Centre de Recherches Mathématiques
CRM Proceedings and Lecture Notes
Volume ??, 2004

# Questions About the Reductions Modulo Primes of an Elliptic Curve

Alina Carmen Cojocaru

## 1. Introduction

This is largely a survey paper in which we discuss new and old problems about the reductions $E_p$ modulo primes $p$ of a fixed elliptic curve $E$ defined over the field of rational numbers. We investigate, in particular, how the "noncyclic" part of the group of points of $E_p$ is distributed, thus making progress toward a conjecture of R. Takeuchi. The new result is Theorem 2 of Section 3.

Many interesting questions that resemble classical problems in number theory, such as Artin's primitive root conjecture, the twin prime conjecture, the Buniakowski–Schinzel hypothesis, can be formulated using the group of points of the reduction modulo a prime of a fixed elliptic curve defined over a global field, say over $\mathbb{Q}$. Before discussing these questions in detail, let us recall the basic definitions and properties of elliptic curves. For precise references or more detailed facts, the reader is referred to [**33, 34**].

An *elliptic curve $E$ defined over* $\mathbb{Q}$ is the locus of an equation of the form

$$E : y^2 = x^3 + ax + b \tag{1.1}$$

(where $a, b \in \mathbb{Z}$ are such that the discriminant $-16(4a^3+27b^2)$ is nonzero), together with a point at infinity $\mathcal{O}$, given in projective coordinates by [0:1:0].

When doing arithmetic over $E$ we are usually concerned with rational solutions of (1.1) or solutions of congruences modulo primes defined by (1.1). We will briefly consider both these aspects.

Let $E(\mathbb{Q})$ be the set of rational points on $E$ together with the point at infinity. Remarkably, we can define an addition law on $E(\mathbb{Q})$ by the simple geometric rule: the sum of three points equals zero (the point at infinity) if and only if the points lie on the same line. With respect to this law, $E(\mathbb{Q})$ becomes an abelian group and, moreover, by a famous result of Mordell published in 1922, a finitely generated abelian group. Therefore $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$, where $r$ is some nonnegative integer called *the* (*arithmetic*) *rank of $E$ over* $\mathbb{Q}$, and $E(\mathbb{Q})_{\text{tors}}$ is the torsion part of $E(\mathbb{Q})$.

2000 *Mathematics Subject Classification.* ??

This research was supported by an NSERC postdoctoral fellowship.

This is the final form of the paper.

We remark that we can talk about an elliptic curve $E$ defined over any field $K$ (for the purpose of this paper, $K$ will have characteristic $\neq 2, 3$). Again, we can define an abelian group structure on the set $E(K)$ of $K$-rational points of $E$ (N.B. $E(K)$ is a finitely generated abelian group if $K$ is a global field). In particular, if $E$ is defined over $\mathbb{Q}$, we can also talk about the group $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.

From now on let $E$ be a fixed elliptic curve defined over $\mathbb{Q}$. There are some natural maps that we can define on $E(\overline{\mathbb{Q}})$. For each $n \in \mathbb{Z}$, let us consider the multiplication by $n$ map defined on $E(\overline{\mathbb{Q}})$. These are group homomorphisms and also morphisms of curves, called isogenies of $E$ over $\overline{\mathbb{Q}}$. If we let $\operatorname{End}_{\overline{\mathbb{Q}}}(E)$ denote the ring of all isogenies of $E$ over $\overline{\mathbb{Q}}$, then we obtain a canonical embedding $\mathbb{Z} \leq \operatorname{End}_{\overline{\mathbb{Q}}}(E)$, which, in "most of the cases," is in fact a ring isomorphism. If it is an isomorphism, then we say that $E$ is *without complex multiplication* (non-CM). If the embedding is strict, then we obtain that $\operatorname{End}_{\overline{\mathbb{Q}}}(E)$ is an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ of class number 1 (hence $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$, by a famous 1965's result of Heegner–Stark–Baker). In this situation we say that $E$ is *with complex multiplication* (CM) and that $\mathbb{Q}(\sqrt{-D})$ is its CM field.

The CM and non-CM situations are very different, as can be seen, for example, from the following. For an arbitrary positive integer $k$ we let $E[k]$ be *the group of $k$-division points of $E$*, that is, the points of $E(\overline{\mathbb{Q}})$ annihilated by $k$. We know that, as $\mathbb{Z}$-modules, $E[k] \simeq \mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/k\mathbb{Z}$. If we adjoin to $\mathbb{Q}$ the $x$- and $y$-coordinates of the $k$-division points of $E$, then we obtain a finite Galois extension of $\mathbb{Q}$ which is unramified outside $kN$, with $N$ denoting the conductor of $E$ in the sense explained below, and which contains the cyclotomic field $\mathbb{Q}(\zeta_k)$. We denote this extension by $\mathbb{Q}(E[k])$ and call it *the $k$-division field of $E$*. We can then define a natural representation

$$\phi_k\colon \operatorname{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{Z}/k\mathbb{Z}),$$

called *the Galois representation associated to $E[k]$*, which is easily seen to be injective. Is this representation surjective? In 1941, M. Deuring showed that in the case of a CM elliptic curve $E$, $\phi_k$ is not surjective for any integer $k > 2$. Moreover, in this situation we have that

$$\phi(k)^2 \leq [\mathbb{Q}(E[k]){:}\mathbb{Q}] \leq k^2 \tag{1.2}$$

for any $k > 2$, where $\phi(\cdot)$ is the Euler function. By contrast, in 1972 J.-P. Serre showed that in the case of a non-CM elliptic curve $E$, there exists a positive integer $A(E)$, depending on $E$, such that $\phi_k$ is surjective for any positive integer $k$ coprime to $A(E)$. Therefore for such $E$ and $k$ we have

$$[\mathbb{Q}(E[k]){:}\mathbb{Q}] = \#\operatorname{GL}_2(\mathbb{Z}/k\mathbb{Z}) = k^4 \prod_{q|k}\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right), \tag{1.3}$$

where the product is over prime divisors $q$ of $k$.

Now let us consider the reduction $E_p$ of $E$ modulo a prime $p > 3$ :

$$E_p : y^2 \equiv x^3 + ax + b \pmod{p}.$$

This is a (not necessarily smooth) curve defined over $\mathbb{F}_p$. There is an arithmetic invariant $N = N_E \in \mathbb{Z}$ of the elliptic curve $E$, called *the conductor of $E$*, which gives us precise information about the reduction of $E$ modulo each prime $p$. One of the properties of this invariant is that $E_p$ is smooth if and only if $p \nmid N$. Clearly, $N$ is a divisor of the discriminant of the polynomial in $x$ defining $E$.

From now on we will consider only primes $p \nmid N$, called *primes of good reduction for* $E$. For such a $p$, $E_p$ is an elliptic curve defined over $\mathbb{F}_p$. This paper is concerned with *questions about the group* $E_p(\mathbb{F}_p)$*, as* $p$ *varies.* The most basic questions about this group are to find its cardinality and to determine its structure.

The Riemann Hypothesis for $E_p$, proved by H. Hasse in 1933, asserts that if we write

$$\#E_p(\mathbb{F}_p) = p + 1 - a_p$$

for some $a_p \in \mathbb{Z}$, then

$$|a_p| \leq 2\sqrt{p}.$$

We say that $p$ is of *supersingular reduction* if $a_p = 0$ and of *ordinary reduction* otherwise.

Hasse's bound implies that the polynomial $X^2 - a_p X + p$ has two complex conjugate roots $\pi_p$, $\overline{\pi}_p$ such that $|\pi_p| = p^{1/2}$. As it turns out, the complex number $\pi_p$ plays the role of the Frobenius map $(x, y) \mapsto (x^p, y^p)$ on $E_p$, after identifying the endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_p)$ with an order in an imaginary quadratic field (ordinary case) or with an order in a quaternion algebra (supersingular case), where $\overline{\mathbb{F}}_p$ denotes an algebraic closure of $\mathbb{F}_p$. Moreover, we have that $\mathbb{Z}[\pi_p] \leq \mathrm{End}_{\mathbb{F}_p}(E_p)$. Now $\mathrm{End}_{\mathbb{F}_p}(E_p)$ is always an order in an imaginary quadratic field. Thus if we denote by $\Delta_p$ the discriminant of this order and by $b_p$ the index of $\mathbb{Z}[\pi_p]$ in $\mathrm{End}_{\mathbb{F}_p}(E_p)$, we obtain the formula

$$a_p^2 - 4p = b_p^2 \Delta_p. \tag{1.4}$$

The classical theory of elliptic curves provides us also with information about the structure of $E_p(\mathbb{F}_p)$. If we let $k$ be a nonzero integer, and if $E_p(\overline{\mathbb{F}}_p)[k]$ denotes the group of $\overline{\mathbb{F}}_p$-points of $E_p$ annihilated by $k$, then $E_p(\overline{\mathbb{F}}_p)[k]$ is isomorphic to $\mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/k\mathbb{Z}$ for any $(k, p) = 1$, and to $\mathbb{Z}/k\mathbb{Z}$ or $\{\mathcal{O}\}$ for any $(k, p) \neq 1$. The group $E_p(\mathbb{F}_p)$ can be viewed as a subgroup of $E_p(\overline{\mathbb{F}}_p)[k]$ for some $k$ such that $\#E_p(\mathbb{F}_p) \mid k$, and so can be written as

$$E_p(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/d_p e_p\mathbb{Z}$$

for uniquely determined positive integers $d_p, e_p$. More precisely, $d_p$ and $e_p$ are given by the formal

$$d_p = \gcd\left\{b_p, \frac{a_p + b_p\delta_p - 2}{2}\right\}, \qquad e_p = \frac{p + 1 - a_p}{d_p^2},$$

where $\delta_p$ is 0 if $\Delta_p \equiv 0 \pmod 4$ and 1 if $\Delta_p \equiv 1 \pmod 4$. We refer the reader to [**8**] for an explanation of how to deduce these formulas.

There is a rich family of questions regarding the group $E_p(\mathbb{F}_p)$ as $p$ varies over primes of good reduction for $E$: what is the percentage of the primes $p$ for which $E_p(\mathbb{F}_p)$ has order divisible by a fixed integer?; what can we say about the asymptotic distribution of the $d_p$'s?; what about the $e_p$'s, or the $\mathbb{Q}(\pi_p)$'s, or the $a_p$'s, or even the $b_p$'s? We will discuss some of these questions in what follows.

Throughout the paper, we will use the notation introduced above, as well as classical notation. More precisely, $p$ will denote a prime of good reduction for a given elliptic curve $E$ defined over $\mathbb{Q}$; $l, q$ will denote arbitrary rational primes; $k$ will denote a positive integer; $x$ will denote a positive real number; for a positive integer $n$, $\phi(n)$ will denote the Euler function of $n$, $\nu(n)$ the number of distinct prime divisors of $n$, and $\mu(n)$ the Möbius function of $n$; for a positive real number $x$, $\pi(x)$ will denote the number of primes $\leq x$ and $\operatorname{li} x$ the logarithmic integral $\int_2^x (\log t)^{-1}\, dt$; det and tr will denote the determinant and trace of a given matrix. Whenever we write $\mathrm{O}_A$, $\ll_A$, $\gg_A$, we will mean that the implied constants depend on $A$; whenever we write O, $\ll$, $\gg$, we will mean that the implied constants are absolute.

## 2. Divisibility of $\#E_p(\mathbb{F}_p)$ by fixed integers

We start our discussion with the simplest of the questions posed above.

Question 1. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $k$ be a fixed positive integer. What is the asymptotic behavior of the function

$$\#\{p \leq x : p \nmid kN, k \mid \#E_p(\mathbb{F}_p)\},$$

as $x \to \infty$?

The key fact which we will use in answering this question is the following classical property of the representation $\phi_k$:

Lemma 1. *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $p$ be a prime and $k$ be a positive integer such that $p \nmid kN$. If $\sigma_p$ denotes the Frobenius at $p$ in $\mathbb{Q}(E[k])/\mathbb{Q}$, then*

$$\operatorname{tr} \phi_k(\sigma_p) \equiv a_p \pmod{k}, \qquad \det \phi_k(\sigma_p) \equiv p \pmod{k}.$$

Therefore,

$$k \mid \#E_p(\mathbb{F}_p) \iff \sigma_p \subseteq C_k, \tag{2.1}$$

where

$$C_k := \{g \in \operatorname{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) : \det \phi_k(g) + 1 - \operatorname{tr} \phi_k(g) \equiv 0 \pmod{k}\}. \tag{2.2}$$

By using the classical Chebotarev density theorem we then obtain:

Theorem 1. *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $k$ be a fixed positive integer. Then, as $x \to \infty$,*

$$\#\{p \leq x : p \nmid kN, k \mid \#E_p(\mathbb{F}_p)\} \sim \frac{\#C_k}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \operatorname{li} x.$$

We remark that it can be shown that $\#C_k$ is $\approx k$ in the CM case and $\approx k^3$ in the non-CM case. Thus, from (1.2) and (1.3), we can deduce that the density above should be $\approx 1/k$.

## 3. Distribution of the $d_p$'s and the cyclicity of $E_p(\mathbb{F}_p)$

Let us be a little more courageous and ask:

Question 2. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $d$ be a fixed positive integer. What is the asymptotic behavior of the function

$$\#\{p \leq x : p \nmid dN, d_p = d\},$$

as $x \to \infty$?

This is already a more difficult question: not only do we want $d|\#E_p(\mathbb{F}_p)$, but also we ask for the stronger conditions that $E_p(\mathbb{F}_p)$ contain a subgroup isomorphic to $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$ and that this be the biggest two-copy of a cyclic group that occurs among the subgroups of $E_p(\mathbb{F}_p)$.

The case $d = 1$ has been extensively studied in the past 25 years. In 1975 [**1**], I. Borosh, C. J. Moreno and H. Porta made several computations which led them to expect that for many elliptic curves $E$ we have $d_p = 1$ (i.e., the group $E_p(\mathbb{F}_p)$ is cyclic) for infinitely many primes $p$. In 1976 [**31**], J.-P. Serre confirmed this expectation by proving, under the assumption of the generalized Riemann hypothesis (GRH) for the Dedekind zeta functions of the division fields $\mathbb{Q}(E[k])$ of $E$, that

$$\#\{p \leq x : p \nmid N, E_p(\mathbb{F}_p) \text{ cyclic}\} \sim \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \operatorname{li} x. \tag{3.1}$$

As explained for example in [**10**], the density above is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$.

There are many aspects of the cyclicity problem that we can consider. Can we remove GRH in Serre's result? Can we obtain effective error terms? What is the size of the smallest prime $p$ for which $E_p(\mathbb{F}_p)$ is cyclic? In 1979 [**26**], M. R. Murty removed GRH in (3.1) in the case of a CM elliptic curve. His unconditional proof made use of class field theoretical (CFT) properties of the division fields of CM elliptic curves (not available in the non-CM case!) and of the large sieve for number fields in the form of a Bombieri–Vinogradov theorem for number fields (due to R. J. Wilson). In 1987 [**27**], M. R. Murty also showed, unconditionally, that for certain non-CM elliptic curves $E$ there exist infinitely many primes $p$ for which $E_p(\mathbb{F}_p)$ is cyclic. In 1990 [**19**], R. Gupta and M. R. Murty used sieve methods to show, unconditionally and for any elliptic curve $E$ such that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, that

$$\#\{p \leq x : p \nmid N, E_p(\mathbb{F}_p) \text{ cyclic}\} \gg_N \frac{x}{(\log x)^2}.$$

Hence, unconditionally, there are infinitely many primes $p$ for which $E_p(\mathbb{F}_p)$ is cyclic if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. In [**2, 3**], the author managed to replace GRH in (3.1) with a $\frac{3}{4}$-quasi GRH (that is, a zero-free region of $\operatorname{Re}(s) > \frac{3}{4}$) in the case of a non-CM elliptic curve $E$. In [**3, 5**] she also obtained a new simpler unconditional proof of (3.1) in the case of a CM elliptic curve $E$ by removing the use of CFT and of the large sieve for number fields, and by using instead the sieve of Eratosthenes. We remark that the proofs of all these results will lead to error terms of the form $\mathrm{O}_N(x \log\log x/(\log x)^2)$ (the conditional formulas for non-CM and CM curves) and $\mathrm{O}_N(x/(\log x)^B)$ or $\mathrm{O}_N(x/[(\log x)(\log\log\log x)])$ (the unconditional formulas for CM curves), where $B$ is any positive integer. However, it is shown in [**3, 10**] that if we assume the full strength of GRH, then these error terms can be improved to $\mathrm{O}_N(x^{5/6}(\log x)^{2/3})$ in the non-CM case and $\mathrm{O}_N(x^{3/4}(\log x)^{1/2})$ in the CM case. The dependence of the $\mathrm{O}_N$-constant on $N$ can also be made explicit. Then, by comparing the main term with the error term, we obtain that, under GRH, the smallest prime $p$ for which $E_p(\mathbb{F}_p)$ is cyclic is $\mathrm{O}_\varepsilon\big((\log N)^{4+\varepsilon}\big)$ in the non-CM case and $\mathrm{O}_\varepsilon\big((\log N)^{2+\varepsilon}\big)$ in the CM case, for any $0 < \varepsilon < 1$.

Now let us return to the general situation stated in Question 2. The same technique as for $d = 1$ can be applied for an arbitrary $d$ and will lead to very similar results. More precisely, we obtain the following:

Theorem 2. *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $d$ be a positive integer.*

(1) *Assume that $E$ is without CM.*
  (a) *If a $\frac{3}{4}$-quasi GRH holds for the Dedekind zeta functions of the division fields of $E$, then*

$$\#\{p \leq x : p \nmid dN, d_p = d\} = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[dk]) : \mathbb{Q}]} \operatorname{li} x + \mathrm{O}_{d,N}\left(\frac{x \log \log x}{(\log x)^2}\right).$$

  (b) *If GRH holds for the Dedekind zeta functions of the division fields of $E$, then*

$$\#\{p \leq x : p \nmid dN, d_p = d\} = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[dk]) : \mathbb{Q}]} \operatorname{li} x + \mathrm{O}_{d,N}(x^{5/6}(\log x)^{2/3}).$$

(2) *Assume that $E$ is with CM.*
  (a) *Unconditionally,*

$$\#\{p \leq x : p \nmid dN, d_p = d\} = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[dk]) : \mathbb{Q}]} \operatorname{li} x + \mathrm{O}_{d,N}\left(\frac{x}{(\log x)(\log \log \log x)}\right).$$

  (b) *If GRH holds for the Dedekind zeta functions of the division fields of $E$, then*

$$\#\{p \leq x : p \nmid dN, d_p = d\} = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[dk]) : \mathbb{Q}]} \operatorname{li} x + \mathrm{O}_{d,N}(x^{3/4}(\log x)^{1/2}).$$

As already mentioned, the proof of this theorem is based on the same arguments as the ones used in the case $d = 1$ (see [**2, 3, 5, 10**]). For clarity, we will give a summary of the proof of part 1(b). The complete proof of the theorem will appear in an upcoming paper.

Before discussing the ideas of the proof, let us point out that, in this generality, Theorem 2 provides answers to a conjecture posed in [**35**]. To be more precise, it was predicted in [**35**, Conjectures 2 and 2'] that, for an elliptic curve $E$ defined over $\mathbb{Q}$ and for an integer $d$,

$$\#\{p \leq x : p \nmid dN, d_p = d\} \sim \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[dk]) : \mathbb{Q}]} \operatorname{li} x,$$

as $x \to \infty$. Thus, by part 1(a) of Theorem 2, this conjectural law is true in the non-CM case under a $\frac{3}{4}$-quasi GRH, and by part 2(a), it is true in the CM case under no hypothesis.

The first key ingredient in the proof of Theorem 2 is the following simple, but important, result (for a proof, see [**26**, pp. 153–154]).

Lemma 2. *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $p$ and $d$ be such that $p \nmid dN$. Then $E_p(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$ if and only if $p$ splits completely in $\mathbb{Q}(E[d])/\mathbb{Q}$.*

Another key ingredient is an effective version of the Chebotarev density theorem, due to J. Lagarias and A. Odlyzko [**22**].

Lemma 3 (Effective Chebotarev Density Theorem). *Let $L/\mathbb{Q}$ be a finite Galois extension, of Galois group $G$, degree $n_L$ and discriminant* $\operatorname{disc}(L/\mathbb{Q})$. *Let $C$ be a conjugacy set (that is, a finite union of conjugacy classes) of $G$. We set*

$$\pi_C(x, L/\mathbb{Q}) := \#\{p \leq x : \sigma_p \subseteq C\},$$

*where $\sigma_p$ is the Frobenius of $p$ in $L/\mathbb{Q}$.*

(1) *There exist positive constants $c_1$ and $c_2$, with $c_1$ effective and $c_2$ absolute, such that, if*

$$\sqrt{\frac{\log x}{n_L}} \geq c_2 \max(\log |d_L|, |d_L|^{1/n_L}),$$

*then*

$$\pi_C(x, L/\mathbb{Q}) = \frac{\#C}{\#G} \operatorname{li} x + \mathrm{O}\left((\#\tilde{C}) x \exp\left(-c_1 \sqrt{\frac{\log x}{n_L}}\right)\right),$$

*where $\tilde{C}$ denotes the set of conjugacy classes contained in $C$.*

(2) *Assume that a $\delta$-quasi GRH holds for the Dedekind zeta function of $L$ (that is, we have a zero-free region of* $\operatorname{Re}(s) > \delta$ *for the Dedekind zeta function of $L$). Then*

$$\pi_C(x, L/\mathbb{Q}) = \frac{\#C}{[L{:}\mathbb{Q}]} \operatorname{li} x + \mathrm{O}\left((\#C) x^{\delta} \left(\frac{\log |\operatorname{disc}(L/\mathbb{Q})|}{[L : \mathbb{Q}]} + \log x\right)\right).$$

Sketch of proof of part 1(b) of Theorem 2. By Lemma 2 and Hasse's bound, we can write

$$\#\{p \leq x : p \nmid dN, d_p = d\} = \sum_{k \leq 2\sqrt{x}} \mu(k) \pi_1(x, \mathbb{Q}(E[dk])/\mathbb{Q}).$$

We split this sum into two parts, according to whether $k < y$ or $y < k \leq 2\sqrt{x}$ for some parameter $y = y(x)$ to be chosen later. We use part 2 of Lemma 3 with $\delta = \frac{1}{2}$ to estimate the first subsum, and obtain

$$\sum_{k \leq y} \mu(k) \pi_1(x, \mathbb{Q}(E[dk])/\mathbb{Q}) = \sum_{k \leq y} \frac{\mu(k)}{[\mathbb{Q}(E[dk]){:}\mathbb{Q}]} \operatorname{li} x + \mathrm{O}_{d,N}(y x^{1/2} \log x).$$

To estimate the sum running over $y < k \leq 2\sqrt{x}$ we note that if a prime $p$ splits completely in $\mathbb{Q}(E[dk])$, then it also does in $\mathbb{Q}(\zeta_{dk})$, since $\mathbb{Q}(\zeta_{dk}) \subseteq \mathbb{Q}(E[dk])$. Hence, for such a prime $p$, we have $p \equiv 1 \pmod{dk}$. On the other hand, by Lemma 4, $p$ must also satisfy $p + 1 - a_p \equiv 0 \pmod{d^2 k^2}$. Therefore we can write

$$\begin{aligned}
&\sum_{y < k \leq 2\sqrt{x}} \mu(k) \pi_1(x, \mathbb{Q}(E[dk])/\mathbb{Q}) \\
&\qquad \leq \sum_{y < k \leq 2\sqrt{x}} \#\{p \leq x : p \nmid dN, p \equiv 1 \pmod{dk}, p + 1 - a_p \equiv 0 \pmod{d^2 k^2}\} \\
&\qquad \leq \sum_{\substack{|a| \leq 2\sqrt{x} \\ a \neq 2}} \sum_{\substack{y < k \leq 2\sqrt{x} \\ k \mid a-2}} \sum_{\substack{p \leq x \\ a_p = a \\ k^2 \mid p+1-a}} 1 + \sum_{y < k \leq 2\sqrt{x}} \sum_{\substack{p \leq x \\ a_p = 2 \\ k^2 \mid p-1}} 1 \\
&\qquad =: \sum\nolimits_1 + \sum\nolimits_2 .
\end{aligned}$$

Now we use elementary estimates to get

$$\begin{aligned}\textstyle\sum_1 &\ll \sum_{y<k\leq 2\sqrt{x}} \left(\frac{x}{k^2}+1\right)\frac{\sqrt{x}}{k} \ll \frac{x\sqrt{x}}{y^2}+\sqrt{x}\log x,\\ \textstyle\sum_2 &\ll \sum_{y<k\leq 2\sqrt{x}} \left(\frac{x}{k^2}+1\right) \ll \frac{x}{y}+\sqrt{x}.\end{aligned}$$

We choose

$$y := \left(\frac{x}{\log x}\right)^{1/3}$$

and, by putting together all of the above, we obtain

$$\#\{p \leq x : p \nmid dN, d_p = d\} = \sum_{k\leq y} \frac{\mu(k)}{[\mathbb{Q}(E[dk]):\mathbb{Q}]} \operatorname{li} x + \mathrm{O}_{d,N}(x^{5/6}(\log x)^{2/3}). \tag{3.2}$$

By using properties (3) of $[\mathbb{Q}(E[dk]):\mathbb{Q}]$ we can also estimate the tail

$$\sum_{k>y} \frac{\mu(k)}{[\mathbb{Q}(E[dk]):\mathbb{Q}]} \operatorname{li} x,$$

and, with a little more care, we can obtain the dependence on $N$ of the occurring $\mathrm{O}_{d,N}$-constants. This requires knowledge of upper bounds in terms of $N$ for the constant $A(E)$ mentioned in Section 1. Such bounds can be found in [**6, 32**]. We can finally show that

$$\begin{aligned}\#\{p \leq x : p \nmid dN, d_p = d\} = \sum_{k\geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[dk]):\mathbb{Q}]} \operatorname{li} x &+ \mathrm{O}_d(x^{5/6}(\log Nx)^{2/3})\\ &+ \mathrm{O}_d\left(\frac{(\log\log x)(\log Nx)}{\log x}(\log N)^3(\log\log 2N)^6\right),\end{aligned}$$

from which we can deduce (under the assumption that the density above is positive) that the size of the smallest prime $p$ such that $d_p = d$ is $\mathrm{O}_{d,\varepsilon}\big((\log N)^{4+\varepsilon}\big)$ for any $0 < \varepsilon < 1$. □

Let us remark that in the above proof of (3.2) we did not use that $E$ was a non-CM elliptic curve. However, the proof of the improved error term occurring in part 2(b) of Theorem 2 does use that in that situation we have a CM elliptic curve. Also, we remark that our proof of (3.2) can be generalized to elliptic curves defined over any number field. This is an advantage that we have over the proofs of parts 1(a) and 2(b) of the theorem, in which we invoke the Brun–Titchmarsh theorem whose number field version is not straightforward. Finally, we point out that it is an easy exercise to obtain the explicit dependence of the occurring O-constants on the integer $d$.

## 4. Primitive points on $E_p(\mathbb{F}_p)$

Having obtained satisfactory answers to the question of how often $d_p = 1$, hence $E_p(\mathbb{F}_p)$ is cyclic, we can proceed to asking a stronger question:

Question 3. Let $E$ be an elliptic curve defined over $\mathbb{Q}$, of conductor $N$ and of arithmetic rank $\geq 1$. Let $a \in E(\mathbb{Q})$ be a point of infinite order. What is the asymptotic behavior of

$$\#\{p \leq x : p \nmid N, E_p(\mathbb{F}_p) = \langle a \pmod p \rangle\},$$

as $x \to \infty$ (N.B. we may need to exclude the primes $p$ dividing the denominators of the coordinates of $a$)?

This question was formulated by S. Lang and H. Trotter in 1976 [**24**]. They conjectured the existence of the density of the primes $p$ for which $E_p(\mathbb{F}_p) = \langle a \pmod p \rangle$, a prediction that could be viewed as an elliptic curve analogue of Artin's primitive root conjecture. We should observe, though, that while in the classical situation of E. Artin the group $\mathbb{F}_p^*$ is always cyclic, in the elliptic curve situation of Lang–Trotter the group $E_p(\mathbb{F}_p)$ may not be cyclic. Therefore it was only natural that we studied the cyclicity of $E_p(\mathbb{F}_p)$ first.

In 1986 [**18**], R. Gupta and M. R. Murty showed that, under GRH, the above conjecture of Lang–Trotter is true for CM elliptic curves. More precisely, they used Chebotarev density arguments and sieve methods for the fields $\mathbb{Q}(E[k], k^{-1}a)$ to prove:

Theorem 3 (R. Gupta, M. R. Murty, 1986). *Let $E$ be a CM elliptic curve defined over $\mathbb{Q}$, of conductor $N$ and of arithmetic rank $\geq 1$. Let $K$ be the CM field of $E$. Let $a \in E(\mathbb{Q})$ be a point of infinite order. If GRH holds for the Dedekind zeta functions of the fields $\mathbb{Q}(E[k], k^{-1}a)$, then there exists a constant $C(E, a)$, depending on $E$ and $a$ (and defined in terms of $\mathbb{Q}(E[k], k^{-1}a)$), such that*

$$\begin{aligned}\#\{p \leq x : p \nmid N, p \text{ splits in } K, E_p(\mathbb{F}_p) = \langle a \pmod p \rangle\}& \\ = C(E, a) \operatorname{li} x + \mathrm{O}_N\left(\frac{x \log\log x}{(\log x)^2}\right)&.\end{aligned}$$

*If $K$ is one of $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$, then the density $C(E, a)$ is positive.*

Currently, nothing is known about the primes $p$ which are inert in the CM field $K$ of $E$. In addition, nothing is known about Question 3 in the case of a non-CM curve.

In 1986 and 1990, R. Gupta and M. R. Murty considered higher rank analogues of Question 3, which were also formulated, with conjectural answers, by Lang and Trotter in 1976 (see [**24**]). They provided conditional and unconditional answers to these questions in both the CM and non-CM cases. For a detailed discussion and precise formulations of their results, we refer the reader to [**18, 19, 29**].

## 5. Square-free orders for $E_p(\mathbb{F}_p)$

We turn our attention to the integers $e_p$ appearing in the description of the group $E_p(\mathbb{F}_p)$. For example, by observing that the cyclicity of $E_p(\mathbb{F}_p)$ is ensured if the order of the group is square-free, we can ask:

Question 4. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. What is the asymptotic behavior of the function

$$\#\{p \leq x : p \nmid N, \#E_p(\mathbb{F}_p) \text{ square-free}\},$$

as $x \to \infty$?

In other words, we are interested in the primes $p$ for which both the conditions that $d_p = 1$ and $e_p$ is square-free are satisfied.

In trying to answer this question, we start with the basic observation that

$$\#E_p(\mathbb{F}_p) \text{ is square-free} \iff q^2 \nmid \#E_p(\mathbb{F}_p) \text{ for any prime } q.$$

Thus we want to estimate the number of primes $p$ for which $q \nmid d_p$ for any $q$ and $q^2 \nmid e_p$ for any $q$. We have seen in Section 4 that the behavior of the $d_p$'s is well understood. The study of the behavior of the $e_p$'s is more challenging, one of the difficulties that we encounter being that the distribution of the $e_p$'s is related to the distribution of primes $p$ (not) splitting completely in "too small" field extensions. Luckily, however, in the CM case we have the following beautiful characterization of the squarefreeness of $e_p$ (for a proof, see [**4**]):

Lemma 4. *Let $E$ be a CM elliptic curve defined over $\mathbb{Q}$, of conductor $N$ and with complex multiplication by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K$. Let $p \nmid N$ be a prime of ordinary good reduction for $E$. Then $\#E_p(\mathbb{F}_p)$ is square-free if and only if $p$ splits completely in $K$, as $(p) = (\pi_p)(\overline{\pi}_p)$, and $\pi_p$ does not split completely in $K(E[\mathfrak{q}])$ for any inert prime ideal $\mathfrak{q}$ of $K$, in $K(E[\mathfrak{q}^2])$ for any ramified prime ideal $\mathfrak{q}$ of $K$, and in $K(E[\mathfrak{q}\overline{\mathfrak{q}}])$, $K(E[\mathfrak{q}^2])$, and $K(E[\overline{\mathfrak{q}}^2])$ for any split prime ideal $\mathfrak{q}$ of $K$. Here, for an ideal $(\alpha)$ of $K$, we denote by $E[(\alpha)]$ the kernel of the multiplication by $\alpha$ map.*

Therefore, by remark (2.1) made in Section 2 and by the above lemma, in order to answer Question 4 for CM elliptic curves with CM by $K$, we need to estimate the number of primes that satisfy Chebotarev conditions in division fields of the form $K(E[q])$ and $K(E[\mathfrak{q}^2])$. These extensions are "sufficiently large," and then, by using Chebotarev density theorems and sieve methods, we can prove:

Theorem 4. *Let $E$ be a CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$, with complex multiplication by the full ring of integers of an imaginary quadratic field.*

(1) *Unconditionally, we have that*

$$\#\{p \le x : p \nmid N, \#E_p(\mathbb{F}_p) \text{ square-free}\} = \sum_{k \ge 1} \frac{\mu(k)\#C_{k^2}}{[\mathbb{Q}(E[k^2]):\mathbb{Q}]} \operatorname{li} x + \mathrm{O}_N\left(\frac{x}{(\log x)(\log\log\log x)}\right).$$

(2) *Under GRH for the Dedekind zeta functions of the division fields of $E$, we have that*

$$\#\{p \le x : p \nmid N, \#E_p(\mathbb{F}_p) \text{ square-free}\} = \sum_{k \ge 1} \frac{\mu(k)\#C_{k^2}}{[\mathbb{Q}(E[k^2]):\mathbb{Q}]} \operatorname{li} x + \mathrm{O}_N(x^{7/8}(\log x)^7).$$

*Here, the conjugacy sets $C_{k^2}$ are as in* (2.2).

Similar, but conditional, asymptotic formulas can also be obtained in the non-CM case, but by using a different and more elaborate approach. For proofs of all these results, we refer the reader to [**3, 4**].

## 6. Prime orders for $E_p(\mathbb{F}_p)$

What if the order of $E_p(\mathbb{F}_p)$ is not only square-free, but also a prime (which means, $d_p = 1$ and $e_p$ is prime)? In other words:

Question 5. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. What is the asymptotic behavior of the function

$$\#\{p \leq x : p \nmid N, \#E_p(\mathbb{F}_p) \text{ prime}\},$$

as $x \to \infty$?

In 1988 [**21**], N. Koblitz showed the relevance of this question to the theoretical study of elliptic curve cryptography. We recall that certain public-key cryptosystems (based on the intractability of the discrete logarithm problem) can be implemented using the group of points of an elliptic curve defined over a finite field. A desirable property of this curve is that the cyclic group generated by a fixed point of the curve have order divisible by a large prime. By choosing the elliptic curve such that its group of points has (large) prime order, the desired property is clearly satisfied for any point.

The basic observation in approaching Question 5 is that

$$\#E_p(\mathbb{F}_p) \text{ is a prime "}\Longleftrightarrow\text{" } q \nmid \#E_p(\mathbb{F}_p) \text{ for any prime } q \leq \sqrt{p}+1,$$

where by "$\Leftrightarrow$" we mean that care should be taken with the prime values of $\#E_p(\mathbb{F}_p)$ which may lie between $\sqrt{p}-1$ and $\sqrt{p}+1$. Then, by using remark (2.1), we can write

$$\#\{p \leq x : \#E_p(\mathbb{F}_p) \text{ prime}\} \text{ "="} \sum_{k \leq \sqrt{x}+1} \mu(k) \#\{p \leq x : \sigma_p \subseteq C_k\}. \tag{6.1}$$

This formula suggests that the number of primes $p \leq x$ for which $\#E_p(\mathbb{F}_p)$ is prime should be

$$\sim C(E) \frac{x}{(\log x)^2}$$

for some (positive) constant $C(E)$ depending on $E$, as already conjectured by Koblitz in [**21**].

Now let us remark further that Question 5 could be viewed as an elliptic curve analogue of the classical twin prime conjecture: we want to count primes $p$ for which $p + (1 - a_p)$ is also a prime. As in the classical case, the densities $\approx 1/k$ of the primes $p$ for which $k \mid \#E_p(\mathbb{F}_p)$ will direct us to serious difficulties in trying to estimate (6.1). Nevertheless, we recall that an ingenious use of the lower bound sieve allowed J. Chen to prove in 1973 that there are infinitely many primes $p$ such that $p+2$ has at most 2 prime divisors. In 2001 [**25**], S. A. Miri and V. K. Murty carried out an elliptic curve version of Chen's method and showed:

Theorem 5 (Miri and Murty [**25**]). *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Assume that GRH holds for the Dedekind zeta functions of the division fields of $E$. Then there exist*

$$\gg_N \frac{x}{(\log x)^2}$$

*primes $p \leq x, p \nmid N$, for which $\#E_p(\mathbb{F}_p)$ has at most* 16 *prime divisors (counted with multiplicities).*

A similar result holds in the CM case, *unconditionally*, as will be explained in [**7**].

## 7. Distribution of the Frobenius fields

In our discussions of Questions 2–5 we were more successful in the CM case than in the non-CM case. One of the features of the CM curves which contributed to our success concerns the imaginary quadratic fields $\mathbb{Q}(\pi_p)$ that were introduced in Section 1. More precisely, this special feature is related to the following question:

Question 6. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $K$ be an imaginary quadratic field. What is the asymptotic behavior of

$$\#\{p \leq x : p \nmid N, a_p \neq 0, \mathbb{Q}(\pi_p) = K\},$$

as $x \to \infty$?

It is not difficult to answer this question in the CM case. First we observe that $\mathbb{Q}(\pi_p) \subseteq \mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then, if $E$ has CM by some field $K$ and if $p$ is an ordinary prime for $E$, we have $K = \mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q}$. Thus we obtain:

Theorem 6. *Let $E$ be a CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $K$ be the CM field of $E$. Then $\mathbb{Q}(\pi_p) = K$ for any prime $p \nmid N$ of ordinary reduction for $E$.*

To answer Question 6 in the non-CM case is far more difficult. It was conjectured by S. Lang and H. Trotter in 1976 [**23**] that if $E$ is a non-CM curve, then, as $x \to \infty$,

$$\#\{p \leq x : p \nmid N, \mathbb{Q}(\pi_p) = K\} \sim C(E, K) \frac{x^{1/2}}{\log x}$$

for some positive constant $C(E, K)$ depending on $E$ and $K$.

In 1981 [**32**], J.-P. Serre asserted that one could obtain nontrivial upper bounds for the above quantity, by using Chebotarev type arguments and Selberg's sieve. Recently, the author, É. Fouvry and M. R. Murty completed the proof of such results by using the much simpler square sieve (see [**9**]). To be more precise, if $p$ is a prime such that $\mathbb{Q}(\pi_p) = K$ for some imaginary quadratic field $K$ of discriminant $\Delta$, then $\Delta(a_p^2 - 4p)$ must be equal to a square. The square sieve is a device that suggests how to obtain upper bounds for the number of squares in a finite (multi)set of positive integers. By applying this sieve to the sequence $\{\Delta(a_p^2 - 4p)\}_{p \leq x}$, and by invoking effective versions of the Chebotarev density theorem, we can prove:

Theorem 7 (Cojocaru, Fouvry, and Murty [**9**]). *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field, where $D$ is positive and square-free. Let $x \geq 3$.*

(1) *Unconditionally, we have that*

$$\#\{p \leq x : p \nmid N, \mathbb{Q}(\pi_p) = K\} \ll_N \frac{x (\log \log x)^{13/12}}{(\log x)^{25/24}} (1 + \nu(D)).$$

*If $\mathcal{D}_E(x)$ denotes the set of (distinct) square-free parts of $4p - a_p^2$ for primes $p \leq x$ of ordinary reduction for $E$, then there exists $x_0 = x_0(N)$ such that, for any $x \geq x_0$,*

$$\#(\mathcal{D}_E(\infty) \cap [1, x]) \gg_N \log \log \log x.$$

*In particular, there are infinitely many distinct fields $\mathbb{Q}(\pi_p)$.*

(2) *If we assume GRH for the Dedekind zeta functions of the division fields of $E$, then*

$$\#\{p \leq x : p \nmid N, \mathbb{Q}(\pi_p) = K\} \ll_N x^{17/18} \log x$$

*and*

$$\#\mathcal{D}_E(x) \gg_N \frac{x^{1/18}}{(\log x)^2}.$$

We note that additional improvements of the above bounds can be obtained by assuming the validity of Artin's holomorphy conjecture and of a pair correlation conjecture (see [**9**]).

## 8. Distribution of the $a_p$'s

Now let us investigate the integers $a_p$. More precisely, let us consider:

Question 7. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $a$ be a fixed integer. What is the asymptotic behavior of

$$\#\{p \leq x : p \nmid N, a_p = a\},$$

as $x \to \infty$?

For example, consider a CM elliptic curve $E$ with CM by $\mathbb{Q}(i)$ and try to count the primes $p$ for which $a_p = 2$. By Theorem 6 and (1.4)), this implies that $p = n^2 + 1$ for some integer $n$. Thus our question can be viewed as an elliptic curve analogue of the classical Buniakowski–Schinzel hypothesis about the prime values of the polynomial $n^2 + 1$.

In 1976 [**23**], S. Lang and H. Trotter conjectured that there exists a constant $C(E)$, depending on $E$, such that, as $x \to \infty$,

$$\#\{p \leq x : p \nmid N, a_p = a\} \sim C(E)\frac{x^{1/2}}{\log x}.$$

The only exception to this conjectural rule occurs in the case $a = 0$ and $E$ a CM curve, about which we know:

Theorem 8 (Deuring [**11**]). *Let $E$ be a CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Then, with finitely many exceptions, a prime $p \nmid N$ is supersingular if and only if it is inert in the CM field of $E$, and so, as $x \to \infty$,*

$$\#\{p \leq x : p \nmid N, a_p = 0\} \sim \frac{1}{2} \cdot \frac{x}{\log x}.$$

If $a \neq 0$ and $E$ is CM, then the Lang–Trotter conjecture is consistent with classical conjectures of Hardy–Littlewood about the distribution of primes in quadratic extensions. If $E$ is non-CM, the Lang–Trotter conjecture seems at least as difficult.

It is easy to obtain upper bounds for the number of primes $p$ for which $a_p = a$ if $E$ is a CM curve and $a \neq 0$. Indeed, in this case we can use (1.4) with $\Delta_p = \Delta$ for some $\Delta$ independent of $p$ to deduce that

$$\#\{p \leq x : p \nmid N, a_p = a\} = \#\left\{p \leq x : p \nmid N, p = \left(\frac{a}{2}\right)^2 - \left(\frac{b_p}{2}\right)^2 \Delta\right\} \ll x^{1/2}.$$

By using sieve theory (e.g., Brun's sieve), one could actually improve this bound to obtain:

THEOREM 9. *Let $E$ be a CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $a$ be a nonzero arbitrary integer. Then*

$$\#\{p \leq x : p \nmid N, a_p = a\} \ll \frac{x^{1/2}}{\log x}.$$

The non-CM situation is not that easy anymore. The first results in this case were obtained by Serre [**32**] (by invoking Chebotarev type arguments) and by V. K. Murty [**30**] (by appealing to different arguments from Serre's). More precisely, we have:

THEOREM 10. *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $a$ be an arbitrary integer.*

(1) (Serre [**32**]) *If $a \neq 0, \pm 2$, then*

$$\#\{p \leq x : p \nmid N, a_p = a\} \ll_N \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}.$$

*If $a = \pm 2$, then*

$$\#\{p \leq x : p \nmid N, a_p = a\} \ll_N \frac{x(\log\log x)^{1/2}(\log\log\log x)^{1/4}}{(\log x)^{5/4}}.$$

*If $a = 0$, then*

$$\#\{p \leq x : p \nmid N, a_p = 0\} \ll_N \frac{x(\log\log x)(\log\log\log x)^{1/2}}{(\log x)^{3/2}}.$$

(2) (Serre, [**32**]) *Assume GRH for the Dedekind zeta functions of the division fields of $E$. If $a \neq 0, \pm 2$, then*

$$\#\{p \leq x : p \nmid N, a_p = a\} \ll_N \frac{x^{5/6}}{(\log x)^{1/3}}.$$

*If $a = \pm 2$, then*

$$\#\{p \leq x : p \nmid N, a_p = a\} \ll_N \frac{x^{7/8}}{(\log x)^{1/2}}.$$

*If $a = 0$, then*

$$\#\{p \leq x : p \nmid N, a_p = 0\} \ll_N x^{3/4}.$$

(3) (Murty [**30**]) *Assume that we have analytic continuation, functional equation and a Riemann Hypothesis for the $L$-series attached to the symmetric powers of the Galois representations of $E$ (for definitions, see* [**30**]*). Then, as $x \to \infty$,*

$$\#\{p \leq x : p \nmid N, a_p = a\} \ll_N x^{3/4}(\log x)^{1/2}.$$

It was also noted by N. Elkies and M. R. Murty (see [**14**, pp. 25–26] and [**16**]) that the upper bound $\mathrm{O}_N(x^{3/4})$ for the number of supersingular primes $\leq x$ can be obtained *unconditionally* by using a result of M. Kaneko [**20**].

The question of finding lower bounds is even more difficult. The only results known at the moment concern supersingular primes.

THEOREM 11. *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$.*

(1) (Elkies [**15**]) *There are infinitely many primes $p$ such that $a_p = 0$. Moreover, if GRH holds for the Dedekind zeta function of any quadratic extension of $\mathbb{Q}$, then, as $x \to \infty$,*

$$\#\{p \le x : p \nmid N, a_p = 0\} \gg \log\log x.$$

(2) (Fouvry and Murty [**17**]) *For any $\delta > 0$, there exists a positive real number $x_0(E, \delta)$ such that*

$$\#\{p \le x : p \nmid N, a_p = 0\} \ge \frac{\log\log\log x}{(\log\log\log\log x)^{1+\delta}}$$

*for any $x > x_0(E, \delta)$.*

## 9. Distribution of the $b_p$'s

Finally, let us turn our attention to the integers $b_p$ appearing in (1.4). It is clear from the definition that they are natural companions of the integers $a_p$. It is natural to ask:

Question 8. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $b$ be a fixed positive integer. What is the asymptotic behavior of

$$\#\{p \le x : p \nmid bN, b_p = b\},$$

as $x \to \infty$?

The case $b = 1$ of this question was investigated by the author and W. Duke in [**8**]. The starting point in these investigations is to put the integers $a_p$ and $b_p$ in a more convenient context. This is accomplished by realizing that the matrix

$$\begin{pmatrix} (a_p + b_p\delta_p)/2 & b_p \\ \big(b_p(\Delta_p - \delta_p)\big)/4 & (a_p - b_p\delta_p)/2 \end{pmatrix},$$

reduced modulo an integer $k$ such that $p \nmid kN$, represents the Frobenius at $p$ in the $k$-division field $\mathbb{Q}(E[k])$ (see [**13**]). Consequently, we have:

Lemma 5. *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $p$ be a prime and $k$ a positive integer such that $p \nmid kN$. Then $k \mid b_p$ if and only if $p$ splits completely in the subfield $J_k$ of $\mathbb{Q}(E[k])$ fixed by the scalars of* $\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})$.

Using this result we can then write

$$\#\{p \le x : p \nmid bN, b_p = b\} = \sum_{k \le 2\sqrt{x}} \mu(k)\#\{p \le x : p \nmid bN, p \text{ splits completely in } J_{bk}\}. \tag{9.1}$$

As in our discussions about the distributions of the $d_p$'s and $e_p$'s, we can apply the Chebotarev density theorem to estimate (9.1), but, again, this will be possible only in a short range of the indices $k$. The challenging part will be to estimate the remaining sum. We point out that, unlike the full $k$-division field, $J_k$ does not contain the cyclotomic field $\mathbb{Q}(\zeta_k)$. Hence the Brun-Titchmarsh theorem that we usually rely on cannot be invoked anymore.

Surprisingly, if $E$ is a CM elliptic curve, then (9.1) can be handled fairly simply, as follows. First we distinguish between ordinary and supersingular primes $p$. Then we note that the ordinary primes contribute very little to our estimates (and this does not happen anymore if $E$ is non-CM!). Indeed, by Lemma 5, we get that

$$\begin{aligned}&\#\{p \leq x : p \nmid bN, a_p \neq 0, b_p = b\}\\ &\qquad\qquad \leq \#\left\{p \leq x : a_p \neq 0, p = \left(\frac{a_p}{2}\right)^2 - \frac{b^2\Delta}{4}\right\} \ll x^{1/2},\end{aligned}$$

where we recall that $\Delta = \Delta_p$ is independent of $p$ in the ordinary case. The main contribution to our final estimates will be given by the supersingular primes of $E$. However, we note that for supersingular primes $p$ such that $b_p = b$ we have $-4p = b^2\Delta_p$, hence $b$ can only be 1 or 2. Thus, if $b \geq 3$, then

$$\#\left\{p \leq x : p \nmid bN, a_p = 0, b_p = b\right\} = 0,$$

and if $b = 1$ or 2, then, by Theorem 8 and Lemma 5,

$$\begin{aligned}&\#\{p \leq x : p \nmid bN, a_p = 0, b_p = 1\} = \#\{p \leq x : p \nmid N, p \text{ is inert in } K \text{ and } J_2\},\\ &\#\{p \leq x : p \nmid bN, a_p = 0, b_p = 2\}\\ &\qquad\qquad = \#\{p \leq x : p \nmid 2N, p \text{ is inert in } K \text{ and splits in } J_2\}.\end{aligned}$$

We finish off by invoking the unconditional effective Chebotarev density theorem for the fields $K$ and $J_2$ (see part 1 of Lemma 3), and we obtain:

THEOREM 12 (Cojocaru and Duke [**8**]). *Let $E$ be a CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $b$ be a positive integer. Then*

$$\#\{p \leq x : p \nmid bN, b_p = b\} = C(E)\operatorname{li} x + \operatorname{error}(x),$$

*where*

$$C(E) = \begin{cases} \frac{1}{2} - 1/[J_2{:}\mathbb{Q}] + 1/[J_2K{:}\mathbb{Q}] & \text{if } b = 1\\ 1/[J_2{:}\mathbb{Q}] - 1/[J_2K{:}\mathbb{Q}] & \text{if } b = 2\\ 0 & \text{if } b \geq 3\end{cases}$$

*and*

$$\operatorname{error}(x) = \begin{cases} \mathrm{O}_N(x/(\log x)^B) & \text{if } b = 1 \text{ or } b = 2\\ \mathrm{O}(x^{1/2}) & \text{if } b \geq 3,\end{cases}$$

*for any $B > 0$.*

Let us note that, as with Theorem 9, by using sieve theory the error term $\mathrm{O}(x^{1/2})$ can be improved to $\mathrm{O}(x^{1/2}/\log x)$.

Clearly, the above proof cannot be emulated if $E$ is a non-CM elliptic curve. In this situation, the key observation for handling the ordinary primes $p$ that split completely in $J_{bk}$ for (large) indices $k$ is that $k^2 \mid 4p - a_p^2$, and so $m(4p - a_p^2)$ is a square for some (small) positive integer $m$. We can now invoke the square sieve that we already appealed to in our approach on Question 6. We obtain:

THEOREM 13 (Cojocaru and Duke [**8**]). *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $b$ be a positive integer. Assume that GRH holds for the division fields of $E$. Then*

$$\#\{p \leq x : p \nmid bN, b_p = b\} = \sum_{k \geq 1} \frac{\mu(k)}{[J_{bk}{:}\mathbb{Q}]}\operatorname{li} x + \mathrm{O}_{b,N,\varepsilon}(x^{53/54+\varepsilon})$$

*for any $0 < \varepsilon < 1$.*

For the details of the proof in the case $b = 1$, we refer the reader to [**8**]. The general case is dealt with the same, mutatis mutandis.

We remark that the integers $b_p^2$ can be interpreted as the orders of the Tate-Shafarevich groups of the curves $E_p$ viewed as constant curves defined over their own function fields (see the explanations in [**8**]). This may lead to new interesting meanings of the above two results. We also remark that if $b_p = 1$, then $d_p = 1$ (i.e., the group $E_p(\mathbb{F}_p)$ is cyclic), and so Question 8 can be viewed as a refinement of Question 2 which we discussed at the beginning of the paper.

## 10. Concluding remarks

As already suggested in our discussions above, there are many questions about $E_p(\mathbb{F}_p)$ which remain unanswered. Among them, the most notable ones are the Lang–Trotter conjectures and the Koblitz conjecture. Other questions of interest concern the positivity of the asymptotic constants that occur in some of our results (e.g., Theorems 2, 4, and 13), and upper bounds for the smallest prime $p$ for which $E_p(\mathbb{F}_p)$ has a given property. These questions will be discussed in a forthcoming paper.

Most of the results that we discussed have (certain) generalizations to elliptic curves defined over number fields. A natural direction of research is to study if similar results can be obtained for elliptic curves defined over function fields. Even more generally, one can study analogous questions about reductions of abelian varieties and Drinfeld modules, even though the formulation of these questions may not be straightforward.

Finally, we remark that there is a vast literature concerning reductions modulo primes of an elliptic curve. In our present survey, many important questions, such as the Sato–Tate conjecture, had to be left out. The only criterion used in selecting the aspects of $E_p(\mathbb{F}_p)$ that we discussed was the author's own current research.

**Acknowledgments.** I am indebted to M. Ram Murty and Manjul Bhargava for their useful comments on previous versions of the paper. I am also indebted to the audiences of my talks on results discussed in this paper, which I gave at CNTA VII and at various universities (Laval, McGill, Carleton, Queen's, Toronto, McMaster, Waterloo, British Columbia, UIUC, and UCLA) during 2002. I am thankful to the organizers of CNTA VII for providing me with financial support for participating in this conference.

## References

1. I. Borosh, C. J. Moreno, and H. Porta, *Elliptic curves over finite fields.* II, Math. Comput. 29 (1975), 951–964.
2. 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), 335–350.
3. ______, *Cyclicity of elliptic curves modulo p*, Ph.D. thesis, Queen's University, Kingston, ON, 2002.
4. ______, *Square-free orders for CM elliptic curves modulo p*, 2002 (preprint).
5. ______, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc. **355** (2003), no. 7, 2651–2662.
6. ______, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. (to appear).
7. ______, *Primality for the group of points of CM elliptic curves modulo p* (in preparation).
8. A. C. Cojocaru and W. Duke, *Reductions of an elliptic curve and their Tate-Shafarevich groups*, Math. Ann. (to appear)

9. A.C. Cojocaru, É. Fouvry, and M. R. Murty, *The square sieve and the Lang–Trotter conjecture*, 2001 (preprint).
10. A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, 2001 (preprint).
11. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Functionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
12. ———, *Teilbarkeitseigenschatten der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung*, Comment. Math. Helv. **19** (1946), 74–82.
13. W. Duke and Á. Tóth, *The splitting of primes in division fields of elliptic curves*, Experiment. Math. **11** (2003), no. 4, 555–565.
14. N. D. Elkies, *Supersingular primes of a given elliptic curve over a number field*, Ph.D. thesis, Harvard University, Cambridge, MA, 1987.
15. ———, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (1987), no. 3, 561–567.
16. ———, *Distribution of supersingular primes*, Journées Arithmétiques, 1989 (Luminy, 1989), Astérisque, vol. 198–200, Soc. Math. France, Paris ,1991, pp. 127–132.
17. É. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), no. 1, 81–104.
18. R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), no. 1, 13–44.
19. ———, *Cyclicity and generation of points modulo p on elliptic curves*, Invent. Math. **101** (1990), no. 1, 225–235.
20. M. Kaneko, *Supersingular $j$-invariants* $\bmod p$, Osaka J. Math. **26** (1989), no. 4, 849–855.
21. N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165.
22. J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields: $L$-functions and Galois Properties (Durham, 1975), Academic Press, London, 1977, pp. 409–464.
23. S. Lang and H. Trotter, *Frobenius distributions in* $\mathrm{GL}_2$*-extensions*, Lecture Notes in Math., vol. 504, Springer-Verlag, Berlin–New York, 1976.
24. ———, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292.
25. S. A. Miri and V. K. Murty, *An application of sieve methods to elliptic curves*, Progress in Cryptology—INDOCRYPT 2001 (Chennai, 2001), Lecture Notes in Comput. Sci., vol. 2247 Springer, Berlin, 2001, pp. 91–98.
26. M. R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), no. 2, 147–168.
27. ———, *On the supersingular reduction of elliptic curves*, Proc. Indian Acad. Sci. Math. Sci. **97** (1987), no. 1-3, 247–250.
28. ———, *Recent developments in elliptic curves*, Proceedings of the Ramanujan Centennial International Conference (Annamalainagar, 1987),RMS Publ., vol. 1, Ramanujan Math. Soc., Annamalainagar, 1988, pp. 45–53.
29. ———, Artin's conjecture and elliptic analogues", Sieve Methods, Exponential Sums and their Applications in Number Theory, (Cardiff, 1995), London Math. Soc. Lecture Note Ser., vol. 237, Cambridge Univ. Press, Cambridge, 1997, pp. 326–344.
30. V. K. Murty, *Explicit formulae and the Lang–Trotter conjecture*, Rocky Mountain J. Math. 15 (1985), no. 2, 535–551.
31. J.-P. Serre, *Résumé des cours de 1977–1978*, Ann. Collège France, Collège de France, Paris, 1978, pp. 67–70.
32. J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Études Sci. Publ. Math. **54** (1981), pp. 123–201.
33. J. H. Silverman, The arithmetic of elliptic curves, Grad. Texts in Math., vol. 106, Springer-Verlag, New York, 1986.
34. ———, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math., vol. 151, Springer-Verlag, New York, 1994.
35. R. Takeuchi, *On the distribution of the group of rational points of reductions of an elliptic curve*, 2003 (preprint).

Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544, USA

*E-mail address*: cojocaru@math.princeton.edu