

Rational points on elliptic curves that are primitive modulo a positive proportion of primes

Manjul Bhargava

16 October 2026

Abstract

In 1977, Lang and Trotter conjectured that, subject to certain necessary arithmetic restrictions, a rational point P of infinite order on an elliptic curve E over $\mathbb{Q}$ should generate its reduction modulo infinitely many primes p —and indeed should do so for a specified positive density of primes. However, to date, even this infinitude was not known unconditionally for any explicit pair (E, P) .

For the curve $E : y^2 = x^3 - 2x$ and point $P = (2, 2)$, we prove the existence of infinitely many—and indeed a positive lower density of—primes for which the reduction of P generates $E(\mathbb{F}_p)$. More precisely, we prove that a common zero-free half-plane $\Re s > 1 - 1/N$ for Dedekind zeta functions gives a lower density of at least $c/(N \log N)$, with $c > 0$ independent of N . The announced theorem of Cureton and Thorner provides $N = 32$. Our proof combines this input with the marked Type II estimates of OpenAI, a sieve with varying cofactor, and estimates for division fields and heights. The same method also applies to other CM elliptic curves and points.

1 Introduction

A natural and famous analogue of Artin’s primitive root conjecture for elliptic curves was formulated in 1977 by Lang and Trotter [10]. Let $E/\mathbb{Q}$ be an elliptic curve, and let $P \in E(\mathbb{Q})$ be a point of infinite order. For a prime p of good reduction, write $\bar{P}$ for the reduction of P in the finite abelian group $E(\mathbb{F}_p)$. The point P is said to be *primitive* modulo p if $E(\mathbb{F}_p) = \langle \bar{P} \rangle$. Subject to certain necessary arithmetic restrictions, Lang and Trotter predicted that P is primitive modulo infinitely many primes p , and indeed predicted a precise positive density for these primes in terms of the Galois actions on the torsion points of E and the division points of P . More precisely, their prediction in these cases is

$$\#\{p < X : E(\mathbb{F}_p) = \langle \bar{P} \rangle\} \sim \delta_{E,P} \text{Li}(X), \quad \delta_{E,P} > 0, \quad (1)$$

where $\text{Li}(X) = \int_2^X dt/\log t$ and bad reduction primes are omitted. This is known as the *Lang–Trotter primitive-point conjecture*; it is also known, naturally, as the elliptic analogue of Artin’s conjecture.

The positive-density asymptotic (1) has not previously been proved unconditionally for any explicitly specified pair (E, P) with $\delta_{E,P} > 0$. In fact, even the infinitude of primes p for which $E(\mathbb{F}_p) = \langle \bar{P} \rangle$ had not previously been proven unconditionally for a single explicit pair (E, P) . Under the generalized Riemann hypothesis (GRH), Gupta and Murty [5] established the predicted positive-density asymptotic for many elliptic curves with complex multiplication and suitable rational points, with the primes restricted to those splitting in the CM field.

The purpose of this article is to prove that the pair (E, P) , where $E/\mathbb{Q}$ is defined by $E : y^2 = x^3 - 2x$ and $P = (2, 2)$, satisfies the positive-proportion part of the Lang–Trotter prediction: P generates $E(\mathbb{F}_p)$ for a positive proportion of primes p .

Theorem 1. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 2x$, and let $P = (2, 2)$, a rational point on E of infinite order. Suppose that, for some real number $N \geq 2$, every Dedekind zeta function has no zeros in the half-plane

$$\Re s > 1 - \frac{1}{N}. \quad (2)$$

Then there is a constant $c > 0$, independent of N , such that

$$\#\{p < X : p \equiv 3 \pmod{8}, E(\mathbb{F}_p) = \langle \overline{P} \rangle\} \geq \frac{c}{N \log N} \frac{X}{\log X} \quad (3)$$

for all sufficiently large X , with a threshold that may depend on N . In particular, P is primitive modulo infinitely many primes, and these primes have positive lower density among all primes.

The methods behind the proof of Theorem 1 apply to many other elliptic curves E and points P as well. In this direction, we will prove the following theorem.

Theorem 2. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by an order in $K = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is squarefree, and suppose that E has a model

$$E : y^2 = x(x^2 + Ax + B), \quad A, B \in \mathbb{Q}. \quad (4)$$

Let $P = (u, v) \in E(\mathbb{Q})$ have infinite order, and put $D = A^2 - 4B$. Suppose that

$$d^{e_1} D^{e_2} u^{e_3} (-3)^{e_4} \in \mathbb{Q}^{\times 2}, \quad e_i \in \{0, 1\} \implies e_1 + e_2 + e_3 \equiv 0 \pmod{2}. \quad (5)$$

Then, under the zero-free hypothesis of Theorem 1, there is a constant $c_{E,P} > 0$, independent of $N \geq 2$, such that

$$\liminf_{X \rightarrow \infty} \frac{\#\{p < X : p \text{ of good reduction, } E(\mathbb{F}_p) = \langle \overline{P} \rangle\}}{\pi(X)} \geq \frac{c_{E,P}}{N \log N}.$$

Table 1 provides some further examples to which Theorem 2 applies. In each case the displayed point has infinite order, and the theorem provides a positive lower density of primes for which its reduction generates the group. We check the required arithmetic hypotheses in Section 7.

Curve E	Point P	$j(E)$	CM field
$y^2 = x^3 - 6x$	$(3, 3)$	1728	$\mathbb{Q}(i)$
$y^2 = x^3 + 14x$	$(2, 6)$	1728	$\mathbb{Q}(i)$
$y^2 = x^3 + 4x^2 + 2x$	$(-2, 2)$	8000	$\mathbb{Q}(\sqrt{-2})$
$y^2 = x^3 - 30x + 56$	$(2, 2)$	8000	$\mathbb{Q}(\sqrt{-2})$
$y^2 = x^3 - 35x + 98$	$(1, 8)$	-3375	$\mathbb{Q}(\sqrt{-7})$
$y^2 = x^3 + 42x^2 - 7x$	$(-7, 42)$	16581375	$\mathbb{Q}(\sqrt{-7})$

Table 1: Further examples covered by Theorem 2.

Previous work and scope of the result

This article forms a follow-up to [1], where we established that every integer a that is neither a square nor -1 is a primitive root modulo a positive lower density of primes. We retain some of the same analytic framework: the marked Type II estimates of OpenAI [11, 13], the zero-free half-plane for Dedekind zeta functions of Cureton and Thorner [3], and a sieve in which a small cofactor is allowed to vary. As before, averaging over the cofactors supplies an extra logarithm needed to go from infinitude to a positive proportion, and a positive smoothed explicit formula controls the small prime divisors of the index.

However, the elliptic-curve problem also requires a number of additional arguments. We begin by selecting inert primes for which the group is cyclic of order $p + 1$ and the chosen point has odd index, and verify the change from prime predecessors to prime successors in the marked estimates. To exclude small odd prime divisors of the index, we adjoin a real cyclotomic field to the field generated by a division point. The resulting multiplicity of degree-one primes gives the summable bound needed to discard these failures. A height bound for multiples of the point handles the distinguished large prime divisor. These arguments establish Theorem 1. For Theorem 2, we verify the corresponding division-field bounds for general CM pairs and give a squareclass criterion that constructs the required arithmetic progressions.

Cureton and Thorner [3, 4] announced that, for every number field K , the Dedekind zeta function $\zeta_K(s)$ has no zeros in $\Re s > 31/32$. Thus their updated theorem supplies $N = 32$ in Theorems 1 and 2; the original version had given $N = 6000$. Together with the marked Type II estimates of OpenAI, this gives the asserted positive proportion. We have retained N in the statements so that any further improvement in the zero-free width can be used directly. The argument gives a lower bound; it does not establish the exact density predicted in (1).

In 1967, Hooley [7] proved the classical Artin conjecture under a suitable generalized Riemann hypothesis. For elliptic curves, Gupta and Murty [5] obtained a GRH asymptotic in 1986 for a fixed point on a curve with CM by a maximal order, restricted to primes splitting in the CM field K . Their positivity theorem applies when $K = \mathbb{Q}(\sqrt{-d})$ with

$$d \in \{11, 19, 43, 67, 163\}. \quad (6)$$

They also studied higher-rank subgroups, including non-CM curves under GRH, and obtained an unconditional finite-set infinitude result for certain CM curves of rank at least six. More precisely, their corollary on page 16 constructs an explicit finite set $S \subset E(\mathbb{Q})$ such that at least one point $P \in S$ is primitive modulo infinitely many primes. However, their argument does not identify which point in S has the property, and it does not give a positive proportion of primes.

Gupta and Murty subsequently treated inert primes in [6]. Under GRH, they obtained a positive lower-density result for the reduction of a subgroup of rank at least two on a CM curve, whenever the predicted density is positive, and the predicted asymptotic for subgroups of rank at least six. This leaves a real distinction between several rational generators and one prescribed point. Chen and Yu [2] subsequently determined explicitly when the density in the split-prime problem is positive. The general single-point problem has remained substantially more difficult than the classical Artin problem, even under GRH. Jones, Pappalardi, and Steinhagen [8] provided a detailed account of the local and entanglement obstructions.

Some arithmetic restrictions in the conjecture of Lang and Trotter are necessary. For example, if all the points of order two of E are rational, then $E(\mathbb{F}_p)$ contains a copy of $(\mathbb{Z}/2\mathbb{Z})^2$ at every odd good prime and cannot be generated by one point. Even when the group can be cyclic, the chosen point can be locally imprimitive. Moreover, the division fields need not be independent, so a density formula must account for their intersections. These qualifications are essential to the

positive-density prediction. The example in Theorem 1 avoids these obstructions by a particularly simple choice of congruence class.

The hypotheses of Theorem 2 arrange that the reduced group is cyclic of order $p + 1$ and that the index of the chosen point is odd. The numbers B, D, u, v are nonzero by nonsingularity and the infinite order of P . Condition (5) says that the quadratic characters associated to d, D, u can all take the value -1 while the character associated to -3 takes the value $+1$.

For $j(E) = 1728$, the criterion has an especially short form: none of $D, u, -Du$ may be a rational square or -3 times a rational square. For example, it applies for every integer $k \geq 1$ to

$$E_k : y^2 = x^3 + (18k^2 - 4)x, \quad P_k = (2, 6k).$$

Section 7 proves the theorem, checks this family, and describes further points on the original curve. The criterion is sufficient; no classification of all admissible CM pairs is intended.

Our result obtains its lower bound entirely from inert primes, where the group order is $p + 1$. It therefore does not recover all the Gupta–Murty cases with GRH replaced by (2), even if one asks only for a positive proportion. There is a simple reason why an inert-prime argument cannot suffice for every one of their pairs: their positivity theorem includes points $P = 2Q$ with Q nontorsion. At an inert odd good prime the group has even order $p + 1$, so the double $\overline{P} = 2\overline{Q}$ cannot generate it. Such pairs must be treated at split primes, whose group orders are the varying norms $N_{K/\mathbb{Q}}(\pi_p - 1) = p + 1 - a_p$. The prime-successor estimates used here give no corresponding factorization theorem for these norms.

Theorem 2 gives sufficient conditions for this inert-prime argument. Its rational 2-torsion and squareclass hypotheses do not hold for all CM curves and points. Section 7 explains the remaining finite Galois conditions, the split-prime obstruction just described, and what the fixed zero-free half-plane already gives for the higher-rank theorem of Gupta and Murty. In particular, their earlier CM subgroup theorem applies when its rank r satisfies $r + 1 \geq N$; this concerns joint generation by the subgroup, rather than one prescribed point.

The strategy of proof

We now describe the proof. This also indicates the purpose of each of the parameters introduced below. Write

$$i_p = [E(\mathbb{F}_p) : \langle \overline{P} \rangle].$$

Our aim is to produce a positive proportion of primes for which $i_p = 1$.

1. *Reduce the problem to prime divisors of the index.* For $p \equiv 3 \pmod{8}$, the group $E(\mathbb{F}_p)$ is cyclic of order $p + 1$, and $\overline{P}$ is not twice another point. Thus i_p is odd. These facts follow from a character sum, the rational 2-torsion, and the duplication formula. We prove them in Section 2.
2. *Restrict the factorization of the group order.* We count primes with

$$p + 1 = 4rQ, \quad r \leq x^\epsilon, \quad Q \text{ prime},$$

and with every prime factor of r greater than a fixed cutoff Y . Here r is the *cofactor*: after removing the forced factor 4 and the distinguished large prime Q , it is what remains of $p + 1$. The prime Q is nearly as large as p , while all the prime factors of r are at most x^ϵ .

3. *Let the cofactor vary.* Keeping r fixed would lead to a prime-pair problem. Instead we sum over a family of cofactors with reciprocal mass

$$\sum_r \frac{1}{r} \gg \frac{\epsilon \log x}{\log Y}.$$

This extra factor of $\log x$ is what permits a positive proportion of primes.

4. *Count the candidate primes.* The marked Type II estimates of OpenAI allow a sieve to retain the condition on $p + 1$ while distinguishing primes from the remaining semiprimes. The resulting candidate count is $\gg \epsilon x / (\log Y \log x)$. Section 3 gives the full cofactor deduction and the required change of sign. The quoted marked estimates themselves are the external analytic input.
5. *Remove the failures of the primitive-point condition.* We first remove the prime divisors of the index coming from r . Choose Y beyond the finitely many exceptional division primes. For $Y < q \leq x^\epsilon$, choose R_q with $qR_q = P$ and set

$$T_q = \mathbb{Q}(R_q, \zeta_q + \zeta_q^{-1}).$$

If $q \mid i_p$, then T_q has $q(q-1)/2$ degree-one primes above p . Its degree is $q^2(q-1)/2$ for all sufficiently large q . Counting these degree-one primes by a positive smoothed explicit formula gives a summable main bound of order $1/q^2$. The total number discarded is

$$\ll \frac{x}{Y \log Y \log x} + \frac{x^{1-1/N+2\epsilon}}{\log x}.$$

Sections 4 and 5 give these arguments.

It remains to remove the large prime Q . If $Q \mid i_p$, then $\bar{P}$ has order at most $4r$. A height estimate shows that the primes where a fixed nontorsion point has order at most T number $O(T^3/\log x)$ in $(x, 2x)$. Thus the large prime costs only $O(x^{3\epsilon}/\log x)$. This explains why we do not need all the prime factors of $p + 1$ to be small: the one large factor is handled by a different argument.

6. *Choose the parameters.* Take $\epsilon = \theta/N$ with a sufficiently small fixed $\theta > 0$, then take Y a sufficiently large fixed multiple of $1/\epsilon$. The two power-saving errors are negligible, and the main loss is smaller than the candidate count. Since $\epsilon/\log Y \gg 1/(N \log N)$, this gives the theorem. Section 6 makes the choices precise.

The real cyclotomic field in T_q deserves emphasis. The field generated by R_q alone would have only q fixed embeddings at a bad prime and would give a main bound of order $1/q$. Adjoining $\zeta_q + \zeta_q^{-1}$ supplies the additional factor $q-1$ because $p \equiv -1 \pmod{q}$. The resulting series over q converges. All that is needed analytically then is a prime-ideal upper bound for this non-Galois field; no general effective Chebotarev theorem is required.

2 The curve, the point, and the chosen primes

We begin with the elementary features of the example. They explain both the equation of the curve and the progression used throughout the proof.

Lemma 3. *The point $P = (2, 2)$ on $E : y^2 = x^3 - 2x$ has infinite order. For every prime $p \equiv 3 \pmod{8}$, the group $E(\mathbb{F}_p)$ is cyclic of order $p + 1$, and $i_p = [E(\mathbb{F}_p) : \langle \overline{P} \rangle]$ is odd.*

Proof. The discriminant of the integral equation is 512, so every odd prime is a prime of good reduction. Direct duplication gives $2P = (9/4, -21/8)$. If P were torsion, then $2P$ would be a finite rational torsion point with nonintegral coordinates, contrary to the Lutz–Nagell theorem; see [17].

For $p \equiv 3 \pmod{4}$, write χ for the quadratic character of $\mathbb{F}_p$, extended by $\chi(0) = 0$. Counting the possible y -coordinates above each $t \in \mathbb{F}_p$ gives

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{t \in \mathbb{F}_p} \chi(t^3 - 2t).$$

The terms at t and $-t$ cancel, because $\chi(-1) = -1$. The term at zero vanishes, so the group order is exactly $p + 1$. Equivalently, the Frobenius trace $a_p = p + 1 - \#E(\mathbb{F}_p)$ is zero.

The structure theorem and the Weil pairing give $E(\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$, with $d \mid e$ and $d \mid p - 1$. Since d also divides $p + 1$, we have $d \mid 2$. The nonzero points of order two have $y = 0$, hence $x = 0$ or $x^2 = 2$. For $p \equiv 3 \pmod{8}$, 2 is a nonsquare, so only $(0, 0)$ is rational. This rules out $d = 2$, which would give three nonzero rational points of order two. Thus $d = 1$ and the group is cyclic.

Finally the duplication formula simplifies to

$$x(2R) = \left(\frac{x(R)^2 + 2}{2y(R)} \right)^2 \quad (y(R) \neq 0). \quad (7)$$

If $2R = \overline{P}$, neither the identity nor a point of order two can be R , so the formula applies. Its right side is a square, whereas $x(\overline{P}) = 2$ is a nonsquare. Hence $\overline{P} \notin 2E(\mathbb{F}_p)$. In a cyclic group of even order n , writing $\overline{P} = kg$ for a generator g , this says that k is odd. Its index is (k, n) , which is therefore odd. $\square$

At these primes the factor 4 always divides $p + 1$, but 8 does not. The lemma has already removed the entire obstruction at 2, including higher powers of 2. It remains to prevent odd primes from dividing the index. We next construct the family of group orders for which this can be done with a fixed zero-free width.

3 Prime successors with a small cofactor

The analytic part of the proof concerns the factorization of $p + 1$ and is independent of the elliptic curve. We prove it for a fixed arithmetic progression, so that it can be used again in the more general theorem.

Fix positive integers M , c , and an integer u , with c a power of two, such that

$$c \mid M, \quad 2 \mid M/c, \quad (u, M) = 1, \quad c \mid u + 1, \quad \left(\frac{u + 1}{c}, \frac{M}{c} \right) = 1. \quad (8)$$

Put $M_0 = M/c$. These conditions mean that a prime $p \equiv u \pmod{M}$ has precisely the power c of two dividing $p + 1$, and that no odd prime dividing M is forced to divide $p + 1$. For our principal example the choices are $M = 8$, $u = 3$, and $c = 4$.

Proposition 4 (Prime-successor candidates). *There are constants $A_0 > 0$, $\epsilon_0 > 0$, and $Y_0 \geq 3$, depending only on the fixed progression in (8), such that the following holds. For every fixed $0 < \epsilon < \epsilon_0$ and $Y \geq Y_0$, the number of primes $p \in (x, 2x)$ satisfying*

$$p \equiv u \pmod{M}, \quad p + 1 = crQ, \quad r \leq x^\epsilon, \quad Q > x^{0.9} \text{ prime}, \quad q \mid r \implies q > Y \quad (9)$$

is at least

$$A_0 \frac{\epsilon}{\log Y} \frac{x}{\log x}$$

for all sufficiently large x . Here q ranges over primes, and the threshold for x may depend on ϵ and Y .

The proof occupies the following subsections. Its analytic input is the marked replacement estimate of [13, 11], in a signed form explained below. We reproduce the cofactor argument of [1], retaining the dependence on both ϵ and Y . This dependence is essential: we will eventually take ϵ proportional to a zero-free width and Y proportional to its reciprocal.

A single fixed cofactor would give the prime-pair scale $x/\log^2 x$. We instead use a family whose reciprocal sum has size $\epsilon \log x/\log Y$. The extra factor of $\log x$ is what produces a positive proportion of primes. The lower bound is proved after summing over the whole family; no lower bound for a pair of primes with an individual fixed cofactor is asserted.

Throughout this section $L = \log x$. We fix a smooth function $0 \leq \Psi \leq 1$, compactly supported in $(1, 2)$, with $\int \Psi > 0$. For an integer $n > 1$, $P^-(n)$ denotes its least prime factor, and $P^-(1) = \infty$. All auxiliary parameters are fixed before x tends to infinity.

3.1 The marked replacement principle

The following input is the only part of the argument specific to the marked construction. We state it in the form needed here. Its role is to let us sieve one factor of a product without losing the condition imposed on the successor of that product. We state the estimate for both signs, since the sources use the predecessor.

Set

$$L = \log x, \quad W = \exp(L^{0.24}), \quad V(y) = \prod_{\ell \leq y} (1 - 1/\ell).$$

Choose a fixed positive integer K , and fixed numbers $0.1 < a_1 < \dots < a_K < 0.2$. Let

$$\mathcal{P}_i = \{\ell \text{ prime} : e^{L^{a_i}} \leq \ell \leq e^{2L^{a_i}}\}, \quad V_i = \sum_{\ell \in \mathcal{P}_i} \frac{1}{\ell}.$$

We call these the marked prime groups. They are disjoint for large x , and $V_i = \log 2 + o(1)$. For a positive integer h , put $h_{\mathcal{P}} = \prod_{\ell \in \cup_i \mathcal{P}_i} \ell^{v_\ell(h)}$, the part of h supported on the marked primes, and define

$$\omega_i(h) = \#\{\ell \in \mathcal{P}_i : \ell \mid h\}, \quad \mathcal{W}(h) = \prod_{i=1}^K \frac{\omega_i(h) 2^{1-\omega_i(h)}}{V_i}. \quad (10)$$

The factor $\omega_i(h)$ counts the choices of a marked prime in the group, while $2^{1-\omega_i(h)}$ limits the weight of integers with many such prime divisors. A factor with $\omega_i = 0$ is zero. For large x ,

$$0 \leq \mathcal{W}(h) \leq B_K \quad (11)$$

with a constant depending only on K : for an integer $j \geq 1$, the factor $j 2^{1-j}$ is at most one, and the V_i are bounded away from zero.

A positive integer is called z -rough if it has no prime factor at most z . The density of rough integers is described by Buchstab's function ω_B : $\omega_B(u) = 1/u$ for $1 \leq u \leq 2$, and $(u\omega_B(u))' = \omega_B(u-1)$ for $u > 2$. For $s > \gamma > 0$, write

$$D_\gamma(s) = \gamma^{-1} \omega_B(s/\gamma), \quad R_\gamma(m) = \mathbf{1}_{P^-(m) > x^\gamma}, \quad B_\gamma(m) = \frac{D_\gamma(\log m/L)}{LV(W)} \mathbf{1}_{P^-(m) > W}. \quad (12)$$

This is the same density as that defined by the prime-product integrals in [13, (10.11)]. Indeed, writing those terms as $D_{\gamma,j}$, one has

$$D_{\gamma,1}(s) = \frac{1}{s}, \quad D_{\gamma,j}(s) = \frac{1}{j!} \int_{\substack{t_i \geq \gamma \ (1 \leq i < j) \\ \sum_{i < j} t_i \leq s - \gamma}} \frac{1}{s - \sum_{i < j} t_i} \prod_{i < j} \frac{dt_i}{t_i} \quad (j \geq 2).$$

The sum over j is locally finite. By symmetry among the j prime factors, multiplication by s cancels one denominator and gives

$$sD_{\gamma,j}(s) = \frac{1}{(j-1)!} \int_{\substack{t_i \geq \gamma \ (1 \leq i < j) \\ \sum_{i < j} t_i \leq s - \gamma}} \prod_{i < j} \frac{dt_i}{t_i}.$$

Differentiating and summing gives $(sD_{\gamma}(s))' = D_{\gamma}(s - \gamma)$ for $s > 2\gamma$, with $sD_{\gamma}(s) = 1$ for $\gamma < s \leq 2\gamma$. Rescaling Buchstab's defining equation therefore identifies the two densities, interval by interval. This also gives their joint continuity on compact subsets of $s > \gamma > 0$.

Proposition 5 (Signed marked replacement). *Fix a modulus M , a reduced residue u , a smooth function Ψ compactly supported in $(1, 2)$, and fixed numbers*

$$\beta > 0, \quad 0 < \gamma < s_- < s_+ < 1.$$

Fix also $\sigma \in \{1, -1\}$. For K sufficiently large in terms of these data and the comparison constants below, the following holds. If $H_m, H_n \geq x^\beta$, $H_m H_n \asymp x$ with fixed comparison constants, and the full m -dyad has logarithmic exponents in $[s_-, s_+]$, then

$$\sum_{\substack{m \in I \\ H_n \leq n < 2H_n}} (R_{\gamma}(m) - B_{\gamma}(m)) b_n \mathbf{1}_{mn \equiv u \pmod{M}} \Psi(mn/x) F_x(mn - \sigma) \mathcal{W}(mn - \sigma) \ll xL^{-6}. \quad (13)$$

Here $I \subseteq [H_m, 2H_m]$ is any interval, $|b_n| \leq 1$ is supported on W -rough integers, and

$$|F_x(h)| \leq 1, \quad F_x(\ell h) = F_x(h) \quad (h \geq 1, \ell \in \bigcup_i \mathcal{P}_i). \quad (14)$$

The estimate has one implied constant and one threshold for x , simultaneously for all permitted dyads, functions F_x , intervals, and coefficients in the fixed exponent window. Thus it also applies to a family of dyads growing with x . The required lower bound on K is independent of F_x and of the particular a_i . Constants and thresholds may depend on the fixed band exponents.

Deduction from the cited estimates. For $\sigma = 1$, we use [13, Lemma 10.2 and Proposition 10.3], with damping parameter $1/2$. The signed extension is checked in detail immediately after this proof; its constants and hypotheses are the same. These results allow every bounded invariant selector F_x , uniformly over its choice. Proposition 10.3 supplies the rough-factor discrepancy $R_{\gamma} - B_{\gamma}$, including real power twists m^{iv} . We explain how to add the progression and the smooth weight, following the proof of [13, Lemma 12.1].

Since $(u, M) = 1$, character orthogonality gives

$$\mathbf{1}_{mn \equiv u \pmod{M}} = \frac{1}{\varphi(M)} \sum_{\lambda \bmod M} \overline{\lambda(u)} \lambda(m) \lambda(n).$$

Here a Dirichlet character is extended by zero on integers not coprime to its modulus. To separate the smooth weight, put

$$\widehat{\psi}(v) = \frac{1}{2\pi} \int_{\mathbb{R}} \Psi(e^t) e^{-ivt} dt.$$

Fourier inversion yields

$$\Psi(mn/x) = \int_{\mathbb{R}} \widehat{\psi}(v) x^{-iv} m^{iv} n^{iv} dv.$$

The function $\widehat{\psi}$ decreases faster than every negative power of $1 + |v|$.

For each character λ and $|v| \leq L$, apply the coefficient criterion of [13, Lemma 10.2], with $C = 2$ and $D_* = 6$, to

$$\alpha_m = \mathbf{1}_I(m) m^{iv} \lambda(m) (R_\gamma(m) - B_\gamma(m)), \quad \beta_n = b_n n^{iv} \lambda(n).$$

Both sequences are supported on W -rough integers and have absolute value at most L^2 for large x . The character-transform estimates required by that criterion are verified in the proof of [13, Proposition 10.3], for every fixed logarithmic modulus range, frequency range, and desired saving. Multiplication by the fixed character λ preserves them: a character χ of modulus $k \leq L^A$ becomes $\lambda\chi$, of modulus $\text{lcm}(M, k) \leq L^{A+1}$ for large x . The factor m^{iv} , with $|v| \leq L$, shifts a tested frequency by at most L ; increasing its fixed logarithmic range by one absorbs this shift. The criterion therefore bounds the inner marked sum by $O(xL^{-6})$, uniformly in λ, v and F_x .

Integrating over $|v| \leq L$ preserves this bound because $\int |\widehat{\psi}(v)| dv$ is finite. On the remaining tail the coefficient bounds and (11) give the sufficient crude bound $O_K(xL^2)$; rapid decay makes its integral $O_{K,\Psi,A}(xL^{-A})$ for every fixed A . Summing over the finitely many characters proves (13).

Finally we record where the two uniformities asserted in the statement come from, since Section 3.5 applies the proposition to a family of $O(L)$ dyads that depends on x .

Uniformity in F_x . In the proof of [11, Theorem 3.1], which [13, Lemma 10.2] re-reads with the coefficient hypothesis isolated, the selector enters at exactly two points. Writing $mn - \sigma = ah$ with a the product of the selected marked primes, invariance gives $F_x(mn - \sigma) = F_x(h)$; and in the Cauchy–Schwarz step of [11, Section 3.1] the bounded factor $F_x(h)q^{\omega(h)}$ is placed in the trivial factor $\sum_h |F_x(h)q^{\omega(h)}|^2 \ll X/Y_*$, so that the expanded square Q_{Y_*} of [11, (3.8)] does not involve F_x at all. Every subsequent estimate—the determinant moment [11, Proposition 4.1] and the major term [11, Proposition 5.1]—concerns α, β and the selected products alone. The number of groups is chosen from the accuracy required of Q_{Y_*} : following [11, Proposition 4.1 and the completion of the proof of Theorem 3.1], one fixes the square accuracy D_1 in terms of (D_*, C) , then E_0 , then the arc exponent A_0 , and finally K , in terms of (δ, C, D_*, q) only. Hence K depends neither on the selector, nor on the band exponents a_i [11, Proposition 4.1], nor on the dyads.

Uniformity over the dyads. The statement of [11, Theorem 3.1] quantifies over all scales $H_m, H_n \geq x^\delta$ with $H_m H_n \asymp x$, the implied constant and threshold depending only on the fixed parameters $(\delta, C, D_*, q, K, a_i)$; [13, Lemma 10.2] adds only the fixed data of its hypothesis (10.6), and [13, Proposition 10.3] adds only (γ, w_-, w_+) and the requested accuracy. Correspondingly, every analytic input of the proof is stated for an arbitrary scale in a range cut out by fixed exponents, with constants depending only on those exponents: the long prime polynomial and logarithmic-phase estimates [11, Lemmas 2.3 and 2.4], uniform for $x^\tau/2 \leq N \leq x^\eta$ and for $\exp(L/(\log L)^2) \leq N \leq 2x^5$ respectively; the rough counts [11, Lemma 2.5], uniform for $x^\delta \leq H \leq x^C$; the root-residue count [11, Lemma 3.3], with error UVx^{-c_δ} , $c_\delta = \delta/1000$; the endpoint norms [11, (3.18)], which involve only the coefficient bound C ; the operator bounds of [11, Section 4], which involve only Y_*, L, K, A_0, q ; and the two major-arc lemmas [11, Lemmas 5.2 and 5.3], stated for $x^\delta \leq H_m, H_n \ll x$. In our application $\delta = \beta = b/2$, and the window hypothesis $[\log H_m/L, \log(2H_m)/L] \subseteq [s_-, s_+] = [1/2 + \xi/2, 1 - b/2]$ holds for every active m -dyad once x is large in terms of b, ξ alone. All parameters on which the constant and threshold depend $(M, u, \Psi, \beta, \gamma, s_\pm, K, a_i)$ are fixed in Section 3.7 before $x \rightarrow \infty$, and none is a function of the dyad. Thus one implied constant and one threshold serve all $O(L)$ dyads, exactly as in the application of [13, Lemma 12.1] to $O(L)$ pairs of dyads in [13, Section 12.4]. $\square$

The selector constructed below satisfies (14), including when $\ell \mid h$. The uniformity just proved applies to the entire cofactor family. In particular, the number K of marked groups will not depend on a zero-free width.

For intuition, R_γ is an exact roughness condition. The weight B_γ imposes only the much weaker condition of being W -rough, and multiplies it by the ratio of the two expected densities. Proposition 5 says that this replacement is valid inside the displayed marked sum. Its proof uses the cited marked Type II estimates and uses no zero-free hypothesis.

The sign in the marked estimate

The cited estimates are written for $mn - 1$. We record how their proofs change for $mn - \sigma$, where $\sigma \in \{1, -1\}$. This is the only extension of that analytic input needed here. The subsequent proof always uses $\sigma = -1$.

The shift σ enters the proof of [11, Theorem 3.1] at the following places and nowhere else: the square-collision bound [11, (3.6)]; the divisor bound [11, (3.9)], used again at [11, (4.60)]; the determinant relation [11, (3.10)] and the kernel [11, (3.11), (3.15)]; the primitivity remark following [11, (3.17)]; the target count [11, (4.23)]; the clean-edge kernel [11, (4.29)]; the dirty-edge residue calculation [11, (4.35)–(4.36)]; and the rational and real phases in the proof of [11, Proposition 5.1]. We go through these in order. Everything else in [11, Sections 3–5]—the root-residue count, the independent-line replacement, the primewise identity, the ghost and truncation estimates, the comparison edges, the rank expansion restoring birth distinctness, and the stripping of the pads—concerns only which group primes divide first coordinates and the geometry of the positions, and never sees σ .

In the marked expansion write $mn - \sigma = ah$, with a the product of one selected prime from every group. Invariance gives $F_x(mn - \sigma) = F_x(h)$. A square collision, in which a selected prime ℓ has $\ell^2 \mid mn - \sigma$, requires $mn \equiv \sigma \pmod{\ell^2}$, which still specifies at most one residue class for n once m is fixed and invertible; this is [11, (3.6)]. Pairs a, b sharing a selected prime are discarded using the divisor bound $\sum_{h \ll X/Y_*} \tau(1 + lh)^2 \ll (X/Y_*)L^3$ of [11, (3.9)], whose proof uses only that $d \mid lh + 1$ forces $(d, l) = 1$ and places h in one class modulo d ; both facts hold verbatim for $d \mid lh + \sigma$. Thus the collision errors and the errors from repeated labels have the same bounds for either sign.

After Cauchy–Schwarz the two equations are

$$mn - \sigma = ah, \quad m'n' - \sigma = bh.$$

For coprime selected products a, b , their common- h condition becomes

$$bmn - am'n' = \sigma(b - a). \tag{15}$$

Conversely, this determinant equation implies the two divisibilities and the equality of the quotients; the quotients are positive on the large variable ranges being considered. Thus the major-arc kernel in [11, (3.11)] becomes

$$H_{\mathcal{M}, \sigma}(t; a, b) = \psi(t/Y_*) \int_{\mathcal{M}} e(\vartheta(t - \sigma b + \sigma a)) d\vartheta.$$

Here Y_* is the dyadic scale of the selected products, ψ is the fixed smooth cutoff in that proof, $e(t) = \exp(2\pi it)$, and $\mathcal{M}$ is the union of its rational major arcs. We use Y_* here to distinguish this scale from our fixed small-prime cutoff Y .

The physical states, boxes, and primitive vectors in the operator proof are unchanged: the primitivity of the physical positions, shown after [11, (3.17)], uses only $|t| \ll Y_* < W$, which holds

for $t = \sigma(b - a)$ with $a, b \asymp Y_*$; and in [11, (4.23)] the raw determinant $j_1 = \sigma D(b - a)$ is still determined by the labels, so a raw edge still has $O(1)$ targets. The clean minor-arc estimate is a norm estimate for the determinant matrix $e(\vartheta \det(v, w))$, multiplied by separate unit-modulus factors at the two endpoints. Changing σ changes only these endpoint factors and the signs of Fourier frequencies; the norm bound is unchanged. The major-arc set is invariant under negation. Explicitly, in the product variable the kernel of [11, (4.29)] becomes

$$\frac{1}{Y_*} \psi\left(\frac{\det(h, l)}{Y_*}\right) \int_{\mathbb{R}/\mathbb{Z} \setminus \mathcal{M}} e(\vartheta \det(h, l)) e(\sigma \vartheta(a - b)) d\vartheta.$$

The substitution $\vartheta \mapsto \sigma \vartheta$ preserves $\mathbb{R}/\mathbb{Z} \setminus \mathcal{M}$, so the Fourier fibers in the product variable are the determinant matrices $\psi(\det(h, l)/Y_*) e(\sigma \vartheta \det(h, l))/Y_*$ with $\vartheta \notin \mathcal{M}$: the same family as in [11, (4.30)]. Hence the Dirichlet approximation [11, (4.31)] and the norm bounds [11, (4.32)–(4.34)] apply verbatim.

There is one residue calculation in the dirty-edge estimate for which it is useful to make the sign explicit. In the notation of [11, Section 4.6], its raw determinant is now

$$j_1 = \sigma P_{\text{full}} - \sigma D p_* Z T_f.$$

The ban on repeated numeric labels gives $p_* \nmid P_{\text{full}}$. Consequently $j_1 \equiv \sigma P_{\text{full}} \not\equiv 0 \pmod{p_*}$, independently of D and Z . The projective-line condition therefore still fixes a single residue $h = h_* \pmod{p_*}$, independently of those two products. (The residue h_* itself depends on σ , through $j_1 \pmod{p_*}$; only its independence of D and Z is used.) Since $h = h_* + p_* k$ for some integer k , the resulting condition is a distance modulo one. In place of [11, (4.36)] we obtain

$$\left\| D Z T_f r_z^* - \frac{P_{\text{full}} r_z^* + \sigma h_*}{p_*} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{16}{p_*},$$

where $\|t\|_{\mathbb{R}/\mathbb{Z}} = \min_{n \in \mathbb{Z}} |t - n|$. The resulting arc has the same length as in the original argument. The phase-separation argument therefore allows at most one product DZ , just as before. The factorization of DZ into old and new labels, the two Schur estimates, and the adjoint argument are unchanged. For the adjoint, reversing an edge interchanges the roles of a, b , replaces t by $-t$, and conjugates the multiplier; since $\mathcal{M} = -\mathcal{M}$, the reversed multiplier is again $\mathbf{1}_{t=\sigma(b-a)} - \int_{\mathcal{M}} e(\vartheta(t - \sigma b + \sigma a)) d\vartheta$ in the reversed labelling, and its raw determinant is again σ times (source full product minus D times the target unshared product). The column estimates in the table of [11, Section 4.6] therefore follow from the row estimates exactly as there. This checks the part of the operator proof in which the nonzero shifted determinant is used arithmetically.

Finally, the major-arc rational phase is

$$e(h[bmn - am'n' - \sigma b + \sigma a]/k).$$

The real phases that depend separately on a, b become $e(-\sigma \lambda b/Y_*) e(\sigma \lambda a/Y_*)$. That is, the endpoint polynomial B_λ of [11, (5.17)] is replaced by $B_{\sigma \lambda}$ at one endpoint and by its conjugate at the other. The bounds used for it— $|B_\lambda| \ll 1$, and the Mellin L^1 -bound $\ll L^{C_5}$ for $f_\lambda(y) = \eta(y) e(-\lambda y)$ in the proof of [11, Proposition 5.1]—are uniform over $|\lambda| \leq 2L^{A_0}$, a range symmetric under $\lambda \mapsto -\lambda$. The rational phase remains a bounded function on $((\mathbb{Z}/k\mathbb{Z})^\times)^6$, expanded in products of six characters with coefficients of modulus at most one, which is all that proof uses of it. The mean-square bound [11, (5.19)] and [11, Lemmas 5.2 and 5.3] do not involve σ .

The character transforms, their mean-square bounds, and the sparse frequency estimate used in [11, Section 5] are thus uniform under these sign changes. The bounded coefficient criterion of

[13, Lemma 10.2] follows with the same accuracy and parameter choices. Its rough-factor version, Proposition 10.3 there, consequently has the signed form used above. This verifies the extension without altering either the required number of marks or its independence from the invariant selector. We use the cited operator estimates themselves; we do not assume a Poisson–Dirichlet theorem in arithmetic progressions.

3.2 A cofactor with a large reciprocal sum

The sieve normalization for a cofactor r is on the scale $x/(rL^2)$. We therefore seek a family for which $\sum 1/r$ has size L ; the prime-pair lower bound will be proved only after summing over this family. The next lemma constructs such a family while keeping its sieve factors close to those of a fixed cofactor.

The constants $\epsilon, \tau > 0$ will be small, with $\epsilon < 0.01$; $Y \geq 3$ will be large. All are fixed before x tends to infinity. Put

$$R = x^{\epsilon/2}, \quad Z = x^{\epsilon/8} = R^{1/4}.$$

Let $\mathcal{R}_x$ consist of squarefree positive integers r_0 with

$$r_0 \leq R, \quad q \mid r_0 \implies Y < q \leq Z, \quad q \notin \bigcup_i \mathcal{P}_i, \quad \sum_{q \mid r_0} \frac{1}{q} \leq \tau. \quad (16)$$

The integer 1 is permitted. Define

$$H_0 = \sum_{r_0 \in \mathcal{R}_x} \frac{1}{r_0}.$$

Lemma 6. *For Y sufficiently large in terms of τ , and then x sufficiently large,*

$$H_0 \asymp_K \frac{\epsilon L}{\log Y}. \quad (17)$$

The comparison constants can be chosen independently of Y, ϵ, τ , within the stated restrictions; the threshold for x can depend on all of them. If s ranges over integers supported on the marked prime groups, then

$$J_{\mathcal{P}} := \sum_s \frac{\mathcal{W}(s)}{s} \asymp_K 1, \quad J_{\mathcal{P}} \geq 1, \quad \sum_{s > x^t} \frac{\mathcal{W}(s)}{s} \ll_K e^{-tL^{1-a_K}} \quad (t > 0 \text{ fixed}). \quad (18)$$

In particular, for the unique decomposition $r = sr_0$ with these disjoint prime supports,

$$J := \sum_{\substack{s \text{ supported on the groups} \\ r_0 \in \mathcal{R}_x}} \frac{\mathcal{W}(s)}{sr_0} = J_{\mathcal{P}} H_0 \gg_K \frac{\epsilon L}{\log Y}, \quad (19)$$

and

$$\sum_{sr_0 > x^\epsilon} \frac{\mathcal{W}(s)}{sr_0} \ll_K H_0 e^{-(\epsilon/2)L^{1-a_K}}. \quad (20)$$

Proof. First omit the bounds on the size of r_0 and on the sum of reciprocals of its prime divisors. The harmonic mass is

$$H = \prod_{\substack{Y < q \leq Z \\ q \notin \bigcup_i \mathcal{P}_i}} (1 + 1/q) \asymp_K \frac{\log Z}{\log Y}.$$

Mertens' product estimate gives constants independent of $Y \geq 3$; deleting the K groups costs only a factor depending on K . Under the probability measure assigning a squarefree product mass $1/(Hr_0)$, the events $q \mid r_0$ are independent, with probabilities $1/(q+1)$. Therefore

$$\mathbb{E} \log r_0 \leq (1 + o(1)) \log Z, \quad \mathbb{E} \sum_{q \mid r_0} \frac{1}{q} \leq \sum_{n > Y} \frac{1}{n(n+1)} \leq \frac{1}{[Y]}.$$

Markov's inequality removes at most $1/4 + o(1)$ for $r_0 > R$, and at most $1/(\tau[Y])$ for the other restriction. With $Y > 10/\tau$, a fixed positive fraction of H remains. This proves (17).

For the marked mass, define $E_i(t) = \prod_{\ell \in \mathcal{P}_i} (1 + t/(\ell - 1))$. Summing over all positive exponents of each prime gives

$$J_{\mathcal{P}} = \prod_{i=1}^K \frac{E'_i(1/2)}{V_i}.$$

Products consisting of exactly one prime to exponent one from each group contribute 1. The upper bound follows from this Euler product. For the tail, put $v = L^{-a_K}$. Since $\ell^v \leq e^2$ at each group prime, $\sum_s \mathcal{W}(s)/s^{1-v} \ll_K 1$, using (11) and the geometric series at each prime. Rankin's inequality proves (18). Finally $r_0 \leq x^{\epsilon/2}$, so $sr_0 > x^\epsilon$ implies $s > x^{\epsilon/2}$. This proves (19)–(20). $\square$

3.3 Counting the integers before sieving

We now encode the desired successor factorization in a weight on integers d . At this stage d need not be prime. It is the large factor Q of $d+1$ that is prime, so distribution in progressions follows from the usual theorems about rational primes.

A selector is simply a function taking the values zero and one. Define, for every $h \geq 1$,

$$F_x(h) = \mathbf{1}_{\{h/h_{\mathcal{P}} = cr_0Q \text{ for some } r_0 \in \mathcal{R}_x, Q > x^{0.9} \text{ prime}\}}, \quad (21)$$

and

$$w(d) = \mathbf{1}_{d \equiv u \pmod{M}} \Psi(d/x) F_x(d+1) \mathcal{W}(d+1), \quad X_0 = \sum_{d \geq 2} w(d). \quad (22)$$

For every group prime ℓ , $(\ell h)_{\mathcal{P}} = \ell h_{\mathcal{P}}$, even if $\ell \mid h$. Hence $F_x(\ell h) = F_x(h)$, exactly as MR requires.

On the support of w , write $d = csr_0Q - 1 = crQ - 1$. The representation is unique: $s = (d+1)_{\mathcal{P}}$; a prime $Q > x^{0.9}$ cannot divide r_0 , and two such primes cannot divide $(d+1)/c < 2x$. All prime divisors of r_0 are at most $Z < x^{0.9}$. Thus

$$r \leq x^{0.11}, \quad \mathcal{W}(d+1) = \mathcal{W}(s), \quad 0 \leq w(d) \leq B_K \quad (23)$$

for large x . We always take Y larger than the prime divisors of M , so $(r, M) = 1$.

Let $t_r = \mathcal{W}(s)$ when $r = sr_0$ is permitted, and zero otherwise. Define

$$A_r = \sum_{\substack{Q > x^{0.9} \text{ prime} \\ crQ - 1 \equiv u \pmod{M}}} \Psi((crQ - 1)/x).$$

Then $X_0 = \sum_r t_r A_r$ and $\sum_r t_r/r = J$. The contribution from $r > x^\epsilon$ is, by $A_r \ll x/r$,

$$O_K \left(x H_0 e^{-(\epsilon/2)L^{1-a_K}} \right). \quad (24)$$

It is negligible relative to xJL^{-A} , for every fixed A .

We shall also need a lower bound relative to the *full* harmonic mass J . Since $J = J_{\mathcal{P}}H_0 \geq H_0$, (20) implies

$$J_{\leq x^\epsilon} := \sum_{r \leq x^\epsilon} \frac{t_r}{r} = J - O_K \left(H_0 e^{-(\epsilon/2)L^{1-a_K}} \right) \geq \frac{J}{2} \quad (25)$$

for all sufficiently large x . The factor $1/2$ is independent of K , although the threshold may depend on it. The restriction $r \leq x^\epsilon$ is imposed only when estimating this tail; it is not inserted into F_x , since doing so would destroy marked-prime invariance.

Lemma 7. *Suppose $0 < \epsilon < \xi < 0.01$, and put $D = x^{1/2-\xi/2}$. For an odd squarefree ℓ , let $A_r(\ell)$ include the additional condition $\ell \mid crQ - 1$, and put*

$$g_r(\ell) = \frac{\mathbf{1}_{(\ell, Mr)=1}}{\varphi(\ell)}, \quad E_r(\ell) = A_r(\ell) - g_r(\ell)A_r.$$

For every fixed $A > 0$,

$$\sum_{r \leq x^\epsilon} t_r \sum_{\substack{\ell \leq D \\ \ell \text{ odd, squarefree}}} |E_r(\ell)| \ll_{A, M, c, \Psi, \epsilon, \xi} xJL^{-A}. \quad (26)$$

Moreover

$$X_0 \asymp_{M, c, \Psi} \frac{xJ}{L}, \quad (27)$$

with comparison constants independent of $K, Y, \tau, \epsilon, \xi$.

Proof. For $r \leq x^\epsilon$ the lower cutoff on Q is automatic. The progression is the reduced class

$$Q \equiv ((u+1)/c)r^{-1} \pmod{M_0}.$$

If $(\ell, Mr) > 1$, both $A_r(\ell)$ and $g_r(\ell)$ vanish. Otherwise the condition on ℓ combines with it into a reduced class modulo $M_0\ell$. The prime variable has scale $T \asymp x/(cr)$. Take $\eta = (\xi - \epsilon)/4$. Then

$$(1 - \epsilon)(1/2 - \eta) - (1/2 - \xi/2) = (\xi - \epsilon)(1 + \epsilon)/4 > 0.$$

Consequently $M_0\ell \leq T^{1/2-\eta}$ throughout the required range, for large x . The Bombieri–Vinogradov theorem, with its maximum over reduced residue classes, and partial summation give

$$\sum_{\ell \leq D} \left| A_r(\ell) - \frac{g_r(\ell)}{\varphi(M_0)} I_r \right| \ll (x/r)L^{-A'}, \quad I_r = \frac{x}{cr} \int_1^2 \frac{\Psi(y)}{\log((xy+1)/(cr))} dy.$$

The smoothing has bounded total variation independently of r . The term $\ell = 1$ evaluates A_r ; replacing $I_r/\varphi(M_0)$ by A_r in the other terms costs at most a factor $O(L)$, since $\sum_{\ell \leq D} 1/\varphi(\ell) \ll L$. Increase A' , multiply by t_r , and sum to obtain (26). Finally $I_r \asymp_\Psi x/(rL)$, uniformly for $\epsilon < 0.01$. The fixed-modulus prime number theorem, with partial summation, gives

$$A_r = \frac{I_r}{\varphi(M_0)} + o_{M, c, \Psi} \left(\frac{x}{rL} \right) \asymp_{M, c, \Psi} \frac{x}{rL} \quad (r \leq x^\epsilon),$$

simultaneously throughout this range. Indeed the prime scale is at least $x^{0.99}/c$, which tends to infinity uniformly in r , and the finitely many reduced classes modulo M_0 have a common error bound. Multiplying by t_r , summing, and using (25) gives comparison with xJ/L , with constants independent of $K, Y, \tau, \epsilon, \xi$. The tail (24) is $o(xJ/L)$, proving (27). $\square$

Only the two-sided comparison (27) is needed. Since r can be a fixed power of x , we retain $\log(x/r)$ in the integral I_r ; it is comparable to L , but its ratio to L need not tend to one.

3.4 The effect of the cofactor on the sieve

For a fixed r , sieving $crQ - 1$ by an odd prime $\ell \nmid Mr$ removes a proportion $1/(\ell - 1)$ of the reduced residue classes of Q . If $\ell \mid r$, it removes nothing. Thus enlarging r increases the surviving local product. The reciprocal-sum restriction makes this increase uniformly small.

Write

$$V_M(y) = \prod_{\substack{2 < \ell \leq y \\ \ell \nmid M}} \left(1 - \frac{1}{\ell - 1}\right), \quad S_M = \lim_{y \rightarrow \infty} \frac{V_M(y)}{V(y)} > 0. \quad (28)$$

For $s \leq x^{0.11}$ supported on the marked primes,

$$\sum_{\ell \mid s} \frac{1}{\ell} \leq 0.11L^{0.9}e^{-L^{0.1}} = o(1).$$

Together with (16), this gives $\sum_{\ell \mid r} 1/\ell \leq \tau + o(1) \leq 2\tau$ for every fixed $\tau > 0$ and all sufficiently large x . Hence, uniformly for contributing $r \leq x^{0.11}$ and all y ,

$$V_M(y) \leq \prod_{2 < \ell \leq y} (1 - g_r(\ell)) \leq e^{20\tau} V_M(y). \quad (29)$$

Indeed deleting the factor at a prime dividing r multiplies the product by $(1 - 1/(\ell - 1))^{-1}$, whose logarithm is at most $10/\ell$ for odd ℓ . Set $E_\tau = e^{20\tau}$. This slightly looser fixed factor absorbs the marked-prime contribution. We retain it in the upper bounds and choose τ small enough at the end of the sieve subtraction.

3.5 Subtracting according to the least prime factor

The argument in this section is an inclusion-exclusion calculation in two stages. We first count integers having no small prime factor. We then subtract those whose least prime factor lies below $x^{1/2-\xi}$. Marked replacement makes the second count accessible.

The elementary sieve input. We use the classical block form of Brun's sieve. If the intersections of bad conditions at squarefree ℓ have mass $X'g(\ell) + E(\ell)$, with g multiplicative, $0 \leq g(p) \leq 1 - \eta_0$, and $\sum_{v < p \leq v^2} g(p) \leq C_0$, then an even depth H , sufficiently large in terms of η_0, C_0 , gives

$$S = X' \prod_{p \leq z} (1 - g(p))(1 + O(e^{-H})) + O\left(\sum_{\ell \leq z^{4H+2}} |E(\ell)|\right). \quad (30)$$

Only products of sieving primes occur in the remainder. For $H = 2$, the corresponding upper bound has an implied constant depending only on η_0, C_0 and remainder range $\ell \leq z^{10}$. These two parameters can be fixed absolutely in our applications. We use the bounded-coefficient form recorded in [13, Lemma 11.1]. Its constants are uniform when H grows. We recall the argument, since the absence of divisor weights in its error is useful here.

Partition the sieving primes into blocks $\mathcal{B}_j = \{p : z^{2^{-j-1}} < p \leq z^{2^{-j}}\}$ and put $h_j = (j + 1)H$. For an object of the weighted set, let b_p be the indicator of the bad condition at p , and let I_j indicate that no condition in block j holds. Define U_j by inclusion-exclusion through the even degree h_j , and let T_j be the sum of its unsigned monomials of degree $h_j + 1$. The elementary binomial identity gives

$$0 \leq I_j \leq U_j, \quad U_j - I_j \leq T_j.$$

Consequently

$$\prod_j U_j - \sum_j T_j \prod_{k \neq j} U_k \leq \prod_j I_j \leq \prod_j U_j.$$

Every coefficient of either bounding polynomial has absolute value at most one. Indeed the supports of the correction terms are disjoint: term j has degree exactly $h_j + 1$ in its j th block, whereas every other correction has degree at most h_j there. The indexing prime products are at most z^{4H+2} , because $\sum_{j \geq 0} (j+1)2^{-j} = 4$.

To compute the main term, temporarily make the b_p independent Bernoulli variables with means $g(p)$. Write $a_j = \mathbb{E}I_j$ and $t_j = \mathbb{E}T_j$. The hypotheses give

$$a_j \geq e^{-C_0/\eta_0}, \quad t_j \leq \frac{C_0^{h_j+1}}{(h_j+1)!}, \quad a_j \leq \mathbb{E}U_j \leq a_j + t_j.$$

Thus $\sum_j t_j/a_j \ll e^{-H}$ for sufficiently large even H ; for $H = 2$ this sum is merely bounded, which is enough for the upper bound. Independence between the blocks shows that both bounding polynomials have mean $\prod_p (1 - g(p))(1 + O(e^{-H}))$. Evaluating them in the original weighted set proves (30), since their coefficients are bounded by one. This proves the form of the sieve used below.

Standard Mertens and Buchstab estimates also give

$$\int_b^{1/2} D_t(1-t) \frac{dt}{t} = D_b(1) - 1, \quad D_b(1) \leq \frac{e^{-\gamma_E}}{b} (1 + C_d e^{-c_d/b}) \quad (31)$$

for sufficiently small fixed $b > 0$. The identity has a direct proof. Substitute $u = 1/t$ on its left. The result is

$$\int_2^{1/b} \omega_B(u-1) du = [u\omega_B(u)]_2^{1/b} = D_b(1) - 1,$$

by the defining differential equation and $2\omega_B(2) = 1$. The inequality is the standard rapid convergence of Buchstab's function to $e^{-\gamma_E}$. Thus the large rough-number terms cancel, leaving the one-prime contribution 1.

The initial lower sieve. Assume henceforth $\epsilon < b < 0.01$. Apply (30) at each $r \leq x^\epsilon$, with $z = x^b$, $g = g_r$, and $H = 2\lfloor 1/(40b) \rfloor$. For small b , $z^{4H+2} \leq x^{0.2+2b} < D$, so (26) controls all errors. Use the lower inequality in (29), and absorb (24). There are absolute $C_s, c_s > 0$ such that

$$S_b := \sum_{P^-(d) > x^b} w(d) \geq \frac{S_M X_0}{L} \left\{ \frac{e^{-\gamma_E}}{b} (1 - C_s e^{-c_s/b}) + o(1) \right\}. \quad (32)$$

After enlarging C_s , one may take $c_s = 1/20$, since $H \geq 1/(20b) - 2$. The constant C_s and an upper bound $b_0 > 0$ on the permitted values of b are fixed before ϵ, Y, τ and the marked groups. The vanishing error and the threshold for x may depend on these later choices. This allows us to choose b before the zero-free width enters the argument.

A prime divisor in a prescribed interval. Next fix $b \leq \gamma < \gamma' \leq 1/2 - \xi$. At $r \leq x^\epsilon$, any prime $x^\gamma < n \leq x^{\gamma'}$ is coprime to Mr . Conditioning on $n \mid d$, the local main mass is $A_r/(n-1)$. Sieve the remaining prime factors of d up to W , with $H = 2\lceil (\log L)^2 \rceil$. The remainder moduli are

$$n\ell \leq x^{1/2-\xi} W^{4H+2} = x^{1/2-\xi+o(1)} < D.$$

The map $(n, \ell) \mapsto n\ell$ is injective, since n is its only prime divisor exceeding W . Thus the summed error uses (26) once, without multiplicity weights. From (29) and Mertens' theorem,

$$\sum_{\substack{x^\gamma < n \leq x^{\gamma'} \\ n \text{ prime}}} \sum_{\substack{n|d \\ P^-(d) > W}} w(d) \leq E_\tau S_M X_0 V(W) \{\log(\gamma'/\gamma) + o(1)\}. \quad (33)$$

The tail $r > x^\epsilon$ remains negligible: for $x \geq 2$, each $d < 2x$ has at most $2/b$ distinct prime divisors greater than x^b . Its contribution is therefore at most $2/b$ times (24), which is $o(X_0 V(W))$. Thus the number of conditioning primes introduces no growing multiplicity into the tail estimate.

The subtraction. Put $U_\xi = \sum_{P^-(d) > x^{1/2-\xi}} w(d)$. For a fixed bin $(\gamma, \gamma'] \subseteq (b, 1/2 - \xi]$, any d whose least prime factor lies in that bin is counted by

$$T_{\gamma, \gamma'} = \sum_{\substack{x^\gamma < n \leq x^{\gamma'} \\ n \text{ prime}}} \sum_{P^-(m) > x^\gamma} w(mn).$$

Use the half-open dyadic partition, so that each pair (m, n) belongs to exactly one box. There are $O(L)$ relevant boxes; both factors have scale at least $x^{b/2}$, and the full m -dyads have exponents in $[1/2 + \xi/2, 1 - b/2]$. Proposition 5, with $\beta = b/2$, replaces $R_\gamma(m)$ by $B_\gamma(m)$, at total cost $O(xL^{-5}) = o(X_0/L)$. The boxes depend on x , so it matters that the implied constant and the threshold in Proposition 5 are the same for every box in the window $[s_-, s_+] = [1/2 + \xi/2, 1 - b/2]$ with $\beta = b/2$; see the end of its proof. The total cost is then $O(L) \cdot O(xL^{-6})$.

The disjoint boxes let us combine the replaced main terms before applying (33); the factor $O(L)$ is paid only in the replacement errors. On the product support, $\log m/L = 1 - \log n/L + O(1/L)$. By continuity of D , and then (33),

$$T_{\gamma, \gamma'} \leq \frac{E_\tau S_M X_0}{L} \left\{ \sup_{\gamma \leq t \leq \gamma'} D_\gamma(1-t) \log(\gamma'/\gamma) + o(1) \right\}. \quad (34)$$

Choose a sufficiently fine fixed partition of $[b, 1/2 - \xi]$. The sum of the expressions in braces, without $o(1)$, is at most $D_b(1) - 1 + 1/20$, by (31) and uniform continuity. Subtraction gives

$$\frac{LU_\xi}{S_M X_0} \geq \frac{e^{-\gamma_E}}{b} (1 - C_s e^{-c_s/b}) - E_\tau (D_b(1) - 1 + 1/20) + o(1). \quad (35)$$

Choose b so small that

$$\frac{e^{-\gamma_E}}{b} (C_s e^{-c_s/b} + C_d e^{-c_d/b}) < 1/10, \quad (36)$$

and then $\tau \leq 0.01$ so small that

$$(E_\tau - 1)(D_b(1) + 1) < 1/10. \quad (37)$$

It follows that

$$U_\xi \geq (3/4 + o(1)) S_M X_0 / L. \quad (38)$$

The choices of b and τ involve no zero-free width. The loss from the enlarged cofactor is $O(\tau/b)$, which is made small by choosing τ after b .

3.6 Removing the remaining semiprimes

After the preceding subtraction, every surviving composite has its prime factors near the square root of x . We show that their total contribution tends to zero with ξ . The constant in this estimate must be independent of the number K of marks; this permits ξ to be chosen before K . A composite contributing to U_ξ , for $\xi < 0.01$, has exactly two prime factors counted with multiplicity. Each lies between $x^{1/2-\xi}$ and $2x^{1/2+\xi}$. Their ordered pairs are covered by at most $C_{\text{dyad}}(\xi L + 1)$ dyadic boxes $\mathcal{B} = [M_1, 2M_1) \times [M_2, 2M_2)$, with

$$x/4 \leq M_1 M_2 \leq 2x, \quad [M_i, 2M_i) \subseteq [x^{0.46}, x^{0.54}] \quad (39)$$

for large x .

Lemma 8. *For any such box,*

$$\sum_{\substack{(m,n) \in \mathcal{B} \\ P^-(m) > W, P^-(n) > W}} w(mn) \leq C_1 X_0 V(W)^2, \quad (40)$$

where C_1 depends at most on M, c, Ψ , uniformly for $\tau \leq 0.01$, and is independent of K, Y, ϵ, b, ξ .

Proof. Fix $r \leq x^{0.11}$, and write $k = cr$. A contributing pair satisfies $mn \equiv -1 \pmod{k}$, and $(mn+1)/k = Q > x^{0.9}$ is prime. At each odd prime $j \leq z' = x^{0.002}$, $j \nmid cr$, forbid $mn \equiv -1 \pmod{j}$; if $j \leq W$, also forbid $mn \equiv 0 \pmod{j}$. There are respectively $j-1$ and $2j-1$ such pairs modulo j , and the conditions are disjoint. For a squarefree product ℓ of these primes, put

$$\rho(\ell) = \prod_{j|\ell} (j-1 + (2j-1)\mathbf{1}_{j \leq W}), \quad g(\ell) = \rho(\ell)/\ell^2.$$

Since the sieving primes are coprime to $k = cr$, the Chinese remainder theorem applies. There are $\varphi(k)$ pairs of residues modulo k satisfying $mn \equiv -1 \pmod{k}$. Counting the pairs in each residue class of the box gives main mass $X'g(\ell)$, where $X' = M_1 M_2 \varphi(k)/k^2$, and error

$$|E(\ell)| \ll \varphi(k)\rho(\ell) \left(\frac{M_1 + M_2}{k\ell} + 1 \right) \ll d(\ell)^2 (M_1 + M_2 + r\ell).$$

Here $d(\ell)$ is the divisor function. Since $\sum_{\ell \leq T} d(\ell)^2 \ll T \log^3(2T)$, summing to $(z')^{10} = x^{0.02}$ gives

$$\sum_{\ell \leq x^{0.02}} |E(\ell)| \ll (x^{0.56} + rx^{0.04})L^3 = o((x/r)L^{-10})$$

uniformly for $r \leq x^{0.11}$. The local densities satisfy $g(j) \leq 7/9$, $g(j) \leq 3/j$. For $j \leq W$ the remaining factor is

$$1 - (3j-2)/j^2 = (1 - 1/j)^3 (1 - 1/(j-1)^2);$$

for $W < j \leq z'$ it is

$$1 - (j-1)/j^2 = (1 - 1/j)(1 + 1/(j(j-1))).$$

The correction products are bounded. Omitting primes dividing r costs at most $\exp(C\tau + o(1))$, by the same reciprocal-sum bound as in (29). The $H = 2$ upper sieve therefore bounds the pairs at this r by

$$O((x/r)V(W)^2V(z')).$$

We may discard the progression and bound Ψ by 1 for this upper bound. Multiply by t_r , sum, and use $V(z') \asymp L^{-1}$ and (27). This gives (40), without introducing the pointwise bound B_K . $\square$

In the range (39), $R_{0.4}(m)$ is exactly the prime indicator and $D_{0.4}(s) = 1/s$. Use marked replacement first in the m -variable and then in the n -variable, with $\beta = b/2$, $s_- = 0.46$, $s_+ = 0.54$, interchanging m, n for the second application, to replace both prime indicators by

$$\frac{\mathbf{1}_{P^-(m) > W}}{V(W) \log m}, \quad \frac{\mathbf{1}_{P^-(n) > W}}{V(W) \log n}.$$

The companion coefficients are bounded by 1 for large x , and are W -rough. By (40), the resulting mass in one box is at most $(0.46)^{-2} C_1 X_0 / L^2$. Thus for a constant C_2 depending only on M, c, Ψ ,

$$\sum_{\substack{d \text{ composite} \\ P^-(d) > x^{1/2-\xi}}} w(d) \leq C_2(\xi + L^{-1}) X_0 / L + o(X_0 / L). \quad (41)$$

All replacements together cost $O(xL^{-5})$. Prime squares are included; counting other semiprimes twice is harmless.

3.7 Fixing the sieve parameters and counting candidates

Proof of Proposition 4. The order of choices is important because the candidate constant must be independent of ϵ and Y . We first make all choices that can be made using the fixed progression alone.

1. Fix M, c, u, Ψ , hence S_M , and take the constant C_2 in (41) uniformly for $0 < \tau \leq 0.01$.
2. Choose $0 < \xi < 0.01$ so that $C_2 \xi < S_M / 8$.
3. Choose $0 < b < \min(b_0, 0.01)$ small enough for (36), using the constants fixed before ϵ . Then choose $0 < \tau \leq 0.01$ satisfying (37), and fix the finite partition used in (35).
4. Choose K large enough for the finitely many applications of marked replacement, and fix the band exponents, for example $a_i = 0.1 + 0.1i/(K+1)$.

These choices are independent of ϵ, Y . Indeed, the first set of replacement parameters consists of

$$\beta = b/2, \quad \gamma \in [b, 1/2 - \xi], \quad [s_-, s_+] = [1/2 + \xi/2, 1 - b/2],$$

with only the finitely many selected values of γ . The second set has $\gamma = 0.4$, $[s_-, s_+] = [0.46, 0.54]$, and the same β . Neither set involves ϵ . The selector does involve ϵ, Y , but Proposition 5 is uniform over that selector.

Put $\epsilon_0 = \min(\xi, b)/10$, and now allow any fixed $0 < \epsilon < \epsilon_0$. Choose $Y \geq Y_0$, where the fixed constant Y_0 exceeds $10/\tau$, the prime divisors of M , and 3. In the arithmetic application we may enlarge Y further to absorb any fixed exceptional primes. Equations (38) and (41) give

$$\sum_{d \text{ prime}} w(d) \geq \frac{1}{2} S_M X_0 / L$$

for all sufficiently large x . Remove the negligible contribution with $r > x^\epsilon$, and use $w(d) \leq B_K$. Let $\mathcal{C}(x; \epsilon, Y)$ denote the candidate set in (9). Equations (19) and (27) now show that

$$\#\mathcal{C}(x; \epsilon, Y) \geq A_0 \frac{\epsilon}{\log Y} \frac{x}{L}, \quad (42)$$

where $A_0 > 0$ is independent of ϵ, Y . The threshold for x may depend on ϵ, Y .

Every candidate has

$$p \equiv u \pmod{M}, \quad p+1 = crQ, \quad r \leq x^\epsilon, \quad Q > x^{0.9} \text{ prime}, \quad (43)$$

and every prime divisor of r exceeds Y . The marked primes exceed any fixed Y once x is sufficiently large. The factors ϵ and $1/\log Y$ in (42) have been kept explicit throughout. This uniformity will be needed when the zero-free width is introduced. $\square$

4 Division points and degree-one primes

We return to $E : y^2 = x^3 - 2x$ and $P = (2, 2)$. We have constructed many candidate primes; we must now bound those for which an odd prime q divides the index of $\bar{P}$. Since $E(\mathbb{F}_p)$ is cyclic on our progression, for $q \mid p+1$ this happens precisely when $\bar{P}$ is a q -multiple in $E(\mathbb{F}_p)$. We express this condition through the Galois action on the solutions of $qR = P$.

For an odd prime q , the set

$$q^{-1}P = \{R \in E(\bar{\mathbb{Q}}) : qR = P\}$$

has q^2 elements: in characteristic zero, multiplication by q is a separable isogeny of degree q^2 , and $E[q] \cong (\mathbb{Z}/q\mathbb{Z})^2$; see [17]. It is a torsor under $E[q]$: choosing one point R_q identifies every other point uniquely with $R_q + T$, $T \in E[q]$. There is no preferred origin until R_q is chosen. Consequently the Galois action is affine, with linear part given by its action on $E[q]$.

Put $L_q = \mathbb{Q}(E[q], q^{-1}P)$. This is a Galois extension. There is a fixed constant q_0 such that

$$\text{Gal}(L_q/\mathbb{Q}(E[q])) = E[q] \cong \mathbb{F}_q^2 \quad (q > q_0). \quad (44)$$

Here is the Kummer-theoretic input. The curve has complex multiplication by $\mathbb{Z}[i]$, with all endomorphisms defined over $K = \mathbb{Q}(i)$. The point P is independent over $\mathbb{Z}[i]$, since a nonzero endomorphism is an isogeny and cannot kill a nontorsion point. Ribet's theorem [14, p. 71], applied over K , says that the division torsor has the full translation group for all but finitely many q . The group over $\mathbb{Q}(E[q])$ contains the group after adjoining K , and is contained in $E[q]$, which proves (44). (In fact $K \subseteq \mathbb{Q}(E[q])$ for odd q : an automorphism fixing $E[q]$ pointwise and acting as conjugation on K would satisfy $([i] - \overline{[i]})T = 2[i]T = 0$ for all $T \in E[q]$, impossible for q odd. So the two groups coincide.) All exceptional primes will be placed below Y .

Let ζ_q be a primitive q th root of unity, and define

$$T_q = \mathbb{Q}(R_q, \zeta_q + \zeta_q^{-1}). \quad (45)$$

Adjoining a point means adjoining both coordinates. The field T_q need not be Galois. It is contained in L_q , since the Weil pairing places $\mathbb{Q}(\zeta_q)$ in $\mathbb{Q}(E[q])$.

Lemma 9. *For $q > q_0$, put $n_q = [T_q : \mathbb{Q}]$. Then*

$$n_q = \frac{q^2(q-1)}{2}, \quad \log |D_{T_q}| \ll n_q \log q.$$

If $p \equiv 3 \pmod{8}$, $p \neq q$, and $q \mid i_p$, then T_q has exactly $q(q-1)/2$ degree-one prime ideals above p .

Proof. Write $V = E[q]$ and let $H_q \subseteq \text{GL}_2(\mathbb{F}_q)$ be the linear Galois image. Full translations imply that the affine image is the whole preimage $V \rtimes H_q$: over every element of H_q , all translations occur.

The determinant map $H_q \rightarrow \mathbb{F}_q^\times$ is surjective, because it is the cyclotomic character by the Weil pairing.

The embeddings of $\mathbb{Q}(\zeta_q + \zeta_q^{-1})$ are indexed by $\mathbb{F}_q^\times / \{\pm 1\}$, and Galois acts on them through the determinant. The affine group acts transitively on

$$q^{-1}P \times (\mathbb{F}_q^\times / \{\pm 1\}). \quad (46)$$

Indeed, first choose a linear element with the desired determinant coset, then use a translation to prescribe the division point. The stabilizer of the chosen pair fixes exactly T_q . The orbit therefore identifies its embeddings with (46), and gives the asserted degree.

For the discriminant bound, we use the Galois extension L_q . It is unramified away from $2q$. At a good prime different from q , multiplication by q on the elliptic scheme is finite etale, as is its fibre above the section P . Properness extends P to a section at every good prime, even when its affine coordinates are not integral. Moreover

$$[L_q : \mathbb{Q}] \leq q^2 |\mathrm{GL}_2(\mathbb{F}_q)| < q^6.$$

The local different bound [16, Section 1.2] for a Galois extension of degree d , ramified only at primes in S , gives

$$\frac{\log |D_L|}{d} \leq \sum_{\ell \in S} (1 + v_\ell(d)) \log \ell.$$

Apply this with $S = \{2, q\}$ and $d < q^6$. The right side is $O(\log q)$. The discriminant formula in a tower gives $|D_{T_q}|^{1/n_q} \leq |D_{L_q}|^{1/[L_q:\mathbb{Q}]}$, proving the bound.

At such a good prime $p \neq q$, the same finite etale argument identifies both the geometric q -torsion and the geometric fibre $q^{-1}P$ with the corresponding fibres after reduction. Indeed, over the strict henselization each finite etale fibre is a disjoint union of sections, so reduction gives bijections compatible with the Galois action. Under these identifications, arithmetic Frobenius acts as the p -power Frobenius on the reduced points; see [17].

Now let $q \mid i_p$. Since $i_p \mid p+1$, we have $p \equiv -1 \pmod{q}$. The characteristic polynomial of Frobenius acting on $E[q]$ is

$$t^2 - a_p t + p = t^2 + p \equiv t^2 - 1 \pmod{q}.$$

As q is odd, its eigenspaces for 1 and -1 each have dimension one. In a cyclic group whose order is divisible by q , an element has index divisible by q if and only if it is a q -multiple. Thus $\bar{P} \in qE(\mathbb{F}_p)$. There are exactly q solutions of $qR = \bar{P}$ in $E(\mathbb{F}_p)$, since the kernel of multiplication by q on this cyclic group has order q .

Affine Frobenius therefore fixes exactly q points of the first factor of (46). Its determinant is -1 , so it fixes every one of the $(q-1)/2$ elements of the second factor. It fixes precisely $q(q-1)/2$ embeddings of T_q . At an unramified prime, the orbits of Frobenius on embeddings have lengths equal to the residue degrees of the primes above p . In particular, its fixed embeddings count the degree-one primes. This proves the assertion. $\square$

The last interpretation is the bridge from an elliptic divisibility condition to a Dedekind zeta function. We need an upper bound only. Every bad rational prime supplies many prime ideals of norm p ; positivity allows us to bound their contribution by the sum over all prime ideals of T_q .

5 A positive explicit formula and the small index divisors

We now use the zero-free half-plane for the first time. The bound below is uniform both in the number field and in the width of the half-plane. These two uniformities allow us to sum over q while keeping the final constant independent of N .

For a number field T , let $\Lambda_T(\mathfrak{a})$ be its von Mangoldt function on nonzero integral ideals: it equals $\log N \mathfrak{p}$ if $\mathfrak{a} = \mathfrak{p}^k$ for a prime ideal $\mathfrak{p}$ and an integer $k \geq 1$, and is zero otherwise. We use a smooth nonnegative weight so that discarding unwanted prime ideals can only decrease the sum.

Lemma 10 (Smoothed prime-ideal bound). *Let T be a number field of degree n and discriminant D_T . Suppose that all its nontrivial zeta zeros satisfy $\Re \rho \leq 1 - \delta$, where $0 < \delta \leq 1/2$. Fix a nonnegative smooth function f supported in $(1/2, 3)$ and at least one on $[1, 2]$. For $x \geq 2$,*

$$\sum_{\mathfrak{a}} \Lambda_T(\mathfrak{a}) f(N \mathfrak{a}/x) \ll_f x + x^{1-\delta} (\log |D_T| + n). \quad (47)$$

The implied constant is independent of T and δ .

Proof. Let $\widehat{f}(s) = \int_0^\infty f(t) t^{s-1} dt$ be the Mellin transform. On the line $\Re s = 2$, the logarithmic derivative of the Dedekind zeta function is absolutely convergent, and Mellin inversion gives

$$\sum_{\mathfrak{a}} \Lambda_T(\mathfrak{a}) f(N \mathfrak{a}/x) = \frac{1}{2\pi i} \int_{(2)} -\frac{\zeta'_T(s)}{\zeta_T(s)} \widehat{f}(s) x^s ds.$$

Write (r_1, r_2) for the signature of T . Moving the line to $\Re s = -1/2$ gives the more precise smoothed explicit formula

$$x \widehat{f}(1) - \sum_{\rho} x^{\rho} \widehat{f}(\rho) - (r_1 + r_2 - 1) \widehat{f}(0) + O_f \left(x^{-1/2} (\log |D_T| + n) \right), \quad (48)$$

where the sum is over nontrivial zeros, with multiplicity. The pole at one gives the first term; the zero at zero has order $r_1 + r_2 - 1$ and gives the displayed residue. On the new line, the functional equation expresses the logarithmic derivative in terms of its absolutely convergent Dirichlet series at $1 - s$, the discriminant, and gamma factors. Consequently

$$\left| \frac{\zeta'_T}{\zeta_T}(-1/2 + it) \right| \ll \log |D_T| + n \log(|t| + 3),$$

with an absolute constant. This proves the uniform bound for the remaining integral. The standard zero count permits horizontal contours avoiding the zeros, and the rapid decay of $\widehat{f}$ makes their integrals tend to zero; see also [13, Lemma 9.2]. Smoothness and compact support give, uniformly for $0 \leq \sigma \leq 1$,

$$|\widehat{f}(\sigma + it)| \ll_{f,A} (1 + |t|)^{-A}$$

for every fixed A . The standard zero count in intervals of unit length is $O(\log |D_T| + n \log(|t| + 3))$. Summing over these intervals, with $A = 3$, yields

$$\sum_{\rho} |\widehat{f}(\rho)| \ll_f \log |D_T| + n.$$

The zero-free hypothesis bounds $|x^{\rho}|$ by $x^{1-\delta}$. The residue at zero is $O_f(n)$, and the remaining integral is $O_f(x^{-1/2}(\log |D_T| + n))$. Both are absorbed by the right side of (47), uniformly for $0 < \delta \leq 1/2$. This proves the lemma. $\square$

For a prime q , let

$$B_q(x) = \#\{x < p < 2x : p \equiv 3 \pmod{8}, q \mid i_p\}.$$

If $q \leq x^\epsilon$ with $\epsilon < 1$, then $q < p$ in this definition. Lemma 9 shows that each such p contributes at least $q(q-1)\log x/2$ to the nonnegative sum in (47) for T_q . Under (2) we obtain

$$B_q(x) \ll \frac{x}{q(q-1)\log x} + \frac{q \log q}{\log x} x^{1-1/N} \quad (q > q_0). \quad (49)$$

The factor q in the error is the quotient of the field degree, which is of order q^3 , by the number of fixed embeddings, which is of order q^2 .

Proposition 11. *Assume (2). For fixed $Y \geq \max(q_0, 3)$ and $0 < \epsilon < 1$, once x is sufficiently large,*

$$\sum_{Y < q \leq x^\epsilon} B_q(x) \ll \frac{x}{Y \log Y \log x} + \frac{x^{1-1/N+2\epsilon}}{\log x}. \quad (50)$$

The implied constant is independent of N, ϵ, Y .

Proof. The elementary prime-counting bound $\pi(t) \ll t/\log t$, followed by partial summation, gives

$$\sum_{q > Y} \frac{1}{q(q-1)} \ll \frac{1}{Y \log Y}, \quad \sum_{q \leq z} q \log q \ll z^2.$$

Sum (49) and take $z = x^\epsilon$. □

Notice that this proposition counts all bad primes in the progression, not just the candidates from the cofactor sieve. It therefore requires no independence between the factorization restrictions and the division fields. Some primes may be counted more than once; this is harmless for the upper bound used in the subtraction.

6 The large prime and completion of the proof

It remains to treat the distinguished prime Q . Unlike the prime divisors of the cofactor, Q is too large for our summed explicit-formula estimate. Its size, however, gives a stronger elementary consequence. If it divides the index, the order of the point is small.

Lemma 12. *Let $E/\mathbb{Q}$ be a fixed elliptic curve and $P \in E(\mathbb{Q})$ a fixed point of infinite order. For $T \geq 1$ and $x \geq 2$,*

$$\#\{x < p < 2x : p \text{ of good reduction, } \text{ord}(\overline{P}) \leq T\} \ll_{E,P} \frac{T^3}{\log x}.$$

Proof. Choose a global minimal integral Weierstrass equation and write $x(nP) = A_n/B_n^2$ in lowest terms, with $B_n > 0$. The comparison of the usual height with the canonical height, together with $\widehat{h}(nP) = n^2 \widehat{h}(P)$, gives $\log B_n \ll_{E,P} n^2$; see [17]. At a good prime, reduction of nP is the identity precisely when nP lies in the kernel of reduction, which in this equation implies $p \mid B_n$. Thus every prime in the displayed set divides at least one of $B_1, \dots, B_{\lfloor T \rfloor}$. The product of these positive integers has logarithm

$$\sum_{n \leq T} \log B_n \ll_{E,P} \sum_{n \leq T} n^2 \ll_{E,P} T^3.$$

Each distinct prime being counted exceeds x and hence contributes at least $\log x$ to this logarithm. Division by $\log x$ proves the bound. □

Proof of Theorem 1. Let $G(X)$ count the primes in (3). Apply Proposition 4 with $M = 8$, $u = 3$, and $c = 4$. We obtain at least

$$A_0 \frac{\epsilon}{\log Y} \frac{x}{\log x}$$

candidates in $(x, 2x)$, each with $p + 1 = 4rQ$, $r \leq x^\epsilon$, and no prime factor of r at most Y . Lemma 3 says that their indices are odd. If $i_p > 1$, a prime divisor of i_p must therefore either divide r or equal Q . The first possibility is covered by Proposition 11. In the second case

$$\text{ord}(\overline{P}) = \frac{p+1}{i_p} \leq \frac{p+1}{Q} = 4r \leq 4x^\epsilon,$$

so Lemma 12 bounds its contribution by $O(x^{3\epsilon}/\log x)$. Consequently, for fixed constants $A_0, C > 0$,

$$G(2x) - G(x) \geq \frac{A_0\epsilon - C/Y}{\log Y} \frac{x}{\log x} - O\left(\frac{x^{1-1/N+2\epsilon} + x^{3\epsilon}}{\log x}\right). \quad (51)$$

The constants here do not depend on N, ϵ, Y .

Fix $0 < \theta < \min(\epsilon_0, 1/4)$ and set $\epsilon = \theta/N$. Choose a fixed $L_0 > 0$ large enough that $L_0 \geq 2C/A_0$ and $L_0/\epsilon \geq \max(Y_0, q_0, 3)$ for all $N \geq 2$, and put $Y = \lceil L_0/\epsilon \rceil$. Then

$$C/Y \leq A_0\epsilon/2, \quad 1 - 1/N + 2\epsilon < 1, \quad 3\epsilon < 1.$$

For every fixed N , the errors in (51) are $o(x/\log x)$. Also $Y \asymp N$ and $\log Y \ll \log N$ uniformly for $N \geq 2$, where the comparison constants depend only on the fixed choices. We conclude that

$$G(2x) - G(x) \gg \frac{1}{N \log N} \frac{x}{\log x}.$$

Apply this to $(X/2, X)$ and decrease the constant to obtain (3). The prime number theorem then gives the positive lower density among all primes. $\square$

Only the threshold for X is allowed to depend on N . All the sieve parameters determining A_0 were fixed before ϵ and Y . This is why the explicit dependence $1/(N \log N)$ survives the proof.

7 Other curves and points

The proof used three properties of a progression: the group order was $p + 1$, the reduced group was cyclic, and the index of the chosen point was odd. We now prove Theorem 2 by arranging these properties with congruences. We retain the model, notation, and squareclass condition from the introduction.

We first construct the progression. For a nonzero rational number a and a prime not dividing its numerator or denominator, (a/p) has its usual meaning as a quadratic residue symbol.

Lemma 13. *Suppose (5) holds. There are positive integers M, c and an integer b , depending only on E, P , with*

$$c \in \{2, 4, 8\}, \quad 2c \mid M, \quad (b, M) = 1, \quad \left(\frac{b+1}{c}, \frac{M}{c}\right) = 1,$$

such that every sufficiently large prime $p \equiv b \pmod{M}$ satisfies

$$\left(\frac{d}{p}\right) = \left(\frac{D}{p}\right) = \left(\frac{u}{p}\right) = -1, \quad p \equiv 1 \pmod{3}, \quad v_2(p+1) = v_2(c). \quad (52)$$

All prime divisors of any prescribed fixed positive integer may be included among the prime divisors of M .

Proof. Condition (5) says exactly that there is a linear functional on the span of $[d], [D], [u], [-3]$ taking the values 1, 1, 1, 0, respectively. Equivalently, the multiquadratic field

$$F = \mathbb{Q}(\sqrt{d}, \sqrt{D}, \sqrt{u}, \sqrt{-3})$$

has an automorphism acting by the signs $-1, -1, -1, +1$ on these four square roots. The field F is contained in a cyclotomic field $\mathbb{Q}(\zeta_{M_0})$, where M_0 can be chosen to divide 8 times an odd squarefree integer. Restriction from this cyclotomic Galois group to $\text{Gal}(F/\mathbb{Q})$ is surjective. It follows that some reduced residue class $b_0 \pmod{M_0}$ realizes the desired signs. We include 8 and 3 in M_0 if necessary. Since $(-3/p) = 1$ is equivalent to $p \equiv 1 \pmod{3}$ for primes $p > 3$, we have $b_0 \equiv 1 \pmod{3}$.

There is one further requirement. No odd prime dividing the progression modulus should be forced to divide $p + 1$. Let $\ell \geq 5$ be an odd prime dividing M_0 . If $b_0 \equiv -1 \pmod{\ell}$, replace its residue modulo ℓ by a different nonzero residue having the same Legendre symbol modulo ℓ . This is possible because each of the two symbol classes contains $(\ell - 1)/2 \geq 2$ residues. The change preserves every quadratic character of conductor dividing M_0 . Make these choices independently at all such ℓ . At 3, the residue 1 already avoids -1 . Additional fixed odd primes may be inserted into the modulus, choosing any nonzero residue other than -1 at each new prime.

Keep the chosen residue modulo 8. If it is 1 or 5, then $v_2(p + 1) = 1$; if it is 3, then $v_2(p + 1) = 2$. If it is 7, choose its lift modulo 16 to be 7, giving $v_2(p + 1) = 3$. In the first three cases either compatible lift to modulus 16 preserves the valuation. The Chinese remainder theorem now gives a class b modulo M , where M is 16 times the product of the chosen odd primes. Set $c = 2^{v_2(b+1)}$. The construction gives $(b, M) = 1$, $2c \mid M$, and $((b + 1)/c, M/c) = 1$, as required. $\square$

Lemma 14. *For every sufficiently large prime in the progression of Lemma 13, the group $E(\mathbb{F}_p)$ is cyclic of order $p + 1$, and the index*

$$i_p = [E(\mathbb{F}_p) : \langle \bar{P} \rangle]$$

is odd.

Proof. We omit the finitely many bad primes, primes ramified in K , and primes dividing the numerators or denominators in our model and point. Since $(d/p) = -1$, the prime p is inert in the CM field. The CM supersingularity theorem, and the fact that a supersingular elliptic curve over $\mathbb{F}_p$ has trace zero for $p > 3$, give $\#E(\mathbb{F}_p) = p + 1$.

Write $E(\mathbb{F}_p) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, where $d_1 \mid d_2$. The Weil pairing gives $d_1 \mid p - 1$, so $d_1 \mid \gcd(p - 1, p + 1) = 2$. The two nonzero 2-torsion points other than $(0, 0)$ have x -coordinates satisfying $x^2 + Ax + B = 0$. Because $(D/p) = -1$, neither is rational over $\mathbb{F}_p$. Thus the group has exactly one nonzero rational point of order two, which excludes $d_1 = 2$. Consequently the group is cyclic.

Finally, the duplication formula for (4) is

$$x(2R) = \left(\frac{x(R)^2 - B}{2y(R)} \right)^2 \quad (y(R) \neq 0).$$

If $2R = \bar{P}$, then R is neither the identity nor a point of order two, so the displayed formula applies. Its right side is a square, whereas $x(\bar{P}) = u$ is a nonsquare. Hence $\bar{P} \notin 2E(\mathbb{F}_p)$. In a cyclic group of even order, this is equivalent to i_p being odd. $\square$

Proof of Theorem 2. Fix b, M, c as in Lemma 13. The prime-successor sieve applies to this progression with the same proof as before: its required local condition is precisely $((b + 1)/c, M/c) = 1$.

Thus there are constants $A_{E,P} > 0$, $\epsilon_0 > 0$, and Y_0 , depending only on the fixed pair, for which

$$\# \left\{ p \in (x, 2x) \mid \begin{array}{l} p \text{ prime, } p \equiv b \pmod{M}, \\ p+1 = crQ, \quad r \leq x^\epsilon, \quad Q \text{ prime,} \\ q \mid r \implies q > Y \quad (q \text{ prime}) \end{array} \right\} \geq A_{E,P} \frac{\epsilon}{\log Y} \frac{x}{\log x} \quad (53)$$

for every fixed $0 < \epsilon < \epsilon_0$ and $Y \geq Y_0$, once x is sufficiently large. The constant is uniform in these two parameters; the threshold for x need not be. In particular, we take Y_0 larger than every odd prime divisor of M .

We record explicitly why the division-field estimate also carries over. All endomorphisms of the CM curve are defined over K . A nonzero endomorphism cannot kill P , since it is an isogeny and P is nontorsion. The CM Kummer theorem of Ribet [14], applied over K , therefore gives

$$\text{Gal}(\mathbb{Q}(E[q], q^{-1}P)/\mathbb{Q}(E[q])) = E[q]$$

for all sufficiently large primes q . The finitely many exceptional primes, including those dividing the conductor of the CM order, can be included in the lower cutoff Y_0 .

Choose R_q with $qR_q = P$ and put $T_q = \mathbb{Q}(R_q, \zeta_q + \zeta_q^{-1})$. Exactly as in the division-field argument above, full translations on the division torsor and surjectivity of the determinant give

$$[T_q : \mathbb{Q}] = q^2(q-1)/2, \quad \log |D_{T_q}| \ll_{E,P} [T_q : \mathbb{Q}] \log q.$$

For the discriminant bound, the normal closure is ramified only at q and a fixed finite set of primes. Its degree is at most q^6 ; the local different bound and the discriminant formula in a tower then give the asserted root-discriminant estimate.

If p lies in our progression and $q \mid i_p$, then $q \mid p+1$, so $p \equiv -1 \pmod{q}$. Frobenius on $E[q]$ has characteristic polynomial $t^2 + p \equiv t^2 - 1 \pmod{q}$. Since the reduced group is cyclic, $q \mid i_p$ is equivalent to $\overline{P} \in qE(\mathbb{F}_p)$. The division torsor thus has exactly q Frobenius-fixed points. Frobenius also fixes all $(q-1)/2$ embeddings of the real cyclotomic field. Hence T_q has $q(q-1)/2$ degree-one primes above p . The positive smoothed Dedekind explicit formula now gives

$$\sum_{Y < q \leq x^\epsilon} \#\{x < p < 2x : p \equiv b \pmod{M}, q \mid i_p\} \ll_{E,P} \frac{x}{Y \log Y \log x} + \frac{x^{1-1/N+2\epsilon}}{\log x}. \quad (54)$$

The implied constant is independent of N, ϵ, Y .

By Lemma 14, the index of every candidate is odd. If it is larger than one, a prime divisor either divides r , in which case it is counted by (54), or is Q . In the latter case $\text{ord}(\overline{P}) \leq cr \leq cx^\epsilon$. The denominator-height argument already proved gives at most $O_{E,P}(x^{3\epsilon}/\log x)$ such primes. Combining this with (53) and (54) yields

$$\#\{x < p < 2x : \langle \overline{P} \rangle = E(\mathbb{F}_p)\} \geq \frac{A_{E,P}\epsilon - C_{E,P}/Y}{\log Y} \frac{x}{\log x} - O_{E,P}\left(\frac{x^{1-1/N+2\epsilon} + x^{3\epsilon}}{\log x}\right).$$

Choose a fixed sufficiently small $\theta > 0$, put $\epsilon = \theta/N$, and then set $Y = \lceil L_0/\epsilon \rceil$, where the fixed constant L_0 is sufficiently large in terms of the pair. The main coefficient is at least $A_{E,P}\epsilon/(2 \log Y)$, while $2\epsilon < 1/N$ and $3\epsilon < 1$. Since $\log Y \ll_{E,P} \log N$ for $N \geq 2$, this proves the result. $\square$

A family of examples with j -invariant 1728

When $E : y^2 = x^3 + Bx$ and $P = (u, v)$, the CM field is $\mathbb{Q}(i)$ and $D = -4B$. In this case condition (5) has a particularly short form:

$$\text{none of } D, u, -Du \text{ belongs to } \mathbb{Q}^{\times 2} \cup (-3)\mathbb{Q}^{\times 2}. \quad (55)$$

Indeed, a forbidden relation in (5) uses an odd number of $[-1], [D], [u]$. The possible products are $-1, D, u, -Du$, and -1 is neither a rational square nor -3 times one. This proves the equivalence of the two conditions.

For example, for every integer $k \geq 1$ consider

$$E_k : y^2 = x^3 + (18k^2 - 4)x, \quad P_k = (2, 6k). \quad (56)$$

The displayed point lies on the displayed curve, and the curve is nonsingular. Duplication gives

$$x(2P_k) = \frac{(9k^2 - 4)^2}{36k^2}.$$

The numerator is prime to 3 and the denominator is divisible by 9, so this coordinate is not integral. If P_k were torsion, then $2P_k$ would be a finite rational torsion point on the integral equation (56), contradicting Lutz–Nagell. Thus P_k has infinite order.

Here $D = -4(18k^2 - 4) < 0$, so D is not a rational square. Also $v_3(D) = 0$, so D is not -3 times a rational square. The number $u = 2$ is neither a square nor -3 times one. Finally,

$$-Du = 16(9k^2 - 2), \quad (3k - 1)^2 < 9k^2 - 2 < (3k)^2.$$

Thus $-Du$ is positive and not a rational square, and consequently is not -3 times a rational square either. Condition (55) holds, and Theorem 2 applies to every pair in (56).

The examples in Table 1

We now check the six pairs listed in the introduction. In each case, substitution shows that the displayed point lies on the curve. For the first two rows, the curve has j -invariant 1728 and CM field $\mathbb{Q}(i)$. In the order that they appear in the table, the squareclasses of $(D, u, -Du)$ are represented by

$$(6, 3, -2), \quad (-14, 2, 7).$$

None of these entries is a rational square or -3 times a rational square. Thus (55) holds for both pairs. The duplication formula gives, in the same order,

$$x(2P) = \frac{25}{4}, \quad \frac{25}{36}.$$

These coordinates are not integral, so Lutz–Nagell proves that both points have infinite order.

The remaining four rows illustrate that the criterion also applies to other CM fields. The classical CM j -invariants of discriminants -8 and -7 are 8000 and -3375 , respectively. For

$$E : y^2 = x^3 + 4x^2 + 2x, \quad P = (-2, 2),$$

we have $A = 4$, $B = 2$, $D = 8$, and $j(E) = 8000$. Thus $d = -2$, and the four squareclasses in (5) are

$$[-2], \quad [2], \quad [-2], \quad [-3].$$

The classes $[-2], [2], [-3]$ are independent, and the only repetition is between the first and third entries. Every square relation therefore has $e_1 = e_3$ and $e_2 = e_4 = 0$, as required. The primes 5 and 7 are primes of good reduction, and direct counting gives

$$\#E(\mathbb{F}_5) = 6, \quad \#E(\mathbb{F}_7) = 8.$$

The rational torsion subgroup injects into both groups, so its order divides 2. Since P has nonzero y -coordinate, it is not a point of order two and hence has infinite order.

For the fourth example, let

$$E : y^2 = x^3 - 30x + 56, \quad P = (2, 2).$$

The change of variable $t = x - 4$ gives

$$y^2 = t(t^2 + 12t + 18), \quad P = (-2, 2)$$

in the coordinates (t, y) . This is the quadratic twist by 3 of the third curve in the table, so it also has j -invariant 8000 and CM field $\mathbb{Q}(\sqrt{-2})$. Here $A = 12$, $B = 18$, $D = 72$, and $u = -2$, so the four relevant squareclasses are

$$[-2], \quad [2], \quad [-2], \quad [-3].$$

Since $[-2], [2], [-3]$ are independent, every square relation has $e_1 = e_3$ and $e_2 = e_4 = 0$, which proves (5). At the good primes 5 and 7 the reduced groups have orders 6 and 8. The rational torsion subgroup therefore has order dividing 2, and the nonzero y -coordinate of P proves that it has infinite order. This curve is not $\mathbb{Q}$ -isogenous to the third curve: at the common good prime 17, their reductions have 12 and 24 points, respectively.

Next, consider

$$E : y^2 = x^3 - 35x + 98, \quad P = (1, 8).$$

This curve has $j(E) = -3375$, so its CM field is $\mathbb{Q}(\sqrt{-7})$. The change of variable $t = x + 7$ gives

$$y^2 = t(t^2 - 21t + 112), \quad P = (8, 8)$$

in the coordinates (t, y) . Hence $D = -7$ and the four relevant squareclasses are

$$[-7], \quad [-7], \quad [2], \quad [-3].$$

Here $[-7], [2], [-3]$ are independent, so every square relation has $e_1 = e_2$ and $e_3 = e_4 = 0$. This again proves (5). At the good primes 3 and 5 one finds

$$\#E(\mathbb{F}_3) = 4, \quad \#E(\mathbb{F}_5) = 6.$$

The same torsion argument proves that P has infinite order.

The final example, $E : y^2 = x^3 + 42x^2 - 7x$ with $P = (-7, 42)$, has j -invariant 16581375, the classical CM value of the order of discriminant -28 . Its CM field is therefore $\mathbb{Q}(\sqrt{-7})$. The squareclasses of $(d, D, u, -3)$ are $(-7, 7, -7, -3)$. Since $[-7], [7], [-3]$ are independent, every square relation has $e_1 = e_3$ and $e_2 = e_4 = 0$, proving (5). The good reductions at 3 and 5 have orders 4 and 6, so rational torsion has order dividing 2. Since P has nonzero y -coordinate, it has infinite order. This completes the verification of all six examples.

Further points on the original curve

The original curve also supplies many points without another squareclass calculation. Write $P_0 = (2, 2)$ and $T = (0, 0)$ on $E_0 : y^2 = x^3 - 2x$. The same argument applies to

$$P = mP_0 + eT, \quad m \text{ any nonzero odd integer}, \quad e \in \{0, 1\}.$$

To see this, enlarge the fixed cutoff Y_0 to exceed every prime divisor of m . In the candidate family $p + 1 = 4rQ$, no prime divisor of m then divides $p + 1$, for all sufficiently large p . Whenever

$\overline{P}_0$ generates the reduced group, write its order as $n = p + 1$. The unique point of order two is $\overline{T} = (n/2)\overline{P}_0$, so $\overline{P} = (m + en/2)\overline{P}_0$. Every odd prime dividing n divides $n/2$ and does not divide m ; moreover $4 \mid n$, so $m + en/2$ is odd. Thus $(m + en/2, n) = 1$, and $\overline{P}$ also generates the group. The argument giving the candidate lower bound is uniform in the enlarged fixed cutoff, and again gives a constant depending on P but not on N .

Comparison with the results of Gupta and Murty

Theorem 2 gives sufficient hypotheses, and it is useful to explain precisely why they do not encompass all the earlier Gupta–Murty cases. There are three separate issues: the curves covered by the stated criterion, the points that can be primitive at inert primes, and generation by a subgroup rather than a single point.

First, our criterion uses a rational point of order two to express the needed conditions by quadratic characters. This is a genuine restriction on the stated theorem. For example, in each of the maximal-order CM fields in (6), the prime 2 is inert and the Galois image over K on $E[2]$ has order three, permuting the three nonzero points transitively. Indeed, the CM ray-class description gives this group as $(\mathcal{O}_K/2\mathcal{O}_K)^\times$: the class number is one and the units $\{\pm 1\}$ reduce trivially modulo two. Since $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_4$, the group has order three. Thus those curves have no rational 2-torsion and are outside our criterion. Their reductions at inert primes can nevertheless be cyclic. What is then missing is a way to impose the condition $\overline{P} \notin 2E(\mathbb{F}_p)$ inside the cofactor sieve.

This finite condition need not be expressible by congruences on p . To see the issue concretely, suppose that the action on the four points of $2^{-1}P$ is the full affine group $\text{AGL}_2(\mathbb{F}_2) \cong S_4$, with its usual linear quotient $\text{GL}_2(\mathbb{F}_2) \cong S_3$. At the inert primes under discussion, linear Frobenius is a transposition. On the division torsor its affine lift can be a transposition, fixing two points, or a 4-cycle, fixing none. The first possibility makes $\overline{P}$ a double; the second does not. These two conjugacy classes have the same image in $S_4^{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z}$. Since intersection with a cyclotomic field sees only an abelian quotient, an arithmetic progression cannot separate these two classes. This example explains the additional input that would be needed: marked estimates retaining a fixed nonabelian Frobenius condition. Such estimates are not proved here. For CM by $\mathbb{Q}(\sqrt{-3})$, there is also a forced factor $3 \mid p + 1$ at inert primes, whose index obstruction would have to be treated directly.

Second, even such an extension could not cover every point in the Gupta–Murty positivity theorem. Let $Q \in E(\mathbb{Q})$ have infinite order and put $P = 2Q$. At an inert odd good prime, $\#E(\mathbb{F}_p) = p + 1$ is even. For any finite abelian group G of even order, multiplication by two has a nontrivial kernel, and hence $2G$ is a proper subgroup of G . It follows that

$$\langle \overline{P} \rangle \subseteq 2E(\mathbb{F}_p) \neq E(\mathbb{F}_p).$$

The earlier split-prime positivity theorem allows these doubled points. Thus restricting the target to positive lower density does not remove the need to treat split primes if all their pairs are to be covered.

At a split good prime, let $\pi_p \in K$ be the CM Frobenius endomorphism, with $\pi_p \overline{\pi}_p = p$. Then

$$\#E(\mathbb{F}_p) = (1 - \pi_p)(1 - \overline{\pi}_p) = N_{K/\mathbb{Q}}(\pi_p - 1) = p + 1 - a_p. \quad (57)$$

The expression is no longer a fixed linear shift of the rational prime. To extend the cofactor method to these primes, one would need a corresponding factorization estimate for (57), together with the compatible division-field conditions. A zero-free half-plane alone does not provide that estimate, and the marked replacement principle used in Section 3 is an estimate for shifted products of rational

integers. We therefore make no assertion that it applies to (57). The same varying group-order issue arises for the non-CM curves in the higher-rank results of Gupta and Murty.

Finally, there is a useful conclusion for subgroups that follows already from their work. Theorem 4 of [5] gives the split-prime asymptotic for a curve with CM by the full ring of integers of its CM field and a free subgroup $\Gamma \subset E(\mathbb{Q})$ of $\mathbb{Z}$ -rank r , assuming a zero-free half-plane $\Re s > r/(r+1)$ for the relevant Dedekind zeta functions. Our hypothesis (2) supplies this whenever $r+1 \geq N$, because

$$1 - \frac{1}{N} \leq \frac{r}{r+1}.$$

In particular, the announced value $N = 32$ permits $r \geq 31$ in that earlier theorem. Its leading constant may vanish; when it is positive, the asymptotic gives a positive proportion. The conclusion concerns generation by the whole subgroup Γ , and does not imply that one prescribed point generates.

There is also an immediate subgroup consequence of our own theorem: if Γ contains a point satisfying Theorem 2, then its reduction is all of $E(\mathbb{F}_p)$ at the same positive proportion of primes. Rank alone does not ensure this hypothesis. Indeed, a subgroup contained in $2E(\mathbb{Q})$, however large its rank, cannot generate at an inert odd prime by the same argument as above.

8 Further questions

The proof isolates a fairly small part of the factorization distribution of $p+1$. It uses a family with one large prime factor and a small cofactor, rather than a full Poisson–Dirichlet law in arithmetic progressions. It also counts bad index divisors on a larger set than the candidates. These choices suffice for positive lower density, but they lose information needed to identify the exact primitive-point density. To obtain that density one would have to control the contribution from the remaining factorization patterns and the intersections of the division-field conditions with substantially greater precision.

Complex multiplication enters at two specific points. It supplies progressions of primes on which $a_p = 0$, hence $\#E(\mathbb{F}_p) = p+1$, and it supplies the Kummer theorem used for the division torsor. For a non-CM curve, the order is $p+1-a_p$ and varies with the Frobenius trace. The prime-successor sieve proved here does not furnish a corresponding factorization statement for these varying orders. This is the main reason the present argument does not automatically extend to arbitrary elliptic curves.

Finally, the fixed-trace question raised by Katz [9, Conjecture 1.6] is of a different nature. For an elliptic curve it asks, in particular, about infinitely many primes with $a_p = 2$. Our primes instead have $a_p = 0$. The identity element in a finite torsion Galois image has trace 2, which explains why finite congruence tests do not themselves exclude trace 2; obtaining equality as an integer is a further problem. Nothing in the present positive-density argument establishes that fixed-trace infinitude.

Formal verification. The accompanying Lean development verifies the signed analytic argument and the deduction of the quantitative lower bound for the main curve $y^2 = x^3 - 2x$, assuming only the analytic and arithmetic results described below. In particular, the passage from $mn-1$ to $mn+1$, uniformity over the growing family of dyads, the candidate-prime estimate, the cofactor tails and full-mass comparison, the Buchstab subtraction, the semiprime bound, and the final parameter choice are proved within the development. It also proves the infinite order of $(2, 2)$, the relevant reduction and odd-index properties of the main curve, and the denominator-height argument.

Conditional on the arithmetic inputs described below, the formal theorem gives $c/(N \log N)$, with $c > 0$ chosen before N .

The analytic results on which these arguments depend are stated as assumptions in Lean; their proofs have not been formalized here. These include the root-residue estimate of [11, Lemma 3.3], the character-transform estimates from the proof of [13, Proposition 10.3], the finite block sieve of [13, Lemma 11.1], the classical fixed-order derivative test [15, Theorem 3], and the classical estimates listed in the development for prime distribution, sieve products, and the smoothed Dedekind explicit formula. The zero-free hypothesis supplied by the announced theorem of Cureton and Thorner [3, 4] is likewise assumed.

The formal proof also assumes four classical arithmetic ingredients: the existence of division points and the usual structure of the geometric q -torsion; Ribet’s theorem giving the full Kummer Galois action for all sufficiently large primes q ; the local different bound used to estimate the discriminants of the division fields; and the unramified specialization of division points, together with the usual characteristic polynomial of Frobenius. These are established results, but the development does not prove them or formally verify their application to the division fields used here. Instead, the required statements for those fields are explicit assumptions in the development. Lean checks the deductions from them, including the degree-one-prime count, the summed small-index-divisor estimate, and the resulting positive lower density.

Thus the formal verification described here is of Theorem 1, assuming the aforementioned analytic and classical arithmetic inputs. The extension to the general CM theorem, Theorem 2, and the verification of its examples, are given in detail in the mathematical text and are not included in this formal verification. The Lean development records its assumptions and references explicitly, and its completed build has no proof placeholders or added global axioms.

Acknowledgments

I thank Peter Sarnak, Paul Pollack, and Jesse Thorner for helpful conversations. GPT-6 was used to help write and formalize the arguments. The author was supported by the National Science Foundation (Grant DMS-1001828).

References

- [1] M. Bhargava, Every nonsquare integer not equal to -1 is a primitive root modulo a positive lower density of primes, Hexagon preprint 2610.00228v1, October 2026. [Preprint](#).
- [2] Y.-M. J. Chen and J. Yu, On primitive points of elliptic curves with complex multiplication, *J. Number Theory* **114** (2005), no. 1, 66–87. [doi:10.1016/j.jnt.2005.02.005](#).
- [3] D. Cureton and J. Thorner, A quasi-Riemann hypothesis for Dedekind zeta functions, Hexagon preprint 2610.00200v2, October 2026. [Preprint](#).
- [4] D. Cureton and J. Thorner, Dedekind Zeta Zero-Free Region, formalization repository, Axiom Math, 2026. [Repository and statement](#).
- [5] R. Gupta and M. Ram Murty, Primitive points on elliptic curves, *Compositio Math.* **58** (1986), no. 1, 13–44. [Numdam](#).
- [6] R. Gupta and M. Ram Murty, Cyclicity and generation of points mod p on elliptic curves, *Invent. Math.* **101** (1990), no. 1, 225–235. [doi:10.1007/BF01231502](#).

- [7] C. Hooley, On Artin’s conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
- [8] N. Jones, F. Pappalardi, and P. Stevenhagen, Locally imprimitive points on elliptic curves, *Math. Proc. Cambridge Philos. Soc.* **180** (2026), 663–683. doi:[10.1017/S0305004125101795](https://doi.org/10.1017/S0305004125101795).
- [9] N. M. Katz, Lang–Trotter revisited, *Bull. Amer. Math. Soc. (N.S.)* **46** (2009), no. 3, 413–457. doi:[10.1090/S0273-0979-09-01257-9](https://doi.org/10.1090/S0273-0979-09-01257-9).
- [10] S. Lang and H. Trotter, Primitive points on elliptic curves, *Bull. Amer. Math. Soc.* **83** (1977), no. 2, 289–292. doi:[10.1090/S0002-9904-1977-14310-3](https://doi.org/10.1090/S0002-9904-1977-14310-3).
- [11] OpenAI, The Poisson–Dirichlet law for prime predecessors, preprint, 24 September 2026, Theorem 3.1 and Sections 3–5; version consulted: repository commit [1581d4cbdd69](https://github.com/openai/gpt-4o/commit/1581d4cbdd69). [Preprint](#).
- [12] OpenAI, The Quasi-Riemann Hypothesis: A Zero-Free Half-Plane $\Re(s) > 7/8$, preprint, 30 September 2026. [Preprint and accompanying files](#).
- [13] OpenAI, Primitive roots for every admissible integer base, preprint, 4 October 2026, Lemma 10.2, Proposition 10.3, and Section 12; version consulted: repository commit [1581d4cbdd69](https://github.com/openai/gpt-4o/commit/1581d4cbdd69). [Preprint](#).
- [14] K. A. Ribet, Dividing rational points on abelian varieties of CM-type, *Compositio Math.* **33** (1976), 69–74. [Author’s copy](#).
- [15] O. Robert, On van der Corput’s k -th derivative test for exponential sums, *Indag. Math.* **27** (2016), no. 2, 559–589. [Author’s manuscript](#).
- [16] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. IHES* **54** (1981), 123–201. [Numdam](#).
- [17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics **106**, Springer, 2009.