefree parts of an. Each coefficient is $O_{a,\tau,\varepsilon}(h^{-\tau+\varepsilon})$. For large R, $aR^{1/6} \le R^{1/3}$. The diagonal terms are $n = 2^i 3^j a b^2,\ (b,6) = 1$. Their sum converges absolutely. The factors at $2, 3$, at primes of e, and at all other primes give precisely (22). If $(a,e) > 1$ the diagonal vanishes. The smoothing error tends to zero for fixed e. □

Proof of Theorem 4.1. Set $Y_\ell = \ell^{s-1/2} N_\ell(s)$. The absolute values of the finite factors away from ℓ in (20) are $O_{s,\varepsilon}(e^\varepsilon)$, and $|A_{e\psi}| \ll_s e^{1/2-\sigma}$. Thus the $L^2(\mathbb{E}_R)$-norm of the terms with $e > E,\ \ell \nmid e$ is

$$\ll_{s,\varepsilon} \sum_{e>E} |g_e| e^{3/4-\sigma+2\varepsilon} = o_{E\to\infty}(1)$$

uniformly in the band. For the omitted terms $e = \ell h,\ h > 1$, one has $k = h$ and $|g_{\ell h}| \le B t_\ell \mu_h$. Convexity in (20) bounds their normalized sum on each line by $O_{s,\varepsilon}(\ell^{-2})$, since $\sigma < 1/2$. In particular $\sup_R \|Y_\ell\|_{L^2(\mathbb{E}_R)} < \infty$.

For a fixed prime $q > 3$ put $B_s(q) = \lim_{R\to\infty} \mathbb{E}_R \chi_\ell(q) Y_\ell$. Truncating e, expanding the ramified numerators following (21) and applying Lemma 4.2 proves existence. Set

$$\beta_{e\psi} = -g_e \mu(e) A_{e\psi} H_{e\psi} \prod_{p\mid e} (1 - p^{-2s})^{-1}.$$

For $q \nmid e$ only the constant monomial in the numerator survives, since each other one introduces a prime of e in the twist in (22). This gives $q^{-z}\beta_{e\psi}\theta(q)$. For $q \mid e$ only the singleton monomial indexed by q survives: the square q^2 disappears from the twist. After scaling by q^z, the absolute value of all these terms is

$$\ll_{s,\varepsilon} q^{1-2\sigma} \sum_{q\mid e} |g_e| e^{1/2-\sigma+\varepsilon} \ll_{s,\varepsilon} q^{-1/2-3\sigma+\varepsilon},$$

by $t_q \ll q^{-2}$ and (8). It follows that

$$q^z B_s(q) = \sum_{e,\psi} \beta_{e\psi} (\chi_e \psi^*)(q) + o(1) \qquad (q \to \infty). \tag{24}$$

The coefficients on the right are absolutely summable. These primitive characters are distinct: their conductors away from six specify e, and the remaining primitive part specifies ψ. Multiplying by any one of them and averaging over all primes $q \le Q$, then sending $Q \to \infty$, recovers the associated $\beta_{e\psi}$ by the prime number theorem in fixed progressions. Each multiplier of g_e in this coefficient is nonzero. This gives reconstruction, with the R-limit taken first.

Deleting $o(\#\{\ell\})$ terms in each band changes a first average by $o(1)$ by (23) and the uniform L^2 bound for Y_ℓ. For $g \ne 0$, (24) implies $B_s(q) \ne 0$ for at least one fixed q. Hence $|\mathbb{E}_R \chi_\ell(q) Y_\ell| \ge 2b > 0$ on every sufficiently large band. Writing $M = \sup_R \|Y_\ell\|_2$, the bound $2b \le b + M\mathbb{P}_R(|Y_\ell| \ge b)^{1/2}$ proves the proportion claim. At $s = \rho/2$ the finite factors $1 - p^{-2s}$ are nonzero. Wherever $N_\ell(s) \ne 0$, division by $\zeta(2s)$ gives the asserted order of the pole. □

5 Additive intervals in the twist parameter

Fix $d \in \mathcal{E}$. Set $S_d(u) = F_u(d)m_u - g_d$ on $\mathcal{U}$ and extend by zero elsewhere. For integers $X, H \geq 1$, write

$$V_{d,X}(H) = \frac{1}{X} \sum_{X<x\leq 2X} \left| \sum_{x<u\leq x+H} S_d(u) \right|^2, \qquad V_d(H) = \lim_{X\to\infty} V_{d,X}(H).$$

Expanding the centered signal gives

$$S_d(u) = \mathbf{1}_{u\in\mathcal{U}} \sum_{e\neq d} g_e F_u(\mathrm{sf}(de)),$$

with the zero extension understood. If the only signed mass is at d, then $F_u(d)m_u = g_d$ at every admissible twist. Thus the variance loses that coordinate. We prove that this is the whole kernel.

Hall established the $\sqrt{H}$ variance scale for squarefree counts in the range $H \leq X^{2/9-\delta}$ [16, Corollary 1]. Gorodetsky, Matomäki, Radziwiłł and Rodgers extend the unsigned asymptotic to $H \leq X^{6/11-\delta}$ [15, Theorem 1]. For comparison between finite-interval moments and their limiting Fourier expressions, see Gorodetsky, Mangerel and Rodgers [14, Proposition 2.1]. Darbar and Das study short-interval variance for a general class of multiplicative functions [9, §2].

Our signal is a sum of corrected character weights, and its coefficient contains their mixed covariances. Cellarosi and Sinai describe the pure point spectrum of the squarefree system [7, equation (12) and Theorems 5.3, 5.6]; denominator exponents one and two already occur in that spectrum. The calculation here determines the additional Gauss coefficients of the local unit characters. Their relative phases, as well as their moduli, determine the cross terms. We retain Hall's exponent 2/9 and prove uniformity over the full coordinate box for these signed signals.

Theorem 5.1. *There is a positive semidefinite quadratic form $\mathcal{H}_d$ such that, as $H \to \infty$,*

$$V_d(H) = \sqrt{H}(\mathcal{H}_d(g) + o_d(1)).$$

The limit defining $V_d(H)$ exists for each fixed H. For fixed $\delta > 0$ the same asymptotic holds for $V_{d,X}(H)$ as $H \to \infty$ with $H \leq X^{2/9-\delta}$. Both normalized remainders tend to zero uniformly over the coordinate box $|g_e| \leq B\mu_e$. The nullspace consists of the profiles supported at d.

5.1 The Fourier formula

First truncate to finitely many e. On the profinite integers $\widehat{\mathbb{Z}}$ with Haar probability, the signal is $f_Q(u)$ times the squarefree mask away from Q, where $24 \mid Q$ and $p^2 \mid Q$ for each $p \mid de$ in the truncation. The centered periodic f_Q includes the local squarefree masks at the primes of Q. The transform of f_Q at zero vanishes by (10). Averaging periodic truncations over $X < x \leq 2X$ gives their Haar integral. The omitted square divisors have summable upper density, so the bounded signals converge in mean square, proving the fixed-H limit. Write $a' = \prod_{p\nmid Q}(1-p^{-2})$, and $\widehat{f_Q}$ for the normalized finite Fourier transform. For fixed $b \geq 1$, let

$$L_Q(b) = \lim_{M\to\infty} \frac{1}{M} \sum_{\substack{m\leq M,\,(m,Q)=1\\ p\mid m\Rightarrow p^2\nmid b}} \mu^2(m) \prod_{p\mid m} (1-p^{-2})^{-2} |\widehat{f_Q}(b\overline{m}^2)|^2.$$

The inverse is modulo Q. Truncate the squarefree mask and Euler product, then use periodicity and the summable tails to see existence. Orthogonality gives

$$\mathcal{H}_d(g) = \frac{(a')^2 Q^{3/2}}{\pi} \sum_{b\geq 1} L_Q(b) b^{-3/2}. \tag{25}$$

Indeed frequencies have unique exterior radical m, with representatives $b/(Qm^2)$, $0 \le b < Qm^2$, $p^2 \nmid b$ for $p \mid m$. The coefficient is $a'\widehat{f}_Q(b\overline{m}^2)\prod_{p\mid m}[-1/(p^2-1)]$. Combine $\pm b$ in Parseval for the Dirichlet kernel. At fixed $b > 0$ set $m = x\sqrt{H}$. The denominator is asymptotic to $(\pi b/(Qm^2))^2$ and $\int_0^\infty \sin^2(\pi b/(Qx^2))\,dx = \pi\sqrt{b/Q}/2$ by integration by parts and the Fresnel integral. Partial summation of the defining mean gives the integral on each compact x-interval. For $b < Qm^2/2$ the elementary bounds $\sin(\pi b/(Qm^2)) \ge 2b/(Qm^2)$ and $\sum_m \min(1, (Hb/(Qm^2))^2) \ll \sqrt{Hb/Q}$ give a summable $O_Q(b^{-3/2})$ majorant after rescaling. The same bounds dominate the two ends of the x integral, and frequency $1/2$ costs $O(1)$. This proves (25).

At an exterior prime $p \mid m$ the factor $-1/(p^2-1)$ is the Fourier coefficient of the missing residue $0 \bmod p^2$, divided by the squarefree density. At a prime carrying a character the local transform is instead given by a Gauss sum. This distinction lets us control the contribution of the omitted strata. For one basis vector indexed by $k = \mathrm{sf}(de) > 1$ the local Fourier coefficients are supported at denominators dividing $24kwm^2$, where $w \mid k$, $\mu^2(m) = 1$, $(m, 6k) = 1$. At each $p \mid k$ the frequency must have denominator exponent one or two. The local Gauss sums have moduli $p^{-1/2}$ and $p^{-3/2}$ there. At an exterior $p \mid m$ the bound is p^{-2} times the inverse squarefree density. Thus coefficient modulus is $\ll k^{-1/2}w^{-1}m^{-2}$. At modulus q the sum of the squared Dirichlet kernel over nonzero fractions a/q is $(H \bmod q)(q - (H \bmod q)) \le q\min(H, q)$. Consequently for a basis vector its variance is

$$\ll \sum_{w\mid k}\frac{1}{w}\sum_{m}\frac{\min(H, 24kwm^2)}{m^2} \ll \sqrt{Hk}\sum_{w\mid k} w^{-1/2}.$$

Minkowski now bounds $H^{-1/4}\sqrt{V_d(H)}$ by $O_{d,\epsilon}(\sum_{e\ne d}|g_e|e^{1/4+\epsilon})$, uniformly in H. The weighted tails tend uniformly to zero on the box by (8). For a fixed truncation the finitely many entries of the polarized form converge as $H \to \infty$, uniformly for its bounded coordinates. Applying the triangle inequality to the square-root variance before and after taking the limit proves uniform convergence on the box and extends (25) by completion. The quantitative kernel assertion follows from Theorem 7.1 below.

5.2 Passing to a finite interval of conductors

For each k extend $F_v(k)$ by zero if $p^2 \mid v$ for some $p \mid k$. An explicit expansion is

$$\widetilde{F}_k(v) = \mu(k)\sum_{a\mid(k,v)}\chi_{k/a}(a)\prod_{p\mid a}\left(\frac{a/p}{p}\right)\,\chi_k(v/a).$$

Only $a = (k, v)$ can contribute and then all extracted primes occur once. In the correlation of shifts $i, j \le H$ expand both squarefree indicators as $\sum_{m^2\mid n}\mu(m)$ and truncate at $m \le R = X^{1/3}$. Each normalized error is $O_\epsilon(X^{-1/3+\epsilon})$ for $H \le X$. Indeed $\sum_{R<m\le\sqrt{3X}}(X/m^2+1) \ll X/R + \sqrt{X}$, and the other divisor truncation has absolute value $O_\epsilon(X^\epsilon)$. In Haar measure use $\sum_{m>R,n\ge1}[m,n]^{-2} \ll_\epsilon R^{-1+\epsilon}$, where brackets denote lcm. For square divisibilities m^2, n^2, and divisors $a \mid k$, $b \mid l$ from the displayed formula, the CRT gives one progression or none. In its integer parameter the remaining two characters have joint period dividing $[k, l]$. The normalized discrepancy from Haar is bounded by

$$O\Big(([k,l]/X)^\alpha[m,n]^{-2(1-\alpha)} + X^{-1}\Big), \quad 0 < \alpha < 1/2,$$

by interpolation. Indeed, if L is the step of the progression, a multiple of $[m, n]^2$, the trivial count gives $O(1/L + 1/X)$. Completing periods in its integer parameter gives $O([k, l]/X)$. Summing costs $O_{d,\alpha,\epsilon}(X^{-\alpha}(\sum_e|g_e|e^{\alpha+\epsilon})^2 + R^2X^{-1}(\sum_e|g_e|e^\epsilon)^2)$ since $\sum_{m,n}[m,n]^{-2(1-\alpha)} < \infty$. Taking $\alpha = 1/3$ gives $O_\epsilon(H^{3/2}X^{-1/3+\epsilon})$ for $(V_{d,X}(H) - V_d(H))/\sqrt{H}$, since there are H^2 shift

pairs. This establishes the stated simultaneous limit. The coordinate bounds in (8) apply to extraction profiles. Finite samples require their own uniform moment bounds.

6 The Gram matrix at index 29

To turn the variance into a numerical condition on a quartic bias, one needs the cross terms with their signs. Some of these entries vanish exactly, which will decide the order in which the minimizing coordinates move. Write K_{ef} for the polarization of (25) on line $d = 29$, and $M_{ef} = K_{ef}/K_{11}$. Its row and column at d are zero. For $k = \mathrm{sf}(de), l = \mathrm{sf}(df)$, both > 1, put $I = \{p : p \mid (k, l)\}$, $D = \{p : p \mid \mathrm{sf}(kl)\}$ and $w_p = \prod_{q\in D,\ q\neq p}(p/q)$. Write $K_p = (1 - 1/p)(1 + 2/p)$, $U_p = (1 - p^{-3/2})(1 + \sqrt{p})/K_p$. Let b be the number of primes $3 \bmod 4$ in $l/(k, l)$ minus the same count for $k/(k, l)$. Then

$$M_{ef} = \frac{\Re(i^b)\prod_{p\in D}(24/p)}{U_{29}}\,\frac{L(3/2,\chi_k\chi_l)}{\zeta(3/2)}\prod_{p\in I}\frac{1 + w_p\sqrt{p}}{K_p}\prod_{p\in D}\frac{1 + w_p/\sqrt{p}}{\sqrt{p}\,K_p}. \tag{26}$$

To verify this identity polarize (25) at $Q = 24[k, l]^2$. At a prime of $[k, l]$ the untwisted local transforms for numerator valuations $0, 1, \geq 2$ are $-p^{-2}, -p^{-2}, 1 - p^{-2}$. For the twisted factor they are $-\bar{\epsilon}_p(24b'/p)(p^{-3/2}, p^{-1/2}, 0)$ with b' the unit part of the numerator and $\epsilon_p = 1$ or i as $p = 1$ or $3 \bmod 4$. These follow by summing a quadratic character first over units and then over p times units. At $p \not| 6[k, l]$ the local series after summation of the squarefree mask is

$$(1 - 1/p)\left(\frac{(1 - p^{-2})^2}{1 - w_p p^{-3/2}} + p^{-1}(1 + w_p p^{-3/2})\right) = \frac{(1 - p^{-1})^2(1 + 2/p)}{1 - w_p p^{-3/2}}.$$

For clarity, take out the common factor $1 - p^{-1}$ from the restriction $p \nmid m$, the scale p^3 from $Q^{3/2}$, and the phase at a one-character prime. The remaining sums over $v_p(b) = 0, 1$ are

$$\begin{aligned} &p^{-3} + w_p\, p^{-3/2}p^{-1} = p^{-3}(1 + w_p\sqrt{p}), && p \in I,\\ &p^{-7/2} + w_p\, p^{-3/2}p^{-5/2} = p^{-7/2}(1 + w_p/\sqrt{p}), && p \in D. \end{aligned}$$

The factor w_p comes from the character of the other primes on the unit part of b. Dividing by the exterior factor with $w_p = 1$ gives the two ramified products in (26), with the missing Euler factors accounted for by $L(3/2, \chi_k\chi_l)/\zeta(3/2)$. At $2, 3$ the finite transform is the phase of the one class modulo 24, times $1/24$, so the phase disappears upon polarization. The diagonal computation gives

$$K_{11} = \frac{(1 - 1/d)(1 + \sqrt{d})}{\pi\sqrt{24}}\prod_{p|6}\frac{1 - p^{-1}}{1 - p^{-3/2}}\prod_{p\nmid 6d}\frac{1 - 3p^{-2} + 2p^{-3}}{1 - p^{-3/2}}, \quad d = 29.$$

The product majorant $|M_{ef}| \leq W_{ef} = U_d^{-1}\prod_{p|[k,l]} U_p \prod_{p\in D} p^{-1}$ follows by bounding the unramified local ratios by one and taking the larger of the two local factors at ramified places. The same bound holds when an actual row vanishes.

In particular $M_{ee} = U_{29}^{-1}\prod_{p|k} U_p$ when $e \neq 29$. If $e \equiv f \pmod 4$ then b is odd and $M_{ef} = 0$. For example, $M_{1,7} = M_{5,7} = 0$. The coordinate bounds imply absolute convergence of all polarized sums by the single-component estimate of Section 5.

7 The sharp stability modulus

The variance quantitatively controls the signed mass away from its exceptional coordinate. The exponent in this control depends on the decay of the coordinate bounds in (8); its logarithmic factor records how many indices can carry nearly extremal mass.

Theorem 7.1. *Fix $d \in \mathcal{E}$ and put*

$$v = \sqrt{\mathcal{H}_d(g)}, \qquad r_0 = 4^{1/3}, \qquad \kappa = \frac{3(r_0 - 1)}{5}.$$

Under (8)*, for $0 < v \le 1/2$,*

$$\sum_{e \neq d} |g_e| \ll_d v^{4/5} [\log(2/v)]^{\kappa}.$$

At $v = 0$ this mass is zero. For $d = 29$ and fixed $B > 0$, the supremum of this mass on the abstract box with energy at most v^2 also satisfies the reverse inequality for all sufficiently small v, even when the coordinates are required to be nonnegative.

Thus the power is $4/5$ as a function of the square root of the variance coefficient, or $2/5$ as a function of the coefficient itself. The optimality assertion concerns the abstract box; it does not assert that its extremizers arise from Liouville signs.

We separate the proof into the extraction of Fourier coefficients, the control of their interference, and a counting estimate. Write

$$h_k = g_{\mathrm{sf}(dk)} \quad (k > 1), \qquad h_1 = 0, \qquad A(k) = \sum_{p \mid k} p^{-1/4}, \qquad w(k) = \frac{1}{\log(\exp(1) + A(k))}.$$

All indices below are squarefree and coprime to six unless stated otherwise. The notation $P^-(S)$ denotes the least prime factor of $S > 1$.

Lemma 7.2 (Retained frequencies and their means)**.** *For $C \ge 2$, set $R_k = C(1 + A(k))^8$. For a finitely supported profile there are numbers L_k, Z_k such that*

$$\mathcal{H}_d(g) \gg_C \sum_{k > 1} w(k) \sqrt{k}\, |L_k + Z_k|^2, \tag{27}$$

where

$$L_k = \sum_{l \mid k} \omega_{kl} h_l, \qquad \omega_{kk} = 1, \qquad |\omega_{kl}| = (k/l)^{-3/2},$$

and

$$|Z_k| \le \sum_{l \mid k} (k/l)^{-3/2} \sum_{\substack{S > 1,\ (S,k) = 1 \\ P^-(S) > R_k}} S^{-1/2} |h_{lS}|. \tag{28}$$

Proof. In Parseval retain the frequencies

$$\pm \frac{1}{24 k m^2}, \qquad m \in \mathcal{M}_k := \{m : \mu^2(m) = 1,\ (m,k) = 1,\ P^-(m) > R_k\},$$

where $m = 1$ is allowed. These frequency sets are disjoint for different k: the primes above three occurring to odd exponent in the reduced denominator recover k.

The set $\mathcal{M}_k$ has a natural density δ_k. The usual squarefree sieve and Mertens' estimate give

$$\delta_k \gg \frac{1}{\log(2R_k)} \prod_{\substack{p \mid k \\ p > R_k}} \frac{p}{p+1} \gg_C w(k).$$

The last product is bounded below uniformly in k, since

$$\sum_{\substack{p \mid k \\ p > R_k}} \frac{1}{p} \le A(k) R_k^{-3/4} \ll_C 1.$$

Under the limiting uniform law on $\mathcal{M}_k$, a squarefree product S of allowed primes has

$$\mathbb{P}(S \mid m) = \prod_{p \mid S} \frac{1}{p+1} \le \frac{1}{S}. \tag{29}$$

Both statements follow first with finitely many local restrictions and then by removing the summable square-divisor tail.

At the frequency $1/(24km^2)$ divide the Fourier coefficient of the full signal by that of its k-th component. If a is the density of $\mathcal{U}$, the latter coefficient has modulus

$$a \prod_{p \mid k} \frac{p^{-1/2}}{1-p^{-2}} \prod_{p \mid m} (p^2-1)^{-1}.$$

A component can contribute only if its index is lS with $l \mid k$ and $S \mid m$. For $S = 1$, the local Fourier coefficients in Section 6 give the displayed ω_{kl}. Their phases do not depend on m, because the occurrences of m^{-2} in the unit characters are squares. These terms therefore sum to L_k. Write $Q_k(m)$ for the sum of the terms with $S > 1$. Replacing an untwisted factor by a unit character at a prime of S multiplies the coefficient modulus by $\sqrt{p}$, so

$$|Q_k(m)| \le \sum_{l \mid k} (k/l)^{-3/2} \sum_{\substack{S>1 \\ S \mid m}} \sqrt{S}\, |h_{lS}|.$$

For finite support, the relevant means exist by the same finite-congruence approximation as above. Let Z_k be the limiting mean of $Q_k(m)$ on $\mathcal{M}_k$. Taking means in this bound and using (29) proves (28).

To pass from the coefficients to (27), first retain finitely many k. In the squared modulus of each coefficient, discard the factors $(1-p^{-2})^{-2} \ge 1$ before averaging. The substitution $m = x\sqrt{H}$ in the argument for (25) then gives a positive constant times

$$\delta_k \sqrt{k}\, \mathbb{E}_{\mathcal{M}_k} |L_k + Q_k(m)|^2.$$

The factor $\sqrt{k}$ follows from

$$\int_0^\infty \sin^2\!\left(\frac{\pi}{24kx^2}\right) dx = \frac{\pi}{2\sqrt{24k}}.$$

The other factor of k comes from the squared Dirichlet kernel and the local coefficient at the primes of k. Partial summation justifies this Riemann-sum limit for each finite collection of congruence conditions; the squarefree tails then remove that restriction. Jensen's inequality bounds the displayed mean below by $|L_k + Z_k|^2$. Use $\delta_k \gg_C w(k)$ and increase the finite set of k to obtain (27). □

Lemma 7.3 (Absorption of the interfering components)**.** *For every profile satisfying* (8)*,*

$$\sum_{k>1} w(k) \sqrt{k}\, |h_k|^2 \ll_d \mathcal{H}_d(g). \tag{30}$$

Proof. Begin with finite support. Put $x_l = l^{1/4} h_l$ and $X_l = |x_l|$, and use the norm of $\ell^2(w)$. After this change of variables, the coefficient from x_l to $k^{1/4} L_k$, for $l \mid k$, has modulus $(k/l)^{-5/4}$. Since $w(rl) \le w(l)$, each shift $x_l \mapsto x_{rl}$ has operator norm at most one. Consequently the off-diagonal part of this triangular operator has norm at most

$$\rho = \sum_{\substack{r>1 \\ (r,6)=1}} \mu^2(r) r^{-5/4} = \frac{\zeta(5/4)}{\zeta(5/2)(1+2^{-5/4})(1+3^{-5/4})} - 1 < 0.925. \tag{31}$$

The final inequality can be checked by integral bounds for the tails of the two zeta series. In particular the diagonal has a positive margin $1-\rho$.

For $j \geq 1$, define the positive operator

$$(J_j X)_l = \sum_{\substack{\omega(S)=j,\ (S,l)=1 \\ P^-(S)>R_l}} S^{-3/4} X_{lS}.$$

If $l \mid k$ then $R_l \leq R_k$. Equation (28) and the same triangular-operator bound show that

$$\left\| \left(k^{1/4} Z_k\right)_k \right\|_{\ell^2(w)} \leq (1+\rho) \sum_{j \geq 1} \|J_j\| \, \|x\|_{\ell^2(w)}.$$

It remains to make this coefficient smaller than $1-\rho$.

Cauchy–Schwarz, with $S^{-3/4} = S^{-5/8} S^{-1/8}$, and $\sum_{p>R} p^{-5/4} \ll R^{-1/4}$ give

$$|(J_j X)_l|^2 \leq \frac{(C_1 R_l^{-1/4})^j}{j!} \sum_{\substack{\omega(S)=j,\ (S,l)=1 \\ P^-(S)>R_l}} S^{-1/4} |X_{lS}|^2.$$

After summing in l and setting $n = lS$, its squared operator norm is bounded by the supremum over n of

$$\sum_{\substack{S \mid n,\ \omega(S)=j \\ P^-(S)>R_l,\ l=n/S}} \frac{w(l)}{w(n)} \frac{(C_1 R_l^{-1/4})^j}{j!} S^{-1/4}. \tag{32}$$

If $A(l) \geq A(n)/2$, the weights are comparable. Using

$$\sum_{\substack{S \mid n \\ \omega(S)=j}} S^{-1/4} \leq \frac{A(n)^j}{j!}, \qquad R_l^{-1/4} = C^{-1/4}(1+A(l))^{-2},$$

bounds this part of (32) by $O((C_2 C^{-1/4})^j/(j!)^2)$. Otherwise, since n is squarefree,

$$A(n) < 2A(S) \leq 2j R_l^{-1/4} \leq 2jC^{-1/4}.$$

Now $w(l)/w(n) \leq \log(\exp(1)+2j)$, and the remaining part is at most

$$\frac{\log(\exp(1)+2j)(C_3 C^{-1/2} j)^j}{(j!)^2}.$$

The sums of the square roots of these bounds converge and are $O(C^{-1/8})$. Fix C so large that

$$(1+\rho) \sum_{j \geq 1} \|J_j\| \leq \frac{1-\rho}{2}.$$

The triangle inequality therefore yields

$$\left\| \left(k^{1/4}(L_k + Z_k)\right)_k \right\|_{\ell^2(w)} \geq \frac{1-\rho}{2} \|x\|_{\ell^2(w)}.$$

Lemma 7.2 proves (30) for finite support.

For a general profile in (8), finite truncations converge in the variance seminorm by the single-component estimate of Section 5 and the moment bound $\sum_e |g_e| e^{1/4+\varepsilon} < \infty$. Apply the inequality to these truncations and use Fatou's lemma on its left-hand side. This proves (30), including the case $\mathcal{H}_d(g) = 0$. □

Lemma 7.4 (Weighted counting)**.** *Set $z_0 = r_0^2$, $V(e) = e/z_0^{\omega(e)}$, and $a(e) = r_0^{-\omega(e)}$. For $x \geq 2$,*

$$\sum_{V(e)\leq x} a(e)(1 + A(e)) \ll x[\log(2x)]^{r_0-1}, \tag{33}$$

$$\sum_{V(e)\leq x} a(e)^2 \ll x. \tag{34}$$

For fixed d and a sufficiently large fixed K, the set

$$\mathcal{T}_U = \left\{ e : (e, 6d) = 1,\ U < V(e) \leq 2U,\ D(e) := \prod_{p|e}(1 + p^{-1/2}) \leq K \right\}$$

satisfies

$$\sum_{e\in\mathcal{T}_U} a(e) \asymp_{d,K} U(\log U)^{r_0-1} \tag{35}$$

for sufficiently large U.

Proof. Every prime factor of an index with $V(e) \leq x$ is at most z_0x, since $p/z_0 > 1$ for $p > 3$. Hence

$$\sum_{V(e)\leq x} \frac{a(e)}{V(e)} \leq \prod_{3<p\leq z_0x} \left(1 + \frac{r_0}{p}\right) \ll [\log(2x)]^{r_0}.$$

Use $\log V(e) = \sum_{p|e} \log(p/z_0)$, remove one prime, and then sum over that prime. Chebyshev's bound gives

$$\sum_{V(e)\leq x} a(e) \log V(e) \ll x \sum_{V(m)\leq x} \frac{a(m)}{V(m)} \ll x[\log(2x)]^{r_0}.$$

On $V(e) > \sqrt{x}$, divide by $(\log x)/2$. On the complement, the preceding harmonic bound gives $O(\sqrt{x}[\log(2x)]^{r_0})$. This proves (33) without $A(e)$. To insert $A(e)$, distinguish a prime factor p and apply that bound to the remaining index; the additional sum is bounded by a constant times $\sum_p p^{-5/4}$.

The same argument with a^2 has harmonic Euler factor $1 + 1/p$. Its harmonic sum is $O(\log(2x))$, and division by $\log x$ yields (34).

The upper bound in (35) follows from (33). For the lower bound, consider squarefree products m of primes at most U^γ and prime to $6d$, weighted proportionally to

$$\frac{a(m)}{V(m)} = \frac{r_0^{\omega(m)}}{m}.$$

The total weight is $\asymp_{d,\gamma} (\log U)^{r_0}$. Under its normalized product law, the prime p is included with probability $r_0/(p + r_0)$, so

$$\mathbb{E} \log V(m) \ll \gamma \log U, \qquad \mathbb{E} \log D(m) \ll \sum_p p^{-3/2} \ll 1.$$

Choose $0 < \gamma < 1/2$ small and then K large. Markov's inequality retains at least half the total weight under both restrictions $V(m) \leq \sqrt{U}$ and $D(m) \leq K/2$.

For each retained m, append a prime

$$\frac{z_0U}{V(m)} < q \leq \frac{2z_0U}{V(m)}.$$

For large U, this prime exceeds U^γ, is coprime to $6d$, and has at least a constant times $U/(V(m) \log U)$ choices by the prime number theorem. The product $e = mq$ lies in $\mathcal{T}_U$: its V-value is in $(U, 2U]$, while $D(mq) \leq K$. The construction is injective because q is the unique prime factor exceeding U^γ. Since $a(mq) = a(m)/r_0$, summing these choices proves the lower bound in (35). □

Proof of Theorem 7.1. Put $\alpha = r_0 - 1$. The identities

$$e^{-1/2} = a(e)V(e)^{-1/2}, \qquad 4^{\omega(e)}e^{-2} = a(e)V(e)^{-2}$$

and partial summation in Lemma 7.4 imply

$$\sum_{V(e)\le U} \frac{e^{-1/2}}{w(\mathrm{sf}(de))} \ll_d \sqrt{U}[\log(2U)]^{\alpha},$$
$$\sum_{V(e)>U} 4^{\omega(e)}e^{-2} \ll U^{-1}[\log(2U)]^{\alpha}.$$

Here $1/w(\mathrm{sf}(de)) \ll_d 1 + A(e)$ and $\mathrm{sf}(de) \asymp_d e$. Apply Cauchy–Schwarz and (30) to the indices with $V(e) \le U$. On the complementary indices use $\mu_e \le \mu_1 4^{\omega(e)}e^{-2}$, which follows directly from (8). We obtain

$$\sum_{e\ne d} |g_e| \ll_d vU^{1/4}[\log(2U)]^{\alpha/2} + U^{-1}[\log(2U)]^{\alpha}.$$

For sufficiently small v, choose

$$U = v^{-4/5}[\log(2/v)]^{2\alpha/5}.$$

Both terms have order $v^{4/5}[\log(2/v)]^{3\alpha/5}$; the remaining compact range of v follows by changing the constant. If $v = 0$, (30) directly gives $h_k = 0$ for every $k > 1$.

For sharpness, let $d = 29$ and use $\mathcal{T}_U$ from Lemma 7.4. Set

$$g_e = \frac{c_B a(e)}{U^2} \quad (e \in \mathcal{T}_U), \qquad g_e = 0 \quad (e \notin \mathcal{T}_U).$$

These coordinates are nonnegative. Moreover

$$\mu_e = \mu_1 \frac{4^{\omega(e)}}{e^2} \prod_{p\mid e}(1 + p^{-1} - 4p^{-2})^{-1} \ge \frac{\mu_1}{K}\frac{4^{\omega(e)}}{e^2} \ge \frac{\mu_1}{4K}\frac{a(e)}{U^2}$$

on this set. Thus the box holds whenever $0 < c_B \le B\mu_1/(4K)$.

The majorant following (26) and $D(e), D(f) \le K$ give

$$|K_{ef}| \ll_K \frac{(e,f)^{3/2}}{\sqrt{ef}} \qquad (e, f \in \mathcal{T}_U).$$

By (34) and partial summation,

$$\sum_{V(m)\le x} \frac{a(m)}{\sqrt{m}} = \sum_{V(m)\le x} \frac{a(m)^2}{\sqrt{V(m)}} \ll \sqrt{x}.$$

Write $f = hm$ with $h = (e, f)$, drop the remaining coprimality restrictions, and use the last bound. For each $e \in \mathcal{T}_U$,

$$\sum_{f\in\mathcal{T}_U} a(f)|K_{ef}| \ll_K e^{-1/2}\sum_{h\mid e} ha(h)\sqrt{\frac{2U}{V(h)}}$$
$$\ll_K \sqrt{\frac{U}{e}}\sum_{h\mid e}\sqrt{h} = \sqrt{U}\,O_K(D(e)) \ll_K \sqrt{U}.$$

Consequently

$$\mathcal{H}_d(g) \ll_B U^{-5/2}(\log U)^{\alpha}, \qquad \sum_{e\ne d}|g_e| \asymp_B U^{-1}(\log U)^{\alpha}.$$

Take a sufficiently large fixed multiple of $v^{-4/5}[\log(2/v)]^{2\alpha/5}$ for U. The energy is at most v^2 and the mass has the required lower order. This proves the reverse inequality. □

Consequently a single line with zero variance gives $c = g_d$. Its missing coordinate is available from the independent twist average (10). Two distinct lines with zero variance force the entire profile to vanish, since their one-dimensional nullspaces intersect only at zero. A small variance controls the mass away from d with the modulus of Theorem 7.1.

8 The least variance compatible with a quartic bias

If $c \ge b > 0$, how small could the variance be on the information (8) alone? The answer gives a threshold against which to compare an arithmetic estimate. Start with $g = B\boldsymbol{\mu}$, where $\boldsymbol{\mu} = (\mu_e)_e$. Reducing the required total frees mass first at the coordinate with the largest gradient. The Gram matrix determines when a second coordinate reaches the same gradient. The vanishing of $M_{1,7}$ and $M_{5,7}$ then makes the third such contact explicit.

Write $\mathcal{S} = \sum_{e,f} \mu_e \mu_f M_{ef}$, $T_e = \sum_f M_{ef}\mu_f$. For a finite set I let M_I denote the principal matrix, T_I the corresponding column and $\mathbf{1}_I$ the column of ones. Each M_I below is positive definite by Theorem 7.1, since $29 \notin I$. Set

$$x_5 = 1 - \frac{T_1 - T_5}{1 - M_{1,5}}, \tag{36}$$

$$x_7 = 1 - \mathbf{1}_I^{\mathsf{T}} M_I^{-1}(T_I - T_7 \mathbf{1}_I), \qquad I = \{1, 5\}. \tag{37}$$

Theorem 8.1. *For $1/3 \le x \le 1$ consider all real profiles with $|g_e| \le B\mu_e$ and $\sum_e g_e \ge Bx$. Their unique minimum of $\mathcal{H}_{29}$ is attained at*

$$g/B = \boldsymbol{\mu} - \sum_{i \in I} z_i \mathbf{e}_i, \qquad z = M_I^{-1}(T_I - y\mathbf{1}_I), \qquad y = \frac{\mathbf{1}_I^{\mathsf{T}} M_I^{-1} T_I - 1 + x}{\mathbf{1}_I^{\mathsf{T}} M_I^{-1} \mathbf{1}_I}.$$

Here $\mathbf{e}_i$ is the coordinate vector, and I is given by the table. The formulas agree at shared endpoints.

Normalized bias x	*Coordinates allowed to move*	*Absolute transition bias*
$x_5 \le x \le 1$	1	$0.29360867 < Bx_5 < 0.29363833$
$x_7 \le x \le x_5$	$1, 5$	$0.19239671 < Bx_7 < 0.19244136$
$1/3 \le x \le x_7$	$1, 5, 7$	$B/3 = 0.16272674\ldots$

The minimum is $K_{11}B^2(\mathcal{S} - 2T_I^{\mathsf{T}} z + z^{\mathsf{T}} M_I z)$. For $|\sum g_e| \ge Bx$ this value is attained by the two opposite signs of the same profile.

Corollary 8.2. *At positive bias at least $1/3$, the unique minimizer is $g^* = B\boldsymbol{\mu} + (1/3 - B)\mathbf{e}_1$, and*

$$0.01386945460 < \mathcal{H}_{29}(g^*) < 0.01387317250. \tag{38}$$

Moreover every feasible g on this positive side satisfies

$$\mathcal{H}_{29}(g) - \mathcal{H}_{29}(g^*) \;\ge\; 0.0020\, \|g - g^*\|_1.$$

The same estimate holds after simultaneous change of sign on the negative side.

Proof of Theorem 8.1. Put $h = g/B$. At a proposed optimum h^* of total x, let $G = Mh^*$. Suppose $G_i = y > 0$ on I, $h^*_e = \mu_e$ and $G_e \le y$ elsewhere. For any feasible h,

$$\langle G, h - h^* \rangle = y\Big(\sum_e h_e - x\Big) + \sum_{e \notin I} (y - G_e)(\mu_e - h_e) \ge 0. \tag{39}$$

The remainder in the quadratic expansion is positive semidefinite. Equality of the energies forces both the linear and quadratic terms to vanish. The latter restricts $h - h^*$ to coordinate

29, and the former forces equal totals, hence $h = h^*$. Solving $G_I = y\mathbf{1}_I$ with $\sum z_i = 1 - x$ gives the formula. The gradient at 5 equals the gradient at 1 in the one-coordinate solution exactly at (36). For the two-coordinate solution the gradient at 7 stays equal to T_7, giving (37).

To verify the inequalities for the other coordinates, write $d = 29$ and $u_p = U_p/p$. At any profile with $0 \le h_e \le \mu_e$, the absolute gradient in row e is bounded by $\sum_f \mu_f W_{ef}$. Summation of the product majorant from Section 6 gives

$$\frac{\sum_f \mu_f W_{ef}}{\mu_1} = Z \prod_{\substack{p \mid e \\ p \neq d}} C_p \begin{cases} 1 + t_d/d, & d \nmid e, \\ 1/d + t_d/U_d, & d \mid e, \end{cases} \qquad C_p = \frac{u_p + t_p U_p}{1 + t_p u_p}, \tag{40}$$

where $Z = \prod_{p>3,\, p\neq d}(1 + t_p u_p) < 1.1530$. For $p \ge 13$, $C_p \le (1 + \sqrt{p})(1/p + 4/p^2)$. The right-hand side is decreasing. With $5, 7, 11$ checked directly, $C_p < 1$ for every relevant p and $C_p < 0.48$ for $p \ge 11$. Every e divisible by 29 or by a prime $p \ge 101$ has envelope below 0.114. The others are tested by multiplying factors $C_p < 1$ and dropping each branch whose envelope already lies below the specified bound.

The following directed bounds give the endpoint checks for h^*. The fourth column bounds every gradient outside the tied indices in the normalization $h = g/B$. For each enumerated row we evaluate T_e through $f = 1000$, bounding the tail by (40) after subtraction of the included terms. The entries T_1, T_5, T_7 used to solve the small systems use the tighter computation below.

x	Tied indices	Common gradient y	Other gradients at most	Rows tested
x_5	$1, 5$	$(0.33103, 0.33112)$	0.30001	7
x_7	$1, 5, 7$	$(0.17029, 0.17034)$	0.16501	22
$1/3$	$1, 5, 7$	$(0.13250, 0.13254)$	0.11401	46

The computation checks $0 < z_i < \mu_i$ for every coordinate already moved at the listed endpoints. A newly tied one has deficit zero there. Equations (36)–(37) give equality of its gradient exactly. Feasibility, positivity of y, and each gradient inequality interpolate affinely between adjacent endpoints. For $x_5 \le x \le 1$, $G_1 - G_e$ for $e \neq 1$ has slope $1 - M_{e1} > 0$. Indeed, if $d \nmid e$, the bound for $|M_{e1}|$ is $\prod_{p|e} U_p/p < 1$. If $d \mid e$ it is at most $d^{-1} \prod_{p|e,\, p\neq d} U_p/p$. The first piece therefore extends to $x = 1$. This proves (39) throughout the range. □

Proof of Corollary 8.2. Here $x = 1/(3B) > x_5$, so $z_1 = 1 - 1/(3B)$. The normalized energy is

$$\mathcal{H}_{29}(g^*)/K_{11} = B^2\mathcal{S} - 2B(B - 1/3)T_1 + (B - 1/3)^2.$$

The certificate retains 1822 nonzero rows with $e \le 6000$, uses 90000 terms in the Dirichlet series of (26), and truncates the exterior prime product at 10^6. For a nonprincipal character it bounds the Dirichlet tail by partial summation from an interval-sum bound, allowing the trivial bound $2/\sqrt{90000}$ throughout. For imprimitive characters the interval bound includes the divisors of the common ramified part by inclusion–exclusion. The omitted rows and columns cost at most twice the positive sum of $\mu_e \mu_f W_{ef}$ with $e > 6000$. This gives

$$\begin{gathered} 0.5783803409869465 < \mathcal{S} < 0.5784280735132444, \\ 0.7296041476233856 < T_1 < 0.7296202326726962, \\ 0.26926546281 < K_{11} < 0.26926546298. \end{gathered} \tag{41}$$

Every decimal endpoint in (41) is an exact rational bound. These printed bounds alone give (38). More generally, write their lower and upper endpoints as S_-, S_+, T_-, T_+, and K_-, K_+.

For a bias $b \le B$ in the first branch, set

$$E_-(b) = K_-\{B^2 S_- - 2B(B-b)T_+ + (B-b)^2\},$$
$$E_+(b) = K_+\{B^2 S_+ - 2B(B-b)T_- + (B-b)^2\}.$$

The quantities in braces are positive at the biases used here, so these expressions enclose the minimum energy. In particular,

$$E_-(1/3) > 0.01386945461096, \qquad E_+(1/3) < 0.01387317249031.$$

The source archive includes an exact-rational calculation using precisely (41).

For stability write $D_e = (Mg^*)_e$ in the original normalization. Equation (40) bounds $|D_e| < 0.01420$ when $29 \mid e$ and $|D_e| < 0.19344$ for a remaining index with some prime factor at least 11. The only remaining rows are $1, 5, 7, 35$. Direct interval evaluation gives $D_1 > 0.2012$, $D_5 < 0.1674$, $D_7 < 0.0833$, $D_{35} < 0.0286$. Let $\Delta = \sum_e g_e - 1/3$ and $L = \sum_{e>1}(B\mu_e - g_e)$. Both are nonnegative, and $g_1 - g_1^* = \Delta + L$. The linear term in the energy difference, including $2K_{11}$, is at least $2K_{11}(0.2012\Delta + 0.0077L)$. Since $\|g - g^*\|_1 = \Delta + 2L$, the stated coefficient follows. □

The remaining arithmetic question. The form in Theorem 5.1 is evaluated from the twist means of the actual logarithmic extraction. Proving $\mathcal{H}_{29}(g) \le 0.01386$ for that profile would exclude $|c| \ge 1/3$ by Corollary 8.2. One can invert the minimum more precisely. Let b_* be the largest absolute total of any profile in the box with $\mathcal{H}_{29}(g) \le 0.01386$. Then

$$0.33321180 < b_* < 0.33324612. \tag{42}$$

Both endpoints are above Bx_5. At a positive target b in this range the least energy is $K_{11}[B^2\mathcal{S} - 2B(B-b)T_1 + (B-b)^2]$. It increases strictly there since its derivative is $2K_{11}By > 0$. The rational bounds (41) give

$$E_+(0.33321180) < 0.013859999436 < 0.01386,$$
$$E_-(0.33324612) > 0.013860000341 > 0.01386.$$

Continuity and the explicit minimizing profiles give (42). Thus an arithmetic proof of the variance target on every extraction would bound every $|c|$ by 0.33324612. It remains to estimate the signed distribution of $C(n)$ among the valuation strata. Likewise an estimate for a family averaged over all integer parameters t would need a restriction argument to apply at $t = D(n)$.

A Marked valuations on moving progressions

We prove the local distribution estimate used in Sections 2.5 and 3.1. Its cubic case also gives a uniform truncation of one signed stratum. Write $L_i(n) = n, n+1, 3n+1, 3n+2$ in this order, and $I = (X, X+H] \cap (a + q\mathbb{Z})$, $0 < H \le X$, $N = H/q$. Let $k \ge 2$ be an integer. For each $p > 3$, the observation $V_k(n)_p$ is zero if $v_p(D(n)) < k$. Otherwise it records the unique site i and the exact exponent $j = v_p(L_i(n))$. In the model $\nu_{a,q,k}$, independently at each $p > 3$, take a Haar-uniform point of the coset $a + q\mathbb{Z}_p$, with probability normalized on that coset, and apply the same observation. At $p \nmid q$ its law is

$$\mathbb{P}(0) = 1 - 4p^{-k}, \qquad \mathbb{P}(i,j) = (1 - p^{-1})p^{-j} \quad (j \ge k).$$

The support of a random configuration is almost surely finite. We use $d_{\mathrm{TV}} = \sup_E |\mathbb{P}(E) - \mathbb{P}'(E)|$.

The comparison with independent local variables goes back to Kubilius [20]. Barban and A. I. Vinogradov improved the classical approximation, as explained by Elliott [4, 11]. Tenenbaum [32, Theorem 1] estimates total variation for truncated prime factors of a random integer. Gorodetsky [13, Theorem 2.3] starts from divisibility errors and bounds the joint distance for prime exponents of a sieve sequence at a chosen set of primes. In our setting each large exponent carries the index of one of four forms, the law conditions on each prime dividing a moving modulus, and all large primes enter the observation. The estimates below give the truncation and counting costs for these data. Counts for pairs of k-free integers in progressions were studied by Brüdern, Perelli and Wooley [6, §3]. For single integers Filaseta [12] treats short intervals, Mangerel [24] obtains power savings for squarefree counts in reduced classes of smooth squarefree moduli, and Parry [28] studies the variance over classes for a prescribed modulus. Here the comparison is simultaneous over all bounded tests of the marked vector.

Theorem A.1. *Fix an integer $k \geq 2$ and $\delta, \varepsilon > 0$. If $N \geq X^{1/(k+1)+\delta}$, then uniformly in H, q, a, including non-reduced classes,*

$$d_{\mathrm{TV}}(\mathcal{L}_I(V_k), \nu_{a,q,k}) \ll_{k,\delta,\varepsilon} X^{-\min(\delta, 1/[3(k+1)])+\varepsilon}. \tag{43}$$

On $H = X$, for any $0 < \delta < 1$ and $q \leq X^{1-\delta}$, one also has

$$\frac{1}{q} \sum_{a \bmod q} d_{\mathrm{TV}}(\mathcal{L}_I(V_k), \nu_{a,q,k}) \ll_{k,\delta,\varepsilon} X^{-\min(\delta, 1/2)/2+\varepsilon}. \tag{44}$$

The free coordinates. For $p^e \parallel q,\ p > 3$, either every $v_p(L_i(a)) < e$, in which case all four valuations are fixed, or one site satisfies $p^e \mid L_i(a)$. In the latter case $v_p(L_i(n)) = e + t$. In the coordinate $n = a + qm$, the form $L_i(n)/p^e$ has unit slope at p, so the model has $\mathbb{P}(t = j) = (1 - 1/p)p^{-j}$ for $j \geq 0$. Keep the site and the base e even when $e < k$, and use t as the free level. Outside $6q$ use level $j - k + 1$ at the marked site. Level zero denotes absence of a free mark. The deterministic map from this finer vector to V_k contracts total variation. We prove both estimates for the finer vector.

The large primes. Fix $2 \leq Z \leq P \leq X^{1/k}$, and write $K_k(q) = 2k^{\omega(q)}$. The probability of a free mark at some $p > Z,\ p \nmid 6q$ is

$$\ll_k Z^{1-k} + \frac{P}{N \log P} + K_k(q) \left(\frac{X}{NP^k} + P^{1-k} \right). \tag{45}$$

For $Z < p \leq P$, each $p^k \mid L_i(n)$ is a single congruence for m. Its count is $N/p^k + O(1)$, giving the first two terms. For $U < p \leq 2U,\ p > P$, switch from p to its cofactor, writing $p^k m' = L_i(n)$. Put $g = (L_i(a), q)$. Then $(m', q) = g$, $m' = gb$ with $(b, q/g) = 1$, $b \ll X/(gU^k)$, and $p^k b \equiv L_i(a)/g \bmod (q/g)$. The kernel of the k-th power on units modulo an odd prime power has at most k elements. At a power of two it has at most $2k$. CRT leaves at most $K_k(q)$ classes for $p \bmod (q/g)$, also when $q/g = 1$. For each m' giving a solution, the derivative of $m' v^k$ is $\gg_k X/U$ on the band and the image interval for $L_i(n)$ has length at most $3H$. Thus the allowed interval of p's has length $O_k(HU/X)$. The count is

$$\ll_k K_k(q) \frac{X}{gU^k} \left(1 + \frac{HUg}{Xq} \right).$$

Dividing by $|I| = N + O(1) \asymp N$ and summing geometric bands proves (45). At the active primes $p \mid q$ a positive free level costs $O(1/p + 1/N)$, so the further large-prime loss is $O(\omega(q)(1/Z + 1/N))$. In the model the corresponding large-prime losses are $O_k(Z^{1-k} + \omega(q)/Z)$.

An arbitrary bounded test. For a free vector z put $b(z) = \prod p^{u_p}$, where u_p is its positive free level. On the integers this divides $D(n) \ll X^4$. For d supported at allowed primes put

$$M_q(d) = d \prod_{p \mid d,\ p \nmid q} p^{k-1}.$$

At each $p^u \parallel d$ specify a compatible site and require free level at least u. There are at most $4^{\omega(d)}$ allocations. For each allocation the event is one class of $m \bmod M_q(d)$, by CRT. Its model probability is $1/M_q(d)$, and the real probability differs by $O(1/N)$.

For any $0 < \theta < 1$ one has

$$\sum_{d > Z} \frac{8^{\omega(d)}}{M_q(d)} \ll_{k,\theta,\varepsilon} q^{\varepsilon} Z^{-1+\theta}. \tag{46}$$

Indeed the Euler factors after inserting $d^{1-\theta}$ are $1 + 8p^{-(k-1)}/(p^{\theta} - 1)$ outside q. Their product converges. At $p \mid q$ the factors are $1 + 8/(p^{\theta} - 1)$, with product $O_{\theta,\varepsilon}(q^{\varepsilon})$. If all retained primes are at most Z but $b(z) > Z$, multiply its prime factors one at a time until the product first exceeds Z. This gives a divisor between Z and Z^2. The allocation counts and (46) bound this probability in the real sample by

$$O_{k,\theta,\varepsilon}(q^{\varepsilon} Z^{-1+\theta} + N^{-1} Z^{2+\varepsilon}). \tag{47}$$

Now erase primes above Z in both laws at the probability costs just proved. For an arbitrary test $|f| \le 1$ on the remaining free vectors, difference f in each occupied coordinate between levels u_p and $u_p - 1$, keeping its site and setting unoccupied coordinates to zero. The mixed coefficient $\alpha_{d,i}$ has modulus at most $2^{\omega(d)}$ for an allocation i, with $\alpha_1 = f(0)$. Telescoping gives $f(z) = \sum_{d \mid b(z)} \alpha_{d,i(z,d)}$. The model expectation of the terms with $d > Z$ costs at most (46) by absolute convergence. In the real law truncation at $d \le Z$ is exact if $b(z) \le Z$. Otherwise the truncated value is bounded by $\prod_{p^u \parallel b(z)} (1 + 2u) \le \tau(b(z))^2 \ll_{\varepsilon} X^{\varepsilon}$, so (47) controls the loss. Finally the two truncated expectations differ by $O_{\varepsilon}(Z^{1+\varepsilon}/N)$, by summing the errors of the congruence counts. All these bounds are independent of the test.

For (43) choose $Z = X^{1/[3(k+1)]}$, $P = (X \log X)^{1/(k+1)}$. In (45) the terms $P/(N \log P)$ and $X/(NP^k)$ are $O_k(X^{1/(k+1)}/[N(\log X)^{k/(k+1)}])$. The small-prime loss Z^2/N is $O(X^{-1/[3(k+1)]})$ in the stated range. Since $K_k(q) \ll_{k,\varepsilon} X^{\varepsilon}$, taking the auxiliary θ, ε sufficiently small proves (43). More precisely the bound, for $N \ge X^{1/(k+1)}/\log X$, is

$$d_{\mathrm{TV}} \ll_{k,\varepsilon} X^{-1/[3(k+1)]+\varepsilon} + K_k(q) \frac{X^{1/(k+1)}}{N(\log X)^{k/(k+1)}}. \tag{48}$$

In particular bounded $\omega(q)$ permits $N \ge X^{1/(k+1)}$ even at the endpoint.

For (44) take $Z = X^{\min(\delta, 1/2)/2} \le X^{1/4}$. Every free mark requires $v_p(D) \ge 2$, including $t > 0$ at a prime of q. Its level is at most $v_p(D) - 1$. The losses from a large prime or a large real complexity are thus dominated by the corresponding events for the global square observation $k = 2, q = 1$. Averaging the real probabilities over the q classes costs at most a constant times the global probability since all class sizes are $X/q + O(1)$. A direct square-divisor count gives $O(Z^{-1} + X^{-1/2})$ for a global large prime. Equation (47) bounds global small-prime complexity by $O_{\theta}(Z^{-1+\theta} + Z^{2+\varepsilon}/X)$. The model tail and the truncated comparison still cost $O(q^{\varepsilon} Z^{-1+\theta} + qZ^{1+\varepsilon}/X)$. Substituting Z and diminishing the auxiliary exponents proves (44). A prescribed class can belong to the exceptional set allowed by (44).

A.1 Truncating the square part on the stratum $K = 1$

Let K_q be the product of the primes $p \nmid 6q$ with positive even valuation in D, and $A_q = \prod_{p \nmid 6q} p^{\lfloor v_p(D)/2 \rfloor}$. Keep the exact indicator J_q that no $p > 3$ dividing q has positive even

valuation. On $K_q = 1$ the product A_q equals

$$A_{\mathrm{odd}} = \prod_{\substack{p \nmid 6q \\ v_p(D) \geq 3 \text{ odd}}} p^{(v_p(D)-1)/2},$$

a function of V_3 alone. For $0 < \alpha < 2$ its model moment is bounded uniformly in q, a by

$$\prod_{p>3} \left(1 + 4(1 - p^{-1}) \sum_{j \geq 1} p^{j\alpha - 2j - 1} \right) < \infty,$$

since the local increment is $O_\alpha(p^{\alpha-3})$. Put $F_{q,T} = C\,\mathbf{1}_{K_q=1,\, A_q \leq T}$. Pointwise, $|C\mathbf{1}_{K=1} - J_q F_{q,T}| \leq \mathbf{1}_{A_{\mathrm{odd}} > T}$. Apply Markov's inequality in the product law and (43) to this last event. For $T \geq 1, \eta > 0$ and $N \geq X^{1/4+\delta}$,

$$\mathbb{E}_I |C\mathbf{1}_{K=1} - J_q F_{q,T}| \ll_{\eta,\delta,\varepsilon} T^{-2+\eta} + X^{-\min(\delta,1/12)+\varepsilon}.$$

On a dyadic interval the first estimate reaches $q \leq X^{3/4-\delta}$. Averaging the left side over classes for $q \leq X^{1-\delta}$ replaces the second term by $O(X^{-\min(\delta,1/2)/2+\varepsilon})$. The bound holds for every cutoff T, including cutoffs varying with X. Valuations equal to two are invisible to V_3. The indicator $K = 1$ has been retained in the signed comparison, while V_2 determines it outright in the square range.

Computations and AI assistance

The accompanying Zenodo source archive contains the parameter construction, the local root-number comparisons, the Gram calculation with outward rounding, and the exact-rational assembly from (41). It includes executable scripts, their recorded outputs, the dependency versions and reproduction commands. The input interval for μ_1 is checked by a directed Euler product; the interval for K_{11} has a separate product certificate. These are the inputs to the full Gram calculation and its gradient checks.

The recorded PARI 2.15.4 checks compare (4) on 154 specializations and (9) on 102 with independently computed root numbers. The large-parameter primality and product bounds, the full Gram calculation at the cutoffs stated above, the endpoint gradients and the final energy enclosure were recomputed. The local Fourier transforms were checked exactly at 1014 frequencies, and the finite interval kernel at 8127 choices of its parameters. The analytic limits and the passage to infinitely many coordinates use the proofs in the text.

The source also supplies the three raw product lists and the corrected product list, the 512 individual prime parameters, and standard-library verification programs. Directed integer bounds certify the numerical steps in Theorems 2.4 and 3.3 and the product errors of Proposition 2.5. A separate exact check covers the local congruences, mixed allocations, power-map fibres and finite differences in Appendix A. The programs compute no logarithmic mean M_r.

OpenAI's ChatGPT assisted with mathematical development and drafting. ChatGPT Codex assisted with the extensions, exposition, bibliographic checks, code and computational verification. The recorded computations concern the stated finite identities and numerical certificates; they do not constitute a formalization of the analytic proofs.

References

[1] N. C. Ankeny, *The least quadratic non residue*, Annals of Mathematics (2) **55** (1952), 65–72. 10.2307/1969420.

[2] E. Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55** (1990), 355–380. 10.1090/S0025-5718-1990-1023756-8.

[3] S. Baluyot and K. Pratt, *Dirichlet L-functions of quadratic characters of prime conductor at the central point*, Journal of the European Mathematical Society **24** (2022), 369–460. 10.4171/JEMS/1084.

[4] M. B. Barban and A. I. Vinogradov, *On the number-theoretic basis of probabilistic number theory*, Doklady Akademii Nauk SSSR **154** (1964), 495–496. English translation in Soviet Mathematics Doklady **5** (1964), 96–98.

[5] S. Bettin, C. David and C. Delaunay, *Non-isotrivial elliptic surfaces with non-zero average root number*, Journal of Number Theory **191** (2018), 1–84. 10.1016/j.jnt.2018.03.007.

[6] J. Brüdern, A. Perelli and T. D. Wooley, *Twins of k-free numbers and their exponential sum*, Michigan Mathematical Journal **47** (2000), 173–190. 10.1307/mmj/1030374676.

[7] F. Cellarosi and Ya. G. Sinai, *Ergodic properties of square-free numbers*, Journal of the European Mathematical Society **15** (2013), 1343–1374. 10.4171/JEMS/394.

[8] L. Cowland Kellock and V. Dokchitser, *Root numbers and parity phenomena*, Bulletin of the London Mathematical Society **55** (2023), 2557–2597. 10.1112/blms.12931.

[9] P. Darbar and M. K. Das, *The variance of a general class of multiplicative functions in short intervals*, arXiv:2208.13238, version 2, 20 June 2026. 10.48550/arXiv.2208.13238.

[10] P. D. T. A. Elliott, *On the distribution of the values of quadratic L-series in the half-plane* $\sigma > 1/2$, Inventiones Mathematicae **21** (1973), 319–338. 10.1007/BF01418793.

[11] P. D. T. A. Elliott, *Probabilistic Number Theory I: Mean-Value Theorems*, Springer, New York, 1979, Grundlehren der mathematischen Wissenschaften, vol. 239. 10.1007/978-1-4612-9989-9.

[12] M. Filaseta, *An elementary approach to short interval results for k-free numbers*, Journal of Number Theory **30** (1988), 208–225. 10.1016/0022-314X(88)90018-2.

[13] O. Gorodetsky, *A Kubilius model for sieve-theoretic sequences*, Analysis Mathematica, published online 14 August 2026, Theorem 2.3. 10.1007/s10476-026-00178-w.

[14] O. Gorodetsky, A. Mangerel and B. Rodgers, *Squarefrees are Gaussian in short intervals*, Journal für die reine und angewandte Mathematik **795** (2023), 1–44. 10.1515/crelle-2022-0066.

[15] O. Gorodetsky, K. Matomäki, M. Radziwiłł and B. Rodgers, *On the variance of squarefree integers in short intervals and arithmetic progressions*, Geometric and Functional Analysis **31** (2021), 111–149. 10.1007/s00039-021-00557-5.

[16] R. R. Hall, *Squarefree numbers on short intervals*, Mathematika **29** (1982), 7–17. 10.1112/S0025579300012110.

[17] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arithmetica **72** (1995), 235–275. 10.4064/aa-72-3-235-275.

[18] H. A. Helfgott, *On the behaviour of root numbers in families of elliptic curves*, arXiv:math/0408141, version 3 (2009). 10.48550/arXiv.math/0408141.

[19] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, vol. 53, Providence, RI (2004). 10.1090/coll/053.

[20] J. Kubilius, *Probabilistic Methods in the Theory of Numbers*, Translations of Mathematical Monographs, vol. 11, American Mathematical Society, 1964. 10.1090/mmono/011.

[21] Y. Lamzouri, X. Li and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Mathematics of Computation **84** (2015), 2391–2412. 10.1090/S0025-5718-2015-02925-1. Theorem 1.4, Lemma 2.4 and equations (4.3), (4.8) in arXiv:1309.3595v3.

[22] Y. Lamzouri, X. Li and K. Soundararajan, *Corrigendum to "Conditional bounds for the least quadratic non-residue and related problems"*, Mathematics of Computation **86** (2017), 2551–2554. 10.1090/mcom/3261.

[23] W. Luo and D. Ramakrishnan, *Determination of modular forms by twists of critical L-values*, Inventiones Mathematicae **130** (1997), 371–398. 10.1007/s002220050189.

[24] A. P. Mangerel, *Squarefree integers in arithmetic progressions to smooth moduli*, Forum of Mathematics, Sigma **9** (2021), e72. 10.1017/fms.2021.67.

[25] H. Mishou and H. Nagoshi, *The universality of quadratic L-series for prime discriminants*, Acta Arithmetica **123** (2006), 143–161. 10.4064/aa123-2-3.

[26] T. Ni, *Rational spanning sets of level-one cusp forms from Eisenstein series at prime levels*, arXiv:2608.04241, version 1 (2026). 10.48550/arXiv.2608.04241.

[27] T. Ni, *Uniform non-vanishing of prime quadratic twists of standard and symmetric square L-functions*, arXiv:2610.11974, version 1 (2026). 10.48550/arXiv.2610.11974.

[28] T. Parry, *A variance for k-free numbers in arithmetic progressions of given modulus*, Journal de théorie des nombres de Bordeaux **33** (2021), 317–360. 10.5802/jtnb.1163.

[29] H. C. Pocklington, *The determination of the prime or composite nature of large numbers by Fermat's theorem*, Proceedings of the Cambridge Philosophical Society **18** (1914), 29–30.

[30] B. Pouly, *An explicit bound below one half for a quartic Liouville correlation*, Zenodo (2026). 10.5281/zenodo.24443184. Public text: hexagon:2611.00891v1.

[31] O. G. Rizzo, *Average root numbers for a nonconstant family of elliptic curves*, Compositio Mathematica **136** (2003), 1–23. 10.1023/A:1022669121502.

[32] G. Tenenbaum, *Crible d'Ératosthène et modèle de Kubilius*, in *Number Theory in Progress*, vol. 2, de Gruyter, 1999, 1099–1130. 10.1515/9783110285581.1099.