

Cyclic reductions of elliptic curves at a positive proportion of primes

Manjul Bhargava
Princeton University

24 October 2026

Abstract

We prove that every elliptic curve over $\mathbb{Q}$ whose points of order two are not all rational has cyclic reduction at a positive lower density of primes. This is the only necessary restriction: full rational two-torsion prevents cyclic reduction at every odd prime of good reduction. More precisely, a common zero-free half-plane $\Re s > 1 - 1/N$ for Dedekind zeta functions gives a lower proportion of at least $c_E/(N \log N)$, with $c_E > 0$ independent of N ; the theorem of Cureton and Thorner supplies $N = 32$. The proof uses the varying-cofactor sieve of our earlier works on primitive roots and primitive points, in conjunction with the marked Type II estimates of OpenAI, to construct candidate primes. We then apply a smoothed explicit formula for Dedekind zeta functions, with nonnegative weights on prime ideals, to bound the number of candidates with noncyclic reduction. This gives a common argument for CM and non-CM curves.

1 Introduction

In this article, we prove the following theorem.

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve whose points of order two are not all rational. Then there exists a positive lower proportion of primes p such that $E(\mathbb{F}_p)$ is cyclic.*

More precisely, let

$$C_E(X) = \#\{p \leq X : p \text{ of good reduction for } E, E(\mathbb{F}_p) \text{ cyclic}\}.$$

Then Theorem 1 states that

$$\liminf_{X \rightarrow \infty} \frac{C_E(X)}{\pi(X)} > 0. \quad (1)$$

The hypothesis in Theorem 1 is necessary. If all the points of order two are rational, then at every odd prime of good reduction the group $E(\mathbb{F}_p)$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, and so is not cyclic. Thus Theorem 1 gives a necessary and sufficient condition for an elliptic curve over $\mathbb{Q}$ to have cyclic reduction at a positive lower proportion of primes.

The study of cyclic reductions of elliptic curves over $\mathbb{Q}$ was initiated in the suggestive numerical investigations of Borosh, Moreno, and Porta [3]. A precise density prediction was given by Serre, who stated it in an equivalent Galois-theoretic form in his 1977–1978 course summary [14, pp. 67–68]. For each integer $m \geq 1$, let $K_m = \mathbb{Q}(E[m])$ be the field generated by the coordinates of the m -torsion points of E ; then Serre predicted that

$$C_E(X) \sim \delta_E \operatorname{Li}(X), \quad \delta_E = \sum_{m \geq 1} \frac{\mu(m)}{[K_m : \mathbb{Q}]}, \quad (2)$$

when $K_2 \neq \mathbb{Q}$, where $\text{Li}(X) = \int_2^X dt/\log t$; see also [10, Sections 2, 3, and 5]. Adapting Hooley's proof of Artin's conjecture under the generalized Riemann hypothesis [9], Serre established this cyclicity asymptotic under GRH and observed that the density δ_E is positive precisely when $K_2 \neq \mathbb{Q}$. A proof was published by Murty [10, Section 5]. Cojocaru and Murty [6] later obtained sharper error terms in this conditional asymptotic.

For curves with complex multiplication, Murty [10] removed the GRH assumption, using the class field theory of CM curves and a number-field version of the Bombieri–Vinogradov theorem. Cojocaru [5] subsequently gave an even simpler proof with explicit error terms. Thus the positive-proportion conclusion was already known in the CM case.

For general elliptic curves, Gupta and Murty [8] proved that cyclic reduction occurs at infinitely many primes whenever $K_2 \neq \mathbb{Q}$. More precisely, their theorem gives the unconditional lower bound

$$C_E(X) \gg_E \frac{X}{(\log X)^2}.$$

For non-CM curves, Cojocaru [4, Theorem 1.2] proved that the asymptotic (2) follows from the weaker hypothesis that the Dedekind zeta functions of K_m , for squarefree m , have no zeros in $\Re s > 3/4$. The zero-free region available to us from Cureton and Thorner [7] is $\Re s > 31/32$, which is weaker and does not supply the hypothesis used by Cojocaru. Our purpose is to obtain the positive-proportion lower bound (1) for every curve with $K_2 \neq \mathbb{Q}$ using this narrower zero-free region.

The analytic framework comes from our earlier works on Artin's primitive root problem [1] and on primitive points on elliptic curves [2]. The varying-cofactor sieve developed there, using the marked Type II estimates of OpenAI [11, 12], produces primes whose predecessor has the form

$$p - 1 = crQ, \quad r \leq x^\epsilon, \quad Q > x^{0.9} \text{ prime}, \quad q \mid r \implies q > Y, \quad (3)$$

where $x < p < 2x$, c is a fixed power of two, and $\epsilon > 0$ and Y are fixed before x tends to infinity. In a suitable fixed arithmetic progression, the number of these primes is at least a constant times

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

Allowing the cofactor r to vary supplies the additional logarithm needed for a positive proportion. The uniformity in ϵ and Y will also be important.

To use these primes, recall that $E(\mathbb{F}_p)$ fails to be cyclic precisely when p splits completely in K_ℓ for some prime $\ell \neq p$. Such an ℓ divides $p - 1$ and satisfies $\ell^2 \mid \#E(\mathbb{F}_p)$. We choose the progression to exclude complete splitting in K_2 . Hasse's bound excludes the distinguished large prime Q in (3). Every remaining obstruction therefore comes from a prime

$$Y < \ell \leq x^\epsilon.$$

This observation makes the predecessor $p - 1$ useful for arbitrary elliptic curves, even though their group orders need not have any fixed form.

The degree of K_ℓ is $\gg_E \ell^2$, and its logarithmic root discriminant is $\ll_E \log \ell$. We apply the explicit formula for its Dedekind zeta function with a nonnegative smooth weight that is at least one on the interval being counted. Every completely split prime p in this interval contributes at least $[K_\ell : \mathbb{Q}] \log p$ to the resulting nonnegative sum, so a zero-free half-plane gives an upper bound for the number of such primes. We count these exceptional primes among all primes and subtract them from the candidate set. Thus the argument needs no joint distribution statement for the cofactor

condition and the division fields. Both the cofactor construction and this smoothed prime-ideal bound are taken from [2]; we give the predecessor version of the construction and the division-field deduction explicitly.

We retain the width of the zero-free half-plane as a parameter in order to make its effect on the lower bound explicit. The quantitative result from which Theorem 1 follows is the following.

Theorem 2. *Let $E/\mathbb{Q}$ be an elliptic curve with $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Suppose that, for some fixed real $N \geq 2$, every Dedekind zeta function has no zeros in the half-plane*

$$\Re s > 1 - \frac{1}{N}. \quad (4)$$

Then there is a constant $c_E > 0$, depending only on E and independent of N , such that

$$C_E(2x) - C_E(x) \geq \frac{c_E}{N \log N} \frac{x}{\log x} \quad (5)$$

for all sufficiently large x . The threshold may depend on E and N , but c_E does not depend on N . After decreasing c_E if necessary, we also have

$$\liminf_{X \rightarrow \infty} \frac{C_E(X)}{\pi(X)} \geq \frac{c_E}{N \log N}. \quad (6)$$

Cureton and Thorner [7, Theorem 1.1] prove that every Dedekind zeta function has no zeros in $\Re s > 31/32$. Their theorem therefore supplies $N = 32$ in Theorem 2.

This paper is organized as follows. In Section 2, we recall the division-field criterion for cyclicity and construct the required arithmetic progression. In Section 3, we deduce the prime-predecessor estimate from the cofactor sieve of [2], recording the changes of sign and the required uniformity. In Section 4, we establish the division-field bounds and apply the smoothed prime-ideal bound to count completely split primes. Finally, in Section 5, we remove the remaining obstructions and prove Theorems 1 and 2.

Notation. Throughout the paper, the letters p, q, ℓ denote rational primes unless otherwise specified. We use $P^-(r)$ for the least prime divisor of an integer $r > 1$, and set $P^-(1) = \infty$. All constants allowed to depend on E may also depend on the fixed progression chosen for E . The parameters N , ϵ , and Y are fixed before x tends to infinity.

2 Cyclicity and a fixed arithmetic progression

We begin with the standard criterion that connects cyclic reduction to complete splitting. Let R_E denote the product of the primes of bad reduction of E .

Lemma 3. *Let $p \geq 3$ be a prime of good reduction for E . The group $E(\mathbb{F}_p)$ is noncyclic if and only if p splits completely in $K_\ell = \mathbb{Q}(E[\ell])$ for some prime $\ell \neq p$. Every such ℓ satisfies*

$$\ell \mid p - 1, \quad \ell^2 \mid \#E(\mathbb{F}_p), \quad \ell \leq \sqrt{p} + 1. \quad (7)$$

Proof. A noncyclic finite abelian group contains a subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ for some prime ℓ . Hasse's bound gives

$$\#E(\mathbb{F}_p) \leq (\sqrt{p} + 1)^2 < p^2 \quad (p \geq 3),$$

so such an ℓ cannot equal p . For $\ell \neq p$, good reduction identifies $E[\ell]$ with the geometric ℓ -torsion of the reduction. Thus $E(\mathbb{F}_p)$ contains $(\mathbb{Z}/\ell\mathbb{Z})^2$ if and only if Frobenius acts trivially on $E[\ell]$, i.e., if and only if p splits completely in K_ℓ . The Weil pairing gives $\ell \mid p - 1$, and the remaining assertions follow from the subgroup and Hasse's bound. These facts may also be found in [16]. $\square$

The progression must exclude complete splitting in K_2 while leaving every odd prime divisor of its modulus coprime to $p - 1$. The following observation gives this compatibility.

Lemma 4. *Let χ be a nontrivial Dirichlet character of conductor f . There is a unit $a \bmod f$ such that $\chi(a) \neq 1$ and*

$$a \not\equiv 1 \pmod{q} \quad \text{for every odd prime } q \mid f.$$

Proof. Write $\chi = \prod_{q^e \parallel f} \chi_q$ by the Chinese remainder theorem. For an odd prime $q \mid f$, let A_q be the units modulo q^e that are not congruent to 1 modulo q ; for $q = 2$, let A_2 be the full group of units modulo 2^e . Suppose that χ is identically 1 on the product of these sets. Fixing all but one coordinate shows that each χ_q is constant on A_q .

The component at two, if present, is therefore trivial. For odd q , multiplication by any unit congruent to 1 modulo q preserves A_q , so constancy forces χ_q to be trivial on the kernel of reduction modulo q . Hence it descends to a character of $\mathbb{F}_q^\times$ that is constant, say with value z , away from 1. If this character is nontrivial, character orthogonality gives

$$0 = 1 + (q - 2)z.$$

Since $|z| = 1$, this is possible only for $q = 3$, with $z = -1$. It follows that either every local character is trivial, contrary to the hypothesis, or the only nontrivial local character is the quadratic character modulo 3. In the latter case the product is constantly -1 on the indicated set, again a contradiction. $\square$

Lemma 5. *Suppose $K_2 \neq \mathbb{Q}$. There are fixed positive integers M, c and an integer u , with c a power of two, such that*

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

and every prime $p \equiv u \pmod{M}$ is of good reduction and does not split completely in K_2 . The modulus M may also be required to be divisible by any prescribed finite set of primes.

Proof. The nontrivial group $\text{Gal}(K_2/\mathbb{Q})$ is a subgroup of S_3 . It is therefore isomorphic to C_2 , C_3 , or S_3 , and has a nontrivial cyclic quotient of order two or three. Consequently K_2 contains an abelian extension $F/\mathbb{Q}$ of degree two or three. By the Kronecker–Weber theorem, there is a nontrivial Dirichlet character χ of conductor f such that a prime $p \nmid f$ splits completely in F if and only if $\chi(p) = 1$.

Choose a residue $a \bmod f$ as in Lemma 4, and choose an odd integer representative $a \neq 1$. Put $k = v_2(a - 1) \geq 1$ and $c = 2^k$. Take M divisible by f , 2^{k+1} , R_E , and the prescribed primes. By the Chinese remainder theorem, extend $a \bmod f$ to a class $u \bmod M$, retaining $a \bmod 2^{k+1}$ and choosing a residue different from 0 and 1 at every newly introduced odd prime. We may take the exponents at these new odd primes to be one.

Then $(u, M) = 1$, $v_2(u - 1) = k$, and no odd prime dividing M divides $u - 1$. These are exactly the conditions in (8). Moreover, a prime $p \equiv u \pmod{M}$ does not divide R_E and satisfies $\chi(p) = \chi(a) \neq 1$. It therefore has good reduction and does not split completely in F , or in K_2 . $\square$

Fix such M, c, u for the remainder of the paper. In particular, c is precisely the power of two dividing $p - 1$ for primes in this progression. The choices depend only on E .

3 Prime predecessors with a small cofactor

We use the varying-cofactor sieve of [2] in its predecessor form. That sieve counts primes $p \equiv u \pmod{M}$ with $p - 1 = crQ$ as in (3) by weighting integers d with $F_x(d-1)\mathcal{W}(d-1)$: the selector F_x records the required factorization, and the marks $\mathcal{W}$ are what make the marked Type II estimates applicable. Summing over the cofactors r with their marked weights gives a weighted harmonic mass comparable to $\epsilon \log x / \log Y$, producing the extra logarithm. The analytic input is the marked Type II estimate of [11, Theorem 3.1], together with the coefficient criterion and rough-factor replacement of [12, Lemma 10.2 and Proposition 10.3]. The arithmetic-progression and smoothing deductions, and the uniformity over invariant selectors and dyadic intervals, are in [2, Proposition 5].

Proposition 6. *Fix M, c, u satisfying (8). There are constants $A > 0$, $\epsilon_0 > 0$, and $Y_0 \geq 3$, depending only on this fixed progression, with the following property. For every fixed $0 < \epsilon < \epsilon_0$ and $Y \geq Y_0$, the set*

$$\mathcal{C}(x; \epsilon, Y) = \{x < p < 2x : p \equiv u \pmod{M}, p - 1 = crQ, r \leq x^\epsilon, Q > x^{0.9} \text{ prime}, P^-(r) > Y\} \quad (9)$$

satisfies

$$\#\mathcal{C}(x; \epsilon, Y) \geq A \frac{\epsilon}{\log Y} \frac{x}{\log x} \quad (10)$$

for all sufficiently large x . The threshold may depend on ϵ and Y , but A , ϵ_0 , and Y_0 do not.

Proof. Proposition 4 of [2] is the corresponding statement for prime successors, with $p + 1 = crQ$ and $u + 1$ in the progression conditions. We record the changes in its proof, which is given in Section 3 of that paper.

Use the same family of cofactors, marked weight $\mathcal{W}$, and invariant selector F_x . If $\mathcal{P}$ is the set of marked primes and $h_{\mathcal{P}}$ is the largest divisor of h supported on $\mathcal{P}$, the selector has the form

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

where $\mathcal{R}_x$ is the cofactor family constructed there. In particular, $F_x(\ell h) = F_x(h)$ for every marked prime ℓ , including when $\ell \mid h$. Replace the weight on integers d by

$$w(d) = \mathbf{1}_{d \equiv u \pmod{M}} \Psi(d/x) F_x(d-1) \mathcal{W}(d-1), \quad (11)$$

where $0 \leq \Psi \leq 1$ is smooth, supported in $(1, 2)$, and has $\int \Psi > 0$. On its support, $d = crQ + 1$, in place of $crQ - 1$. The required marked replacement is [2, Proposition 5] with $\sigma = 1$, the original sign in [11, 12]. Its constants are uniform over the invariant selectors and all dyadic intervals in the fixed exponent ranges used in the sieve.

Put $M_0 = M/c$. The progression for the prime variable Q becomes

$$Q \equiv ((u-1)/c)r^{-1} \pmod{M_0}. \quad (12)$$

Take Y_0 larger than every prime divisor of M . Then $(r, M) = 1$, and (12) is a reduced residue class. For an odd prime $\ell \nmid Mr$, the condition $\ell \mid crQ + 1$ excludes the single nonzero residue $Q \equiv -(cr)^{-1} \pmod{\ell}$. If $\ell \mid Mr$, no permitted residue is excluded. Thus the multiplicative sieve density remains

$$g_r(d) = \frac{\mathbf{1}_{(d, Mr)=1}}{\varphi(d)} \quad (d \text{ odd and squarefree}). \quad (13)$$

The distribution estimate of [2, Lemma 7] follows unchanged from Bombieri–Vinogradov, which is uniform over reduced residue classes. The smooth main integral has $\log((xy-1)/(cr))$ in place of $\log((xy+1)/(cr))$ in its denominator; all comparisons used there are identical.

In the rough-pair estimate of [2, Lemma 8], the congruence is now $mn \equiv 1 \pmod{cr}$, which has $\varphi(cr)$ solutions in pairs of residue classes. At an odd sieving prime $\ell \nmid cr$, the conditions $mn \equiv 1 \pmod{\ell}$ and $mn \equiv 0 \pmod{\ell}$ have, respectively, $\ell - 1$ and $2\ell - 1$ solutions, and these sets are disjoint. Hence the local counts and the resulting bound are unchanged, including the independence of its constant from the number of marked groups.

The cofactor mass and tail estimates involve only the factorization of $d - 1$ and are otherwise the same. Their full harmonic mass is $\gg_K \epsilon \log x / \log Y$, where K is the number of marked groups. The cutoff $r \leq x^\epsilon$ is imposed by discarding the negligible tail after the marked estimates; it is not inserted into F_x , since doing so would destroy its invariance. The block sieve, Buchstab subtraction, and removal of the remaining semiprimes therefore give the same lower bound as in [2, Proposition 4]. As in the last subsection of its Section 3, first fix all sieve parameters and K using only the progression, and then choose ϵ and Y . The boundedness of the marked weights converts the weighted lower bound into (10), with a constant independent of these two parameters. $\square$

The proof uses only the analytic estimates and cofactor construction of [2]; the elliptic curve and rational point considered there play no role in Proposition 6. In particular, the proposition applies to the progression of Lemma 5 for an arbitrary elliptic curve satisfying $K_2 \neq \mathbb{Q}$.

4 Completely split primes in division fields

For a prime ℓ , put

$$n_\ell = [K_\ell : \mathbb{Q}], \quad D_\ell = |\text{disc}(K_\ell)|.$$

The following familiar bounds allow us to treat CM and non-CM curves together.

Lemma 7. *For every prime ℓ ,*

$$n_\ell \gg_E \ell^2, \quad \frac{\log D_\ell}{n_\ell} \ll_E \log(2\ell). \quad (14)$$

Proof. If E has no complex multiplication, Serre's open image theorem [13, Théorème 2] gives

$$\text{Gal}(K_\ell/\mathbb{Q}) = \text{GL}_2(\mathbb{F}_\ell)$$

for all sufficiently large ℓ . Hence $n_\ell \asymp \ell^4$ in this case. If E has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field F , the main theorem of complex multiplication gives an image of bounded index, depending only on E , in $(\mathcal{O}/\ell\mathcal{O})^\times$ over F ; see [17, Chapter II]. Outside a fixed finite set of primes, this group has order $(\ell - 1)^2$ or $\ell^2 - 1$. Since

$$[F(E[\ell]) : F] = [K_\ell : K_\ell \cap F] \leq n_\ell,$$

we obtain $n_\ell \gg_E \ell^2$. Enlarging the implied constant accommodates the finitely many remaining primes in either case.

For the discriminant, the Néron–Ogg–Shafarevich criterion gives

$$\text{rad}(D_\ell) \mid \ell R_E,$$

and the faithful action on $E[\ell]$ gives $n_\ell \leq |\text{GL}_2(\mathbb{F}_\ell)| < \ell^4$. The general discriminant bound for a Galois extension [15, Proposition 6] is

$$\log D_\ell \leq (n_\ell - 1) \log \text{rad}(D_\ell) + n_\ell \log n_\ell.$$

Consequently,

$$\frac{\log D_\ell}{n_\ell} \leq \log R_E + 5 \log \ell,$$

which proves the second bound. $\square$

We next recall the consequence of the smoothed explicit formula needed here. For a number field T , let Λ_T be the von Mangoldt function on its nonzero integral ideals: $\Lambda_T(\mathfrak{p}^j) = \log N \mathfrak{p}$ for a prime ideal $\mathfrak{p}$ and $j \geq 1$, and Λ_T is zero otherwise. We choose a nonnegative smooth weight, so that discarding unwanted prime ideals can only decrease the sum.

Lemma 8 (Smoothed prime-ideal bound). *Let T be a number field of degree n and absolute discriminant D_T . Suppose that all nontrivial zeros of ζ_T have real part at most $1 - \delta$, where $0 < \delta \leq 1/2$. Fix a nonnegative smooth function f supported in $(1/2, 3)$ and at least one on $[1, 2]$. Then*

$$\sum_{\mathfrak{a}} \Lambda_T(\mathfrak{a}) f(N \mathfrak{a}/x) \ll_f x + x^{1-\delta} (\log D_T + n) \quad (x \geq 2), \quad (15)$$

with an implied constant independent of T and δ .

Proof. This is [2, Lemma 10]. We recall why its uniformity does not cost a factor depending on $1/\delta$. If $\hat{f}$ is the Mellin transform of f , the smoothed explicit formula gives a pole term $x \hat{f}(1)$, a zero term

$$- \sum_{\rho} x^{\rho} \hat{f}(\rho),$$

and a remaining contribution $O_f(\log D_T + n)$ for $x \geq 2$. Smoothness and the usual zero count give

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

The zero-free hypothesis bounds each $|x^{\rho}|$ by $x^{1-\delta}$, proving (15) with the asserted uniformity. $\square$

Proposition 9. *Let $N \geq 2$ be real, and suppose that every Dedekind zeta function has no zeros in $\Re s > 1 - 1/N$. Let*

$$B_\ell(x) = \#\{x < p < 2x : p \text{ splits completely in } K_\ell\}.$$

Then

$$B_\ell(x) \ll_E \frac{x}{\ell^2 \log x} + \frac{x^{1-1/N} \log(2\ell)}{\log x}. \quad (16)$$

Consequently, for $Y \geq 3$ and $z \geq 2$,

$$\sum_{Y < \ell \leq z} B_\ell(x) \ll_E \frac{x}{Y \log Y \log x} + \frac{x^{1-1/N} z}{\log x}. \quad (17)$$

All implied constants are independent of N , Y , and z .

Proof. Choose f as in Lemma 8, fixed once and for all. A completely split prime $p \in (x, 2x)$ gives n_ℓ distinct prime ideals of norm p in K_ℓ , and hence contributes at least $n_\ell \log x$ to the nonnegative sum in (15). Applying that lemma with $\delta = 1/N$ and dividing by $n_\ell \log x$ gives

$$B_\ell(x) \ll \frac{x}{n_\ell \log x} + \frac{x^{1-1/N}}{\log x} \left(\frac{\log D_\ell}{n_\ell} + 1 \right).$$

Lemma 7 proves (16). Finally, the elementary prime estimates

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

give (17). The first follows by partial summation from $\pi(t) \ll t/\log t$, and the second is Chebyshev's bound. $\square$

The factor n_ℓ contributed by a completely split prime is essential: it leaves only the logarithmic root discriminant in the error term. We have used the explicit formula for the Dedekind zeta function itself, so no separate effective Chebotarev theorem is required.

5 Proof of the main theorems

Let $E/\mathbb{Q}$ satisfy $K_2 \neq \mathbb{Q}$, and fix the progression of Lemma 5. We may decrease ϵ_0 in Proposition 6 so that $\epsilon_0 < 1/10$. Fix, for the moment, $0 < \epsilon < \epsilon_0$ and $Y \geq Y_0$.

Suppose $p \in \mathcal{C}(x; \epsilon, Y)$ and $E(\mathbb{F}_p)$ is noncyclic. By Lemma 3, p splits completely in K_ℓ for some prime $\ell \neq p$ satisfying (7). The progression excludes $\ell = 2$. Since

$$\ell \mid p - 1 = crQ$$

and c is a power of two, either $\ell \mid r$ or $\ell = Q$. For all sufficiently large x , the latter is impossible, because

$$Q > x^{0.9} > \sqrt{2x} + 1 \geq \sqrt{p} + 1.$$

Thus $\ell \mid r$ and

$$Y < \ell \leq r \leq x^\epsilon. \quad (18)$$

Suppose that every Dedekind zeta function has no zeros in $\Re s > 1 - 1/N$, for a fixed real $N \geq 2$. Proposition 9 therefore shows that the number of noncyclic candidates is at most

$$C_1 \frac{x}{Y \log Y \log x} + C_2 \frac{x^{1-1/N+\epsilon}}{\log x}, \quad (19)$$

where C_1, C_2 depend only on E . Combining (10) and (19), we obtain

$$C_E(2x) - C_E(x) \geq \left(\frac{A\epsilon}{\log Y} - \frac{C_1}{Y \log Y} - C_2 x^{-1/N+\epsilon} \right) \frac{x}{\log x} \quad (20)$$

for all sufficiently large x , with the threshold permitted to depend on the fixed parameters.

We now choose these parameters, keeping the dependence on N explicit. Fix

$$0 < \alpha < \min(1, 2\epsilon_0)$$

and then fix $B \geq 2$, depending only on E , so large that

$$2B \geq Y_0, \quad \frac{C_1}{B} \leq \frac{A\alpha}{4}.$$

For each fixed $N \geq 2$, put

$$\epsilon = \frac{\alpha}{N}, \quad Y = BN. \quad (21)$$

These choices are admissible in Proposition 6. The second term in parentheses in (20) is at most one quarter of the first. Moreover,

$$x^{-1/N+\epsilon} = x^{-(1-\alpha)/N} \longrightarrow 0 \quad (x \rightarrow \infty),$$

so for all sufficiently large x the third term is also at most one quarter of the first. We conclude that

$$C_E(2x) - C_E(x) \geq \frac{A\alpha}{2N \log(BN)} \frac{x}{\log x}. \quad (22)$$

Since $N \geq 2$,

$$\log(BN) \leq \left(1 + \frac{\log B}{\log 2}\right) \log N.$$

The constant

$$d_E = \frac{A\alpha}{2(1 + \log B / \log 2)} > 0$$

is independent of N , and (22) proves (5) with d_E in place of c_E .

For the lower proportion, apply this bound with $x = X/2$ and use the prime number theorem. It gives

$$\liminf_{X \rightarrow \infty} \frac{C_E(X)}{\pi(X)} \geq \frac{d_E}{2N \log N}.$$

Taking $c_E = d_E/2$ proves both assertions of Theorem 2. The zero-free half-plane $\Re s > 31/32$ of Cureton and Thorner now proves Theorem 1.

The argument isolates a set of primes on which every obstruction to cyclicity lies in the short range (18). It does not evaluate the full inclusion-exclusion sum in (2), or prove an asymptotic with that constant. Its conclusion is a positive lower proportion, uniformly expressed in terms of the available zero-free width.

Formal verification. The accompanying Lean development verifies the positive-proportion argument for integral Weierstrass models of elliptic curves from explicit analytic and arithmetic inputs. It proves the construction of the fixed progression and shows that, among the candidate primes, every obstruction to cyclicity—a subgroup $(\mathbb{Z}/\ell\mathbb{Z})^2$ in $E(\mathbb{F}_p)$, corresponding to complete splitting in K_ℓ —has $Y < \ell \leq x^\epsilon$. The bound for these exceptional primes, their subtraction, and the final parameter choice are proved within the development. The formal theorem gives $c_E/(N \log N)$, with $c_E > 0$ chosen before N , including the lower-proportion conclusion and its specialization to $N = 32$.

The analytic inputs are the zero-free hypothesis supplied by [7], the candidate-prime estimate from [1, 2], the prime number theorem, the elementary prime-sum estimates, and the smoothed prime-ideal bound of Lemma 8. The last bound is proved in [2, Lemma 10] from Mellin inversion, the Dedekind zeta functional equation, and the standard zero count, with a constant independent of the field and the zero-free width. It is an explicit hypothesis in Lean because that analytic derivation has not been formalized. The arithmetic inputs are standard facts about torsion, reduction, and division fields. These inputs are supplied as explicit hypotheses; Lean checks the deductions from them. The development records its assumptions and references explicitly, and its completed build has no proof placeholders or added global axioms.

The Lean sources for [1], [2], and the current article are available at <https://github.com/bhargavanjul/FormalizedProofs/>.

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] M. Bhargava, Rational points on elliptic curves that are primitive modulo a positive proportion of primes, Hexagon preprint 2610.00294v1, October 2026. [Preprint](#).
- [3] I. Borosh, C. J. Moreno, and H. Porta, Elliptic curves over finite fields. II, *Math. Comp.* **29** (1975), no. 131, 951–964. [Article](#).
- [4] A. C. Cojocaru, On the cyclicity of the group of $\mathbb{F}_p$ -rational points of non-CM elliptic curves, *J. Number Theory* **96** (2002), no. 2, 335–350. [doi:10.1006/jnth.2002.2789](#).
- [5] A. C. Cojocaru, Cyclicity of CM elliptic curves modulo p , *Trans. Amer. Math. Soc.* **355** (2003), no. 7, 2651–2662. [doi:10.1090/S0002-9947-03-03283-5](#).
- [6] A. C. Cojocaru and M. Ram Murty, Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik’s problem, *Math. Ann.* **330** (2004), no. 3, 601–625. [doi:10.1007/s00208-004-0562-x](#).
- [7] D. Cureton and J. Thorner, A quasi-Riemann hypothesis for Dedekind zeta functions, Hexagon preprint 2610.00200v2, October 2026. [Preprint](#).
- [8] 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](#).
- [9] C. Hooley, On Artin’s conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
- [10] M. Ram Murty, On Artin’s conjecture, *J. Number Theory* **16** (1983), no. 2, 147–168. [doi:10.1016/0022-314X\(83\)90039-2](#).
- [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. [Preprint](#).
- [12] 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. [Preprint](#).
- [13] J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331. [doi:10.1007/BF01405086](#).
- [14] J.-P. Serre, Résumé des cours de 1977–1978, *Annuaire du Collège de France* (1978), 67–70. [Original course summary](#).
- [15] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. IHES* **54** (1981), 123–201. [Numdam](#).

- [16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics **106**, Springer, 2009.
- [17] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer, 1994.