# Bounded gaps between primes with a given primitive root, II

Roger C. Baker[*]

Department of Mathematics
Brigham Young University
Provo, UT 84602, USA

Paul Pollack[†]

Department of Mathematics
University of Georgia
Athens, GA 30602, USA

#### Abstract

Let $m$ be a natural number, and let $\mathscr{Q}$ be a set containing at least $\exp(Cm)$ primes. We show that one can find infinitely many strings of $m$ consecutive primes each of which has some $q \in \mathscr{Q}$ as a primitive root, all lying in an interval of length $O_{\mathscr{Q}}(\exp(C'm))$. This is a bounded gaps variant of a theorem of Gupta and Ram Murty. We also prove a result on an elliptic analogue of Artin's conjecture. Let $E/\mathbb{Q}$ be an elliptic curve with an irrational 2-torsion point. Assume GRH. Then for every $m$, there are infinitely many strings of $m$ consecutive primes $p$ for which $E(\mathbb{F}_p)$ is cyclic, all lying an interval of length $O_E(\exp(C''m))$. If $E$ has CM, then the GRH assumption can be removed. Here $C$, $C'$, and $C''$ are absolute constants.

2010 *Mathematics subject classification.* Primary: 11A07, Secondary: 11G05

*Key words and phrases.* Artin's conjecture, bounded gaps, elliptic Artin, Maynard–Tao theorem, primitive root.

[*] email: baker@math.byu.edu

[†] email: pollack@math.uga.edu

# 1 Introduction

In 1927, Artin proposed the following conjecture: *If $g$ is not a square and $g \neq -1$, then there are infinitely many primes $p$ for which $g$ is a primitive root modulo $p$.* Artin's conjecture remains unsolved, but investigations in this direction have led to many deep and beautiful results (see [Mor12]).

In 1967, Hooley [Hoo67] showed that Artin's conjecture is a consequence of the Generalized Riemann Hypothesis for Dedekind zeta functions (hereafter GRH). In [Pol14], it was shown how Hooley's proof could be merged with the method of Maynard–Tao for producing bounded gaps between primes: *On GRH, for every nonsquare $g \neq -1$ and every $m$, there are infinitely many runs of $m$ consecutive primes all possessing $g$ as a primitive root and lying in an interval of length $O_m(1)$.*

There is not a single $g$ for which the conclusion of Artin's conjecture is known to hold unconditionally. However, in 1984 Gupta and Ram Murty [GM84] described how to produce many finite sets of integers some member of which satisfies Artin's conjecture. Their method was refined by Ram Murty and Srinivasan [MS87], Gupta, Ram Murty, and Kumar Murty [GMM87], and by Heath-Brown [HB86]. It follows from the results in this last paper that Artin's conjecture holds for at least one $g \in \{2, 3, 5\}$. We prove a result in this direction where the primes produced are consecutive and contained in an interval of bounded length.

Recall that nonzero $q_1, \dots, q_r \in \mathbb{Z}$ are said to be *multiplicatively independent* if $q_1^{e_1} \cdots q_r^{e_r} = 1$ in integers $e_1, \dots, e_r$ only when $e_1 = \cdots = e_r = 0$.

**Theorem 1.1.** *Let $\mathscr{Q}$ be a set of $r$ multiplicatively independent integers. Assume that the elements $q_1, \dots, q_r$ of $\mathscr{Q}$ satisfy the following technical condition:*

> *If $e_0, e_1, \dots, e_r$ are nonnegative integers for which $(-3)^{e_0} q_1^{e_1} \cdots q_r^{e_r}$ is a square, then $\sum_{i=0}^{r} e_i$ is even.* (*)

*Let $m$ be a natural number. If $r \geq \exp(Cm)$, then there are infinitely many runs of $m$ consecutive primes $p_1 < \cdots < p_m$ all of which possess some element of $\mathscr{Q}$ as a primitive root, where also*

$$p_m - p_1 \leq \mathfrak{f}(\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_r})/\mathbb{Q}) \cdot \exp(C'm).$$

*Here $C$ and $C'$ are (positive) absolute constants, and $\mathfrak{f}(K/\mathbb{Q})$ denotes the conductor of the abelian extension $K/\mathbb{Q}$.*

*Remark.* Of course, (*) holds whenever $q_1, \dots, q_r$ are distinct (positive) primes.

The techniques used to attack Artin's conjecture can also be used to answer statistical questions about reductions of elliptic curves. Here the general setup is as follows: Let $E/\mathbb{Q}$ be an elliptic curve. For all but finitely many primes $p$, one can reduce $E$ mod $p$ to obtain an elliptic curve defined over $\mathbb{F}_p$. What can one say about the structure of the group $E(\mathbb{F}_p)$ as $p$ varies? It is known that $E(\mathbb{F}_p)$ is always generated by two elements, and so it is particularly natural to ask when one suffices. In other words, how often is $E(\mathbb{F}_p)$ a cyclic group?

If all of the 2-torsion of $E$ is defined over $\mathbb{Q}$, then $(\mathbb{Z}/2\mathbb{Z})^2$ sits inside $E(\mathbb{Q})$, and so $E(\mathbb{F}_p)$ is cyclic for at most finitely many primes $p$. So assume $E$ has an irrational 2-torsion point. Assuming GRH, Serre showed that there are infinitely many primes $p$ with $E(\mathbb{F}_p)$ cyclic, using Hooley's approach [Hoo67] to Artin's conjecture. In fact, Serre [Ser78] obtained an asymptotic formula for the number of such $p \leq x$, as $x \to \infty$. Ram Murty [Mur83] showed that when $E$ has CM, Serre's asymptotic formula can be proved unconditionally; a simpler argument for the same conclusion has been given by Cojocaru [Coj03]. See [CM04] and [AM10] for investigations into the size of the error term in Serre's formula.

We prove the following bounded gaps result.

**Theorem 1.2.** *Let $E/\mathbb{Q}$ be an elliptic curve with an irrational 2-torsion point. Let $m$ be a natural number. If GRH holds, then there are infinitely many runs of $m$ consecutive primes $p_1 < p_2 < \cdots < p_m$ for which $E(\mathbb{F}_p)$ is cyclic, where*

$$p_m - p_1 \leq \mathrm{rad}(\Delta_E) \cdot \exp(C''m).$$

*Here $\mathrm{rad}(\Delta_E)$ is the product of the primes of bad reduction, and $C''$ is an absolute constant. If $E$ has CM, then the GRH assumption can be removed.*

The CM case of Theorem 1.2 is particularly easy because of the abundance of supersingular primes. According to a criterion of Deuring (see, e.g., [Lan87, Theorem 12, p. 182]), a prime $p$ of good reduction is supersingular precisely when there is a unique prime in the CM field lying above $p$. As we explain below, this implies that $\mathbb{E}(\mathbb{F}_p)$ is cyclic for all primes from a certain arithmetic progression. This allows us to appeal to a recent theorem of Banks–Freiberg–Turnage-Butterbaugh [BFTB] about long runs of such primes in short intervals.

It is perhaps slightly unsettling that we produce only supersingular primes in the CM case. In general, this is unavoidable. For instance, consider the curve $E$ given by $y^2 = x^3 + x$, whose 2-torsion points are defined over $\mathbb{Q}(i)$. Since $E$ has CM by $\mathbb{Z}[i]$, Deuring's criterion tells us that a prime $p$ of good ordinary reduction splits in $\mathbb{Q}(i)$, and so $E(\mathbb{F}_p)$ contains $(\mathbb{Z}/2\mathbb{Z})^2$ for all such $p$. Our final theorem says that *if* there are infinitely many $p$ of good ordinary reduction with $E(\mathbb{F}_p)$ cyclic, then the set of these $p$ has bounded gaps.

**Theorem 1.3.** *Let $E/\mathbb{Q}$ be a CM elliptic curve. Assume that there are infinitely many primes $p$ of good ordinary reduction for which $E(\mathbb{F}_p)$ is cyclic. Then there are infinitely many tuples of $m$ such primes $p_1 < \cdots < p_m$ with $p_m - p_1 \ll \exp(O_E(m))$.*

Unfortunately, the method of proof of Theorem 1.3 does not allow us to impose the condition that the primes produced here are consecutive.

It would be desirable to remove the GRH assumption altogether from Theorem 1.2. We note that in [GM90], Gupta and Ram Murty showed unconditionally that if $E$ has an irrational 2-torsion point, then there are always infinitely many primes $p$ with $E(\mathbb{F}_p)$ cyclic (but they do not get the order of magnitude for the count predicted by Serre's asymptotic formula). Their proof relies on a sieve result seemingly unavailable in our context.

## Notation

The letters $\ell$ and $p$ are reserved for primes. We write $p^{-}(n)$ for the smallest prime factor of $n$, with the convention that $p^{-}(1) = \infty$. We use $\mathrm{rad}(n)$ to denote the largest squarefree divisor of $n$. We use $C_1, C_2, \dots$ for absolute positive constants that are be thought of as large. If $F$ is a number field, $\mathbb{Z}_F$ denotes its ring of integers, and we write $\Delta_F$ for the absolute discriminant of $F$. If $E$ is an elliptic curve defined over $\mathbb{Q}$, we let $\Delta_E$ denote the minimal discriminant of $E/\mathbb{Q}$. We write $\mathbb{P}(\cdot)$ for the probability of an event and $\mathbb{E}[\cdot]$ for the expectation of a random variable.

# 2 Preliminaries for the proof of Theorem 1.1

If $q_1, \dots, q_r \in \mathbb{Z}$ and $p \nmid q_1 \cdots q_r$, we write $\langle q_1, \dots, q_r \bmod p\rangle$ for the subgroup of $\mathbb{F}_p^{\times}$ generated by the mod $p$ reductions of the $q_i$. The next lemma is due to Ram Murty and Srinivasan [MS87] (compare with [GM84, Lemma 2]).

**Lemma 2.1.** *Let $q_1, \dots, q_r$ be multiplicatively independent integers, and let $Y \geq 1$. The number of primes p for which*

$$\#\langle q_1, \dots, q_r \bmod p\rangle \leq Y$$

*is $O(Y^{1+\frac{1}{r}})$. Here the implied constant may depend on the $q_i$.*

*Proof.* We include the short proof. Suppose that $\#\langle q_1, \dots, q_r \bmod p\rangle \leq Y$. By the pigeonhole principle, as $e_1, \dots, e_r$ run independently from 0 through $\lfloor Y^{1/r} \rfloor$, two expressions of the form $q_1^{e_1} \cdots q_r^{e_r}$ must coincide mod $p$. Consequently, for some choice of integers $e_i'$ with each $|e_i'| \leq Y^{1/r}$ and not all $e_i' = 0$, $p$ divides the numerator of the nonzero rational number $q_1^{e_1'} \cdots q_r^{e_r'} - 1$. This numerator is (crudely) bounded above by $2\max\{|q_1|, \dots, |q_r|\}^{rY^{1/r}}$ and so has $O(Y^{1/r})$ prime divisors. Summing over the $O(Y)$ possibilities for the $e_i'$ completes the proof. □

The following lemma is used to construct an admissible collection of linear functions to which Maynard's machinery can be applied.

**Lemma 2.2.** *Let $q_1, \dots, q_r$ be nonzero integers satisfying (*). Let $v = 16\prod_{\ell \mid q_1 \cdots q_r,\ \ell > 2} \ell$. One can select an integer $u$ coprime to $v$ so that both of the following hold:*

1. *For every $p \equiv u \pmod{v}$, the Legendre symbols $\left(\frac{q_1}{p}\right) = \cdots = \left(\frac{q_r}{p}\right) = -1$.*
2. *If $T$ is the largest power of 2 dividing $u-1$, then $T \in \{2,4,8\}$, and $\gcd(\frac{u-1}{T}, v) = 1$.*

*Proof.* For $r = 3$, this lemma was proved by Heath-Brown. Since the argument for the general case is the same, we only outline the main steps, referring the reader to [HB86, pp. 35–36] for the details. By estimating $\sum_{p \leq x} \left(1 - \left(\frac{-3}{p}\right)\right) \prod_{i=1}^{r} \left(1 - \left(\frac{q_i}{p}\right)\right)$ from below — keeping (*) in mind — one shows that there are infinitely many primes $p$ with

$\left(\frac{-3}{p}\right) = \left(\frac{q_1}{p}\right) = \cdots = \left(\frac{q_r}{p}\right) = -1$. Fix one and call it $p_0$. For each odd prime $\ell$ dividing $q_1 \cdots q_r$, put

$$u_\ell = \begin{cases} p_0 & \text{if } \ell \nmid p_0 - 1, \\ 4p_0 & \text{otherwise,} \end{cases} \quad \text{and put} \quad u_2 = \begin{cases} p_0 & \text{if } 16 \nmid p_0 - 1, \\ p_0 - 8 & \text{otherwise.} \end{cases}$$

Then for all odd primes $\ell \mid q_1 \cdots q_r$, we see that $\ell \nmid u_\ell - 1$. (We have used here that $p_0 \equiv -1 \pmod 6$, since $\left(\frac{-3}{p}\right) = -1$.) One checks that it suffices to choose $u$ as a solution to the simultaneous congruences

$$u \equiv u_\ell \pmod{\ell}\ \forall \text{ odd } \ell \mid q_1 \dots q_r \quad \text{and} \quad u \equiv u_2 \pmod{16}. \qquad \square$$

Let $\mathscr{L}$ be a set of $k$ distinct linear functions, say $L_1(n) = a_1 n + b_1, \dots, L_k(n) = a_k n + b_k$, where each $a_i, b_i \in \mathbb{Z}$ and every $a_i > 0$. We say that $\mathscr{L}$ is *admissible* if for each prime $p$, there is some integer $n_p$ for which $p \nmid \prod_{i=1}^{k} L_i(n_p)$. Note that if each $(a_i, b_i) = 1$, to check admissibility it suffices to check primes $p \le k$.

**Lemma 2.3.** *Let $q_1, \dots, q_r$ be nonzero integers satisfying (*), and let $u$ and $v$ be chosen as in Lemma 2.2. Let $\kappa$ be a natural number. There are integers $a_1 < \cdots < a_\kappa$, each congruent to $u$ mod $v$, for which the $2\kappa$ linear functions*

$$\begin{aligned} L_1(n) &= vn + a_1, & \dots,\quad L_\kappa(n) &= vn + a_\kappa, \\ \tilde{L}_1(n) &= \frac{v}{T}n + \frac{a_1 - 1}{T}, & \dots,\quad \tilde{L}_\kappa(n) &= \frac{v}{T}n + \frac{a_\kappa - 1}{T} \end{aligned}$$

*make up an admissible family. Moreover, we can select the $a_i$ in such a way that*

$$a_\kappa - a_1 \le v \cdot (2\kappa)^{C_1}.$$

*Proof.* By the fundamental lemma of the sieve, if $C_1$ is large enough, then the number of integers $A \in [0, (2\kappa)^{C_1}]$ for which $p^-((vA + u)(\frac{v}{T}A + \frac{u-1}{T})) > 2\kappa$ exceeds

$$\frac{1}{2}((2\kappa)^{C_1}) \prod_{p \le 2\kappa} (1 - 2/p).$$

Increasing $C_1$ if necessary, this lower bound exceeds $\kappa$. Pick $\kappa$ of these integers, say $A_1 < \cdots < A_\kappa$. The theorem follows upon choosing $a_i = vA_i + u$. Indeed, for primes $p \le 2\kappa$, we have arranged matters so that $p \nmid \prod_{i=1}^{\kappa} L_i(0)\tilde{L}_i(0)$. $\square$

*Remark.* In the next section, we will show that all of the $\tilde{L}_i$ are almost primes at the same time that several of the $L_i$ are prime. A similar strategy appears in work of Li and Pan [LP14], who seem to have been the first to notice that the Maynard–Tao method can be applied with auxiliary 'almost prime' conditions added. In the context of the earlier GPY method, this observation was made by Pintz [Pin10].

# 3 Proof of Theorem 1.1

The following key proposition is contained in recent work of Maynard [May14].

**Proposition 3.1.** *Fix an admissible family $\mathscr{L}$ of $k$ distinct linear functions, where $k \geq 2$. Suppose that $x$ is sufficiently large, $x > x_0(\mathscr{L})$. There is a probability measure on*

$$\mathscr{A}(x) := \{n \in \mathbb{Z} : x \leq n < 2x\}$$

*with all of the following properties:*

(1) *The probability mass at any single $n \in \mathscr{A}(x)$ is*

$$\ll x^{-1}(\log x)^k \left( \prod_{i=1}^{k} \prod_{p | L_i(n)} 4 \right) \exp(O(k \log k)).$$

(2) *For each $L \in \mathscr{L}$,*

$$\mathbb{P}(L(n) \text{ is prime}) \gg \frac{\log k}{k}.$$

(3) *Suppose that $\rho \in [k\frac{(\log\log x)^2}{\log x}, \frac{1}{25}]$. For each $L \in \mathscr{L}$,*

$$\mathbb{E}\Bigg[ \sum_{\substack{p | L(n) \\ p < x^{\rho}}} 1 \Bigg] \ll \rho^2 k^4 (\log k)^2.$$

(4) *Suppose that $L(n) = a_0 n + b_0$ is a linear function not belonging to $\mathscr{L}$. Suppose also that $|a_0|, |b_0| \leq x$ and that $\Delta_L$, defined by*

$$\Delta_L := a_0 \prod_{j=1}^{k} |a_0 b_j - b_0 a_j|,$$

*is nonzero. Then*

$$\mathbb{P}(p^-(L(n)) > x^{1/25}) \ll \frac{\Delta_L/\varphi(\Delta_L)}{\log x}.$$

*Although $x_0$ may depend on $\mathscr{L}$, all implied constants in this statement are absolute.*

*Proof (sketch).* This follows from [May14, Proposition 6.1]. In the setup of that proposition, $\mathscr{A}$ is the set of natural numbers, $\mathscr{L}$ is as above, $\mathscr{P}$ is the set of all primes, $B = 1$, $\theta = 2/5$, and $\alpha = 1$. The probability measure on $\mathscr{A}(x)$ assigns to each $n$ the probability mass $w(n)/\sum_{n \in \mathscr{A}(x)} w(n)$. Our (1) follows from Proposition 6.1(1) together with the immediately preceding estimate for $w_n$; we also use Maynard's lower bounds on $\mathfrak{S}(\mathscr{L})$ and $I_k(F)$ given in (8.2) and Lemma 8.6, respectively. Our (2) is deduced from

Proposition 6.1(1,2); here we use the estimate $J_k/I_k \gg \log k/k$ and the observation that for each $L(n) = a_L n + b_L \in \mathscr{L}$, we have (in Maynard's notation)

$$\#\mathscr{P}_{L,\mathscr{A}}(x) = \sum_{\substack{a_L x + b_L \le p < 2a_L x + b_L \\ p \equiv b_L \pmod{a_L}}} 1 \sim \frac{1}{\varphi(a_L)} \frac{a_L x}{\log x} \sim \frac{a_L}{\varphi(a_L)} \frac{\#\mathscr{A}(x)}{\log x}.$$

Our (3) comes from Proposition 6.1(1,4), and (4) comes from Proposition 6.1(1,3). □

We now prove Theorem 1.1.

*Proof.* Assume that $r \ge \exp(C_2 m)$, and let $\kappa = \lceil \exp(C_3 m) \rceil$. Let $c$ be a small positive absolute constant. The necessary constraints on the constants $C_2$, $C_3$, and $c$ will emerge in the proof.

Let $q_1', \dots, q_r'$ be the integers obtained from $q_1, \dots, q_r$ by replacing each $q_i$ with its squarefree part. That is, $q_i'$ is the unique squarefree integer for which $q_i/q_i'$ is a square. Since $q_1, \dots, q_r$ satisfy (*), so do $q_1', \dots, q_r'$. Let $k = 2\kappa$, and let $L_i$ and $\tilde{L}_i$, for $1 \le i \le \kappa$, be the linear functions produced by Lemma 2.3 applied with $q_1', \dots, q_r'$. Every prime dividing $q_1' \cdots q_r'$ divides $f := \mathfrak{f}(\mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_r})/\mathbb{Q})$, and thus $v = 16 \prod_{\ell \mid q_1' \cdots q_r',\ \ell > 2} \ell$ divides $16f$.

We now invoke Proposition 3.1. We will show that with positive probability, an $n \in \mathscr{A}(x)$ satisfies all of

(i) at least $m$ of $L_1(n)$, …, $L_\kappa(n)$ are prime,

(ii) $p^-(L_i(n)) \ge x^{\frac{c}{k^3 \log k}}$ and $p^-(\tilde{L}_i(n)) \ge x^{\frac{c}{k^3 \log k}}$ for all $i = 1, \dots, \kappa$,

(iii) all integers in the interval $[L_1(n), L_\kappa(n)]$ that are not one of the $L_i(n)$ are composite,

(iv) whenever $p = L(n)$ is prime with $L \in \{L_1, \dots, L_\kappa\}$, $p$ possesses some element of $\mathscr{Q}$ as a primitive root.

If (i)–(iv) hold for $n$, then the set of primes in $[L_1(n), L_\kappa(n)]$ has at least $m$ elements, each one of which possesses some element of $\mathscr{Q}$ as a primitive root. Moreover, the difference between the largest and smallest such primes is at most

$$L_\kappa(n) - L_1(n) = a_\kappa - a_1 \le v(2\kappa)^{C_1} \le f \exp(C_4 m),$$

provided that $C_4$ is large enough in terms of $C_1$ and $C_3$. Thus, we obtain Theorem 1.1 with $C = C_2$ and $C' = C_4$.

To begin analyzing (i)–(iv), let $\mathscr{P}$ be the set of primes, and consider the random variable $X := \sum_{i=1}^{\kappa} \mathbf{1}_{\mathscr{P}}(L_i(n))$. Proposition 3.1(2) and our choice of $\kappa$ yield $\mathbb{E}[X] \gg C_3 m$. We assume $C_3$ is large enough that $\mathbb{E}[X] > m$. Noting the inequality

$$\mathbf{1}_{X \ge m} \ge \kappa^{-1}(X - (m-1)),$$

and taking expectations, we find that (i) holds with probability at least $\kappa^{-1}$.

Let $L$ be one of the linear functions in $\mathscr{L}$. Then

$$\mathbb{P}(p^-(L(n)) < x^{c/(k^3 \log k)}) \leq \mathbb{E}\Bigg[\sum_{p \mid L(n),\ p < x^{c/(k^3 \log k)}} 1\Bigg].$$

So from Proposition 3.1(3), (ii) fails with probability

$$\ll k \cdot \left(\frac{c}{k^3 \log k}\right)^2 k^4 (\log k)^2.$$

We may assume $c > 0$ is small enough that the odds of failure are less than $\frac{1}{2}\kappa^{-1}$. Then (i) and (ii) hold simultaneously with probability at least $\frac{1}{2}\kappa^{-1}$.

We claim that (iii) fails with probability $o(1)$, as $x \to \infty$. It is enough to show that if $a$ is a fixed integer from $[a_1, a_\kappa]$, and $a \notin \{a_1, \dots, a_\kappa\}$, then the probability that $L(n) := vn + a$ is prime is $o(1)$. This follows immediately from Proposition 6.1(4) if $L$ is not a rational multiple of any $L_i$ or $\tilde{L}_i$. Since $L$ has leading coefficient $v$ and $a \notin \{a_1, \dots, a_\kappa\}$, $L$ is not a multiple of any $L_i$. Since each $\tilde{L}_i$ has leading coefficient $v/T$, if $L$ is a multiple of some $\tilde{L}_i$, then $L = T\tilde{L}_i$; but then $T \mid L(n)$ and so $L(n)$ is composite for all $n \in \mathscr{A}(x)$.

Now assume that (ii) holds but that (iv) fails. We will show that this occurs with probability $o(1)$, as $x \to \infty$. In view of our previous estimates, this will complete the proof of Theorem 1.1.

Assume that $p = L(n)$ is prime, with $L \in \{L_1, \dots, L_\kappa\}$, but that $p$ fails to have any $q \in \mathscr{Q}$ as a primitive root. From Lemma 2.2(1) and our choice of $\mathscr{L}$, each $q \in \mathscr{Q}$ is is a nonsquare modulo $p$. Thus, for each $q \in \mathscr{Q}$, there is a prime $s = s_q$ dividing $(p-1)/T$ for which $q$ is an $s$th power modulo $p$. Put $t = \lceil 2c^{-1}k^3 \log k \rceil$. Since (ii) holds, $\Omega((p-1)/T) \leq t$. (We assume here, as elsewhere in the proof, that $x$ is sufficiently large.) Recalling that $k = 2\lceil \exp(C_3 m) \rceil$, we assume $C_2$ is large enough that

$$\exp(C_2 m) > (t-1)t.$$

Since $\#\mathscr{Q} = r \geq \exp(C_2 m)$, the pigeonhole principle guarantees that at least $t$ values of $q \in \mathscr{Q}$ share the same value of $s_q$; call this common value $s$. Relabeling, we can assume these are $q_1, \dots, q_t$. Then

$$\#\langle q_1, \dots, q_t \bmod p \rangle \leq \frac{p-1}{s} \leq \frac{p-1}{p^-((p-1)/T)} \leq x^{1 - \frac{c}{2k^3 \log k}} \leq x^{1-\frac{1}{t}}.$$

By Lemma 2.1, $p$ is restricted to a set of size $\ll_{\mathscr{Q}} (x^{1-1/t})^{1+1/t} = x^{1-\frac{1}{t^2}}$. Given $L$, the prime $p = L(n)$ determines $n$, restricting $n$ also to a set of size $O_{\mathscr{Q}}(x^{1-1/t^2})$. Since there are $O_m(1)$ possibilities for $L$, the number of $n \in \mathscr{A}(x)$ for which (ii) holds but (iv) fails is $O_{\mathscr{Q},m}(x^{1-1/t^2})$.

Since $n$ satisfies (ii), each of $L_1(n), \dots, L_\kappa(n)$ has at most $t$ prime factors. So from Proposition 3.1(i), the probability mass at $n$ is at $O_m(x^{-1}(\log x)^k)$. Thus, the probability of selecting an $n$ detected in the previous paragraph is $O_{m,\mathscr{Q}}((\log x)^k x^{-1/t^2})$, which is $o(1)$ as $x \to \infty$. □

# 4 Preparation for the proof of Theorem 1.2

We begin with some background on elliptic curves. For each prime $\ell$, let $K_\ell$ denote the $\ell$-torsion field $\mathbb{Q}(E[\ell])$. It is well-known and easy to check that $K_\ell$ is a Galois extension of $\mathbb{Q}$. Now let $p$ be a prime of good reduction for $E$. Clearly, $E(\mathbb{F}_p)$ is cyclic if and only if it does not contain $(\mathbb{Z}/\ell\mathbb{Z})^2$ for any prime $\ell$. The following lemma, due to Ram Murty [Mur83, p. 159], shows that whether or not $E(\mathbb{F}_p)$ is cyclic amounts to a series of conditions on the splitting of $p$ in the fields $K_\ell$.

**Lemma 4.1.** *Let $p$ be a prime of good reduction for $E$. If $\ell$ is a prime with $\ell \neq p$, then $E(\mathbb{F}_p)$ contains $(\mathbb{Z}/\ell\mathbb{Z})^2$ if and only if $p$ splits completely in $K_\ell$. As a consequence, $\mathbb{E}(\mathbb{F}_p)$ is cyclic if and only if for all primes $\ell \neq p$,*

$$p \text{ does not split completely in } K_\ell. \tag{4.1}$$

*Remark.* If $E(\mathbb{F}_p)$ contains $(\mathbb{Z}/\ell\mathbb{Z})^2$, then $\ell^2 \mid \#E(\mathbb{F}_p) \leq (\sqrt{p}+1)^2$, and so it suffices to test (4.1) for

$$\ell \leq \sqrt{p}+1. \tag{4.2}$$

If we assume the GRH, then the following theorem of Lagarias and Odlyzko [LO77] gives a satisfactory estimate for the frequency with which primes split completely in $K_\ell$. We state the result incorporating a small improvement by Serre [Ser81, §2.4].

**Proposition 4.2** (Effective Chebotarev theorem, on GRH)**.** *Let $K$ be a finite Galois extension of $\mathbb{Q}$, and let $\mathcal{C}$ be a conjugacy class of* $\operatorname{Gal}(K/\mathbb{Q})$. *The number of unramified primes $p \leq x$ with $\left[\frac{K/\mathbb{Q}}{p}\right] = \mathcal{C}$ is given by*

$$\frac{\#\mathcal{C}}{[K:\mathbb{Q}]}\operatorname{Li}(x) + O\left(\#\mathcal{C}\cdot x^{1/2}\left(\frac{\log|\Delta_K|}{[K:\mathbb{Q}]} + \log x\right)\right),$$

*for all $x \geq 2$. Here the $O$-constant is absolute.*

*Remark.* To estimate the $O$-term, we will use the following estimate valid for any Galois extension $K/\mathbb{Q}$ (see [Ser81, Proposition 6]):

$$\frac{1}{[K:\mathbb{Q}]}\log|\Delta_K| \leq \log\ [K:\mathbb{Q}] + \sum_{p\mid\Delta_K}\log p. \tag{4.3}$$

To apply (4.3), we need to understand which primes ramify in $K_\ell$. The following result can be derived from a criterion of Néron–Ogg–Shafarevich [Sil09, Theorem 7.1, p. 201].

**Lemma 4.3.** *Let $E/\mathbb{Q}$ be an elliptic curve. Every prime that ramifies in $K_\ell$ divides $\ell\cdot\Delta_E$.*

We will find bounded gaps among primes $p$ produced by certain linear functions, with coefficients chosen to give $p$ a "leg up" in terms of $E(\mathbb{F}_p)$ being cyclic. To build these functions, we need the following analogue of Lemma 2.2.

**Lemma 4.4.** *Let $M$ be either a quadratic or abelian cubic extension of $\mathbb{Q}$. Let $f = \mathfrak{f}(M/\mathbb{Q})$, and let $v = 2^4 3^3 \prod_{\ell \mid f,\ \ell > 3} \ell$. One can select an integer $u$ coprime to $v$ so that both of the following hold:*

(1) *For every prime $p \equiv u \pmod{v}$, $p$ is inert in $M$.*

(2) *If $T$ is the largest power of $2$ dividing $u-1$, then $T \in \{2, 4, 8\}$, and $\gcd(\frac{u-1}{T}, v) = 1$.*

*Proof.* We make free use of the correspondence between abelian extensions of $\mathbb{Q}$ and groups of primitive Dirichlet characters, as reviewed in [Was97, Chapter 3].

If $M/\mathbb{Q}$ is quadratic, then $f$ is the absolute value of a fundamental discriminant, whereas if $M/\mathbb{Q}$ is abelian cubic, then

$$f = 9q_1 \cdots q_k \quad \text{or} \quad f = q_1 \cdots q_k, \quad \text{for distinct primes} \quad q_i \equiv 1 \pmod{6}.$$

Thus, $2^4 \nmid f$, $3^3 \nmid f$, and every prime $\ell > 3$ that divides $f$ appears to the first power only. Let $H$ be the subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ that fixes $M$. We identify $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ with $(\mathbb{Z}/f\mathbb{Z})^\times$. Note that $H$ has index $[M : \mathbb{Q}] > 1$. Since $M$ is cyclic of prime degree, an unramified prime $p$ either remains inert or splits completely, the latter holding exactly when $p \bmod f \in H$.

Choose an integer $u_0$ with

$$\gcd(u_0, f) = 1, \quad u_0 \bmod f \notin H, \quad \text{and} \quad u_0 \equiv 2 \pmod{3}. \tag{4.4}$$

This is clearly possible if $3 \nmid f$. If $3 \mid f$, we argue by contradiction: If there is no such $u_0$, then $\#H > \#\{1 \le h \le f : \gcd(h, f) = 1, h \equiv 2 \pmod{3}\} = \frac{1}{2}\varphi(f)$, where the inequality is strict since $1 \bmod f \in H$. But then $H = \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$, a contradiction.

We can also assume that

$$u_0 \equiv 1 \pmod{2}. \tag{4.5}$$

Indeed, if $f$ is even, this condition is automatic, whereas if $f$ is odd but $u_0$ is even, we can replace $u_0$ by $u_0 + 3f$. Finally, we can assume that

$$16 \nmid u_0 - 1, \tag{4.6}$$

by replacing $u_0$ with $u_0 + \mathrm{lcm}[24, f]$ if necessary.

If $M/\mathbb{Q}$ is quadratic, then for each prime $\ell > 3$ dividing $f$, put

$$u_\ell = \begin{cases} u_0 & \text{if } \ell \nmid u_0 - 1, \\ 4u_0 & \text{otherwise.} \end{cases}$$

Then $\ell \nmid u_\ell - 1$. If $M/\mathbb{Q}$ is abelian cubic, then for each prime $\ell > 3$ dividing $f$, put

$$u_\ell = \begin{cases} u_0 & \text{if } \ell \nmid u_0 - 1, \\ -8u_0 & \text{otherwise.} \end{cases}$$

In this case, we again have that $\ell \nmid u_\ell - 1$. Finally, select $u$ so that

$$u \equiv u_0 \pmod{2^4 \cdot 3^3} \quad \text{and} \quad u \equiv u_\ell \pmod{\ell}\ \forall \ell \mid f \text{ with } \ell > 3.$$

This puts $u$ in a well-defined coprime residue class modulo $v$.

We now check (1) and (2). In the case when $M/\mathbb{Q}$ is quadratic, $u \equiv u_0 g^2 \pmod{f}$ for some integer $g$. Since $H$ has index 2, $g^2 \bmod f \in H$. Since $u_0 \bmod f \notin H$, we find that $u \bmod f \notin H$. So if $p \equiv u \pmod{v}$, then $p \bmod f \notin H$ (notice $f \mid v$) and so $p$ is inert in $M$. An analogous argument works when $M/\mathbb{Q}$ is abelian cubic; in that case, $H$ has index 3 and $u \equiv u_0 g^3 \pmod{f}$ for some $g$. This completes the verification of (1). Since $u \equiv u_0 \pmod{16}$, (4.5) and (4.6) yield $T \in \{2, 4, 8\}$. Since $u \equiv u_0 \pmod{3}$, (4.4) shows that $3 \nmid u - 1$. For each prime $\ell > 3$ dividing $v$, our choices of $u_\ell$ ensure that $\ell \nmid u - 1$. Hence, $\gcd(\frac{u-1}{T}, v) = 1$, which completes the proof of (2). □

By imitating the deduction of Lemma 2.3 from Lemma 2.2, we obtain the following consequence of Lemma 4.4.

**Lemma 4.5.** *Let $M$ be either a quadratic or abelian cubic extension of $\mathbb{Q}$. Let $u$ and $v$ be chosen as in Lemma 4.4. Let $\kappa$ be a natural number. There are integers $a_1 < \cdots < a_\kappa$, each congruent to $u$ mod $v$, for which the $2\kappa$ linear functions*

$$\begin{aligned} L_1(n) &= vn + a_1, & \ldots,\quad L_\kappa(n) &= vn + a_\kappa, \\ \tilde{L}_1(n) &= \frac{v}{T}n + \frac{a_1 - 1}{T}, & \ldots,\quad \tilde{L}_\kappa(n) &= \frac{v}{T}n + \frac{a_\kappa - 1}{T} \end{aligned}$$

*make up an admissible family. Moreover, we can select the $a_i$ in such a way that*

$$a_\kappa - a_1 \leq v \cdot (2\kappa)^{C_5}.$$

# 5 Proof of Theorem 1.2

## 5.1 The GRH case

By assumption, $K_2 \neq \mathbb{Q}$. Since $K_2$ is the splitting field of a cubic polynomial, it has a subfield $M$ that is either quadratic or abelian cubic over $\mathbb{Q}$. Let $\kappa = \lceil \exp(C_6 m) \rceil$, where $C_6$ is a large absolute constant. Let $k = 2\kappa$, and let $\mathscr{L}$ consist of the linear functions $L_1, \ldots, L_\kappa$, $\tilde{L}_1, \ldots, \tilde{L}_\kappa$ constructed in Lemma 4.5. Recall that each $L_i$ has leading coefficient $v = 2^4 3^3 \prod_{\ell \mid f,\ \ell > 3} \ell$, where $f$ is the conductor of $M$. If $\ell \mid f$, then $\ell \mid \Delta_{K_2}$, and so $\ell = 2$ or $\ell$ is a prime of bad reduction. Consequently,

$$v \mid 2^4 3^3 \cdot \operatorname{rad}(\Delta_E).$$

We warn the reader of the following innocuous abuse of notation: If $L = L_i$, we will write $\tilde{L}$ for $\tilde{L}_i$.

Assume $x$ is large. We will show that if $c > 0$ is a sufficiently small absolute constant, then with positive probability, an $n \in \mathscr{A}(x)$ satisfies all of

(i) at least $m$ of $L_1(n), \ldots, L_\kappa(n)$ are prime,

(ii) $p^-(L_i(n)) \geq x^{\frac{c}{k^3 \log k}}$ and $p^-(\tilde{L}_i(n)) \geq x^{\frac{c}{k^3 \log k}}$ for all $i = 1, \ldots, \kappa$,

(iii) all integers in the interval $[L_1(n), L_\kappa(n)]$ that are not one of the $L_i(n)$ are composite,

(iv) if $p = L(n)$ is prime with $L \in \{L_1, \ldots, L_\kappa\}$, then $p$ is inert in every $K_\ell$ with $\ell > x^{1/3}$ and $\ell \neq p$,

(v) if $p = L(n)$ is prime with $L \in \{L_1, \ldots, L_\kappa\}$, then $E(\mathbb{F}_p)$ is cyclic.

If all of (i)–(v) hold for $n$, then the set of primes $p \in [L_1(n), L_\kappa(n)]$ has at least $m$ elements, all of these have $E(\mathbb{F}_p)$ cyclic, and the gap between the largest and smallest is at most

$$L_\kappa(n) - L_1(n) \leq v \cdot (2\kappa)^{C_5} \leq \operatorname{rad}(\Delta_E) \cdot \exp(C_7 m);$$

the GRH half of Theorem 1.2 follows.

For the sake of readability, in the remainder of the proof we suppress the dependence of implied constants on $E$.

To handle (i)–(iii), we proceed as in the proof of Theorem 1.1. Arguments given there show that if we fix $C_6$ sufficiently large and $c$ sufficiently small, then (i) and (ii) hold simultaneously with probability at least $\frac{1}{2}\kappa^{-1}$, while (iii) fails with probability $o(1)$, as $x \to \infty$.

Now suppose that (i)–(iii) hold for $n$ but that (iv) fails. We will show that this occurs with probability $o(1)$. Observe that for each $n \in [x, 2x)$ and each $L \in \{L_1, \ldots, L_\kappa\}$, the integer $L(n)$ is smaller than $3vx$.

We start by bounding the number of $p \leq 3vx$ which split completely in $K_\ell$ for some $\ell > x^{1/3}$ with $\ell \neq p$. In that case, $(\mathbb{Z}/\ell\mathbb{Z})^2$ sits inside $E(\mathbb{F}_p)$, and so

$$\ell^2 \mid p + 1 - a_p. \tag{5.1}$$

Since $\mathbb{Q}(\zeta_l) \subset K_\ell$ (by properties of the Weil pairing [Sil09, Corollary 8.1.1]),

$$\ell \mid p - 1. \tag{5.2}$$

Comparing (5.1) and (5.2) shows that $\ell \mid 2 - a_p$. If $a_p \neq 2$, then

$$0 < |2 - a_p| < 2 + 2\sqrt{3vx} < x^{2/3} < \ell^2;$$

hence $\ell$ is uniquely determined by $a = a_p$, as the largest prime dividing $|2 - a|$. Fixing $a \neq 2$, (5.1) shows that the number of corresponding $p \leq 3vx$ is $\ll \frac{x}{\ell^2} + 1 \ll x^{1/3}$. By the Hasse bound, $|a| \ll \sqrt{x}$, and so summing on the possible values of $a$ shows that $O(x^{5/6})$ values of $p$ arise in this way. On the other hand, when $a = 2$, (4.2) and (5.1) imply that the number of corresponding $p$ is

$$\ll \sum_{\ell \in (x^{1/3}, \sqrt{3vx}+1]} \left(\frac{x}{\ell^2} + 1\right) \ll x^{2/3}.$$

So there are a total of $O(x^{5/6})$ of these primes $p$.

Since (i)–(iii) hold while (iv) fails, there is an $L \in \{L_1, \dots, L_\kappa\}$ such that $p = L(n)$ is among the primes counted in the previous paragraph. There are $O_m(1)$ possibilities for $L$, and so $O_m(x^{5/6})$ possibilities for $n \in \mathscr{A}(x)$. From (ii) and Proposition 3.1(1), the probability mass at each such $n$ is $O_m(x^{-1}(\log x)^k)$. So the probability that (i)–(iii) hold but (iv) fails is $O_m(x^{-1/6}(\log x)^k)$, which is $o(1)$ as $x \to \infty$.

To complete the proof, we show the probability (i)–(iv) hold but (v) fails is also $o(1)$.

Suppose $p = L(n)$ is prime, with $L \in \{L_1, \dots, L_\kappa\}$, but that $E(\mathbb{F}_p)$ is not cyclic. From Lemma 4.4(1) and our choice of $\mathscr{L}$, $p$ is inert in $M$, and a fortiori does not split completely in $K_2$. So $\mathbb{E}(\mathbb{F}_p)$ must split completely in $K_\ell$ for some $\ell > 2$. Since $\ell \mid p - 1 = T \cdot \tilde{L}(n)$, (ii) and (iv) imply that

$$x^{c/(k^3 \log k)} \le \ell \le x^{1/3}. \tag{5.3}$$

We now count how many $p \le 3vx$ split completely in $K_\ell$ for some $\ell$ in the range (5.3) with $\ell \ne p$. Making the same appeal to Proposition 3.1(1) we saw earlier in the proof, it is enough to prove that the number of these $p$ is

$$\ll x^{1-\frac{c}{k^3 \log k}} + x^{5/6} \log x. \tag{5.4}$$

We invoke GRH. By effective Chebotarev, the number of $p \le 3vx$ splitting completely in $K_\ell$ is

$$\ll \frac{x}{[K_\ell : \mathbb{Q}] \log x} + x^{1/2} \left( \log x + \frac{1}{[K_\ell : \mathbb{Q}]} \log |\Delta_{K_\ell}| \right).$$

Since every prime dividing $\Delta_{K_\ell}$ divides $\ell \cdot \Delta_E$, (4.3) shows that this upper bound is

$$\ll \frac{x}{[K_\ell : \mathbb{Q}] \log x} + x^{1/2} \log([K_\ell : \mathbb{Q}] \cdot \ell x). \tag{5.5}$$

If $E$ has CM, then for all large primes $\ell$, the degree of $K_\ell/\mathbb{Q}$ is either $2(\ell-1)^2$ or $2(\ell^2-1)$, according to whether or not $\ell$ splits in the CM field. In particular, $[K_\ell : \mathbb{Q}] \asymp \ell^2$. If the non-CM case, we have $[K_\ell : \mathbb{Q}] = \#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \asymp \ell^4$ for all large primes $\ell$. (These results are due to Serre [Ser72]; see [CCS13, Theorem 18] for a detailed discussion of the CM case.) Thus, the sum of (5.5) over the range (5.3) is

$$\ll \frac{x}{\log x} \sum \frac{1}{\ell^2} + x^{1/2} \log x \sum_\ell 1 \ll x^{1-\frac{c}{k^3 \log k}} + x^{5/6} \log x,$$

which agrees with (5.4). This completes the proof in the GRH case.

## 5.2 Unconditional proof in the CM case

As already mentioned in the introduction, we will deal entirely with supersingular primes in this part of the proof.

Suppose that $p \geq 5$ is supersingular but that $E(\mathbb{F}_p)$ is not cyclic. Choose an $\ell \neq p$ for which $p$ splits completely in $K_\ell$. Then $\ell^2 \mid \#E(\mathbb{F}_p) = p+1$ and $\ell \mid p-1$, forcing $\ell = 2$. Consequently, $p$ splits in the quadratic or abelian cubic subfield $M$ of $K_2$.

Let $F$ be the CM field. We look for primes $p$ of good reduction that are inert in $F$ — guaranteeing that $p$ is supersingular — and inert in $M$. If $F = M$, it is clear that there are infinitely many such primes; otherwise, this follows from the linear disjointness of $F$ and $M$ over $\mathbb{Q}$. Since $F/\mathbb{Q}$ and $M/\mathbb{Q}$ are abelian, the set of such $p$ contains all primes in a certain arithmetic progression modulo $q := f_1 f_2$, where $f_1 = \mathfrak{f}(F/\mathbb{Q})$ and $f_2 = \mathfrak{f}(M/\mathbb{Q})$. Since $E$ is defined over $\mathbb{Q}$, its CM field $F$ must be one of the nine imaginary quadratic fields of class number 1 (see, e.g., Serre's chapter in [CF86]), and so $f_1 \ll 1$. On the other hand, since every odd prime dividing $f_2$ divides $\Delta_E$, and since $f_2$ is squarefree apart from bounded powers of 2 and 3, the modulus $q = f_1 f_2 \ll f_2 \ll \mathrm{rad}(\Delta_E)$.

Corollary 3 of [BFTB] asserts that for any fixed coprime progression mod $q$, there are infinitely many tuples of $m$ consecutive primes $p_1 < p_2 < \cdots < p_m$ with $p_m - p_1 \ll_{q,m} 1$. In fact, it is straightforward to modify their argument to get an upper bound of $q \exp(O(m))$ (cf. [Tho14, Theorem 2(2)] when $m = 2$). The theorem follows.

*Remark.* In the non-CM case, we do not have an unconditional bounded gaps result for primes $p$ with $E(\mathbb{F}_p)$ cyclic. But if 'cyclic' is replaced by 'has an element of order $> p^{3/4-\epsilon}$', then such a result follows quickly from work of Duke [Duk03].

Let $E/\mathbb{Q}$ be any elliptic curve. (No assumption on the rational torsion is needed here.) For each prime $p$ of good reduction, write $E(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}$ for natural numbers $d_p$ and $e_p$ where $d_p \mid e_p$. Clearly, $d_p^2 \leq \#E(\mathbb{F}_p) \leq (\sqrt{p}+1)^2$, so that $d_p \leq 2\sqrt{p}$.

Duke shows (see [Duk03, eq. (8)]) that for each $n \leq 2\sqrt{x}$, the number of $p \leq x$ for which $n \mid d_p$ is $O(x^{3/2}n^{-3})$. A fortiori, the same bound holds for how often $d_p = n$. Consequently, the number of $p \leq x$ with $d_p > x^{1/4+\epsilon/2}$ is $O(x^{1-\epsilon})$. Whenever $d_p \leq x^{1/4+\epsilon/2}$, the group $E(\mathbb{F}_p)$ has an element of order

$$e_p \geq \frac{\#E(\mathbb{F}_p)}{x^{1/4+\epsilon/2}} \gg p x^{-\frac{1}{4}-\frac{\epsilon}{2}}.$$

Summing dyadically, we conclude that $E(\mathbb{F}_p)$ has an element of order $> p^{\frac{3}{4}-\epsilon}$ for all but $O_\epsilon(x^{1-\epsilon})$ primes $p \leq x$. This exceptional set is so sparse that it follows immediately from Maynard's lower bound results (see [May14, Theorem 3.1]) that the set of nonexceptional $p$ has bounded gaps. More precisely, this set contains arbitrarily long runs of primes contained in bounded length intervals.

# 6 Proof of Theorem 1.3

We begin by stating a variant of Proposition 3.1 for sets of primes described by Chebotarev conditions.

**Proposition 6.1.** *Let $K/\mathbb{Q}$ be a Galois extension, and let $\mathcal{C}$ be a fixed conjugacy class of* $\mathrm{Gal}(K/\mathbb{Q})$. *Let*

$$\mathscr{P}(\mathcal{C}) = \{p : p \nmid \Delta_K, \left[\frac{K/\mathbb{Q}}{p}\right] = \mathcal{C}\}.$$

*Suppose $a_1 < a_2 < \cdots < a_\kappa$ are odd integers for which the $k = 2\kappa$ linear functions*

$$\begin{gathered} L_1(n) = 2n + a_1, \quad L_2(n) = 2n + a_2, \quad \ldots, \quad L_\kappa(n) = 2n + a_\kappa, \\ \tilde{L}_1(n) = n + \frac{a_1 - 1}{2}, \quad \tilde{L}_2(n) = n + \frac{a_2 - 1}{2}, \quad \ldots, \quad \tilde{L}_\kappa(n) = n + \frac{a_\kappa - 1}{2} \end{gathered} \tag{6.1}$$

*form an admissible collection; call this collection $\mathscr{L}$. Suppose that $x$ is sufficiently large, $x > x_0(K, \mathscr{L})$. There is a probability measure on $\mathscr{A}(x) = \{n \in \mathbb{Z} : x \le n < 2x\}$ with all of the following properties:*

(1) *The probability mass at any single $n \in \mathscr{A}(x)$ is*

$$\ll_K x^{-1}(\log x)^k \left( \prod_{i=1}^{k} \prod_{\substack{p \mid L_i(n) \\ p \nmid 2\Delta_K}} 4 \right) \exp(O(k \log k)).$$

(2) *For each $L \in \mathscr{L}$,*

$$\mathbb{P}(L(n) \text{ belongs to } \mathscr{P}(\mathcal{C})) \gg_K \frac{\log k}{k}.$$

(3) *Let $\rho \in [k\frac{(\log\log x)^2}{\log x}, \frac{1}{30[K:\mathbb{Q}]}]$. For each $L \in \mathscr{L}$,*

$$\mathbb{E}\Bigg[ \sum_{\substack{p \mid L(n) \\ p \le x^\rho,\ p \nmid 2\Delta_K}} 1 \Bigg] \ll \rho^2 k^4 (\log k)^2.$$

*The implied constant in (3) is absolute.*

*Proof (sketch).* The main technical input is supplied by a variant of the Bombieri–Vinogradov theorem due to Murty and Murty [MM87], which asserts that $\mathscr{P}(\mathcal{C})$ has level of distribution $\theta$ for any fixed

$$\theta < \min\{\frac{1}{2}, \frac{2}{[K:\mathbb{Q}]}\};$$

here the moduli of the arithmetic progressions are assumed coprime to $\Delta_K$. We now argue as in the proof of Proposition 3.1. Specifically, the Murty–Murty theorem allows us to apply [May14, Proposition 6.1] with $\mathscr{A} = \mathbb{N}$, $\mathscr{L}$ as given, $\mathscr{P} = \mathscr{P}(\mathcal{C}, K)$, $B = 2\Delta_K$, $\theta = \min\{\frac{1}{3}, \frac{1}{[K:\mathbb{Q}]}\}$, and $\alpha = 1$. Defining the probability mass at $n$ as $w(n)/\sum_{n \in \mathscr{A}(x)} w(n)$, the result follows. (For similar applications of the Murty–Murty theorem, see [Tho14] and [May14, Theorem 3.5].) □

The proof of Theorem 1.3 also uses the following criterion, which is contained in work of Cojocaru [Coj03, Lemmas 2.2 and 2.3].

**Lemma 6.2.** *Suppose that $E/\mathbb{Q}$ has CM by an order in the imaginary quadratic field $F$. Let $p$ be a prime of good ordinary reduction, and let $\ell$ be a prime with $\ell \neq p$. If $p$ splits completely in $K_\ell$, then there is a $\pi \in \mathbb{Z}_F$ with $\pi \equiv 1 \pmod{\ell}$ and $N(\pi) = p$.*

*Proof of Theorem 1.3.* We begin by specifying the parameters needed for our application of Proposition 6.1.

Let $F$ be the CM field of $E$. Let $\mathscr{Q}$ be the set of primes dividing $2\Delta_F\Delta_E$, and let $K$ be the compositum of $F$ and all of the fields $K_\ell := \mathbb{Q}(E[\ell])$ for $\ell \in \mathscr{Q}$. Then $K/\mathbb{Q}$ is Galois and every prime dividing $\Delta_K$ belongs to $\mathscr{Q}$. Choose a conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(K/\mathbb{Q})$ where every prime $p \in \mathscr{P}(\mathcal{C})$ is such that

- $p$ splits in $F$,
- $p$ does not split completely in any of the fields $K_\ell$ with $\ell \in \mathscr{Q}$.

Any large prime $p$ of ordinary reduction for which $E(\mathbb{F}_p)$ is cyclic satisfies both of these conditions, and so such a $\mathcal{C}$ must exist.

Let $\kappa = \lceil \exp(C_K m) \rceil$, where $C_K$ is a sufficiently large constant depending on $K$. Mimicking the proof of Lemma 2.3, we can choose odd integers $a_1 < \cdots < a_\kappa$ for which (6.1) is admissible, with $a_\kappa - a_1 \le (2\kappa)^{C_8}$. Then

$$a_\kappa - a_1 \ll \exp(O_E(m)). \tag{6.2}$$

We are now in a position to apply Proposition 6.1. If $C_K$ is sufficiently large and $c$ is sufficiently small (both allowed to depend on $K$), then an $n \in \mathscr{A}(x)$ satisfies both of the following conditions with probability $\gg_m 1$:

(i) at least $m$ of $L_1(n), \ldots, L_\kappa(n)$ belong to $\mathscr{P}(\mathcal{C})$,

(ii) whenever a prime $\ell \le x^{c/(k^3 \log k)}$ divides $\prod_{i=1}^{\kappa} L_i(n)\tilde{L}_i(n)$, $\ell$ also divides $2\Delta_K$.

Indeed, this follows from arguments seen already in the proofs of Theorems 1.1 and 1.2, the only difference being that we appeal to Proposition 6.1 instead of Proposition 3.1. We now introduce the statement

(iii) Whenever $p = L(n) \in \mathscr{P}(\mathcal{C})$, with $L \in \{L_1, \ldots, L_\kappa\}$, the group $E(\mathbb{F}_p)$ is cyclic.

We will show that the probability (i) and (ii) hold but (iii) fails is $o(1)$, as $x \to \infty$, so that (i)–(iii) hold with positive probability for all large $x$. This will complete the proof; indeed, if $n \in \mathscr{A}(x)$ satisfies (i)–(iii), and $p_1 < p_2 < \cdots < p_m$ are primes from $\mathscr{P}(\mathcal{C})$ drawn from $\{L_1(n), \ldots, L_\kappa(n)\}$, then the claimed bound on $p_m - p_1$ follows from (6.2), while the fact that each of the primes is of good ordinary reduction follows from the choice of $\mathcal{C}$.

Suppose (i) and (ii) hold and that $p = L_i(n) \in \mathscr{P}(\mathcal{C})$, where $i \in \{1, 2, \ldots, \kappa\}$. As we have just remarked, $p$ is a prime of good ordinary reduction. If $E(\mathbb{F}_p)$ is not cyclic, then $p$ spits completely in $K_\ell$ for some $\ell \neq p$. Then $\ell \mid p - 1 = 2\tilde{L}_i(n)$, so that either $\ell \mid 2\Delta_K$ or $\ell \ge x^{c/(k^3 \log k)}$. But if $\ell \mid 2\Delta_K$, then $\ell \in \mathscr{Q}$, and so the choice of $\mathcal{C}$ guarantees that

$p$ does not split completely in $K_\ell$. So it must be that $\ell \geq x^{c/(k^3 \log k)}$. Since $p \leq 5x$ for large $x$, we also have that $\ell \leq \sqrt{5x}+1$, after recalling (4.2).

Let us count primes $p \leq 5x$ of good ordinary reduction that split completely in $K_\ell$ for some $\ell \neq p$ with

$$x^{c/(k^3 \log k)} \leq \ell \leq \sqrt{5x}+1. \tag{6.3}$$

From Lemma 6.2, there is a $\pi_p \in \mathbb{Z}_F$ with $\pi_p \equiv 1 \pmod{\ell}$ and $N(\pi_p) = p$. The number of $\pi \in \mathbb{Z}_F$ with $\pi \equiv 1 \pmod{\ell}$ and $N(\pi) \leq 5x$ is $O(\frac{x}{\ell^2}+1)$, by an elementary lattice point counting argument (e.g., see [Mur83, Lemma 5] or [Coj03, Lemma 2.6]). Summing on $\ell$ in the range (6.3) shows that the number of $p$ in question is

$$\ll x^{1-\frac{c}{k^3 \log k}} + x^{1/2}.$$

If $n$ satisfies (i) and (ii), Proposition 6.1(1) shows that the probability mass at $n$ is $O_{K,m}(x^{-1}(\log x)^k)$. Consequently, the probability that $L(n)$ is one of the primes counted in the preceding paragraph is $o(1)$, as $x \to \infty$. □

## Acknowledgments

We are indebted to Pete L. Clark for helpful conversations on the theory of elliptic curves. This research began while the second author enjoyed a very pleasant visit to Brigham Young University. He thanks the BYU mathematics department for their hospitality and the NSF for their support under award DMS-1402268.

# References

[AM10] A. Akbary and V. K. Murty, *An analogue of the Siegel-Walfisz theorem for the cyclicity of CM elliptic curves mod p*, Indian J. Pure Appl. Math. **41** (2010), 25–37.

[BFTB] W. D. Banks, T. Freiberg, and C. L. Turnage-Butterbaugh, *Consecutive primes in tuples*, submitted. Preprint version available online as `arXiv:1311.7003 [math.NT]`.

[CCS13] P. L. Clark, B. Cook, and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), 447–479.

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1986, reprint of the 1967 original.

[CM04] A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. **330** (2004), 601–625.

[Coj03] A. C. Cojocaru, *Cyclicity of CM elliptic curves modulo $p$*, Trans. Amer. Math. Soc. **355** (2003), 2651–2662 (electronic).

[Duk03] W. Duke, *Almost all reductions modulo $p$ of an elliptic curve have a large exponent*, C. R. Math. Acad. Sci. Paris **337** (2003), 689–692.

[GM84] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), 127–130.

[GM90] ______, *Cyclicity and generation of points mod $p$ on elliptic curves*, Invent. Math. **101** (1990), 225–235.

[GMM87] R. Gupta, M. R. Murty, and V. K. Murty, *The Euclidean algorithm for $S$-integers*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 189–201.

[HB86] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), 27–38.

[Hoo67] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[Lan87] S. Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987.

[LO77] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: $L$-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.

[LP14] H. Li and H. Pan, *Bounded gaps between primes of the special form*, preprint available as `arXiv:1403.4527 [math.NT]`, 2014.

[May14] J. Maynard, *Dense clusters of primes in subsets*, preprint available as `arXiv:1405.2593 [math.NT]`, 2014.

[MM87] M. R. Murty and V. K. Murty, *A variant of the Bombieri-Vinogradov theorem*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 243–272.

[Mor12] P. Moree, *Artin's primitive root conjecture—a survey*, Integers **12** (2012), 1305–1416.

[MS87] M. R. Murty and S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. **30** (1987), 80–85.

[Mur83] M. R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), 147–168.

[Pin10] J. Pintz, *Are there arbitrarily long arithmetic progressions in the sequence of twin primes?*, An irregular mind, Bolyai Soc. Math. Stud., vol. 21, János Bolyai Math. Soc., Budapest, 2010, pp. 525–559.

[Pol14] P. Pollack, *Bounded gaps between primes with a given primitive root*, Algebra Number Theory (2014), to appear. Preprint available as `arXiv:1404.4007 [math.NT]`.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Ser78] ———, *Résumé des cours de l'année scolaire, 1977–1978*, Annuaire du Collège de France (1978), 67–70.

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Tho14] J. Thorner, *Bounded gaps between primes in Chebotarev sets*, Research in the Mathematical Sciences **1** (2014), article #4, 16 pages.

[Was97] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.