This is a ``preproof'' accepted article for *Canadian Journal of Mathematics*
This version may be subject to change during the production process.
DOI: 10.4153/S0008414X25101156

OPPOSING AVERAGE CONGRUENCE CLASS BIASES IN THE CYCLICITY AND KOBLITZ CONJECTURES FOR ELLIPTIC CURVES

SUNG MIN LEE, JACOB MAYLE, AND TIAN WANG

ABSTRACT. The cyclicity and Koblitz conjectures ask about the distribution of primes of cyclic and prime-order reduction, respectively, for elliptic curves over $\mathbb{Q}$. In 1976, Serre gave a conditional proof of the cyclicity conjecture, but the Koblitz conjecture (refined by Zywina in 2011) remains open. The conjectures are now known unconditionally "on average" due to work of Banks–Shparlinski and Balog–Cojocaru–David. Recently, there has been a growing interest in the cyclicity conjecture for primes in arithmetic progressions (AP), with relevant work by Akbal–Güloğlu and Wong. In this paper, we adapt Zywina's method to formulate the Koblitz conjecture for AP and refine a theorem of Jones to establish results on the moments of the constants in both the cyclicity and Koblitz conjectures for AP. In doing so, we uncover a somewhat counterintuitive phenomenon: On average, these two constants are oppositely biased over congruence classes. Finally, in an accompanying repository, we give Magma code for computing the constants discussed in this paper.

1. INTRODUCTION

Let E be an elliptic curve defined over the rationals, and let N_E denote the conductor of E. For a prime p not dividing N_E (called a *good prime* for E), we write $\widetilde{E}_p$ to denote the reduction of E modulo p. The curve $\widetilde{E}_p$ is an elliptic curve over the finite field $\mathbb{F}_p$. Hence, the set of $\mathbb{F}_p$-points, denoted $\widetilde{E}_p(\mathbb{F}_p)$, forms a finite abelian group. It is well known that

$$\widetilde{E}_p(\mathbb{F}_p) \simeq \mathbb{Z}/d_p(E)\mathbb{Z} \oplus \mathbb{Z}/e_p(E)\mathbb{Z} \quad \text{and} \quad p+1-2\sqrt{p} \leq |\widetilde{E}_p(\mathbb{F}_p)| \leq p+1+2\sqrt{p}$$

for some positive integers $d_p(E)$ and $e_p(E)$ such that $d_p(E) \mid e_p(E)$.

There has been considerable interest, dating back to the 1970s, in studying the distribution of primes p for which $\widetilde{E}_p(\mathbb{F}_p)$ has certain properties. In particular, one defines a good prime p to be of *cyclic reduction* for E if $\widetilde{E}_p(\mathbb{F}_p)$ is a cyclic group and of *Koblitz reduction* for E if $|\widetilde{E}_p(\mathbb{F}_p)|$ is a prime. It is worth noting that every prime p of Koblitz reduction is also of cyclic reduction, since every group of prime order is cyclic. Let $\mathcal{X}$ be either "cyc" or "prime" and $\mathcal{X}_E(p)$ be either "p is of cyclic reduction" or "p is of Koblitz reduction" for E, respectively. Define the counting function

$$\pi_E^{\mathcal{X}}(x) := \#\{p \leq x : p \nmid N_E \text{ and } \mathcal{X}_E(p) \text{ holds}\}.$$

The problem of determining asymptotics for $\pi_E^{\mathcal{X}}(x)$ is called the *cyclicity problem* or *Koblitz problem*, depending on the context. As noted in [4, 33], the Koblitz problem can be viewed as an elliptic curve analog of the twin prime conjecture.

It is natural to consider finer versions of the cyclicity and Koblitz problems which restrict to primes lying in arithmetic progressions. To discuss this, fix integers n, k with $n \geq 1$ and define

$$\pi_E^{\mathcal{X}}(x; n, k) := \#\{p \leq x : p \equiv k \pmod{n},\ p \nmid N_E,\ \text{and } \mathcal{X}_E(p) \text{ holds}\}.$$

Date: June 18, 2025.
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.

Note that if n and k are not coprime, then there is at most one prime congruent to k modulo n, so $\pi_E^{\mathcal{X}}(x; n, k)$ is trivially bounded. As such, we will always take the integers n and k to be coprime. Broadly speaking, the goal of this paper is to examine the constants that appear in the conjectural asymptotics of $\pi_E^{\mathcal{X}}(x; n, k)$ and explore how they are influenced by the choice of k modulo n. Before introducing our contributions, we outline aspects of the rich history of the cyclicity and Koblitz problems relevant to our work.

We begin with the cyclicity problem, which has its origin in 1975 when I. Borosh, C. J. Moreno, and H. Porta [8, pp. 962–963] speculated that the density of primes of cyclic reduction exists and can be expressed as an Euler product.[1] In 1976, J.-P. Serre [52] observed that the cyclicity problem bears a resemblance to Artin's primitive root conjecture, which was proven under the Generalized Riemann Hypothesis (GRH) by C. Hooley [29] a decade prior. With this insight, Serre proposed the following conjecture, which he proved as a theorem under GRH.

Conjecture 1.1 (Cyclicity Conjecture [52, pp. 465–468])**.** If $E/\mathbb{Q}$ is an elliptic curve, then

$$\pi_E^{\mathrm{cyc}}(x) \sim C_E^{\mathrm{cyc}} \cdot \frac{x}{\log x}, \tag{1}$$

as $x \to \infty$, where $C_E^{\mathrm{cyc}} \geq 0$ is the explicit constant defined in (18).

Serre noted that $C_E^{\mathrm{cyc}} = 0$ if and only if $\mathbb{Q}(E[2]) = \mathbb{Q}$, in which case we interpret (1) as stating that $\pi_E^{\mathrm{cyc}}(x)$ is bounded as $x \to \infty$.

Conjecture 1.1 has been extensively studied by various mathematicians since then. M. Ram Murty [47] proved that the conjecture holds unconditionally for CM curves. Later, using a lower bound sieve method, Gupta and Murty [27] showed unconditionally for non-CM curves that

$$\pi_E^{\mathrm{cyc}}(x) \gg_E \frac{x}{\log^2 x},$$

as $x \to \infty$ unless $\mathbb{Q}(E[2]) = \mathbb{Q}$. See, for example, [5, 13–15, 23, 30, 59] for some recent work on the problem.

In 2022, Y. Akbal and A. M. Güloğlu [1] studied the cyclicity problem for primes lying in an arithmetic progression. They proved that, under GRH,

$$\pi_E^{\mathrm{cyc}}(x; n, k) \sim C_{E,n,k}^{\mathrm{cyc}} \cdot \frac{x}{\log x}, \tag{2}$$

as $x \to \infty$, where $C_{E,n,k}^{\mathrm{cyc}}$ is the explicit constant defined in (21). As before, if $C_{E,n,k}^{\mathrm{cyc}} = 0$, then we interpret (2) as stating that $\pi_E^{\mathrm{cyc}}(x; n, k)$ is bounded as $x \to \infty$. In 2015, J. Brau [11] obtained a formula for the constant $C_{E,n,k}^{\mathrm{cyc}}$ for all Serre curves outside of a small class (see Remark 1.8). N. Jones and the first author [32] determined all the possible scenarios in which the constant $C_{E,n,k}^{\mathrm{cyc}}$ vanishes. Additionally, P.-J. Wong [60] established (2) unconditionally for CM elliptic curves.

While Conjecture 1 remains open without assuming GRH, researchers have found success in proving the conjecture is true "on average" in various senses. As observed in [7, Remark 7(v)], there are two broad approaches regarding the average results. One approach is to compute the density of elliptic curves E over $\mathbb{F}_p$ for which $E(\mathbb{F}_p)$ is cyclic, and average it over all primes p. Another approach is to count the number of primes for which an elliptic curve over $\mathbb{Q}$ has cyclic reduction and then average over the family of elliptic curves ordered by height. The former is called the "local" viewpoint while the latter is called the "global" viewpoint.

[1] In 1977, S. Lang and H. Trotter [34] considered a related problem on the density of primes p for which the reduction of a given rational point P on E generates $\widetilde{E}_p(\mathbb{F}_p)$.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

In 1999, S. G. Vlăduţ [57] obtained some statistics related to the cyclicity problem for elliptic curves over finite fields. In particular, he determined the ratio

$$\frac{\#\{E \in \mathcal{F}_p : E(\mathbb{F}_p) \text{ is cyclic}\}}{\#\mathcal{F}_p}, \tag{3}$$

where $\mathcal{F}_p$ denotes the set of isomorphism classes of elliptic curves over $\mathbb{F}_p$. Later, E.-U. Gekeler [25] built upon this result to obtain the local result for the average cyclicity problem. He computed that the average of (3) over all primes p is C^{cyc}, which is defined in (20).

In 2009, building upon Vlăduţ's work, W. D. Banks and I. E. Shparlinski [5] deduced a global result for the average cyclicity problem and demonstrated that it aligns with Gekeler's local result. To set notation: For positive real numbers A and B, let $\mathcal{F} := \mathcal{F}(A, B)$ denote the family of elliptic curves $E/\mathbb{Q}$ defined by a short Weierstrass model

$$E\colon Y^2 = X^3 + aX + b, \tag{4}$$

for some $a, b \in \mathbb{Z}$ satisfying $|a| \leq A$ and $|b| \leq B$. Banks and Shparlinski proved the following.

Theorem 1.2 ([5, Theorem 18]). *Let $x > 0$ and $\epsilon > 0$. Let $A := A(x)$ and $B := B(x)$ be parameters satisfying $x^\epsilon \leq A, B \leq x^{1-\epsilon}$, and $AB \geq x^{1+\epsilon}$. Then, we have*

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \pi_E^{\text{cyc}}(x) \sim C^{\text{cyc}} \cdot \frac{x}{\log x}, \qquad \text{as } x \to \infty.$$

Later, the inequality conditions on A and B in the theorem above were significantly relaxed by A. Akbary and A. T. Felix [2, Corollary 1.5].

Building upon Banks and Shparlinski's methods, the first author refined the results to consider primes in arithmetic progressions [37, Theorem 1.3]. To summarize his results, under the same assumptions of Theorem 1.2, for $n \leq \log x$ and k coprime to n, there exists a positive constant $C_{n,k}^{\text{cyc}}$ for which

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \pi_E^{\text{cyc}}(x; n, k) \sim C_{n,k}^{\text{cyc}} \cdot \frac{x}{\log x}, \qquad \text{as } x \to \infty.$$

The average constant $C_{n,k}^{\text{cyc}}$ is given explicitly in (23).

Related to the cyclicity problem is the Koblitz problem, which seeks to understand the asymptotics of $\pi_E^{\text{prime}}(x)$ and has significance for elliptic curve cryptography [48, 55]. In 1988, N. Koblitz [33] made a conjecture analogous to Conjecture 1.1. In particular, it follows from the conjecture that a non-CM elliptic curve $E/\mathbb{Q}$ has infinitely many primes of Koblitz reduction unless E is rationally isogenous to an elliptic curve with nontrivial rational torsion. The Koblitz conjecture remained open for over 20 years until Jones gave a counterexample, which appears in [62, Section 1.1]. The fundamental issue with the conjecture, which the counterexample exploits, is its failure to account for the possibility of entanglements of division fields. Properly accounting for this possibility, D. Zywina [62] refined the Koblitz conjecture as follows.

Conjecture 1.3 (Refined Koblitz Conjecture, [62, Conjecture 1.2]). If $E/\mathbb{Q}$ is an elliptic curve, then

$$\pi_E^{\text{prime}}(x) \sim C_E^{\text{prime}} \cdot \frac{x}{(\log x)^2}, \tag{5}$$

as $x \to \infty$, where $C_E^{\text{prime}} \geq 0$ is the explicit constant defined in (27).

Similar to the cyclicity case, the constant C_E^{prime} may vanish. In this case, we interpret (5) as indicating that $\pi_E^{\text{prime}}(x)$ is bounded as $x \to \infty$. Beyond the statement of the conjecture provided

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

above, Zywina made the conjecture more generally for elliptic curves over number fields and allowed for a parameter t to consider primes p for which $|\widetilde{E}_p(\mathbb{F}_p)|/t$ is prime.

Conjecture 1.3 is often referred to as an elliptic curve analogue of the twin prime conjecture. Assuming that the events "p is prime" and "$|\widetilde{E}_p(\mathbb{F}_p)|$ is prime" are independent, and applying the Hardy–Littlewood heuristic [28], one would expect that $\pi_E^{\text{prime}}(x)$ should grow like a constant times $x/\log^2 x$, unless E has an intrinsic obstruction preventing the existence of primes of Koblitz reduction. Although Conjecture 1.3 remains open even under GRH, upper bounds for $\pi_E^{\text{prime}}(x)$ have been studied by several authors. A notable result is due to A. C. Cojocaru [17], who proved that for a non-CM $E/\mathbb{Q}$ of conductor N_E, we have

$$\pi_E^{\text{prime}}(x) \ll_{N_E} \frac{x}{\log^2 x} \tag{6}$$

as $x \to \infty$, under the quasi-GRH. (See [17, p. 268].) For CM curves, she applied Selberg's sieve to prove that the upper bound holds unconditionally, independently of the conductor. Later, C. David and J. Wu [21] improved (6) into an effective upper bound for non-CM curves under the quasi-GRH. However, a lower bound for $\pi_E^{\text{prime}}(x)$ remains unknown.

A related problem is to understand how many prime factors the group order $|\widetilde{E}_p(\mathbb{F}_p)|$ has as p varies. One of the first major advances in this direction was made by S. A. Miri and V. K. Murty [45]. Given a positive integer N, let $\nu(N)$ denote the number of prime factors of N, counted with multiplicity. They demonstrated that, assuming GRH, for any non-CM elliptic curve $E/\mathbb{Q}$,

$$\#\{p \le x : \nu(|E_p(\mathbb{F}_p)|) \le 16\} \gg_E \frac{x}{\log^2 x},$$

as $x \to \infty$. This line of research was continued by many mathematicians, leading to successive improvements: the bound of 16 was reduced to 8 for non-CM curves under GRH, and to 5 for CM curves unconditionally (see, for example, [17, 21, 54]).

In 2011, A. Balog, A. C. Cojocaru, and C. David obtained a local result for the average version of the Koblitz problem and applied it to deduce the following global results.

Theorem 1.4 ([4, Theorem 1]). *Set $x > 0$ and $\epsilon > 0$. Let $A := A(x)$ and $B := B(x)$ be parameters satisfying $x^\epsilon < A, B$ and $AB > x\log^{10} x$. There exists a constant $C^{\text{prime}} > 0$ for which*

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \pi_E^{\text{prime}}(x) \sim C^{\text{prime}} \cdot \frac{x}{\log^2 x}, \qquad \text{as } x \to \infty.$$

The average constant C^{prime} is defined in (33). The inequality conditions on A and B can also be relaxed as in Akbary and Felix [2, Equation (1.8)].

A natural inquiry is whether each of these average results is consistent with the corresponding conjectured outcomes on average. This question was answered by Jones [30], assuming an affirmative answer to Serre's uniformity question (Question 2.3).

Theorem 1.5 ([30, Theorem 6]). *Assume an affirmative answer to Serre's uniformity question. Let $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$. There exists an exponent $\gamma > 0$ such that for any positive integer t, we have*

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \left|C_E^{\mathcal{X}} - C^{\mathcal{X}}\right|^t \ll_t \max\left\{\left(\frac{\log B\cdot\log^7 A}{B}\right)^{t/t+1}, \frac{\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}}\right\},$$

as $\min\{A,B\} \to \infty$.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

In particular, by taking $t = 1$, Theorem 1.5 gives a result on the average value of the constants $C_E^{\mathcal{X}}$. Indeed, suppose that $A \coloneqq A(x)$ and $B \coloneqq B(x)$ tend to infinity as $x \to \infty$ and assume an affirmative answer to Serre's uniformity question and that $(\log B \log^7 A)/B \to 0$ as $x \to \infty$. Then for $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$, we have

$$\frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} C_E^{\mathcal{X}} \to C^{\mathcal{X}}.$$

This verifies that the average of the constants $C_E^{\mathcal{X}}$ aligns with the average constants $C^{\mathcal{X}}$.

In this paper, we utilize Zywina's approach to propose the Koblitz constant $C_{E,n,k}^{\text{prime}}$ for primes in arithmetic progressions. Unlike the cyclicity problem, the average version of the Koblitz constant $C_{E,n,k}^{\text{prime}}$ has not yet been considered. We address this gap in the literature by providing a candidate for $C_{n,k}^{\text{prime}}$, the average version of $C_{E,n,k}^{\text{prime}}$, in (42). We illustrate the suitability of these conjectural constants by proving an analogous version of Theorem 1.5 for them.

We start by formulating the Koblitz conjecture for primes in arithmetic progressions.

Conjecture 1.6. If $E/\mathbb{Q}$ is an elliptic curve, then there exists $C_{E,n,k}^{\text{prime}} \geq 0$ for which

$$\pi_E^{\text{prime}}(x; n, k) \sim C_{E,n,k}^{\text{prime}} \cdot \frac{x}{\log^2 x},$$

as $x \to \infty$, where $C_{E,n,k}^{\text{prime}}$ is the explicit constant defined in (35).

As before, if $C_{E,n,k}^{\text{prime}} = 0$, we interpret the above as saying that $\pi_E^{\text{prime}}(x; n, k)$ is bounded as $x \to \infty$. As one piece of evidence to suggest $C_{n,k}^{\text{prime}}$ is the correct average constant, we compare it with the constant $C_{E,n,k}^{\text{prime}}$ for Serre curves which, by Jones [31], make up a density 1 set of elliptic curves when ordered by naive height.

To state our theorem, we first introduce some notation. Associated to E, we define the constant

$$L = \prod_{\ell \mid m_E} \ell^{\alpha_\ell}, \qquad \text{where} \qquad \alpha_\ell = \begin{cases} v_\ell(n) & \text{if } \ell \mid n, \\ 1 & \text{otherwise,} \end{cases} \tag{7}$$

where m_E denotes the adelic level of E (defined in Sections 2.1 and 2.3) and $v_\ell(n)$ denotes the ℓ-adic valuation of n. The constants m_E and L play a crucial role in computing $C_{E,n,k}^{\text{cyc}}$ and $C_{E,n,k}^{\text{prime}}$. For a Serre curve E, Proposition 2.4 gives a straightforward formula for m_E,

$$m_E = \begin{cases} 2|\Delta'| & \text{if } \Delta' \equiv 1 \pmod 4, \\ 4|\Delta'| & \text{otherwise,} \end{cases}$$

where Δ' denotes the squarefree part of the discriminant Δ_E of any Weierstrass model of E.

Theorem 1.7. *Let $E/\mathbb{Q}$ be a Serre curve and let m_E, Δ', and L be as above. If $m_E \nmid L$, then*

$$C_{E,n,k}^{\text{cyc}} = C_{n,k}^{\text{cyc}} \qquad \text{and} \qquad C_{E,n,k}^{\text{prime}} = C_{n,k}^{\text{prime}}.$$

Otherwise, if $m_E \mid L$, then

$$C_{E,n,k}^{\text{cyc}} = C_{n,k}^{\text{cyc}} \left(1 + \tau^{\text{cyc}} \frac{1}{5} \prod_{\substack{\ell \mid L \\ \ell \nmid 2n}} \frac{1}{\ell^4 - \ell^3 - \ell^2 + \ell - 1} \right),$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$C^{\text{prime}}_{E,n,k} = C^{\text{prime}}_{n,k}\left(1 + \tau^{\text{prime}} \prod_{\substack{\ell | L \\ \ell \nmid 2n}} \frac{1}{\ell^3 - 2\ell^2 - \ell + 3}\right),$$

where $\tau^{\text{cyc}}, \tau^{\text{prime}} \in \{\pm 1\}$ *are defined in Definition 5.1.*

Remark 1.8. For a Serre curve E, the constant $C^{\text{cyc}}_{E,n,k}$ was previously obtained by Brau [11, Proposition 2.5.8] under the assumption that $\Delta' \notin \{-2,-1,2\}$. Our formula for $C^{\text{cyc}}_{E,n,k}$ does not require this assumption and it aligns with Brau's.

As another piece of evidence, we also consider the moments of the constants $C^{\text{cyc}}_{E,n,k}$ and $C^{\text{prime}}_{E,n,k}$ for $E \in \mathcal{F}$. Building upon Jones's methods, we improve Theorem 1.5 unconditionally as follows.

Theorem 1.9. *Let n be a positive integer and k be coprime to n. Then there exists an exponent $\gamma > 0$ such that for any positive integer t, we have*

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \left|C^{\text{cyc}}_{E,n,k} - C^{\text{cyc}}_{n,k}\right|^t \ll_t \max\left\{\left(\frac{n\log B \log^7 A}{B}\right)^{\frac{3t}{3t+1}}, \frac{\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}}\right\},$$

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \left|C^{\text{prime}}_{E,n,k} - C^{\text{prime}}_{n,k}\right|^t \ll_{n,t} \max\left\{\left(\frac{n\log B \log^7 A}{B}\right)^{\frac{2t}{2t+1}}, \left(\log\log(\max\{A^3,B^2\})\right)^t \frac{\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}}\right\},$$

as $\min\{A,B\} \to \infty$.

Observe that as $\min\{A,B\} \to \infty$, we have

$$\frac{\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}} \to 0.$$

This gives us the following corollary.

Corollary 1.10. *Fix $n \in \mathbb{N}$. Let k be coprime to n. Let $A \coloneqq A(x)$ and $B \coloneqq B(x)$ both tend to infinity as $x \to \infty$. With the same notation as in Theorem 1.9 and for $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$, we have that*

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} C^{\mathcal{X}}_{E,n,k} \to C^{\mathcal{X}}_{n,k},$$

provided that as $x \to \infty$,

$$\left(\frac{n\log B \log^7 A}{B}\right) \to 0$$

in the cyclicity case and

$$\left(\frac{n\log B \log^7 A}{B}\right) \to 0, \qquad \frac{\left(\log\log(\max\{A^3,B^2\})\right)^t \log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}} \to 0$$

in the Koblitz case.

Based on the above considerations, the constant $C^{\text{prime}}_{n,k}$ that we propose in this paper appears to be a plausible candidate for the average counterpart of $C^{\text{prime}}_{E,n,k}$.

The average constants $C^{\text{cyc}}_{n,k}$ and $C^{\text{prime}}_{n,k}$ are given explicitly and we can compute their values (to any given precision) using the Magma [9] scripts available in this paper's GitHub repository [38]. Below are tables with the values of $C^{\mathcal{X}}_{n,k}$ for $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$ and small moduli n.

$n \setminus k$	1	2	3	4	5
2	0.813752	–	–	–	–
3	0.398219	0.415533	–	–	–
4	0.406876	–	0.406876	–	–
5	0.202164	0.203863	0.203863	0.203863	–
6	0.398219	–	–	–	0.415533

TABLE 1. The value of $C^{\text{cyc}}_{n,k}$ to six decimal places.

$n \setminus k$	1	2	3	4	5
2	0.505166	–	–	–	–
3	0.280648	0.224518	–	–	–
4	0.252583	–	0.252583	–	–
5	0.131482	0.124562	0.124562	0.124562	–
6	0.280648	–	–	–	0.224518

TABLE 2. The value of $C^{\text{prime}}_{n,k}$ to six decimal places.

From the table, we observe that $C^{\mathcal{X}}_{2,1} = C^{\mathcal{X}}$. Moreover, in each table, the sum of the values across any given row yields $C^{\mathcal{X}}$. In Proposition 4.1 and Proposition 4.6, we prove (reassuringly) that these simple checks hold for all moduli.

Let p be a good prime for E. As noted previously,

$$|\widetilde{E}_p(\mathbb{F}_p)| \text{ is prime } \implies \widetilde{E}_p(\mathbb{F}_p) \text{ is cyclic.}$$

Hence, for an arbitrary elliptic curve $E/\mathbb{Q}$, one might suspect that if primes in a certain congruence class are more likely to be primes of Koblitz reduction, then they are also more likely to be primes of cyclic reduction. However, the tables above suggest that the contrary holds on average. Indeed, it follows from the formulas (23) and (42) for $C^{\mathcal{X}}_{n,k}$ that these two average constants are oppositely biased for any given modulus n. More specifically, for any k coprime to n, we have

$$C^{\text{cyc}}_{n,1} \leq C^{\text{cyc}}_{n,k} \leq C^{\text{cyc}}_{n,-1} \qquad \text{while} \qquad C^{\text{prime}}_{n,1} \geq C^{\text{prime}}_{n,k} \geq C^{\text{prime}}_{n,-1}.$$

Furthermore, we have $C^{\text{cyc}}_{n,1} < C^{\text{cyc}}_{n,-1}$ and $C^{\text{prime}}_{n,1} > C^{\text{prime}}_{n,-1}$ if and only if n is not a power of two. The phenomenon of primes being statistically biased over congruence classes is referred to as the average congruence class bias and was first observed in the cyclicity problem by the first author in [37].

Lastly, it is notable that in both tables, $C^{\mathcal{X}}_{5,2} = C^{\mathcal{X}}_{5,3} = C^{\mathcal{X}}_{5,4}$. This is because, for a fixed n, the value of $C^{\mathcal{X}}_{n,k}$ depends solely on whether k is congruent to 1 or not modulo each prime factor of n. Therefore, for a fixed modulus n that is supported by s distinct odd primes, there are at most 2^s distinct values of $C^{\mathcal{X}}_{n,k}$. Whether there are exactly 2^s distinct values is a question proposed by the first author in [37].

1.1. **Outline of the paper.** Sections 2 and 3 provide the essential groundwork for proving the main results. In Section 2, we introduce the properties of Galois representations of elliptic curves. In particular, we introduce the definition of the adelic level and characterize the Galois images of Serre curves and CM curves. In Section 3, we determine the sizes of certain subsets of matrix groups that will be used in calculating the Euler factors of product expansions of $C^{\text{cyc}}_{E,n,k}$ and $C^{\text{prime}}_{E,n,k}$.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Sections 4 and 5 are dedicated to the computation of the constants $C_{E,n,k}^{\mathcal{X}}$ for $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$. These computations extend Zywina's approach (a method that originates from Lang and Trotter's work [36] on the Lang-Trotter conjecture) to obtain C_E^{prime}. The general idea is to interpret the conditions for primes of Koblitz reduction for E in terms of mod m Galois representations, establish the heuristic constant at each level m, and then take the limit as $m \to \infty$. In Section 4, we apply this idea to reformulate the constants C_E^{cyc} and $C_{E,n,k}^{\text{cyc}}$ and express $C_{E,n,k}^{\text{prime}}$ in the form of an almost Euler product. We also propose the average constant $C_{n,k}^{\text{prime}}$ as a complete Euler product. In Section 5, we examine the special case where E is a Serre curve, proving Theorem 1.7 which gives explicit formulas for $C_{E,n,k}^{\text{cyc}}$ and $C_{E,n,k}^{\text{prime}}$ in this case. A critical aspect of these computations involves extracting as many Euler factors as possible from the limits (35) and (45), leading to the crucial definition of L in (7).

Sections 6 and 7 establish bounds for moments of $C_{E,n,k}^{\text{cyc}}$ and $C_{E,n,k}^{\text{prime}}$ for $E \in \mathcal{F}$. In Section 6, we build on the work carried out in Section 5 to bound $C_{E,n,k}^{\text{prime}}$ for non-Serre, non-CM curves and CM curves. Using a result due to D. W. Masser and G. Wüstholz [41], we bound $C_{E,n,k}^{\text{prime}}$ for non-Serre, non-CM curves in terms of the naive height of E. This approach allows us to avoid assuming an affirmative answer to Serre's uniformity question, in contrast to Jones. For CM elliptic curves, we first derive the conjectural constant $C_{E,n,k}^{\text{prime}}$ using a similar method to that of Section 4 and Section 5 and bound it directly from its formula. In Section 7, we adapt the method of Jones [30] to complete the moments computations and prove Theorem 1.9.

Finally, in Section 8, we provide numerical examples that support our results. The numerical examples are computed using the Magma code available in this paper's GitHub repository [38]:

https://github.com/maylejacobj/CyclicityKoblitzAPs

We now summarize the main functions of the repository. The functions `AvgCyclicityAP` and `AvgKoblitzAP` allow one to compute $C_{n,k}^{\text{cyc}}$ and $C_{n,k}^{\text{prime}}$ for given coprime integers n and k, and were used to produce the tables above. Next, the functions `CyclicityAP` and `KoblitzAP` allow one to compute the constants $C_{E,n,k}^{\text{cyc}}$ and $C_{E,n,k}^{\text{prime}}$ for any given non-CM elliptic curve E. These functions are based on Proposition 4.10 and Proposition 4.4 and rely crucially on Zywina's `FindOpenImage` function [61] to compute the adelic image of E. The functions `SerreCurveCyclicityAP` and `SerreCurveKoblitzAP` compute $C_{E,n,k}^{\text{cyc}}$ and $C_{E,n,k}^{\text{prime}}$ for a given Serre curve E using Theorem 1.7 and do not require Zywina's `FindOpenImage`. Lastly, the repository contains code for the examples in Section 8.

1.2. **Notation and conventions.** We now give a brief overview of the notation used throughout the paper.

- For functions $f, g\colon \mathbb{R} \to \mathbb{R}$, we write $f \ll g$ or $f = \mathbf{O}(g)$ if there exists $C > 0$ and $x_0 \geq 0$ such that $|f(x)| \leq Cg(x)$ for all $x > x_0$. If C depends on a parameter m, we write $f \ll_m g$ or $f = \mathbf{O}_m(g)$.
- In the same setting as above, we write $f \sim g$ to denote that $\lim_{x\to\infty} f(x)/g(x) = 1$.
- Let A and B be positive real numbers. Let $\mathcal{F} \coloneqq \mathcal{F}(A, B)$ denote the family of models $Y^2 = X^3 + aX + b$ of elliptic curves for which $|a| \leq A$ and $|b| \leq B$.
- Given a subfamily $\mathcal{G} \subseteq \mathcal{F}$ of elliptic curves, let f and g be functions defined from $\mathcal{G}$ to $\mathbb{R}$. We write $f \ll g$ if there exists an absolute constant $M > 0$ for which $|f(E)| \leq Mg(E)$ for all $E \in \mathcal{G}$. When M depends on a parameter m, we write $f \ll_m g$.
- p and ℓ denote rational primes, n a positive integer, and k an integer coprime to n.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

- We write $p^a \parallel n$ if $p^a \mid n$ and $p^{a+1} \nmid n$. In this case, a is called the p-adic valuation of n, and is denoted by $v_p(n)$.
- Given a positive integer n, n^{odd} denotes the odd part of n, i.e., $n^{\text{odd}} = n/2^{v_2(n)}$.
- We sometimes write (m, n) as shorthand for $\gcd(m, n)$.
- m^∞ denotes an arbitrarily large power of m. Thus, $\gcd(n, m^\infty)$ denotes $\prod_{p\mid(n,m)} p^{v_p(n)}$. If every prime factor of n divides m, then we write $n \mid m^\infty$.
- $\left(\frac{\cdot}{d}\right)$ denotes the Jacobi symbol.
- ϕ denotes the Euler totient function.
- μ denotes the Möbius function.
- $G(m)$ denotes the image of a subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ under the reduction modulo m map.
- Given that $d \mid m$ and $M \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, M_d denotes the reduction of M modulo d.
- If $\mathcal{A}$ is the empty set, then we take $\prod_{a\in\mathcal{A}} a$ to be 1.

1.3. **Acknowledgments.** This paper emerged from some initial conversations at the 2023 LuCaNT (LMFDB, Computation, and Number Theory) conference held at ICERM (Institute for Computational and Experimental Research in Mathematics). We are grateful to the conference organizers and the organizations that provided funding. An earlier version of this manuscript appears in the first author's doctoral thesis. We are thankful for the doctoral committee members for their helpful comments. The third author, who conducted most of the work at the Max Planck Institute for Mathematics, is grateful for its funding and stimulating atmosphere of research.

2. Preliminaries

2.1. **Galois representations and the adelic level.** Let $E/\mathbb{Q}$ be an elliptic curve. Associated to E, we consider the *adelic Tate module*, which is given by the inverse limit

$$T(E) := \varprojlim E[n]$$

where $E[n]$ denotes the n-torsion subgroup of $E(\overline{\mathbb{Q}})$. Let $\widehat{\mathbb{Z}}$ denote the ring of profinite integers. It is well known that $T(E)$ is a free $\widehat{\mathbb{Z}}$-module of rank 2. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on $T(E)$, giving rise to the *adelic Galois representation* of E,

$$\rho_E\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(T(E)).$$

Upon fixing a $\widehat{\mathbb{Z}}$-basis for $T(E)$, we consider ρ_E as a map

$$\rho_E\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Let G_E denote the image of ρ_E, which, because of the above choice of basis, is defined only up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. With respect to the profinite topology on $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, the subgroup G_E is necessarily closed since ρ_E is a continuous map.

We now state a foundational result of Serre, known as Serre's open image theorem.

Theorem 2.1 (Serre, [49, Théorème 3])**.** *If $E/\mathbb{Q}$ is without complex multiplication, then G_E is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. In particular, the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ is finite.*

Suppose that $E/\mathbb{Q}$ is a non-CM elliptic curve. For each positive integer m, let π_m be the natural reduction map

$$\pi_m\colon\ \mathrm{GL}_2(\widehat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Let $G_E(m)$ be the image of the mod m Galois representation

$$\rho_{E,m}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

defined by the composition $\pi_m \circ \rho_E$. It follows from Theorem 2.1 that there exists a positive integer m for which

$$G_E = \pi_m^{-1}(G_E(m)). \tag{8}$$

One may observe that (8) is equivalent to the statement that for every $n \in \mathbb{N}$,

$$G_E(n) = \pi^{-1}(G_E(\gcd(n,m))) \tag{9}$$

where $\pi\colon \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \operatorname{GL}_2(\mathbb{Z}/\gcd(n,m)\mathbb{Z})$ denotes the natural reduction map. The least positive integer m with this property is called the *adelic level* of E, and is denoted by m_E. The constant m_E accounts for both the nonsurjectivity of the ℓ-adic Galois representations of E as well as the entanglements between their images.

We now give a fundamental property of m_E that we will use several times.

Lemma 2.2. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E. For any $d_1, d_2 \in \mathbb{N}$ with $d_1 \mid m_E^\infty$ and $(d_2, m_E) = 1$, we have*

$$G_E(d_1 d_2) \simeq G_E(d_1) \times \operatorname{GL}_2(\mathbb{Z}/d_2\mathbb{Z})$$

via the map $\operatorname{GL}_2(\mathbb{Z}/d_1 d_2\mathbb{Z}) \to \operatorname{GL}_2(\mathbb{Z}/d_1\mathbb{Z}) \times \operatorname{GL}_2(\mathbb{Z}/d_2\mathbb{Z})$.

Proof. By the given conditions, we have $(d_1, d_2) = 1$. Set $d' = \gcd(d_1, m_E)$. Let $\pi\colon \operatorname{GL}_2(\mathbb{Z}/d_1d_2\mathbb{Z}) \to \operatorname{GL}_2(\mathbb{Z}/d'\mathbb{Z})$ and $\pi_1\colon \operatorname{GL}_2(\mathbb{Z}/d_1\mathbb{Z}) \to \operatorname{GL}_2(\mathbb{Z}/d'\mathbb{Z})$ be the natural reduction maps. By the Chinese remainder theorem, π can be identified with

$$\pi_1 \times \operatorname{triv}\colon \operatorname{GL}_2(\mathbb{Z}/d_1\mathbb{Z}) \times \operatorname{GL}_2(\mathbb{Z}/d_2\mathbb{Z}) \to \operatorname{GL}_2(\mathbb{Z}/d'\mathbb{Z}) \times \{1\}.$$

By (9), we have that

$$G_E(d_1d_2) = \pi^{-1}(G_E(d')) \simeq (\pi_1 \times \operatorname{triv})^{-1}(G_E(d')) = G_E(d_1) \times \operatorname{GL}_2(\mathbb{Z}/d_2\mathbb{Z}). \qquad \square$$

We conclude this subsection by recalling Serre's uniformity question.

Question 2.3. Does there exist an absolute constant c such that for each elliptic curve $E/\mathbb{Q}$,

$$G_E(\ell) = \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

holds for all rational primes $\ell > c$?

While Question 2.3 remains open, it is widely conjectured to be true with $c = 37$ [56, 63] and considerable partial progress has been made toward its resolution [3, 24, 39, 43, 49, 50].

2.2. **Serre curves.** In this subsection, we introduce the generic class of elliptic curves $E/\mathbb{Q}$ with maximal adelic Galois image G_E, and provide an explicit description of G_E for curves in this class.

Serre noted [49] that for an elliptic curve $E/\mathbb{Q}$, the adelic Galois representation ρ_E cannot be surjective[2], that is, the adelic level m_E is never 1. We briefly give the argument here. If E has complex multiplication, then $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ is necessarily infinite [49], so we restrict our attention to the case that E is non-CM. Assume that E is defined by the factored Weierstrass equation

$$Y^2 = (X - e_1)(X - e_2)(X - e_3)$$

with $e_1, e_2, e_3 \in \overline{\mathbb{Q}}$. Then, the 2-torsion of E is given by

$$E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Consequently, $\operatorname{Aut}(E[2])$ can be identified with S_3. The discriminant Δ_E of E is given by

$$\Delta_E = [(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)]^2. \tag{10}$$

[2]Over some number fields $K \neq \mathbb{Q}$, there exist elliptic curves E/K for which ρ_E is surjective [26].

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Let Δ' denote the squarefree part of Δ_E, i.e., the unique squarefree integer such that $\Delta_E/\Delta' \in (\mathbb{Q}^\times)^2$. Note that the discriminant Δ_E depends on the Weierstrass model of E, but Δ' does not.

Let us first assume that $\Delta_E \notin (\mathbb{Q}^\times)^2$. Let d_E be the conductor of $\mathbb{Q}(\sqrt{\Delta_E})$, that is, the smallest positive integer such that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_{d_E})$. It is straightforward to check that

$$d_E = \begin{cases} |\Delta'| & \text{if } \Delta' \equiv 1 \pmod 4, \\ 4|\Delta'| & \text{otherwise.} \end{cases}$$

Let us define the quadratic character associated to $\mathbb{Q}(\sqrt{\Delta_E})$ as follows,

$$\chi_{\Delta_E}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\text{rest.}} \operatorname{Gal}(\mathbb{Q}(\sqrt{\Delta_E})/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}.$$

Fix $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Viewing $\rho_{E,2}(\sigma) \in G_E(2) \subseteq \operatorname{Aut}(E[2]) \simeq S_3$, by (10), we notice that

$$\chi_{\Delta_E}(\sigma)\left(\sqrt{\Delta_E}\right) = \epsilon(\rho_{E,2}(\sigma))\left(\sqrt{\Delta_E}\right),$$

where $\epsilon\colon S_3 \to \{\pm 1\}$ denotes the signature map.[3] Hence, $\chi_{\Delta_E}(\sigma) = \epsilon(\rho_{E,2}(\sigma))$.

On the other hand, we have that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_{d_E})$. Since $\operatorname{Gal}(\mathbb{Q}(\zeta_{d_E})/\mathbb{Q}) \simeq (\mathbb{Z}/d_E\mathbb{Z})^\times$, there exists a unique quadratic character $\alpha\colon \operatorname{Gal}(\mathbb{Q}(\zeta_{d_E})/\mathbb{Q}) \to \{\pm 1\}$ for which $\chi_{\Delta_E}(\sigma) = \alpha(\det \circ \rho_{E,d_E}(\sigma))$ for any $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, we have

$$\epsilon(\rho_{E,2}(\sigma)) = \alpha(\det \circ \rho_{E,d_E}(\sigma)) \tag{11}$$

for any $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let $M_E := \operatorname{lcm}(2, d_E)$. Consider the subgroup

$$H_E(M_E) = \{M \in \operatorname{GL}_2(\mathbb{Z}/M_E\mathbb{Z}) : \epsilon(M_2) = \alpha(\det M_{d_E})\},$$

where M_2 and M_{d_E} denote the reductions of M modulo 2 and d_E, respectively. Note that the index of $H_E(M_E)$ in $\operatorname{GL}_2(\mathbb{Z}/M_E\mathbb{Z})$ is 2 and that $G_E(M_E) \subseteq H_E(M_E)$ by (11). We define

$$H_E := \pi^{-1}(H_E(M_E)) \tag{12}$$

where $\pi\colon \operatorname{GL}_2(\widehat{\mathbb{Z}}) \to \operatorname{GL}_2(\mathbb{Z}/M_E\mathbb{Z})$ is the natural reduction map. Then H_E is an index 2 subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ that contains G_E. We say that E is a *Serre curve* if $H_E = G_E$, that is, $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : G_E] = 2$.

In the above discussion, we supposed that $\Delta_E \notin (\mathbb{Q}^\times)^2$. We now consider the opposite case that $\Delta_E \in (\mathbb{Q}^\times)^2$. Let $\mathbb{Q}(E[2]) = \mathbb{Q}(e_1, e_2, e_3)$ denote the 2-division field of E. Observe that $[\mathbb{Q}(E[2]) : \mathbb{Q}]$ divides 3, and hence $[\operatorname{GL}_2(\mathbb{Z}/2\mathbb{Z}) : G_E(2)]$ is divisible by 2. Thus, by [42, Proposition 2.14], $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : G_E] \geq 12$, which follows by considering the index of the commutator of G_E in $\operatorname{SL}_2(\widehat{\mathbb{Z}})$. In particular, E cannot be a Serre curve in this case.

Serre curves are useful for us for two key reasons. First, as mentioned in the introduction, Jones [31] showed that they are "generic" in the sense that the density of the subfamily of Serre curves among the family of all elliptic curves ordered by naive height is 1. Second, the adelic image G_E of a Serre curve E can be explicitly described, as we will now discuss.

Proposition 2.4. *Let $E/\mathbb{Q}$ be a Serre curve and write Δ' to denote the squarefree part of the discriminant of E. Then*

$$m_E = \begin{cases} 2|\Delta'| & \text{if } \Delta' \equiv 1 \pmod 4, \\ 4|\Delta'| & \text{otherwise.} \end{cases} \tag{13}$$

[3]Note that the value of $\epsilon(\rho_{E,2}(\sigma))$ is independent of the choice of isomorphism $\operatorname{Aut}(E[2]) \simeq S_3$.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Furthermore, for any positive integer m,

$$G_E(m) = \begin{cases} \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) & \text{if } m_E \nmid m, \\ H_E(m) & \text{if } m_E \mid m, \end{cases}$$

where $H_E(m)$ denotes the image of H_E, defined in (12), under the reduction modulo m map.

Proof. The proof of (13) can be found in [30, pp. 696–697]. Hence, $m_E = M_E$ where M_E is defined as above. Now, let m be a positive integer. By [30, Equation (13)] and (9), one may deduce that $G_E(m) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ if $m_E \nmid m$. Suppose $m_E \mid m$. Then, $G_E(m) \subseteq H_E(m)$. The containment must be equal; otherwise, the index of G_E in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is greater than $[\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : H_E(m)] = [\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : H_E(m_E)] = 2$, contradicting the assumption that $E/\mathbb{Q}$ is a Serre curve. □

In order to compute $C^{\mathcal{X}}_{E,n,k}$, we need to know G_E (meaning we must know the adelic level m_E and the image of G_E modulo m_E). For Serre curves, this is particularly tractable, and was exploited in the work of Jones [30]. We now give the description of G_E for Serre curves.

First, we define $\chi_4 \colon (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}$ and $\chi_8 \colon (\mathbb{Z}/8\mathbb{Z})^\times \to \{\pm 1\}$ as follows:

$$\chi_4(k) = \begin{cases} 1 & \text{if } k \equiv 1 \pmod 4 \\ -1 & \text{if } k \equiv 3 \pmod 4 \end{cases}, \quad \chi_8(k) = \begin{cases} 1 & \text{if } k \equiv 1, 7 \pmod 8 \\ -1 & \text{if } k \equiv 3, 5 \pmod 8 \end{cases}.$$

We define the character $\psi_m \colon \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \{\pm 1\}$ associated to E by

$$\psi_m = \prod_{\ell^\alpha \| m} \psi_{\ell^\alpha},$$

where $\psi_{\ell^\alpha} \colon \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) \to \{\pm 1\}$ is defined for $M \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})$ by

$$\psi_{\ell^\alpha}(M) = \begin{cases} \left(\frac{\det M_\ell}{\ell}\right) & \text{if } \ell \text{ is odd}, \\ \epsilon(M_2) & \text{if } \ell = 2, \alpha \geq 1, \text{ and } \Delta' \equiv 1 \pmod 4, \\ \chi_4(\det M_4)\epsilon(M_2) & \text{if } \ell = 2, \alpha \geq 2, \text{ and } \Delta' \equiv 3 \pmod 4, \\ \chi_8(\det M_8)\epsilon(M_2) & \text{if } \ell = 2, \alpha \geq 3, \text{ and } \Delta' \equiv 2 \pmod 8, \\ \chi_8(\det M_8)\chi_4(\det M_4)\epsilon(M_2) & \text{if } \ell = 2, \alpha \geq 3, \text{ and } \Delta' \equiv 6 \pmod 8, \\ 1 & \text{otherwise}. \end{cases}$$

As noted in [30, p. 701], given $m_E \mid m$, one may see that for $M \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we have

$$\epsilon(M_2)\left(\frac{\Delta'}{\det M_{m_E}}\right) = \psi_m(M).$$

In particular, we have $H_E(m) = \ker \psi_m$. Thus G_E is the preimage of $\ker \psi_m$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

2.3. **Galois representations in the CM case.** Having discussed Galois representations for non-CM elliptic curves, we now turn to the CM case. Suppose that E has CM by an order $\mathcal{O}$ in an imaginary quadratic field K. In this case, the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts naturally on $T(E)$, which is a one-dimensional $\widehat{\mathcal{O}}$-module, where $\widehat{\mathcal{O}}$ denotes the profinite completion of $\mathcal{O}$. Hence, we can construct the adelic Galois representation associated to E,

$$\rho_E \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T(E)) \simeq \mathrm{GL}_1(\widehat{\mathcal{O}}) \simeq \widehat{\mathcal{O}}^\times.$$

Let G_E denote the image of ρ_E. We now state Serre's open image theorem for CM elliptic curves.

Theorem 2.5 (Serre, [49, p. 302, Corollaire]). *If $E/\mathbb{Q}$ has CM by $\mathcal{O}$, then G_E is an open subgroup of $\widehat{\mathcal{O}}^\times$. In particular, the index $[\widehat{\mathcal{O}}^\times : G_E]$ is finite.*

For each positive integer m, consider the natural reduction map

$$\pi_m \colon \widehat{\mathcal{O}}^\times \to (\mathcal{O}/m\mathcal{O})^\times.$$

Let $G_E(m)$ denote the image of the modulo m Galois representation

$$\rho_{E,m} : \mathrm{Gal}(\overline{K}/K) \to (\mathcal{O}/m\mathcal{O})^\times$$

defined by the composition $\pi_m \circ \rho_E$. It follows from Theorem 2.5 that

$$G_E = \pi_m^{-1}(G_E(m)) \tag{14}$$

for some positive integer m. As in the non-CM case, (14) is equivalent to the statement that for every $n \in \mathbb{N}$,

$$G_E(n) = \pi^{-1}(G_E(\gcd(n, m))), \tag{15}$$

where $\pi \colon (\mathcal{O}/n\mathcal{O})^\times \to (\mathcal{O}/\gcd(n, m)\mathcal{O})^\times$ is the natural reduction map.

In the CM case, we follow [30, p. 693] to define m_E to be the smallest positive integer m such that (15) holds and for which

$$4 \left(\prod_{\ell \text{ ramifies in } K} \ell \right) \text{ divides } m. \tag{16}$$

One can prove the following using the same argument sketched in the proof of Lemma 2.2.

Lemma 2.6. *Let $E/\mathbb{Q}$ be a CM elliptic curve of level m_E. For any $d_1, d_2 \in \mathbb{N}$ with $d_1 \mid m_E^\infty$ and $(d_2, m_E) = 1$, we have*

$$G_E(d_1 d_2) \simeq G_E(d_1) \times (\mathcal{O}/d_2\mathcal{O})^\times.$$

Lemmas 2.2 and 2.6 are used to express the constants $C_{E,n,k}^{\mathrm{cyc}}$ and $C_{E,n,k}^{\mathrm{prime}}$ as almost Euler products. It is worth noting that both lemmas hold even if m_E is replaced by any positive multiple of it. Thus, the minimality condition in the definition of m_E for both non-CM and CM curves is not required from a theoretical perspective for us. Nonetheless, the minimality of m_E is useful for our computations as it allows us to extract more Euler factors.

Let $K/\mathbb{Q}$ be an imaginary quadratic field. We denote its ring of integers by $\mathcal{O}_K$. Let $\mathcal{O}$ be an order of K. The index $f = [\mathcal{O}_K : \mathcal{O}]$ is necessarily finite and is called the *conductor* of $\mathcal{O}$. Let χ_K be the Dirichlet character defined by

$$\chi_K(\ell) = \begin{cases} 0 & \text{if } \ell \text{ ramifies in } K, \\ 1 & \text{if } \ell \text{ splits in } K, \\ -1 & \text{if } \ell \text{ is inert in } K. \end{cases} \tag{17}$$

Let d_K be the discriminant of K. One can check that

$$\chi_K(\ell) = \left(\frac{d_K}{\ell} \right)$$

for each odd prime ℓ. By [46, Theorem 9.13], we see that χ_K is a primitive quadratic character.

We now state a lemma on the size of the image of mod ℓ^α Galois representation of E for $\ell \nmid f m_E$.

Lemma 2.7. *Let $E/\mathbb{Q}$ be a CM elliptic curve. For $\ell \nmid f m_E$, we have*

$$|G_E(\ell^\alpha)| = \ell^{2(\alpha-1)}(\ell - 1)(\ell - \chi_K(\ell)).$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Proof. Since $\mathcal{O}$ is an order of class number 1, we have

$$\mathcal{O}/(\ell\mathcal{O}_K \cap \mathcal{O}) = \mathcal{O}/\ell\mathcal{O} \simeq \mathcal{O}_K/\ell\mathcal{O}_K$$

for any $\ell \nmid f$. (See [20, Proposition 7.20].) By Lemma 2.6, we have $G_E(\ell^\alpha) \simeq (\mathcal{O}_K/\ell^\alpha\mathcal{O}_K)^\times$. Applying [12, Equation (4)], we obtain the desired results. □

Moreover, we have the following uniformity result for CM elliptic curves over $\mathbb{Q}$.

Proposition 2.8. *There is an absolute constant C such that*

$$fm_E \leq C$$

holds for all CM elliptic curves $E/\mathbb{Q}$.

Proof. It suffices to show that the index $[\widehat{\mathcal{O}}^\times : G_E]$, the product of ramified primes in (16), and the conductor $f = [\mathcal{O}_K : \mathcal{O}]$ of the CM-order $\mathcal{O}$ are uniformly bounded for $E/\mathbb{Q}$. This follows from the fact that there are only finitely many endomorphism rings for CM elliptic curves over $\mathbb{Q}$ and [10, Theorem 1.1]. In fact, for CM elliptic curves $E/\mathbb{Q}$, it is known that the conductor of $\mathcal{O}$ is at most 3. (See [53, Appendix C, Example 11.3.2].) □

3. Counting matrices

In this section, we will establish counting results that will play pivotal roles in determining the cyclicity and Koblitz constants for arithmetic progressions. We first outline the general strategy.

Let ℓ be a prime and $\mathcal{P}_\ell$ be a property that certain matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ satisfy. Let m and n be positive integers and k be coprime to n. Suppose that we are interested in counting the size of the set

$$X(m) := \{M \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : M_\ell \text{ satisfies } \mathcal{P}_\ell \text{ for each } \ell \mid m, \det M \equiv k \pmod{\gcd(n,m)}\},$$

where M_ℓ denotes the reduction of M modulo ℓ. By the Chinese remainder theorem, it suffices to count the size of $X(\ell^a)$ for each $\ell^a \parallel m$. Also, note that the reduction map $\pi : \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ induces a surjective map $X(\ell^a) \to X(\ell)$ and further $X(\ell^a) = \pi^{-1}(X(\ell))$. Consequently, the problem of counting the size of $X(m)$ reduces to counting the size of $X(\ell)$ for each $\ell \mid m$.

The condition that ℓ is a prime of cyclic or Koblitz reduction for E can be interpreted as a condition on matrices modulo primes. Thus, with the above strategy in mind, we give a lemma and corollary that will be used to compute the cyclicity constant $C_{E,n,k}^{\mathrm{cyc}}$ for non-CM curves.

Lemma 3.1. *Let ℓ be a prime, a be a positive integer, and k be an integer coprime to ℓ. Fix $M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $\det M \equiv k \pmod{\ell}$. For any integer $\widetilde{k}$ with $\widetilde{k} \equiv k \pmod{\ell}$, we have*

$$\#\left\{\widetilde{M} \in \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) : \widetilde{M} \equiv M \pmod{\ell}, \det \widetilde{M} \equiv \widetilde{k} \pmod{\ell^a}\right\} = \ell^{3(a-1)}.$$

Proof. Let $\pi\colon \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ denote the reduction modulo ℓ map, which is a surjective group homomorphism. For any $M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we have that

$$\pi^{-1}(M) = \left\{\widetilde{M} \in \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) : \widetilde{M} \equiv M \pmod{\ell}\right\}.$$

The image of $\pi^{-1}(M)$ under $\det\colon \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) \to (\mathbb{Z}/\ell^a\mathbb{Z})^\times$ is

$$\det(\pi^{-1}(M)) = \{k' \in (\mathbb{Z}/\ell^a\mathbb{Z})^\times : k' \equiv k \pmod{\ell}\}.$$

Hence, for any integer $\widetilde{k}$ with $\widetilde{k} \equiv k \pmod{\ell}$, we have

$$\#\left\{\widetilde{M} \in \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) : \widetilde{M} \equiv M \pmod{\ell}, \det \widetilde{M} \equiv \widetilde{k} \pmod{\ell^a}\right\} = \frac{|\pi^{-1}(M)|}{|\det(\pi^{-1}(M))|}.$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Finally, we note that $|\pi^{-1}(M)| = |\ker(\pi)| = \ell^{4(a-1)}$ and $|\det(\pi^{-1}(M))| = \ell^{a-1}$. □

Corollary 3.2. *Fix a prime ℓ and positive integer a. Let k be an integer coprime to ℓ. Then*

$$\#\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) : M \not\equiv I \pmod{\ell}, \det M \equiv k \pmod{\ell^a}\}$$
$$= \begin{cases} \ell^{3(a-1)} \cdot (\ell^3 - \ell - 1) & \text{if } k \equiv 1 \pmod{\ell}, \\ \ell^{3(a-1)} \cdot (\ell^3 - \ell) & \text{if } k \not\equiv 1 \pmod{\ell}. \end{cases}$$

Proof. Let $M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If $M \not\equiv I \pmod{\ell}$, then any lifting $\widetilde{M}$ of M in $\mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z})$ satisfies $\widetilde{M} \not\equiv I \pmod{\ell}$. If $k \not\equiv 1 \pmod{\ell}$, then $\det M \equiv k \pmod{\ell}$ guarantees that $M \not\equiv I \pmod{\ell}$. Since the determinant map $\det\colon \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ is a surjective group homomorphism, one can check that there are $\ell^3 - \ell$ matrices M in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $\det M \equiv k \pmod{\ell}$. On the other hand, if $k \equiv 1 \pmod{\ell}$, we have one less choice for M. Along with Lemma 3.1, we obtain the desired results. □

The next lemma gives a corollary that will be useful when computing the Koblitz constant $C_{E,n,k}^{\mathrm{prime}}$ for non-CM curves.

Lemma 3.3. *Let ℓ be an odd prime, t be an integer, and d be an integer coprime to ℓ. Then we have*

$$\#\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det M \equiv d \pmod{\ell}, \operatorname{tr} M \equiv t \pmod{\ell}\} = \ell^2 + \ell \cdot \left(\frac{t^2 - 4d}{\ell}\right),$$

where $\left(\frac{\cdot}{\ell}\right)$ denotes the Legendre symbol. If $\ell = 2$, then we have

$$\#\{M \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \det M \equiv 1 \pmod{2}, \operatorname{tr} M \equiv t \pmod{2}\} = \begin{cases} 4 & \text{if } t \equiv 0 \pmod{2}, \\ 2 & \text{if } t \equiv 1 \pmod{2}. \end{cases}$$

Proof. The case when $\ell = 2$ follows from a direct calculation. See [18, Lemma 2.7] for the case when ℓ is odd. □

Corollary 3.4. *Fix a prime ℓ and positive integer a. Let k be an integer coprime to ℓ. Then*

$$\#\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z}) : \det(M - I) \not\equiv 0 \pmod{\ell}, \det M \equiv k \pmod{\ell^a}\}$$
$$= \begin{cases} \ell^{3(a-1)} \cdot (\ell^3 - \ell^2 - \ell) & \text{if } k \equiv 1 \pmod{\ell}, \\ \ell^{3(a-1)} \cdot (\ell^3 - \ell^2 - 2\ell) & \text{if } k \not\equiv 1 \pmod{\ell}. \end{cases}$$

Proof. Let $M \in \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z})$ be such that $\det M \equiv k \pmod{\ell^a}$ and note that

$$\det(M - I) \equiv 0 \pmod{\ell} \iff \operatorname{tr} M \equiv k + 1 \pmod{\ell}.$$

Thus, if $\ell \neq 2$, we have that

$$\left(\frac{(k+1)^2 - 4k}{\ell}\right) = \left(\frac{(k-1)^2}{\ell}\right) = \begin{cases} 0 & \text{if } k \equiv 1 \pmod{\ell}, \\ 1 & \text{if } k \not\equiv 1 \pmod{\ell}. \end{cases}$$

By Lemma 3.3, this completes the proof when $\ell \neq 2$. When $\ell = 2$ and $a = 1$, it is straightforward to check that the lemma holds. □

Now, we turn our attention to the CM case. Let K be an imaginary quadratic field and write $\mathcal{O}_K$ to denote the ring of integers of K. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank 2. Fixing a $\mathbb{Z}$-basis, we can identify $\mathrm{GL}_1(\mathcal{O}_K) = \mathcal{O}_K^\times$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z})$. In the following discussion (and henceforth) the determinant of g for $g \in \mathcal{O}_K^\times$ means the determinant of g considered as

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

a matrix in $\mathrm{GL}_2(\mathbb{Z})$. Moreover, we note that for any odd rational prime ℓ and integer $a \geq 1$, the determinant of any element in $\ell^a \mathcal{O}_K$ lies in $\ell^a\mathbb{Z}$, so we obtain the induced determinant map $\det\colon (\mathcal{O}_K/\ell^a\mathcal{O}_K)^\times \to (\mathbb{Z}/\ell^a\mathbb{Z})^\times$, which does not depend on the choice of the basis.

Lemma 3.5. *Let K be an imaginary quadratic field and $\mathcal{O}_K$ be the ring of integers of K. Let ℓ be an odd rational prime unramified in K and a be a positive integer. Let k be an integer that is coprime to ℓ and fix $g \in (\mathcal{O}_K/\ell\mathcal{O}_K)^\times$ with $\det g \equiv k \pmod{\ell}$. Then*

$$\#\left\{\widetilde{g} \in (\mathcal{O}_K/\ell^a\mathcal{O}_K)^\times : \widetilde{g} \equiv g \pmod{\ell\mathcal{O}_K}, \det\widetilde{g} \equiv k \pmod{\ell^a}\right\} = \ell^{a-1}.$$

Proof. The reduction map $\pi\colon (\mathcal{O}_K/\ell^a\mathcal{O}_K)^\times \to (\mathcal{O}_K/\ell\mathcal{O}_K)^\times$ is a surjective group homomorphism. Regardless of whether ℓ splits or is inert in K, we have $|\ker\pi| = \ell^{2(a-1)}$ by Lemma 2.7. Therefore,

$$\#\left\{\widetilde{g} \in (\mathcal{O}_K/\ell^a\mathcal{O}_K)^\times : \widetilde{g} \equiv g \pmod{\ell\mathcal{O}_K}\right\} = |\pi^{-1}(g)| = |\ker\pi| = \ell^{2(a-1)}.$$

The image of $\pi^{-1}(g)$ under $\det\colon (\mathcal{O}_K/\ell^a\mathcal{O}_K)^\times \to (\mathbb{Z}/\ell^a\mathbb{Z})^\times$ is

$$\det(\pi^{-1}(g)) = \left\{k' \in (\mathbb{Z}/\ell^a\mathbb{Z})^\times : k' \equiv k \pmod{\ell}\right\}.$$

Thus, we have $\left|\det(\pi^{-1}(g))\right| = \ell^{a-1}$. Finally, note that

$$\#\left\{\widetilde{g} \in (\mathcal{O}/\ell^a\mathcal{O})^\times : \widetilde{g} \equiv g \pmod{\ell\mathcal{O}_K}, \det g \equiv k \pmod{\ell^a}\right\} = \frac{|\pi^{-1}(g)|}{|\det(\pi^{-1}(g))|} = \ell^{a-1}.$$

□

We now prove a corollary that will be used for the computation of the Koblitz constant $C_{E,n,k}^{\mathrm{prime}}$ for CM curves.

Corollary 3.6. *Let K be an imaginary quadratic field. Fix an odd rational prime ℓ that is unramified in K. Let k be an integer that is coprime to ℓ. If ℓ splits in K, then*

$$\begin{aligned}\#\{g \in (\mathcal{O}_K/\ell^a\mathcal{O}_K)^\times &: \det(g-1) \not\equiv 0 \pmod{\ell}, \det g \equiv k \pmod{\ell^a}\}\\ &= \begin{cases}\ell^{a-1}(\ell-2) & \text{if } k \equiv 1 \pmod{\ell},\\ \ell^{a-1}(\ell-3) & \text{if } k \not\equiv 1 \pmod{\ell}.\end{cases}\end{aligned}$$

If ℓ is inert in K, then

$$\begin{aligned}\#\{g \in (\mathcal{O}_K/\ell^a\mathcal{O}_K)^\times &: \det(g-1) \not\equiv 0 \pmod{\ell}, \det g \equiv k \pmod{\ell^a}\}\\ &= \begin{cases}\ell^{a} & \text{if } k \equiv 1 \pmod{\ell},\\ \ell^{a-1}(\ell+1) & \text{if } k \not\equiv 1 \pmod{\ell}.\end{cases}\end{aligned}$$

Proof. By Lemma 3.5, it suffices to consider the case where $a = 1$. Suppose ℓ splits in K. Then we have that $\mathcal{O}_K/\ell\mathcal{O}_K \simeq \mathbb{F}_\ell \times \mathbb{F}_\ell$ and the determinant map $\det\colon \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times \to \mathbb{F}_\ell^\times$ is identified with the multiplication map $(a, b) \mapsto ab$. Thus, the set in question can be expressed as

$$\left\{(g_1, g_2) \in \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times : g_1 - 1, g_2 - 1 \in \mathbb{F}_\ell^\times, g_1 g_2 \equiv k \pmod{\ell}\right\}.$$

Hence, any element in the set is of the form (g, kg^{-1}) where both g and kg^{-1} are not congruent to 1 modulo ℓ. Thus, the size of the set is $\ell - 2$ if $k \equiv 1 \pmod{\ell}$ and $\ell - 3$ otherwise.

Now, suppose ℓ is inert in K. Then we have $\mathcal{O}_K/\ell\mathcal{O}_K \simeq \mathbb{F}_{\ell^2}$ and the determinant map $\det\colon \mathbb{F}_{\ell^2} \to \mathbb{F}_\ell$ is identified with the norm map $N_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell}\colon x \mapsto x^{\ell+1}$. Thus, the set in question can be expressed as

$$\left\{g \in \mathbb{F}_{\ell^2}^\times : (g-1)^{\ell+1} \in \mathbb{F}_\ell^\times, g^{\ell+1} \equiv k \pmod{\ell}\right\}.$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

For each k coprime to ℓ, there are exactly $\ell+1$ choices of $g \in \mathbb{F}_{\ell^2}^\times$ with $g^{\ell+1} \equiv k \pmod{\ell}$. In case $k \equiv 1 \pmod{\ell}$, we have one less choice due to the constraint $(g-1)^{\ell+1} \in \mathbb{F}_\ell^\times$. □

4. Definitions of the constants

4.1. **On the cyclicity constant.** We keep the notation from Section 2.1. In this subsection, we introduce the definition of the cyclicity constant C_E^{cyc}, given by Serre, and its average counterpart C^{cyc}. For coprime integers n and k, we introduce the cyclicity constant for primes in arithmetic progression $C_{E,n,k}^{\mathrm{cyc}}$, given by Akbal and Güloğlu, and its average counterpart $C_{n,k}^{\mathrm{cyc}}$.

First of all, Serre [52, pp. 465–468] defined the cyclicity constant C_E^{cyc} to be

$$C_E^{\mathrm{cyc}} := \sum_{n\geq 1} \frac{\mu(n)}{[\mathbb{Q}(E[n]):\mathbb{Q}]}, \tag{18}$$

where $\mu(\cdot)$ denotes the Möbius function and $\mathbb{Q}(E[n])$ is the n-th division field of E. He proved that, under GRH, C_E^{cyc} is the density of primes of cyclic reduction for E; see Conjecture 1.1.

For a non-CM elliptic curve $E/\mathbb{Q}$, Jones [30, p. 692] observed that (18) can be expressed as an almost Euler product involving the adelic level of E. Specifically, he showed that

$$C_E^{\mathrm{cyc}} = \left(\sum_{d\mid m_E} \frac{\mu(d)}{[\mathbb{Q}(E[d]):\mathbb{Q}]}\right) \prod_{\ell\nmid m_E} \left(1 - \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right). \tag{19}$$

The average counterpart of C_E^{cyc} is

$$C^{\mathrm{cyc}} := \prod_{\ell} \left(1 - \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \approx 0.813752. \tag{20}$$

As mentioned in the introduction, Gekeler [25] demonstrated that C^{cyc} represents the average cyclicity constant from the local viewpoint. Later, Banks and Shparlinski [5] verified that the constant also describes the density of primes of cyclic reduction on average in the global sense. Furthermore, Jones [30] verified that the average of C_E^{cyc} coincides with C^{cyc}.

Let ζ_n denote a primitive n-th root of unity, and let $\sigma_k \in \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ map $\zeta_n \mapsto \zeta_n^k$. Define

$$\gamma_{n,k}(\mathbb{Q}(E[d])) := \begin{cases} 1 & \text{if } \sigma_k \text{ fixes } \mathbb{Q}(E[d]) \cap \mathbb{Q}(\zeta_n) \text{ pointwise,} \\ 0 & \text{otherwise.} \end{cases}$$

Akbal and Güloğlu [1] defined the constant $C_{E,n,k}^{\mathrm{cyc}}$ as follows,

$$C_{E,n,k}^{\mathrm{cyc}} := \sum_{d\geq 1} \frac{\mu(d)\gamma_{n,k}(\mathbb{Q}(E[d]))}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n):\mathbb{Q}]}. \tag{21}$$

They proved that this constant represents the density of primes $p \equiv k \pmod{n}$ of cyclic reduction for E, under GRH. Recently, Jones and the first author [32] demonstrated that for a non-CM elliptic curve $E/\mathbb{Q}$, this density can be expressed as an almost Euler product as follows,

(22)

$$C_{E,n,k}^{\mathrm{cyc}} = \left(\sum_{d\mid m_E} \frac{\mu(d)\gamma_{n,k}(\mathbb{Q}(E[d]))}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n):\mathbb{Q}]}\right) \prod_{\substack{\ell\nmid m_E \\ \ell\mid(n,k-1)}} \left(1 - \frac{\phi(\ell)}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell\nmid nm_E} \left(1 - \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right).$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Finally, the average counterpart of $C^{\mathrm{cyc}}_{E,n,k}$ is given by

$$C^{\mathrm{cyc}}_{n,k} := \frac{1}{\phi(n)} \prod_{\ell \mid (n,k-1)} \left(1 - \frac{\phi(\ell)}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell \nmid n} \left(1 - \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right). \tag{23}$$

Observe that (23) coincides with (22) if m_E is taken to be 1. While $m_E = 1$ is impossible for any given elliptic curve over $\mathbb{Q}$, it is plausible to think that the role of m_E is inconsequential when considered over the family of all elliptic curves ordered by height. Indeed, as mentioned in the introduction, the first author [37] demonstrated that $C^{\mathrm{cyc}}_{n,k}$ represents the average density of primes $p \equiv k \pmod n$ of cyclic reduction for the family of elliptic curves ordered by height.

We now prove a proposition that serves as a reasonableness check for $C^{\mathrm{cyc}}_{n,k}$. While it can be derived from the main theorem of [37], we opt to include a self-contained proof to draw a parallel with the upcoming Proposition 4.6.

Proposition 4.1. *For any positive integer n, we have*

$$\sum_{\substack{1 \le k \le n \\ (n,k)=1}} C^{\mathrm{cyc}}_{n,k} = C^{\mathrm{cyc}},$$

where C^{cyc} and $C^{\mathrm{cyc}}_{n,k}$ are defined in (20) and (23), respectively.

Proof. For notational convenience, we define

$$f(\ell) = 1 - \frac{\phi(\ell)}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.$$

It suffices to verify that

$$F(n) := \frac{1}{\phi(n)} \sum_{\substack{1 \le k \le n \\ (k,n)=1}} \prod_{\substack{\ell \mid n \\ k \equiv 1 (\ell)}} f(\ell) = \prod_{\ell \mid n} \left(1 - \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right). \tag{24}$$

First, we prove that (24) holds for $n = p^a$, a prime power. Observe that

$$\begin{aligned} F(p^a) &= \frac{1}{\phi(p^a)} \sum_{\substack{1 \le k \le p^a \\ (k,p^a)=1}} \prod_{\substack{\ell \mid p^a \\ k \equiv 1 (\ell)}} f(\ell) \\ &= \frac{1}{\phi(p^a)} \left(p^{a-1} f(p) + p^{a-1}(p-2)\right) = 1 - \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/p\mathbb{Z})|}. \end{aligned}$$

Now, we prove that F is multiplicative. Let p^a be a prime power and n be a positive integer coprime to p. Then

$$\begin{aligned} F(p^a n) &= \frac{1}{\phi(p^a n)} \sum_{\substack{1 \le k \le p^a n \\ (k,p^a n)=1}} \prod_{\substack{\ell \mid p^a n \\ k \equiv 1 (\ell)}} f(\ell) \\ &= \frac{1}{\phi(p^a)} \cdot \frac{1}{\phi(n)} \left[\sum_{\substack{1 \le k \le p^a n \\ (k,pn)=1 \\ k \equiv 1 (p)}} f(p) \prod_{\substack{\ell \mid n \\ k \equiv 1 (\ell)}} f(\ell) + \sum_{\substack{1 \le k \le p^a n \\ (k,pn)=1 \\ k \not\equiv 1 (p)}} \prod_{\substack{\ell \mid n \\ k \equiv 1 (\ell)}} f(\ell) \right] \end{aligned}$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$= \frac{\left(p^{a-1} + p^{a-1}(p-2)\right)}{\phi(p^a)} \cdot \frac{1}{\phi(n)} \left[\sum_{\substack{1 \le k \le n \\ (k,n)=1}} \prod_{\substack{\ell \mid n \\ k \equiv 1 (\ell)}} f(\ell) \right] = F(p^a) \cdot F(n).$$

This completes the proof. □

4.2. **On the Koblitz constant.** We keep the notation from Section 2.1. Now we give the definition of the Koblitz constant C_E^{prime} defined by Zywina and its average counterpart C^{prime} given by Balog, Cojocaru, and David. Based on Zywina's method, for coprime integers n and k, we propose the Koblitz constant $C_{E,n,k}^{\text{prime}}$ for primes in arithmetic progression and its average counterpart $C_{n,k}^{\text{prime}}$.

Let $E/\mathbb{Q}$ be a non-CM elliptic curve of conductor N_E and m be a positive integer. For $p \nmid mN_E$, let Frob_p be a Frobenius element at p in $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (see [51, 2.1, I-6] for the definition of Frob_p). We have that

$$|\widetilde{E}_p(\mathbb{F}_p)| \equiv \det(I - \rho_{E,m}(\text{Frob}_p)) \pmod{m}. \tag{25}$$

by [53, Chapter V. Theorem 2.3.1]. Thus, we see that an odd prime p is of Koblitz reduction if and only if the right-hand side of (25) is invertible modulo m, for every $m < |\widetilde{E}_p(\mathbb{F}_p)|$ such that $\gcd(p, m) = 1$.[4] For such an integer m, we set

$$\Psi^{\text{prime}}(m) := \left\{ M \in \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \det(I - M) \in (\mathbb{Z}/m\mathbb{Z})^\times \right\}. \tag{26}$$

Define the ratio

$$\delta_E^{\text{prime}}(m) := \frac{|G_E(m) \cap \Psi^{\text{prime}}(m)|}{|G_E(m)|}.$$

The Koblitz constant, proposed by Zywina [62], is defined by

$$C_E^{\text{prime}} := \lim_{m \to \infty} \frac{\delta_E^{\text{prime}}(m)}{\prod_{\ell \mid m} (1 - 1/\ell)}, \tag{27}$$

where the limit is taken over all positive integers ordered by divisibility.

We start by proving some properties of $\delta_E^{\text{prime}}(\cdot)$, which were originally remarked in [62].

Proposition 4.2. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E. Then $\delta_E^{\text{prime}}(\cdot)$, as an arithmetic function, satisfies the following properties:*

(1) for any positive integer m, $\delta_E^{\text{prime}}(m) = \delta_E^{\text{prime}}(\text{rad}(m))$;

(2) for any prime $\ell \nmid m_E$ and integer d coprime to ℓ, $\delta_E^{\text{prime}}(d\ell) = \delta_E^{\text{prime}}(d) \cdot \delta_E^{\text{prime}}(\ell)$.

Therefore, (27) can be expressed as follows,

$$C_E^{\text{prime}} = \frac{\delta_E^{\text{prime}}(\text{rad}(m_E))}{\prod_{\ell \mid m_E}(1 - 1/\ell)} \cdot \prod_{\ell \nmid m_E} \frac{\delta_E^{\text{prime}}(\ell)}{1 - 1/\ell}. \tag{28}$$

Proof. We first prove item (1). Let $r = \text{rad}(m)$ and $\varpi \colon G_E(m) \to G_E(r)$ be the usual reduction map. In particular, ϖ is a surjective group homomorphism. We will show that

$$\varpi^{-1}\left(G_E(r) \cap \Psi^{\text{prime}}(r)\right) = G_E(m) \cap \Psi^{\text{prime}}(m). \tag{29}$$

---

[4] This biconditional statement fails if $|\widetilde{E}_p(\mathbb{F}_p)| = p^r$ for some integer $r \ge 2$. However, this can only happen if $p = 2$ due to the Hasse bound.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Let $M \in G_E(r) \cap \Psi^{\text{prime}}(r)$ and $\widetilde{M} \in \varpi^{-1}(M)$. Recall that $\det(M - I)$ is invertible modulo r and that m is only supported by the prime factors of r. Thus, $\det(\widetilde{M} - I)$ is invertible modulo m and $\widetilde{M} \in G_E(m) \cap \Psi^{\text{prime}}(m)$. The other inclusion is obvious, and hence (29) is obtained. Therefore,

$$\delta_E^{\text{prime}}(m) = \frac{\left|G_E(m) \cap \Psi^{\text{prime}}(m)\right|}{|G_E(m)|} = \frac{\left|\varpi^{-1}\left(G_E(r) \cap \Psi^{\text{prime}}(r)\right)\right|}{|\varpi^{-1}\left(G_E(r)\right)|} = \delta_E^{\text{prime}}(r).$$

We now prove item (2). By Lemma 2.2, we have an isomorphism,

$$G_E(d\ell) \simeq G_E(d) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}). \tag{30}$$

It suffices to show that the isomorphism induces a bijection between the two sets

$$G_E(d\ell) \cap \Psi^{\text{prime}}(d\ell) \text{ and } \left(G_E(d) \cap \Psi^{\text{prime}}(d)\right) \times \left(\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \cap \Psi^{\text{prime}}(\ell)\right). \tag{31}$$

Take $M \in G_E(d\ell) \cap \Psi^{\text{prime}}(d\ell)$. By a similar argument to the proof of (1), we have that $M_d \in G_E(d) \cap \Psi^{\text{prime}}(d)$ and $M_\ell \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \cap \Psi^{\text{prime}}(\ell)$. Now, let $M' \in G_E(d) \cap \Psi^{\text{prime}}(d)$ and $M'' \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \cap \Psi^{\text{prime}}(\ell)$. Viewing $(M', M'') \in G_E(d) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, there exists a unique element $M \in G_E(d\ell)$ with $M_d = M'$ and $M_\ell = M''$ by (30). Since $\det(M' - I) \in (\mathbb{Z}/d\mathbb{Z})^\times$ and $\det(M'' - I) \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, we have $\det(M - I) \in (\mathbb{Z}/d\ell\mathbb{Z})^\times$; in particular, $M \in \Psi^{\text{prime}}(d\ell)$. Therefore, (31) is established.

Along with (30), we obtain

$$\begin{aligned}
\delta_E^{\text{prime}}(d\ell) &= \frac{\left|G_E(d\ell) \cap \Psi^{\text{prime}}(d\ell)\right|}{|G_E(d\ell)|} \\
&= \frac{|G_E(d) \cap \Psi^{\text{prime}}(d)|}{|G_E(d)|} \cdot \frac{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \cap \Psi^{\text{prime}}(\ell)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} \\
&= \delta_E^{\text{prime}}(d) \cdot \delta_E^{\text{prime}}(\ell).
\end{aligned}$$

This completes the proof. ☐

Remark 4.3. Suppose that $\ell \nmid m_E$ and $M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Note that $\det(M - I) \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ if and only if 1 is not an eigenvalue of M. One can check from Table 12.4 in [35, XVIII] that

$$\#\left\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : M \text{ has eigenvalues 1 and } k\right\} = \begin{cases} \ell^2 + \ell & \text{if } k \not\equiv 1 \pmod{\ell}, \\ \ell^2 & \text{if } k \equiv 1 \pmod{\ell}. \end{cases}$$

Thus, we see that

$$\frac{\delta_E^{\text{prime}}(\ell)}{1 - 1/\ell} = \frac{\ell}{\ell - 1} \cdot \left(1 - \frac{(\ell-2)(\ell^2+\ell) + \ell^2}{(\ell^2-1)(\ell^2-\ell)}\right) = 1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)} \sim 1 - \frac{1}{\ell^2} \quad \text{as } \ell \to \infty, \tag{32}$$

and hence the infinite product in (28) converges absolutely.

The average counterpart of C_E^{prime} is given by

$$C^{\text{prime}} := \prod_\ell \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right) \approx 0.505166. \tag{33}$$

As mentioned earlier, Balog, Cojocaru, and David [4] demonstrated that C^{prime} represents the average Koblitz constant, while Jones [30] verified that the average of C_E^{prime} coincides with C^{prime}. Unlike for the cyclicity problem, the Koblitz problem has not yet been studied for primes in arithmetic progressions. We construct $C_{E,n,k}^{\text{prime}}$ in a parallel way to Zywina's method and propose a candidate for the average constant $C_{n,k}^{\text{prime}}$.

Let $E/\mathbb{Q}$ be a non-CM elliptic curve of conductor N_E and m be a positive integer. For a prime $p \nmid nN_E$, let Frob_p be a Frobenius element lying above p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We have that

$$\det(\rho_{E,n}(\mathrm{Frob}_p)) \equiv p \pmod{n}.$$

Along with (25), let us consider the set

$$\Psi_{n,k}^{\mathrm{prime}}(m) := \left\{ M \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \det(I-M) \in (\mathbb{Z}/m\mathbb{Z})^\times, \det M \equiv k \pmod{\gcd(m,n)} \right\}. \tag{34}$$

One may note that $\rho_{E,m}(\mathrm{Frob}_p) \in G_E(m) \cap \Psi_{n,k}^{\mathrm{prime}}(m)$ if and only if $p \equiv k \pmod{\gcd(n,m)}$ and $|\widetilde{E}_p(\mathbb{F}_p)|$ is invertible $\mathbb{Z}/m\mathbb{Z}$. For this reason, we consider the ratio

$$\delta_{E,n,k}^{\mathrm{prime}}(m) := \frac{\left|G_E(m) \cap \Psi_{n,k}^{\mathrm{prime}}(m)\right|}{|G_E(m)|}.$$

Building upon Zywina's approach, we are led to define

$$C_{E,n,k}^{\mathrm{prime}} := \lim_{m\to\infty} \frac{\delta_{E,n,k}^{\mathrm{prime}}(m)}{\prod_{\ell \mid m}(1-1/\ell)}, \tag{35}$$

where the limit is taken over all positive integers, ordered by divisibility.

Proposition 4.4. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E and n be a positive integer. Let L be defined as in (7). Then, $\delta_{E,n,k}^{\mathrm{prime}}(\cdot)$, as an arithmetic function, satisfies the following properties:*

(1) Let $L \mid L' \mid L^\infty$. Then, $\delta_{E,n,k}^{\mathrm{prime}}(L) = \delta_{E,n,k}^{\mathrm{prime}}(L')$;

(2) Let ℓ^α be a prime power and d be a positive integer with $(\ell, Ld) = 1$. Then, $\delta_{E,n,k}^{\mathrm{prime}}(d\ell^a) = \delta_{E,n,k}^{\mathrm{prime}}(d) \cdot \delta_{E,n,k}^{\mathrm{prime}}(\ell^\alpha)$.

(3) Let $\ell^\alpha \parallel n$ and $(\ell, L) = 1$. Then, for any $\beta > \alpha$, $\delta_{E,n,k}^{\mathrm{prime}}(\ell^\beta) = \delta_{E,n,k}^{\mathrm{prime}}(\ell^\alpha)$. Further, if $\ell \nmid nL$, we have $\delta_{E,n,k}^{\mathrm{prime}}(\ell^\beta) = \delta_{E}^{\mathrm{prime}}(\ell)$.

Therefore, (35) can be expressed as follows,

$$C_{E,n,k}^{\mathrm{prime}} = \frac{\delta_{E,n,k}^{\mathrm{prime}}(L)}{\prod_{\ell \mid L}(1-1/\ell)} \cdot \prod_{\substack{\ell \nmid m_E \\ \ell^\alpha \parallel n}} \frac{\delta_{E,n,k}^{\mathrm{prime}}(\ell^\alpha)}{1-1/\ell} \cdot \prod_{\ell \nmid n m_E} \frac{\delta_{E}^{\mathrm{prime}}(\ell)}{1-1/\ell}. \tag{36}$$

and the infinite product converges absolutely.

Proof. Let us prove item (1). Consider the natural reduction map $\varpi\colon G_E(L') \to G_E(L)$, which is a surjective group homomorphism. We will show that

$$\varpi^{-1}\left(G_E(L) \cap \Psi_{n,k}^{\mathrm{prime}}(L)\right) = G_E(L') \cap \Psi_{n,k}^{\mathrm{prime}}(L') \tag{37}$$

Let $M \in G_E(L) \cap \Psi_{n,k}^{\mathrm{prime}}(L)$ and $\widetilde{M} \in \varpi^{-1}(M)$. Recall that $\det(M-I)$ is invertible modulo L and that L' is only supported by the prime factors of L. Thus, $\det(\widetilde{M-I})$ is invertible modulo L'. Since $\gcd(n,L) = \gcd(n,L')$, we also have $\det \widetilde{M} \equiv k \pmod{\gcd(n,L')}$. Thus, $\widetilde{M} \in G_E(L') \cap \Psi_{n,k}^{\mathrm{prime}}(L')$. The other inclusion is obvious, and hence (37) is obtained. Therefore, we have

$$\delta_{E,n,k}^{\mathrm{prime}}(L') = \frac{\left|G_E(L') \cap \Psi_{n,k}^{\mathrm{prime}}(L')\right|}{|G_E(L')|} = \frac{\left|\varpi^{-1}\left(G_E(L) \cap \Psi_{n,k}^{\mathrm{prime}}(L)\right)\right|}{|\varpi^{-1}(G_E(L))|} = \delta_{E,n,k}^{\mathrm{prime}}(L).$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Let us prove item (2). By Lemma 2.2, we have an isomorphism,

$$G_E(d\ell^\alpha) \simeq G_E(d) \times \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}). \tag{38}$$

It suffices to show that the isomorphism induces a map between the sets

$$G_E(d\ell^\alpha) \cap \Psi^{\mathrm{prime}}_{n,k}(d\ell^\alpha) \text{ and } \left(G_E(d) \cap \Psi^{\mathrm{prime}}_{n,k}(d)\right) \times \left(\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) \cap \Psi^{\mathrm{prime}}_{n,k}(\ell^\alpha)\right). \tag{39}$$

Say $M \in G_E(d\ell^\alpha) \cap \Psi^{\mathrm{prime}}_{n,k}(d\ell^\alpha)$. By a similar argument to the proof of (1), one may see that $M_d \in G_E(d) \cap \Psi^{\mathrm{prime}}_{n,k}(d)$ and $M_{\ell^\alpha} \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) \cap \Psi^{\mathrm{prime}}_{n,k}(\ell^\alpha)$. Now, let $M' \in G_E(d) \cap \Psi^{\mathrm{prime}}(d)$ and $M'' \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) \cap \Psi^{\mathrm{prime}}(\ell^\alpha)$. Viewing $(M', M'') \in G_E(d) \times \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})$, there exists a unique element $M \in G_E(d\ell^\alpha)$ with $M_d = M'$ and $M_{\ell^\alpha} = M''$ by (38). Note that since $\det(M' - I) \in (\mathbb{Z}/d\mathbb{Z})^\times$ and $\det(M'' - I) \in (\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times$, we have $\det(M - I) \in (\mathbb{Z}/d\ell^\alpha\mathbb{Z})^\times$; in particular, $M \in \Psi^{\mathrm{prime}}_{n,k}(d\ell^\alpha)$. Therefore, (39) is established.

Along with (38), we obtain

$$\begin{aligned}\delta^{\mathrm{prime}}_{E,n,k}(d\ell^\alpha) &= \frac{\left|G_E(d\ell^\alpha) \cap \Psi^{\mathrm{prime}}_{n,k}(d\ell^\alpha)\right|}{|G_E(d\ell^\alpha)|} \\ &= \frac{|G_E(d) \cap \Psi^{\mathrm{prime}}(d)|}{|G_E(d)|} \cdot \frac{|\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) \cap \Psi^{\mathrm{prime}}(\ell^\alpha)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})|} = \delta^{\mathrm{prime}}_{E,n,k}(d) \cdot \delta^{\mathrm{prime}}_{E,n,k}(\ell^\alpha).\end{aligned}$$

Finally, let us prove item (3). Since $\ell \nmid m_E$, by Lemma 2.2, $G_E(\ell^\alpha)$ and $G_E(\ell^\beta)$ are the full groups, $\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})$. Let $\varpi\colon \mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})$ be the natural reduction map which is a surjective group homomorphism. By a similar argument as in the proof of item (1), it suffices to check that

$$\varpi^{-1}\left(\Psi^{\mathrm{prime}}_{n,k}(\ell^\alpha)\right) = \Psi^{\mathrm{prime}}_{n,k}(\ell^\beta). \tag{40}$$

Take $M \in \Psi^{\mathrm{prime}}_{n,k}(\ell^\alpha)$ and let $\widetilde{M} \in \varpi^{-1}(M)$. By the same reasoning in the proof of item (1), $\det(\widetilde{M} - I)$ is invertible modulo ℓ^β. Since $\gcd(n, \ell^\alpha) = \gcd(n, \ell^\beta) = \ell^\alpha$, we also have $\det \widetilde{M} \equiv k \pmod{\ell^\alpha}$. The other inclusion is obvious, and hence (40) is obtained. Thus, we have

$$\delta^{\mathrm{prime}}_{E,n,k}(\ell^\beta) = \frac{\left|\Psi^{\mathrm{prime}}_{n,k}(\ell^\beta)\right|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})|} = \frac{\left|\varpi^{-1}\left(\Psi^{\mathrm{prime}}_{n,k}(\ell^\alpha)\right)\right|}{|\varpi^{-1}\left(\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})\right)|} = \delta^{\mathrm{prime}}_{E,n,k}(\ell^\alpha).$$

In case $\ell \nmid nL$, let $\varpi\colon \mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. It suffices to check

$$\varpi^{-1}\left(\Psi^{\mathrm{prime}}(\ell)\right) = \Psi^{\mathrm{prime}}_{n,k}(\ell^\beta). \tag{41}$$

Note that the condition $\det M \equiv k \pmod{\gcd(n, \ell)}$ is trivial, and hence $\Psi^{\mathrm{prime}}_{E,n,k}(\ell) = \Psi^{\mathrm{prime}}_E(\ell)$. Let $M \in \Psi^{\mathrm{prime}}_E(\ell)$. Note that every lifting $\widetilde{M} \in \varpi^{-1}(M)$ belongs to $\Psi^{\mathrm{prime}}_{E,n,k}(\ell^\beta)$. The other inclusion is obvious, and hence (41) is obtained. Thus, we have

$$\delta^{\mathrm{prime}}_{E,n,k}(\ell^\beta) = \frac{\left|\Psi^{\mathrm{prime}}_{n,k}(\ell^\beta)\right|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})|} = \frac{\left|\varpi^{-1}\left(\Psi^{\mathrm{prime}}(\ell)\right)\right|}{|\varpi^{-1}(\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}))|} = \delta^{\mathrm{prime}}_E(\ell).$$

By grouping the prime factors of M in (35) according to whether they divide L or not, we obtain (36). The absolute convergence of (36) follows from Remark 4.3. □

The following lemma allows us to express $C^{\mathrm{prime}}_{E,n,k}$ more explicitly.

Lemma 4.5. *Suppose $\ell^\alpha \parallel n$ and $\ell \nmid m_E$. Then*

$$\frac{\delta^{\text{prime}}_{E,n,k}(\ell^\alpha)}{1-1/\ell} = \begin{cases} \frac{1}{\phi(\ell^\alpha)}\left(1-\frac{\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) & \text{if } k \equiv 1 \pmod{\ell}, \\ \frac{1}{\phi(\ell^\alpha)}\left(1-\frac{\ell^2+\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) & \text{if } k \not\equiv 1 \pmod{\ell}. \end{cases}$$

Proof. By the assumption, we have $G_E(\ell^\alpha) \simeq \operatorname{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})$. Recall that

$$\Psi^{\text{prime}}_{n,k}(\ell^\alpha) = \left\{M \in \operatorname{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : \det(M-I) \in (\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times, \det M \equiv k \pmod{\gcd(n,\ell^\alpha)}\right\}.$$

whose cardinality was determined in Corollary 3.4. A brief calculation reveals the desired result. □

Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E. Let $n = n_1 n_2$ where $n_1 = \gcd(n, m_E^\infty)$ and $(n_2, m_E) = 1$. By (32), (36), and Lemma 4.5, we have

$$C^{\text{prime}}_{E,n,k} = \frac{\delta^{\text{prime}}_{E,n,k}(L)}{\prod_{\ell \mid L}(1-1/\ell)} \cdot \frac{1}{\phi(n_2)} \prod_{\substack{\ell \nmid m_E \\ \ell \mid n \\ \ell \nmid k-1}} \left(1 - \frac{\ell^2+\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \nmid m_E \\ \ell \mid (n,k-1)}} \left(1 - \frac{\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right)$$
$$\cdot \prod_{\ell \nmid n m_E} \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right).$$

We now propose the average counterpart of $C^{\text{prime}}_{E,n,k}$,

(42)
$$C^{\text{prime}}_{n,k} := \frac{1}{\phi(n)} \prod_{\substack{\ell \mid n \\ \ell \nmid k-1}} \left(1 - \frac{\ell^2+\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell \mid (n,k-1)} \left(1 - \frac{\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell \nmid n} \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right).$$

The formula for $C^{\text{prime}}_{n,k}$ coincides with $C^{\text{prime}}_{E,n,k}$ if one takes $m_E = 1$, similar to the case for $C^{\text{cyc}}_{n,k}$ in (23). Parallel to Proposition 4.1, we show that $C^{\text{prime}}_{n,k}$ behaves as expected when we sum over k.

Proposition 4.6. *For any positive integer n, we have*

$$\sum_{\substack{1 \le k \le n \\ (n,k)=1}} C^{\text{prime}}_{n,k} = C^{\text{prime}},$$

where C^{prime} and $C^{\text{prime}}_{n,k}$ are defined in (33) and (42), respectively.

Proof. For notational convenience, we define

$$f_1(\ell) = 1 - \frac{\ell^2+\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}, \qquad f_2(\ell) = 1 - \frac{\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}$$

To show the desired equation, we need to verify that

$$F(n) := \frac{1}{\phi(n)} \sum_{\substack{1 \le k \le n \\ (k,n)=1}} \prod_{\substack{\ell \mid n \\ k \not\equiv 1 (\ell)}} f_1(\ell) \prod_{\substack{\ell \mid n \\ k \equiv 1 (\ell)}} f_2(\ell) = \prod_{\ell \mid n} \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right). \tag{43}$$

First, we prove that (43) is true for $n = p^a$, a prime power. Observe that

$$F(p^a) = \frac{1}{\phi(p^a)} \left(p^{a-1}(f_1(p)(p-2) + f_2(p))\right)$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$= \frac{p^{a-1}}{\phi(p^a)}\left[(p-2)\left(1-\frac{p^2+p}{|\operatorname{GL}_2(\mathbb{Z}/p\mathbb{Z})|}\right)+\left(1-\frac{p}{|\operatorname{GL}_2(\mathbb{Z}/p\mathbb{Z})|}\right)\right]$$
$$= 1-\frac{p^2-p-1}{(p-1)^3(p+1)}.$$

Let us prove that F is multiplicative. Let n be coprime to p^a, a prime power. We see that

$$\begin{aligned}
F(p^a n) &= \frac{1}{\phi(p^a n)} \sum_{\substack{1\le k\le p^a n\\ (k,pn)=1}} \prod_{\substack{\ell \mid pn\\ k\not\equiv 1(\ell)}} f_1(\ell) \prod_{\substack{\ell\mid pn\\ k\equiv 1(\ell)}} f_2(\ell)\\
&= \frac{1}{\phi(p^a)}\frac{1}{\phi(n)}\left[\sum_{\substack{1\le k\le p^a n\\ (k,pn)=1\\ k\not\equiv 1(p)}} f_1(p) \prod_{\substack{\ell\mid n\\ k\not\equiv 1(\ell)}} f_1(\ell)\prod_{\substack{\ell\mid n\\ k\equiv 1(\ell)}} f_2(\ell) + \sum_{\substack{1\le k\le p^a n\\ (k,pn)=1\\ k\equiv 1(p)}} f_2(p)\prod_{\substack{\ell\mid n\\ k\not\equiv 1(\ell)}} f_1(\ell)\prod_{\substack{\ell\mid n\\ k\equiv 1(\ell)}} f_2(\ell)\right]\\
&= \frac{f_1(p)(p-2)p^{a-1}}{\phi(p^a)}\frac{1}{\phi(n)}\sum_{\substack{1\le k\le n\\ (k,n)=1}} \prod_{\substack{\ell\mid n\\ k\not\equiv 1(\ell)}} f_1(\ell)\prod_{\substack{\ell\mid n\\ k\equiv 1(\ell)}} f_2(\ell)\\
&\qquad + \frac{f_2(p)p^{a-1}}{\phi(p^a)}\frac{1}{\phi(n)}\sum_{\substack{1\le k\le n\\ (k,n)=1}} \prod_{\substack{\ell\mid n\\ k\not\equiv 1(\ell)}} f_1(\ell)\prod_{\substack{\ell\mid n\\ k\equiv 1(\ell)}} f_2(\ell)\\
&= \frac{1}{\phi(p^a)}\left(p^{a-1}(f_1(p)(p-2)+f_2(p))\right)\cdot F(n) = F(p^a)F(n).
\end{aligned}$$

This completes the proof. □

4.3. **Applying Zywina's approach for the cyclicity problem.** Zywina [62] refined the Koblitz conjecture by improving the heuristic explanation for the constant C_E^{prime}. In essence, he interprets the desired property of a prime of Koblitz reduction in terms of Galois representations, examines the ratio of elements with the desired property in each finite level $G_E(m)$, and considers the limit of that ratio as m approaches infinity. In this subsection, we apply Zywina's approach to determine the heuristic densities of primes of cyclic reduction for E and verify their concurrence with the densities proposed by Serre and Akbal–Güloğlu.

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and fix a good prime $p \neq 2$. We now give a criterion for p to be a prime of cyclic reduction for E.[5] Let Frob_p denote a Frobenius element in $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at p. By [19, Lemma 2.1], we have that

$$\begin{aligned}
\widetilde{E}_p(\mathbb{F}_p) \text{ is cyclic } &\iff \forall \text{ primes } \ell\neq p,\ \widetilde{E}_p(\mathbb{F}_p) \text{ does not contain a subgroup isomorphic to } \mathbb{Z}/\ell\mathbb{Z}\oplus\mathbb{Z}/\ell\mathbb{Z}\\
&\iff \forall \text{ primes } \ell\neq p,\ \rho_{E,\ell}(\operatorname{Frob}_p)\not\equiv I \pmod{\ell}\\
&\iff \forall m\in\mathbb{N} \text{ with } p\nmid m \text{ and } \forall \text{ prime } \ell\mid m,\ \rho_{E,\ell}(\operatorname{Frob}_p)\not\equiv I \pmod{\ell}.
\end{aligned}$$

Drawing a parallel to (26), we consider the set

$$\Psi^{\text{cyc}}(m) := \{M\in\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z}) : M\not\equiv I \ (\text{mod } \ell) \text{ for all } \ell\mid m\},$$

[5]Note that if $p=2$ is a prime of good reduction for E, then $\widetilde{E}_2(\mathbb{F}_2)$ is necessarily cyclic.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

and the ratio

$$\delta_E^{\mathrm{cyc}}(m) := \frac{|G_E(m) \cap \Psi^{\mathrm{cyc}}(m)|}{|G_E(m)|}.$$

Taking the limit of $\delta_E^{\mathrm{cyc}}(m)$ over all positive integers, ordered by divisibility, we expect to obtain the heuristic density of primes of cyclic reduction.

Proposition 4.7. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E. Then $\delta_E^{\mathrm{cyc}}(\cdot)$, as an arithmetic function, satisfies the following properties:*

(1) for any positive integer m, $\delta_E^{\mathrm{cyc}}(m) = \delta_E^{\mathrm{cyc}}(\mathrm{rad}(m))$;
(2) for any prime $\ell \nmid m_E$ and integer d coprime to ℓ, $\delta_E^{\mathrm{cyc}}(d\ell) = \delta_E^{\mathrm{cyc}}(d) \cdot \delta_E^{\mathrm{cyc}}(\ell)$.

Therefore, the heuristic density of primes of cyclic reduction can be expressed as follows,

$$\lim_{m\to\infty} \delta_E^{\mathrm{cyc}}(m) = \delta_E^{\mathrm{cyc}}(\mathrm{rad}(m_E)) \cdot \prod_{\ell \nmid m_E} \delta_E^{\mathrm{cyc}}(\ell).$$

Proof. Follows similarly to the proof of Proposition 4.2. □

Remark 4.8. One can easily check that for $\ell \nmid m_E$,

$$\delta_E^{\mathrm{cyc}}(\ell) = 1 - \frac{1}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} \sim 1 - \frac{1}{\ell^4}, \qquad \text{as } \ell \to \infty \tag{44}$$

and hence the infinite product converges absolutely.

We now verify that the limit $\lim_{m\to\infty} \delta_E^{\mathrm{cyc}}(m)$ appearing in Proposition 4.7 coincides with the cyclicity constant C_E^{cyc} originally defined by Serre [52, pp. 465–468].

Proposition 4.9. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then we have*

$$C_E^{\mathrm{cyc}} = \delta_E^{\mathrm{cyc}}(\mathrm{rad}(m_E)) \cdot \prod_{\ell \nmid m_E} \left(1 - \frac{1}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right).$$

Proof. Let $R = \mathrm{rad}(m_E)$. By (19) and (44), it suffices to check

$$\sum_{d \mid m_E} \frac{\mu(d)}{[\mathbb{Q}(E[d]) : \mathbb{Q}]} = \delta_E^{\mathrm{cyc}}(R).$$

Let m be a positive integer and $d \mid m$. We define

$$S'_E(m) := \{M \in G_E(m) : M \not\equiv I \pmod{\ell} \text{ for all } \ell \mid m\}$$
$$S_E^{(d)}(m) := \{M \in G_E(m) : M \equiv I \pmod{d}\}.$$

From the definition, one may observe that $G_E(R) \cap \Psi^{\mathrm{cyc}}(R) = S'_E(R)$. Thus, we have

$$\delta_E^{\mathrm{cyc}}(R) = \frac{|S'_E(R)|}{|G_E(R)|}.$$

Also, note that $S_E^{(d)}(d) = \{I\}$. Let $\varpi\colon G_E(m) \to G_E(d)$ be the natural reduction map. Then,

$$\frac{|S_E^{(d)}(m)|}{|G_E(m)|} = \frac{\left|\varpi^{-1}(S_E^{(d)}(d))\right|}{|\varpi^{-1}(G_E(d))|} = \frac{\left|S_E^{(d)}(d)\right|}{|G_E(d)|} = \frac{1}{|G_E(d)|}.$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Observe that $S'_E(R) = G_E(R) - \bigcup_{\ell \mid R} S_E^{(\ell)}(R)$. By the principle of inclusion-exclusion, we obtain

$$\delta_E^{\rm cyc}(R) = \frac{|S'_E(R)|}{|G_E(R)|} = \sum_{d \mid R} \frac{\mu(d)}{|G_E(d)|} = \sum_{d \mid m_E} \frac{\mu(d)}{[\mathbb{Q}(E[d]) : \mathbb{Q}]}.$$

This completes the proof. □

Now, we construct a heuristic density of primes of cyclic reduction that lie in an arithmetic progression. Consider

$$\Psi_{n,k}^{\rm cyc}(m) := \{M \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : M \not\equiv I \pmod{\ell} \text{ for all } \ell \mid m, \det M \equiv k \pmod{\gcd(m,n)}\}.$$

We define

$$\delta_{E,n,k}^{\rm cyc}(m) := \frac{\left|G_E(m) \cap \Psi_{n,k}^{\rm cyc}(m)\right|}{|G_E(m)|}.$$

Drawing parallels from Zywina's approach, we consider the limit

$$\lim_{m \to \infty} \delta_{E,n,k}^{\rm cyc}(m), \tag{45}$$

where the limit is taken over all positive integers, ordered by divisibility. We'll prove in Proposition 4.12 that (45) coincides with $C_{E,n,k}^{\rm cyc}$ as defined in [1]. To do so, we'll first give some properties of $\delta_{E,n,k}^{\rm cyc}(\cdot)$.

Proposition 4.10. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E. Fix a positive integer n. Set L as in (7). Then, $\delta_{E,n,k}^{\rm cyc}(\cdot)$, as an arithmetic function, satisfies the following properties:*

(1) Let $L \mid L' \mid L^\infty$. Then, $\delta_{E,n,k}^{\rm cyc}(L) = \delta_{E,n,k}^{\rm cyc}(L')$;

(2) Let ℓ^α be a prime power and d be a positive integer with $(\ell, Ld) = 1$. Then, $\delta_{E,n,k}^{\rm cyc}(d\ell^a) = \delta_{E,n,k}^{\rm cyc}(d) \cdot \delta_{E,n,k}^{\rm cyc}(\ell^\alpha)$.

(3) Let $\ell^\alpha \parallel n$ and $(\ell, L) = 1$. Then, for any $\beta > \alpha$, $\delta_{E,n,k}^{\rm cyc}(\ell^\beta) = \delta_{E,n,k}^{\rm cyc}(\ell^\alpha)$. Further, if $\ell \nmid nL$, we have $\delta_{E,n,k}^{\rm cyc}(\ell^\beta) = \delta_E^{\rm cyc}(\ell)$.

Therefore, (45) can be expressed as follows,

$$\lim_{m \to \infty} \delta_{E,n,k}^{\rm cyc}(m) = \delta_{E,n,k}^{\rm cyc}(L) \cdot \prod_{\substack{\ell \nmid m_E \\ \ell^\alpha \parallel n}} \delta_{E,n,k}^{\rm cyc}(\ell^\alpha) \cdot \prod_{\ell \nmid n m_E} \delta_E^{\rm cyc}(\ell). \tag{46}$$

and the product converges absolutely.

Proof. One can argue similarly to the proof of Proposition 4.4 to obtain the desired results. The absolute convergence of (46) follows from Remark 4.8. □

The next lemma allows us to describe (46) explicitly.

Lemma 4.11. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E. Suppose $\ell^a \parallel n$ and $\ell \nmid m_E$. For any k coprime to n, we have*

$$\delta_{E,n,k}^{\rm cyc}(\ell^a) = \begin{cases} \frac{1}{\phi(\ell^a)} & \text{if } \ell \mid n \text{ and } \ell \nmid (k-1) \\ \frac{1}{\phi(\ell^a)} \left(1 - \frac{\phi(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) & \text{if } \ell \mid (n, k-1). \end{cases}$$

Proof. Since $\ell \nmid m_E$, we have $G_E(\ell^a) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z})$, and hence $|G_E(\ell^a)| = (\ell^2-1)(\ell^2-\ell)\ell^{4(a-1)}$. Applying Corollary 3.2, we obtain the desired results. □

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E. Let $n = n_1n_2$ where $n_1 = \gcd(n, m_E^\infty)$ and $(n_2, m_E) = 1$. By (44), (46), and Lemma 4.11, we obtain

$$\lim_{m\to\infty} \delta^{\mathrm{cyc}}_{E,n,k}(m) = \frac{\delta^{\mathrm{cyc}}_{E,n,k}(L)}{\phi(n_2)} \prod_{\substack{\ell\nmid m_E \\ \ell\mid(n,k-1)}} \left(1 - \frac{\phi(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell\nmid nm_E} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right). \tag{47}$$

We now prove that (47) equals the cyclicity constant proposed by Akbal and Gülğlu.

Proposition 4.12. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of adelic level m_E and n be a positive integer. Let $n = n_1n_2$ where $n_1 = \gcd(n, m_E^\infty)$ and $(n_2, m_E) = 1$. Then we have*

$$C^{\mathrm{cyc}}_{E,n,k} = \frac{\delta^{\mathrm{cyc}}_{E,n,k}(L)}{\phi(n_2)} \prod_{\substack{\ell\nmid m_E \\ \ell\mid(n,k-1)}} \left(1 - \frac{\phi(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell\nmid nm_E} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right).$$

Proof. Define

$$S'_{E,n,k}(m) := \{\sigma \in \mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q}) : \sigma|_{\mathbb{Q}(\zeta_n)} = \sigma_k, \sigma|_{\mathbb{Q}(E[\ell])} \not\equiv 1 \text{ for all } \ell \mid m\}.$$

Let $R = \mathrm{rad}(m_E)$. By [32, p. 13], (22) can be expressed as follows,

$$\frac{|S'_{E,n,k}(R)|}{|\mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_n)/\mathbb{Q})|} \prod_{\substack{\ell\nmid m_E \\ \ell(n,k-1)}} \left(1 - \frac{\phi(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell\nmid nm_E} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right). \tag{48}$$

Thus, it suffices to verify that

$$\frac{|S'_{E,n,k}(R)|}{|\mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_n))/\mathbb{Q}|} = \frac{\delta^{\mathrm{cyc}}_{E,n,k}(L)}{\phi(n_2)}.$$

By the Weil pairing, we have $\mathbb{Q}(\zeta_{n_2}) \subseteq \mathbb{Q}(E[n_2])$. Thus, we see that $\mathbb{Q}(E[R])\mathbb{Q}(\zeta_{n_1})$ and $\mathbb{Q}(\zeta_{n_2})$ must be linearly disjoint by Lemma 2.2, and hence

$$\mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(E[R]\mathbb{Q}(\zeta_{n_1}))/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{n_2})/\mathbb{Q}).$$

Under the isomorphism, the set $S'_{E,n,k}(R)$ can be identified as $S'_{E,n_1,k}(R) \times \{\sigma_k\}$, and hence $|S'_{E,n,k}(R)| = |S'_{E,n_1,k}(R)|$. Thus, we have

$$\frac{|S'_{E,n,k}(R)|}{|\mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_n)/\mathbb{Q})|} = \frac{1}{\phi(n_2)} \cdot \frac{|S'_{E,n_1,k}(R)|}{|\mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_{n_1})/\mathbb{Q})|}.$$

Remark that $\mathbb{Q}(E[R]) \subseteq \mathbb{Q}(E[L])$ and $\mathbb{Q}(\zeta_{n_1}) \subseteq \mathbb{Q}(E[L])$ by the definition of L. Thus, the usual restriction $\varpi\colon G_E(L) \to \mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_{n_1})/\mathbb{Q})$ gives a surjective group homomorphism.

Viewing $G_E(L)$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/L\mathbb{Z})$, we may observe that

$$\begin{aligned}
\varpi^{-1}(S'_{E,n_1,k}(R)) &= \left\{\widetilde{\sigma} \in G_E(L) : \widetilde{\sigma}|_{\mathbb{Q}(\zeta_{n_1})} = \sigma_k, \widetilde{\sigma}|_{\mathbb{Q}(E[\ell])} \not\equiv 1 \pmod{\ell} \text{ for all } \ell \mid L\right\} \\
&= G_E(L) \cap \{M \in \mathrm{GL}_2(\mathbb{Z}/L\mathbb{Z}) : \det M \equiv k \pmod{n_1}, M \not\equiv I \pmod{\ell} \text{ for all } \ell \mid L\} \\
&= G_E(L) \cap \Psi^{\mathrm{cyc}}_{n,k}(L).
\end{aligned}$$

Therefore,

$$\frac{|S'_{E,n_1,k}(R)|}{|\mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_{n_1})/\mathbb{Q})|} = \frac{\left|\varpi^{-1}\left(S'_{E,n_1,k}(R)\right)\right|}{|\varpi^{-1}(\mathrm{Gal}(\mathbb{Q}(E[R])\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}))|} = \frac{\left|G_E(L) \cap \Psi^{\mathrm{cyc}}_{n,k}(L)\right|}{|G_E(L)|} = \delta^{\mathrm{cyc}}_{E,n,k}(L).$$

This completes the proof. ∎

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Remark 4.13. As one may have observed from Conjecture 1.1 and Conjecture 1.3, the conjectural growth rates of $\pi_E^{\mathrm{cyc}}(x)$ and $\pi_E^{\mathrm{prime}}(x)$ are different. Thus, there is an intrinsic difference between C_E^{cyc} and C_E^{prime}. In particular, C_E^{cyc} can be interpreted as the (conjectural) density of primes of cyclic reduction for E whereas C_E^{prime} should not be interpreted analogously. A similar remark holds for $\pi_E^{\mathrm{cyc}}(x;n,k)$ and $\pi_E^{\mathrm{prime}}(x;n,k)$ and their respective constants.

5. On the cyclicity and Koblitz constants for Serre curves

We begin by fixing some notation that will hold throughout the section. Let $E/\mathbb{Q}$ be a Serre curve of discriminant Δ_E, n be a positive integer, and k be an integer coprime to n. Let Δ' be the squarefree part of Δ_E. By Proposition 2.4, we have

$$m_E = \begin{cases} 2|\Delta'| & \text{if } \Delta' \equiv 1 \pmod 4, \\ 4|\Delta'| & \text{otherwise.} \end{cases}$$

Let L be defined as in (7). The goal of this section is to develop formulas for $C_{E,n,k}^{\mathrm{cyc}}$ and $C_{E,n,k}^{\mathrm{prime}}$ with our assumption that E is a Serre curve. By Proposition 4.4 and Proposition 4.10, it suffices to compute $\delta_{E,n,k}^{\mathrm{cyc}}(L)$ and $\delta_{E,n,k}^{\mathrm{prime}}(L)$.

For an integer n, we set $n = n_1 n_2$ where $n_1 = (n, m_E^\infty)$ and $(n_2, m_E) = 1$. There are two cases to consider: $m_E \nmid L$ and $m_E \mid L$. The former occurs if and only if one of the following holds:

- $\Delta' \equiv 3 \pmod 4$ and $2 \nmid n$;
- $\Delta' \equiv 2 \pmod 4$ and $4 \nmid n$.

We write $L = 2^\alpha \cdot L^{\mathrm{odd}}$ where L^{odd} is an odd integer; observe that $|\Delta'|$ divides L^{odd}. We now define two sign functions that depend on Δ', k and appear in Theorem 1.7.

Definition 5.1. Let $E/\mathbb{Q}$ be a Serre curve of discriminant Δ_E. Let Δ' and k defined as above. Assume $m_E \mid L$. We define $\tau = \tau(\Delta', k)$ as follows.

- If $\Delta' \equiv 1 \pmod 4$, we define $\tau = -1$.
- If $\Delta' \equiv 3 \pmod 4$, then $4 \mid n$. We define

$$\tau = \begin{cases} -1 & \text{if } k \equiv 1 \pmod 4, \\ 1 & \text{if } k \equiv 3 \pmod 4. \end{cases}$$

- If $\Delta' \equiv 2 \pmod 8$, then $8 \mid n$. We define

$$\tau = \begin{cases} -1 & \text{if } k \equiv 1, 7 \pmod 8, \\ 1 & \text{if } k \equiv 3, 5 \pmod 8. \end{cases}$$

- If $\Delta' \equiv 6 \pmod 8$, then $8 \mid n$. We define

$$\tau = \begin{cases} -1 & \text{if } k \equiv 1, 3 \pmod 8, \\ 1 & \text{if } k \equiv 5, 7 \pmod 8. \end{cases}$$

Finally, we define $\tau^{\mathcal{X}} := \tau^{\mathcal{X}}(\Delta', n, k) \in \{\pm 1\}$ as follows,

$$\tau^{\mathrm{cyc}} := \tau \prod_{\substack{\ell \mid L^{\mathrm{odd}} \\ \ell \nmid n}} (-1) \prod_{\substack{\ell \mid (n, L^{\mathrm{odd}}) \\ \ell \nmid k-1}} \left(\frac{k}{\ell}\right),$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$\tau^{\text{prime}} := -\tau \prod_{\substack{\ell \mid (n, L^{\text{odd}}) \\ \ell \nmid k-1}} \left(\frac{k}{\ell}\right).$$

Having defined τ^{cyc} and τ^{prime}, the rest of the section is devoted to proving Theorem 1.7. First, suppose $m_E \nmid L$. Then, by Proposition 2.4, we have $G_E(L) \simeq \mathrm{GL}_2(\mathbb{Z}/L\mathbb{Z}) \simeq \prod_{\ell^\alpha \| L} \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})$. One can check that the isomorphism induces bijections between the sets,

$$\Psi^{\mathcal{X}}_{n,k}(L) \quad \text{and} \quad \prod_{\ell^\alpha \| L} \Psi^{\mathcal{X}}_{n,k}(\ell^\alpha), \tag{49}$$

for $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$. Let ℓ be a prime factor of L. If $\ell \nmid n$, then we have $\alpha = 1$ by (7). The condition $\det M \equiv k \pmod{\gcd(n, \ell)}$ becomes trivial, and hence we have

$$\Psi^{\mathcal{X}}_{n,k}(\ell^\alpha) = \Psi^{\mathcal{X}}(\ell)$$

for $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$.

On the other hand, suppose $\ell^\alpha \| n$. We have already determined the size of $\Psi^{\mathcal{X}}_{n,k}(\ell^\alpha)$ in Corollary 3.2 and Corollary 3.4. Based on those counts, we obtain the following.

Lemma 5.2. *We have*

(1) $$\Psi^{\text{cyc}}_{n,k}(L) = \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left((\ell^2-1)(\ell^2-\ell)-1\right) \prod_{\substack{\ell^\alpha \| (L,n) \\ \ell \mid k-1}} \left(\ell^{3(\alpha-1)}(\ell^3-\ell-1)\right) \prod_{\substack{\ell^\alpha \| (L,n) \\ \ell \nmid k-1}} \left(\ell^{3(\alpha-1)}(\ell^3-\ell)\right).$$

(2) $$\Psi^{\text{prime}}_{n,k}(L) = \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(\ell(\ell^3-2\ell^2-\ell+3)\right) \prod_{\substack{\ell^\alpha \| (L,n) \\ \ell \mid k-1}} \left(\ell^{3(\alpha-1)}(\ell^3-\ell^2-\ell)\right) \prod_{\substack{\ell^\alpha \| (L,n) \\ \ell \nmid k-1}} \left(\ell^{3(\alpha-1)}(\ell^3-\ell^2-2\ell)\right).$$

Based on Lemma 5.2.(1), we obtain

$$\begin{aligned}
\delta^{\text{cyc}}_{E,n,k}(L) &= \prod_{\substack{\ell^\alpha \| (n,L) \\ \ell \mid k-1}} \frac{\ell^{3(\alpha-1)}(\ell^3-\ell-1)}{|\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})|} \prod_{\substack{\ell^\alpha \| (n,L) \\ \ell \nmid k-1}} \frac{\ell^{3(\alpha-1)}(\ell^3-\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})|} \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \\
&= \prod_{\ell^\alpha \| (n,L)} \frac{1}{\ell^{\alpha-1}} \prod_{\substack{\ell \mid (n,L) \\ \ell \mid k-1}} \left(\frac{1}{\ell-1} - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \mid (n,L) \\ \ell \nmid k-1}} \left(\frac{1}{\ell-1}\right) \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \\
&= \frac{1}{\phi(n_1)} \prod_{\substack{\ell \mid (n,L) \\ \ell \mid k-1}} \left(1 - \frac{\phi(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right).
\end{aligned} \tag{50}$$

Thus, (47) and (50) give

$$\begin{aligned}
C^{\text{cyc}}_{E,n,k} = \frac{1}{\phi(n_1)} &\prod_{\substack{\ell \mid L \\ k \equiv 1 (\ell)}} \left(1 - \frac{\phi(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \\
&\cdot \frac{1}{\phi(n_2)} \prod_{\substack{\ell \nmid m_E \\ \ell \mid (n,k-1)}} \left(1 - \frac{\phi(\ell)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell \nmid n m_E} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right)
\end{aligned}$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$= \frac{1}{\phi(n)} \prod_{\ell \mid (n,k-1)} \left(1 - \frac{\phi(\ell)}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell \nmid n} \left(1 - \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) = C_{n,k}^{\text{cyc}}.$$

Hence, we obtain that $C_{E,n,k}^{\text{cyc}} = C_{n,k}^{\text{cyc}}$ if $m_E \nmid L$.

Similarly, for the Koblitz case, applying Lemma 5.2.(2), we see

(51)

$$\frac{\delta_{E,n,k}^{\text{prime}}(L)}{\prod_{\ell \mid L}(1-1/\ell)} = \prod_{\substack{\ell^\alpha \| (n,L) \\ \ell \nmid k-1}} \frac{\ell \cdot \ell^{3(\alpha-1)} \cdot (\ell^3 - \ell^2 - 2\ell)}{(\ell-1)|\operatorname{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})|} \prod_{\substack{\ell^\alpha \| (n,L) \\ \ell \mid k-1}} \frac{\ell \cdot \ell^{3(\alpha-1)} \cdot (\ell^3 - \ell^2 - \ell)}{(\ell-1)|\operatorname{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})|} \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right)$$

$$= \frac{1}{\phi(n_1)} \prod_{\substack{\ell \mid (n,L) \\ \ell \nmid k-1}} \left(1 - \frac{\ell^2+\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \mid (n,L) \\ \ell \mid k-1}} \left(1 - \frac{\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right).$$

Thus, Proposition 4.4, Lemma 4.5, and (51) give

$$C_{E,n,k}^{\text{prime}} = \frac{1}{\phi(n_1)} \prod_{\substack{\ell \mid (n,L) \\ \ell \mid k-1}} \left(1 - \frac{\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \mid (n,L) \\ \ell \nmid k-1}} \left(1 - \frac{\ell^2+\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \mid L \\ \ell \nmid n}} \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right)$$

$$\cdot \frac{1}{\phi(n_2)} \prod_{\substack{\ell \nmid m_E \\ \ell \mid n \\ \ell \mid k-1}} \left(1 - \frac{\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\substack{\ell \nmid m_E \\ \ell \mid n \\ \ell \nmid k-1}} \left(1 - \frac{\ell^2+\ell}{|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) \prod_{\ell \nmid n m_E} \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right)$$

$$= C_{n,k}^{\text{prime}}.$$

This completes the proof of the theorem for the case where $m_E \nmid L$.

Now, suppose that $m_E \mid L$. This case is a bit more involved. First, we recall from Section 2.2 the definition of ψ_{ℓ^α} and the fact that $G_E(L) = \ker \psi_L$. By [30, Lemma 16] and (49) we have

$$\left|G_E(L) \cap \Psi_{n,k}^{\mathcal{X}}(L)\right| = \frac{1}{2}\left(\left|\Psi_{n,k}^{\mathcal{X}}(L)\right| + \prod_{\ell^\alpha \| L} \left(\left|Y_{\ell^\alpha,+}^{\mathcal{X}}\right| - \left|Y_{\ell^\alpha,-}^{\mathcal{X}}\right|\right)\right), \tag{52}$$

for $\mathcal{X} \in \{\text{cyc}, \text{prime}\}$, where

$$Y_{\ell^\alpha,\pm}^{\text{cyc}} := \{M \in \operatorname{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : \psi_{\ell^\alpha}(M) = \pm 1, M \not\equiv I \pmod{\ell}, \det M \equiv k \pmod{\gcd(\ell^\alpha, n)}\},$$

$$Y_{\ell^\alpha,\pm}^{\text{prime}} := \{M \in \operatorname{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : \psi_{\ell^\alpha}(M) = \pm 1, \det(M-I) \not\equiv 0 \pmod{\ell}, \det M \equiv k \pmod{\gcd(\ell^\alpha, n)}\}.$$

The sets $Y_{\ell^\alpha,+}^{\text{cyc}}$, $Y_{\ell^\alpha,-}^{\text{cyc}}$, $Y_{\ell^\alpha,+}^{\text{prime}}$, and $Y_{\ell^\alpha,-}^{\text{prime}}$ all depend on n and k, though we do not include this dependence in the notation for brevity. We first focus on the size of $|Y_{\ell^\alpha,+}^{\mathcal{X}}| - |Y_{\ell^\alpha,-}^{\mathcal{X}}|$ for primes ℓ dividing L^{odd}.

Lemma 5.3. *We have*

(1)

$$\prod_{\ell^\alpha \| L^{\text{odd}}} \left(|Y_{\ell^\alpha,+}^{\text{cyc}}| - |Y_{\ell^\alpha,-}^{\text{cyc}}|\right) =$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$\prod_{\substack{\ell | L^{\text{odd}} \\ \ell \nmid n}} (-1) \prod_{\substack{\ell^\alpha \| (n, L^{\text{odd}}) \\ \ell | k-1}} \ell^{3(\alpha-1)}(\ell^3-\ell-1) \prod_{\substack{\ell^\alpha \| (n, L^{\text{odd}}) \\ \ell \nmid k-1}} \left(\frac{k}{\ell}\right) \ell^{3(\alpha-1)}(\ell^3-\ell).$$

(2)

$$\prod_{\ell^\alpha \| L^{\text{odd}}} \left(|Y^{\text{prime}}_{\ell^\alpha,+}| - |Y^{\text{prime}}_{\ell^\alpha,-}|\right) =$$

$$\prod_{\substack{\ell | L^{\text{odd}} \\ \ell \nmid n}} \ell \prod_{\substack{\ell^\alpha \| (n, L^{\text{odd}}) \\ \ell | k-1}} \ell^{3(\alpha-1)}(\ell^3-\ell^2-\ell) \prod_{\substack{\ell^\alpha \| (n, L^{\text{odd}}) \\ \ell \nmid k-1}} \left(\frac{k}{\ell}\right) \ell^{3(\alpha-1)}(\ell^3-\ell^2-2\ell).$$

Proof. From the definition of ψ_{ℓ^α} for an odd prime $\ell \mid L$, we have

$$\left|Y^{\text{cyc}}_{\ell^\alpha,\pm}\right| = \#\left\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : \left(\frac{\det M}{\ell}\right) = \pm 1, M \not\equiv I \pmod{\ell}, \det M \equiv k \pmod{\ell^\alpha}\right\},$$

$$\left|Y^{\text{prime}}_{\ell^\alpha,\pm}\right| = \#\left\{M \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : \left(\frac{\det M}{\ell}\right) = \pm 1, \det(M-I) \not\equiv 0 \pmod{\ell}, \det M \equiv k \pmod{\ell^\alpha}\right\}.$$

By Corollaries 3.2 and 3.4, it is easy to check that

$$\left|Y^{\text{cyc}}_{\ell^\alpha,+}\right| = \begin{cases} \ell^{3(\alpha-1)}\left(\ell^3-\ell-1\right) & \text{if } \ell \mid n \text{ and } k \equiv 1 \pmod{\ell}, \\ \ell^{3(\alpha-1)}(\ell^3-\ell) & \text{if } \ell \mid n, k \not\equiv 1 \pmod{\ell}, \text{ and } \left(\frac{k}{\ell}\right) = 1, \\ 0 & \text{if } \ell \mid n, \left(\frac{k}{\ell}\right) = -1, \\ \frac{(\ell^2-\ell)(\ell^2-1)}{2} - 1 & \text{if } \ell \nmid n, \end{cases}$$

$$\left|Y^{\text{cyc}}_{\ell^\alpha,-}\right| = \begin{cases} 0 & \text{if } \ell \mid n \text{ and } \left(\frac{k}{\ell}\right) = 1, \\ \ell^{3(\alpha-1)}(\ell^3-\ell) & \text{if } \ell \mid n \text{ and } \left(\frac{k}{\ell}\right) = -1, \\ \frac{(\ell^2-\ell)(\ell^2-1)}{2} & \text{if } \ell \nmid n, \end{cases}$$

$$\left|Y^{\text{prime}}_{\ell^\alpha,+}\right| = \begin{cases} \ell^{3(\alpha-1)}(\ell^3-\ell^2-\ell) & \text{if } \ell \mid n \text{ and } k \equiv 1 \pmod{\ell} \\ \ell^{3(\alpha-1)}(\ell^3-\ell^2-2\ell) & \text{if } \ell \mid n \text{ and } k \not\equiv 1 \pmod{\ell}, \text{ and } \left(\frac{k}{\ell}\right) = 1, \\ 0 & \text{if } \ell \mid n \text{ and } \left(\frac{k}{\ell}\right) = -1, \\ \frac{(\ell-1)(\ell^3-\ell^2-2\ell)}{2} + \ell & \text{if } \ell \nmid n, \end{cases}$$

$$\left|Y^{\text{prime}}_{\ell^\alpha,-}\right| = \begin{cases} 0 & \text{if } \ell \mid n \text{ and } \left(\frac{k}{\ell}\right) = 1, \\ \ell^{3(\alpha-1)}(\ell^3-\ell^2-2\ell) & \text{if } \ell \mid n \text{ and } \left(\frac{k}{\ell}\right) = -1, \\ \frac{(\ell-1)(\ell^3-\ell^2-2\ell)}{2} & \text{if } \ell \nmid n. \end{cases}$$

The result now follows from some simple computations. □

Finally, we evaluate $|Y^{\mathcal{X}}_{\ell^\alpha,+}| - |Y^{\mathcal{X}}_{\ell^\alpha,-}|$ when $\ell = 2$.

Lemma 5.4. *For fixed Δ' and k, let τ be defined as in Definition 5.1. Then*

(1) $|Y^{\text{cyc}}_{2^\alpha,+}| - |Y^{\text{cyc}}_{2^\alpha,-}| = \tau \cdot 2^{3(\alpha-1)}$

(2) $|Y^{\text{prime}}_{2^\alpha,+}| - |Y^{\text{prime}}_{2^\alpha,-}| = -(2\tau) \cdot 2^{3(\alpha-1)}$.

Proof. First, we assume $\Delta' \equiv 1 \pmod{4}$. Then, by the definition of $\psi_{2^\alpha}(\cdot)$,

$$Y^{\text{cyc}}_{2^\alpha,\pm} = \{M \in \mathrm{GL}_2(\mathbb{Z}/2^\alpha\mathbb{Z}) : \epsilon(M_2) = \pm 1, M \not\equiv I \pmod{2}, \det M \equiv k \pmod{2^\alpha}\},$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$Y_{2^\alpha,\pm}^{\rm prime}=\left\{M\in \mathrm{GL}_2(\mathbb{Z}/2^\alpha\mathbb{Z}) : \epsilon(M_2)=\pm1, \det(M-I)\not\equiv 0 \pmod 2, \det M\equiv k \pmod{2^\alpha}\right\}.$$

Let $h_\pm^{\rm cyc}=|Y_{2,\pm}^{\rm cyc}|$. In the case where $\alpha=1$, it is clear that $h_+^{\rm cyc}=2$ and $h_-^{\rm cyc}=3$. For $\alpha\ge 2$, by Lemma 3.1, we obtain

$$\left|Y_{2^\alpha,\pm}^{\rm cyc}\right| = h_\pm^{\rm cyc}\cdot 2^{3(\alpha-1)}$$

and hence $|Y_{2^\alpha,+}^{\rm cyc}|-|Y_{2^\alpha,-}^{\rm cyc}|=-2^{3(\alpha-1)}$.

Let us check the size of $Y_{2^\alpha,\pm}^{\rm prime}$. In the case where $\alpha=1$, we have that

$$Y_{2,+}^{\rm prime}=\left\{\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\} \quad\text{and}\quad Y_{2,-}^{\rm prime}=\emptyset.$$

Setting $h_\pm^{\rm prime}:=|Y_{2,\pm}^{\rm prime}|$, we see that $h_+^{\rm prime}=2$ and $h_-^{\rm prime}=0$. By Lemma 3.1, we obtain

$$\left|Y_{2^\alpha,\pm}^{\rm prime}\right| = h_\pm^{\rm prime}\cdot 2^{3(\alpha-1)}$$

and hence $|Y_{2^\alpha,+}^{\rm prime}|-|Y_{2^\alpha,-}^{\rm prime}|=2\cdot 2^{3(\alpha-1)}$.

Next, we assume $\Delta'\equiv 3 \pmod 4$. Then, by the definition of $\psi_{2^\alpha}(\cdot)$, we have

$$Y_{2^\alpha,\pm}^{\rm cyc}=\left\{M\in \mathrm{GL}_2(\mathbb{Z}/2^\alpha\mathbb{Z}) : \epsilon(M_2)\chi_4(k)=\pm1, M\not\equiv I \pmod 2, \det M\equiv k \pmod{2^\alpha}\right\},$$
$$Y_{2^\alpha,\pm}^{\rm prime}=\left\{M\in \mathrm{GL}_2(\mathbb{Z}/2^\alpha\mathbb{Z}) : \epsilon(M_2)\chi_4(k)=\pm1, \det(M-I)\not\equiv 0 \pmod 2, \det M\equiv k \pmod{2^\alpha}\right\}.$$

Then

$$|Y_{2^\alpha,+}^{\rm cyc}|-|Y_{2^\alpha,-}^{\rm cyc}|=\begin{cases}-2^{3(\alpha-1)} & \text{if } k\equiv 1 \pmod 4,\\ 2^{3(\alpha-1)} & \text{if } k\equiv 3 \pmod 4.\end{cases}$$
$$|Y_{2^\alpha,+}^{\rm prime}|-|Y_{2^\alpha,-}^{\rm prime}|=\begin{cases}2^{3\alpha-2} & \text{if } k\equiv 1 \pmod 4,\\ -2^{3\alpha-2} & \text{if } k\equiv 3 \pmod 4.\end{cases}$$

Similar arguments can be applied to deduce the results for $\Delta'\equiv 2 \pmod 8$ and $\Delta'\equiv 6 \pmod 8$. □

With the results of the above lemmas in hand, we now determine $|G_E(L)\cap\Psi_{n,k}^{\mathcal{X}}|$. Let us treat the cyclicity case first. By Lemma 5.4 and (52), we find that

$$\begin{aligned}|G_E(L)\cap\Psi_{n,k}^{\rm cyc}| &= \frac12\left(|\Psi_{n,k}^{\rm cyc}(L)|+\prod_{\ell^\alpha\| L}\left(|Y_{\ell^\alpha,+}^{\rm cyc}|-|Y_{\ell^\alpha,-}^{\rm cyc}|\right)\right)\\ &=\frac12\left(\prod_{\substack{\ell^\alpha\|(L,n)\\ \ell\mid k-1}}\ell^{3(\alpha-1)}(\ell^3-\ell-1)\prod_{\substack{\ell^\alpha\|(L,n)\\ \ell\nmid k-1}}\ell^{3(\alpha-1)}(\ell^3-\ell)\prod_{\substack{\ell\mid L\\ \ell\nmid n}}(|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|-1)\right.\\ &\qquad\left.+2^{3(\alpha-1)}\tau\prod_{\substack{\ell^\alpha\|(n,L^{\rm odd})\\ \ell\mid k-1}}\ell^{3(\alpha-1)}(\ell^3-\ell-1)\prod_{\substack{\ell^\alpha\|(n,L^{\rm odd})\\ \ell\nmid k-1}}\left(\frac{k}{\ell}\right)\ell^{3(\alpha-1)}(\ell^3-\ell)\prod_{\substack{\ell\mid L^{\rm odd}\\ \ell\nmid n}}(-1)\right)\end{aligned}$$

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$$= \frac{1}{2} \prod_{\ell^\alpha \| (L,n)} \ell^{3(\alpha-1)} \prod_{\substack{\ell | (L^{\mathrm{odd}},n) \\ \ell | k-1}} (\ell^3 - \ell - 1) \prod_{\substack{\ell | (L^{\mathrm{odd}},n) \\ \ell \nmid k-1}} (\ell^3 - \ell) \left(5 \prod_{\substack{\ell | L^{\mathrm{odd}} \\ \ell \nmid n}} (|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| - 1) + \tau^{\mathrm{cyc}} \right).$$

Since we are assuming that $m_E \mid L$, $G_E(L)$ must be an index 2 subgroup of $\operatorname{GL}_2(\mathbb{Z}/L\mathbb{Z})$. Thus, we have

$$|G_E(L)| = \frac{1}{2} \cdot \prod_{\ell^\alpha \| L} |\operatorname{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})| = \frac{1}{2} \cdot \prod_{\ell^\alpha \| L} \ell^{4(\alpha-1)} |\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|. \tag{53}$$

Along with Proposition 4.10 and Lemma 4.11, a short computation reveals that

$$C_{E,n,k}^{\mathrm{cyc}} = \frac{|G_E(L) \cap \Psi_{n,k}^{\mathrm{cyc}}(L)|}{|G_E(L)|} \prod_{\substack{\ell \nmid m_E \\ \ell^\alpha \| n}} \delta_{E,n,k}^{\mathrm{cyc}}(\ell^\alpha) \prod_{\ell \nmid n m_E} \delta_E^{\mathrm{cyc}}(\ell)$$

$$= C_{n,k}^{\mathrm{cyc}} \left(1 + \tau^{\mathrm{cyc}} \frac{1}{5 \prod_{\substack{\ell | L^{\mathrm{odd}} \\ \ell \nmid n}} (|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| - 1)} \right).$$

Now we move on to the Koblitz case. By Lemma 5.4, we have $|Y_{2^\alpha,+}^{\mathrm{prime}}| - |Y_{2^\alpha,-}^{\mathrm{prime}}| = -\tau 2^{3\alpha-2}$. Hence, by (52), a simple calculation reveals that $|G_E(L) \cap \Psi_{n,k}^{\mathrm{prime}}(L)|$ equals

$$\frac{1}{2} \left(|\Psi_{n,k}^{\mathrm{prime}}(L)| + \prod_{\ell^\alpha \| L} (|Y_{\ell^\alpha,+}^{\mathrm{prime}}| - |Y_{\ell^\alpha,-}^{\mathrm{prime}}|) \right)$$

$$= \frac{1}{2} \left(\prod_{\substack{\ell^\alpha \| (L,n) \\ \ell | k-1}} \ell^{3(\alpha-1)} (\ell^3 - \ell^2 - \ell) \prod_{\substack{\ell^\alpha \| (L,n) \\ \ell \nmid k-1}} \ell^{3(\alpha-1)} (\ell^3 - \ell^2 - 2\ell) \prod_{\substack{\ell | L \\ \ell \nmid n}} \ell(\ell^3 - 2\ell^2 - \ell + 3) \right.$$

$$\left. -2^{3\alpha-2}\tau \prod_{\substack{\ell^\alpha | (n,L^{\mathrm{odd}}) \\ \ell | k-1}} \ell^{3(\alpha-1)} (\ell^3 - \ell^2 - \ell) \prod_{\substack{\ell^\alpha | (n,L^{\mathrm{odd}}) \\ \ell \nmid k-1}} \left(\frac{k}{\ell}\right) \ell^{3(\alpha-1)} (\ell^3 - \ell^2 - 2\ell) \prod_{\substack{\ell | L^{\mathrm{odd}} \\ \ell \nmid n}} \ell \right)$$

$$= \frac{1}{2} \prod_{\ell^\alpha \| L} \ell^{3(\alpha-1)} \prod_{\substack{\ell | (L,n) \\ \ell | k-1}} (\ell^3 - \ell^2 - \ell) \prod_{\substack{\ell | (L,n) \\ \ell \nmid k-1}} (\ell^3 - \ell^2 - 2\ell) \left(\prod_{\substack{\ell | L \\ \ell \nmid n}} \ell(\ell^3 - 2\ell^2 - \ell + 3) + \tau^{\mathrm{prime}} \prod_{\substack{\ell | L \\ \ell \nmid n}} \ell \right).$$

Finally, by Proposition 4.4, Lemma 4.5, (51), and (53), we get

$$C_{E,n,k}^{\mathrm{prime}} = \frac{|G_E(L) \cap \Psi_{n,k}^{\mathrm{prime}}(L)|}{|G_E(L)| \cdot \prod_{\ell | L} (1 - 1/\ell)} \prod_{\substack{\ell \nmid m_E \\ \ell^\alpha \| n}} \frac{\delta_{E,n,k}^{\mathrm{prime}}(\ell^\alpha)}{1 - 1/\ell} \prod_{\ell \nmid n m_E} \frac{\delta_E^{\mathrm{prime}}(\ell)}{1 - 1/\ell}$$

$$= C_{n,k}^{\text{prime}}\left(1+\frac{\tau^{\text{prime}}\cdot\prod_{\substack{\ell|L\\ \ell\nmid n}}\ell}{\prod_{\substack{\ell|L\\ \ell\nmid n}}\ell(\ell^3-2\ell^2-\ell+3)}\right) = C_{n,k}^{\text{prime}}\left(1+\frac{\tau^{\text{prime}}}{\prod_{\substack{\ell|L\\ \ell\nmid n}}(\ell^3-2\ell^2-\ell+3)}\right).$$

This completes the proof of Theorem 1.7.

6. On the Koblitz constant for non-Serre curves

6.1. **Bounding the Koblitz constant for non-CM, non-Serre curves.** In this subsection, we will determine an upper bound for $C_{E,n,k}^{\text{prime}}$ in the case of non-CM, non-Serre curves.

Let $E/\mathbb{Q}$ be a non-CM, non-Serre curve, defined by the model (4), of adelic level m_E. Let L be defined as in (7). Then we write $L = L_1L_2$ such that L_2 is the product of prime powers $\ell^\alpha \parallel L$ with $\ell \notin \{2,3,5\}$ and $G_E(\ell) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. By [16, Appendix, Theorem 1], $G_E(L_2) \simeq \mathrm{GL}_2(\mathbb{Z}/L_2\mathbb{Z})$. Let $\varpi\colon \mathrm{GL}_2(\mathbb{Z}/L\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/L_2\mathbb{Z})$ be the natural reduction map. Note that

$$\varpi\left(G_E(L)\cap\Psi_{n,k}^{\text{prime}}(L)\right) \subseteq G_E(L_2)\cap\Psi_{n,k}^{\text{prime}}(L_2).$$

Since ϖ is a surjective group homomorphism, we have

$$\begin{aligned}\delta_{E,n,k}^{\text{prime}}(L) &= \frac{\left|G_E(L)\cap\Psi_{n,k}^{\text{prime}}(L)\right|}{|G_E(L)|}\\ &\le \frac{\left|\varpi^{-1}\left(G_E(L_2)\cap\Psi_{n,k}^{\text{prime}}(L_2)\right)\right|}{|\varpi^{-1}(G_E(L_2))|} = \frac{\left|G_E(L_2)\cap\Psi_{n,k}^{\text{prime}}(L_2)\right|}{|G_E(L_2)|} = \delta_{E,n,k}^{\text{prime}}(L_2).\end{aligned} \tag{54}$$

Since ρ_{E,L_2} is surjective, we apply the same argument as in the proof of Lemma 4.5 and obtain

$$\frac{\delta_{E,n,k}^{\text{prime}}(L_2)}{\prod_{\ell|L_2}(1-1/\ell)} \le 1.$$

Before proceeding to bound the constant $C_{E,n,k}^{\text{prime}}$, we first state a standard analytic result.

Lemma 6.1. *For any positive integer M, we have*

$$\prod_{\ell|M}\left(1-\frac{1}{\ell}\right)^{-1} \ll \max\{1,\log\log M\}.$$

Proof. Follows from Mertens' theorem [44, p. 53, (15)]. See [62, p. 767] for the argument. □

From Lemma 4.5, Lemma 6.1, (32), (36), and (54), we obtain

$$\begin{aligned}C_{E,n,k}^{\text{prime}} &= \frac{\delta_{E,n,k}^{\text{prime}}(L)}{\prod_{\ell|L}(1-1/\ell)}\prod_{\substack{\ell^\alpha\|n\\ \ell\nmid m_E}}\frac{\delta_{E,n,k}^{\text{prime}}(\ell^\alpha)}{1-1/\ell}\prod_{\ell\nmid nm_E}\frac{\delta_{E,n,k}^{\text{prime}}(\ell)}{1-1/\ell}\\ &\le \frac{1}{\prod_{\ell|L_1}(1-1/\ell)}\cdot\frac{\delta_{E,n,k}^{\text{prime}}(L_2)}{\prod_{\ell|L_2}(1-1/\ell)} \le \prod_{\ell|L_1}\frac{1}{1-1/\ell} \ll \max\{1,\log\log\mathrm{rad}(L_1)\}.\end{aligned} \tag{55}$$

Our next task is to bound $\mathrm{rad}(L_1)$ in terms of a and b appearing in the short Weierstrass model (4) of E. Write $j_E \in \mathbb{Q}$ to denote the j-invariant of E and $h := h(j_E)$ for the Weil height of j_E. If

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

$\ell \mid L_1$, then either $\ell \leq 5$ or $\rho_{E,\ell}$ is not surjective. By the main theorem of [41], there exist absolute constant κ and λ for which $\rho_{E,\ell}$ is surjective for all $\ell > \kappa(\max\{1,h\})^\lambda$. Since $\mathrm{rad}(L_1)$ is squarefree, we have

$$\begin{aligned} &\mathrm{rad}(L_1) \leq 30 \prod_{\ell \leq \kappa(\max\{1,h\})^\lambda} \ell \\ (56) \qquad &\implies \log \mathrm{rad}(L_1) \ll \sum_{\ell \leq \kappa(\max\{1,h\})^\lambda} \log \ell \ll (\max\{1,h\})^\lambda \log \max\{1,h\}. \end{aligned}$$

Since E is given by the model (4), we have that

$$h = h(j_E) \ll \log \max\{|a|^3, |b|^2\}. \tag{57}$$

Combining (55), (56), and (57), we obtain the following result.

Proposition 6.2. *Let $E/\mathbb{Q}$ be a non-CM, non-Serre curve given by (4). Then we have*

$$C_{E,n,k}^{\mathrm{prime}} \ll \log \log \max\{|a|^3, |b|^2\}.$$

6.2. **Bounding the Koblitz constant for CM curves.** In this subsection, we focus on CM elliptic curves $E/\mathbb{Q}$. The goal is to show that the constant $C_{E,n,k}^{\mathrm{prime}}$ is bounded independent of the choice of the CM curve (Proposition 6.7). We keep the notation from Section 2.3.

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. Let p be a prime of Koblitz reduction for $E/\mathbb{Q}$. Since $[K:\mathbb{Q}] = 2$, the prime p either splits completely, stays inert, or ramifies over $K/\mathbb{Q}$.

If p does not split over $K/\mathbb{Q}$, then by Deuring's criterion [22], p is a supersingular prime for E and we have $a_p(E) = 0$. Therefore,

$$|\widetilde{E}_p(\mathbb{F}_p)| = p + 1,$$

which is an even number if $p > 2$. Thus, an odd supersingular prime cannot be a prime of Koblitz reduction for E.

Now suppose p splits completely in K and let $\mathbf{p}$ be a prime lying above p. We consider two cases depending on the value of D modulo 4. Following the notation of [58, Chapter 2.2], when $D \equiv 1, 2 \pmod 4$, let $M, N \in \mathbb{Z}$ be such that $\mathbf{p}$ is generated by $M + N\sqrt{-D}$ for some $M, N \in \mathbb{Z}$. In this case, the Frobenius trace satisfies $a_p(E) = 2M$, so $|\widetilde{E}_p(\mathbb{F}_p)| = p + 1 - a_p(E)$ is always even for odd primes p. Therefore, $\pi_E^{\mathrm{prime}}(x)$ is uniformly bounded.

On the other hand, if $D \equiv 3 \pmod 4$, then we can let $M, N \in \mathbb{Z}$ be such that $M + N(1+\sqrt{-D})/2$ generates $\mathbf{p}$. Let us define a binary quadratic form

$$f_D(x,y) = x^2 + xy + \left(\frac{1+D}{4}\right) y^2 \in \mathbb{Z}[x,y].$$

Then, one can check

$$p = N_{K/\mathbb{Q}}(\mathbf{p}) = f_D(M,N) \quad \text{and} \quad |\widetilde{E}_p(\mathbb{F}_p)| = f_D(M-1,N).$$

Thus, we see that this is related to studying integer pairs $(M,N) \in \mathbb{Z}^2$ for which both $f_D(M,N)$ and $f_D(M-1,N)$ are primes. This setup is a special case of the multivariate Bateman–Horn conjecture [6], which generalizes the Hardy–Littlewood conjecture to the setting of several variables [28].

This idea can be used to note additional CM curves for which $\pi_E^{\mathrm{prime}}(x)$ is bounded. Suppose $D \equiv 7 \pmod 8$. (In fact, $K = \mathbb{Q}(\sqrt{-7})$ is the only CM field satisfying the property.) A direct calculation shows that there are no integer pairs (M,N) for which both $f_D(M,N)$ and $f_D(M-1,N)$ are odd, and thus prime. Consequently, for this curve $\pi_E^{\mathrm{prime}}(x)$ is uniformly bounded. An alternative

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

way to see this is to observe that every elliptic curve E with CM field $\mathbb{Q}(\sqrt{-7})$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z}$.

We now turn to our original formulation of the prime-counting function. Note that $\mathbb{F}_p \simeq \mathbb{F}_{\mathbf{p}}$ and the $\widetilde{E}_p$ is isomorphic to $\widetilde{E}_{\mathbf{p}}$ as an elliptic curve over the base field. In particular,

$$|\widetilde{E}_p(\mathbb{F}_p)| = |\widetilde{E}_{\mathbf{p}}(\mathbb{F}_{\mathbf{p}})|.$$

Thus, we obtain

$$\begin{aligned}\pi_E^{\text{prime}}(x;n,k) &:= \#\{p \le x : p \nmid N_E, |\widetilde{E}_p(\mathbb{F}_p)| \text{ is prime}, p \equiv k \pmod n\}\\ &= \#\{p \le x : p \nmid N_E, |\widetilde{E}_p(\mathbb{F}_p)| \text{ is prime}, p \text{ splits over } K/\mathbb{Q}, p \equiv k \pmod n\} + \mathbf{O}(1)\\ &= \frac{1}{2}\#\{\mathbf{p} : N_{K/\mathbb{Q}}(\mathbf{p}) \le x, N_{K/\mathbb{Q}}(\mathbf{p}) \nmid N_E, |\widetilde{E}_{\mathbf{p}}(\mathbb{F}_{\mathbf{p}})| \text{ is prime},\\ &\qquad N_{K/\mathbb{Q}}(\mathbf{p}) \text{ is a rational prime}, N_{K/\mathbb{Q}}(\mathbf{p}) \equiv k \pmod n\} + \mathbf{O}(1).\end{aligned}$$

The Koblitz conjecture in arithmetic progressions for CM elliptic curves can be formulated as follows:

Conjecture 6.3. Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K. Let m_E be as in Lemma 2.6, n be a positive integer, and k be an integer coprime to n. Then there exists a constant $C_{E/K,n,k}^{\text{prime}}$ defined in (62) such that

$$\pi_E^{\text{prime}}(x;n,k) \sim \frac{C_{E/K,n,k}^{\text{prime}}}{2} \cdot \frac{x}{\log^2 x} \qquad \text{as } x \to \infty. \tag{58}$$

If the constant vanishes, we interpret (58) as stating that there are only finitely many primes $p \equiv k \pmod n$ of Koblitz reduction for E.

Comparing with Conjecture 1.6, we have

$$C_{E,n,k}^{\text{prime}} = \frac{C_{E/K,n,k}^{\text{prime}}}{2}, \tag{59}$$

where $C_{E/K,n,k}^{\text{prime}}$ is defined in (60).

We now introduce some notation used to determine the constant $C_{E/K,n,k}^{\text{prime}}$. For a positive integer m, let us fix a $\mathbb{Z}/m\mathbb{Z}$-basis of $\mathcal{O}/m\mathcal{O}$. This allows us to view $\mathrm{GL}_1(\mathcal{O}/m\mathcal{O}) = (\mathcal{O}/m\mathcal{O})^\times$ a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let $\det\colon (\mathcal{O}/m\mathcal{O})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ be the determinant map, defined in the natural way. Fixing a standard orthogonal basis of $\mathcal{O}/m\mathcal{O}$, N is identified with the determinant map. Thus, drawing a parallel from (34), we are led to define

$$\Psi_{K,n,k}^{\text{prime}}(m) = \left\{g \in (\mathcal{O}/m\mathcal{O})^\times : \det(g-1) \in (\mathbb{Z}/m\mathbb{Z})^\times, \det g \equiv k \pmod{\gcd(m,n)}\right\}.$$

Observe that $\rho_{E,m}(\mathrm{Frob}_{\mathbf{p}}) \in G_E(m) \cap \Psi_{K,n,k}^{\text{prime}}(m)$ if and only if $|\widetilde{E}_{\mathbf{p}}(\mathbb{F}_{\mathbf{p}})|$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ and $\det(\rho_{E,m}(\mathrm{Frob}_{\mathbf{p}})) \equiv k \pmod{\gcd(m,n)}$. Hence, we are led to define

$$\delta_{E/K,n,k}^{\text{prime}}(m) := \frac{\left|G_E(m) \cap \Psi_{K,n,k}^{\text{prime}}(m)\right|}{|G_E(m)|}.$$

Drawing a parallel from (35), we set

$$C_{E/K,n,k}^{\text{prime}} := \lim_{m\to\infty} \frac{\delta_{E/K,n,k}^{\text{prime}}(m)}{\prod_{\ell \mid m}(1-1/\ell)}, \tag{60}$$

where the limit is taken over all positive integers ordered by divisibility.

Lemma 6.4. *Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}$ of conductor f in an imaginary quadratic field K. Let m_E be as in Lemma 2.6. and $\chi := \chi_K$ be given as in (17). For each rational prime $\ell \nmid fm_E$ and $\ell \nmid n$, we have*

$$\frac{\delta^{\text{prime}}_{E/K,n,k}(\ell)}{1-1/\ell} = 1 - \chi(\ell)\frac{\ell^2-\ell-1}{(\ell-\chi(\ell))(\ell-1)^2}.$$

For each prime $\ell \nmid fm_E$ and $\ell^\alpha \parallel n$, we have

$$\frac{\delta^{\text{prime}}_{E/K,n,k}(\ell^\alpha)}{1-1/\ell} = \begin{cases} \dfrac{1}{\phi(\ell^\alpha)}\left(1-\chi(\ell)\dfrac{1}{(\ell-\chi(\ell))(\ell-1)}\right) & \text{if } \ell^\alpha \parallel n \text{ and } k \equiv 1 \pmod{\ell}, \\ \dfrac{1}{\phi(\ell^\alpha)}\left(1-\chi(\ell)\dfrac{\ell+1}{(\ell-\chi(\ell))(\ell-1)}\right) & \text{if } \ell^\alpha \parallel n \text{ and } k \not\equiv 1 \pmod{\ell}. \end{cases}$$

Proof. First, we consider the case where $\ell \nmid nfm_E$. By Lemma 2.6, we have $G_E(\ell) \simeq (\mathcal{O}_K/\ell\mathcal{O}_K)^\times$ and the condition $\det g \equiv k \pmod{\gcd(\ell,n)}$ trivially holds. Hence

$$G_E(\ell) \cap \Psi^{\text{prime}}_{K,n,k}(\ell) = \{g \in (\mathcal{O}_K/\ell\mathcal{O}_K)^\times : \det(g-1) \not\equiv 0 \pmod{\ell}\}.$$

Therefore, by Corollary 3.6, we get

$$|\Psi^{\text{prime}}_{K,n,k}(\ell)| = (\ell-2)^2 \quad \text{or} \quad |\Psi^{\text{prime}}_{K,n,k}(\ell)| = \ell^2-2$$

depending on whether ℓ splits or is inert in K.

Now we assume $\ell^\alpha \parallel n$. Similarly, we have $G_E(\ell^\alpha) \simeq (\mathcal{O}_K/\ell^\alpha\mathcal{O}_K)^\times$ and hence

$$G_E(\ell^\alpha) \cap \Psi^{\text{prime}}_{K,n,k}(\ell^\alpha) = \Psi^{\text{prime}}_{K,n,k}(\ell^\alpha).$$

Then the condition $\det g \equiv k \pmod{\gcd(\ell^\alpha, n)}$ becomes $\det g \equiv k \pmod{\ell^\alpha}$. So we get

$$\Psi^{\text{prime}}_{K,n,k}(\ell^\alpha) = \left\{g \in (\mathcal{O}_K/\ell^\alpha\mathcal{O}_K)^\times : \det(g-1) \not\equiv 0 \pmod{\ell}, \det g \equiv k \pmod{\ell^\alpha}\right\}.$$

If $k \equiv 1 \pmod{\ell}$, then by Corollary 3.6,

$$|\Psi^{\text{prime}}_{K,n,k}(\ell^\alpha)| = \ell^{\alpha-1}(\ell-2) \quad \text{or} \quad |\Psi^{\text{prime}}_{K,n,k}(\ell^\alpha)| = \ell^\alpha$$

depending on whether ℓ splits or is inert in K. If $k \not\equiv 1 \pmod{\ell}$, then

$$|\Psi^{\text{prime}}_{K,n,k}(\ell^\alpha)| = \ell^{\alpha-1}(\ell-3) \quad \text{or} \quad |\Psi^{\text{prime}}_{K,n,k}(\ell^\alpha)| = \ell^{\alpha-1}(\ell+1),$$

depending on whether ℓ splits or is inert in K. □

For a CM elliptic curve $E/\mathbb{Q}$ with CM by an order $\mathcal{O}$ of conductor f, we set

$$L := \prod_{\ell \mid fm_E} \ell^{\alpha_\ell}, \qquad \text{where } \alpha_\ell = \begin{cases} v_\ell(n) & \text{if } \ell \mid n, \\ 1 & \text{otherwise.} \end{cases} \tag{61}$$

To save notation, we will write ℓ^α instead of ℓ^{α_ℓ}.

Proposition 6.5. *Let $E/\mathbb{Q}$ have a CM by an order $\mathcal{O}$ of conductor f in an imaginary quadratic field K. Let $\chi := \chi_K$ be as given in (17). Let m_E be as in Lemma 2.6. Let L be defined as in (61). Fix a positive integer n. Then, $\delta^{\text{prime}}_{E/K,n,k}(\cdot)$, as an arithmetic function, satisfies the following properties:*

(1) Let $L \mid L' \mid L^\infty$. Then, $\delta^{\text{prime}}_{E/K,n,k}(L) = \delta^{\text{prime}}_{E/K,n,k}(L')$;

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

(2) Let ℓ^α be a prime power and d be a positive integer with $(\ell, Ld) = 1$. Then, $\delta^{\mathrm{prime}}_{E/K,n,k}(d\ell^\alpha) = \delta^{\mathrm{prime}}_{E/K,n,k}(d) \cdot \delta^{\mathrm{prime}}_{E/K,n,k}(\ell^\alpha)$.

(3) Let $\ell^\alpha \parallel n$ and $(\ell, L) = 1$. Then, for any $\beta > \alpha$, $\delta^{\mathrm{prime}}_{E/K,n,k}(\ell^\beta) = \delta^{\mathrm{prime}}_{E/K,n,k}(\ell^\alpha)$. Further, if $\ell \nmid nL$, we have $\delta^{\mathrm{prime}}_{E/K,n,k}(\ell^\beta) = \delta^{\mathrm{prime}}_{E/K,n,k}(\ell)$.

Therefore, (60) can be expressed as

$$C^{\mathrm{prime}}_{E/K,n,k} = \frac{\delta^{\mathrm{prime}}_{E/K,n,k}(L)}{\prod_{\ell \mid L}(1 - 1/\ell)} \cdot \prod_{\substack{\ell \nmid fm_E \\ \ell^\alpha \parallel n}} \frac{\delta^{\mathrm{prime}}_{E/K,n,k}(\ell^\alpha)}{1 - 1/\ell} \cdot \prod_{\ell \nmid nfm_E} \left(1 - \chi(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi(\ell))(\ell - 1)^2}\right). \tag{62}$$

Proof. One can prove (1)-(3) following the same strategy as in the proof of Proposition 4.4. One only needs to replace m_E by fm_E and $\mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})$ by $(\mathcal{O}/\ell^\alpha\mathcal{O})^\times$. Therefore, from these results, we get

$$C^{\mathrm{prime}}_{E/K,n,k} = \frac{\delta^{\mathrm{prime}}_{E/K,n,k}(L)}{\prod_{\ell \mid L}(1 - 1/\ell)} \cdot \prod_{\substack{\ell \nmid fm_E \\ \ell^\alpha \parallel n}} \frac{\delta^{\mathrm{prime}}_{E/K,n,k}(\ell^\alpha)}{1 - 1/\ell} \cdot \prod_{\ell \nmid nfm_E} \frac{\delta^{\mathrm{prime}}_{E/K,n,k}(\ell)}{1 - 1/\ell}.$$

Now, we see that (62) follows from Lemma 6.4. □

Remark 6.6. Given that $\ell \nmid nfm_E$, we observe that

$$\begin{aligned} \frac{\delta^{\mathrm{prime}}_{E/K,n,k}(\ell)}{1 - 1/\ell} &= 1 - \chi_K(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi_K(\ell))(\ell - 1)^2} \\ &= \left(1 - \frac{\chi_K(\ell)}{\ell} + \mathbf{O}\left(\frac{1}{\ell^2}\right)\right) \\ &= \left(1 - \frac{\chi_K(\ell)}{\ell}\right)\left(1 + \mathbf{O}\left(\frac{1}{\ell^2}\right)\right). \end{aligned}$$

Thus, we have

$$\prod_{\ell \nmid fm_E n} \left(1 - \chi_K(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi_K(\ell))(\ell - 1)^2}\right) = \prod_{\ell \nmid fm_E n} \left(1 - \frac{\chi_K(\ell)}{\ell}\right)\left(1 + \mathbf{O}\left(\frac{1}{\ell^2}\right)\right).$$

Note that this is a product of an Euler factorization of $L(s, \chi_K)^{-1}$ at $s = 1$ (with some correction factor) and an absolutely convergent product. Since $L(1, \chi_K) \neq 0$ for a non-trivial character χ_K, the infinite product in (62) is conditionally convergent.

By (58), (59), Lemma 6.4, and Proposition 6.5, we can explicitly formulate the conjectural Koblitz constant for CM elliptic curves. Let $n = n_1 n_2$ where $n_1 \mid (fm_E)^\infty$ and $(n_2, fm_E) = 1$. (In

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

particular, n_2 is the product of ℓ^α for which $\ell^\alpha \parallel n$ with $\ell \nmid L$.) We have

$$C^{\text{prime}}_{E,n,k} = \frac{1}{2} \cdot \frac{1}{\phi(n_2)} \cdot \frac{\delta^{\text{prime}}_{E/K,n,k}(L)}{\prod_{\ell \mid L}(1-1/\ell)} \cdot \prod_{\substack{\ell^\alpha \parallel n \\ \ell \nmid L \\ \ell \mid k-1}} \left(1 - \chi_K(\ell)\frac{\ell}{(\ell-\chi_K(\ell))(\ell-1)}\right) \cdot \prod_{\substack{\ell^\alpha \parallel n \\ \ell \nmid L \\ \ell \nmid k-1}} \left(1 - \chi_K(\ell)\frac{\ell+1}{(\ell-\chi_K(\ell))(\ell-1)}\right) \cdot \prod_{\ell \nmid n f m_E} \left(1 - \chi_K(\ell)\frac{\ell^2-\ell-1}{(\ell-\chi_K(\ell))(\ell-1)^2}\right). \tag{63}$$

Proposition 6.7. *For any CM elliptic curve $E/\mathbb{Q}$, we have*

$$C^{\text{prime}}_{E,n,k} \ll_n 1.$$

Proof. Note that the finite product terms in (63) are all bounded by 1. By definition, we have

$$\delta^{\text{prime}}_{E/K,n,k}(L) \leq 1,$$

and hence,

$$\frac{\delta^{\text{prime}}_{E/K,n,k}(L)}{\prod_{\ell \mid L}(1-1/\ell)} \ll \max\{1, \log\log \operatorname{rad}(f m_E)\} \ll 1,$$

by Proposition 2.8 and Lemma 6.1. Finally, the infinite product, up to a correction factor depending on n, is universally bounded, since there are only finitely many possibilities for K. ☐

7. Moments

The goal of this section is to complete the proof of Theorem 1.9. We begin by setting forth the general strategy. Let $x > 0$ and $A = A(x)$ and $B = B(x)$ be positive real-valued functions such that $A(x) \to \infty$ and $B(x) \to \infty$ as $x \to \infty$. Let $\mathbb{E}^{a,b}$ be an elliptic curve given by the model

$$\mathbb{E}^{a,b} \colon Y^2 = X^3 + aX + b,$$

for some $a, b \in \mathbb{Z}$ and $4a^3 + 27b^2 \neq 0$. Define

$$\mathcal{F} := \mathcal{F}(x) = \left\{\mathbb{E}^{a,b} \colon |a| \leq A, |b| \leq B\right\}.$$

Our objective is to compute, for any positive integer t, the t-th moment

$$\frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} \left|C^{\mathcal{X}}_{E,n,k} - C^{\mathcal{X}}_{n,k}\right|^t, \tag{64}$$

where $\mathcal{X}$ denotes either "cyc" or "prime". We know that (64) can be expressed as

$$\frac{1}{|\mathcal{F}|}\left(\sum_{\substack{E \in \mathcal{F} \\ E \text{ is Serre}}} \left|C^{\mathcal{X}}_{E,n,k} - C^{\mathcal{X}}_{n,k}\right|^t + \sum_{\substack{E \in \mathcal{F} \\ E \text{ is non-CM} \\ E \text{ is non-Serre}}} \left|C^{\mathcal{X}}_{E,n,k} - C^{\mathcal{X}}_{n,k}\right|^t + \sum_{\substack{E \in \mathcal{F} \\ E \text{ is CM}}} \left|C^{\mathcal{X}}_{E,n,k} - C^{\mathcal{X}}_{n,k}\right|^t\right),$$

where "E is Serre" indicates that "E is a Serre curve", etc. In order to bound (64), we are going to bound each of the three sums separately.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

For the first sum, recall that we proved explicit formulas for the constants $C_{E,n,k}^{\mathcal{X}}$ for Serre curves in Section 5 and found that these constants closely align with their average counterparts $C_{n,k}^{\mathcal{X}}$. For the second and third sums, we will use the fact due to Jones [31] that non-Serre curves are rare. For the cyclicity case, we will use the fact that $C_{E,n,k}^{\mathrm{cyc}}$ is bounded above by $1/\phi(n)$, which follows from (48) (and is sensible, since under GRH, $C_{E,n,k}^{\mathrm{cyc}}$ describes the density of some subset of the primes congruent to k modulo n). However, for the Koblitz case it is not clear that $C_{E,n,k}^{\mathrm{prime}}$ should be bounded by a constant independent of E, so we will instead employ the bounds of Proposition 6.2 and Proposition 6.7.

We first deal with the moments computation for Serre curves. Let $\mathbb{E}^{a,b}/\mathbb{Q}$ be a Serre curve defined by the model

$$\mathbb{E}^{a,b}\colon Y^2 = X^3 + aX + b,$$

of adelic level $m_{\mathbb{E}^{a,b}}$. Let $\Delta'_{a,b}$ denote the squarefree part of the discriminant of $\mathbb{E}^{a,b}$. Recall that $m_{\mathbb{E}^{a,b}}$ is only supported by 2 and the prime factors of $\Delta'_{a,b}$ (see Proposition (2.4)). Set

$$L_{\mathbb{E}^{a,b}} = \frac{|\Delta'_{a,b}|}{\gcd(|\Delta'_{a,b}|, n)}.$$

By Theorem 1.7, we have

$$\left|C_{\mathbb{E}^{a,b},n,k}^{\mathrm{cyc}} - C_{n,k}^{\mathrm{cyc}}\right| \leq \frac{1}{5} C_{n,k}^{\mathrm{cyc}} \prod_{\substack{\ell \mid m_{\mathbb{E}^{a,b}} \\ \ell \nmid 2n}} \frac{1}{\ell^4 - \ell^3 - \ell^2 + \ell - 1} \ll \frac{1}{\mathrm{rad}(m_{\mathbb{E}^{a,b}})^3} \ll \frac{1}{L_{\mathbb{E}^{a,b}}^3},$$

$$\left|C_{\mathbb{E}^{a,b},n,k}^{\mathrm{prime}} - C_{n,k}^{\mathrm{prime}}\right| \leq C_{n,k}^{\mathrm{prime}} \prod_{\substack{\ell \mid m_{\mathbb{E}^{a,b}} \\ \ell \nmid 2n}} \frac{1}{\ell^3 - 2\ell^2 - \ell + 3} \ll \frac{1}{\mathrm{rad}(m_{\mathbb{E}^{a,b}})^2} \ll \frac{1}{L_{\mathbb{E}^{a,b}}^2}.$$

Let us set $r_{\mathrm{cyc}} = 3$ and $r_{\mathrm{prime}} = 2$. Then, we obtain

$$\left|C_{\mathbb{E}^{a,b},n,k}^{\mathcal{X}} - C_{n,k}^{\mathcal{X}}\right| \ll \frac{1}{L_{\mathbb{E}^{a,b}}^{r_{\mathcal{X}}}} = \left(\frac{\gcd\left(|\Delta'_{a,b}|, n\right)}{|\Delta'_{a,b}|}\right)^{r_{\mathcal{X}}},$$

given that $\mathbb{E}^{a,b}/\mathbb{Q}$ is a Serre curve.

Observing that $|\mathcal{F}| \sim 4AB$ as $x \to \infty$, we have for any $A, B, Z \geq 2$ and $t \geq 1$,

$$\frac{1}{|\mathcal{F}|} \sum_{\substack{E \in \mathcal{F} \\ E \text{ is Serre}}} \left|C_{E,n,k}^{\mathcal{X}} - C_{n,k}^{\mathcal{X}}\right|^t \ll \frac{1}{AB} \sum_{\substack{|a| \leq A \\ |b| \leq B \\ \Delta'_{a,b} \neq 0 \\ \frac{|\Delta'_{a,b}|}{(|\Delta'_{a,b}|, n)} < Z}} 1 + \frac{1}{AB} \sum_{\substack{|a| \leq A \\ |b| \leq B \\ \Delta'_{a,b} \neq 0 \\ \frac{|\Delta'_{a,b}|}{(|\Delta'_{a,b}|, n)} \geq Z}} \frac{1}{Z^{r_{\mathcal{X}} t}}. \tag{65}$$

Lemma 7.1. *With the notation above, we have*

$$\sum_{\substack{|a| \leq A \\ |b| \leq B \\ \Delta'_{a,b} \neq 0 \\ \frac{|\Delta'_{a,b}|}{(|\Delta'_{a,b}|, n)} < Z}} 1 \ll n \log B \cdot A \cdot \log^7 A \cdot Z + B.$$

Proof. It follows similarly to the argument given in [30, Section 4.2]. ∎

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Let $Z = \left(B/n \log B \log^7 A\right)^{1/(r_{\mathcal{X}}t+1)}$. By (65) and Lemma 7.1, we see that

$$\frac{1}{|\mathcal{F}|} \sum_{\substack{E\in\mathcal{F}\\ E \text{ is Serre}}} \left|C^{\mathcal{X}}_{E,n,k} - C^{\mathcal{X}}_{n,k}\right|^t \ll \left(\frac{1}{A} + \frac{nZ\log B \log^7 A}{B}\right) + \frac{1}{Z^{r_{\mathcal{X}}t}} \ll \left(\frac{n\log B\log^7 A}{B}\right)^{\frac{r_{\mathcal{X}}t}{r_{\mathcal{X}}t+1}}. \tag{66}$$

By [30, Theorem 25] and (66), there exists $\gamma > 0$ such that for any positive integer t,

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \left|C^{\text{cyc}}_{E,n,k} - C^{\text{cyc}}_{n,k}\right|^t \ll_t \max\left\{\left(\frac{n\log B\log^7 A}{B}\right)^{\frac{3t}{3t+1}}, \frac{\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}}\right\}.$$

This completes the proof for the cyclicity case.

For primes of Koblitz reduction, by Proposition 6.2, Proposition 6.7, and [30, Theorem 25], there exists $\gamma > 0$ such that for any positive integer t,

$$\frac{1}{|\mathcal{F}|}\sum_{\substack{E\in\mathcal{F}\\ E \text{ is non-CM}\\ E \text{ is non-Serre}}} \left|C^{\text{prime}}_{E,n,k} - C^{\text{prime}}_{n,k}\right|^t \ll_t \log\log(\max\{A^3,B^2\})^t \frac{\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}},$$

$$\frac{1}{|\mathcal{F}|}\sum_{\substack{E\in\mathcal{F}\\ E \text{ is CM}}} \left|C^{\text{prime}}_{E,n,k} - C^{\text{prime}}_{n,k}\right|^t \ll_{t,n} \frac{\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}}.$$

Therefore, we obtain the inequality claimed in the statement of Theorem 1.9.

8. Numerical examples

8.1. **Example 1.** Let E be the elliptic curve with LMFDB [40] label `1728.w1`, which is given by

$$E\colon y^2 = x^3 + 6x - 2.$$

From the curve's LMFDB page, we note that it is a Serre curve with adelic level $m_E = 6$. Zywina [62, Section 5] computed the Koblitz constant of E,

$$C^{\text{prime}}_E \approx 0.561296.$$

Running either our Magma functions `KoblitzAP` or `SerreCurveKoblitzAP` [38] on E with modulus $n = 6$, we find that

$$C^{\text{prime}}_{E,6,1} = C^{\text{prime}}_E \quad \text{and} \quad C^{\text{prime}}_{E,6,5} = 0.$$

This result can be verified "manually" by studying the mod 6 Galois image of E, as we now discuss.

The mod 6 Galois image $G_E(6)$ is an index 2 subgroup of $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ generated by

$$G_E(6) = \left\langle \begin{pmatrix}1&1\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\5&5\end{pmatrix}, \begin{pmatrix}5&0\\5&1\end{pmatrix}\right\rangle.$$

From this description, we compute that

$$\{\operatorname{tr} M \pmod 6 : M \in G_E(6) \text{ and } \det M \equiv 5 \pmod 6\} = \{0,2,4\}.$$

Thus, if p is a good prime for E that is congruent to 5 modulo 6, then

$$|\widetilde{E}_p(\mathbb{F}_p)| \equiv p + 1 - \operatorname{tr}\rho_{E,6}(\mathrm{Frob}_p) \equiv 1 + 1 - 0 \equiv 0 \pmod 2.$$

Hence $|\widetilde{E}_p(\mathbb{F}_p)|$ is even for all good primes p congruent to 5 modulo 6. By Hasse's bound and computing a few values of $|\widetilde{E}_p(\mathbb{F}_p)|$, we find that $|\widetilde{E}_p(\mathbb{F}_p)|$ is never 2 for such primes p. Thus, the only good primes p for which $|\widetilde{E}_p(\mathbb{F}_p)|$ is prime are congruent to 1 modulo 6.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

8.2. **Example 2.** Let E be the elliptic curve with LMFDB label `200.e1`, which is given by

$$E\colon y^2 = x^3 + 5x - 10.$$

From this curve's LMFDB page, we learn that E is a Serre curve with adelic level $m_E = 8$. Running our Magma function `SerreCurveKoblitzAP` on E with $n = 8$, we find that

$$C^{\mathrm{prime}}_{E,8,1} = C^{\mathrm{prime}}_{E,8,3} = \tfrac{1}{2} C^{\mathrm{prime}}_{E} \quad \text{and} \quad C^{\mathrm{prime}}_{E,8,5} = C^{\mathrm{prime}}_{E,8,7} = 0$$

where

$$C^{\mathrm{prime}}_{E} \approx 0.505166.$$

Running our Magma function `SerreCurveCyclicityAP` on E with $n = 8$, we find that

$$C^{\mathrm{cyc}}_{E,8,1} = C^{\mathrm{cyc}}_{E,8,3} = \tfrac{1}{5} C^{\mathrm{cyc}}_{E} \quad \text{and} \quad C^{\mathrm{cyc}}_{E,8,5} = C^{\mathrm{cyc}}_{E,8,7} = \tfrac{3}{10} C^{\mathrm{cyc}}_{E}.$$

where

$$C^{\mathrm{cyc}}_{E} \approx 0.813752.$$

The values obtained above align well with numerical data for the curve. Among all primes of Koblitz reduction for E up to 10^7, 11114 are congruent to 1 modulo 8 and 11259 are congruent to 3 modulo 8; none are congruent to 5 or 7 modulo 8. Among all primes of cyclic reduction for E up to 10^7, 108096 are congruent to 1 modulo 8, 108251 are congruent to 3 modulo 8, 162234 are congruent to 5 modulo 8, and 162286 are congruent to 7 modulo 8.

8.3. **Example 3.** Let E be the elliptic curve with LMFDB label `864.a1`, which is given by

$$E\colon y^2 = x^3 - 216x - 1296.$$

This curve does not have complex multiplication and is not a Serre curve. Its adelic index is 24 and adelic level is $m_E = 12$. Running our Magma function `KoblitzAP` on E with $n = 12$, we find that

$$C^{\mathrm{prime}}_{E,12,1} = \tfrac{3}{7} C^{\mathrm{prime}}_{E}, \quad C^{\mathrm{prime}}_{E,12,5} = 0, \quad C^{\mathrm{prime}}_{E,12,7} = \tfrac{4}{7} C^{\mathrm{prime}}_{E}, \quad C^{\mathrm{prime}}_{E,12,11} = 0$$

where

$$C^{\mathrm{prime}}_{E} \approx 0.785814.$$

Running our Magma function `CyclicityAP` on E with $n = 12$, we find that

$$C^{\mathrm{cyc}}_{E,12,1} = \tfrac{3}{19} C^{\mathrm{cyc}}_{E}, \quad C^{\mathrm{cyc}}_{E,12,5} = \tfrac{6}{19} C^{\mathrm{cyc}}_{E}, \quad C^{\mathrm{cyc}}_{E,12,7} = \tfrac{4}{19} C^{\mathrm{cyc}}_{E}, \quad C^{\mathrm{cyc}}_{E,12,11} = \tfrac{6}{19} C^{\mathrm{cyc}}_{E}.$$

where

$$C^{\mathrm{cyc}}_{E} \approx 0.789512.$$

As with the previous example, these values agree well with the numerical data for the curve, which is available through our GitHub repository [38].

8.4. **Example 4.** Let $n = 6$ and E be the CM elliptic curve with LMFDB label `432.d1` defined by

$$y^2 = x^3 - 4. \tag{67}$$

We keep the notation from Section 2.3. From the LMFDB, we know that

(1) E has CM by the maximal order $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ of the CM field $K = \mathbb{Q}(\sqrt{-3})$.
(2) E has discriminant $\Delta_E = -2^8 3^3$. So 2 and 3 are the only primes of bad reduction for E.
(3) The map

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \longrightarrow (\mathcal{O}/\ell\mathcal{O})^\times$$

is surjective for all primes ℓ.

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

Invoking the proof of [62, Proposition 2.7], we see that m_E is only supported by 2 and 3. Further,

$$f = 1,\ L = n_1 = n = 6,\ n_2 = 1.$$

Therefore, for k coprime to 6, by (63),

$$C_{E,6,k}^{\text{prime}} = \frac{3}{2} \cdot \frac{|G_E(6) \cap \Psi_{K,6,k}^{\text{prime}}(6)|}{|G_E(6)|} \cdot \prod_{\ell \nmid 6} \left(1 - \chi_K(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi_K(\ell))(\ell - 1)^2}\right).$$

By adapting Suther land's `Galrep` code [56], we compute $G_E(6)$ in Magma and find that

$$\left|\Psi_{K,6,k}^{\text{prime}}(6) \cap G_E(6)\right| = \begin{cases} 2 & \text{if } k \equiv 1 \pmod 6, \\ 0 & \text{if } k \equiv 5 \pmod 6. \end{cases}$$

Thus, we conclude that

$$C_{E,6,1}^{\text{prime}} = C_E^{\text{prime}} \quad \text{and} \quad C_{E,6,5}^{\text{prime}} = 0$$

where

$$C_E^{\text{prime}} = \frac{1}{2} \cdot \prod_{\ell \nmid 6} \left(1 - \chi_K(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi_K(\ell))(\ell - 1)^2}\right) \approx 0.505448.$$

In fact, we can verify that $C_{E,6,5}^{\text{prime}} = 0$ using Deuring's criterion. If p is a rational prime such that $p \equiv 5 \pmod 6$, then p is inert in the CM field $\mathbb{Q}(\sqrt{-3})$. By Deuring's criterion, p is supersingular, and hence $|\widetilde{E}_p(\mathbb{F}_p)| = p + 1$. Since p is an odd prime, we see that p cannot be a prime of Koblitz reduction for E.

References

1. Yildirim Akbal and Ahmet M. Güloğlu, *Cyclicity of elliptic curves modulo primes in arithmetic progressions*, Canad. J. Math. **74** (2022), no. 5, 1277–1309. MR 4504664
2. Amir Akbary and Adam Tyler Felix, *On invariants of elliptic curves on average*, Acta Arith. **168** (2015), no. 1, 31–70. MR 3337211
3. Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944. MR 3961086
4. Antal Balog, Alina-Carmen Cojocaru, and Chantal David, *Average twin prime conjecture for elliptic curves*, Amer. J. Math. **133** (2011), no. 5, 1179–1229. MR 2843097
5. William D. Banks and Igor E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math. **173** (2009), 253–277. MR 2570668
6. Paul T. Bateman and Roger A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367. MR 148632
7. Renee Bell, Clifford Blakestad, Alina Carmen Cojocaru, Alexander Cowan, Nathan Jones, Vlad Matei, Geoffrey Smith, and Isabel Vogt, *Constants in Titchmarsh divisor problems for elliptic curves*, Res. Number Theory **6** (2020), no. 1, Paper No. 1, 24. MR 4041152
8. I. Borosh, C. J. Moreno, and H. Porta, *Elliptic curves over finite fields. II*, Math. Comput. **29** (1975), 951–964. MR 404264
9. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478
10. Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. **305** (2020), no. 1, 43–88. MR 4077686

11. Julio Brau, *Galois representations of elliptic curves and abelian entanglements*, Leiden University, 2015, Doctoral Thesis.
12. Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231. MR 2869057
13. Francesco Campagna and Peter Stevenhagen, *Cyclic reduction densities for elliptic curves*, Res. Number Theory **9** (2023), no. 3, Paper No. 61, 21. MR 4623047
14. Alina Carmen Cojocaru, *On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves*, J. Number Theory **96** (2002), no. 2, 335–350. MR 1932460
15. ______, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc. **355** (2003), no. 7, 2651–2662. MR 1975393
16. ______, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. **48** (2005), no. 1, 16–31, With an appendix by Ernst Kani. MR 2118760
17. ______, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289. MR 2167436
18. Alina Carmen Cojocaru, Etienne Fouvry, and M. Ram Murty, *The square sieve and the Lang-Trotter conjecture*, Canad. J. Math. **57** (2005), no. 6, 1155–1177. MR 2178556
19. Alina Carmen Cojocaru and M. Ram Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. **330** (2004), no. 3, 601–625. MR 2099195
20. David A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989, Fermat, class field theory and complex multiplication. MR 1028322
21. Chantal David and Jie Wu, *Almost prime values of the order of elliptic curves over finite fields*, Forum Math. **24** (2012), no. 1, 99–119. MR 2879973
22. Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR 5125
23. Luke Fredericks, *Average cyclicity for elliptic curves in torsion families*, 2021, arXiv:2101.06202.
24. Lorenzo Furio and Davide Lombardo, *Serre's uniformity question and proper subgroups of $c_{ns}^+(p)$*, 2023, arXiv:2305.17780.
25. Ernst-Ulrich Gekeler, *The distribution of group structures on elliptic curves over finite prime fields*, Doc. Math. **11** (2006), 119–142. MR 2226271
26. Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507. MR 2778661
27. Rajiv Gupta and M. Ram Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), no. 1, 225–235. MR 1055716
28. G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70. MR 1555183
29. Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR 207630
30. Nathan Jones, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685–710. MR 2534114
31. ______, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570. MR 2563740
32. Nathan Jones and Sung Min Lee, *On the acyclicity of reductions of elliptic curves modulo primes in arithmetic progressions*, 2022, arXiv:2206.00872.
33. Neal Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165. MR 917870
34. S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292. MR 427273

35. Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556
36. Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, vol. Vol. 504, Springer-Verlag, Berlin-New York, 1976, Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. MR 568299
37. Sung Min Lee, *On the average congruence class bias for cyclicity and divisibility of the groups of* $\mathbb{F}_p$*-points of elliptic curves*, 2023, arXiv:2308.14681.
38. Sung Min Lee, Jacob Mayle, and Tian Wang, *Github repository associated with "Opposing average congruence class biases in the cyclicity and Koblitz conjectures for elliptic curves"*, https://github.com/maylejacobj/CyclicityKoblitzAPs, 2024.
39. Pedro Lemos, *Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 137–146. MR 3885140
40. The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, 2024, [Online; accessed 24 August 2024].
41. D. W. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), no. 3, 247–254. MR 1209248
42. Jacob Mayle and Rakvi, *Serre curves relative to obstructions modulo 2*, LuCaNT: LMFDB, computation, and number theory, Contemp. Math., vol. 796, Amer. Math. Soc., [Providence], RI, 2024, pp. 103–128. MR 4732685
43. Barry Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230
44. Franz Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. Reine Angew. Math. **78** (1874), 46–62. MR 1579612
45. S. Ali Miri and V. Kumar Murty, *An application of sieve methods to elliptic curves*, Progress in cryptology—INDOCRYPT 2001 (Chennai), Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001, pp. 91–98. MR 1934487
46. Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007. MR 2378655
47. M. Ram Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), no. 2, 147–168. MR 698163
48. Erkay Savaş, Thomas A. Schmidt, and Çetin K. Koç, *Generating elliptic curves of prime order*, Cryptographic hardware and embedded systems—CHES 2001 (Paris), Lecture Notes in Comput. Sci., vol. 2162, Springer, Berlin, 2001, pp. 142–158. MR 1945401
49. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR 387283
50. ——, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559
51. ——, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. MR 1484415
52. ——, *Oeuvres/Collected papers. III. 1972–1984*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2013, Reprint of the 2003 edition [of the 1986 original MR0926691]. MR 3223094
53. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094
54. Jörn Steuding and Annegret Weng, *On the number of prime divisors of the order of elliptic curves modulo p*, Acta Arith. **117** (2005), no. 4, 341–352. MR 2140162

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press

55. Peter Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 161–176. MR 1846457
56. Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), Paper No. e4, 79. MR 3482279
57. S. G. Vlăduţ, *Cyclicity statistics for elliptic curves over finite fields*, Finite Fields Appl. **5** (1999), no. 1, 13–25. MR 1667099
58. Daqing Wan and Ping Xi, *Lang–trotter conjecture for cm elliptic curves*, 2024, arXiv:2109.14256.
59. Peng-Jie Wong, *Cyclicity and exponents of CM elliptic curves modulo p in short intervals*, Trans. Amer. Math. Soc. **373** (2020), no. 12, 8725–8749. MR 4177274
60. ———, *Cyclicity and Exponent of Elliptic Curves Modulo p in Arithmetic Progressions*, Q. J. Math. **75** (2024), no. 2, 757–777. MR 4765791
61. David Zywina, GitHub repository related to *explicit open images for elliptic curves over $\mathbb{Q}$*, https://github.com/davidzywina/OpenImage.
62. ———, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769. MR 2805578
63. ———, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, 2015, arXiv:1508.07660.

Sung Min Lee, College of Arts and Sciences, Dakota State University, Madison, SD, USA
Email address: john.lee1@dsu.edu

Jacob Mayle, Department of Mathematics, Wake Forest University, Winston-Salem, NC, USA
Email address: maylej@wfu.edu

Tian Wang, Department of Mathematics & Statistics, Concordia University, Montreal, Quebec, Canada
Email address: tian.wang@concordia.ca

https://doi.org/10.4153/S0008414X25101156 Published online by Cambridge University Press