PRIMES, ELLIPTIC CURVES AND CYCLIC GROUPS: A SYNOPSIS

ALINA CARMEN COJOCARU

Abstract. The main question addressed in this paper focuses on the frequency with which the reductions modulo primes of a rational elliptic curve give rise to cyclic groups. This question is part of a broad theme of investigations about the distribution of Frobenius in an infinite family of division fields defined by an elliptic curve over a global field (or in variations of such families in other arithmetic-geometric contexts). Illustrative of many of the ideas, methods and obstacles that occur in the broader theme, the investigations of the cyclicity question are foundational for a researcher interested in pursuing analytic studies of primes in arithmetic-geometric contexts. While most of the paper is a survey of prior results, the statement and detailed outline of proof of the more refined version of part (i) of Theorem 48, given in Section 10.1, are new.

Contents

Date: March 15, 2016.

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 primes 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 with $\mathbb{F}_p^\times$: *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 throughout the paper will be:

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 $\overline{E}(\mathbb{F}_p)$ comparable 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 showed the precise behaviour of primes in arithmetic progressions. This is currently 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 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 celebrated conjectures about primes from the 1920s, such as:

Conjecture 6. *(Artin's Primitive Root Conjecture:)*
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 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, R. Murty and 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 Artin's Primitive Root Conjecture and many references, we refer the reader to [Mo].

The study of problems about primes 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 error terms and their

uniformity in the modulus m in Dirichlet's Theorem. 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 provided by Lagarias and Odlyzko in the 1970s, using analytic methods in *algebraic number theory:*

Theorem 9. *(Effective Chebotarev Density Theorem* [LaOd]*)*
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) *a* δ*-quasi-GRH for the Dedekind zeta function of* K *(that is, a zero-free region of* $\mathrm{Re}(s) > \delta$ *for the Dedekind zeta function of* K*) 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 can be proven about $\pi(x, m, a)$ for larger m, and, in more generality, about $\pi_C(x, K/\mathbb{Q})$ for sufficiently large families of number fields K.

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 provided by Theorem 9 is mostly open. In Sections 8-10 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; outstanding pieces of work have been completely left out! This is an ongoing field of research where phenomenal advances continue to be made. For a classical introduction and references, we refer the reader to [Da];l for recent presentations of sieve methods and further references, we refer the reader to [CoMu-book] and [FrIw-book]. The goal of our succinct presentation has been to provide a flavour of the study of primes which may be echoed in arithmetic-geometric contexts.

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 will give a brief introduction to the most basic properties of elliptic curves. We refer the reader to [Si] and [Wa] 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

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

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 with 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** (or non-CM) and, respectively, **with Complex Multiplication** (or CM);*

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

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

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 will be that of

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

For the rest of this section we 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 (which had been conjectured by Ogg):

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

(i) *(Mazur* [Ma77], [Ma78]*)*

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* [Ol]*)*

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

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

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

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

be the reduction of E modulo p (in itself, an elliptic curve). Define the reduction map

$$E(\mathbb{Q})_{tors} \longrightarrow \overline{E}(\mathbb{F}_p)$$

$$\mathcal{O} \mapsto \mathcal{O}$$

$$P = (x(P), y(P)) \mapsto \overline{P} = (x(P) (\text{mod}\, p), y(P) (\text{mod}\, p))$$

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

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

Theorem 19. *(Average Rational Torsion Theorem* [Gr]*)*
For $A, B \geq 1$, 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 $|a| \leq A, |b| \leq B$. Then, for $A = x^2$, $B = x^3$ with $x \to \infty$, we have

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

Remark 20. The "almost all" statement above also hold in a more refined sense, as proven in [CoHa] and [CoGrJo].

The study of the arithmetic rank $r = r(E)$ is the focus of major research on both the algebraic and analytic side of arithmetic geometry. Already in 1901, Poincaré [Poi] asked for the range of possible values of r and , to this day, it is not known 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 that compute $r(E)$ successfully. Ensuring, in general, that the algorithms terminate, is an open problem that relates to the celebrated Birch & Swinnerton-Dyer Conjecture, formulated in the 1960s [BSD]. 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 $s = 1$, which relates to the value of the L-function $L(E,s)$ of E at $s = 1$; this, by the Birch & Swinnerton-Dyer Conjecture, 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 $A, B \geq 1$, 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 $|a| \leq A, |b| \leq B$. Then, for $A = x^2$, $B = x^3$ with $x \to \infty$, we have

(i) *(Bhargava - Shankar* [BhSh]*)*

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

(ii) *(Young* [Yo]*)*

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

Remark 22. "Almost all" statements such as the ones above also hold in a more refined sense; see the references in Poonen's survey [Poo] for such works and results preceding the ones stated above.

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 $E(\mathbb{Q})_{\mathrm{tors}}$; on the other hand, knowledge about the reductions

$\overline{E}/\mathbb{F}_p$ - more precisely, about *infinitely many* groups $\overline{E}(\mathbb{F}_p)$ - also 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 is realized by understanding the Artin symbol at p (the "Frobenius") in the division fields of E, whose main properties we review 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 $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The group action gives rise to a Galois representation

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

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

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

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 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 $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m])$. Consequently, 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* [We55], [We55bis]*)*
Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$.

(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 $\widehat{O} := \varprojlim_m O/mO$, we have that $\mathbb{Q}(E_{tors})$ is a free $\widehat{O}$-module of rank 1, acted on by $G_K := \mathrm{Gal}\left(\overline{K}/K\right)$, and that 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 $m \geq 1$,

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

where $\omega : (O/mO)^\times \longrightarrow (O/\gcd(m, m_E)\, O)^\times$ 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, 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*

$$\mathrm{Gal}(K(E[m])/K) \simeq (O/m_1O)^\times \times H_{m_2}$$

for some $H_{m_2} \leq (O/m_2O)^\times$.

Theorem 28. *(Open Image Theorem for non-CM Elliptic Curves* [Se72]*)*
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

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

where $\omega : \mathrm{GL}_2\left(\hat{\mathbb{Z}}\right) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$ 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, 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 all integers $m \geq 1$,

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

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

Lemma 31. *(*[Se72, 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 as 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 $A, B \geq 1$, 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 $|a| \leq A, |b| \leq B$. Then, for $A = x^2$, $B = x^3$ with $x \to \infty$, we have

(i) *(Jones* [Jo10]*)*

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

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

(ii) *(Radakrishnan* [Ra]*)*

$\forall\, \varepsilon > 0$,

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

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 53 which we shall outline in Section 10.

Remark 35. The "almost all" statements above also hold in a more refined sense, as proven in [CoGrJo].

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

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

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

(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 $\mathbb{Q}(\pi_p)$.*

In light of these properties, 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 $\Delta_p \equiv 0, 1 (\mathrm{mod}\, 4))$, we can also define 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* [DuTo]*)*
Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3) and let $p \nmid \Delta_E$. 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 have:

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

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

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

6. Cyclicity questions

At the end of Section 1 we promised that we will formulate more explicit versions of our two guiding Questions 1 and 2. It is time to do so:

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

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

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

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

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 $\lim_{x\to\infty} f(x) = \infty$,

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

We also add some food for thought:

Question 42.

(1) *Where do the asymptotic formulae in Conjectures 40 and 41 come from?*
(2) *What numerical data supports Conjectures 40 and 41?*
(3) *What is the expected error term in either asymptotic formula of Conjecture 40 or 41?*
(4) *What theoretical evidence supports Conjectures 40 and 41?*
(5) *Can we prove Conjectures 40 and 41? If not, what are the main obstacles?*
(6) *What is the conjectural constant $C_{cyclic}(E)$?*
(7) *When is the conjectural constant $C_{cyclic}(E)$ positive?*
(8) *What is the range for the conjectural constant $C_{cyclic}(E)$? Can it ever be 1? When it is close to 1, what does it imply about $E(\mathbb{Q})_{tors}$?*
(9) *What global properties of E, if any, impact Conjectures 40 and 41?*
(10) *What is a broader framework for Conjectures 40 and 41?*

7. Heuristics and upcoming challenges

Let us start investigating the Cyclicity Conjecture. The starting point is the following consequence to Theorem 37:

Lemma 43. *(Cyclicity Criterion)*
Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation (3) and let $p \nmid \Delta_E$.

(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 ∞) and a parameter $z = z(x) > 0$ (to be thought of as growing with x);
  - $\mathcal{A} := \{p \leq x : p \nmid \Delta_E\}$;
  - $\mathcal{A}_\ell := \{p \in \mathcal{A} : p \neq \ell, p \text{ splits completely in } \mathbb{Q}(E[\ell])\}$, for all primes $\ell < z$.
- 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

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

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 very convincing numerical evidence performed on over 300 elliptic curves with $x = 10^5$; see the upcoming [CoFiInYi].

Why is this a heuristical reasoning and not a proof? Two immediate crucial points have been completely overlooked:

(Point 1) We have ignored the relation between the range of the index m 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 add some clarity to each of these points:

(Point 1bis) By Lemma 43, 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

$$m(x) := \sqrt{x}+1. \tag{12}$$

(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 have

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

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

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

Unfortunately, with such a raw reasoning, we have reached a superfluous triviality: the number of primes up to x (with additional properties) is estimated from above by a function that exceeds the number of integers up to x. A more refined analysis is 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).

We will discuss studies of these aspects in the next sections.

8. Cyclicity: asymptotic

The good news is that the heuristical reasoning towards Conjecture 40, outlined in Section 7, can be developed into a proof! This was achieved for the first time by Serre [Se77], under GRH, via a method inspired from Hooley's conditional proof of Artin's Primitive Root Conjecture. After Serre, Cojocaru and R. Murty provided 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 [Mu83], [Co02], [Co03], [CoMu].

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

Proposition 44. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $x, y > 0$ with $y = y(x) \leq \sqrt{x} + 1$, growing with x.*

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

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

(ii) *Assuming $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \ncong \mathbb{Z}$, we have*

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

Proof. A proof of part (i) appears in [Co02, pp. 343-344]; see also [CoMu, p. 613]. A proof of part (ii) appears in [Co03, p. 2569]; see also [CoMu, pp. 616-618]. We outline the proof of (i).

Applying part (ii) of Theorem 25, part (ii) of Theorem 36, part (i) of Lemma 43, and (12), followed by elementary estimates, we obtain

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

□

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

Theorem 45. *(Cojocaru-Murty Splitting Mean Theorem)*

Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$\frac{1}{\sqrt{x}} \sum_{m \geq 1} \left(\#\{p \leq x : p \text{ splits completely in } \mathbb{Q}(E[m])\} - \frac{1}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} \pi(x) \right) \ll r(E, x), \tag{14}$$

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 $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \ncong \mathbb{Z}$, 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 $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \ncong \mathbb{Z}$,*

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

Proof. We sketch the proofs of parts (ii) and (iv). For part (i), proceed as in the proof of Theorem 1.2 of [Co02]. For part (iii), proceed as in the unconditional proof of the main theorem given in Section 6 of [Mu83]; see also the follow-up [AkMu].

(ii) The main idea of 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, we 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):

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

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

Over the second range, we apply part (i) of Proposition 44:

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

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 44, and making the choice $y \asymp \left(\frac{x}{(\log x)^2}\right)^{\frac{1}{4}}$. □

Remark 46. To prove parts (i) and (iii) of Theorem 45, the sum over m is split according to whether m is y-smooth or not. This is the splitting of the classical "simple asymptotic sieve" and was the one used by Serre in [Se77]. In [CoMu], Cojocaru and Murty noted that, under GRH, this splitting is not necessary and that the naive splitting explained above suffices; 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 new distinction between this classical conjecture and Conjecture 40.

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

Theorem 47. *(Cojocaru-Murty/Serre Cyclicity Theorem* [Co02]*,* [CoMu]*,* [Mu83]*)*
Let $E/\mathbb{Q}$ be an elliptic curve. Then

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

where $r(E,x)$ is as in Theorem 45, under the assumptions therein.

Proof. Starting from (11), we follow the approach in the proof of Theorem 45, 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 $m \leq y$), and is estimated from above by 1 everywhere else. The original sources of the proofs are: [CoMu] under GRH, [Co02] under $\frac{3}{4}$-quasi GRH, [Mu83] unconditionally for $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\cong \mathbb{Z}$; see also [Se77], [Co03] and [AkMu]. □

Remark 48. It can be proven that the constant $C_{\mathrm{cyclic}}(E) := \sum_{m\geq 1} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}$ is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$; see [CoMu]. Calculations related to this constant appear in [CoFiInYi] and [CoMu].

Methods similar to proving Theorems 45 and 47 can be employed to investigate Conjecture 41, leading to answers to Conjecture 41:

Theorem 49. *(Duke's Large Exponent Theorem* [Du]*)*
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 either 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 our Proposition 44 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

$$\begin{aligned}
\#\{p \le x : f(p) < d_{1,p}\} &= \#\{p \le z : f(p) < d_{1,p}\} + \#\{z < p \le x : f(p) < d_{1,p}\} \\
&\le \pi(z) + \sum_{g(z)\le m} \#\{p \le x : m | d_{1,p}\} \\
&< \frac{2z}{\log z} + \sum_{g(z)\le m\le \sqrt{x}+1} \#\{p \le x : p \text{ splits completely in } \mathbb{Q}(E[m])\}. \qquad (20)
\end{aligned}$$

(i) Using part (i) of Proposition 44 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 44 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 and satisfies $g(z) < y < \sqrt{x} + 1$, and which 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 44 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 50. We refer the reader to [Du] for a formulation of Theorem 49 with fewer conditions on $f(x)$.

Remark 51. Further applications of these methods have been pursued in several other works, including: [Ak], [AkGh], [AkFe], [FeMu], [FrKu], [FrPo], [Ki], and [Wu].

9. Cyclicity: lower bound

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

Theorem 52. *(Gupta-Murty Cyclicity Lower Bound* [GuMu]*)*
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 43 that a prime p for which $\overline{E}(\mathbb{F}_p)$ is cyclic does not split completely in $\mathbb{Q}(E[2])$. This is nontrivial, by our hypothesis, 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 [FoIw] implies the existence of some $\varepsilon>0$ such that

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

satisfies

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

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

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

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 44, we obtain

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

and 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 $a \neq 2$ 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. □

10. Cyclicity: average

Further theoretical evidence towards Conjecture 40 is provided by:

Theorem 53. *(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* [BaSh]*)*
Let $x > 0$, $\varepsilon > 0$, and $A = A(x), B = B(x)$ be such that

$$x^\varepsilon \le A, B \le x^{1+\varepsilon},$$

$$AB \ge x^{1+\varepsilon}.$$

Then

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

where

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

(ii) *(Jones* [Jo09]*)*

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

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

10.1. **Cyclicity: averaging the prime counting function.** We will outline the proof of a more general version of part (i) of Theorem 53, based on ideas that originate in [BaSh]. Our presentation draws inspiration from [BaCoDa] and [CoIwJo].

- 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 $|a|\le A, |b|\le B$, respectively, and we associate to each $E_{a,b}\in\mathcal{C}(A,B)$ the weight $\alpha_a\beta_b$. We measure the capacity of the sequences $\mathcal{A}$, $\mathcal{B}$ by the following means:

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

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

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

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

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

- 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

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

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 now 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 $p \ge 5$ we obtain:

$$\begin{aligned}
\sideset{}{^*}\sum_{s(\mathrm{mod}\,p)}\sideset{}{^*}\sum_{t(\mathrm{mod}\,p)} w_p(s,t)\ \gamma(s,t) &= \sum_{\substack{\widehat{(s,t)}\\ p\nmid\Delta(s,t)}}\sum_{\hat{u}} w_p(su^4,tu^6)\,\gamma(su^4,tu^6)\\
&= \sum_{\widehat{(s,t)}} w_p(s,t)\sum_{\hat{u}}\gamma(su^4,tu^6)\\
&= \sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\ \frac{|\mathrm{Aut}(E_{s,t})|}{p-1}\sum_{\hat{u}}\gamma(su^4,tu^6)\\
&= \frac{1}{p-1}\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\sum_{u(\mathrm{mod}\,p)}^{*}\gamma(su^4,tu^6)\\
&= \frac{1}{p-1}\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\sum_{u(\mathrm{mod}\,p)}^{*}\left(\sum_{\substack{|a|\le A\\ a\equiv su^4(\mathrm{mod}\,p)}}^{*}\alpha_a\right)\left(\sum_{\substack{|b|\le B\\ b\equiv tu^6(\mathrm{mod}\,p)}}^{*}\beta_b\right).
\end{aligned}$$

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

$$\begin{aligned}
&\frac{1}{p-1}\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\sum_{u(\mathrm{mod}\,p)}^{*}\left(\sum_{\substack{|a|\le A\\ a\equiv su^4(\mathrm{mod}\,p)}}^{*}\alpha_a\right)\left(\sum_{\substack{|b|\le B\\ b\equiv tu^6(\mathrm{mod}\,p)}}^{*}\beta_b\right)\\
&= \frac{1}{(p-1)^3}\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\sum_{u(\mathrm{mod}\,p)}^{*}\left(\sum_{\chi_1}\overline{\chi}_1(su^4)\sum_{|a|\le A}\alpha_a\chi_1(a)\right)\left(\sum_{\chi_2}\overline{\chi}_2(tu^6)\sum_{|b|\le B}\beta_b\chi_2(b)\right)\\
&= \frac{1}{(p-1)^3}\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\sum_{\chi_1}\overline{\chi}_1(s)\sum_{\chi_2}\overline{\chi}_2(t)\left(\sum_{u(\mathrm{mod}\,p)}^{*}\overline{\chi}_1^4\overline{\chi}_2^6(u)\right)\left(\sum_{|a|\le A}\alpha_a\chi_1(a)\right)\left(\sum_{|b|\le B}\beta_b\chi_2(b)\right)\\
&= \frac{1}{(p-1)^2}\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\sum_{\chi_1}\overline{\chi}_1(s)\sum_{\substack{\chi_2\\ \chi_1^4\chi_2^6=\chi_0}}\overline{\chi}_2(t)\left(\sum_{|a|\le A}\alpha_a\chi_1(a)\right)\left(\sum_{|b|\le B}\beta_b\chi_2(b)\right)\\
&= \frac{1}{(p-1)^2}\sum_{\chi_1}\sum_{\substack{\chi_2\\ \chi_1^4\chi_2^6=\chi_0}}\left(\sum_{s(\mathrm{mod}\,p)}^{*}\sum_{t(\mathrm{mod}\,p)}^{*} w_p(s,t)\,\overline{\chi}_1(s)\overline{\chi}_2(t)\right)\left(\sum_{|a|\le A}\alpha_a\chi_1(a)\right)\left(\sum_{|b|\le B}\beta_b\chi_2(b)\right).
\end{aligned}$$

Finally, we split 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

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

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. As usual, 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

$$\begin{aligned}
\mathcal{S}_4(\mathcal{A},\mathcal{B},x) &\le \sum_{5\le p\le x} \sum_{\substack{\chi\neq\chi_0\\ \chi^4=\chi_0}} \left| \sum_{|a|\le A} \alpha_a \chi(a) \right| \left| \sum_{\substack{|b|\le B\\ p\nmid b}} \beta_b \right|, \\
\mathcal{S}_6(\mathcal{A},\mathcal{B},x) &\le \sum_{5\le p\le x} \sum_{\substack{\chi\neq\chi_0\\ \chi^6=\chi_0}} \left| \sum_{\substack{|a|\le A\\ p\nmid a}} \alpha_a \right| \left| \sum_{|b|\le B} \beta_b \chi(b) \right|.
\end{aligned}$$

This leads to estimating sums of the form

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

or

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

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

Proceeding as in [BaCoDa, Lemma 6] and [CoIwJo, Section 5], we can prove:

Proposition 54. *For any integer $k \ge 1$,*

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

This suffices for our final main estimates. However, by recalling that we are working with characters of order 4 or 6, proceeding as in [CoIwJo, Prop. 10] it is possible to obtain a better result:

Proposition 55. *For $m \in \{4,6\}$, we have*

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

Then

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

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

Now let us focus on $\mathcal{S}_\infty(\mathcal{A},\mathcal{B},x)$; we proceed similarly to [BaCoDa, Lemma 6] and [CoIwJo, Section 4]. A double application of the Cauchy-Schwarz Inequality gives

$$\begin{aligned}
\mathcal{S}_\infty(\mathcal{A},\mathcal{B},x) \quad \leq \quad & \left(\sum_{5\leq p\leq x} \sum_{\chi_1\neq\chi_0} \sum_{\substack{\chi_2\neq\chi_0 \\ \chi_1^4\chi_2^6=\chi_0}} \frac{1}{p(p-1)^3} \left| \sum_{s(\mathrm{mod}\, p)}^{*} \sum_{t(\mathrm{mod}\, p)}^{*} w_p(s,t)\, \overline{\chi}_1(s)\overline{\chi}_2(t) \right|^2 \right)^{\frac{1}{2}} \\
& \cdot \left(\sum_{5\leq p\leq x} \sum_{\chi_1\neq\chi_0} \sum_{\substack{\chi_2\neq\chi_0 \\ \chi_1^4\chi_2^6=\chi_0}} \frac{p}{\phi(p)} \left(\sum_{\substack{|a|\leq A \\ p\nmid a}} \alpha_a\chi_1(a) \right)^2 \left(\sum_{\substack{|b|\leq B \\ p\nmid b}} \beta_b\chi_2(b) \right)^2 \right)^{\frac{1}{2}} \\
\leq \quad & \left(\sum_{5\leq p\leq x} \sum_{\chi_1\neq\chi_0} \sum_{\substack{\chi_2\neq\chi_0 \\ \chi_1^4\chi_2^6=\chi_0}} \frac{1}{p(p-1)^3} \left| \sum_{s(\mathrm{mod}\, p)}^{*} \sum_{t(\mathrm{mod}\, p)}^{*} w_p(s,t)\, \overline{\chi}_1(s)\overline{\chi}_2(t) \right|^2 \right)^{\frac{1}{2}} \\
& \cdot \left(\sum_{5\leq p\leq x} \sum_{\chi_1\neq\chi_0} \sum_{\substack{\chi_2\neq\chi_0 \\ \chi_1^4\chi_2^6=\chi_0}} \frac{p}{\phi(p)} \left(\sum_{\substack{|a|\leq A \\ p\nmid a}} \alpha_a\chi_1(a)^4 \right)^4 \right)^{\frac{1}{4}} \\
& \cdot \left(\sum_{5\leq p\leq x} \sum_{\chi_1\neq\chi_0} \sum_{\substack{\chi_2\neq\chi_0 \\ \chi_1^4\chi_2^6=\chi_0}} \frac{p}{\phi(p)} \left(\sum_{\substack{|b|\leq B \\ p\nmid b}} \beta_b\chi_2(b)^4 \right)^4 \right)^{\frac{1}{4}}.
\end{aligned} \tag{32}$$

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

$$\begin{aligned}
&\sum_{\chi_1 \neq \chi_0} \sum_{\substack{\chi_2 \neq \chi_0 \\ \chi_1^4 \chi_2^6 = \chi_0}} \left| \sideset{}{^*}\sum_{s (\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t (\mathrm{mod}\, p)} w_p(s,t)\, \overline{\chi}_1(s) \overline{\chi}_2(t) \right|^2 \\
\leq\ & \sum_{\chi_1} \sum_{\chi_2} \sideset{}{^*}\sum_{s (\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t (\mathrm{mod}\, p)} w_p(s,t)\, \overline{\chi}_1(s) \overline{\chi}_2(t) \sideset{}{^*}\sum_{s' (\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t' (\mathrm{mod}\, p)} w_p(s',t')\, \chi_1(s') \chi_2(t') \\
=\ & \sideset{}{^*}\sum_{s (\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t (\mathrm{mod}\, p)} \sideset{}{^*}\sum_{s' (\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t' (\mathrm{mod}\, p)} w_p(s,t)\, w_p(s',t') \sum_{\chi_1} \chi_1(s^{-1}s') \sum_{\chi_2} \chi_2(t^{-1}t') \\
=\ & (p-1)^2 \sideset{}{^*}\sum_{s (\mathrm{mod}\, p)} \sideset{}{^*}\sum_{t (\mathrm{mod}\, p)} |w_p(s,t)|^2 \\
\leq\ & (p-1)^4.
\end{aligned}$$

Summing over p, we obtain

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

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 56.

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

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

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 [Ho, p. 245] (see also [Vl, Lemma 6.1, pp. 22–23]), we have:

Theorem 57.

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

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

Proposition 58.

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

Then

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

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 53.

10.2. **Cyclicity: averaging the individual constants.** We will outline the proof of a more general version of part (ii) of Theorem 53, following [Jo09]. Precisely, for an arbitrary integer $k\ge1$, 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 $C_{\mathrm{cyclic}}(E)\le1$ 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 [Jo10] for the statement we give below), leading to

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

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

Proposition 59. *(*[Jo09, Prop. 15 p. 698]*)*
Let $E/\mathbb{Q}$ be a Serre curve. Then

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

Thus

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

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

Lemma 60. [Jo09, Lemma 22, pp. 705–708]

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

Then

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

We now choose

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

and deduce that

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

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

11. Global perspectives

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

11.1. **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 $\wp$. By 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

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

In analogy with Theorems 47 and 49, we have:

Theorem 61. *(Cojocaru-Tóth Cyclicity Theorem* [CoTo]*)*

(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.

11.2. **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 $\overline{\Psi}(\mathbb{F}_\wp)$. By 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 47 and 49, we have:

Theorem 62. *(Cojocaru-Shulman Cyclicity Theorem* [CoSh]*)*

(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.

12. Conclusions

The investigations of our two guiding Questions 1 and 2 may be expanded in both depth and breadth.

For example, remaining in the context of elliptic curves $E/\mathbb{Q}$, 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 may investigate the asymptotic behaviour of

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

by noting that $|\overline{E}(\mathbb{F}_p)|$ squarefree, or prime, implies that $\overline{E}(\mathbb{F}_p)$ is cyclic, we may also investigate 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 may even investigate the asymptotic behaviour of

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

Similar investigations may also be pursued in the context of an elliptic curve E/K defined over a global field K, in the context of higher dimensional abelian varieties over K, that of modular forms, of generic Drinfeld modules, and so on. Many of such investigations have been motivated by conjectures proposed by Lang and Trotter in the 1970s ([LaTr76], [LaTr77]) and have been pursued in all these contexts since. We will return to an account of this expanded program in a sequel to this paper.

References

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

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

[AkFe] A. Akbari and A.T. Felix, *On invariants of elliptic curves on average,* Acta Arith. 168, 2015, no. 1, pp. 31–70.

[AkMu] 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 (1), 2010, pp. 25–37.

[BaCoDa] A. Balog, A.C. Cojocaru and C. David, *Average twin prime conjecture for elliptic curves,* American Journal of Mathematics, Vol. 133, No. 5, 2011, pp. 1179–1229.

[BaSh] W.D. Banks and I.E. Shparlinski, *SatoTate, cyclicity, and divisibility statistics on average for elliptic curves of small height,* Israel J. Math. 173, 2009, pp. 253–277.

[BhSh] 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

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

[Co02] A.C. Cojocaru, *On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves,* Journal of Number Theory vol. 96, no. 2, 2002, pp. 335–350.

[Co03] A.C. Cojocaru, *Cyclicity of CM elliptic curves modulo p,* Trans. Amer. Math. Soc. 355, 2003, pp. 2651–2662.

[Co04] A.C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve,* CRM Proceedings and Lecture Notes, vol. 36, 2004, pp. 61–79.

[CoGrJo] A.C. Cojocaru, D. Grant and N. Jones, *One parameter families of elliptic curves with maximal Galois representations,* Proceedings of the London Mathematical Society, 2011, 103(4), pp. 654–675.

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

[CoHa] A.C. Cojocaru and C. Hall, *Uniform results for Serre's theorem for elliptic curves,* International Mathematics Research Notices, 2005, no. 50, pp. 3065–3080.

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

[CoMu] A.C. Cojocaru and M.R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem,* Mathematische Annalen 330, 2004, pp. 601–625.

[CoMu-book] A.C. Cojocaru and M.R. Murty, *An introduction to sieve methods and their applications,* 224 pages, London Mathematical Society Student Texts, Cambridge University Press, 2005.

[CoSh] 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. vol. 67(6), 2015, pp. 1326–1357.

[CoTo] A.C. Cojocaru and Á. Tóth, *Distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field,* Journal of Number theory 132, 2012, pp. 953–965.

[Da] H. Davenport, *Multiplicative number theory,* Graduate Texts in Mathematics, 74, Springer Verlag 2000.

[De] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper,* Abh. Math. Sem. Hamburg 14, 1941, pp. 197 – 272.

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

[DuTo] W. Duke and Á. Tóth, *The splitting of primes in division fields of elliptic curves,* Experimental Mathematics 11, 2002, no.4, pp. 555–565.

[FeMu] A.T. Felix and M.R. Murty, *On the asymptotics for invariants of elliptic curves modulo p,* J. Ramanujan Math. Soc. 28, 2013, no. 3, pp. 271–298.

[FoIw] É. Fouvry and H. Iwaniec, *Primes in arithmetic progressions,* Acta Arithmetica 42, 1983, pp. 197 – 218.

[FrIw-book] J. Friedlander and H. Iwaniec, *Opera de Cribro,* American Math. Society, Colloquium Publications Vol. 57, AMS 2010.

[FrKu] T. Freiberg and P. Kulberg, *On the average exponent of elliptic curves modulo p,* IMRN 2014, no. 8, pp. 2265–2293.

[FrPo] T. Freiberg and P. Pollack, *The average of the first invariant factor for reductions of CM elliptic curves mod p,* to appear in IMRN.

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

[GuMu] R. Gupta and M.R. Murty, *Cyclicity and generation of points mod p on elliptic curves,* Invent. Math. 101, 1990, no. 1, pp. 225–235.

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

[InWeLu] K.-H. Indlekofer, S. Wehmeier and L.G. Lucht, *Mean behaviour and distribution properties of multiplicative functions,* Computers and Mathematics with Application 48, 2004, pp. 1947–1971.

[Jo09] N. Jones, *Averages of elliptic curve constants,* Math. Ann. 345, 2009, pp. 685–710.

[Jo10] N. Jones, *Almost all elliptic curves are Serre curves,* Trans. Amer. Math. Soc. vol. 362, no. 3, 2010, pp. 1547 – 1570.

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

[LaOd] 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.

[LaTr76] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions,* Lecture Notes in Mathematics 504, Springer Verlag, 1976.

[LaTr77] S. Lang, H. Trotter, *Primitive points on elliptic curves,* Bulletin of the American Mathematical Society vol. 83, no. 2, March 1977.

[Ma77] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. No. 47, 1977, pp. 33 – 106.

[Ma78] B. Mazur, *Rational isogenies of prime degree,* Inventiones Mathematicae 44, 1978, pp. 129–162.

[Mo] 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.

[Mu83] M.R. Murty, *On Artin's conjecture,* J. Number Theory 16, 1983, pp. 147–168.

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

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

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

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

[Sc] R. Schoof, *The exponents of the groups of points on the reductions of an elliptic curve,* in: G. van der Geer, Arithmetic Algebraic Geometry, Progress in Math. 89 , Birkhuser, New York 1991, ISBN 0-8176-3513-0, pp. 325–336.

[Se72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Inventiones Mathematicae 15, 1972, pp. 259–331.

[Se77] J-P. Serre, *Résumé des cours de 1977-1978,* Annuaire du Collège de France 1978, pp. 67–70.

[Se81] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev,* Publ. Math. I.H.E.S., no. 54, 1981, pp. 123–201.

[Se85] J-P. Serre, *Résumé des cours de 1985-1986,* Annuaire du Collège de France, 1986, pp. 95–99.

[Se89] J-P. Serre, *Lectures on the Mordell-Weil theorem,* Aspects of Mathematics, Vieweg, Braunschweig, 1989. Contemp. Math. 133, 1992, pp. 175 – 193.

[Si] J.H. Silverman, *The arithmetic of elliptic curves,* Graduate Texts in Mathematics 106, Springer Verlag 2000.

[Vl] S.G. Vladut, *Cyclicity statistics for elliptic curves over finite fields,* Finite Fields and their Applications 5, 1999, pp. 13–25.

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

[We55] A. Weil, *Om a certain type of characters of the idèle-class group of an algebraic number-field,* Proc. Int. Symp., Tokyo-Nikko, 1955, pp. 1–7.

[We55bis] A. Weil, *On the theory of complex multiplication,* Proc. Int. Symp., Tokyo-Nikko, 1955, pp. 9–22.

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

[Yo] M.P. Young, *Low-lying zeros of families of elliptic curves,* J. Amer. Math. Soc. 19 no 1, 2006, pp. 205 – 250.

(Alina Carmen Cojocaru)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;
- Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania

E-mail address, Alina Carmen Cojocaru: cojocaru@uic.edu