A REFINEMENT OF KOBLITZ'S CONJECTURE

DAVID ZYWINA

Abstract. Let E be an elliptic curve over the rationals. In 1988, Koblitz conjectured an asymptotic for the number of primes p for which the cardinality of the group of $\mathbb{F}_p$-points of E is prime. However, the constant occurring in his asymptotic does not take into account that the distributions of the $|E(\mathbb{F}_p)|$ need not be independent modulo distinct primes. We shall describe a corrected constant. We also take the opportunity to extend the scope of the original conjecture to ask how often $|E(\mathbb{F}_p)|/t$ is an integer and prime for a fixed positive integer t, and to consider elliptic curves over arbitrary number fields. Several worked out examples are provided to supply numerical evidence for the new conjecture.

1. Introduction

Motivated by applications to elliptic curve cryptography and the heuristic methods of Hardy and Littlewood [HL23], N. Koblitz made the following conjecture:

Conjecture 1.1 ([Kob88, Conjecture A])**.** *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ with conductor N_E. Assume that E is not $\mathbb{Q}$-isogenous to a curve with nontrivial $\mathbb{Q}$-torsion. Then*

$$|\{p \le x \text{ prime} : p \nmid N_E,\ |E(\mathbb{F}_p)| \text{ is prime}\}| \sim C_E \frac{x}{(\log x)^2}$$

as $x \to \infty$, where C_E is an explicit positive constant.

However, the description of the constant C_E in [Kob88] is not always correct (and more seriously, our corrected version of the constant is not necessarily positive). The additional phenomena that needs to be taken into account is that the divisibility conditions modulo distinct primes, unlike the more classical cases considered by Hardy and Littlewood, need not be independent. Lang and Trotter have successfully dealt with this non-independence in their conjectures [LT76]. A similar modification was required for the original constant of Artin's conjecture; see [Ste03] for a nice historical overview.

1.1. **An example.** As an illustration, consider the following example kindly provided by N. Jones. Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 = x^3 + 9x + 18$; this curve has conductor $2^4 3^4$, and is not isogenous over $\mathbb{Q}$ to an elliptic curve with non-trivial $\mathbb{Q}$-torsion. Conjecture 1.1 predicts that $|E(\mathbb{F}_p)|$ is prime for infinitely many primes p; however for $p > 5$, $|E(\mathbb{F}_p)|$ is always composite!

For a positive integer m, let ϑ_m be the density of the set of primes p for which $|E(\mathbb{F}_p)|$ is divisible by m; intuitively, we may think of this as the probability that m divides $|E(\mathbb{F}_p)|$ for a "random" p. We can compute these ϑ_m by applying the Chebotarev density theorem to the extensions $\mathbb{Q}(E[m])/\mathbb{Q}$ where $\mathbb{Q}(E[m])$ is the extension of $\mathbb{Q}$ generated by the coordinates of the m-torsion points of E. For our elliptic curve, we have $\vartheta_2 = 2/3$ and $\vartheta_3 = 3/4$. It is thus natural to expect that $\vartheta_6 = \vartheta_2\vartheta_3 = 1/2$ (i.e., that the congruences modulo 2 and 3 are *independent* of each other); however, one actually has $\vartheta_6 = 5/12$. The inclusion-exclusion principle then tells us that the "probability" that $|E(\mathbb{F}_p)|$ is relatively prime to 6 is $1 - \vartheta_2 - \vartheta_3 + \vartheta_6 = 0$.

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11N05.

Key words and phrases. Elliptic curves modulo p, Galois representations, Koblitz conjecture.

This lack of independence is explained by the observation that $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[3])$ are not linearly disjoint over $\mathbb{Q}$. They both contain $\mathbb{Q}(i)$:

- The point $(x,y)=(-3,6i)$ in $E(\mathbb{Q}(i))$ has order 3, so $\mathbb{Q}(E[3])$ contains $\mathbb{Q}(i)$. If p splits in $\mathbb{Q}(i)$ (i.e., $p\equiv 1 \bmod 4$), then $(-3,6i)$ will give a point in $E(\mathbb{F}_p)$ of order 3; hence $|E(\mathbb{F}_p)|\equiv 0 \bmod 3$.
- The points in $E[2]-\{0\}$ are of the form $(x,0)$, where x is a root of $x^3+9x+18$. The discriminant of this cubic is $\Delta=-2^4 3^6$, so $\mathbb{Q}(E[2])$ contains $\mathbb{Q}(\sqrt{\Delta})=\mathbb{Q}(i)$. If $p>3$ is inert in $\mathbb{Q}(i)$ (i.e., $p\equiv 3 \bmod 4$), then Δ is not a square modulo p and one checks that $E(\mathbb{F}_p)$ has exactly one point of order 2; hence $|E(\mathbb{F}_p)|\equiv 0 \bmod 2$.

For $p\geq 5$, we deduce that $|E(\mathbb{F}_p)|$ is divisible by 2 or 3. Therefore $|E(\mathbb{F}_p)|$ is prime only in the case where it equals 2 or 3 (which happens only for $p=5$ where $|E(\mathbb{F}_5)|=3$).

It is now natural to ask if $|E(\mathbb{F}_p)|/3$ (or $|E(\mathbb{F}_p)|/2$) is prime for infinitely many p? Our refinement/generalization of Koblitz's conjecture predicts that the answer is *yes*, and we will supply numerical evidence in §6.

1.2. **The refined Koblitz conjecture.** Before stating our conjecture, we set some notation that will hold throughout the paper. For a number field K, denote the ring of integers of K by $\mathcal{O}_K$, and let Σ_K be the set of non-zero prime ideals of $\mathcal{O}_K$. For each prime $\mathfrak{p}\in\Sigma_K$, we have a residue field $\mathbb{F}_{\mathfrak{p}}=\mathcal{O}_K/\mathfrak{p}$ whose cardinality we denote by $N(\mathfrak{p})$. Let $\Sigma_K(x)$ be the (finite) set of primes $\mathfrak{p}\in\Sigma_K$ with $N(\mathfrak{p})\leq x$.

For an elliptic curve E over K, let S_E be the set of $\mathfrak{p}\in\Sigma_K$ for which E has bad reduction. For $\mathfrak{p}\in\Sigma_K-S_E$, let $E(\mathbb{F}_{\mathfrak{p}})$ be the corresponding group of $\mathbb{F}_{\mathfrak{p}}$-points (more precisely, the $\mathbb{F}_{\mathfrak{p}}$-points of the Néron model $\mathbb{E}/\mathcal{O}_K$ over E/K). For a field extension L/K, we will denote by E_L the corresponding base extension of E.

Conjecture 1.2. *Let E be an elliptic curve defined over a number field K, and let t be a positive integer. Then there is an explicit constant $\mathcal{C}_{E,t}\geq 0$ such that*

$$P_{E,t}(x):=|\{\mathfrak{p}\in\Sigma_K(x)-S_E : |E(\mathbb{F}_{\mathfrak{p}})|/t \text{ is a prime}\}|\sim \mathcal{C}_{E,t}\frac{x}{(\log x)^2}$$

as $x\to\infty$.

If $\mathcal{C}_{E,t}>0$, then the above conjecture implies in particular that there are infinitely many $\mathfrak{p}$ for which $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is an integer and is prime. If $\mathcal{C}_{E,t}=0$, then we *define* the above asymptotic to mean that $P_{E,t}(x)$ is bounded as a function of x (equivalently, that $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is a prime number for only finitely many $\mathfrak{p}\in\Sigma_K-S_E$). Our constant $\mathcal{C}_{E,t}$ will be described in §2.

The expression $\mathcal{C}_{E,t}\,x/(\log x)^2$ in Conjecture 1.2 has been used for its simplicity. The heuristics in §2.4 suggest that the expression

$$\mathcal{C}_{E,t}\int_{t+1}^{x}\frac{1}{\log(u+1)-\log t}\frac{du}{\log u} \tag{1.1}$$

will be a better approximation of $P_{E,t}(x)$, and this is what we will use to test our conjecture. We will not study the error term of our conjecture (i.e., the difference between $P_{E,t}(x)$ and the expression (1.1)), though we remark that our data suggests that it could be $O(x^{\theta})$ for any $\theta>1/2$.

1.3. **Overview.** In §2, we describe the constant $\mathcal{C}_{E,t}$ occurring in Conjecture 1.2. We shall express the constant in terms of the Galois representations arising from the torsion points of our elliptic curve. To have a computationally useful version, we treat separately the CM and non-CM cases. In §2.4 we give a brief heuristic for our conjecture. In §3, we describe the common factor t_E of all the $|E(\mathbb{F}_{\mathfrak{p}})|$. It is of course necessary to have t_E divide t for Conjecture 1.2 to be interesting. In §4, we calculate $\mathcal{C}_{E,1}$ assuming that $E/\mathbb{Q}$ is a Serre curve.

In §5–8, we consider four specific elliptic curves. We describe the Galois action on their torsion points, compute constants $\mathcal{C}_{E,t}$ for interesting t, and then supply numerical evidence for Conjecture 1.2.

In the final section, we describe some of the partial progress that has been made on Koblitz's conjecture in the last decade. Some of the recent study on the conjecture requires our corrected constant.

Acknowledgments. Thanks to Nathan Jones for comments and providing the example in §1.1. Special thanks to Chantal David and Bjorn Poonen. The experimental evidence for our conjecture was computed using `PARI/GP` [PG08]. We also used `Magma` [BCP97] to check some group theoretic claims and `Maple` to approximate integrals. This research was supported by an NSERC postgraduate scholarship.

2. The constant

Throughout this section, we will fix an elliptic curve E defined over a number field K and a positive integer t. The letter ℓ will always denote a rational prime.

2.1. **Description of the constant.** To understand the divisibility of the numbers $|E(\mathbb{F}_\mathfrak{p})|$, it is useful to recast everything in term of Galois representations. For each positive integer m, let $E[m]$ be the group of m-torsion in $E(\overline{K})$, where $\overline{K}$ is a fixed algebraic closure of K. The natural Galois action induces a representation

$$\rho_m\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m])$$

whose image we will denote by $G(m)$. Let $K(E[m])$ be the fixed field of $\ker(\rho_m)$ in $\overline{K}$; so ρ_m induces an isomorphism $\mathrm{Gal}(K(E[m])/K) \xrightarrow{\sim} G(m)$. If $\mathfrak{p} \in \Sigma_K - S_E$ does not divide m, then ρ_m is unramified at $\mathfrak{p}$ (i.e., $\mathfrak{p}$ is unramified in $K(E[m])$) and $\rho_m(\mathrm{Frob}_\mathfrak{p})$ will denote the corresponding Frobenius conjugacy class in $G(m)$. Note that the notation does not mention the curve E which will always be clear from context.

The group $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2, and a choice of $\mathbb{Z}/m\mathbb{Z}$-basis for $E[m]$ determines an isomorphism $\mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ that is unique up to an inner automorphism of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For a prime ideal $\mathfrak{p} \in \Sigma_K - S_E$ with $\mathfrak{p} \nmid m$, we have a congruence

$$|E(\mathbb{F}_\mathfrak{p})| \equiv \det(I - \rho_m(\mathrm{Frob}_\mathfrak{p})) \mod m.$$

For $m \geq 1$, define the set

$$\Psi_t(m) = \big\{A \in \mathrm{Aut}(E[m]) : \det(I - A) \in t \cdot (\mathbb{Z}/m\mathbb{Z})^\times\big\}. \tag{2.1}$$

Thus for a prime $\mathfrak{p} \in \Sigma_K - S_E$ with $\mathfrak{p} \nmid m$, we find that $|E(\mathbb{F}_\mathfrak{p})|/t$ is invertible modulo $\frac{m}{\gcd(m,t)}$ if and only if $\rho_m(\mathrm{Frob}_\mathfrak{p}) \subseteq G(m) \cap \Psi_t(m)$. In particular, $|E(\mathbb{F}_\mathfrak{p})|/t$ is an integer if and only if $\rho_t(\mathrm{Frob}_\mathfrak{p}) \subseteq G(t) \cap \Psi_t(t)$. Define the number

$$\delta_{E,t}(m) := \frac{|G(m) \cap \Psi_t(m)|}{|G(m)|}$$

By the Chebotarev density theorem, $\delta_{E,t}(m)$ is the natural density of the set of $\mathfrak{p} \in \Sigma_K - S_E$ for which $|E(\mathbb{F}_\mathfrak{p})|/t$ is invertible modulo $m/\gcd(m,t)$. The connection with Conjecture 1.2 is that if $|E(\mathbb{F}_\mathfrak{p})|/t$ is an integer and prime, then it is invertible modulo all positive integers $m < |E(\mathbb{F}_\mathfrak{p})|/t$.

Definition 2.1. With notation as above, define

$$\mathcal{C}_{E,t} := \lim_{m \to +\infty} \frac{\delta_{E,t}(m)}{\prod_{\ell \mid m}(1 - 1/\ell)}$$

where the limit runs over all positive integers ordered by divisibility. This is our predicted constant for Conjecture 1.2.

If $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is an integer, then to check that it is invertible modulo m we need only verify that it is invertible modulo $\prod_{\ell\mid m}\ell$. So to check if $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is an integer that is relatively prime to m, we need only consider the value of $|E(\mathbb{F}_{\mathfrak{p}})|$ modulo $t\prod_{\ell\mid m}\ell$. For each m, we have $\delta_{E,t}(tm)=\delta_{E,t}(t\prod_{\ell\mid m}\ell)$, so an equivalent definition of our constant is

$$\mathcal{C}_{E,t}=\lim_{Q\to+\infty}\frac{\delta_{E,t}\big(t\prod_{\ell\le Q}\ell\big)}{\prod_{\ell\le Q}(1-1/\ell)}.$$

This expression for $\mathcal{C}_{E,t}$ is often preferable since it requires knowledge only of the groups $G(tm)$ for m *squarefree*.

We shall see in §2.2 and §2.3 that the limit of Definition 2.1 does indeed converge, and hence $\mathcal{C}_{E,t}$ is well-defined. It will also be apparent that $\mathcal{C}_{E,t}=0$ if and only if $\delta_{E,t}(m)=0$ for some m, which gives the following qualitative version of our conjecture:

Conjecture 2.2. *Let E be an elliptic curve over a number field K and let t be a positive integer. There are infinitely many $\mathfrak{p}\in\Sigma_K$ for which $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is a prime integer if and only if there are no "congruence obstructions", i.e., for every $m\ge 1$ there exists a prime $\mathfrak{p}\in\Sigma_K-S_E$ with $\mathfrak{p}\nmid m$ such that $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is invertible modulo m.*

2.2. **The constant for non-CM elliptic curves.** The following renowned theorem of Serre, gives the general structure of the groups $G(m)$.

Theorem 2.3 (Serre [Ser72])**.** *Let E/K be an elliptic curve without complex multiplication. There is a positive integer M such that if m and n are positive integers with n relatively prime to Mm, then*

$$G(mn)=G(m)\times\mathrm{Aut}(E[n]).$$

Proposition 2.4. *Let E/K be an elliptic curve without complex multiplication and let t be a positive integer. Let M be a positive integer such that*

$$G\Big(t\prod_{\ell\mid tm}\ell\Big)=G\Big(t\prod_{\ell\mid t\gcd(M,m)}\ell\Big)\times\prod_{\ell\mid m,\,\ell\nmid tM}\mathrm{Aut}(E[\ell])$$

for all squarefree m (in particular, one can take M as in Theorem 2.3). Then

$$\mathcal{C}_{E,t}=\frac{\delta_{E,t}\big(t\prod_{\ell\mid tM}\ell\big)}{\prod_{\ell\mid tM}(1-1/\ell)}\prod_{\ell\nmid tM}\Big(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big).$$

Proof. Let Q be a real number greater than tM. From the assumption of the proposition, we have

$$G(t\textstyle\prod_{\ell\le Q}\ell)=G(t\prod_{\ell\mid tM}\ell)\times\prod_{\ell\nmid tM,\ell\le Q}\mathrm{Aut}(E[\ell]).$$

Therefore

$$\delta_{E,t}(t\textstyle\prod_{\ell\le Q}\ell)=\delta_{E,t}(t\prod_{\ell\mid tM}\ell)\prod_{\ell\nmid tM,\ell\le Q}\delta_{E,t}(\ell),$$

and hence

$$\frac{\delta_{E,t}\big(t\prod_{\ell\le Q}\ell\big)}{\prod_{\ell\le Q}(1-1/\ell)}=\frac{\delta_{E,t}\big(t\prod_{\ell\mid tM}\ell\big)}{\prod_{\ell\mid tM}(1-1/\ell)}\prod_{\ell\nmid tM,\ell\le Q}\frac{\delta_{E,t}(\ell)}{1-1/\ell}.\tag{2.2}$$

For any $\ell \nmid tM$, we have

$$\begin{aligned}\delta_{E,t}(\ell) &= 1 - \frac{|\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : \det(I-A) = 0\}|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|} \\ &= 1 - \sum_{a \in \mathbb{F}_\ell^\times} \frac{|\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : \text{the eigenvalues of } A \text{ are 1 and } a\}|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|}\end{aligned}$$

and by Lemma 2.5 below,

$$\frac{\delta_{E,t}(\ell)}{1-1/\ell} = \frac{1}{1-1/\ell}\Big(1 - \frac{(\ell-2)(\ell^2+\ell)+1\cdot\ell^2}{\ell(\ell-1)^2(\ell+1)}\Big).$$

A easy calculation then shows that $\dfrac{\delta_{E,t}(\ell)}{1-1/\ell} = 1 - \dfrac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}$. Substituting this into (2.2), gives

$$\frac{\delta_{E,t}\big(t\prod_{\ell|tM}\ell\big)}{\prod_{\ell|tM}(1-1/\ell)} \prod_{\ell\nmid tM, \ell\le Q}\Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big).$$

Letting $Q \to +\infty$, we deduce that the limit defining $\mathcal{C}_{E,t}$ is convergent and that it has the stated value. □

Lemma 2.5. *For $a \in \mathbb{F}_\ell^\times$,*

$$|\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : A \text{ has eigenvalues } 1 \text{ and } a\}| = \begin{cases} \ell^2+\ell & \text{if } a \neq 1, \\ \ell^2 & \text{if } a = 1. \end{cases}$$

Proof. This follows easily from Table 12.4 in [Lan02, XVIII], which describes the conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_\ell)$. □

Remark 2.6. For later reference, we record the following numerical approximation:

$$\mathfrak{C} := \prod_\ell \Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big) \approx 0.505166168239435774. \tag{2.3}$$

So to estimate $\mathcal{C}_{E,t}$, it suffices to find M and then compute $\delta_{E,t}(t\prod_{\ell|tM}\ell)$.

2.3. **The constant for CM elliptic curves.** Let E be an elliptic curve over a number field K with complex multiplication, and let $R = \mathrm{End}(E_{\overline{K}})$. The ring R is an order in the imaginary quadratic field $F := R \otimes_{\mathbb{Z}} \mathbb{Q}$.

For each positive integer m, we have a natural action of R/mR on $E[m]$. The group $E[m]$ is a free R/mR-module of rank 1, so we have a *canonical* isomorphism $\mathrm{Aut}_{R/mR}(E[m]) = (R/mR)^\times$. If all the endomorphism of E are defined over K, then the actions of R and $\mathrm{Gal}(\overline{K}/K)$ on $E[m]$ commute, and hence we may view $\rho_m(\mathrm{Gal}(\overline{K}/K))$ as a subgroup of $(R/mR)^\times$.

Proposition 2.7. *Let E be an elliptic curve over a number field K with complex multiplication. Assume that all the endomorphisms in $R = \mathrm{End}(E_{\overline{K}})$ are defined over K. There is a positive integer M such that if m and n are positive integers with n relatively prime to Mn, then*

$$G(mn) = G(m) \times (R/nR)^\times.$$

Proof. (For an overview and further references, see [Ser72, §4.5]) For a prime ℓ, define $R_\ell = R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $F_\ell = F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Let $T_\ell(E)$ be the ℓ-adic Tate module of E (i.e, the inverse limit of the groups $E[\ell^i]$ with multiplication by ℓ as transition maps). The Tate module $T_\ell(E)$ is a free R_ℓ-module of rank 1 (see the remarks at the end of §4 of [ST68]), we thus have a *canonical* isomorphism $\mathrm{Aut}_{R_\ell}(T_\ell(E)) = R_\ell^\times$. The actions of $\mathrm{Gal}(\overline{K}/K)$ and R_ℓ on $T_\ell(E)$ commute with each other since we

have assumed that all the endomorphisms of E are defined over K. Combining our representations ρ_{ℓ^i} gives a Galois representation

$$\widehat{\rho}_\ell\colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}_{R_\ell}(T_\ell(E)) = R_\ell^\times.$$

The theory of complex multiplication implies that the representation

$$\widehat{\rho} := \prod_\ell \widehat{\rho}_\ell\colon \operatorname{Gal}(\overline{K}/K) \to \prod_\ell R_\ell^\times$$

has open image, and our proposition is an immediate consequence.

We now describe the representation $\widehat{\rho}$ in further detail (this will be useful later when we actually want to compute a suitable M). Since the endomorphism in R are defined over K, the action of R on the Lie algebra of E gives a homomorphism $R \to K$. This allows us to identify F with a subfield of K. By class field theory, we may view $\widehat{\rho}_\ell$ as a continuous homomorphism $I \to R_\ell^\times \subseteq F_\ell^\times$ that is trivial on $K^\times$, where I is the group of ideles of K with its standard topology. For each prime ℓ, define $K_\ell := K \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \prod_{\mathfrak{p}|\ell} K_{\mathfrak{p}}$. For an element $a \in I$, let a_ℓ be the component of a in $K_\ell^\times$. From [ST68, §4.5 Theorems 10 & 11], there is a unique homomorphism $\varepsilon\colon I \to F^\times$ such that

$$\widehat{\rho}_\ell(a) = \varepsilon(a) N_{K_\ell/F_\ell}(a_\ell^{-1})$$

for all ℓ and $a \in I$. The homomorphism ε is continuous and $\varepsilon(x) = x$ for all $x \in K^\times$.

Since ε is continuous, there is a set $S \subseteq \Sigma_K$ such that ε is 1 on $\prod_{\mathfrak{p}\in\Sigma_K - S} \mathcal{O}_{K,\mathfrak{p}}^\times \subseteq I$; in fact, we may take $S = S_E$. Let M be a positive integer such that

- $N_{K_\ell/F_\ell}\colon (\mathcal{O}_K \otimes \mathbb{Z}_\ell)^\times \to R_\ell^\times$ is surjective for all $\ell \nmid M$.
- E has good reduction at all $\mathfrak{p} \in \Sigma_K$ for which $\mathfrak{p} \nmid M$.

Take any $b = (b_\ell) \in \prod_\ell R_\ell^\times$ with $b_\ell = 1$ for all $\ell | M$. For each ℓ, there is an $a_\ell \in (\mathcal{O}_K \otimes \mathbb{Z}_\ell)^\times \subseteq K_\ell^\times$ such that $N_{K_\ell/F_\ell}(a_\ell^{-1}) = b_\ell$. Let a be the corresponding element of I with archimedean component equal to 1. Then

$$\widehat{\rho}(a) = (\widehat{\rho}_\ell(a))_\ell = (\varepsilon(a) N_{K_\ell/F_\ell}(a_\ell^{-1}))_\ell = (N_{K_\ell/F_\ell}(a_\ell^{-1}))_\ell = (b_\ell)_\ell.$$

Since (b_ℓ) was an arbitrary element of $\prod_\ell R_\ell^\times$ with $b_\ell = 1$ for $\ell | M$, we conclude that $\widehat{\rho}(\operatorname{Gal}(\overline{K}/K)) \supseteq \{1\} \times \prod_{\ell\nmid M} R_\ell^\times$. Our M thus agrees with the one in the statement of the propostion. □

Proposition 2.8. *Let E be an elliptic curve over a number field K with complex multiplication. Assume that all the endomorphisms in $R = \operatorname{End}(E_{\overline{K}})$ are defined over K. Let χ be the Kronecker character corresponding to the imaginary quadratic extension $F = R \otimes \mathbb{Q}$ of $\mathbb{Q}$. Let M be a positive integer as in Proposition 2.7 which is also divisible by all the primes dividing the discriminant of F or the conductor of the order R. For any positive integer t, we have*

$$\mathcal{C}_{E,t} = \frac{\delta_{E,t}\big(t\prod_{\ell|tM}\ell\big)}{\prod_{\ell|tM}(1-1/\ell)} \cdot \prod_{\ell\nmid tM}\Big(1 - \chi(\ell)\frac{\ell^2-\ell-1}{(\ell-\chi(\ell))(\ell-1)^2}\Big).$$

Proof. Let Q be a real number greater than tM. By Proposition 2.7, we have

$$G(t\textstyle\prod_{\ell\le Q}\ell) = G(t\prod_{\ell|tM}\ell) \times \prod_{\ell\nmid tM,\ell\le Q}(R/\ell R)^\times.$$

Therefore

$$\delta_{E,t}\big(t\textstyle\prod_{\ell\le Q}\ell\big) = \delta_{E,t}\big(t\prod_{\ell|tM}\ell\big) \prod_{\ell\nmid tM,\ell\le Q}\delta_{E,t}(\ell),$$

and hence

$$\frac{\delta_{E,t}(t\prod_{\ell\le Q}\ell)}{\prod_{\ell\le Q}(1-1/\ell)}=\frac{\delta_{E,t}(t\prod_{\ell\mid tM}\ell)}{\prod_{\ell\mid tM}(1-1/\ell)}\prod_{\ell\nmid tM,\ell\le Q}\frac{\delta_{E,t}(\ell)}{1-1/\ell}. \tag{2.4}$$

Now take any $\ell\nmid tM$. Under the identification $\mathrm{Aut}_{R/\ell R}(E[\ell])=(R/\ell R)^\times$, for $a\in(R/\ell R)^\times$ we find that $\det(I-a)$ agrees with $N(1-a)$ where N is the norm map from $R/\ell R$ to $\mathbb{Z}/\ell\mathbb{Z}$. So $\delta_{E,t}(\ell)$ equals

$$\frac{|\{a\in(R/\ell R)^\times: N(1-a)\in(\mathbb{Z}/\ell\mathbb{Z})^\times\}|}{|(R/\ell R)^\times|}=\frac{|\{a\in(R/\ell R)^\times: 1-a\in(R/\ell R)^\times\}|}{|(R/\ell R)^\times|}.$$

From our assumptions on M, ℓ is unramified in F and $R/\ell R=\mathcal{O}_F/\ell\mathcal{O}_F$. One can then verify that $|(\mathcal{O}_F/\ell\mathcal{O}_F)^\times|=(\ell-1)(\ell-\chi(\ell))$, and

$$|\{a\in(\mathcal{O}_F/\ell\mathcal{O}_F)^\times: 1-a\in(\mathcal{O}_F/\ell\mathcal{O}_F)^\times\}|=\ell^2-\big(\chi(\ell)(\ell-2)+(\ell-1)\big).$$

An easy calculation then shows $\frac{\delta_{E,t}(\ell)}{1-1/\ell}=1-\chi(\ell)\frac{\ell^2-\ell-1}{(\ell-\chi(\ell))(\ell-1)^2}$. Substituting this into (2.4), gives

$$\frac{\delta_{E,t}(t\prod_{\ell\mid tM}\ell)}{\prod_{\ell\mid tM}(1-1/\ell)}\prod_{\ell\nmid tM,\ell\le Q}\Big(1-\chi(\ell)\frac{\ell^2-\ell-1}{(\ell-\chi(\ell))(\ell-1)^2}\Big).$$

Letting $Q\to+\infty$, we deduce that the limit defining $\mathcal{C}_{E,t}$ is (conditionally) convergent and has the stated value (the convergence can be seen by a comparison with the Euler product of the L-function $L(s,\chi)$ at $s=1$ which converges to a non-zero number). □

2.3.1. *Case where not all the endomorphisms are defined over base field.* Let us now consider the case where not all the endomorphisms of E over K. Choose an embedding $F\subseteq\overline{K}$. The endomorphisms of E are defined over KF, and KF is a quadratic extension of K. We break up the conjecture into two cases.

Primes that split in KF. Let $\mathfrak{p}\in\Sigma_K-S_E$ be a prime ideal that splits in KF, i.e., there are two distinct primes $\mathfrak{P}_1,\mathfrak{P}_2\in\Sigma_{KF}$ lying over $\mathfrak{p}$. The maps $E(\mathbb{F}_\mathfrak{p})\to E(\mathbb{F}_{\mathfrak{P}_i})$ are group isomorphisms. So we have

$$\begin{aligned}&|\{\mathfrak{p}\in\Sigma_K(x)-S_E:\mathfrak{p}\text{ splits in }KF,\ |E(\mathbb{F}_\mathfrak{p})|/t\text{ is prime}\}|\\ =&\frac{1}{2}|\{\mathfrak{P}\in\Sigma_{KF}(x)-S_{E_{KF}}:|E(\mathbb{F}_\mathfrak{P})|/t\text{ is prime}\}|+O(\sqrt{x})=\frac{1}{2}P_{E_{KF},t}(x)+O(\sqrt{x})\end{aligned}$$

Therefore Conjecture 1.2 implies that

$$|\{\mathfrak{p}\in\Sigma_K(x)-S_E:\mathfrak{p}\text{ splits in }KF,\ |E(\mathbb{F}_\mathfrak{p})|/t\text{ is prime}\}|\sim\frac{\mathcal{C}_{E_{KF},t}}{2}\frac{x}{(\log x)^2} \tag{2.5}$$

as $x\to\infty$, and the constant $\mathcal{C}_{E_{KF},t}$ can be computed as in Proposition 2.8 (if $\mathcal{C}_{E_{KF},t}=0$, then there is a congruence obstruction and the left hand side of (2.5) is indeed bounded).

Primes that are inert in KF. Let $\mathfrak{p}\in\Sigma_K-S_E$ be a prime that is inert in KF, i.e., $\mathfrak{p}\mathcal{O}_{KF}$ is a prime ideal of $\mathcal{O}_{KF}$. For these primes we always have $|E(\mathbb{F}_\mathfrak{p})|=N(\mathfrak{p})+1$, so

$$\begin{aligned}&|\{\mathfrak{p}\in\Sigma_K(x)-S_E:\mathfrak{p}\text{ is inert in }KF,\ |E(\mathbb{F}_\mathfrak{p})|/t\text{ is prime}\}|\\ =&|\{\mathfrak{p}\in\Sigma_K(x):\mathfrak{p}\text{ is inert in }KF,\ (N(\mathfrak{p})+1)/t\text{ is prime}\}|+O(1);\end{aligned}$$

Our conjecture combined with the split case above imply that

$$|\{\mathfrak{p}\in\Sigma_K(x):\mathfrak{p}\text{ is inert in }KF,\ (N(\mathfrak{p})+1)/t\text{ is prime}\}|\sim C\frac{x}{(\log x)^2} \tag{2.6}$$

as $x \to \infty$ where $C = \mathcal{C}_{E,t} - \mathcal{C}_{E_{KF},t}/2$. We can also give the more intrinsic definition

$$C = \lim_{Q \to +\infty} \frac{\delta_t'(t \prod_{\ell \le Q} \ell)}{\prod_{\ell \le Q}(1-1/\ell)}$$

where $\delta_t'(m)$ is the density of the set of $\mathfrak{p} \in \Sigma_K$ for which $\mathfrak{p}$ is inert in KF and $(N(\mathfrak{p})+1)/t$ is invertible modulo $m/\gcd(t,m)$. The asymptotics of (2.6) depends only on K and KF, and not the specific curve E. We will not consider this case any further.

2.4. **Heuristics.** We will now give a crude heuristic for Conjecture 1.2 (one could also give a more systematic heuristic as in [LT76]).

The prime number theorem states the number of rational primes less than x is asymptotic to $x/\log x$ as $x \to \infty$. Intuitively, this means that a random natural number n is prime with probability $1/\log n$. This probabilistic model, called *Cramér's model*, is useful for making conjectures. Of course the event "n is prime" is deterministic, i.e., has probability 0 or 1.

If the primality of the integers in the sequence $\{|E(\mathbb{F}_{\mathfrak{p}})|/t\}_{\mathfrak{p} \in \Sigma_K - S_E}$ were assumed to behave like random integers, then the likelihood that $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is prime would be

$$\frac{1}{\log\left(|E(\mathbb{F}_{\mathfrak{p}})|/t\right)} \approx \frac{1}{\log(N(\mathfrak{p})+1) - \log t}$$

(the last line is reasonable because of Hasse's bound, $\Big||E(\mathbb{F}_{\mathfrak{p}})| - (N(\mathfrak{p})+1)\Big| \le 2\sqrt{N(\mathfrak{p})}$).

However, the $|E(\mathbb{F}_{\mathfrak{p}})|/t$ are certainly not random integers with respect to congruences (in particular, they might not all be integers!). To salvage our model, we need to take into account these congruences. Fix a positive integer m which we will assume is divisible by $t\prod_{\ell \mid t}\ell$. For all but finitely many $\mathfrak{p}$, if $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is prime then it is invertible modulo m. The density of $\mathfrak{p} \in \Sigma_K - S_E$ for which $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is an integer and invertible modulo m is $\delta_{E,t}(m)$, while the density of the set of natural numbers that are invertible modulo m is $\prod_{\ell \mid m}(1-1/\ell)$. By taking into account the congruences modulo m, we expect

$$\frac{\delta_{E,t}(m)}{\prod_{\ell \mid m}(1-1/\ell)} \cdot \frac{1}{\log(N(\mathfrak{p})+1) - \log t}$$

to be a better approximation for the probability that $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is prime for a "random" $\mathfrak{p} \in \Sigma_K - S_E$. Taking into account all possible congruences, our heuristics suggest that $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is prime for a "random" $\mathfrak{p} \in \Sigma_K - S_E$ with probability

$$\mathcal{C}_{E,t} \cdot \frac{1}{\log(N(\mathfrak{p})+1) - \log t}$$

where

$$\mathcal{C}_{E,t} = \lim_{Q \to +\infty} \frac{\delta_{E,t}(t \prod_{\ell \le Q} \ell)}{\prod_{\ell \le Q}(1-1/\ell)}.$$

We have already seen that this limit converges.

Using our heuristic model, the expected number of $\mathfrak{p} \in \Sigma_K(x) - S_E$ such that $|E(\mathbb{F}_{\mathfrak{p}})|/t$ is prime, should then be well approximated by

$$\sum_{\substack{\mathfrak{p} \in \Sigma_K(x) - S_E \\ N(\mathfrak{p}) \ge t}} \frac{\mathcal{C}_{E,t}}{\log(N(\mathfrak{p})+1) - \log t} \sim \mathcal{C}_{E,t} \int_{t+1}^{x} \frac{1}{\log(u+1) - \log t} \frac{du}{\log u}.$$

The restriction of $\mathfrak{p}$ in the above sum to those with $N(\mathfrak{p}) \ge t$ is included simply to ensure that each term of the sum is well-defined and positive. The integral expression follows from the prime

number theorem for the field K, and is asymptotic to $x/(\log x)^2$. We can now conjecture that

$$P_{E,t}(x) \sim \mathcal{C}_{E,t} \int_{t+1}^{x} \frac{1}{\log(u+1) - \log t} \frac{du}{\log u}$$

as $x \to \infty$.

Remark 2.9. In the setting of Conjecture 1.1 with $t = 1$, Koblitz assumed that the divisibility conditions were independent and hence his constant was $\prod_{\ell} \frac{\delta_{E,1}(\ell)}{1 - 1/\ell}$.

3. Common factor of the $|E(\mathbb{F}_{\mathfrak{p}})|$

Let E be an elliptic curve over a number field K. There may be an integer greater than one which divides almost all of the $|E(\mathbb{F}_{\mathfrak{p}})|$, which is an obvious obstruction to the primality of the values $|E(\mathbb{F}_{\mathfrak{p}})|$. Thus it will be necessary to divide by this common factor before addressing any questions of primality. In this section we describe the common factor and explain how it arises from the global arithmetic of E.

The following well-known result says that the K-rational torsion of E injects into $E(\mathbb{F}_{\mathfrak{p}})$ for almost all $\mathfrak{p}$ (for a proof see [Kat81, Appendix]). Define the finite set

$$\widetilde{S}_E := S_E \cup \{\mathfrak{p} \in \Sigma_K : e_{\mathfrak{p}} \geq p - 1 \text{ where } \mathfrak{p} \text{ lies over the prime } p\}$$

where $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ over p.

Lemma 3.1. *For all $\mathfrak{p} \in \Sigma_K - \widetilde{S}_E$, reduction modulo $\mathfrak{p}$ induces an injective group homomorphism*

$$E(K)_{\text{tors}} \hookrightarrow E(\mathbb{F}_{\mathfrak{p}}).$$

In particular, $|E(K)_{\text{tors}}|$ divides $|E(\mathbb{F}_{\mathfrak{p}})|$ for all $\mathfrak{p} \in \Sigma_K - \widetilde{S}_E$.

The integer $|E(\mathbb{F}_{\mathfrak{p}})|$ is a K-isogeny invariant of the elliptic curve E. So for all $\mathfrak{p} \in \Sigma_K - \widetilde{S}_E$, we find that $|E(\mathbb{F}_{\mathfrak{p}})|$ is divisible by

$$t_E := \text{lcm}_{E'} |E'(K)_{\text{tors}}|, \tag{3.1}$$

where E' varies over all elliptic curves that are isogenous to E over K. One can also show that

$$t_E = \max_{E'} |E'(K)_{\text{tors}}|. \tag{3.2}$$

From our discussion above, t_E divides $|E(\mathbb{F}_{\mathfrak{p}})|$ for almost all $\mathfrak{p} \in \Sigma_K$ (in particular, Conjecture 1.2 is only interesting when t_E divides t). The following theorem of Katz shows that t_E is the largest integer with this property.

Theorem 3.2 (Katz [Kat81, Theorem 2(bis)])**.** *Let Σ be a subset of $\Sigma_K - \widetilde{S}_E$ with density 1. Then*

$$t_E = \gcd_{\mathfrak{p} \in \Sigma} |E(\mathbb{F}_{\mathfrak{p}})|.$$

There is an elliptic curve E' which is K-isogenous to E satisfying $t_E = |E'(K)_{\text{tors}}|$. Thus our conjecture with $t = t_E$ predicts how frequently the groups $E'(\mathbb{F}_{\mathfrak{p}})/E'(K)_{\text{tors}}$ have prime cardinality as $\mathfrak{p}$ varies, this was mentioned by Koblitz in the final remarks of [Kob88] as a natural way to generalize his paper. Koblitz's original conjecture was restricted to those elliptic curves over $\mathbb{Q}$ with $t_E = 1$.

Remark 3.3. Using the characterization of t_E from Theorem 3.2, we can also express t_E in terms of our Galois representations. It is the largest integer t such that $\det(I - \rho_t(g)) \equiv 0 \bmod t$ for all $g \in G(t)$.

4. Serre Curves

4.1. **The constant $\mathcal{C}_{E,1}$ for Serre curves.** Throughout this section, we assume that E is a elliptic curve over $\mathbb{Q}$ without complex multiplication. For each $m \geq 1$, we have defined a Galois representation $\rho_m\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[m])$. Combining them all together, we obtain a single representation

$$\widehat{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

A theorem of Serre [Ser72] says that that the index of $G(m)$ in $\mathrm{Aut}(E[m])$ is bounded by a constant that depends only on E; equivalently, $\widehat{\rho}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Serre has also shown that the map $\widehat{\rho}$ is *never* surjective [Ser72, Proposition 22]. He proves this by showing that $\widehat{\rho}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ lies in a specific index 2 subgroup H_E of $\mathrm{Aut}(E_{\mathrm{tors}})$ (see §4.2 for details). Following Lang and Trotter, we make the following definition.

Definition 4.1. An elliptic curve E over $\mathbb{Q}$ is a *Serre curve* if $\widehat{\rho}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is an index 2 subgroup of $\mathrm{Aut}(E_{\mathrm{tors}})$.

Serre curves are thus elliptic curves over $\mathbb{Q}$ whose Galois action on their torsion points are as "large as possible". For examples of Serre curves, see §5 and [Ser72, §5.5]. Jones has shown that "most" elliptic curves over $\mathbb{Q}$ are Serre curves [Jon10]. Thus Serre curves are prevalent and we have a complete understanding of the groups $G(m)$ (see below), so they are worthy of special consideration. We are particularly interested in Conjecture 1.2 with $t = 1$.

Proposition 4.2. *Let $E/\mathbb{Q}$ be a Serre curve. Let D be the discriminant of the number field $\mathbb{Q}(\sqrt{\Delta})$ where Δ is the discriminant of any Weierstrass model of E over $\mathbb{Q}$. Then*

$$\mathcal{C}_{E,1} = \begin{cases} \mathfrak{c}\Big(1 + \displaystyle\prod_{\ell \mid D} \frac{1}{\ell^3 - 2\ell^2 - \ell + 3}\Big) & \text{if } D \equiv 1 \mod 4, \\ \mathfrak{c} & \text{if } D \equiv 0 \mod 4 \end{cases}$$

where $\mathfrak{c} = \prod_{\ell}\Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big)$.

The proof of Proposition 4.2 will be given in §4.3.

Remark 4.3.

(i) In the paper [Jon09], Jones studies the constant $\mathcal{C}_{E,1}$ as $E/\mathbb{Q}$ varies over certain families of elliptic curves. The "main term" of his results comes from the contribution of the Serre curves.

(ii) There are elliptic curves defined over number fields $K \neq \mathbb{Q}$ for which $\widehat{\rho}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{Aut}(E_{\mathrm{tors}})$. The first example was give by A. Greicius [Gre07] (also see [Zyw10]).

4.2. **The group H_E.** We shall now describe the desired group H_E (see [Ser72, p. 311] for further details). Let D be the discriminant of the number field $L := \mathbb{Q}(\sqrt{\Delta})$ where Δ is the discriminant of any Weierstrass model of E over $\mathbb{Q}$ (note that L is independent of the choice of model). Define the character

$$\chi_D\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \{\pm 1\},$$

where the first map is restriction.

The field L is contained in $\mathbb{Q}(E[2])$. Let $\varepsilon\colon \mathrm{Aut}(E[2]) \to \{\pm 1\}$ be the character which corresponds to the signature map under any isomorphism $\mathrm{Aut}(E[2]) \cong \mathfrak{S}_3$. One checks that $\chi_D(\sigma) = \varepsilon(\rho_2(\sigma))$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Since L is an abelian extension of $\mathbb{Q}$, it must lie in a cyclotomic extension[1] of $\mathbb{Q}$. Set $d := |D|$; it is the smallest positive integer for which $L \subseteq \mathbb{Q}(\zeta_d)$ where $\zeta_d \in \overline{\mathbb{Q}}$ is a primitive d-th root of

[1]This is where the assumption $K = \mathbb{Q}$ is important

unity. The homomorphism $\det \circ \rho_d : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/d\mathbb{Z})^\times$ factors through the usual isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/d\mathbb{Z})^\times$. Thus there exists a unique character $\alpha\colon (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ such that $\chi_D(\sigma) = \alpha(\det \rho_d(\sigma))$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The minimality of d implies that α is a primitive Dirichlet character of conductor d.

Combining our two descriptions of χ_D, we have $\varepsilon(\rho_2(\sigma)) = \alpha(\det \rho_d(\sigma))$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Define the integer $M_E := \mathrm{lcm}(d, 2)$, and the group

$$H(M_E) := \big\{ g \in \mathrm{Aut}(E[M_E]) : \varepsilon(A \bmod 2) = \alpha(\det(A \bmod d)) \big\}.$$

which has index 2 in $\mathrm{Aut}(E[M_E])$. By the above discussion, $H(M_E)$ contains $G(M_E)$. The index 2 subgroup H_E of $\mathrm{Aut}(E_{\mathrm{tors}})$ mentioned earlier is just the inverse image of $H(M_E)$ under the natural map $\mathrm{Aut}(E_{\mathrm{tors}}) \to \mathrm{Aut}(E[M_E])$, and E is a Serre curve if and only if $\widehat{\rho}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = H_E$.

Proposition 4.4. *Let $E/\mathbb{Q}$ be a Serre curve, and let m be a positive integer. If $M_E | m$, then the group $G(m)$ is the inverse image of $H(M_E)$ under the natural map $\mathrm{Aut}(E[m]) \to \mathrm{Aut}(E[M_E])$. If $M_E \nmid m$, then $G(m) = \mathrm{Aut}(E[m])$.*

Proof. Define the group

$$H = \big\{ A \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) : \varepsilon(A \bmod 2) = \alpha(\det(A \bmod d)) \big\};$$

it is an index 2 subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For each integer m, let $H(m)$ be the image of H under the reduction modulo m map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. If $E/\mathbb{Q}$ is a Serre curve, then $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = H_E \cong H$ and $G(m) \cong H(m)$ for all m. It thus suffices to prove the analogous results for the groups $H(m)$.

First suppose that m is divisible by M_E. The group H is the inverse image of $H(M_E)$ under the reduction modulo M_E map $r_{M_E}\colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/M_E\mathbb{Z})$. The map r_{M_E} equals the composition $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/M_E\mathbb{Z})$ arising from reduction modulo m and M_E, so $H(m)$ equals the inverse image of $H(M_E)$ under reduction modulo M_E.

We may now suppose that m is not divisible by M_E, equivalently not divisible by 2 or not divisible by d. Take any $B \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. We will show that there is an $A \in H$ such that $A \equiv B \pmod m$, and hence B belongs to $H(m)$. Since B was arbitrary, we will deduce that $H(m) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

First suppose that 2 does not divide m. Define $n = \mathrm{lcm}(m, M_E)$ which we can write in the form $2^e n'$ with n' odd. Take any $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ for which $\det(B) \equiv x \pmod m$. Let A_{odd} be a matrix in $\mathrm{GL}_2(\prod_{\ell \neq 2} \mathbb{Z}_\ell)$ such that A_{odd} modulo m equals B and such that $\det(A_{\mathrm{odd}}) \equiv x \pmod{n'}$. The homomorphism

$$\mathrm{GL}_2(\mathbb{Z}_2) \to \{\pm 1\} \times \mathbb{Z}_2^\times, \quad C \mapsto \big(\varepsilon(C \bmod 2), \det(C)\big)$$

is surjective, so there is a matrix $A_2 \in \mathrm{GL}_2(\mathbb{Z}_2)$ such that $\det(A_2) \equiv x \pmod{2^e}$ and $\varepsilon(A_2 \bmod 2) = \alpha(x \bmod d)$. Let A be the matrix $(A_2, A_{\mathrm{odd}}) \in \mathrm{GL}_2(\mathbb{Z}_2) \times \mathrm{GL}_2(\prod_{\ell \neq 2} \mathbb{Z}_\ell) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$. The matrix A belongs to H since $\varepsilon(A \bmod 2) = \alpha(x \bmod d) = \alpha(\det(A \bmod d))$, and it satisfies $A \equiv B \pmod m$.

Now suppose that d does not divide m and that m is even. Then there is an element $x \in (\mathbb{Z}/\mathrm{lcm}(m,d)\mathbb{Z})^\times$ such that $\det(B) \equiv x \pmod m$ and $\alpha(x \bmod d) = \varepsilon(B \bmod 2)$; this uses that $d \nmid m$ and that α is a primitive Dirichlet character of conductor d. There exists an $A \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $B \equiv A \pmod m$ and $\det(A) \equiv x \pmod{\mathrm{lcm}(m,d)}$. The matrix A belongs to H since

$$\varepsilon(A \bmod 2) = \varepsilon(B \bmod 2) = \alpha(x \bmod d) = \alpha(\det(A \bmod d)),$$

and it satisfies $A \equiv B \pmod m$. □

4.3. **Proof of Proposition 4.2.** Let $E/\mathbb{Q}$ be a Serre curve, and keep the notation introduced in §4.2.

Let us first consider the case where $D \equiv 0 \bmod 4$. The integer $M_E = d = |D|$ is divisible by 4, so by Proposition 4.4, we have $G(m) = \mathrm{Aut}(E[m])$ for all *squarefree* m. By Proposition 2.4, with $t = 1$ and $M = 1$, we have $\mathcal{C}_{E,1} = \prod_\ell \left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right)$.

We shall now restrict to the case where $D \equiv 1 \bmod 4$. In this case, the integer $M_E = \mathrm{lcm}(2,d) = 2d = 2|D|$ is squarefree. By Proposition 4.4, we have $G(M_E \cdot m) = H(M_E) \times \mathrm{Aut}(E[m])$ for all *squarefree* m relatively prime to M_E. Thus by Proposition 2.4, with $t = 1$ and $M = M_E$, we have

$$\mathcal{C}_{E,1} = \frac{|H(M_E) \cap \Psi_1(M_E)|/|H(M_E)|}{\prod_{\ell | M_E}(1-1/\ell)} \prod_{\ell \nmid M_E} \Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big). \tag{4.1}$$

Since d is odd and α is a quadratic character of conductor d, we find that α is the Jacobi symbol $\left(\frac{\cdot}{d}\right)$. The set $H(M_E) \cap \Psi_1(M_E)$ then has the same cardinality as the set

$$X = \big\{A \in \mathrm{GL}_2(\mathbb{Z}/M_E\mathbb{Z}) : \varepsilon(A \bmod 2) = \Big(\tfrac{\det(A \bmod d)}{d}\Big),\ \det(I-A) \in (\mathbb{Z}/M_E\mathbb{Z})^\times\big\}.$$

Take any element $A \in X$. Setting $A_2 := A \bmod 2$, we have $\det(I - A_2) = 1$ and $\det(A_2) = 1$ in $\mathbb{Z}/2\mathbb{Z}$. The only matrices in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ that satisfy these conditions are: $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$. These two matrices have order 3 in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, and hence $\varepsilon(A_2) = 1$. Since d is odd, $H(M_E) \cap \Psi_1(M_E)$ has twice as many element as the set

$$Y = \{A \in \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}) : \Big(\tfrac{\det(A)}{d}\Big) = 1, \det(I-A) \in (\mathbb{Z}/d\mathbb{Z})^\times\}.$$

For each prime $\ell | d$, define the sets

$$Y_\ell^{\pm} := \big\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \left(\tfrac{\det(A)}{\ell}\right) = \pm 1,\ \det(I-A) \neq 0\big\}.$$

Under the isomorphism $\mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}) \cong \prod_{\ell | d} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, the set Y corresponds to the disjoint union of sets:

$$\bigcup_{\substack{J \subseteq \{\ell : \ell | d\} \\ |J| \text{ even}}} \prod_{\ell \in J} Y_\ell^- \times \prod_{\ell | d,\, \ell \notin J} Y_\ell^+.$$

Therefore,

$$\begin{aligned} |H(M_E) \cap \Psi_1(M_E)| = 2|Y| &= 2 \sum_{f | d} \frac{1+\mu(f)}{2} \prod_{\ell | f} |Y_\ell^-| \prod_{\ell | \frac{d}{f}} |Y_\ell^+| \\ &= \prod_{\ell | d} (|Y_\ell^+| + |Y_\ell^-|) + \prod_{\ell | d} (|Y_\ell^+| - |Y_\ell^-|), \end{aligned} \tag{4.2}$$

where μ is the Möbius function.

Lemma 4.5. *For $\ell | d$ and $\varepsilon \in \{\pm 1\}$,*

$$\frac{|Y_\ell^+| + \varepsilon |Y_\ell^-|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|(1-1/\ell)} = \begin{cases} 1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)} & \text{if } \varepsilon = +1, \\ \frac{\ell}{(\ell-1)^3(\ell+1)} & \text{if } \varepsilon = -1. \end{cases}$$

Proof. We use Lemma 2.5 to compute the $|Y_\ell^{\pm}|$:

$$\begin{aligned}|Y_\ell^{\pm}| &= |\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \left(\tfrac{\det A}{\ell}\right) = \pm 1\}| \\ &\quad - |\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \left(\tfrac{\det A}{\ell}\right) = \pm 1,\ \det(I-A) = 0\}| \\ &= \frac{1}{2}|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| - \sum_{a \in \mathbb{F}_\ell^\times,\, (\frac{a}{\ell}) = \pm 1} |\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : A \text{ has eigenvalues } 1 \text{ and } a\}| \\ &= \frac{1}{2}\ell(\ell-1)^2(\ell+1) - \frac{\ell-1}{2}(\ell^2+\ell) + \frac{1}{2}(1 \pm 1)\ell\end{aligned}$$

The rest is a direct calculation. □

Using (4.2), $|H(M_E)| = \frac{1}{2}\prod_{\ell | M_E} |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| = 3\prod_{\ell | d} |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|$, and Lemma 4.5, we have:

$$\begin{aligned}&\frac{|H(M_E) \cap \Psi_1(M_E)|/|H(M_E)|}{\prod_{\ell | M_E}(1-1/\ell)} \\ =&\frac{1}{3 \cdot \frac{1}{2}}\Big(\prod_{\ell | d} \frac{|Y_\ell^+| + |Y_\ell^-|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|(1-1/\ell)} + \prod_{\ell | d} \frac{|Y_\ell^+| - |Y_\ell^-|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|(1-1/\ell)}\Big) \\ =&\frac{2}{3}\Big(\prod_{\ell | d}\Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big) + \prod_{\ell | d} \frac{\ell}{(\ell-1)^3(\ell+1)}\Big) \\ =&\frac{2}{3}\prod_{\ell | d}\Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big)\Big(1 + \prod_{\ell | d} \frac{\frac{\ell}{(\ell-1)^3(\ell+1)}}{1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}}\Big) \\ =&\prod_{\ell | M_E = 2d}\Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big)\Big(1 + \prod_{\ell | d} \frac{1}{\ell^3 - 2\ell^2 - \ell + 3}\Big).\end{aligned}$$

Proposition 4.2 follows by combining this expression with (4.1) and noting that $d = |D|$.

5. Example: $y^2 = x^3 + 6x - 2$

In this section, we consider the elliptic curve E over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 = x^3 + 6x - 2$. This curve is a Serre curve (for a proof, see [LT76, Part I §7]).

The given Weierstrass model has discriminant $\Delta = -2^6 3^5$, and hence $\mathbb{Q}(\sqrt{\Delta})$ has discriminant -3. By Proposition 4.2 and (2.3),

$$\mathcal{C}_{E,1} = \frac{10}{9}\prod_{\ell}\Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big) \approx 0.56129574248826197129793 85\ldots \tag{5.1}$$

In the following table, the "expected number" of $p \le x$ with $p \nmid 6$ such that $|E(\mathbb{F}_p)|$ is prime is

$$\mathcal{C}_{E,1}\int_2^x \frac{1}{\log(u+1)}\frac{du}{\log u}$$

rounded to the nearest integer.

TABLE 1. Number of $p \le x$ with $p \nmid 6$ such that $|E(\mathbb{F}_p)|$ is prime.

x	Actual	Expected	x	Actual	Expected
20000000	45285	45592	520000000	810038	810610
40000000	83272	83564	540000000	837904	838429
60000000	118991	119317	560000000	865500	866145
80000000	153257	153735	580000000	893592	893763
100000000	186727	187209	600000000	921156	921287
120000000	219604	219958	620000000	948710	948720
140000000	251728	252123	640000000	975828	976066
160000000	283381	283799	660000000	1003310	1003328
180000000	314686	315058	680000000	1030626	1030508
200000000	345255	345953	700000000	1057836	1057610
220000000	375910	376526	720000000	1084734	1084636
240000000	406162	406810	740000000	1111877	1111589
260000000	436059	436833	760000000	1138685	1138470
280000000	465712	466619	780000000	1165267	1165282
300000000	495338	496186	800000000	1192027	1192027
320000000	524820	525552	820000000	1218668	1218707
340000000	553850	554731	840000000	1245563	1245324
360000000	583047	583736	860000000	1272004	1271878
380000000	611978	612577	880000000	1298490	1298373
400000000	640571	641265	900000000	1324972	1324810
420000000	668855	669809	920000000	1351413	1351190
440000000	697006	698216	940000000	1377897	1377514
460000000	725494	726493	960000000	1404065	1403784
480000000	753548	754648	980000000	1430213	1430001
500000000	781819	782685	1000000000	1456288	1456166

Remark 5.1. The predicted constant in [Kob88] was $9/10 \cdot \mathcal{C}_{E,1}$. This would have led to a predicted value of ≈ 1310549 in the last entry of Table 1.

6. EXAMPLE: $y^2 = x^3 + 9x + 18$

Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 = x^3 + 9x + 18$. The discriminant of our Weierstrass model is $\Delta = -2^8 3^6$. This is the curve mentioned in §1.1. It is not isogenous over $\mathbb{Q}$ to a curve with nontrivial $\mathbb{Q}$-torsion (in the notation of §3, $t_E = 1$), but we have $\mathcal{C}_{E,1} = 0$. We saw that $|E(\mathbb{F}_p)|$ was divisible by 3 if $p \equiv 1 \bmod 4$ and divisible by 2 if $p \equiv 3 \bmod 4$. In this section we will give numerical evidence for Conjecture 1.2 with $t \in \{2, 3, 6\}$.

We now state, without proof, enough information about the groups $G(m)$ so that one may compute the constants $\mathcal{C}_{E,2}$, $\mathcal{C}_{E,3}$ and $\mathcal{C}_{E,6}$.

- **2-torsion.** We have $G(2) = \mathrm{Aut}(E[2])$.
- **4-torsion.** Viewing $\mathrm{Aut}(E[2])$ as the symmetric group on $E[2] - \{0\}$, let $\varepsilon\colon \mathrm{Aut}(E[4]) \to \mathrm{Aut}(E[2]) \to \{\pm 1\}$ be the signature homorphism. Let χ be the non-identity character of $(\mathbb{Z}/4\mathbb{Z})^\times$. Then $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(i)$ implies that $G(4)$ is contained in the group

$$\{A \in \mathrm{Aut}(E[4]) : \varepsilon(A) = \chi(\det(A))\},$$

and this is actually an equality. We then have

$$\rho_4\big(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))\big) = \{A \in \operatorname{Aut}(E[4]) : \varepsilon(A) = \chi(\det(A)) = 1\}.$$

The maximal abelian extension of $\mathbb{Q}(i)$ in $\mathbb{Q}(E[4])$ is $\mathbb{Q}(i, \alpha, \sqrt{6})$ where α is a root of $x^3 + 9x + 18$. (Group theory with $G(4)$ tells us that it is a degree six extension of $\mathbb{Q}(i)$. In general, one always has $\mathbb{Q}(i, \sqrt[4]{\Delta}) \subseteq \mathbb{Q}(E[4])$; for our curve $\mathbb{Q}(i, \sqrt[4]{\Delta}) = \mathbb{Q}(i, \sqrt[4]{-9}) = \mathbb{Q}(i, \sqrt{6})$.)

• **3-torsion.** Choose a $\mathbb{Z}/3\mathbb{Z}$-basis of $E[3]$ whose first vector is $P := (-3, 6i)$. Then with respect to this basis, $G(3) = \rho_3(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$.

• **9-torsion.** The group $G(9)$ is the inverse image of $G(3)$ under the map $\operatorname{Aut}(E[9]) \to \operatorname{Aut}(E[3])$. The maximal abelian extension of $\mathbb{Q}(i)$ in $\mathbb{Q}(E[9])$ is $\mathbb{Q}(i, \zeta_9)$. Let $\beta\colon G(9) \to \{\pm 1\}$ be the homomorphism for which $\sigma(P) = \beta(\rho_9(\sigma))P$ for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

• **36-torsion.** We may view $G(36)$ as a subgroup of $G(4) \times G(9)$, where we have already described $G(4)$ and $G(9)$. To work out $G(36)$, one needs to know the field $\mathbb{Q}(E[4]) \cap \mathbb{Q}(E[9])$. We claim that $\mathbb{Q}(E[4]) \cap \mathbb{Q}(E[9]) = \mathbb{Q}(i)$. Suppose that $\mathbb{Q}(E[4]) \cap \mathbb{Q}(E[9]) \supsetneq \mathbb{Q}(i)$; then the solvability of $G(4)$ implies that there is a nontrivial abelian extension $L/\mathbb{Q}(i)$ in $\mathbb{Q}(E[4]) \cap \mathbb{Q}(E[9])$. However the maximal abelian extension of $\mathbb{Q}(i)$ in $\mathbb{Q}(E[4])$ and $\mathbb{Q}(E[9])$ is $\mathbb{Q}(i, \alpha, \sqrt{6})$ and $\mathbb{Q}(i, \zeta_9)$, respectively. Thus $L \subseteq \mathbb{Q}(i, \alpha, \sqrt{6}) \cap \mathbb{Q}(i, \zeta_9) = \mathbb{Q}(i)$. We deduce that

$$G(36) = \big\{(A, B) \in \operatorname{Aut}(E[4]) \times \operatorname{Aut}(E[9]) : \varepsilon(A) = \chi(\det(A)) = \beta(B)\big\}$$

and

$$\rho_{36}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \big\{(A, B) \in \operatorname{Aut}(E[4]) \times \operatorname{Aut}(E[9]) : \varepsilon(A) = \chi(\det(A)) = \beta(B) = 1\big\}.$$

• **5-torsion.** The group $G(5)$ is the unique subgroup of $\operatorname{Aut}(E[5])$ of order 96. The image in $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ is isomorphic to the symmetric group S_4 (this is one of the exceptional cases in [Ser72, Prop. 16]). The maximal abelian extension of $\mathbb{Q}$ in $\mathbb{Q}(E[5])$ is $\mathbb{Q}(\zeta_5)$.

• **ℓ-torsion, $\ell \geq 7$.** For every prime $\ell \geq 7$, we have $G(\ell) = \operatorname{Aut}(E[\ell])$. Group theory shows that for any squarefree positive integer m relatively prime to $2 \cdot 3 \cdot 5$, we have $G(m) = \prod_{\ell \mid m} \operatorname{Aut}(E[\ell])$. The maximal abelian extension of $\mathbb{Q}$ in $\mathbb{Q}(E[m])$ is $\mathbb{Q}(\zeta_m)$.

• For any squarefree positive integer m relatively prime to $2 \cdot 3 \cdot 5$, we claim that

$$G(36 \cdot 5 \cdot \textstyle\prod_{\ell \mid m} \ell) = G(36) \times G(5) \times \prod_{\ell \mid m} \operatorname{Aut}(E[\ell]). \tag{6.1}$$

Since $G(36)$ and $G(5)$ are solvable, it suffices to show that the maximal abelian extensions of $\mathbb{Q}$ in $\mathbb{Q}(E[36])$, $\mathbb{Q}(E[5])$, and $\mathbb{Q}(E[m])$ are pairwise linearly disjoint over $\mathbb{Q}$ (this is clear since the intersection of any two of these fields is an unramified extension of $\mathbb{Q}$).

Take any $t \in \{2, 3, 6\}$. From the above description, we may apply Proposition 2.4 with $M = 30$ to obtain

$$\mathcal{C}_{E,t} = \frac{\delta_{E,t}(36 \cdot 5)}{\prod_{\ell \mid 2 \cdot 3 \cdot 5}(1 - 1/\ell)} \prod_{\ell \geq 7} \Big(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\Big).$$

Since $G(36 \cdot 5) = G(36) \times G(5)$, we have

$$\mathcal{C}_{E,t} = \frac{\delta_{E,t}(36)}{(1 - 1/2)(1 - 1/3)} \frac{\delta_{E,t}(5)}{1 - 1/5} \prod_{\ell \geq 7} \Big(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\Big).$$

We have $\delta_{E,t}(5) = \delta_{E,1}(5)$ since t is relatively prime to 5, and using our description of $G(5)$ one can show that $\delta_{E,t}(5) = \delta_{E,1}(5) = 77/96$. Hence

$$\mathcal{C}_{E,t} = \delta_{E,t}(36) \frac{1232}{219} \prod_{\ell} \Big(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\Big).$$

Using our description of $G(36)$, one can show that $\delta_{E,2}(36)=1/8$, $\delta_{E,3}(36)=5/27$, and $\delta_{E,6}(36)=1/12$. We record the resulting constants in the next lemma.

Lemma 6.1. *For the elliptic curve E over $\mathbb{Q}$ defined by $y^2=x^3+9x+18$, we have*

$$\mathcal{C}_{E,2}=\frac{154}{219}\mathfrak{C} \quad \mathcal{C}_{E,3}=\frac{6160}{5913}\mathfrak{C} \quad \mathcal{C}_{E,6}=\frac{308}{657}\mathfrak{C}$$

where $\mathfrak{C}=\prod_{\ell}\Big(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big)$.

In the following table, the "expected number" of $p\le x$ with $p\nmid 6$ such that $|E(\mathbb{F}_p)|/t$ is prime is

$$\mathcal{C}_{E,t}\int_{t+1}^{x}\frac{1}{\log(u+1)}\frac{du}{\log u}$$

rounded to the nearest integer, where $\mathcal{C}_{E,t}$ is estimated using Lemma 6.1 and (2.3).

TABLE 2. Number of $p\le x$ with $p\nmid 6$ such that $|E(\mathbb{F}_p)|/t$ is prime.

	$t=2$		$t=3$		$t=6$	
x	Actual	Expected	Actual	Expected	Actual	Expected
40000000	55118	55244	83736	84036	39554	39634
80000000	101556	101444	154113	154134	72535	72537
120000000	145334	144995	220046	220165	103413	103490
160000000	187516	186949	283458	283747	133307	133271
200000000	228440	227774	345198	345597	161983	162224
240000000	268461	267730	405675	406118	190166	190543
280000000	307911	306986	464711	465565	217926	218348
320000000	346499	345657	523022	524117	245405	245727
360000000	384950	383827	580584	581901	272350	272739
400000000	422640	421560	637825	639017	299112	299433
440000000	459555	458907	694394	695541	325385	325845
480000000	496734	495907	750663	751535	351567	352005
520000000	533405	532594	806485	807050	377507	377936
560000000	570295	568996	861533	862129	403533	403659
600000000	606622	605135	916370	916807	428958	429192
640000000	642830	641032	970514	971114	454130	454548
680000000	678475	676705	1024511	1025079	479230	479741
720000000	713909	712169	1077829	1078722	504194	504782
760000000	749026	747436	1130770	1132066	529125	529680
800000000	784432	782518	1183934	1185128	553804	554443
840000000	819581	817427	1236561	1237925	578378	579081
880000000	854213	852172	1288783	1290470	603045	603599
920000000	888701	886761	1341501	1342777	627523	628004
960000000	923138	921202	1393453	1394859	651810	652301
1000000000	957322	955502	1445188	1446724	675851	676497

7. CM EXAMPLE: $y^2=x^3-x$

Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2=x^3-x$. This curve has complex multiplication by $R=\mathbb{Z}[i]$, where i corresponds to the endomorphism $(x,y)\mapsto(-x,iy)$ defined over $\mathbb{Q}(i)$. The curve E has conductor 2^5.

The torsion group $E(\mathbb{Q}(i))_{\text{tors}}$ has order 8 and is generated by $(i, 1-i)$ and $(1,0)$. So for those primes p that split in $\mathbb{Q}(i)$ (i.e., $p \equiv 1 \bmod 4$), we find that $|E(\mathbb{F}_p)|$ is divisible by 8. In this section, we give numerical evidence for Conjecture 1.2 with $t = 8$. We will study it in the form given in (2.5), which predicts that

$$\begin{aligned} &|\{p \le x : p \equiv 1 \bmod 4,\ |E(\mathbb{F}_p)|/8 \text{ is prime}\}| \\ &\sim \frac{\mathcal{C}_{E_{\mathbb{Q}(i)},8}}{2} \int_9^x \frac{1}{\log(u+1) - \log 8} \frac{du}{\log u} \end{aligned} \tag{7.1}$$

as $x \to \infty$ (we have used the integral version of the conjecture since it should give a better approximation). This particular curve was studied by Iwaniec and Jiménez Urroz in [IJU06] where they proved that

$$|\{p \le x : p \equiv 1 \bmod 4,\ |E(\mathbb{F}_p)|/8 \text{ is a product of one or two primes}\}| \gg \frac{x}{(\log x)^2}$$

using sieve theoretic methods. We now describe the constant $\mathcal{C}_{E_{\mathbb{Q}(i)},8}$:

Lemma 7.1. *Let E be the elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 - x$. Then*

$$\mathcal{C}_{E_{\mathbb{Q}(i)},8} = \prod_{\ell \ne 2} \Big(1 - \chi(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi(\ell))(\ell-1)^2}\Big)$$

where $\chi(\ell) = (-1)^{(\ell-1)/2}$. We have $\mathcal{C}_{E_{\mathbb{Q}(i)},8} \approx 1.067350894$.

Proof. Since E has conductor 2^5, the curve $E_{\mathbb{Q}(i)}$ has good reduction away from the prime $(1+i)$. For the curve $E_{\mathbb{Q}(i)}$, fix notation as in the proof of Proposition 2.7 (in particular, $K = F = \mathbb{Q}(i)$ and $R = \mathbb{Z}[i]$). Checking the two conditions in the second half of the proof of Proposition 2.7, we find that the Proposition holds for $E_{\mathbb{Q}(i)}$ with $M = 2$.

The discriminant of $\mathbb{Q}(i)$ is -4 and the conductor of the order R is 1, so by Proposition 2.8 we have

$$\mathcal{C}_{E_{\mathbb{Q}(i)},8} = \frac{\delta_{E_{\mathbb{Q}(i)},8}(16)}{(1-1/2)} \prod_{\ell \ne 2} \Big(1 - \chi(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi(\ell))(\ell-1)^2}\Big)$$

where χ is the Kronecker character of $\mathbb{Q}(i)$ (and hence $\chi(\ell) = (-1)^{(\ell-1)/2}$). To prove the required product description of $\mathcal{C}_{E_{\mathbb{Q}(i)},8}$, it remains to show that $\delta_{E_{\mathbb{Q}(i)},8}(16) = 1/2$. Consider the representation

$$\widehat{\rho}_2 \colon \operatorname{Gal}(\overline{\mathbb{Q}(i)}/\mathbb{Q}(i)) \to (R \otimes \mathbb{Z}_2)^\times = (\mathbb{Z}_2[i])^\times$$

arising from the Galois action on the Tate module $T_2(E)$. It is well known that $\widehat{\rho}_2$ has image equal to $1 + \mathfrak{p}_2^3$ where $\mathfrak{p}_2$ is the prime ideal $(1+i)\mathbb{Z}_2[i]$ (for example, see [KS99, 9.4]). In particular,

$$G(16) = \rho_{16}\big(\operatorname{Gal}(\overline{\mathbb{Q}(i)}/\mathbb{Q}(i))\big) = \big(1+\mathfrak{p}_2^3\big)/\big(1+16\mathbb{Z}_2[i]\big) = \big(1+\mathfrak{p}_2^3\big)/\big(1+\mathfrak{p}_2^8\big).$$

Under our identification of $\operatorname{Aut}_{\mathbb{Z}_2[i]}(T_2(E))$ with $\mathbb{Z}_2[i]^\times$, we find that $\det(I-a)$ agrees with $N(1-a)$ where N is the norm map from $\mathbb{Z}_2[i]$ to $\mathbb{Z}_2$. We deduce that $\delta_{E_{\mathbb{Q}(i)},8}(16)$ is the proportion of $a \in \big(1+\mathfrak{p}_2^3\big)/\big(1+\mathfrak{p}_2^8\big)$ for which $N(1-a) \equiv 8 \bmod 16$; this is indeed equal to $1/2$.

With respect to how one estimates the constant, we simply note that

$$\mathcal{C}_{E,8} = L(1,\chi)^{-1} \prod_{\ell \ne 2} \Big(1 - \chi(\ell) \frac{\ell^2 - \ell - 1}{(\ell - \chi(\ell))(\ell-1)^2}\Big)\Big(1 - \frac{\chi(\ell)}{\ell}\Big)^{-1}.$$

The product is now absolutely convergent and $L(1,\chi) = \pi/4$ by the class number formula. □

In the following table, the "Actual" column is the value of the left hand side of (7.1), while the "Expected" column is the right hand side of (7.1) with the approximation from Lemma 7.1.

TABLE 3. Number of $p \le x$ with $p \equiv 1 \bmod 4$ such that $|E(\mathbb{F}_p)|/8$ is prime.

x	Actual	Expected	x	Actual	Expected
20000000	49847	50063	520000000	865909	866300
40000000	91074	91134	540000000	895323	895804
60000000	129660	129648	560000000	924773	925193
80000000	166429	166631	580000000	954215	954472
100000000	202316	202534	600000000	983415	983645
120000000	237402	237612	620000000	1012618	1012717
140000000	271865	272024	640000000	1041478	1041691
160000000	305749	305882	660000000	1070519	1070571
180000000	338987	339266	680000000	1099310	1099359
200000000	372142	372237	700000000	1127947	1128060
220000000	404768	404844	720000000	1156596	1156676
240000000	437027	437124	740000000	1185077	1185209
260000000	469002	469110	760000000	1213434	1213663
280000000	500848	500827	780000000	1241996	1242040
300000000	532345	532298	800000000	1270215	1270341
320000000	563613	563542	820000000	1298419	1298570
340000000	594570	594575	840000000	1326489	1326728
360000000	625409	625412	860000000	1354726	1354817
380000000	656138	656065	880000000	1382946	1382839
400000000	686710	686546	900000000	1410787	1410796
420000000	716542	716864	920000000	1438522	1438689
440000000	746751	747028	940000000	1466143	1466520
460000000	776709	777047	960000000	1493786	1494291
480000000	806405	806928	980000000	1521276	1522003
500000000	836080	836677	1000000000	1548766	1549657

8. EXAMPLE: $X_0(11)$

In this section we consider the elliptic curve $E = X_0(11)$ defined over $\mathbb{Q}$. The modular interpretation of $X_0(11)$ is not important for our purposes; it suffices to know that $y^2+y = x^3-x^2-10x-20$ is a minimal Weierstrass model for $E/\mathbb{Q}$. The curve E has conductor 11 and hence has good reduction away from 11. By Theorem 3.2, t_E divides $|E(\mathbb{F}_p)|$ for each prime $p \nmid 2 \cdot 11$, and since $|E(\mathbb{F}_3)| = 5$, we deduce that t_E divides 5. The rational point $(x,y) = (5,5)$ of E has order 5, and thus 5 divides t_E. We deduce that $t_E = 5$ and in particular that $E(\mathbb{Q})_{\mathrm{tors}}$ is generated by $(5,5)$. In this section we shall test Conjecture 1.2 with $t = t_E = 5$.

Lang and Trotter have worked out the Galois theory for this elliptic curve, and in particular have shown that Theorem 2.3 holds with $M = 2 \cdot 5 \cdot 11$ (see [LT76, Part I, §8] for full details). By

Proposition 2.4, we have

$$\mathcal{C}_{E,5} = \frac{\delta_{E,5}(2\cdot 5^2\cdot 11)}{\prod_{\ell\mid 2\cdot 5\cdot 11}(1-1/\ell)} \prod_{\ell\nmid 2\cdot 5\cdot 11}\Big(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big) \tag{8.1}$$

$$= \delta_{E,5}(2\cdot 5^2\cdot 11)\frac{345600}{78913}\prod_{\ell}\Big(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big).$$

We shall now describe the structure of the group $G(2\cdot 5^2\cdot 11)$ and then compute $\delta_{E,5}(2\cdot 5^2\cdot 11)$. Those not interested in this computation can skip ahead to the data.

For all $\ell\neq 5$, we have $G(\ell)=\mathrm{Aut}(E[\ell])$. There is a basis of $E[5^2]$ over $\mathbb{Z}/25\mathbb{Z}$ for which $G(5^2)$ becomes the group

$$\left\{\begin{pmatrix}1+5a & 5b\\ 5c & u\end{pmatrix} : a,b,c\in\mathbb{Z}/25\mathbb{Z}, u\in(\mathbb{Z}/25\mathbb{Z})^\times\right\}.$$

To ease computation, identify $G(5^2)$ with this matrix group. Fixing a basis, we can also identify $G(2)$ and $G(11)$ with the full groups $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$ respectively.

Let $\varepsilon\colon G(2)\to\{\pm 1\}$ be the signature map (i.e, compose any isomorphism $G(2)\cong\mathfrak{S}_3$ with the usual signature), and define the homomorphisms

$$\phi_{11}\colon G(11)\twoheadrightarrow \mathbb{F}_{11}^\times/\{\pm 1\},\quad A\mapsto \pm\det(A)$$

and

$$\alpha\colon G(5^2)\twoheadrightarrow\mathbb{Z}/5\mathbb{Z},\quad \left(\begin{smallmatrix}1+5a & 5b\\ 5c & u\end{smallmatrix}\right)\mapsto a \mod 5.$$

The group $\mathbb{F}_{11}^\times/\{\pm1\}$ is cyclic of order 5 with generator ± 2, so it makes sense to define a homomorphism $\phi_5\colon G(5^2)\to\mathbb{F}_{11}^\times/\{\pm1\}$ by

$$\phi_5(A)=(\pm 2)^{\alpha(A)}.$$

We have a natural inclusion $G(2\cdot 5^2\cdot 11)\subseteq G(2)\times G(5^2)\times G(11)$, which gives us the following description of $G(2\cdot 5^2\cdot 11)$:

$$G(2\cdot 5^2\cdot 11)=\left\{(A_2,A_5,A_{11})\in G(2)\times G(5^2)\times G(11) : \begin{array}{r}\phi_5(A_5)=\phi_{11}(A_{11}),\\ \left(\frac{\det(A_{11})}{11}\right)=\varepsilon(A_2)\end{array}\right\}.$$

Lemma 8.1. $|G(2\cdot 5^2\cdot 11)|=19800000$.

Proof. We first use the fact that ε surjects onto $\{\pm1\}$, and $|G(2)|=6$.

$$\begin{aligned}
&|G(2\cdot 5^2\cdot 11)|\\
=&|\{(A_2,A_5,A_{11})\in G(2)\times G(5^2)\times G(11) : \phi(A_5)=\phi(A_{11}), \left(\tfrac{\det(A_{11})}{11}\right)=\varepsilon(A_2)\}|\\
=&3\cdot|\{(A_5,A_{11})\in G(5^2)\times G(11) : \phi(A_5)=\phi(A_{11}), \left(\tfrac{\det(A_{11})}{11}\right)=1\}|\\
&+3\cdot|\{(A_5,A_{11})\in G(5^2)\times G(11) : \phi(A_5)=\phi(A_{11}), \left(\tfrac{\det(A_{11})}{11}\right)=-1\}|\\
=&3\cdot|\{(A_5,A_{11})\in G(5^2)\times G(11) : \phi(A_5)=\phi(A_{11})\}|
\end{aligned}$$

We now use that ϕ_5 and ϕ_{11} surject onto a common group of order 5.

$$\begin{aligned}
|G(2\cdot 5^2\cdot 11)| &= 3\cdot|\{(A_5,A_{11})\in G(5^2)\times G(11) : \phi(A_5)=\phi(A_{11})\}|\\
&= 3|G(5^2)||G(11)|/5 = \frac{3}{5}(5^3\cdot 20)(11^2-1)(11^2-11)=19800000
\end{aligned}$$

□

Lemma 8.2. $\delta_{E,5}(2\cdot 5^2\cdot 11)=9/50$.

Proof. To ease notation, define $\mathcal{B}(m) := G(m) \cap \Psi_t(m)$. First note that an element $A \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) = G(2)$ is in $\mathcal{B}(2)$ if and only if $\det(I-A) = \det(A) = 1$. One quickly verifies that $\mathcal{B}(2) = \{\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)\}$. These two elements have order three, so $\varepsilon(A) = 1$ for all $A \in \mathcal{B}(2)$.

$$\begin{aligned}
&|\mathcal{B}(2\cdot 5^2\cdot 11)|\\
=&|\{(A_2, A_5, A_{11}) \in \mathcal{B}(2)\times \mathcal{B}(5^2)\times \mathcal{B}(11) : \phi(A_5) = \phi(A_{11}), \left(\tfrac{\det(A_{11})}{11}\right) = \varepsilon(A_2)\}|\\
=&2\cdot |\{(A_5, A_{11}) \in \mathcal{B}(5^2)\times \mathcal{B}(11) : \phi(A_5) = \phi(A_{11}), \det(A_{11}) \in (\mathbb{F}_{11}^\times)^2\}|\\
=&2\sum_{x\in \mathbb{F}_{11}^\times/\{\pm 1\}} |\{A \in \mathcal{B}(5^2) : \phi_5(A) = x\}||\{A \in \mathcal{B}(11) : \phi_{11}(A) = x, \det(A) \in (\mathbb{F}_{11}^\times)^2\}|
\end{aligned}$$

Take any $A = \left(\begin{smallmatrix}1+5a & 5b\\ 5c & u\end{smallmatrix}\right) \in G(5)$. We have $\det(I-A) = 5a(u-1) \in t_E(\mathbb{Z}/25\mathbb{Z})^\times = 5(\mathbb{Z}/25\mathbb{Z})^\times$ if and only if $a \not\equiv 0 \pmod 5$ and $u \not\equiv 1 \pmod 5$. Given $a \in \mathbb{Z}/5\mathbb{Z}$, we find that

$$|\{A \in \mathcal{B}(5^2) : \alpha(A) = a\}| = \begin{cases} 5^2\cdot 15 = 375 & \text{if } a \not\equiv 0 \pmod 5\\ 0 & \text{if } a \equiv 0 \pmod 5,\end{cases}$$

and hence for $b \in \mathbb{F}_{11}^\times$,

$$|\{A \in \mathcal{B}(5^2) : \phi_5(A) = \pm b\}| = \begin{cases} 375 & \text{if } b \neq \pm 1\\ 0 & \text{if } b = \pm 1.\end{cases}$$

Our expression for $|\mathcal{B}(2\cdot 5^2\cdot 11)|$ thus simplifies to the following,

$$|\mathcal{B}(2\cdot 5^2\cdot 11)| = 750 \sum_{x\in \mathbb{F}_{11}^\times/\{\pm 1\} - \{\{\pm 1\}\}} |\{A \in \mathcal{B}(11) : \phi_{11}(A) = x, \det(A) \in (\mathbb{F}_{11}^\times)^2\}|.$$

Take any $x \in \mathbb{F}_{11}^\times/\{\pm 1\}$. Since -1 is not a square in $\mathbb{F}_{11}^\times$, the class x contains a unique element $b_x \in (\mathbb{F}_{11}^\times)^2$.

$$|\{A \in \mathcal{B}(11) : \phi_{11}(A) = x,\ \det(A) \in (\mathbb{F}_{11}^\times)^2\}| = |\{A \in \mathcal{B}(11) : \det(A) = b_x\}|.$$

So our expression for $|\mathcal{B}(2\cdot 5^2\cdot 11)|$ simplifies further to

$$|\mathcal{B}(2\cdot 5^2\cdot 11)| = 750 \sum_{b\in (\mathbb{F}_{11}^\times)^2 - \{1\}} |\{A \in \mathrm{GL}_2(\mathbb{F}_{11}) : \det(A) = b,\ \det(I-A) \neq 0\}|.$$

Using Lemma 2.5, we obtain

$$\begin{aligned}
|\mathcal{B}(2\cdot 5^2\cdot 11)| &= 750 \sum_{b\in (\mathbb{F}_{11}^\times)^2 - \{1\}} \Big(|\mathrm{GL}_2(\mathbb{F}_{11})|/10 - (11^2+11)\Big)\\
&= 750\cdot 4\cdot ((11^2-1)(11^2-11)/10 - (11^2+11)) = 3564000.
\end{aligned}$$

Therefore using the previous lemma, we have

$$\delta_{E,5}(2\cdot 5^2\cdot 11) = |\mathcal{B}(2\cdot 5^2\cdot 11)|/|G(2\cdot 5^2\cdot 11)| = 3564000/19800000 = 9/50. \qquad \square$$

We finally describe the constant $\mathcal{C}_{X_0(11),5}$ from Conjecture 1.2. Lemma 8.2 and (8.1) imply that

$$\mathcal{C}_{X_0(11),5} = \frac{62208}{78913}\prod_{\ell}\Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big). \tag{8.2}$$

In the following table, the "expected number" of $p \le x$ with $p \neq 11$ such that $|X_0(11)(\mathbb{F}_p)|/5$ is prime is

$$\mathcal{C}_{X_0(11),5}\int_6^x \frac{1}{\log(u+1) - \log 5}\frac{du}{\log u} \tag{8.3}$$

rounded to the nearest integer, where $\mathcal{C}_{X_0(11),5}$ is estimated using (8.2) and (2.3).

TABLE 4. Number of $p \le x$ with $p \neq 11$ such that $|X_0(11)(\mathbb{F}_p)|/5$ is prime.

x	Actual	Expected	x	Actual	Expected
20000000	36051	36091	520000000	629151	628797
40000000	66143	65814	540000000	650676	650253
60000000	94050	93715	560000000	671998	671626
80000000	120806	120523	580000000	693377	692921
100000000	146748	146560	600000000	714783	714139
120000000	172172	172007	620000000	735972	735285
140000000	197180	196979	640000000	756879	756360
160000000	221586	221554	660000000	777830	777368
180000000	245768	245790	680000000	798736	798311
200000000	269776	269730	700000000	819665	819190
220000000	293290	293410	720000000	840621	840008
240000000	316771	316855	740000000	861196	860768
260000000	340034	340090	760000000	881992	881470
280000000	363448	363133	780000000	902549	902117
300000000	386413	385999	800000000	923181	922709
320000000	409103	408703	820000000	943660	943250
340000000	431644	431255	840000000	964135	963740
360000000	453854	453667	860000000	984561	984180
380000000	476378	475947	880000000	1005037	1004572
400000000	498621	498103	900000000	1025528	1024917
420000000	520651	520143	920000000	1045814	1045217
440000000	542604	542072	940000000	1066059	1065472
460000000	564364	563898	960000000	1086151	1085683
480000000	586046	585624	980000000	1106398	1105852
500000000	607563	607255	1000000000	1126420	1125980

Remark 8.3. The term $\log 5$ in (8.3) is numerically important. For example, we find that $\mathcal{C}_{X_0(11),5} \cdot \int_6^{10^9} (\log(u+1)\log u)^{-1} du \approx 1033120$, which is a worse approximation of $P_{X_0(11),5}(10^9)$ than that given in Table 4.

9. Recent progress

We briefly describe some of the progress that has been made on Koblitz's conjecture. This very short survey is not meant to be exhaustive and sometimes we only state special cases of results; one should consult the cited papers for more details and developments. In this section, we limit ourselves to elliptic curves defined over $\mathbb{Q}$.

First of all, there are currently no examples where Conjecture 1.2 is known to hold besides those trivial cases where $\mathcal{C}_{E,t} = 0$ (and thus have a congruence obstruction). Moreover, there are no known examples of elliptic curves E and integers t for which $\lim_{x\to\infty} P_{E,t}(x) = \infty$.

Much of the recent progress has been made by applying methods from sieve theory (including methods that were used to study twin primes or Sophie Germain primes). Recall that the conjecture that there are infinitely many Sophie Germain primes is equivalent to there being infinitely many

primes p for which $(p-1)/2$ is prime (this is an analogue of Conjecture 1.2 with $K=\mathbb{Q}$, $t=2$ and E replaced by the group scheme $\mathbb{G}_m$).

9.1. **Non-CM curves.** Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Miri and Murty [MM01] showed, assuming GRH, that there are $\gg x/(\log x)^2$ primes $p\le x$ for which $|E(\mathbb{F}_p)|$ has at most 16 prime divisors. Steuding and Weng [SW05a, SW05b] improved this to 9 factors. Assuming GRH and $t_E=1$, David and Wu [DW08] have shown that

$$|\{p\le x : |E(\mathbb{F}_p)| \text{ has at most 8 prime factors}\}| \ge 2.646\cdot \mathcal{C}_{E,1}\frac{x}{(\log x)^2}$$

for $x\gg_E 1$, where $\mathcal{C}_{E,1}$ is the constant of Conjecture 1.2.

We now mention some upper bounds obtained under GRH (though weakening of this conjecture can also be used). Cojocaru [Coj05] proved that $P_{E,1}(x)\ll x/(\log x)^2$; which of course should be the best possible general bound, up to improvement of the implicit constant. David and Wu [DW08] have shown that for any $\varepsilon>0$, one has

$$P_{E,1}\le (10+\varepsilon)\mathcal{C}_{E,1}\frac{x}{(\log x)^2}$$

for all $x\gg_{E,\varepsilon} 1$. In the general setting of Conjecture 1.2, one has the bound

$$P_{E,t}(x)\le (22+o(1))\mathcal{C}_{E,t}\frac{x}{(\log x)^2}$$

where the $o(1)$ term depends on E and t; this is Theorem 1.3 of [Zyw08] (this theorem uses $t=t_E$, but the proof carries through for general t).

For *unconditional* upper bounds, Cojocaru [Coj05] proved that $P_{E,1}(x)\ll x/(\log x\log\log\log x)$. This can be strengthened to $P_{E,1}(x)\le (24+o(1))\mathcal{C}_{E,1}\cdot x/(\log x\log\log x)$, see [Zyw08, Theorem 1.3]. However, this is still not strong enough to prove that

$$\sum_{p,\,|E(\mathbb{F}_p)| \text{ is prime}} \frac{1}{p} < \infty$$

(which would be the analogue of Brun's theorem that $\sum_{p \text{ and } p+2 \text{ are prime}} 1/p<\infty$).

9.2. **CM elliptic curves.** Now consider a CM elliptic curve E over $\mathbb{Q}$. If $t_E=1$, then Cojocaru [Coj05, Theorem 4] has shown that

$$|\{p\le x : |E(\mathbb{F}_p)| \text{ has at most 5 prime factors}\}| \gg \frac{x}{(\log x)^2}$$

(note that this theorem does *not* depend on GRH). If E has CM by the maximal order $\mathcal{O}_F$ of an imaginary quadratic extension $F/\mathbb{Q}$, then Jiménez Urroz [JU08] has proved that

$$|\{p\le x : p \text{ splits in } F,\ |E(\mathbb{F}_p)|/t_{E_F} \text{ has at most 2 prime factors}\}| \gg \frac{x}{(\log x)^2}$$

(this extends a result of Iwaniec and Jiménez Urroz mentioned at the beginning of §7).

9.3. **The conjecture on average.** We now consider the functions $P_{E,1}(x)$ averaged over a family of elliptic curves. Fix $\alpha>1/2$ and $\beta>1/2$ with $\alpha+\beta>3/2$. Let $\mathcal{F}(x)$ be the set of $(a,b)\in\mathbb{Z}^2$ with $|a|\le x^\alpha$ and $|b|\le x^\beta$ for which $4a^3+27b^2\ne 0$. For $(a,b)\in\mathcal{F}(x)$, let $E(a,b)$ be the elliptic curve over $\mathbb{Q}$ defined by the affine equation $Y^2=X^3+aX+b$. Balog, Cojocaru, and David [BCD07] have proved that

$$\frac{1}{|\mathcal{F}(x)|}\sum_{(a,b)\in\mathcal{F}(x)} P_{E(a,b),1}(x) \sim \mathfrak{C}\frac{x}{(\log x)^2} \tag{9.1}$$

as $x \to \infty$, where $\mathfrak{C} = \prod_{\ell} \Big(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\Big)$. Informally, this says that Koblitz's conjecture holds "on average".

9.4. **The constant on average.** Assuming a positive answer to a question of Serre[2], Jones [Jon09] proved that (9.1) is also true on the level of constants; i.e.,

$$\lim_{x\to\infty} \frac{1}{|\mathcal{F}(x)|} \sum_{(a,b)\in\mathcal{F}(x)} \mathcal{C}_{E(a,b),1} = \mathfrak{C}.$$

Finally, we explain how this can be proven *unconditionally* (we state it in a fashion similar to [Jon09, Theorem 6]).

Proposition 9.1. *Let $\mathcal{F}(x)$ be the set of $(a,b) \in \mathbb{Z}^2$ with $|a| \le x$ and $|b| \le x$ such that $4a^3 + 27b^2 \neq 0$. Then there is an absolute constant $\gamma > 0$ such that for any integer $k \ge 1$, we have*

$$\frac{1}{|\mathcal{F}(x)|} \sum_{(a,b)\in\mathcal{F}(x)} |\mathcal{C}_{E(a,b),1} - \mathfrak{C}|^k \ll_k \frac{(\log x)^\gamma}{\sqrt{x}}.$$

Proof. (Sketch) We first consider a fixed non-CM elliptic curve E over $\mathbb{Q}$. Let M be the positive squarefree integer for which $\ell \nmid M$ if and only if $\ell \ge 5$ and $G(\ell) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Some group theory shows that

$$G(Mm) = G(M) \times \prod_{\ell \mid m} \mathrm{Aut}(E[\ell])$$

for any squarefree integer m relatively prime to M. By [Mas98, Theorem 3], there is an absolute constant $\kappa \ge 0$ such that $M \ll \max\{1, h(E)^\kappa\}$ where $h(E)$ is the logarithmic absolute semistable Faltings height of E. By [Sil86], we have $h(E) \ll h(j_E)$ where j_E is the j-invariant of E and h is the usual height of a rational number.

By Proposition 2.4 with the above M,

$$\mathcal{C}_{E,1} = \frac{\delta_{E,1}\big(\prod_{\ell\mid M}\ell\big)}{\prod_{\ell\mid M}(1-1/\ell)} \prod_{\ell\nmid M} \Big(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\Big) \le \prod_{\ell\mid M}(1-1/\ell)^{-1}.$$

If y is the smallest prime for which $\prod_{\ell\le y}\ell \le M$, then

$$\prod_{\ell\mid M}(1-1/\ell)^{-1} \le \prod_{\ell\le y}(1-1/\ell)^{-1} \ll \log y$$

where the last inequality follows from Mertens' theorem. So

$$\mathcal{C}_{E,1} \ll \log y \ll \log\Big(\sum_{\ell\le y}\log\ell\Big) \le \log\log M.$$

Therefore, for any non-CM elliptic curve over $\mathbb{Q}$ we have

$$\mathcal{C}_{E,1} \ll \log\log\log(h(j_E) + 16) \tag{9.2}$$

(the 16 is added simply to make sure the right-hand side is alway well-defined and positive). One can also check that $\mathcal{C}_{E,1} \ll 1$ for CM elliptic curves $E/\mathbb{Q}$.

[2]Does there exists a constant C such that for any non-CM elliptic curve $E/\mathbb{Q}$, we have $\rho_\ell(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell \ge C$?

Let $\mathcal{S}(x)$ be the set of $(a,b) \in \mathcal{F}(x)$ for which $E(a,b)$ is a Serre curve (cf. §4). Theorem 10 of [Jon09] implies that

$$\frac{1}{|\mathcal{F}(x)|} \sum_{(a,b)\in\mathcal{S}(x)} |\mathcal{C}_{E(a,b),1} - \mathfrak{C}|^k \ll_k \frac{(\log x)^8}{\sqrt{x}}; \tag{9.3}$$

a key point is that the difference $\mathcal{C}_{E(a,b),1} - \mathfrak{C}$ has a nice description (cf. Proposition 4.2).

For each $(a,b) \in \mathcal{F}(x)$, we have $h(j_{E(a,b)}) \ll \log x$. Therefore by (9.2) we have

$$\frac{1}{|\mathcal{F}(x)|} \sum_{(a,b)\in\mathcal{F}(x)-\mathcal{S}(x)} |\mathcal{C}_{E(a,b),1} - \mathfrak{C}|^k \ll_k \frac{|\mathcal{F}(x)-\mathcal{S}(x)|}{|\mathcal{F}(x)|} (\log\log\log\log x)^k.$$

By [Jon10, Theorem 4], there is a constant $\beta > 0$ such that $|\mathcal{F}(x) - \mathcal{S}(x)|/|\mathcal{F}(x)| \ll (\log x)^\beta/\sqrt{x}$. Therefore

$$\frac{1}{|\mathcal{F}(x)|} \sum_{(a,b)\in\mathcal{F}(x)-\mathcal{S}(x)} |\mathcal{C}_{E(a,b),1} - \mathfrak{C}|^k \ll_k \frac{(\log x)^\beta}{\sqrt{x}} \tag{9.4}$$

for some constant $\beta > 0$. The proposition follows immediately by combining (9.3) and (9.4). □

References

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265. ↑1.3

[Coj05] Alina Carmen Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289. ↑9.1, 9.2

[BCD07] Antal Balog, Alina Cojocaru, and Chantal David, *Average twin prime conjecture for elliptic curves* (2007). arXiv:0709.1461v1 [math.NT]. ↑9.3

[DW08] Chantal David and Jie Wu, *Almost prime values of the order of elliptic curves over finite fields* (2008). arXiv:0812.2860v1 [math.NT]. ↑9.1

[Gre07] Aaron Greicius, *Elliptic curves with surjective global Galois representation*, Ph.D. thesis, University of California, Berkeley, 2007. ↑ii

[HL23] 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), 1–70. ↑1

[IJU06] H. Iwaniec and J. Jiménez Urroz, *Orders of CM elliptic curves modulo p with at most two primes* (2006). http://upcommons.upc.edu/e-prints/handle/2117/1169. ↑7

[JU08] Jorge Jiménez Urroz, *Almost prime orders of CM elliptic curves modulo p*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 74–87. ↑9.2

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570. ↑4.1, 9.4

[Jon09] ———, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685–710. ↑i, 9.4, 9.4

[Kat81] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. ↑3, 3.2

[KS99] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. ↑7

[Kob88] 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. ↑1.1, 1, 3, 5.1

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. ↑2.2

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers; Lecture Notes in Mathematics, Vol. 504. ↑1, 2.4, 5, 8

[Mas98] David Masser, *Multiplicative isogeny estimates*, J. Austral. Math. Soc. Ser. A **64** (1998), no. 2, 178–194. ↑9.4

[MM01] 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. ↑9.1

[PG08] The PARI Group, *PARI/GP, version* `2.3.4`, The PARI Group, Bordeaux, 2008. available from `http://pari.math.u-bordeaux.fr/`. ↑1.3

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑2.3, 2.3, 4.1, 4.1, 4.2, 6

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

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. ↑2.3

[Sil86] Joseph H. Silverman, *Heights and elliptic curves*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 253–265. ↑9.4

[SW05a] 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. ↑9.1

[SW05b] ———, *Erratum: "On the number of prime divisors of the order of elliptic curves modulo p" [Acta Arith. **117** (2005), no. 4, 341–352; MR 2140162]*, Acta Arith. **119** (2005), no. 4, 407–408. ↑9.1

[Ste03] Peter Stevenhagen, *The correction factor in Artin's primitive root conjecture*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 383–391. Les XXIIèmes Journées Arithmetiques (Lille, 2001). ↑1

[Zyw10] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826. ↑ii

[Zyw08] ———, *The Large Sieve and Galois Representations* (2008). arXiv:0812.2222v1 [math.NT]. ↑9.1

Department of Mathematics, University of Pennsylvania,, Philadelphia, PA 19104-6395, USA
E-mail address: `zywina@math.upenn.edu`