PRIMES, ELLIPTIC CURVES AND CYCLIC GROUPS: A SYNOPSIS

ALINA CARMEN COJOCARU

Communicated by Vasile Brînzănescu

The main question addressed in this paper is: given a rational elliptic curve, what is the frequency with which its reductions modulo primes give rise to cyclic groups? This question is part of a broader theme of investigating the distribution of Frobenius in an infinite family of finite, Galois field extensions defined by an arithmetic-geometric object. Illustrative of ideas, methods and obstacles that occur in the broader theme, the study of the cyclicity question is foundational for a researcher interested in pursuing studies of distribution of primes in arithmetic-geometric contexts. While most of the paper is a survey of prior results, the proof of part (i) of the Cyclicity on Average Theorem from Section 9 is new.

AMS 2010 Subject Classification: 11G05, 11N36, 11R45.

Key words: prime numbers, density theorems, character sums, cyclic groups, elliptic curves.

1. INTRODUCTION

Throughout the 20th century, the analogies between the group of units $k^\times$ of a finite field k and the group of points $E(k)$ of an elliptic curve E/k, defined over k, have been both stimulating and rewarding. Prominent theoretical advances, such as the conditional resolution and the unconditional quasi-resolution of Artin's Primitive Root Conjecture, and striking applications, such as the development of elliptic curve public key cryptography, are rooted in the exploration of the properties of these two groups and in the similarities that they exhibit.

The purpose of this paper is to focus on $k = \mathbb{F}_p$, the finite field with p elements (with p always denoting a prime) and to present a succinct overview of results about the reductions $\overline{E}/\mathbb{F}_p$ modulo p of an arbitrary elliptic curve $E/\mathbb{Q}$, with a particular focus on two inter-related arithmetic properties of $\overline{E}(\mathbb{F}_p)$ that highlight similarities of this group to $\mathbb{F}_p^\times$: *group structure* and *growth of group exponent,* as functions of p. Recalling that $\mathbb{F}_p^\times$ is a cyclic group of order and exponent both equal to $p-1$, our motivating questions are:

A.C. Cojocaru's work on this material was partially supported by the Simons Collaboration Grant under Award No. 318454.

Question 1. Given an elliptic curve $E/\mathbb{Q}$, how often is the group $\overline{E}(\mathbb{F}_p)$ cyclic?

Question 2. Given an elliptic curve $E/\mathbb{Q}$, how often are the order and the exponent of $\overline{E}(\mathbb{F}_p)$ close in size?

In Section 6, we will formulate more explicit versions of these questions.

2. **PRIMES**

A fundamental problem in number theory is that of understanding the **primes**. Already around 300 BC, using a simple argument, Euclid showed that there are infinitely many primes. About two millennia later (1850s), Chebysheff showed that the prime counting function

$$\pi(x) := \#\{p \leq x : p \text{ prime}\}$$

is bounded, from above and below, by constant multiples of $\frac{x}{\log x}$. In the 1890s, following Riemann's groundbreaking insights from 1859 on the Riemann zeta function, Hadamard and de la Vallée Poussin proved, independently, the asymptotic for $\pi(x)$, previously conjectured by Legendre and Gauss in the late 1700s:

THEOREM 3 (The Prime Number Theorem).

$$\pi(x) \sim \frac{x}{\log x}.$$

This is by no means the end of the study of primes. Not only there are infinitely many of them, but infinitely many of them (seem to) appear in interesting sequences. For example, Euclid-type arguments have been used to show that infinitely many primes lie in certain arithmetic progressions. Moreover, using *analytic methods*, in the 1830s Dirichlet obtained a more refined understanding of the behaviour of primes in arithmetic progressions. Following de la Vallée Poussin's work on primes, Dirichlet's result is now often stated as follows:

THEOREM 4 (Dirichlet's Theorem for Primes in Arithmetic Progressions). *For any coprime integers a, m with $m \geq 1$, we have*

$$\pi(x, m, a) := \#\{p \leq x : p \equiv a (\mathrm{mod}\, m)\} \sim \frac{1}{\phi(m)}\, \pi(x),$$

where $\phi(m)$ denotes the Euler function of m (notation to be followed throughout).

Theorem 4 is only a particular case of the more general Chebotarev Density Theorem, proven by Chebotarev in the 1920s. In its simplest form, this theorem states:

THEOREM 5 (The Chebotarev Density Theorem). *For a finite, Galois extension $K/\mathbb{Q}$ and a conjugacy class $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$, we have*

$$\pi_C(x, K/\mathbb{Q}) := \#\left\{p \leq x : \left(\frac{K/\mathbb{Q}}{p}\right) = C\right\} \sim \frac{|C|}{[K:\mathbb{Q}]}\pi(x), \tag{1}$$

where $\left(\frac{K/\mathbb{Q}}{p}\right)$ is the Artin symbol at p in the extension $K/\mathbb{Q}$.

Other sets of primes, conjectured to be infinite, have been the focus of several celebrated conjectures, such as:

CONJECTURE 6 (Artin's Primitive Root Conjecture, 1920s). *Given α an integer, different from $0, \pm 1$ and not a square, $\exists\, C(\alpha) > 0$ such that*

$$\#\{p \leq x : \mathbb{F}_p^\times = \langle \alpha (\mathrm{mod}\, p) \rangle\} \sim C(\alpha)\, \pi(x). \tag{2}$$

While this conjecture is still open, significant progress has been attained towards proving it. Indeed, in 1967 Hooley proved (2) under the Generalized Riemann Hypothesis (GRH). Moreover, in 1983, using new results of Iwaniec and of Fouvry & Iwaniec on primes in arithmetic progressions, Gupta and M.R. Murty proved the first unconditional result about (2): roughly stated, among any suitably independent 13 numbers α, at least one satisfies Artin's Primitive Root Conjecture. In 1985, the size 13 was brought down to 7 by Gupta, M.R. Murty and V.K. Murty, and soon after, following important work of Bombieri, Friedlander and Iwaniec, the size was brought down to 3 by Heath-Brown. For a thorough presentation of progress on Artin's Primitive Root Conjecture, we refer the reader to [41].

The study of problems such as (2) reveals the importance of the study of primes in arithmetic progressions, for varying moduli. This, in turn, reveals the importance of the study of the error terms and their uniformity in the modulus m in Dirichlet's Theorem for Primes in Arithmetic Progressions. In this direction, analytic methods have successfully been used to prove the following now-classical results:

THEOREM 7 (The Siegel-Walfisz Theorem). *$\forall A > 0$ and $\forall m \leq (\log x)^A$, $\exists\, C(A) > 0$ such that, $\forall a$ with $(a, m) = 1$,*

$$\pi(x, m, a) = \frac{1}{\phi(m)}\pi(x) + \mathrm{O}\left(x \exp\left(-C(A)\sqrt{\log x}\right)\right).$$

THEOREM 8 (Conditional Effective Dirichlet's Theorem). *$\forall m \leq \frac{x^{\frac{1}{2}}}{(\log x)^3}$ and $\forall a$ with $(a, m) = 1$, GRH (for Dirichlet L-functions) is equivalent to*

$$\pi(x, m, a) = \frac{1}{\phi(m)}\pi(x) + \mathrm{O}\left(x^{\frac{1}{2}} \log(mx)\right).$$

An immediate question to ask is whether similar statements hold in the general setting of the Chebotarev Density Theorem. For this, answers were obtained by Lagarias and Odlyzko in the 1970s, using analytic methods in *algebraic number theory:*

THEOREM 9 (Effective Chebotarev Density Theorem [38]). *For a finite, Galois extension $K/\mathbb{Q}$ and $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$ a conjugacy class, we have that*

(i) *there exist positive constants C_1 and C_2, with C_1 effective and C_2 absolute, such that, if*

$$\sqrt{\frac{\log x}{[K:\mathbb{Q}]}} \geq C_2 \max\left(\log|\operatorname{disc}(K/\mathbb{Q})|, |\operatorname{disc}(K/\mathbb{Q})|^{\frac{1}{[K:\mathbb{Q}]}}\right),$$

then

$$\pi_C(x, K/\mathbb{Q}) = \frac{|C|}{[K:\mathbb{Q}]}\pi(x) + \mathrm{O}\left(|\tilde{C}|\, x \exp\left(-C_1\sqrt{\frac{\log x}{[K:\mathbb{Q}]}}\right)\right),$$

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

(ii) *for any $\frac{1}{2} \leq \delta < 1$, the δ-quasi-GRH for the Dedekind zeta function ζ_K of K (that is, ζ_K admits a zero-free region of $\mathrm{Re}(s) > \delta$) is equivalent to*

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

Another immediate question to ask is what statements hold for $\pi(x, m, a)$ for larger m, and, in more generality, what statements hold for $\pi_C(x, K/\mathbb{Q})$ for sufficiently large families of number fields K (note that what large means needs to be clarified).

Brun's work from the second decade of the 1900s marked the birth of *sieve methods* and led to important advances towards answering the above question in the classical context of primes in arithmetic progressions:

THEOREM 10 (The Brun-Titchmarsh Theorem, 1930s). *$\forall\ \varepsilon > 0$, $\forall\ m \leq x^{1-\varepsilon}$ and $\forall a$ with $(a, m) = 1$,*

$$\pi(x, m, a) \ll \frac{x}{\phi(m)\log(x/m)}.$$

THEOREM 11 (The Barban-Davenport-Halberstam Theorem, 1960s). *$\forall A > 0$ and $\forall\ \frac{x}{(\log x)^A} \leq Q \leq x$,*

$$\sum_{m \leq Q}\sum_{(a,m)=1}\left|\pi(x, m, a) - \frac{1}{\phi(m)}\,\pi(x)\right|^2 \ll Q\, x\, \log x.$$

THEOREM 12 (The Bombieri-Vinogradov Theorem, 1960s). $\forall A > 0\ \exists B > 0$ *such that*

$$\sum_{m \leq \frac{x^{\frac{1}{2}}}{(\log x)^B}} \max_{y \leq x} \max_{(a,m)=1} \left| \pi(y, m, a) - \frac{1}{\phi(m)}\, \pi(y) \right| \ll \frac{x}{(\log x)^A}.$$

In the context of the Chebotarev Density Theorem, the question of understanding $\pi_C(x, K/\mathbb{Q})$ for ranges larger than the ones of Theorem 9 is mostly open. In Sections 7–9, we will present some answers when K belongs to the family of division fields defined by an elliptic curve.

The study of primes is much richer and involved than what we have recalled so briefly; regrettably, for brevity, we left out many outstanding pieces of work. For a classical introduction to this field, we refer the reader to [20] and [31], while for more recent accounts, we refer the reader to [17,26] and [34]. Our presentation has focused on one flavour of the study of primes that we wish to echo in the arithmetic-geometric context of elliptic curves, as follows.

3. ELLIPTIC CURVES

An **elliptic curve** E **over a field** K is a smooth, projective curve, defined over K, of genus 1, and having a fixed K-rational point $\mathcal{O} \in E(K)$, called the **point at infinity** of E. The set of K-rational points $E(K)$ is endowed with a group law defined through the chord-tangent method. With respect to this law, $E(K)$ becomes an abelian group.

In what follows, we recall the most basic properties of elliptic curves. We refer the reader to [53] and [55] for a thorough introduction, including proofs and original references. For properties not covered in these texts, we provide references ourselves.

For a field extension L/K, L**-morphisms between elliptic curves** E/K and E'/K are morphisms $E \longrightarrow E'$, defined over L, that map $\mathcal{O} \in E$ to $\mathcal{O} \in E'$; the ring of L-endomorphisms of E is denoted by $\mathrm{End}_L(E)$, and the ring of L-automorphisms of E is denoted by $\mathrm{Aut}_L(E)$.

When $\mathrm{char}\, K \neq 2, 3$, an elliptic curve E/K is expressed as a **Weierstrass equation**

$$E_{a,b} : y^2 = x^3 + ax + b, \tag{3}$$

with $a, b \in K$ and $\Delta_E = \Delta_{a,b} := -16\left(4a^3 + 27b^2\right) \neq 0$.

Associated to an elliptic curve E/K, and in particular to a Weierstrass equation (3), we have the j-invariant $j_E = j_{a,b} := -1728\frac{4a^3}{\Delta_{a,b}}$, which encodes

the $\overline{K}$-isomorphism class of E: two elliptic curves $E_{a,b}/K$, $E_{a',b'}/K$ are $\overline{K}$-isomorphic if and only if $j_{a,b} = j_{a',b'}$, *i.e.* if and only if

$$\exists\, u \in \overline{K}^{\times} \text{ such that } a = u^4 a' \text{ and } b = u^6 b'. \tag{4}$$

Furthermore, there is an isomorphism from $E_{a,b}$ to $E_{a',b'}$ defined over $K(u)$. When $K = \mathbb{F}_p$, one obtains that

$$\text{(5)}\quad \text{the number of elliptic curves } E_{a',b'} \text{ which are } \mathbb{F}_p\text{-isomorphic to } E_{a,b} \text{ equals } \frac{p-1}{\left|\mathrm{Aut}_{\overline{\mathbb{F}}_p}(E_{a,b})\right|}.$$

The algebraic structure of the ring of endomorphisms of an elliptic curve has a deep impact on the arithmetic of the curve. We have the following structure theorems:

THEOREM 13 (Endomorphism Ring Classification Theorem). *Let E/K be an elliptic curve. Then the ring $\mathrm{End}_{\overline{K}}(E)$ is isomorphic to either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. Moreover,*

(i) *if $\mathrm{char}\, K = 0$, only the first two possibilities occur, in which case we say that E/K is* **without Complex Multiplication** *(non-CM) or, respectively,* **with Complex Multiplication** *(with CM);*

(ii) *if $\mathrm{char}\, K > 0$, then only the latter two possibilities occur, in which case we say that E/K is* **ordinary** *or, respectively,* **supersingular**.

THEOREM 14 (Automorphism Ring Classification Theorem). *Let E/K be an elliptic curve. If $\mathrm{char}\, K \neq 2, 3$, then there is a $\mathrm{Gal}(\overline{K}/K)$-module isomorphism*

$$\mathrm{Aut}_{\overline{K}}(E) \simeq \mu_n,$$

where

$$n := \begin{cases} 6 & \text{if } \ j_E = 0, \\ 4 & \text{if } \ j_E = 1728, \\ 2 & \text{if } \ j_E \neq 0, 1728, \end{cases}$$

and $\mu_n \subseteq \mathbb{C}^{\times}$ denotes the group of n-th roots of unity in the complex plane. In particular, if $p \geq 5$, $K = \mathbb{F}_p$, and $E = E_{a,b}$ is defined by (3) for some residue classes $a (\mathrm{mod}\, p)$, $b (\mathrm{mod}\, p)$, then

$$\left|\mathrm{Aut}_{\overline{\mathbb{F}}_p}(E)\right| = \begin{cases} 6 & \text{if } p|a \text{ and } p \equiv 1 (\mathrm{mod}\, 3), \\ 4 & \text{if } p|b \text{ and } p \equiv 1 (\mathrm{mod}\, 4), \\ 2 & \text{otherwise.} \end{cases}$$

From this point on, our main setting throughout the paper is that of

an elliptic curve $E/\mathbb{Q}$ defined by (3) with integer coefficients,
whose reductions modulo primes $p \nmid \Delta_E$ we denote by $\overline{E}/\mathbb{F}_p$.

We now recall basic properties of $E/\mathbb{Q}$ and $\overline{E}/\mathbb{F}_p$; in the next sections, we expand on these properties as guided by our investigations of Questions 1 and 2.

In the 1920s, Mordell proved that $E(\mathbb{Q})$ is a finitely generated abelian group:

THEOREM 15 (Mordell's Theorem). *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors},$$

where $r = r(E)$ is some non-negative integer, called **the arithmetic rank of** *$E/\mathbb{Q}$, and where $E(\mathbb{Q})_{tors}$ is the group of points of finite order in $E(\mathbb{Q})$, called* **the torsion subgroup of** *$E(\mathbb{Q})$.*

Several results about the points of finite order of $E/\mathbb{Q}$, proven over the course of the 20th century, have led to the complete classification of the group structure of the torsion subgroup:

THEOREM 16 (Rational Torsion Classification Theorem). *Let $E/\mathbb{Q}$ be an elliptic curve.*

(i) *(Mazur [39, 40])*
The torsion subgroup $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

$$\{\mathcal{O}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

Moreover, each of these groups occurs infinitely often.

(ii) *(Olson [43])*
Assuming that $E/\mathbb{Q}$ is with CM, the torsion subgroup $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

$$\{\mathcal{O}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

In practice, we can determine $E(\mathbb{Q})_{\text{tors}}$ relatively quickly by combining Theorem 16 with the following two results:

THEOREM 17 (Nagell-Lutz Rational Torsion Criterion). *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3). Let $P \in E(\mathbb{Q})_{tors} \backslash \{\mathcal{O}\}$ have coordinates $(x(P), y(P))$. Then*

$$x(P), y(P) \in \mathbb{Z}$$

and

$$\text{either} \quad 2P = \mathcal{O}, \quad \text{or} \quad y(P)^2 | 4a^3 + 27b^2.$$

THEOREM 18 (Reduction Modulo p Theorem). *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3). For a prime $p \nmid \Delta_E$, let*

$$\overline{E}/\mathbb{F}_p : y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p) \tag{6}$$

be the reduction of E modulo p. Define the reduction map

$$E(\mathbb{Q})_{tors} \longrightarrow \overline{E}(\mathbb{F}_p)$$
$$\mathcal{O} \mapsto \mathcal{O}$$
$$P = (x(P), y(P)) \mapsto \overline{P} = (x(P) (\mathrm{mod}\, p), y(P) (\mathrm{mod}\, p)).$$

If $p \nmid 2\Delta_E$, then the reduction map is an injective group homomorphism.

Typically (in a sense that needs to be clarified), $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial:

THEOREM 19 (Average Rational Torsion Theorem [29]). *For $x > 0$, consider the family $\mathcal{C}(x^2, x^3)$ of $\mathbb{Q}$-isomorphism classes of elliptic curves $E = E_{a,b}$ defined by (3) with $a, b \in \mathbb{Z}$ and $|a| \leq x^2, |b| \leq x^3$. Then*

$$\frac{1}{|\mathcal{C}(x^2, x^3)|} \# \left\{ E \in \mathcal{C}(x^2, x^3) : E(\mathbb{Q})_{tors} \neq \{\mathcal{O}\} \right\} \ll \frac{1}{x^2}.$$

Remark 20. The "almost all" statement above also holds in a one-parameter sense, as proven in [14] and [12].

The study of the arithmetic rank $r = r(E)$ is the focus of major ongoing research on both the algebraic and analytic side of arithmetic geometry. Already in 1901, Poincaré [44] asked for the range of possible values of r, but, to this day, it is still unknown whether r is bounded. In practice, for an elliptic curve $E/\mathbb{Q}$ defined by (3) with a, b moderate in size, there are algorithms to compute $r(E)$ successfully. However, to ensure in general that the algorithms terminate is an open problem that relates to the celebrated Birch & Swinnerton-Dyer Conjecture, formulated in the 1960s [8]. Briefly, the sum

$$\sum_p \frac{|\overline{E}(\mathbb{F}_p)|}{p}$$

relates to the behaviour of the logarithmic derivative of the Hasse-Weil zeta function of E at $s = 1$, and this relates to the value of the L-function $L(E, s)$ of E at $s = 1$; by the Birch & Swinnerton-Dyer Conjecture, this, in turn, relates to the arithmetic rank of $E(\mathbb{Q})$: $r(E)$ equals the **analytic rank** $r_{\mathrm{an}}(E) := \mathrm{ord}_{s=1} L(E, s)$.

Typically (again in a sense that needs to be clarified), the rank of $E/\mathbb{Q}$ is small:

THEOREM 21 (Average Rank Theorem). *For $x > 0$, consider the family $\mathcal{C}(x^2, x^3)$ of $\mathbb{Q}$-isomorphism classes of elliptic curves $E = E_{a,b}$ defined by (3) with $a, b \in \mathbb{Z}$ and $|a| \leq x^2, |b| \leq x^3$. Then*

(i) *(Bhargava – Shankar [7])*

$$\limsup_{x\to\infty} \frac{1}{|\mathcal{C}(x^2,x^3)|} \sum_{E\in\mathcal{C}(x^2,x^3)} r(E) < \frac{885}{1000};$$

(ii) *(Young [59])*

$$\limsup_{x\to\infty} \frac{1}{|\mathcal{C}(x^2,x^3)|} \sum_{E\in\mathcal{C}(x^2,x^3)} r_{an}(E) \leq \frac{25}{14}.$$

Remark 22. "Almost all" statements such as the ones above also hold in other senses; see the references in Poonen's survey [45] for more on this topic.

In summary, on one hand, knowledge about the reductions $\overline{E}/\mathbb{F}_p$ – more precisely, about *finitely many* groups $\overline{E}(\mathbb{F}_p)$ – relates to the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$; on the other hand, knowledge about the reductions $\overline{E}/\mathbb{F}_p$ – more precisely, about *infinitely many* groups $\overline{E}(\mathbb{F}_p)$ – relates to the arithmetic rank $r(E)$ of $E/\mathbb{Q}$. Two emerging questions arise:

Question 23. Given an elliptic curve $E/\mathbb{Q}$ and a prime $p \nmid \Delta_E$, what is the group structure of $\overline{E}(\mathbb{F}_p)$?

Question 24. Given an elliptic curve $E/\mathbb{Q}$ and a prime $p \nmid \Delta_E$, what is the group order of $\overline{E}(\mathbb{F}_p)$?

We will answer these questions in Section 5.

4. DIVISION FIELDS

In exploring the properties of the reductions modulo primes of an elliptic curve $E/\mathbb{Q}$, a key feature is the way the arithmetic of $\overline{E}/\mathbb{F}_p$ relates to that of $E/\mathbb{Q}$. This feature is encoded in the Artin symbol ("the Frobenius") at p in a division field of E. We review its main properties below.

For every integer $m \geq 1$, we let $E[m]$ be the group of m-division points of $E(\overline{\mathbb{Q}})$, *i.e.*

$$E[m] := \left\{P \in E\left(\overline{\mathbb{Q}}\right) : mP = \mathcal{O}\right\}.$$

This is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2, acted on by the absolute Galois group $G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The group action gives rise to a Galois representation

$$\varphi_{E,m} : G_{\mathbb{Q}} \longrightarrow \text{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

defined by restricting $\sigma \in G_{\mathbb{Q}}$ to $E[m]$ and by composing with an isomorphism

$$\text{Aut}(E[m]) \simeq \text{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Taking the inverse limit over all m (ordered by divisibility) and choosing bases compatibly leads to a continuous Galois representation

$$\varphi_E : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}})$$

and to its projections

$$\varphi_{E,m^\infty} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_m).$$

Here, $\hat{\mathbb{Z}}$ denotes the inverse limit over all m of the rings $\mathbb{Z}/m\mathbb{Z}$, and, using the isomorphism $\hat{\mathbb{Z}} \simeq \prod_{\ell} \mathbb{Z}_\ell$ given by the Chinese Remainder Theorem, $\mathbb{Z}_m$ denotes the quotient ring of $\hat{\mathbb{Z}}$ corresponding to $\prod_{\ell | m} \mathbb{Z}_\ell$.

In the language of these representations, we have

$$\mathbb{Q}(E[m]) = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\varphi_{E,m}} \text{ and } \mathbb{Q}(E_{\mathrm{tors}}) := \bigcup_{m \geq 1} \mathbb{Q}(E[m]) = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\varphi_E}.$$

THEOREM 25. *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3). Let $m \geq 1$ be an integer.*

(i) *(The Néron-Ogg-Shafarevich Criterion)*
If p ramifies in $\mathbb{Q}(E[m])/\mathbb{Q}$, then $p | m\Delta_E$.

(ii) *(Consequences to the existence of the Weil pairing)*
Denoting by ζ_m a primitive m-th root of unity, we have $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m])$. In particular, for a prime $p \nmid m\Delta_E$, if p splits completely in $\mathbb{Q}(E[m])$, then $p \equiv 1 (\mathrm{mod}\, m)$.

THEOREM 26 (Open Image Theorem for CM Elliptic Curves [56,57]). *Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \ncong \mathbb{Z}$. Then:*

(i) *$\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is an order O in an imaginary quadratic field K, necessarily of class number 1;*

(ii) *denoting by $\widehat{O} := \varprojlim^{m} O/mO$, $\mathbb{Q}(E_{tors})$ is a free $\widehat{O}$-module of rank 1, acted on by $G_K := \mathrm{Gal}\left(\overline{K}/K\right)$, and the representation*

$$\varphi_E|_{G_K} : G_K \longrightarrow \mathrm{GL}_1\left(\widehat{O}\right) = \left(\widehat{O}\right)^\times \tag{7}$$

has open image, that is,

$$\left| \left(\widehat{O}\right)^\times : \varphi_E|_{G_K}(G_K) \right| < \infty.$$

In particular, there exists a smallest integer $m_E \geq 1$ such that for each $m \geq 1$,

$$\mathrm{Gal}(K(E[m])/K) \simeq \mathrm{pr}^{-1}\left(\mathrm{Gal}(K(E[\gcd(m, m_E)])/K)\right),$$

where $\mathrm{pr} : (O/mO)^\times \longrightarrow (O/\gcd(m, m_E)\, O)^\times$ is the natural projection.

COROLLARY 27. *Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq O \not\simeq \mathbb{Z}$. With notation as above, for any integer $m \geq 1$, written uniquely as $m = m_1 m_2$ for some integers m_1, m_2 with $(m_1, m_E) = 1$ and $m_2 | m_E^{\infty}$, we have*

$$\mathrm{Gal}(K(E[m])/K) \simeq (O/m_1 O)^{\times} \times H_{m_2}$$

for some $H_{m_2} \leq (O/m_2 O)^{\times}$.

THEOREM 28 (Open Image Theorem for non-CM Elliptic Curves [48]). *Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. Then φ_E has open image, that is,*

$$\left|\mathrm{GL}_2\left(\hat{\mathbb{Z}}\right) : \varphi_E(G_{\mathbb{Q}})\right| < \infty.$$

In particular, there exists a smallest integer $m_E \geq 1$ such that

$$\varphi_E(G_{\mathbb{Q}}) = \mathrm{pr}^{-1}(\varphi_{E,m_E}(G_{\mathbb{Q}})),$$

where $\mathrm{pr} : \mathrm{GL}_2\left(\hat{\mathbb{Z}}\right) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$ is the natural projection.

COROLLARY 29. *Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. With notation as above, for any integer $m \geq 1$, written uniquely as $m = m_1 m_2$ for some integers m_1, m_2 with $(m_1, m_E) = 1$ and $m_2 | m_E^{\infty}$, we have*

$$\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z}) \times H_{m_2}$$

for some $H_{m_2} \leq \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z})$.

A useful consequence to the above two open image results is:

PROPOSITION 30. *Let $E/\mathbb{Q}$ be an elliptic curve. Define*

$$\gamma := \begin{cases} 1 & \text{if } \mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}, \\ 2 & \text{if } \mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}. \end{cases}$$

Then, for any integer $m \geq 1$,

$$\frac{m^{\frac{4}{\gamma}}}{\log\log m} \ll_E [\mathbb{Q}(E[m]) : \mathbb{Q}] \ll m^{\frac{4}{\gamma}}.$$

We conclude this section with a few words about the maximal image of φ_E.

LEMMA 31 ([48], Section 5.5). *Let $E/\mathbb{Q}$ be an elliptic curve. There exists a subgroup $H_E < \mathrm{GL}_2\left(\hat{\mathbb{Z}}\right)$ such that $\left|\mathrm{GL}_2\left(\hat{\mathbb{Z}}\right) : H_E\right| = 2$ and $\varphi_E(G_{\mathbb{Q}}) \leq H_E$.*

In particular, there exists no elliptic curve $E/\mathbb{Q}$ for which $|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})| = 1$ for all integers $m \geq 1$. Rather, the best we can hope for is captured in the following definition:

Definition 32. An elliptic curve $E/\mathbb{Q}$ is called a **Serre curve** if

$$|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})| \leq 2 \quad \forall m \geq 1.$$

It is useful to know:

Proposition 33. *Let $E/\mathbb{Q}$ be a Serre curve with Weierstrass equation (3). Then*

(i) $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$;

(ii) $E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$;

(iii) $m_E = \begin{cases} 2\,|(\Delta_E)_{sf}| & \text{if } (\Delta_E)_{sf} \equiv 1 (\mathrm{mod}\, 4), \\ 4\,|(\Delta_E)_{sf}| & \text{otherwise,} \end{cases}$

where $(\Delta_E)_{sf}$ denotes the squarefree part of Δ_E.

While deciding whether an elliptic curve is a Serre curve is a difficult task in practice, Serre curves not only exist in abundance, but they dominate the pool of elliptic curves! Indeed, typically (in a sense that needs to be clarified), an elliptic curve $E/\mathbb{Q}$ is a Serre curve:

Theorem 34 (Serre Curves in Families). *For $x > 0$, consider the family $\mathcal{C}(x^2, x^3)$ of $\mathbb{Q}$-isomorphism classes of elliptic curves $E = E_{a,b}$ defined by (3) with $a, b \in \mathbb{Z}$ and $|a| \leq x^2, |b| \leq x^3$. Then*

(i) *(Jones [36])*

$$\frac{1}{|\mathcal{C}(x^2, x^3)|} \# \left\{E \in \mathcal{C}(x^2, x^3) : E \text{ is not a Serre curve}\right\} \ll \frac{(\log x)^c}{x}$$

where $c > 0$ is an explicit, absolute constant;

(ii) *(Radakrishnan [46])*
$\forall\, \varepsilon > 0$,

$$\frac{1}{|\mathcal{C}(x^2, x^3)|} \# \left\{E \in \mathcal{C}(x^2, x^3) : E \text{ is not a Serre curve}\right\} = C\frac{1}{x^2} + \mathrm{O}_\varepsilon\left(\frac{1}{x^{3-\varepsilon}}\right),$$

where $C > 0$ is an explicit, absolute constant.

While Radakrishnan's Theorem is stronger than Jones', the latter suffices for the proof of part (ii) of Theorem 52; see Section 9.

Remark 35. The "almost all" statements above also hold in a one-parameter sense, as proven in [12].

5. REDUCTIONS

For $E/\mathbb{Q}$ an elliptic curve and $p \nmid \Delta_E$, we now summarize notation and properties associated to the pair (E, p). We define the integer

$$a_p = a_p(E) := -\sum_{x (\mathrm{mod}\, p)} \left(\frac{x^3 + ax + b}{p} \right) \tag{8}$$

and observe that

$$|\overline{E}(\mathbb{F}_p)| = p + 1 - a_p. \tag{9}$$

We define the polynomial

$$P_{E,p}(X) := X^2 - a_p X + p \in \mathbb{Z}[X] \tag{10}$$

and, writing its irreducible factorization as

$$P_{E,p}(X) = (X - \pi_p)(X - \pi_p') \in \mathbb{C}[X],$$

we observe that

$$\begin{aligned} \pi_p + \pi_p' &= a_p, \\ \pi_p \cdot \pi_p' &= p. \end{aligned}$$

THEOREM 36 (Fundamental Properties of the Frobenius of E mod p). *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3) and let $p \nmid \Delta_E$. With the above notation, we have:*

(i) $|a_p| < 2\sqrt{p}$, $\pi_p' = \overline{\pi}_p$, *and* $|\pi_p| = \sqrt{p}$;

(ii) π_p *may be identified with the p-th power Frobenius endomorphism*

$$\begin{aligned} \overline{E}\left(\overline{\mathbb{F}}_p\right) &\longrightarrow \overline{E}\left(\overline{\mathbb{F}}_p\right) \\ (x, y) &\mapsto (x^p, y^p) \\ \mathcal{O} &\mapsto \mathcal{O} \end{aligned}$$

and this identification gives rise to the ring embeddings

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_p] \subseteq \mathrm{End}_{\mathbb{F}_p}(\overline{E});$$

(iii) $\mathbb{Z}[\pi_p]$ *and* $\mathrm{End}_{\mathbb{F}_p}(\overline{E})$ *are $\mathbb{Z}$-orders in the ring of integers $O_{\mathbb{Q}(\pi_p)}$ of the imaginary quadratic field $\mathbb{Q}(\pi_p)$.*

As a consequence, there exist integers $c_p, c_p' \geq 1$ such that

$$\begin{aligned} \mathbb{Z}[\pi_p] &= \mathbb{Z} + c_p O_{\mathbb{Q}(\pi_p)}, \\ \mathrm{End}_{\mathbb{F}_p}(\overline{E}) &= \mathbb{Z} + c_p' O_{\mathbb{Q}(\pi_p)}, \\ c_p' &\mid c_p. \end{aligned}$$

Denoting the discriminant of the order $\mathrm{End}_{\mathbb{F}_p}(\overline{E})$ by Δ_p, we observe that it relates to the above data through the relation

$$\Delta_p = \frac{a_p^2 - 4p}{b_p^2},$$

where

$$b_p := \frac{c_p}{c_p'}.$$

Since $\Delta_p \equiv 0, 1 (\mathrm{mod}\, 4)$), let us also define the integer

$$\delta_p := \begin{cases} 0 & \text{if } \Delta_p \equiv 0 (\mathrm{mod}\, 4), \\ 1 & \text{if } \Delta_p \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

THEOREM 37 (Global Characterization of Frobenius in Division Fields [23]). *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3) and let $p \nmid \Delta_E$. Then the integral matrix*

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

when reduced modulo any integer m coprime to p, represents the class of the Artin symbol $\left(\frac{\mathbb{Q}(E[m])/\mathbb{Q}}{p}\right)$ in $\varphi_{E,m}(G_{\mathbb{Q}})$.

As an immediate corollary, we obtain:

THEOREM 38 (Group Structure of E mod p). *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3) and let $p \nmid \Delta_E$. Then there exist uniquely determined integers $d_{1,p}, d_{2,p} \geq 1$, possibly equal to 1, such that*

$$\begin{aligned} \overline{E}(\mathbb{F}_p) &\simeq \mathbb{Z}/d_{1,p}\mathbb{Z} \times \mathbb{Z}/d_{2,p}\mathbb{Z}, \\ d_{1,p} &\mid d_{2,p}. \end{aligned}$$

Moreover,

$$\begin{aligned} d_{1,p} &= \gcd\left(b_p, \frac{a_p + b_p\delta_p}{2} - 1\right), \\ d_{2,p} &= \frac{p + 1 - a_p}{d_{1,p}}. \end{aligned}$$

With this, we have answered both Questions 23 and 24. Related to our original guiding Questions 1 and 2, we also recall:

THEOREM 39 (Exponent Growth Theorem [47]). *Let $E/\mathbb{Q}$ be an elliptic curve defined by (3) and let $p \nmid \Delta_E$. Assume that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. Then, with notation as in Theorem 38,*

$$\frac{d_{2,p}}{\sqrt{p}} \gg_E \frac{\log p}{(\log\log p)^2}.$$

We might now conclude that the group structure and the growth of the exponent of $\overline{E}(\mathbb{F}_p)$ do not indicate strong similarities with those of $\mathbb{F}_p^\times$. This, however, is not the whole story, and we shall unravel the missing pieces in the next sections.

6. CYCLICITY QUESTIONS, HEURISTICS, AND UPCOMING CHALLENGES

It is time to formulate more explicit versions of the two guiding Questions 1 and 2, as promised at the end of Section 1.

CONJECTURE 40 (Cyclicity Conjecture). *Let $E/\mathbb{Q}$ be an elliptic curve. Then either $\mathbb{Q}(E[2]) = \mathbb{Q}$, in which case*

$$\#\{p \le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \ll_E 1,$$

or $\mathbb{Q}(E(2)) \neq \mathbb{Q}$, in which case there exists a constant $C_{cyclic}(E) > 0$ such that

$$\#\{p \le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \sim C_{cyclic}(E) \cdot \pi(x).$$

CONJECTURE 41 (Exponent Growth Conjecture). *Let $E/\mathbb{Q}$ be an elliptic curve. Then, for any increasing function $f : \mathbb{R} \longrightarrow (0, \infty)$ with $\lim_{x\to\infty} f(x) = \infty$,*

$$\#\left\{p \le x : d_{2,p} > \frac{|\overline{E}(\mathbb{F}_p)|}{f(p)}\right\} \sim \pi(x).$$

For the rest of the section, let us discuss an approach towards the Cyclicity Conjecture. The starting point is the following consequence to Theorem 37:

LEMMA 42 (Cyclicity Criterion). *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3) and let $p \nmid \Delta_E$. Then:*

(i) *for any prime $\ell \neq p$, $\overline{E}(\mathbb{F}_p) \supseteq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ if and only if p splits completely in $\mathbb{Q}(E[\ell])$;*

(ii) *the group $\overline{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in $\mathbb{Q}(E[\ell])$ for any prime $\ell \neq p$.*

With this criterion in hand, we set the following *sieve problem*:

- we are given
  - an elliptic curve $E/\mathbb{Q}$;
  - a real number $x > 0$ (to be thought of as approaching ∞);
  - a parameter $z = z(x) > 0$ (to be thought of as growing with x);
  - $\mathcal{A} := \{p \le x : p \nmid \Delta_E\}$;
  - $\mathcal{A}_\ell := \{p \in \mathcal{A} : p \neq \ell, p \text{ splits completely in } \mathbb{Q}(E[\ell])\}$, for each prime $\ell < z$.

- we want to estimate
$$\left| \mathcal{A} \setminus \bigcup_{\ell \leq z} \mathcal{A}_\ell \right|.$$
Note that, by the Inclusion-Exclusion Principle,
$$\left| \mathcal{A} \setminus \bigcup_{\ell \leq z} \mathcal{A}_\ell \right| = \sum_{m \leq m(x)} \mu(m) \left| \mathcal{A}_m \right|,$$
where $\mu(m)$ is the Möbius function of m, $\mathcal{A}_m := \bigcap_{\ell | m} \mathcal{A}_\ell$, and m are positive, squarefree integers in a suitable range $[1, m(x)]$ defined by $z(x)$.

Rephrased, the cyclicity problem becomes the sieve problem

$$\#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} = \sum_{m \leq m(x)} \mu(m) \cdot \#\{p \leq x : p \text{ splits completely in } \mathbb{Q}(E[m])\}. \tag{11}$$

Based on this formula and reasoning *heuristically* via the Chebotarev Density Theorem, it is natural to predict that
$$\#\left\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\right\} \sim \left(\sum_{m \geq 1} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} \right) \pi(x).$$
This prediction is supported by numerical evidence performed on over 300 elliptic curves with $x = 10^5$; see the upcoming [13].

Note that two immediate crucial points have been completely overlooked:

(Point 1) We have ignored the relation between $m(x)$ and the parameter x.
(Point 2) We have summed the main terms of the asymptotic formulae provided by the Chebotarev Density Theorem without paying any attention to the accumulation of error terms.

Let us look at these points more closely.

(Point 1bis). By Lemma 42, a prime p splits completely in $\mathbb{Q}(E[m])$ if and only if $\overline{E}(\mathbb{F}_p)$ contains two copies of $\mathbb{Z}/m\mathbb{Z}$. Consequently, for such a p we have $m^2 | p + 1 - a_p$. Recalling that $|a_p| < 2\sqrt{p}$, we deduce that $m < \sqrt{p} + 1$. Hence we may take
$$m(x) := \sqrt{x} + 1. \tag{12}$$

(Point 2bis). By the conditional Effective Chebotarev Density Theorem (part (ii) of Theorem 9) and the properties of the division fields $\mathbb{Q}(E[m])$ (part (i) of Theorem 25 and Proposition 30), under GRH we obtain

$$(13)\quad \#\left\{p \le x : p \text{ splits completely in } \mathbb{Q}(E[m])\right\} = \frac{1}{[\mathbb{Q}(E[m]) : \mathbb{Q}]}\pi(x) + \mathrm{O}_E\left(x^{\frac{1}{2}}\log(mx)\right).$$

Combining these two observations, the immediate emerging estimate of the accumulated error term is:

$$\left|\#\left\{p \le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\right\} - \sum_{m \le \sqrt{x}+1} \frac{1}{[\mathbb{Q}(E[m]) : \mathbb{Q}]}\pi(x)\right| \ll x \log x.$$

Unfortunately, with such a raw reasoning, we have reached a triviality; and a more refined analysis is thus needed!

To conclude, our analysis requires a better understanding of the division fields $\mathbb{Q}(E[m])$, in two aspects:

- the (sum of the) main terms in (13);
- the (sum of the) error terms in (13).

These shall be discussed in the next sections.

7. CYCLICITY: ASYMPTOTIC

The heuristical reasoning towards Conjecture 40, outlined in Section 7, can be morphed into a proof. This was achieved for the first time by Serre [49], under GRH, via a method inspired by Hooley's conditional proof of Artin's Primitive Root Conjecture. After Serre, Cojocaru and Murty obtained several new proofs of Conjecture 40, conditional and unconditional, and highlighted the growth of the emerging error terms as functions of x and of E; see [9,10,16,42].

The essence of these proofs, which allows for overcoming the insufficiency of the Chebotarev Density Theorem, may be rephrased as follows:

PROPOSITION 43. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $x, y > 0$ with $y = y(x) \le \sqrt{x}+1$, growing with x.*

(i) *Under no additional assumptions, we have*

$$\sum_{m>y} \#\{p \le x : p \text{ splits completely in } \mathbb{Q}(E[m])\} \ll \frac{x^{\frac{3}{2}}}{y^2} + \frac{x}{y} + \sqrt{x}\log\frac{x}{y} + \sqrt{x}.$$

(ii) *Assuming $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, we have*

$$\sum_{m>y} \#\{p \le x : p \text{ splits completely in } \mathbb{Q}(E[m])\} \ll \frac{x}{y} + \sqrt{x}\log x.$$

Proof. A proof of part (i) appears in [9, pp. 343–344]; see also [16, p. 613]. A proof of part (ii) appears in [10, p. 2569]; see also [16, pp. 616–618]. We outline the proof of (i).

Applying part (ii) of Theorem 25, part (ii) of Theorem 36, part (i) of Lemma 42, and (12), followed by elementary estimates, we obtain

$$\begin{aligned}
&\sum_{m>y} \#\{p \le x : p \text{ splits completely in } \mathbb{Q}(E[m])\} \\
&= \sum_{y<m\le\sqrt{x}+1} \#\{p \le x : p \text{ splits completely in } \mathbb{Q}(E[m])\} \\
&\le \sum_{y<m\le\sqrt{x}+1} \#\{p \le x : p \equiv 1 (\mathrm{mod}\, m) \text{ and } p+1-a_p \equiv 0 (\mathrm{mod}\, m^2)\} \\
&\le \sum_{\substack{a\in\mathbb{Z}\setminus\{2\} \\ |a|\le 2\sqrt{x}}} \sum_{\substack{y<m\le\sqrt{x}+1 \\ m|a-2}} \sum_{\substack{p\le x \\ a_p=a \\ m^2|p+1-a}} 1 + \sum_{y<m\le\sqrt{x}+1} \sum_{\substack{p\le x \\ a_p=2 \\ m^2|p+1-a}} 1 \\
&\ll \sum_{y<m\le\sqrt{x}+1} \left(\frac{x}{m^2}+1\right)\left(\frac{\sqrt{x}}{m}+1\right) + \sum_{y<m\le\sqrt{x}+1} \left(\frac{x}{m^2}+1\right) \\
&\ll \frac{x^{\frac{3}{2}}}{y^2} + \frac{x}{y} + \sqrt{x}\log\frac{x}{y} + \sqrt{x}. \quad \square
\end{aligned}$$

Combining this proposition with Chebotarev arguments, we obtain a "Chebotarev on average" type theorem:

THEOREM 44 (Cojocaru-Murty Splitting on Average Theorem). *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

(14)
$$\frac{1}{\sqrt{x}} \sum_{m\ge 1} \left(\#\{p \le x : p \textit{ splits completely in } \mathbb{Q}(E[m])\} - \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\pi(x) \right) = r(E,x),$$

where:

(i) *assuming a $\frac{3}{4}$-quasi GRH,*

$$r(E,x) = \mathrm{O}_E\left(\frac{x^{\frac{1}{2}}\log\log x}{(\log x)^2}\right);$$

(ii) *assuming GRH,*

$$r(E,x) = \mathrm{O}_E\left(x^{\frac{1}{3}}(\log x)^{\frac{2}{3}}\right);$$

(iii) *assuming* $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, *for any* $c > 0$,

$$r(E,x) = \mathrm{O}_{E,c}\left(\frac{x^{\frac{1}{2}}}{(\log x)^c}\right);$$

(iv) *assuming GRH and* $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$,

$$r(E,x) = \mathrm{O}_E\left(x^{\frac{1}{4}}(\log x)^{\frac{1}{2}}\right).$$

Proof. We sketch the proofs of parts (ii) and (iv). For part (i), proceed as in the proof of Theorem 1.2 of [9]. For part (iii), proceed as in the unconditional proof of the main theorem given in Section 6 of [42] (see also the follow-up [4]).

(ii) The main idea of the proof is to make use of the average over m. Recalling (12), the maximal range of m in the sum under consideration is $1 \leq m \leq \sqrt{x}+1$. While not large (compare it with the maximal range $1 \leq m \leq x$ for primes splitting completely in $\mathbb{Q}(\zeta_m)$), this range exceeds what can be tackled by a direct application of the Effective Chebotarev Density Theorem, even under GRH; see (13). To overcome this obstacle, choose a parameter $y = y(x) < \sqrt{x}+1$ and split the sum into two, according to whether $1 \leq m \leq y$ or $y < m \leq \sqrt{x}+1$.

Over the first range, we apply (13):

$$\sum_{m\leq y} \#\{p \leq x : p \text{ splits completely in } \mathbb{Q}(E[m])\} \tag{15}$$
$$= \sum_{m\leq y} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\pi(x) + \mathrm{O}_E\left(yx^{\frac{1}{2}}\log x\right);$$

this is the only place where we will be using GRH.

Over the second range, we apply part (i) of Proposition 43:

$$\sum_{y<m\leq\sqrt{x}+1} \#\{p \leq x : p \text{ splits completely in } \mathbb{Q}(E[m])\} \ll \frac{x^{\frac{3}{2}}}{y^2}+\frac{x}{y}+\sqrt{x}\log\frac{x}{y}+\sqrt{x}. \tag{16}$$

By choosing $y \asymp \left(\frac{x}{\log x}\right)^{\frac{1}{3}}$, we obtain

$$\sum_{m\leq\sqrt{x}+1} \#\{p \leq x : p \text{ splits completely in } \mathbb{Q}(E[m])\}$$
$$= \sum_{m\leq y} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\pi(x) + \mathrm{O}_E\left(x^{\frac{5}{6}}(\log x)^{\frac{2}{3}}\right).$$

By Proposition 30,

$$\sum_{m>y} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]} \ll \sum_{m>y} \frac{\log\log m}{m^{\frac{4}{\gamma}}} \ll \frac{\log\log x}{y^{\frac{4}{\gamma}-1}}. \tag{17}$$

This completes the proof of part (iii).

(iv) We proceed as above with the exception of using part (ii), instead of part (i), of Proposition 43, and of making the choice $y \asymp \left(\frac{x}{(\log x)^2}\right)^{\frac{1}{4}}$. □

Remark 45. To prove parts (i) and (iii) of Theorem 44, the sum over m is partitioned into two according to whether m is y-smooth or not, as in the classical "simple asymptotic sieve". This is the approach followed by Serre in [49]. In [16], Cojocaru and Murty noted that, under GRH, the simple asymptotic sieve approach is not necessary and that, instead, it suffices to partition the sum over m simply according to whether m is less than y or not; their approach is the one used to prove parts (ii) and (iv). While this is a very simple observation, it has two surprising consequences:

- significant improvements in the error terms;
- a departure from the approach on Artin's Primitive Root Conjecture, signaling a contrast between this classical conjecture and Conjecture 40.

We are now ready to present theoretical evidence towards Conjecture 40:

THEOREM 46 (Cojocaru-Murty-Serre Cyclicity Theorem [9, 16, 42, 49]). *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$\#\{p \le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} = \sum_{m\ge 1} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\pi(x) + \mathrm{O}\left(\sqrt{x}\cdot r(E,x)\right),$$

where $r(E,x)$ is as in Theorem 44, under the assumptions therein.

Proof. Starting from (11), we follow the approach from Theorem 44, with the only difference that $\mu(m)$ is preserved as such in the sum of the main terms (*i.e.* over the range m y-smooth, or over the range $m \le y$), and is estimated from above by 1 everywhere else. The original sources of the proofs are: [16] under GRH, [9] under $\frac{3}{4}$-quasi GRH, [42] unconditionally for $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$. See also [10,49] and [4]. □

Remark 47. It can be proven that the constant

$$C_{\mathrm{cyclic}}(E) := \sum_{m\ge 1} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}$$

is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$; see [16]. Calculations related to this constant appear in [13] and [16].

Methods similar to proving Theorems 44 and 46 can be employed to investigate Conjecture 41, leading to:

THEOREM 48 (Duke's Large Exponent Theorem [22]). *Let $E/\mathbb{Q}$ be an elliptic curve. Let $f : (0,\infty) \longrightarrow (0,\infty)$ be such that $\lim_{x\to\infty} f(x) = \infty$. Then*

$$\#\left\{p \le x : d_{2,p} \ge \frac{|\overline{E}(\mathbb{F}_p)|}{f(p)}\right\} \sim \pi(x) \tag{18}$$

provided any one of the following holds:

(i) $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$ *and* $f(x) \asymp x^{\frac{1}{4}}(\log x)^{\frac{1}{2}+\varepsilon} \quad \forall \varepsilon > 0$;

(ii) $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$ *and* $f(x) \asymp (\log x)^{1+\varepsilon} \quad \forall \varepsilon > 0$;

(iii) *GRH and* $f(x) \asymp (\log\log x)^{\frac{1}{3}+\varepsilon} \quad \forall \varepsilon > 0$.

Proof. We will present a proof that uses Proposition 43 and highlights the intimate relation between the cyclicity and the large exponent problems. Recalling that $d_{1,p}d_{2,p} = |\overline{E}(\mathbb{F}_p)|$, we deduce that proving (18) is equivalent to proving

$$\#\{p \le x : f(p) < d_{1,p}\} = \mathrm{o}(\pi(x)). \tag{19}$$

To do this, choose a parameter $z = z(x) > 0$, which grows with x and which shall be specified later. Define

$$g(z(x)) := \inf\{f(p) : z < p < x\},$$

which also grows with x, *i.e.* $\lim_{x\to\infty} g(z(x)) = \infty$. Then

(20)

$$\begin{aligned}\#\{p \le x : f(p) < d_{1,p}\} &= \#\{p \le z : f(p) < d_{1,p}\} + \#\{z < p \le x : f(p) < d_{1,p}\} \\ &\le \pi(z) + \sum_{g(z)\le m} \#\{p \le x : m | d_{1,p}\} \\ &< \frac{2z}{\log z} + \sum_{g(z)\le m\le\sqrt{x}+1} \#\{p \le x : p \text{ splits completely in } \mathbb{Q}(E[m])\}.\end{aligned}$$

(i) Using part (i) of Proposition 43 with $y = g(z)$, choosing $z \asymp \frac{x}{\log x}$, and recalling that $f(x) \asymp x^{\frac{1}{4}}(\log x)^{\frac{1}{2}+\varepsilon}$, we obtain (19).

(ii) Using part (ii) of Proposition 43 with $y = g(z)$, choosing $z \asymp \frac{x}{\log x}$, and recalling that $f(x) \asymp (\log x)^{1+\varepsilon}$, we obtain (19).

(iii) We assume GRH. To improve our results, we introduce a new parameter $y = y(x)$, which grows with x, satisfies $g(z) < y < \sqrt{x} + 1$, and shall be specified later. As in parts (i) and (ii), we choose $z \asymp \frac{x}{\log x}$. By part (ii) of the

Effective Chebotarev Density Theorem (where GRH is used) and by part (i) of Proposition 43 and (17) (which are unconditional), we obtain

$$\begin{aligned} & \sum_{g(z)\le m\le \sqrt{x}+1} \#\{p\le x : p \text{ splits completely in } \mathbb{Q}(E[m])\} \\ = & \sum_{g(z)\le m\le y} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\pi(x) + \mathrm{O}\left(yx^{\frac{1}{2}}\log x\right) + \mathrm{O}\left(\frac{x^{\frac{3}{2}}}{y^2}+\frac{x}{y}+\sqrt{x}\log x\right) \\ = & \mathrm{O}\left(\frac{\log\log x}{f(x)^3}\cdot\pi(x)\right) + \mathrm{O}\left(yx^{\frac{1}{2}}\log x\right) + \mathrm{O}\left(\frac{x^{\frac{3}{2}}}{y^2}+\frac{x}{y}+\sqrt{x}\log x\right). \end{aligned}$$

Recalling that $f(x)\asymp(\log\log x)^{\frac{1}{3}+\varepsilon}$ and choosing $y\asymp\left(\frac{x}{\log x}\right)^{\frac{1}{2}}$, we obtain (19). □

Remark 49. We refer the reader to [22] for a formulation of Theorem 48 with fewer conditions on $f(x)$.

Remark 50. Further applications of these methods have been pursued in several other works, including [1–3, 24, 27, 28, 37] and [58].

8. CYCLICITY: LOWER BOUND

While Conjecture 40 is known only conditionally for a non-CM elliptic curve, we have the following unconditional result:

THEOREM 51 (Gupta-Murty Cyclicity Lower Bound [30]). *Let $E/\mathbb{Q}$ be an elliptic curve. Assuming that $\mathbb{Q}(E[2])\neq\mathbb{Q}$, we have*

$$\#\{p\le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \gg \frac{x}{(\log x)^2}.$$

Proof. The main idea of the proof is to capture, among the primes $p\le x$ with $\overline{E}(\mathbb{F}_p)$ cyclic, a subset of primes in an arithmetic progression that contains at least $\frac{x}{(\log x)^2}$ primes.

To do this, recall from part (ii) of Lemma 42 that a prime p for which $\overline{E}(\mathbb{F}_p)$ is cyclic does not split completely in $\mathbb{Q}(E[2])$. By our hypothesis, the extension $\mathbb{Q}\subseteq\mathbb{Q}(E[2])$ is nontrivial, and since $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{\Delta_E})\subseteq\mathbb{Q}(E[2])$, it contains a nontrivial *abelian* extension of $\mathbb{Q}$. Thus there is an arithmetic progression $\alpha(\mathrm{mod}\, q)$ such that

$$p\equiv\alpha(\mathrm{mod}\, q) \;\Rightarrow\; p \text{ does not split completely in } \mathbb{Q}(E[2]). \tag{21}$$

With this progression in hand, we remark that a lower bound sieve argument in the style of Fouvry and Iwaniec [25] implies the existence of some $\varepsilon>0$ such that the set

$$\mathcal{S}_\varepsilon(x) := \Big\{p \le x : p \equiv \alpha (\mathrm{mod}\, q), \\ \text{all odd prime factors of } p-1 \text{ are distinct and greater than } x^{\frac{1}{4}+\varepsilon}\Big\}$$

satisfies

$$|\mathcal{S}_\varepsilon(x)| \gg \frac{x}{(\log x)^2}. \tag{22}$$

We now estimate the number of primes $p \in \mathcal{S}_\varepsilon(x)$ for which $\overline{E}(\mathbb{F}_p)$ is cyclic:

$$\begin{aligned} &\#\{p \le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \\ &\quad \ge \#\Big\{p \le x : p \text{ does not split completely in } \mathbb{Q}(E[\ell])\ \forall \ell \text{ and} \\ &\qquad \text{all odd prime factors of } p-1 \text{ are distinct and greater than } x^{\frac{1}{4}+\varepsilon}\Big\} \\ &\quad \ge \#\{p \in \mathcal{S}_\varepsilon(x) : p \text{ does not split completely in } \mathbb{Q}(E[\ell])\ \forall \ell \text{ odd}\} \\ &\quad = |\mathcal{S}_\varepsilon(x)| - \#\{p \in \mathcal{S}_\varepsilon(x) : p \text{ splits completely in } \mathbb{Q}(E[\ell]) \text{ for some } \ell \text{ odd}\}. \end{aligned} \tag{23}$$

To estimate the latter from above, we partition the primes p according to their Frobenius trace a_p. Proceeding similarly to the proof of part (i) of Proposition 43, we obtain that

$$\begin{aligned} &\#\{p \in \mathcal{S}_\varepsilon(x) : p \text{ splits completely in } \mathbb{Q}(E[\ell]) \text{ for some } \ell \text{ odd}\} \\ &\le \sum_{\substack{a \in \mathbb{Z} \\ |a| \le 2\sqrt{x}}} \sum_{3 \le \ell \le \sqrt{x}+1} \#\{p \in \mathcal{S}_\varepsilon(x) : a_p = a, p \text{ splits completely in } \mathbb{Q}(E[\ell])\}. \end{aligned} \tag{24}$$

Note that the primes ℓ under summation satisfy $\ell^2 | p+1-a$ and $\ell | p-1$, hence $\ell | a-2$. Since $p \in \mathcal{S}_\varepsilon(x)$, we must have that $a \ne 2$ and, moreover, that ℓ is determined by a for large x. Thus the double sum in (24) is

$$\ll \sum_{|a| \le 2\sqrt{x}} \left(\frac{x}{\ell_a^2} + 1\right) \ll x^{1-2\varepsilon}.$$

Using this estimate in (23), together with (22), we deduce that

$$\#\{p \le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \gg \frac{x}{(\log x)^2},$$

which completes the proof. □

9. CYCLICITY: AVERAGE

Further theoretical evidence towards Conjecture 40 is provided by:

THEOREM 52 (Banks-Shparlinski-Jones Cyclicity on Average Theorem). *For $A, B \ge 1$, consider the family $\mathcal{C}(A,B)$ of $\mathbb{Q}$-isomorphism classes of elliptic curves $E = E_{a,b}$ defined by (3) with $a, b \in \mathbb{Z}$ and $|a| \le A, |b| \le B$.*

(i) *((Banks-Shparlinski [6])*
Let $x > 0$, $\varepsilon > 0$, and $A = A(x), B = B(x)$ be such that

$$x^{\varepsilon} \leq A, B \leq x^{1+\varepsilon},$$
$$AB \geq x^{1+\varepsilon}.$$

Then

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{E \in \mathcal{C}(A,B)} \#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \sim C_{cyclic}^{average}\, \pi(x), \tag{25}$$

where

$$C_{cyclic}^{average} := \prod_{\ell} \left(1 - \frac{1}{\ell(\ell-1)(\ell^2-1)}\right).$$

(ii) *(Jones [35])*
Let $x > 0$ and $A = A(x), B = B(x)$ be such that

$$\lim_{x \to \infty} \frac{(\log A(x))^7 \cdot \log B(x)}{B(x)} = 0.$$

Then

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{E \in \mathcal{C}(A,B)} C_{cyclic}(E) \sim C_{cyclic}^{average}. \tag{26}$$

9.1. **Cyclicity: averaging the prime counting function**

We will outline the proof of a more general version of part (i) of Theorem 52, based on ideas that originate in [6]. Moreover, our presentation also draws inspiration from [5] and [15].

- To ensure no bias towards intrinsic features of the elements of $\mathcal{C}(A,B)$, we let

$$\mathcal{A} = (\alpha_a),\ \mathcal{B} = (\beta_b)$$

be arbitrary sequences of complex numbers supported on $|a| \leq A, |b| \leq B$, respectively, and we associate to each $E_{a,b} \in \mathcal{C}(A,B)$ the weight $\alpha_a \beta_b$. We set

$$|\mathcal{A}| := \sum_{|a| \leq A} \alpha_a, \qquad ||\mathcal{A}|| := \left(\sum_{|a| \leq A} |\alpha_a|^2 \tau(a)\right)^{\frac{1}{2}},$$
$$|\mathcal{B}| := \sum_{|b| \leq B} \beta_b, \qquad ||\mathcal{B}|| := \left(\sum_{|b| \leq B} |\beta_b|^2 \tau(b)\right)^{\frac{1}{2}},$$

where $\tau(\cdot)$ denotes the divisor function, and we note that, by the Cauchy-Schwarz Inequality,

$$|\mathcal{A}| \le ||\mathcal{A}||A^{\frac{1}{2}}, \quad |\mathcal{B}| \le ||\mathcal{B}||B^{\frac{1}{2}}.$$

- For a prime p and a pair of integers (a,b), we define

$$w_p(a,b) := \begin{cases} 1 & \text{if } p \nmid \Delta_{a,b} \text{ and } \overline{E}_{a,b}(\mathbb{F}_p) \text{ is cyclic,} \\ 0 & \text{otherwise.} \end{cases}$$

Our goal is to evaluate asymptotically the bilinear form

$$\mathcal{S}(\mathcal{A},\mathcal{B};x) := \sum_{|a|\le A} \sum_{\substack{|b|\le B \\ \Delta_{a,b}\neq 0}} \alpha_a \beta_b \sum_{p\le x} w_p(a,b), \tag{27}$$

or, rather, the bilinear form

$$\mathcal{S}^*(\mathcal{A},\mathcal{B};x) := \sum_{|a|\le A} \sum_{\substack{|b|\le B \\ \Delta_{a,b}\neq 0}} \alpha_a \beta_b \sum_{\substack{p\le x \\ p\nmid ab}} w_p(a,b), \tag{28}$$

related to the first via the relation

$$|\mathcal{S}(\mathcal{A},\mathcal{B};x) - \mathcal{S}^*(\mathcal{A},\mathcal{B};x)| \le \| \mathcal{A} \| \cdot \| \mathcal{B} \| . \tag{29}$$

We partition $\mathcal{C}(A,B)$ into subsets of curves according to their Weierstrass models modulo p. Note that, without any relevant loss, we may restrict the sum over $p \le x$ to primes $5 \le p \le x$. We obtain

$$\begin{aligned} \mathcal{S}^*(\mathcal{A},\mathcal{B},x) &= \sum_{5\le p\le x} \sum_{s(\mathrm{mod}\, p)}{}^{*} \sum_{t(\mathrm{mod}\, p)}{}^{*} \sum_{\substack{|a|\le A \\ a\equiv s(\mathrm{mod}\, p)}}{}^{*} \sum_{\substack{|b|\le B \\ b\equiv t(\mathrm{mod}\, p) \\ p\nmid \Delta_{a,b}}}{}^{*} \alpha_a\beta_b\, w_p(a,b) \\ &= \sum_{5\le p\le x} \sum_{s(\mathrm{mod}\, p)}{}^{*} \sum_{t(\mathrm{mod}\, p)}{}^{*} w_p(s,t) \sum_{\substack{|a|\le A \\ a\equiv s(\mathrm{mod}\, p)}}{}^{*} \sum_{\substack{|b|\le B \\ b\equiv t(\mathrm{mod}\, p) \\ p\nmid \Delta_{a,b}}}{}^{*} \alpha_a\beta_b \\ &=: \sum_{5\le p\le x} \sum_{s(\mathrm{mod}\, p)}{}^{*} \sum_{t(\mathrm{mod}\, p)}{}^{*} w_p(s,t)\ \gamma(s,t). \end{aligned}$$

Here, "$*$" next to the sigma sums signifies that we are only summing over invertible residue classes modulo p. The notation $\gamma(s,t)$ for the double sum over s and t was introduced for simplifying the exposition in the next step.

For each $p \ge 5$, we partition the set of Weierstrass models modulo p into $\mathbb{F}_p$-isomorphism classes. For this, recall that given pairs of residue classes $(s,t)(\mathrm{mod}\, p)$, $(s',t')(\mathrm{mod}\, p)$, the elliptic curves $E_{s,t}$, $E_{s',t'}$ are $\mathbb{F}_p$-isomorphic if and only if there exists $u(\mathrm{mod}\, p)$ invertible satisfying $s' \equiv su^4(\mathrm{mod}\, p)$ and $t' \equiv tu^6(\mathrm{mod}\, p)$. For ease of notation, we shall use $\widehat{(s,t)}$ for the coset of $(s,t)(\mathrm{mod}\, p)$

modulo $\mathbb{F}_p$-isomorphism, and $\hat{u}$ for the coset of $u (\mathrm{mod}\, p)$ modulo multiplication by ± 1. By Theorem 14, for a fixed $p \geq 5$ we obtain:

$$\sum_{s (\mathrm{mod}\, p)}{}^{*} \sum_{t (\mathrm{mod}\, p)}{}^{*} w_p(s,t)\ \gamma(s,t) = \sum_{\substack{\widehat{(s,t)} \\ p \nmid \Delta(s,t)}} \sum_{\hat{u}} w_p(su^4, tu^6)\ \gamma(su^4, tu^6)$$

$$= \sum_{\widehat{(s,t)}} w_p(s,t) \sum_{\hat{u}} \gamma(su^4, tu^6)$$

$$= \sum_{s (\mathrm{mod}\, p)}{}^{*} \sum_{t (\mathrm{mod}\, p)}{}^{*} w_p(s,t)\ \frac{|\mathrm{Aut}(E_{s,t})|}{p-1} \sum_{\hat{u}} \gamma(su^4, tu^6)$$

$$= \frac{1}{p-1} \sum_{s (\mathrm{mod}\, p)}{}^{*} \sum_{t (\mathrm{mod}\, p)}{}^{*} w_p(s,t) \sum_{u (\mathrm{mod}\, p)}{}^{*} \gamma(su^4, tu^6)$$

$$= \frac{1}{p-1} \sum_{s (\mathrm{mod}\, p)}{}^{*} \sum_{t (\mathrm{mod}\, p)}{}^{*} w_p(s,t) \sum_{u (\mathrm{mod}\, p)}{}^{*} \left(\sum_{\substack{|a| \leq A \\ a \equiv su^4 (\mathrm{mod}\, p)}}{}^{*} \alpha_a \right) \left(\sum_{\substack{|b| \leq B \\ b \equiv tu^6 (\mathrm{mod}\, p)}}{}^{*} \beta_b \right).$$

We use χ_1 and χ_2 to denote arbitrary Dirichlet characters modulo p, and χ_0 to denote the trivial character modulo p. Applying the orthogonality relations, we obtain:

$$\frac{1}{p-1} \sum_{s (\mathrm{mod}\, p)}{}^{*} \sum_{t (\mathrm{mod}\, p)}{}^{*} w_p(s,t) \sum_{u (\mathrm{mod}\, p)}{}^{*} \left(\sum_{\substack{|a| \leq A \\ a \equiv su^4 (\mathrm{mod}\, p)}}{}^{*} \alpha_a \right) \left(\sum_{\substack{|b| \leq B \\ b \equiv tu^6 (\mathrm{mod}\, p)}}{}^{*} \beta_b \right)$$

$$= \frac{1}{(p-1)^3} \sum_{s (\mathrm{mod}\, p)}{}^{*} \sum_{t (\mathrm{mod}\, p)}{}^{*} w_p(s,t) \sum_{u (\mathrm{mod}\, p)}{}^{*} \left(\sum_{\chi_1} \overline{\chi}_1(su^4) \sum_{|a| \leq A} \alpha_a \chi_1(a) \right) \left(\sum_{\chi_2} \overline{\chi}_2(tu^6) \sum_{|b| \leq B} \beta_b \chi_2(b) \right)$$

$$= \frac{1}{(p-1)^3} \sum_{s (\mathrm{mod}\, p)}{}^{*} \sum_{t (\mathrm{mod}\, p)}{}^{*} w_p(s,t) \sum_{\chi_1} \overline{\chi}_1(s) \sum_{\chi_2} \overline{\chi}_2(t) \left(\sum_{u (\mathrm{mod}\, p)}{}^{*} \overline{\chi}_1^4 \overline{\chi}_2^6(u) \right) \left(\sum_{|a| \leq A} \alpha_a \chi_1(a) \right) \left(\sum_{|b| \leq B} \beta_b \chi_2(b) \right)$$

$$= \frac{1}{(p-1)^2} \sideset{}{^*}\sum_{s(\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t(\mathrm{mod}\, p)} w_p(s,t) \sum_{\chi_1} \overline{\chi}_1(s) \sum_{\substack{\chi_2 \\ \chi_1^4\chi_2^6=\chi_0}} \overline{\chi}_2(t) \left(\sum_{|a|\le A} \alpha_a \chi_1(a)\right) \left(\sum_{|b|\le B} \beta_b \chi_2(b)\right)$$

$$= \frac{1}{(p-1)^2} \sum_{\chi_1} \sum_{\substack{\chi_2 \\ \chi_1^4\chi_2^6=\chi_0}} \left(\sideset{}{^*}\sum_{s(\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t(\mathrm{mod}\, p)} w_p(s,t)\, \overline{\chi}_1(s)\overline{\chi}_2(t)\right) \left(\sum_{|a|\le A} \alpha_a \chi_1(a)\right) \left(\sum_{|b|\le B} \beta_b \chi_2(b)\right).$$

We partition the character sum above into smaller character sums according to whether: $\chi_1 = \chi_2 = \chi_0$; $\chi_1 \neq \chi_0$, $\chi_2 = \chi_0$; $\chi_1 = \chi_0$, $\chi_2 \neq \chi_0$; $\chi_1 \neq \chi_0$, $\chi_2 \neq \chi_0$. More precisely, we write

$$\mathcal{S}^*(\mathcal{A},\mathcal{B},x) = \sum_{5\le p\le x} \frac{1}{(p-1)^2} \left(\sideset{}{^*}\sum_{s(\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t(\mathrm{mod}\, p)} w_p(s,t)\right)\left(\sum_{\substack{|a|\le A \\ p\nmid a}} \alpha_a\right)\left(\sum_{\substack{|b|\le B \\ p\nmid b}} \beta_b\right)$$

$$+ \sum_{5\le p\le x} \frac{1}{(p-1)^2} \sum_{\substack{\chi\neq\chi_0 \\ \chi^4=\chi_0}} \left(\sideset{}{^*}\sum_{s(\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t(\mathrm{mod}\, p)} w_p(s,t)\, \overline{\chi}(s)\right)\left(\sum_{|a|\le A} \alpha_a \chi(a)\right)\left(\sum_{\substack{|b|\le B \\ p\nmid b}} \beta_b\right)$$

$$+ \sum_{5\le p\le x} \frac{1}{(p-1)^2} \sum_{\substack{\chi\neq\chi_o \\ \chi^6=\chi_0}} \left(\sideset{}{^*}\sum_{s(\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t(\mathrm{mod}\, p)} w_p(s,t)\, \overline{\chi}(t)\right)\left(\sum_{\substack{|a|\le A \\ p\nmid a}} \alpha_a\right)\left(\sum_{|b|\le B} \beta_b \chi(b)\right)$$

$$+ \sum_{5\le p\le x} \frac{1}{(p-1)^2} \sum_{\chi_1\neq\chi_0} \sum_{\substack{\chi_2\neq\chi_0 \\ \chi_1^4\chi_2^6=\chi_0}} \left(\sideset{}{^*}\sum_{s(\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t(\mathrm{mod}\, p)} w_p(s,t)\, \overline{\chi}_1(s)\overline{\chi}_2(t)\right) \left(\sum_{|a|\le A} \alpha_a \chi_1(a)\right) \left(\sum_{|b|\le B} \beta_b \chi_2(b)\right)$$

and we denote each of these sums by

$$\mathcal{S}_0(\mathcal{A},\mathcal{B},x),\ \mathcal{S}_4(\mathcal{A},\mathcal{B},x),\ \mathcal{S}_6(\mathcal{A},\mathcal{B},x),\ \text{and}\ \mathcal{S}_\infty(\mathcal{A},\mathcal{B},x),$$

respectively. The main term is encoded in $\mathcal{S}_0(\mathcal{A},\mathcal{B},x)$.

Let us focus on $\mathcal{S}_4(\mathcal{A},\mathcal{B},x)$ and $\mathcal{S}_6(\mathcal{A},\mathcal{B},x)$. By trivially estimating $|w_p(s,t)|$ and $|\chi(s)|$, $|\chi(t)|$, we obtain

$$\mathcal{S}_4(\mathcal{A},\mathcal{B},x) \leq \sum_{5\leq p\leq x}\sum_{\substack{\chi\neq\chi_0\\ \chi^4=\chi_0}}\left|\sum_{|a|\leq A}\alpha_a\chi(a)\right|\left|\sum_{\substack{|b|\leq B\\ p\nmid b}}\beta_b\right|,$$

$$\mathcal{S}_6(\mathcal{A},\mathcal{B},x) \leq \sum_{5\leq p\leq x}\sum_{\substack{\chi\neq\chi_0\\ \chi^6=\chi_0}}\left|\sum_{\substack{|a|\leq A\\ p\nmid a}}\alpha_a\right|\left|\sum_{|b|\leq B}\beta_b\chi(b)\right|.$$

This leads to estimating sums of the form

$$\mathcal{S}(\mathcal{A},x) := \sum_{p\leq x}\sum_{\chi\neq\chi_0}\left|\sum_{|a|\leq A}\alpha_a\chi(a)\right|,$$

or

$$\mathcal{S}^{(m)}(\mathcal{A},x) := \sum_{p\leq x}\sum_{\substack{\chi\neq\chi_0\\ \mathrm{ord}\,\chi=m}}\left|\sum_{|a|\leq A}\alpha_a\chi(a)\right|$$

for $m\in\{4,6\}$.

Proceeding as in [5, Lemma 6] and [15], we can prove:

PROPOSITION 53. *For any integer $k\geq 1$,*

$$\mathcal{S}(\mathcal{A},x) \ll_{\varepsilon,k} \| \mathcal{A} \|\ x^{\varepsilon}\left(\frac{x^{1+\frac{1}{2k}}}{(\log x)^{1-\frac{1}{2k}}}+\sqrt{A}\frac{x^{1-\frac{1}{2k}}}{(\log x)^{1-\frac{1}{2k}}}\right).$$

This suffices for our final main estimates. However, by recalling that we are working with characters of order 4 or 6, proceeding as in [15] it is possible to obtain a better result:

PROPOSITION 54. *For $m\in\{4,6\}$, we have*

$$\mathcal{S}^{(m)}(\mathcal{A},x) \ll \| \mathcal{A} \| \cdot \left(A^{\frac{1}{4}}x + A^{\frac{1}{2}}x^{\frac{7}{8}}\right).$$

It follows that

$$\mathcal{S}_4(\mathcal{A},\mathcal{B},x) \ll \| \mathcal{A} \| \cdot \| \mathcal{B} \| \cdot\sqrt{B}\left(A^{\frac{1}{4}}x + A^{\frac{1}{2}}x^{\frac{7}{8}}\right), \tag{30}$$

$$\mathcal{S}_6(\mathcal{A},\mathcal{B},x) \ll \| \mathcal{A} \| \cdot \| \mathcal{B} \| \cdot\sqrt{A}\left(B^{\frac{1}{4}}x + B^{\frac{1}{2}}x^{\frac{7}{8}}\right). \tag{31}$$

Now let us focus on $\mathcal{S}_\infty(\mathcal{A},\mathcal{B},x)$, for which we proceed similarly to [5, Lemma 6] and [15].

A double application of the Cauchy-Schwarz Inequality gives

$$(32)\quad \mathcal{S}_\infty(\mathcal{A},\mathcal{B},x)$$

$$\le \left(\sum_{5\le p\le x}\sum_{\chi_1\ne\chi_0}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{1}{p(p-1)^3}\left|\sideset{}{^*}\sum_{s(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t(\mathrm{mod}\,p)} w_p(s,t)\,\overline{\chi}_1(s)\overline{\chi}_2(t)\right|^2\right)^{\frac12}$$

$$\cdot\left(\sum_{5\le p\le x}\sum_{\chi_1\ne\chi_0}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{p}{\phi(p)}\left(\sum_{\substack{|a|\le A\\ p\nmid a}}\alpha_a\chi_1(a)\right)^2\left(\sum_{\substack{|b|\le B\\ p\nmid b}}\beta_b\chi_2(b)\right)^2\right)^{\frac12}$$

$$\le \left(\sum_{5\le p\le x}\sum_{\chi_1\ne\chi_0}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{1}{p(p-1)^3}\left|\sideset{}{^*}\sum_{s(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t(\mathrm{mod}\,p)} w_p(s,t)\,\overline{\chi}_1(s)\overline{\chi}_2(t)\right|^2\right)^{\frac12}$$

$$\cdot\left(\sum_{5\le p\le x}\sum_{\chi_1\ne\chi_0}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{p}{\phi(p)}\left(\sum_{\substack{|a|\le A\\ p\nmid a}}\alpha_a\chi_1(a)^4\right)\right)^{\frac14}$$

$$\cdot\left(\sum_{5\le p\le x}\sum_{\chi_1\ne\chi_0}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{p}{\phi(p)}\left(\sum_{\substack{|b|\le B\\ p\nmid b}}\beta_b\chi_2(b)^4\right)\right)^{\frac14}.$$

To estimate the first factor, we complete the sums over χ_1, χ_2 to sums over all characters mod p and, by the orthogonality relations, we obtain

$$\sum_{\chi_1\ne\chi_0}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\left|\sideset{}{^*}\sum_{s(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t(\mathrm{mod}\,p)} w_p(s,t)\,\overline{\chi}_1(s)\overline{\chi}_2(t)\right|^2$$

$$\le \sum_{\chi_1}\sum_{\chi_2}\sideset{}{^*}\sum_{s(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t(\mathrm{mod}\,p)} w_p(s,t)\,\overline{\chi}_1(s)\overline{\chi}_2(t)$$

$$\sideset{}{^*}\sum_{s'(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t'(\mathrm{mod}\,p)} w_p(s',t')\,\chi_1(s')\chi_2(t')$$

$$= \sideset{}{^*}\sum_{s(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{s'(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t'(\mathrm{mod}\,p)} w_p(s,t)\,w_p(s',t')\sum_{\chi_1}\chi_1(s^{-1}s')\sum_{\chi_2}\chi_2(t^{-1}t')$$

$$= (p-1)^2\sideset{}{^*}\sum_{s(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t(\mathrm{mod}\,p)}|w_p(s,t)|^2 \le (p-1)^4.$$

Summing over p, we obtain

(33)
$$\left(\sum_{5\le p\le x}\sum_{\chi_1\neq\chi_0}\sum_{\substack{\chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{1}{p(p-1)^3}\left|\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\,\overline{\chi}_1(s)\overline{\chi}_2(t)\right|^2\right)^{\frac{1}{2}} \ll \frac{x^{\frac{1}{2}}}{(\log x)^{\frac{1}{2}}}.$$

To estimate the second (respectively third) factor in (32), we note that for a fixed p and for each Dirichlet character χ_1 (respectively χ_2) modulo p, there exist at most six (respectively four) characters χ_2 (respectively χ_1) such that $\chi_1^4\chi_2^6=\chi_0$; by expanding out the squares and by the large sieve inequality, we obtain:

Proposition 55.

$$\sum_{5\le p\le x}\sum_{\chi_1\neq\chi_0}\sum_{\substack{\chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{p}{\phi(p)}\left(\sum_{\substack{|a|\le A\\ p\nmid b}}\alpha_a\chi_1(a)^4\right)^4 \ll \left(x^2+A^2\right)||\mathcal{A}||^4; \tag{34}$$

$$\sum_{5\le p\le x}\sum_{\chi_1\neq\chi_0}\sum_{\substack{\chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\frac{p}{\phi(p)}\left(\sum_{\substack{1\le b\le B\\ p\nmid b}}\beta_b\chi_2(b)^4\right)^4 \ll \left(x^2+B^2\right)||\mathcal{B}||^4. \tag{35}$$

By putting together (32)–(35), we obtain

$$\mathcal{S}_\infty(\mathcal{A},\mathcal{B},x) \ll ||\mathcal{A}||\cdot||\mathcal{B}||\cdot\frac{x^{\frac{1}{2}}}{(\log x)^{\frac{1}{2}}}\left(x^2+A^2\right)^{\frac{1}{4}}\left(x^2+B^2\right)^{\frac{1}{4}}. \tag{36}$$

Finally, let us estimate $\mathcal{S}_0(\mathcal{A},\mathcal{B},x)$. By [32, p. 245] (see also [54, Lemma 6.1, pp. 22–23]), we have:

Theorem 56.

$$\left|\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t) - \prod_{\ell|p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)\cdot(p-1)^2\right| \le p^{\frac{3}{2}+\mathrm{o}(1)}. \tag{37}$$

By [33, Thm. 3, p. 1957], we have:

Proposition 57.

$$\sum_{p\le x}\prod_{\ell|p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right) = \prod_{\ell}\left(1-\frac{1}{\ell(\ell-1)^2(\ell+1)}\right)\cdot\pi(x)+\mathrm{O}\left(\frac{x}{(\log x)^B}\right).$$

Then

$$\mathcal{S}_0(\mathcal{A},\mathcal{B},x) = |\mathcal{A}|\cdot|\mathcal{B}|\sum_{p\le x}\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell(\ell^2-1)}\right)+\mathrm{O}\left(\frac{\sqrt{x}}{\log x}||\mathcal{A}||\cdot||\mathcal{B}||\cdot\sqrt{AB}\right)$$

$$= |\mathcal{A}|\cdot|\mathcal{B}|\prod_{\ell}\left(1-\frac{1}{\ell(\ell-1)^2(\ell+1)}\right)\cdot\pi(x)+\mathrm{O}\left(\frac{x}{(\log x)^k}||\mathcal{A}||\cdot||\mathcal{B}||\cdot\sqrt{AB}\right).$$

It is time to put everything together:

$$\begin{aligned}\mathcal{S}(\mathcal{A},\mathcal{B};x) &= |\mathcal{A}|\cdot|\mathcal{B}|\prod_{\ell}\left(1-\frac{1}{\ell(\ell-1)^2(\ell+1)}\right)\cdot\pi(x)\\ &+ \mathrm{O}\left(\frac{x}{(\log x)^k}||\mathcal{A}||\cdot||\mathcal{B}||\cdot\sqrt{AB}\right)\\ &+ \mathrm{O}\left(\|\mathcal{A}\|\cdot\|\mathcal{B}\|\cdot\sqrt{B}\left(A^{\frac14}x+A^{\frac12}x^{\frac78}\right)\right)\\ &+ \mathrm{O}\left(\|\mathcal{A}\|\cdot\|\mathcal{B}\|\cdot\sqrt{A}\left(B^{\frac14}x+B^{\frac12}x^{\frac78}\right)\right)\\ &+ \mathrm{O}\left(||\mathcal{A}||\cdot||\mathcal{B}||\cdot\frac{x^{\frac12}}{(\log x)^{\frac12}}\left(x^2+A^2\right)^{\frac14}\left(x^2+B^2\right)^{\frac14}\right).\end{aligned}$$

By choosing $\alpha_a = 1$ and $\beta_b = 1$ for all a, b, and A, B such that $x^\varepsilon \le A, B \le x^{1+\varepsilon}$, $AB \ge x^{1+\varepsilon}$, the above implies the asymptotic formula (25) claimed in part (i) of Theorem 52.

9.2. **Cyclicity: averaging the individual constants**

We outline the proof of a more general version of part (ii) of Theorem 52, following [35]. Precisely, for an arbitrary integer $k \ge 1$, we estimate, from above, the k-th moment

$$\frac{1}{|\mathcal{C}(A,B)|}\sum_{E\in\mathcal{C}(A,B)}\left|C_{\mathrm{cyclic}}(E)-C_{\mathrm{cyclic}}^{\mathrm{average}}\right|^k, \tag{38}$$

by distinguishing between the non-Serre curves and the Serre curves in $\mathcal{C}(A,B)$; the latter's contribution is shown to dominate.

Starting with the simple observation that $C_{\mathrm{cyclic}}(E) \le 1$ for any elliptic curve $E/\mathbb{Q}$, we see that

$$\frac{1}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E\text{ non-Serre curve}}}\left|C_{\mathrm{cyclic}}(E)-C_{\mathrm{cyclic}}^{\mathrm{average}}\right|^k$$

$$\ll \frac{1}{|\mathcal{C}(A,B)|}\#\left\{E\in\mathcal{C}(A,B) : E\text{ non-Serre curve}\right\}.$$

The latter is estimated using part (i) of Theorem 34 (see [36] for the statement we give below), leading to

$$(39)\quad \frac{1}{|\mathcal{C}(A,B)|} \sum_{\substack{E\in\mathcal{C}(A,B)\\ E \text{ non-Serre curve}}} \left|C_{\text{cyclic}}(E) - C_{\text{cyclic}}^{\text{average}}\right|^k \ll \frac{AB(\log\min\{A,B\})^\gamma}{\sqrt{\min\{A,B\}}}.$$

Let us now focus on Serre curves. Arguments using character sum estimates lead to:

Proposition 58 (Prop. 15 p. 698 [35]). *Let $E/\mathbb{Q}$ be a Serre curve. Then*

$$C_{cyclic}(E) := \begin{cases} C_{cyclic}^{average}\left(1 + \dfrac{\mu(m_E)}{\prod\limits_{\ell\mid m_E}(|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|-1)}\right) & \text{if } (\Delta_E)_{sf} \equiv 1 (\bmod 4), \\ C_{cyclic}^{average} & \text{otherwise.} \end{cases}$$

It follows that

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{\substack{E\in\mathcal{C}(A,B)\\ E \text{ Serre curve}}} \left|C_{\text{cyclic}}(E) - C_{\text{cyclic}}^{\text{average}}\right|^k \ll \frac{1}{|\mathcal{C}(A,B)|} \sum_{\substack{E\in\mathcal{C}(A,B)\\ E \text{ Serre curve}}} \frac{1}{|(\Delta_E)_{\text{sf}}|^k}$$
$$\asymp \frac{1}{AB} \sum_{|a|\le A} \sum_{\substack{|b|\le B\\ \Delta_{a,b}\neq 0}} \frac{1}{|(4a^3+27b^2)_{\text{sf}}|^k}.$$

We choose a parameter $z = z(x)$, to be defined later, and partition the double sum above according to whether $\left|(4a^3+27b^2)_{\text{sf}}\right|$ is less, or greater, than z. By counting ideals of bounded norm in various quadratic fields, we obtain:

Lemma 59 (Lemma 22, pp. 705–708 [35]).

$$\#\left\{(a,b)\in\mathbb{Z}\times\mathbb{Z} : |a|\le A, |b|\le B, 4a^3+27b^2\neq 0, \left|(4a^3+27b^2)_{sf}\right| \le z\right\}$$
$$\ll z\, A(\log A)^7(\log B) + B.$$

Then

$$\frac{1}{AB} \sum_{|a|\le A} \sum_{\substack{|b|\le B\\ \Delta_{a,b}\neq 0}} \frac{1}{|(4a^3+27b^2)_{\text{sf}}|^k} \le \frac{1}{AB} \sum_{|a|\le A} \sum_{\substack{|b|\le B\\ \Delta_{a,b}\neq 0\\ (\Delta_{a,b})_{\text{sf}}\le z}} \frac{1}{|(4a^3+27b^2)_{\text{sf}}|^k}$$
$$+ \frac{1}{AB} \sum_{|a|\le A} \sum_{\substack{|b|\le B\\ (\Delta_{a,b})_{\text{sf}}> z}} \frac{1}{z^k}$$
$$\ll z\, A(\log A)^7(\log B) + B + \frac{1}{z^k}.$$

We now choose

$$z \asymp \left(\frac{B}{(\log A)^7 \, (\log B)} \right)^{\frac{1}{k+1}},$$

and deduce that

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{\substack{E \in \mathcal{C}(A,B) \\ E \text{ Serre curve}}} \left| C_{\text{cyclic}}(E) - C_{\text{cyclic}}^{\text{average}} \right|^k \ll \left(\frac{(\log A)^7 \, (\log B)}{B} \right)^{\frac{k}{k+1}}. \tag{40}$$

The bounds (39) and (40), put together, lead to the desired upper bound for the kth moment (38), and hence to (26).

10. GLOBAL PERSPECTIVES

Our guiding Questions 1 and 2 may also be formulated in function field settings, as we briefly discuss below.

10.1. Cyclicity: elliptic curves over function fields

Let K be a global field of characteristic $p \geq 5$ and constant field $\mathbb{F}_q$. Let E/K be an elliptic curve over K with j-invariant $j_E \notin \mathbb{F}_q$. All but finitely many primes $\wp$ of K are of good reduction for E/K. We denote by $\mathcal{P}_E$ the collection of these primes, and for each $\wp \in \mathcal{P}_E$, we consider the residue field $\mathbb{F}_\wp$ at $\wp$ and the abelian group $\overline{E}(\mathbb{F}_\wp)$ defined by the reduction of E modulo $\wp$. From the theory of torsion points for elliptic curves, there exist uniquely determined integers $d_{1,\wp}, d_{2,\wp} \geq 1$, possibly equal to 1, such that

$$\begin{aligned} \overline{E}(\mathbb{F}_\wp) &\simeq \mathbb{Z}/d_{1,\wp}\mathbb{Z} \times \mathbb{Z}/d_{2,\wp}\mathbb{Z}, \\ d_{1,\wp} &\mid d_{2,\wp}. \end{aligned}$$

In analogy with Theorems 46 and 48, we have:

THEOREM 60 (Cojocaru-Tóth Cyclicity and Large Exponent Theorem [19]).

(i) *The Dirichlet density of the set*

$$\{\wp \in \mathcal{P}_E : \overline{E}(\mathbb{F}_\wp) \text{ is cyclic}\}$$

exists and equals

$$\sum_{\substack{m \geq 1 \\ (m,p)=1}} \frac{\mu(m)}{[K(E[m]) : K]},$$

where $\mu(m)$ is the Möbius function of m and $K(E[m])$ is the m-th division field of E/K.

(ii) *Let* $f : (0,\infty) \longrightarrow (0,\infty)$ *be such that* $\lim_{x\to\infty} f(x) = \infty$. *The Dirichlet density of the set*

$$\left\{\wp \in \mathcal{P}_E : d_{2,\wp} > \frac{|\overline{E}(\mathbb{F}_\wp)|}{f(\deg \wp)}\right\}$$

exists and equals 1.

10.2. **Cyclicity: Drinfeld modules**

Another function field analogue of Questions 1 and 2 can be formulated in the setting of Drinfeld modules. For this, let q be a prime power, $A := \mathbb{F}_q[T]$, $K := \mathbb{F}_q(T)$, and Ψ a generic Drinfeld A-module over K, of rank $r \geq 2$. All but finitely many primes $\wp$ of K are of good reduction for Ψ. We denote by $\mathcal{P}_\Psi$ the collection of these primes, and for each $\wp \in \mathcal{P}_\Psi$, we consider the residue field $\mathbb{F}_\wp$ at $\wp$ and the A-module structure on $\mathbb{F}_\wp$, denoted $\overline{\Psi}(\mathbb{F}_\wp)$, defined by the reduction of Ψ modulo $\wp$. We denote by $\left|\chi\left(\overline{\Psi}\left(\mathbb{F}_\wp\right)\right)\right|_\infty$ the norm (defined by the prime at infinity $\frac{1}{T}$ of K) of the Euler-Poincaré characteristic of the A-module $\overline{\Psi}(\mathbb{F}_\wp)$. From the theory of torsion points for Drinfeld modules and that of finitely generated modules over a PID, there exist uniquely determined monic polynomials $d_{1,\wp}, \ldots, d_{r,\wp} \in A$, possibly 1, such that

$$\overline{\Psi}(\mathbb{F}_\wp) \simeq_A A/d_{1,\wp}A \times \ldots \times A/d_{r,\wp}A \tag{41}$$

and

$$d_{1,\wp} | \ldots | d_{r,\wp}.$$

The polynomials $d_{1,\wp}, \ldots, d_{r,\wp}$ are the elementary divisors of the A-module $\overline{\Psi}(\mathbb{F}_\wp)$, with the rth one, the exponent, having the property that $d_{r,\wp}\lambda = 0$ for all $\lambda \in \overline{\Psi}(\mathbb{F}_\wp)$. Here, $d_{r,\wp}\lambda := \overline{\Psi}(d_{r,\wp})(\lambda)$. In analogy with Theorems 46 and 48, we have:

THEOREM 61 (Cojocaru-Shulman Cyclicity and Large Exponent Theorem [18]).

(i) *The Dirichlet density of the set*

$$\{\wp \in \mathcal{P}_\Psi : d_{1,\wp} = 1\}$$

exists and equals

$$\sum_{\substack{m\in A\\ m \text{ monic}}} \frac{\mu_A(m)}{[K(\Psi[m]) : K]}, \tag{42}$$

where $\mu_A(m)$ *is the Möbius function of* m *and* $K(\Psi[m])$ *is the* m*-th division field of* Ψ.

(ii) *Assume that* $r = 2$ *and let* $f : (0, \infty) \longrightarrow (0, \infty)$ *be such that* $\lim_{x \to \infty} f(x) = \infty$. *The Dirichlet density of the set*

$$\left\{ \wp \in \mathcal{P}_\Psi : |d_{2,\wp}|_\infty > \frac{\left|\chi\left(\overline{\Psi}\left(\mathbb{F}_\wp\right)\right)\right|_\infty}{q^{f(\deg \wp)}} \right\}$$

exists and equals 1.

11. FURTHER REMARKS

The investigations of the guiding Questions 1 and 2 may be expanded in both depth and breadth. For example, preserving the context of elliptic curves $E/\mathbb{Q}$, we observe that the cyclicity of $\overline{E}(\mathbb{F}_p)$ relates to questions about the distribution of the integers a_p and b_p, introduced in Section 5, and to questions about the arithmetic of the integers $p+1-a_p$. Indeed, by noting that $b_p = 1$ implies that $\overline{E}(\mathbb{F}_p)$ is cyclic, we are led to investigating the asymptotic behaviour of

$$\#\{p \leq x : b_p = 1\};$$

by noting that $|\overline{E}(\mathbb{F}_p)|$ is squarefree, or prime, implies that $\overline{E}(\mathbb{F}_p)$ is cyclic, we are led to investigating the asymptotic behaviour of

$$\#\{p \leq x : |\overline{E}(\mathbb{F}_p)| \text{ is squarefree}\}$$

and

$$\#\{p \leq x : |\overline{E}(\mathbb{F}_p)| \text{ is prime}\};$$

by noting that the primality of $|\overline{E}(\mathbb{F}_p)|$ is realized when $a_p = 1$, we are led to investigating the asymptotic behaviour of

$$\#\{p \leq x : a_p = 1\}.$$

Similar investigations may be pursued in the more general contexts of an elliptic curve E/K defined over a global field K, a higher dimensional abelian variety over K, a modular form, a generic Drinfeld module, and so on. In a sequel to this paper, we shall present an overview of progress in these directions.

REFERENCES

[1] A. Akbary, *On the greatest prime divisor of* N_p. J. Ramanujan Math. Soc. **23** (2008), *3*, 259–282.

[2] A. Akbary and D. Ghioca, *A geometric variant of Titchmarsh divisor problem.* Int. J. Number Theory **8** (2012), *1*, 53–69.

[3] A. Akbari and A.T. Felix, *On invariants of elliptic curves on average.* Acta Arith. **168** (2015) *1*, 31–70.

[4] 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), *1*, 25–37.

[5] A. Balog, A.C. Cojocaru and C. David, *Average twin prime conjecture for elliptic curves.* Amer. J. Math. **133** (2011), *5*, 1179–1229.

[6] W.D. Banks and I.E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height.* Israel J. Math. **173** (2009), 253–277.

[7] M. Bhargava and A. Shankar, *The average size of the* 5*-Selmer group of elliptic curves is* 6 *and the average rank is less than* 1. arxiv:1312.7859v1 [math.NT] 30 Dec. 2013.

[8] B.J. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves II.* J. Reine Angew. Math. **218** (1965), 79–108.

[9] 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), *2*, 335–350.

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

[11] A.C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve.* CRM Proc. Lecture Notes **36** (2004), 61–79.

[12] A.C. Cojocaru, D. Grant and N. Jones, *One parameter families of elliptic curves with maximal Galois representations.* Proc. London Math. Soc. **103** (2011), *4*, 654–675.

[13] A.C. Cojocaru, M. Fitzpatrick, T. Insley and H. Yilmaz, *Reductions modulo primes of Serre curves.* In preparation.

[14] A.C. Cojocaru and C. Hall, *Uniform results for Serre's theorem for elliptic curves.* Int. Math. Res. Not. IMRN **50** (2005), *50*, 3065–3080.

[15] A.C. Cojocaru, H. Iwaniec and N. Jones, *The average asymptotic behaviour of the Frobenius fields of an elliptic curve.* Under revisions.

[16] 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.

[17] A.C. Cojocaru and M.R. Murty, *An introduction to sieve methods and their applications.* London Math. Soc. Stud. Texts, Cambridge University Press, 2005.

[18] A.C. Cojocaru and A.M. Shulman, *The distribution of the first elementary divisor of the reductions of a generic Drinfeld module of arbitrary rank.* Canadian J. Math. **67** (2015), *6*, 1326–1357.

[19] A.C. Cojocaru and Á. Tóth, *Distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field.* J. Number Theory **132** (2012), 953–965.

[20] H. Davenport, *Multiplicative Number Theory.* Grad. Texts in Math. **74**, Springer Verlag 2000.

[21] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Semin. Univ. Hambg. **14** (1941), 197–272.

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

[23] W. Duke and Á. Tóth, *The splitting of primes in division fields of elliptic curves.* Exp. Math. **11** (2002), *4*, 555–565.

[24] A.T. Felix and M.R. Murty, *On the asymptotics for invariants of elliptic curves modulo p.* J. Ramanujan Math. Soc. **28** (2013), *3*, 271–298.

[25] É. Fouvry and H. Iwaniec, *Primes in arithmetic progressions.* Acta Arith. **42** (1983), 197–218.

[26] J. Friedlander and H. Iwaniec, *Opera de Cribo.* Amer. Math. Soc. Colloq. Publ. **57** (2010).

[27] T. Freiberg and P. Kulberg, *On the average exponent of elliptic curves modulo p.* Int. Math. Res. Not. IMRN **8** (2014), 2265–2293.

[28] T. Freiberg and P. Pollack, *The average of the first invariant factor for reductions of CM elliptic curves mod p.* To appear in Int. Math. Res. Not. IMRN.

[29] D. Grant, *A formula for the number of elliptic curves with exceptional primes.* Compos. Math. **122** (2000), 151–164.

[30] R. Gupta and M.R. Murty, *Cyclicity and generation of points mod p on elliptic curves.* Invent. Math. **101** (1990), *1*, 225–235.

[31] H.H. Halberstam and H.-E. Richert, *Sieve methods.* London Academic Press, 1974.

[32] E.W. Howe, *On the group orders of elliptic curves over finite fields.* Compos. Math. **85** (1993), 229–247.

[33] K.-H. Indlekofer, S. Wehmeier and L.G. Lucht, *Mean behaviour and distribution properties of multiplicative functions.* Comput. Math. Appl. **48** (2004), 1947–1971.

[34] H. Iwaniec and E. Kowalski, *Analytic number theory.* Amer. Math. Soc. Colloq. Publ. **53** (2004).

[35] N. Jones, *Averages of elliptic curve constants.* Math. Ann. **345** (2009), 685–710.

[36] N. Jones, *Almost all elliptic curves are Serre curves.* Trans. Amer. Math. Soc. **362** (2010), *3*, 1547–1570.

[37] S. Kim, *Average behaviors of invariant factors in Mordell-Weil groups of CM elliptic curves modulo p.* Finite Fields Appl. **30** (2014), 178–190.

[38] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem.* In: A. Fröhlich (Ed.), *Algebraic Number Fields.* Academic Press, New York, 1977, pp. 409–464.

[39] B. Mazur, *Modular curves and the Eisenstein ideal.* Publ. Math. Inst. Hautes Études Sci. **47** (1977), 33–106.

[40] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. **44** (1978), 129–162.

[41] P. Moree (with contributions by A.C. Cojocaru, W. Gajda and H. Graves), *Artin's primitive root conjecture – a survey.* Integers **12A** (2012), John Selfridge Memorial Issue, #A13.

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

[43] L. Olson, *Points of finite order on elliptic curves with complex multiplication.* Manuscripta Math. **14** (1974), 195–205.

[44] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques.* J. Pures Appl. Math. **95** (1901), *7*, 161–234.

[45] B. Poonen, *Average rank of elliptic curves – after Manjul Bhargava and Arul Shankar.* Séminaire BOURBAKI, 64éme année, 2011–2012, no.1049.

[46] V. Radhakrishnan, *Asymptotic formula for the number of non-Serre curves in a two-parameter family,* PhD Thesis. University of Colorado at Boulder, 2008.

[47] R. Schoof, *The exponents of the groups of points on the reductions of an elliptic curve.* In: G. van der Geer (Ed.), *Arithmetic Algebraic Geometry.* Progr. Math. **89**, Birkäuser, New York 1991, 325–336.

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

[49] J-P. Serre, *Résumé des cours de 1977–1978.* Annuaire du Collège de France 1978, 67–70.

[50] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev.* Publ. Math. Inst. Hautes Ètudes Sci. **54** (1981), 123–201.

[51] J-P. Serre, *Résumé des cours de 1985–1986.* Annuaire du Collège de France 1986, 95–99.

[52] J-P. Serre, *Lectures on the Mordell-Weil theorem.* Aspects of Mathematics, Vieweg, Braunschweig, 1989. Contemp. Math. **133** (1992), 175–193.

[53] J.H. Silverman, *The arithmetic of elliptic curves.* Grad. Texts in Math. **106**, Springer Verlag, 2000.

[54] S.G. Vladut, *Cyclicity statistics for elliptic curves over finite fields.* Finite Fields Appl. **5** (1999), 13–25.

[55] L.C. Washington, *Elliptic Curves: Number Theory and Cryptology.* Chapman & Hall/ CRC, Boca Raton, Florida, 2003.

[56] A. Weil, *Om a certain type of characters of the idèle-class group of an algebraic number-field.* Proc. Int. Symp. Tokyo-Nikko, 1955, 1–7.

[57] A. Weil, *On the theory of complex multiplication.* Proc. Int. Symp. Tokyo-Nikko, 1955, 9–22.

[58] J. Wu, *The average exponent of elliptic curves modulo p.* J. Number Theory **135** (2014), 28–35.

[59] M.P. Young, *Low-lying zeros of families of elliptic curves.* J. Amer. Math. Soc. **19** (2006), *1*, 205–250.

Received 1 August 2016

University of Illinois at Chicago,
Department of Mathematics, Statistics
and Computer Science,
851 S Morgan St, 322 SEO,
Chicago, 60607, IL, USA

Institute of Mathematics "Simion Stoilow"
of the Romanian Academy,
21 Calea Grivitei Street,
Bucharest 010702,
Romania
cojocaru@uic.edu