On the number of F_p-valued points of elliptic curves

Okumura, Shinya

出版情報：Journal of Math-for-Industry (JMI). 5 (B), pp.111-128, 2013-10. Faculty of Mathematics, Kyushu University
バージョン：
権利関係：

Journal of Math-for-Industry, Vol. 5 (2013B-4), pp. 111–128

Math-for-industry
Education & Research Hub

On the number of $\mathbb{F}_p$-valued points of elliptic curves

Shinnya Okumura

Received on May 13, 2013 / Revised on July 29, 2013

Abstract. We present a conjecture refining those of Koblitz and Zywina on the primality and divisibility of the number of $\mathbb{F}_p$-valued points of elliptic curves when p varies satisfying a congruence condition. We give also numerical data which support our conjecture.

Keywords. elliptic curves modulo p, Galois representations, Koblitz's conjecture, Zywina's conjecture

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ defined by a Weierstrass equation with integer coefficients. Let $E(\mathbb{F}_p)$ be the group of $\mathbb{F}_p$-valued points of E mod p where p is a prime number such that E has good reduction at p. Let $\pi_E(x)$ be the number of prime numbers $p \leqq x$ such that E has good reduction at p and $|E(\mathbb{F}_p)|$ is a prime. In [5] Koblitz conjectured that if E is not $\mathbb{Q}$-isogenous to an elliptic curve which has non-trivial $\mathbb{Q}$-torsion points (we note that $|E(\mathbb{F}_p)|$ is a $\mathbb{Q}$-isogeny invariant of E), then

$$\pi_E(x) \sim C_E \frac{x}{(\log x)^2} \quad \text{as } x \to \infty, \tag{1}$$

where C_E is a constant depending on E. For more detail on the constant C_E, see §2.1.

A motivation for this conjecture is the elliptic curve cryptography (ECC). This cryptosystem is based on intractability of the discrete logarithm problem for elliptic curves defined over a finite field (DLPEC) (see [6] and [10]). We cannot use an arbitrary elliptic curves over a finite field for ECC, because there are methods by which we can solve DLPEC for special elliptic curves. For example, the Pohlig-Hellman method works well if all of the prime numbers dividing $|E(\mathbb{F}_p)|$ are small (see [4]). Thus if we want to use E for ECC, then we must check whether $|E(\mathbb{F}_p)|$ is a very large prime number (or at least divisible by a very large prime number). See [11] and [1] for other necessary conditions for ECC.

In [16] Zywina refined Koblitz's conjecture and generalized it to the number field case. Let E_K be an elliptic curve defined over a number field K and O_K the ring of integers of K. Let $E_K(\mathbb{F}_\mathfrak{p})$ be the group of $\mathbb{F}_\mathfrak{p}$ -valued points of E_K mod $\mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal of O_K and $\mathbb{F}_\mathfrak{p}$ is the residue field at $\mathfrak{p}$. We define the sets

- $\Sigma_K := \{\text{prime ideals of } O_K\}$,
- $\Sigma_K(x) := \{\mathfrak{p} \in \Sigma_K : N_K(\mathfrak{p}) \leqq x\}$,
- $S_{E_K} := \{\mathfrak{p} \in \Sigma_K : E \text{ has bad reduction at } \mathfrak{p}\}$,
- $\pi_{E_K,t}(x) := \big|\{\mathfrak{p} \in \Sigma_K(x) - S_{E_K} : t \mid |E(\mathbb{F}_\mathfrak{p})|, |E(\mathbb{F}_\mathfrak{p})|/t \text{ is prime}\}\big|$.

where $N_K(\mathfrak{p})$ is the norm of $\mathfrak{p}$. He conjectured that, for any positive integer t,

$$\pi_{E_K,t}(x) \sim C_{E_K,t} \frac{x}{(\log x)^2} \quad \text{as } x \to \infty, \tag{2}$$

where $C_{E_K,t}$ is a constant depending on E_K and t. For more detail on the constant $C_{E_K,t}$, see §2.2.

In this paper we consider, in the case $K = \mathbb{Q}$, how the probability that $|E(\mathbb{F}_p)|/t$ is prime varies with a if we impose the congruence condition $p \equiv a \pmod b$ with $\gcd(a,b) = 1$. Our conjecture is as follows:

Conjecture 1. *Let E be an elliptic curve over $\mathbb{Q}$ defined by a Weierstrass equation with integer coefficients and let a, b and t any positive integers with $\gcd(a,b) = 1$. Let $\pi_{E,t,a,b}(x)$ be the number of prime numbers $p \leqq x$ such that E has good reduction at p, $|E(\mathbb{F}_p)|$ is divisible by t, $|E(\mathbb{F}_p)|/t$ is a prime and $p \equiv a \pmod b$. Let $\pi_{a,b}(x)$ be the number of prime numbers $p \leqq x$ such that $p \equiv a \pmod b$. Then*

$$P_E(t,a,b,x) := \frac{\pi_{E,t,a,b}(x)}{\pi_{a,b}(x)} \sim C_{E,t,a,b} \frac{C_{E,t}}{\log x} \tag{3}$$

as $x \to \infty$, where $C_{E,t}$ is the constant which occurs in Zywina's conjecture, and $C_{E,t,a,b}$ is a constant depending on E, t, a and b, and is defined in §3 (see (7) in the non-CM case and (9) in the CM case).

Note that $\pi_{a,b}(x) \sim \frac{1}{\varphi(b)}\pi(x)$ as $x \to \infty$ where $\varphi(\cdot)$ is the Euler function and $\pi(x)$ is the number of prime numbers less than x. Note that it is possible that $C_E, C_{E_K,t}$ or $C_{E,t,a,b}$ is equal to 0 and this means that the number of such primes are finite. In fact, it can be shown that if $C_E, C_{E_K,t}$ or $C_{E,t,a,b} = 0$, then $|E(\mathbb{F}_p)|/t$ is not invertible modulo m for some m and for all sufficient large p (see,

§2 and §3). Note that the value of $C_{E,t,a,b}$ does vary with $a \pmod b$. How it varies depends on the "defect" of the Galois representation associated with E; see §3.

These three conjectures are based on the same arguments as to deduce the twin primes conjecture by Hardy and Littlewood ([3]), together with some input from Galois representations attached to the torsion subgroup of E and the Chebotarev density theorem. In particular our method is based on Zywina's method, because Koblitz's conjecture is not always correct. A difference between the method of them is in the usage of Serre's theorems about the image of Galois representation. About these matters, we will explain in detail in §2 including Koblitz's conjecture. So §2 is of expository nature.

In general, it is not so easy to calculate the value of the constant $C_{E,t,a,b}$ from its definition. In Section 3, we give explicit presentations of this constant (Theorems 3 and 4), which are our main results in this paper and are actually used in the calculations for explicit examples in §4.

In §4, we calculate the constant $C_{E,t,a,b}$ for specific three elliptic curves and give tables and graphs of $P_E(t,a,b,x)$ for $x \leqq 10^{10}$.

In appendix we also consider the divisibility of $|E(\mathbb{F}_p)|$ and we will prove theorem on 2-divisibility of $|E(\mathbb{F}_p)|$ for $p \equiv a \pmod b$. Moreover we will give three elliptic curves E for which $|E(\mathbb{F}_p)|$ is divisible by 3 if $p \equiv a \pmod b$ for some a, b.

Acknowledgments I am grateful to my supervisor Yuichiro Taguchi for comments, corrections, and suggestions on this research. I am also grateful to Takakazu Satoh for comments and corrections.

2. Conjectures of Koblitz and Zywina

In this section we recall the conjectures of Koblitz and Zywina.

2.1. Koblitz's conjecture

Before presenting Koblitz's conjecture, let us recall the following arguments[1] on the probability that both p and $(p-1)/2$ are prime for a random prime p, because this is used in §3.2.2. The heuristic argument is as follows: For an odd prime ℓ such that $\ell \neq p$,

$$P(\ell \nmid (p-1)/2 \mid p\colon \text{prime}) = 1 - \frac{1}{\ell - 1},$$
$$P(\ell \nmid n) = 1 - \frac{1}{\ell},$$

and

$$P((p-1)/2\colon \text{prime} \mid p\colon \text{prime}) \approx P(n\colon \text{prime}) \times \prod_{\ell \geqq 3} \frac{P(\ell \nmid (p-1)/2 \mid p\colon \text{prime})}{P(\ell \nmid n)},$$

where $P(\mathrm{A})$ is the probability that A happens and $P(\mathrm{A} \mid \mathrm{B})$ is the probability that A happens under the hypothesis that B has happened. Note that $P(n\colon \text{prime})$ (resp. $P(\ell \nmid n)$) is the probability that a random natural number n is prime (resp. not divisible by a prime ℓ). For other argument of this type, see [9].

Now, we explain Koblitz's conjecture. Because of the prime number theorem, a large random natural number n is prime with probability $1/\log n$. It implies that if $|E(\mathbb{F}_p)|$ behaves like a random integer when p varies, then $|E(\mathbb{F}_p)|$ is prime with probability

$$\frac{1}{\log |E(\mathbb{F}_p)|} = \frac{1}{\log(p+1-t)} \approx \frac{1}{\log(p+1)}. \tag{4}$$

The last approximation is justified because $|t| \leqq 2\sqrt{p}$ ($t := |E(\mathbb{F}_p)| - (p+1)$) by Hasse's theorem. Thus we can expect the probability that p and $|E(\mathbb{F}_p)|$ are both prime is $\frac{1}{(\log p)\log(p+1)} \approx \frac{1}{(\log p)^2}$ and so we can expect the number of such primes $p \leqq x$ is asymptotic to

$$\frac{x}{(\log x)^2} \quad \text{as } x \to \infty.$$

However, $|E(\mathbb{F}_p)|$ does not behave like a random integer. For example, the probability that a random natural number is prime to an integer m is $\Pi_{\ell \mid m}(1 - \frac{1}{\ell})$ and we denote it by P_m. But, the probability that $|E(\mathbb{F}_p)|$ is prime to m is not always equal to P_m. To explain it we recall the following theorem called the Chebotarev density theorem.

Theorem 1. *Let L/K be a (finite) Galois extension of number fields and let $\mathcal{C} \subseteq \mathrm{Gal}(L/K)$ be any subset which is stable by $\mathrm{Gal}(L/K)$-conjugation. For each $\mathfrak{p} \in \Sigma_K$ which is unramified in L, let $\mathrm{Frob}_\mathfrak{p} \subseteq \mathrm{Gal}(L/K)$ denote the conjugacy class of the Frobenius element attached to any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$. Then*

$$\lim_{x \to \infty} \frac{|\{\mathfrak{p} \in \Sigma_K(x) \mid \mathfrak{p} \text{ is unramified in } L,\ \mathrm{Frob}_\mathfrak{p} \subseteq \mathcal{C}\}|}{|\Sigma_K(x)|} = \frac{|\mathcal{C}|}{|\mathrm{Gal}(L/K)|}.$$

Proof. See [15]. □

This theorem says that the probability that a randomly chosen prime ideal $\mathfrak{p}$ satisfies $\mathrm{Frob}_\mathfrak{p} \subseteq \mathcal{C}$ is $\frac{|\mathcal{C}|}{|\mathrm{Gal}(L/K)|}$.

We denote $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by $G_\mathbb{Q}$. Because $G_\mathbb{Q}$ acts on $E[m]$ in a natural way, there is a Galois representaion

$$\rho_m\colon G_\mathbb{Q} \longrightarrow \mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}).$$

We denote $\mathrm{Im}\,\rho_m$ and $GL_2(\mathbb{Z}/m\mathbb{Z})$ by $G(m)$ and G_m respectively. Identitying $\mathrm{Aut}(E[m])$ with G_m we consider

[1] This is similar to that for twin primes conjecture by Hardy and Littlewood.

$G(m)$ as a subgroup of G_m. It is obvious that $\operatorname{Ker}\rho_m$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[m]))$ where the field $\mathbb{Q}(E[m])$ is obtained from $\mathbb{Q}$ by adjoining the coordinates of all points of $E[m]$. Thus we have an isomorphism $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \cong G(m) \subseteq G_m$. For each prime $p \nmid m$ such that E has good reduction at p, ρ_m is unramified at p (i.e., p is unramified in $\mathbb{Q}(E[m])$) and $\rho_m(\mathrm{Frob}_p)$ will denote the corresponding Frobenius conjugacy class in $G(m)$. Then we have a congruence

$$|E(\mathbb{F}_p)| \equiv \det(I_2 - \rho_m(\mathrm{Frob}_p)) \pmod{m}, \tag{5}$$

where I_2 is the identity of G_m (See [13]). It follows from (5) that $|E(\mathbb{F}_p)|$ is prime to m if and only if $\rho_m(\mathrm{Frob}_p) \bmod \ell$ does not have an eigenvalue 1 for all prime divisor ℓ of m. (Note that even if we replace $\mathbb{Q}$, p and E by K, $\mathfrak{p}$ and E_K respectively, the above fact about Galois representaions is correct.) Thus the probability that $|E(\mathbb{F}_p)|$ is prime to m, is

$$P_{E,m} := \frac{|\{A \in G(m) \mid \det(I_2 - A) \in (\mathbb{Z}/m\mathbb{Z})^\times\}|}{|G_m|}$$

by Theorem 1. If m is prime and ρ_m is surjective, then one can check that $P_{E,m} = (1 - \frac{(m-2)(m^2+m)+m^2}{m(m-1)^2(m+1)}) \neq P_m = 1 - \frac{1}{m}$.

Then Koblitz assumed to be

$$P_{E,m} = \prod_{\ell \mid m} P_{E,\ell}. \tag{6}$$

and defined the constant $C_E := \prod_{\ell \geqq 3} \frac{P_{E,\ell}}{P_\ell}$. So Koblitz conjectured as in (1) by similar arguments as in the beginning of this section.

2.2. Zywina's conjecture

Koblitz further conjectured that C_E is positive if and only if E is not $\mathbb{Q}$-isogenous to an elliptic curve which has non-trivial $\mathbb{Q}$-torsion points. However, this is not true. The reason is as follows. For distinct primes ℓ_1 and ℓ_2, $\mathbb{Q}(E[\ell_1])$ and $\mathbb{Q}(E[\ell_2])$ are not necessarily linearly disjoint over $\mathbb{Q}$, because $\mathbb{Q}(E[\ell_1]) \cap \mathbb{Q}(E[\ell_2])$ is not always equal to $\mathbb{Q}$. Thus $\mathrm{Gal}(\mathbb{Q}(E[\ell_1\ell_2])/\mathbb{Q})$ is not always isomorphic to $\mathrm{Gal}(\mathbb{Q}(E[\ell_1])/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(E[\ell_2])/\mathbb{Q})$. So even if $G_{\ell_1\ell_2}$ is isomorphic to $G_{\ell_1} \times G_{\ell_2}$, $G(\ell_1\ell_2)$ is not always isomorphic to $G(\ell_1) \times G(\ell_2)$. So (6) is not always correct and such an example is given in [16].

Now, we start to explain Zywina's conjecture. For $m \geqq 1$ and a positive integer t, he defined the set

$$\psi_t(m) := \{A \in G(m) \mid \det(I_2 - A) \in t \cdot (\mathbb{Z}/m\mathbb{Z})^\times\}.$$

For a prime $\mathfrak{p} \in \Sigma_K - S_{E_K}$ with $\mathfrak{p} \nmid m$, we find that $|E_K(\mathbb{F}_\mathfrak{p})|/t$ is invertible mod $\frac{m}{\gcd(t,m)}$ if and only if $\rho_m(\mathrm{Frob}_\mathfrak{p}) \subseteq G(m) \cap \psi_t(m)$. In particular, $|E_K(\mathbb{F}_\mathfrak{p})|/t$ is an integer if and only if $\rho_t(\mathrm{Frob}_\mathfrak{p}) \subseteq G(t) \cap \psi_t(t)$. Define the constant

$$\delta_{E_K,t}(m) := \frac{|\psi_t(m)|}{|G(m)|}.$$

By Theorem 1, this constant is the probability that $|E_K(\mathbb{F}_\mathfrak{p})|/t$ is invertible mod $\frac{m}{\gcd(t,m)}$ for a random $\mathfrak{p} \in \Sigma_K - S_{E_K}$ and so he defined the constant

$$C_{E_K,t} := \lim_{m \to \infty} \frac{\delta_{E_K,t}(m)}{P_m},$$

where the limit runs over all positive integers ordered by divisibility. So he conjectured like (2).

Remark 1. If $|E_K(\mathbb{F}_\mathfrak{p})|/t$ is an integer, then to check that it is invertible mod m we need only verify that it is invertible mod $\prod_{\ell \mid m} \ell$. So to check if $|E_K(\mathbb{F}_\mathfrak{p})|/t$ is an integer that is relatively prime to m, we need only consider the value of $|E_K(\mathbb{F}_\mathfrak{p})| \bmod t\prod_{\ell \mid m} \ell$. For each m, we have $\delta_{E_K,t}(tm) = \delta_{E_K,t}(t\prod_{\ell \mid m} \ell)$, so an equivalent definition of his constant is

$$C_{E_K,t} := \lim_{Q \to \infty} \frac{\delta_{E_K,t}(t\prod_{\ell \leqq Q} \ell)}{\prod_{\ell \leqq Q}(1 - 1/\ell)}.$$

By definition of $C_{E_K,t}$, we have $C_{E_K,t} = 0$ if and only if $\delta_{E_K,t}(m) = 0$ for some m, so he also conjectured as follows.

Conjecture 2. *Let E_K be an elliptic curve over a number field K and t a positive integer. There are infinitely many $\mathfrak{p} \in \Sigma_K$ for which $|E_K(\mathbb{F}_\mathfrak{p})|/t$ is a prime integer if and only if there are no "congruence obstructions," i.e., for every $m \geqq 1$ there exists a prime $\mathfrak{p} \in \Sigma_K - S_{E_K}$ with $\mathfrak{p} \nmid m$ such that $|E_K(\mathbb{F}_\mathfrak{p})|/t$ is invertible mod m.*

2.2.1. Calculation of $C_{E_K,t}$

First, we assume that E_K is an elliptic curve without complex multiplication.

As we explained in the Introduction, Zywina use the following theorem which was proved by Serre, to calculate his constant.

Theorem 2. *Let E_K/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*

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

Proof. See [14]. □

Proposition 1. *Let E_K/K be an elliptic curve without complex multiplication and t a positive integer. Let M be a positive integer such that*

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

for all square-free m (in particular, one can take M as in Theorem 2). Then

$$C_{E_K,t} = \frac{\delta_{E_K,t}(t\prod_{\ell \mid tM} \ell)}{\prod_{\ell \mid tM} P_\ell} \prod_{\ell \nmid tM} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right).$$

Proof. See [16]. □

By this proposition, it suffices to find M and then calculate $\delta_{E_K,t}(\Pi_{\ell\nmid tM}\ell)$.

Next, we assume that E_K has complex multiplication. Let $R := \mathrm{End}_{\overline{K}}(E_K)$ and $F := R\otimes_{\mathbb{Z}}\mathbb{Q}$, then R is an order of the imaginary quadratic field F. For each positive integer m, we have a natural action of R/mR on $E_K[m]$. $E_K[m]$ is a free R/mR-module of rank 1, so we have a canonical isomorphism $\mathrm{Aut}_{R/mR}(E_K[m]) = (R/mR)^\times$. If all the endomorphism of E_K are defined over K, then the actions of R and G_K on $E_K[m]$ commute, and so we may consider $\rho_m(G_K)$ to be a subgroup of $(R/mR)^\times$.

Proposition 2. *Let E_K/K be an elliptic curve with complex multiplication. Assume that all the endomorphism of E_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 Mm, then*

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

Proof. See [16]. □

Proposition 3. *Let E_K/K be an elliptic curve with complex multiplication. Assume that all the endomorphism of E_K are defined over K. Let χ be the Kronecker character corresponding to F. Let M be a positive integer as in Proposition 2 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*

$$C_{E_K,t} = \frac{\delta_{E_K,t}(t\prod_{\ell\nmid tM}\ell)}{\prod_{\ell\mid tM}P_\ell}\prod_{\ell\nmid tM}\left(1-\chi(\ell)\frac{\ell^2-\ell-1}{(\ell-\chi(\ell))(\ell-1)^2}\right).$$

Proof. See [16]. □

3. Conjecture with congruence condition

In this section we define the constant $C_{E,t,a,b}$ which appear in our Conjecture 1, and give explicit presentations of it (Theorems 3 and 4). We treat the non-CM and CM cases separately.

3.1. The constant $C_{E,t,a,b}$ in the non-CM case

Suppose that E does not have complex multiplication. Suppose that t is a positive integer and b has the prime factorization

$$b = \prod_{\ell\mid b}\ell^{r(\ell)}.$$

We define several sets used in our conjecture

$$G_a(\ell^n) := \{A\in G(\ell^n)\mid \det(A) = a\},$$
$$G_{a,t}(\ell^n) := G_a(\ell^n)\cap\psi_t(\ell^n),$$
$$\psi_{a,b,t}(m) :=$$
$$\{A\in\psi_t(m)\mid A \bmod \ell^n\in G_a(\ell^n)\text{ for all }\ell^n\|\gcd(b,m)\},$$
$$\Sigma_{a,b} := \{p\colon\text{ prime}\mid p\equiv a\ (\mathrm{mod}\ b)\},$$

where m is a positive integer. Let $m(z) = \prod_{\ell\leqq z,\ell\mid b}\ell^{r(\ell)}\prod_{\ell\leqq z,\ell\nmid b}\ell$ where z is a positive integer. We assume that $z>\max(t,b,M)$ where M is a square-free integer which occurs in Proposition 2. Then $|E(\mathbb{F}_p)|/t$ is an integer, relatively prime to $m(z)$ and $p\equiv a \bmod b$ if and only if $\rho_{tm(z)}(\mathrm{Frob}_p)\subseteq\psi_{a,b,t}(tm(z))$. Thus the constant

$$\frac{|\psi_{a,b,t}(tm(z))|}{|G(tm(z))|}$$

is the probability that, for a random p, $|E(\mathbb{F}_p)|/t$ is an integer, relatively prime to $m(z)$ and $p\equiv a \bmod b$. So the probability that for a random $p\in\Sigma_{a,b}$, $|E(\mathbb{F}_p)|/t$ is an integer and relatively prime to $m(z)$ is $\varphi(b)\frac{|\psi_{a,b,t}(tm(z))|}{|G(tm(z))|}$. So we define

$$C'_{E,t,a,b} := \lim_{z\to\infty}\frac{\varphi(b)\frac{|\psi_{a,b,t}(tm(z))|}{|G(tm(z))|}}{\prod_{\ell\mid m(z)}P_\ell}.$$

We also define

$$C_{E,t,a,b} := \lim_{z\to\infty}\frac{\varphi(b)\frac{|\psi_{a,b,t}(tm(z))|}{|G(tm(z))|}}{\delta_{E,t}(tm(z))}. \tag{7}$$

By Remark 1, we have $\delta_{E,t}(tm(z)) = \delta_{E,t}(t\prod_{\ell\leqq z}\ell)$ and so

$$C'_{E,t,a,b} = C_{E,t,a,b}C_{E,t}.$$

We conjecture that, in the non-CM case, Conjecture 1 holds with this $C_{E,t,a,b}$.

Theorem 3. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Let M be a constant which occurs in Proposition 2. For each positive integers a, $b = \prod_{\ell\mid b}\ell^{r(\ell)}$ and t with $\gcd(a,b)=1$, we define*

$$C''_{E,t,a,b} := \frac{\prod_{\ell\mid\gcd(Mt,b)}(\ell^{r(\ell)}-\ell^{r(\ell)-1})}{|\psi_t(t\prod_{\ell\mid Mt,\ell\nmid b}\ell\prod_{\ell\mid\gcd(Mt,b)}\ell^{r(\ell)})|}$$
$$\times\left|\psi_{a,b,t}\left(t\prod_{\ell\mid Mt,\ell\nmid b}\ell\prod_{\ell\mid\gcd(Mt,b)}\ell^{r(\ell)}\right)\right|$$

Then the constant $C_{E,t,a,b}$ which is defined as above is calculated as follows:

$$C_{E,t,a,b} = \begin{cases} C''_{E,t,1,b}\prod_{\ell\mid b,\ell\nmid Mt}\frac{(\ell-1)(\ell^2-\ell-1)}{\ell^3-2\ell^2-\ell+3} & \text{if } a=1,\\ C''_{E,t,a,b}\prod_{\ell\mid b,\ell\nmid Mt}\frac{(\ell^2-1)(\ell-2)}{\ell^3-2\ell^2-\ell+3} & \text{if } a\neq 1.\end{cases} \tag{8}$$

Proof. First, we identify $\psi_{a,b,t}(tm(z))$ with the direct product set

$$\prod_{\ell\nmid btM}\psi_t(\ell)\times\prod_{\ell\mid b,\ell\nmid tM}G_{a,t}(\ell^{r(\ell)})$$
$$\times\psi_{a,b,t}\left(t\prod_{\ell\mid Mt,\ell\nmid b}\ell\prod_{\ell\mid\gcd(Mt,b)}\ell^{r(\ell)}\right),$$

where ℓ runs over all $\ell\mid m(z)$. There are ℓ^{n-1} ways to lift an element of $\mathbb{Z}/\ell\mathbb{Z}$ to elements of $\mathbb{Z}/\ell^n\mathbb{Z}$. Thus $G(\ell^n) = G_{\ell^n}$ for all $n\geqq 1$, if $\ell\nmid tM$ and we have

$$\frac{|G_{a,t}(\ell^n)|}{|\psi_t(\ell^n)|} = \frac{\ell^{3(n-1)}|G_{a,t}(\ell)|}{\ell^{4(n-1)}|\psi_t(\ell)|} = \frac{|G_{a,t}(\ell)|}{\ell^{n-1}|\psi_t(\ell)|}.$$

Thus we have

$$\begin{aligned}C_{E,t,a,b} &= \lim_{z\to\infty}\frac{\varphi(b)|\psi_{a,b,t}(tm(z))|}{|\psi_t(tm(z))|}\\ &= \frac{|\psi_{a,b,t}(t\prod_{\ell|Mt,\ell\nmid b}\ell\prod_{\ell|\gcd(Mt,b)}\ell^{r(\ell)})|}{|\psi_t(t\prod_{\ell|Mt,\ell\nmid b}\ell\prod_{\ell|\gcd(Mt,b)}\ell^{r(\ell)})|}\\ &\quad\times\prod_{\ell|b}(\ell^{r(\ell)}-\ell^{r(\ell)-1})\prod_{\ell|b,\ell\nmid tM}\frac{|G_{a,t}(\ell^{r(\ell)})|}{|\psi_t(\ell^{r(\ell)})|}\\ &= C''_{E,t,a,b}\prod_{\ell|b,\ell\nmid tM}(\ell^{r(\ell)}-\ell^{r(\ell)-1})\frac{|G_{a,t}(\ell)|}{\ell^{r(\ell)-1}|\psi_t(\ell)|}\\ &= C''_{E,t,a,b}\prod_{\ell|b,\ell\nmid tM}\frac{(\ell-1)|G_{a,t}(\ell)|}{|\psi_t(\ell)|}.\end{aligned}$$

Note that if $\gcd(Mt,b)=1$, then $C''_{E,t,a,b}=1$. The rest of proof of this theorem follows from the next lemmas and proposition. □

Lemma 1. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. For each positive integers a, $b=\prod_{\ell|b}\ell^{r(\ell)}$ and t with $\gcd(a,b)=1$, we have*

$$C_{E,t,a,b}=C''_{E,t,a,b}\prod_{\ell|b,\ell\nmid Mt}C_{E,1,a,\ell}.$$

Proof. We note that if $\gcd(m,t)=1$, then $\psi_t(m)=\psi_1(m)$. Thus the assertion is clear from the definition of $C_{E,t,a,b}$. □

Lemma 2. **(i)** *For $a\in(\mathbb{Z}/\ell\mathbb{Z})^\times$, we have*

$$|\{A\in G_\ell \mid A \text{ has eigenvalues } 1 \text{ and } a\}| = \begin{cases}\ell^2+\ell & \text{if } a\neq 1,\\ \ell^2 & \text{if } a=1.\end{cases}$$

(ii) *If $\ell\neq 2$, then for all $d\in(\mathbb{Z}/\ell\mathbb{Z})^\times$ and $t\in\mathbb{Z}/\ell\mathbb{Z}$, we have*

$$|\{A\in G_\ell \mid \det(A)=d,\mathrm{tr}(A)=t\}| = \ell\left(\ell+\left(\frac{t^2-4d}{\ell}\right)\right),$$

where $\left(\frac{\cdot}{\ell}\right)$ is the Legendre symbol.

Proof. See Table 12.4 in [7, XVIII] □

Lemma 3. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication, Let M be a constant which occurs in Proposition 2 and t a positive integer. If $\ell\nmid tM$, then we have*

(i)

$$|G_{a,t}(\ell)|=|G_{a,1}(\ell)|=\begin{cases}\ell(\ell^2-1)-\ell^2 & \text{if } a=1,\\ \ell(\ell^2-1)-\ell(\ell+1) & \text{if } a\neq 1.\end{cases}$$

(ii) $|\psi_t(\ell)|=|\psi_1(\ell)|=\ell(\ell^2-1)(\ell-1)-\ell^2-(\ell-2)(\ell^2+\ell)$.

Proof. Because $G_a=\ell(\ell^2-1)$ for all $a\in(\mathbb{Z}/\ell\mathbb{Z})^\times$, the result is clear from Lemma 2. □

Proposition 4. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication, Let M be the constant which occurs in Proposition 2 and t a positive integer. If $\ell\nmid tM$, then we have*

$$C_{E,1,a,\ell}=\begin{cases}\frac{(\ell-1)(\ell^2-\ell-1)}{\ell^3-2\ell^2-\ell+3} & \text{if } a=1,\\ \frac{(\ell^2-1)(\ell-2)}{\ell^3-2\ell^2-\ell+3} & \text{if } a\neq 1.\end{cases}$$

Proof. By Lemma 3 and the definition of $C_{E,1,a,\ell}$,

$$C_{E,1,1,\ell}=\frac{(\ell-1)|G_{1,1}(\ell)|}{|\psi_1(\ell)|}=\frac{(\ell-1)(\ell^2-\ell-1)}{\ell^3-2\ell^2-\ell+3}.$$

Similarly, we get the formula for $a\neq 1$. □

3.2. The constant $C_{E,t,a,b}$ in the CM case

Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication. We use the following notation throughout this section.

$R:=\mathrm{End}_{\overline{\mathbb{Q}}}(E)$, $F:=R\otimes_{\mathbb{Z}}\mathbb{Q}$, and $F\cong\mathbb{Q}(\sqrt{D})$ with square-free D.

Moreover, let M be the constant determined for E from Proposition 3. It is well-known that $R\cong\mathbb{Z}+\mathbb{Z}f\alpha$ where f is a positive integer called the conductor of R and

$$\alpha=\begin{cases}\sqrt{D} & \text{if } D\equiv 2,\ 3\pmod 4,\\ \frac{1+\sqrt{D}}{2} & \text{if } D\equiv 1\pmod 4.\end{cases}$$

We want to use Proposition 2 to define $C_{E,t,a,b}$. However, not all the endomorphisms of E are defined over $\mathbb{Q}$. So we consider E as an elliptic curve over F. Let $\Sigma^{\mathrm{split}}_{F,a,b}$ be the set of prime ideal $\mathfrak{p}$ of O_F such that $N_F(\mathfrak{p})=p\equiv a\pmod b$ and $\Sigma^{\mathrm{split}}_{F,a,b}(x)$ the set of prime ideal $\mathfrak{p}\in\Sigma^{\mathrm{split}}_{F,a,b}$ suth that $N_F(\mathfrak{p})\leqq x$ (note that we do not consider primes which ramify in F, because such primes are finitely many). Let $\pi^{\mathrm{split}}_{E_F,t,a,b}(x)$ be the number of prime ideal $\mathfrak{p}\in\Sigma^{\mathrm{split}}_{F,a,b}(x)$ such that E has good reduction at $\mathfrak{p}$, $|E(\mathbb{F}_\mathfrak{p})|$ is divisible by t and $|E(\mathbb{F}_\mathfrak{p})|/t$ is a prime. Let $\pi^{\mathrm{split}}_{E,F,t,a,b}(x)$ be the number of prime number $p\in\pi_{a,b}(x)$ such that p splits completely in F, E has good reduction at p, $|E(\mathbb{F}_p)|$ is divisible by t and $|E(\mathbb{F}_p)|/t$ is a prime. We also define $\Sigma^{\mathrm{inert}}_{F,a,b}$, $\Sigma^{\mathrm{inert}}_{F,a,b}(x)$ and $\pi^{\mathrm{inert}}_{E,F,t,a,b}(x)$ in the similar way. If p spilits completely in F and $pO_F=\mathfrak{p}_1\mathfrak{p}_2$, then $E(\mathbb{F}_p)\cong E(\mathbb{F}_{\mathfrak{p}_i})$. Thus

$$\begin{aligned}\pi_{E,t,a,b}(x)&=\pi^{\mathrm{split}}_{E,F,t,a,b}(x)+\pi^{\mathrm{inert}}_{E,F,t,a,b}(x)+O(1),\\ \pi^{\mathrm{split}}_{E,F,t,a,b}(x)&=\frac{1}{2}\pi^{\mathrm{split}}_{E_F,t,a,b}(x),\end{aligned}$$

and we conjecture as follows:

$$\pi^{\mathrm{split}}_{E_F,t,a,b}(x)\sim C^{\mathrm{split}}_{E_F,t,a,b}\pi_{E_F,t}(x)\sim C^{\mathrm{split}}_{E_F,t,a,b}C_{E_F,t}\frac{x}{(\log x)^2},$$

$$\pi^{\mathrm{inert}}_{E,F,t,a,b}(x)\sim C^{\mathrm{inert}}_{t,a,b}\frac{x}{(\log x)^2},$$

$$\pi_{E,t,a,b}(x)\sim\left(\frac{1}{2}C^{\mathrm{split}}_{E_F,t,a,b}C_{E_F,t}+C^{\mathrm{inert}}_{t,a,b}\right)\frac{x}{(\log x)^2},$$

as $x \to \infty$. So we define

$$C_{E,t,a,b} := \begin{cases} \varphi(b)\frac{\frac{1}{2}C^{\mathrm{split}}_{E_F,t,a,b}C_{E_F,t}+C^{\mathrm{inert}}_{t,a,b}}{C_{E,t}} & \text{if } C_{E,t} \neq 0, \\ 0 & \text{if } C_{E,t} = 0. \end{cases} \quad (9)$$

We conjecture that, in the CM case, Conjecture 1 holds with this $C_{E,t,a,b}$.

Theorem 4. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication. Let $a, b = \prod_{\ell|b} \ell^{r(\ell)}$ and t be positive integers with $\gcd(a,b) = 1$. We define*

$$C''_{E,t,a,b} := \frac{|\psi_{a,b,t}(t\prod_{\ell|Mt,\ell\nmid b}\ell\prod_{\ell|\gcd(Mt,b)}\ell^{r(\ell)})|}{|\psi_t(t\prod_{\ell|Mt,\ell\nmid b}\ell\prod_{\ell|\gcd(Mt,b)}\ell^{r(\ell)})|}.$$

Then the following holds:

(i) *The constant $C^{\mathrm{split}}_{E_F,t,a,b}$ which is defined as above is expressed as follows:*

$$C^{\mathrm{split}}_{E_F,t,a,b} = C''_{E,t,1,b}\prod_{\ell\nmid Mt,\ell|b} C^{\mathrm{split}}_{E_F,t,a,\ell^{r(\ell)}},$$

and $C^{\mathrm{split}}_{E_F,t,a,\ell^{r(\ell)}}$ is determined by the value of $\left(\frac{D}{\ell}\right)$ as follows:

(i-i) *if $\left(\frac{D}{\ell}\right) = 1$, then for all $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ we have*

$$C^{\mathrm{split}}_{E_F,t,a,\ell^{r(\ell)}} = \begin{cases} \prod_{\ell\nmid Mt,\ell|b}\frac{1}{\ell^{r(\ell)-1}(\ell-2)} & \text{if } a = 1, \\ \prod_{\ell\nmid Mt,\ell|b}\frac{\ell-3}{\ell^{r(\ell)-1}(\ell-2)^2} & \text{if } a \neq 1. \end{cases}$$

(i-ii) *if $\left(\frac{D}{\ell}\right) = -1$, then for all $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ we have*

$$C^{\mathrm{split}}_{E_F,t,a,\ell^{r(\ell)}} = \begin{cases} \prod_{\ell\nmid Mt,\ell|b}\frac{\ell}{\ell^{r(\ell)-1}(\ell^2-2)} & \text{if } a = 1, \\ \prod_{\ell\nmid Mt,\ell|b}\frac{\ell+1}{\ell^{r(\ell)-1}(\ell^2-2)} & \text{if } a \neq 1. \end{cases}$$

(ii) *Let f_F be the conductor of F. Define integers d, f'_E, e, f', t', h, t'' successively by*

$$\gcd(b, f_F) = d, \quad f_F = df'_F,$$
$$\gcd(bf'_F, t) = e, \quad bf'_F = f'e, \quad t = t'e,$$
$$\gcd(e, t') = h, \quad t' = t''h.$$

Let J be a subset of $(\mathbb{Z}/bf'_F\mathbb{Z})^\times$ which consists of classes of primes p satisfying $p \equiv a \pmod b$ and $\chi_F(p) = -1$ where χ_F is the Kronecker character associated to F. Then the constant $C^{\mathrm{inert}}_{t,a,b}$ is given by

$$C^{\mathrm{inert}}_{t,a,b} = \frac{1}{\varphi(bf'_F)}\sum_{c\in J} C_{c,bf'_F,t},$$

where $C_{c,bf'_F,t}$ is given as follows: There are integers α_i $(i \in J)$ and we have; If $e \nmid (1+c)$ or $\ell \mid f'$ and $t\ell \mid (1+c)$ for some prime ℓ, then $C_{c,bf'_F,t} = 0$. Otherwise we have

$$C_{c_i,bf'_F,t} = \begin{cases} \frac{1}{\varphi(t'')h}\prod_{\ell\nmid bf'_Ft'}\frac{\ell(\ell-2)}{(\ell-1)^2}\prod_{\ell|f'}\frac{\ell}{\ell-1} & \text{if } t \mid (\alpha_i+1), \\ \frac{1}{\varphi(t'')h}\prod_{\ell\nmid bf'_Ft'}\frac{\ell(\ell-2)}{(\ell-1)^2}\prod_{\ell|bf'_Ft'}\frac{\ell}{\ell-1} & \text{if } t \nmid (\alpha_i+1). \end{cases}$$

We prove this theorem in §3.2.1 and §3.2.2.

3.2.1. Calculation of $C^{\mathrm{split}}_{E,t,a,b}$

The following lemma is an easy corollary of class field theory.

Lemma 4. *Let f_F be the conductor of F. Then there are integers $a_1, a_2, \ldots, a_{\frac{\varphi(f_F)}{2}}$ with $a_i \not\equiv a_j \pmod{f_F}$ $(i \neq j)$ such that for each $p \nmid f_F D$, p splits completely in F if and only if $p \equiv a_i \pmod{f_F}$ for some i where $\varphi(\cdot)$ is the Euler function.*

By this lemma, the probability that p splits completely in F and the probability that p is inert in F are $\frac{1}{2}$, respectively. Thus by the prime number theorem, we have

$$|\Sigma^{\mathrm{split}}_{F,0,1}(x)| \sim \frac{1}{2}\frac{2x}{\log x} = \frac{x}{\log x},$$
$$|\Sigma^{\mathrm{inert}}_{F,0,1}(x)| \sim \frac{1}{2}\frac{\sqrt{x}}{\log\sqrt{x}} = \frac{\sqrt{x}}{\log x},$$

and so

$$|\Sigma_F(x)| \sim \frac{x+\sqrt{x}}{\log x}, \qquad \frac{|\Sigma^{\mathrm{inert}}_{F,0,1}(x)|}{|\Sigma_F(x)|} \to 0,$$

as $x \to \infty$. This means that if $z > \max(t, M, b)$, then we may consider $\frac{|\psi_{t,a,b}(tm(z))|}{|G(tm(z))|}$ to be the probability that a random $\mathfrak{p}$ is in $\Sigma^{\mathrm{split}}_{F,a,b}(x)$ and such that $|E(\mathbb{F}_\mathfrak{p})|/t$ is an integer which is relatively prime to $m(z)$. So we define

$$C^{\mathrm{split}}_{E_F,t,a,b} := \lim_{z\to\infty}\frac{\frac{|\psi_{t,a,b}(tm(z))|}{|G(tm(z))|}}{\delta_{E_F,t}(tm(z))}.$$

From now on, we assume that any prime factor of $2fd_F$ also divides M as in Proposition 3 where d_F is the discriminant of F. By Proposition 2, if $\ell \nmid M$, then $G(\ell^n) \cong (R/\ell^nR)^\times$ for each $n \geqq 1$ and $(R/\ell^nR)^\times$ is isomorphic to a Cartan subgroup of G_{ℓ^n}. More precisely, if $\left(\frac{D}{\ell}\right) = 1$, then $(R/\ell^nR)^\times$ is isomorphic to a split Cartan subgroup and if $\left(\frac{D}{\ell}\right) = -1$, then $(R/\ell^nR)^\times$ is isomorphic to a non-split Cartan subgroup. We denote one of the split and non-split Cartan subgroups of G_{ℓ^n} by $C^{\mathrm{s}}_{\ell^n}$ and $C^{\mathrm{ns}}_{\ell^n}$, respectively. We can represent $C^{\mathrm{s}}_{\ell^n}$ and $C^{\mathrm{ns}}_{\ell^n}$ as a group of diagonal matrices and the matrices representing the multiplication by a element of $(R/\ell^nR)^\times$ when we write it in some $\mathbb{Z}/\ell^n\mathbb{Z}$-base as a free $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank 2. So when the $\mathbb{Z}/\ell^n\mathbb{Z}$-basis is $\{1, f\alpha\}$, we have

Lemma 5. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication. If $\ell \nmid M$, then for each $n \geqq 1$ the following holds:*

(i) *In the split case, we have*

$$G(\ell^n) \cong C^{\mathrm{s}}_{\ell^n} \cong \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z}/\ell^n\mathbb{Z}, \\ ab \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \end{array}\right\}.$$

(ii) *In the non-split case,*

(ii-1) *If* $D \equiv 2,\ 3 \pmod 4$, *we have*

$$G(\ell^n) \cong C^{\mathrm{ns}}_{\ell^n} \cong \left\{ \begin{pmatrix} a & bf^2D \\ b & a \end{pmatrix} \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z}/\ell^n\mathbb{Z}, \\ a^2 - b^2 f^2 D \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \end{array} \right\}.$$

(ii-2) *If* $D \equiv 1 \pmod 4$ *and* $D = 4m+1$, *we have*

$$G(\ell^n) \cong C^{\mathrm{ns}}_{\ell^n} \cong \left\{ \begin{pmatrix} a & bf^2m \\ b & a+bf \end{pmatrix} \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z}/\ell^n\mathbb{Z}, \\ a(a+bf) - b^2 f^2 m \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \end{array} \right\}.$$

Since for each $n \geqq 2$, there are ℓ^{n-1} ways to lift an element of $\mathbb{Z}/\ell\mathbb{Z}$ to an element of $\mathbb{Z}/\ell^n\mathbb{Z}$, this lemma implies that, if $\ell \nmid Mt$, then $|G_a(\ell^n)| = |G_1(\ell^n)| = \ell^{n-1}|G_1(\ell)|$ and $|\psi_t(\ell^n)| = \ell^{2(n-1)}|\psi_t(\ell)|$ for each $a \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$. Thus if $\ell \nmid Mt$, then

$$\frac{|G_{a,t}(\ell^n)|}{|\psi_t(\ell^n)|} = \frac{|G_{a,1}(\ell^n)|}{|\psi_1(\ell^n)|} = \frac{\ell^{n-1}|G_{a,1}(\ell)|}{\ell^{2(n-1)}|\psi_1(\ell)|} = \frac{|G_{a,1}(\ell)|}{\ell^{n-1}|\psi_1(\ell)|}.$$

Thus we have

$$C^{\mathrm{split}}_{E_F,t,a,b} = C''_{E,t,a,b} \prod_{\ell \mid b, \ell \nmid tM} \frac{|G_{a,1}(\ell)|}{\ell^{r(\ell)-1}|\psi_1(\ell)|},$$

where $b = \prod_{\ell \mid b} \ell^{r(\ell)}$. Thus we have the next lemma.

Lemma 6. *Let* E *be an elliptic curve defined over* $\mathbb{Q}$ *with complex multiplication and let* $a,\ b = \prod_{\ell \mid b} \ell^{r(\ell)}$ *and* t *be positive integers with* $\gcd(a,b) = 1$. *Then*

$$C^{\mathrm{split}}_{E_F,t,a,b} = C''_{E,t,a,b} \prod_{\ell \nmid Mt, \ell \mid b} C^{\mathrm{split}}_{E_F,1,a,\ell^{r(\ell)}}.$$

Lemma 7. *Let* E *be an elliptic curve defined over* $\mathbb{Q}$ *with complex multiplication. Let* t *be a positive integer. Suppose that* $\ell \nmid Mt$.

(i) *If* $\left(\frac{D}{\ell}\right) = 1$, *then for all* $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ *we have*

$$|\psi_t(\ell)| = |\psi_1(\ell)| = (\ell-2)^2,$$
$$|G_{a,t}(\ell)| = |G_{a,1}(\ell)| = \begin{cases} \ell - 2 & \text{if } a = 1, \\ \ell - 3 & \text{if } a \neq 1. \end{cases}$$

(ii) *If* $\left(\frac{D}{\ell}\right) = -1$, *then for all* $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ *we have*

$$|\psi_t(\ell)| = |\psi_1(\ell)| = \ell^2 - 2,$$
$$|G_{a,t}(\ell)| = |G_{a,1}(\ell)| = \begin{cases} \ell & \text{if } a = 1, \\ \ell + 1 & \text{if } a \neq 1. \end{cases}$$

Proof. Suppose that $\left(\frac{D}{\ell}\right) = 1$. Then $G(\ell) = C^{\mathrm{s}}_\ell$. Thus (i) is clear from Lemma 5. Next, suppose that $\left(\frac{D}{\ell}\right) = -1$ and $D \equiv 1 \pmod 4$. Then $G(\ell) = C^{\mathrm{ns}}_\ell$ and we write $D = 4m+1$. Since $\det\colon C_{ns,\ell} \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ is surjective, $G_a(\ell) = G_1(\ell) = \ell + 1$. Let A be any element of C^{ns}_ℓ and we write $A = \begin{pmatrix} a & bf^2m \\ b & a+bf \end{pmatrix}$. Then if $\det(I_2 - A) = a^2 - (2-bf)a + 1 - bf(1+bfm) = 0$, then $a = \frac{2-bf \pm \sqrt{(2-bf)^2 + 4bf(1+bfm) - 4}}{2} = \frac{2-bf \pm bf\sqrt{D}}{2}$ (note that from the assumption on M, $2 \mid M$. Thus $\ell \neq 2$). Since $\left(\frac{D}{\ell}\right) = -1$ and $\ell \nmid f$, $\det(I_2 - A) = 0$ if and only if $b = 0$ and $a = 1$, i.e., $A = I_2$. It implies that (ii) is correct when $D \equiv 1 \pmod 4$. Similarly, when $D \equiv 2,\ 3 \pmod 4$, we can prove (ii). □

Proposition 5. *Let* E *be an elliptic curve defined over* $\mathbb{Q}$ *with complex multiplication. Let* $a,\ b = \prod_{\ell \mid b} \ell^{r(\ell)}$ *and* t *be positive integers with* $\gcd(a,b) = 1$. *Suppose that* $\ell \nmid Mt$.

(i) *If* $\left(\frac{D}{\ell}\right) = 1$, *then for all* $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$

$$C^{\mathrm{split}}_{E_F,1,a,\ell^{r(\ell)}} = \begin{cases} \frac{1}{\ell^{r(\ell)-1}(\ell-2)} & \text{if } a = 1, \\ \frac{\ell-3}{\ell^{r(\ell)-1}(\ell-2)^2} & \text{if } a \neq 1. \end{cases}$$

(ii) *If* $\left(\frac{D}{\ell}\right) = -1$, *then for all* $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$

$$C^{\mathrm{split}}_{E_F,1,a,\ell^{r(\ell)}} = \begin{cases} \frac{\ell}{\ell^{r(\ell)-1}(\ell^2-2)} & \text{if } a = 1, \\ \frac{\ell+1}{\ell^{r(\ell)-1}(\ell^2-2)} & \text{if } a \neq 1. \end{cases}$$

Proof. This is clear from Lemma 7. □

(i) of Theorem 4 follows from this proposition and Lemma 6.

3.2.2. Calculation of $C^{\mathrm{inert}}_{t,a,b}$

Suppose that $p \nmid f_F D$. In the following, we explain the condition that a prime p is inert in F and $p \equiv a \pmod b$ to calculate $C^{\mathrm{inert}}_{t,a,b}$. By Lemma 4, we can take integers $b_1, b_2, \ldots, b_{\frac{\varphi(f_F)}{2}}$ such that p is inert in F if and only if $p \equiv b_i \pmod{f_F}$. If $\gcd(f_F, b) = 1$, then p is inert in F and $p \equiv a \pmod b$ if and only if $p \equiv c_i \pmod{bf_F}$ where $c_i \equiv b_i \pmod{f_F}$ and $c_i \equiv a \pmod b$. Suppose that $\gcd(f_F, b) = d > 1$, $b = b'd$ and $f_F = f'_F d$. Then $\mathrm{lcm}(f_F, b) = bf'_F = b'f_F$. Then $p \equiv a \pmod b$ if and only if $p \equiv a + \gamma_0 b,\ a + \gamma_1 b, \ldots,$ or $a + \gamma_n b \pmod{bf'_F}$ where $n, \gamma_0, \ldots, \gamma_n$ are integers such that $\gcd(a + \gamma_i b, bf'_F) = 1$ and $\gamma_i \not\equiv \gamma_j \pmod{f'_F}$ for $i \neq j$. Similarly, $p \equiv b_i \pmod{f_F}$ if and only if $p \equiv b_i + \delta_{i,0} f_F, \ldots, b_i + \delta_{i,m} f_F \pmod{b'f_F}$ ($\gcd(a_i + \delta_{i,j} f_F, b'f_F) = 1,\ \delta_{i,j} \not\equiv \delta_{i,k} \pmod{b'}$ for $j \neq k$). So we have to find the condition that there are integers γ_j and $\delta_{i,k}$ such that $a + \gamma_j b \equiv b_i + \delta_{i,k} f_F \pmod{bf'_F}$.

$$\begin{aligned} a + \gamma_j b \equiv b_i + \delta_{i,k} f_F \pmod{bf'_F} &\iff \gamma_j b \equiv b_i - a + \delta_{i,k} f_F \pmod{bf'_F}. \end{aligned}$$

Thus $b_i - a + \delta_{i,k} f_F$ must be divisible by b. So

$$\begin{aligned} b_i - a + \delta_{i,k} f_F \equiv 0 \pmod b &\iff \delta_{i,k} f_F \equiv a - b_i \pmod b. \end{aligned}$$

Thus $a - b_i$ must be divisible by d. If $d \mid (a - b_i)$, then

$$\begin{aligned} \delta_{i,k} f'_F \equiv \frac{a - b_i}{d} \pmod{b'} &\iff \delta_{i,k} \equiv f_F'^{-1} \cdot \frac{a - b_i}{d} \pmod{b'}. \end{aligned}$$

For this $\delta_{i,k}$, $b_i - a + \delta_{i,k} f_F \equiv 0 \pmod{b}$ and so

$$\gamma_j \equiv \frac{b_i - a + \delta_{i,k} f_F}{b} \pmod{f'_F}.$$

Thus if $d \mid (a - b_i)$, then there is an unique element $\alpha_i \in \mathbb{Z}/f'_F\mathbb{Z}$ and $\beta_i \in \mathbb{Z}/b'\mathbb{Z}$ such that p is inert in F and $p \equiv a \pmod{b}$ if and only if $p \equiv a + \alpha_i b \equiv b_i + \beta_i f_F \pmod{bf'_F}$ for some $i = 1, \dots, \frac{\varphi(f_F)}{2}$. So, if $d \mid (a - b_i)$, there is an unique element $\epsilon_i \in \mathbb{Z}/bf'_F\mathbb{Z}$ such that p is inert in F and $p \equiv a \pmod{b}$ if and only if $p \equiv \epsilon_i \pmod{bf'_F}$ for some $i = 1, \dots, \frac{\varphi(f_F)}{2}$. If p is inert in F, then $|E(\mathbb{F}_p)| = p + 1$. Thus we have proved the next lemma.

Lemma 8. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication. Let a, b and t be positive integers with $\gcd(a, b) = 1$. Let f'_F, d and J be integers and the subset of $(\mathbb{Z}/bf'_F\mathbb{Z})^\times$ in Theorem 4 (ii). Let $\pi_{t,a,b}(x)$ be the number of prime numbers $p \leqq x$ such that $(p+1)/t$ is a prime and $p \equiv a \pmod{b}$. Let $I := \{i \in \{1, \dots, \frac{\varphi(f_F)}{2}\} l d \mid (a - b_i)\}$. Then we have $|I| = |J|$ and there are integers c_i, ϵ_i such that*

$$\begin{aligned}
&\pi^{\mathrm{inert}}_{E,F,t,a,b}(x) \\
&= \begin{cases} \sum_{i=1}^{\frac{\varphi(f_F)}{2}} \pi_{t,c_i,bf_F}(x) + O(1) & \text{if } d = 1, \\ \sum_{i \in I} \pi_{t,\epsilon_i,bf'_F}(x) + O(1) & \text{if } d > 1,\ f_F = df'_F, \end{cases} \\
&= \sum_{c \in J} \pi_{t,c,bf'_F}(x) + O(1).
\end{aligned}$$

Lemma 9. *Let b, f'_F, d, e, t' and h be the constants in Theorem 4 (ii). Let J be the subset of $(\mathbb{Z}/bf'_F\mathbb{Z})^\times$ in Theorem 4 (ii). Then for each $c \in J$ we have*

$$\begin{aligned}
&P\big(t \mid (p+1) \,\big|\, p \text{ is a prime, } p \equiv c \pmod{bf'_F}\big) \\
&\qquad = \begin{cases} \frac{1}{\varphi(t'')h} & \text{if } e \mid (1 + c),\ t' = t''h, \\ 0 & \text{if } e \nmid (1 + c). \end{cases}
\end{aligned}$$

Proof. $t \mid (p + 1)$ if and only if $p \equiv -1 \pmod{t}$. First, suppose that $e = 1$. Then by the Chinese Remainder Theorem, there is an unique element $\alpha \in (\mathbb{Z}/bf'_F t\mathbb{Z})^\times$ such that $\alpha \equiv c \pmod{bf'_F}$ and $\alpha \equiv -1 \pmod{t}$. Since $(\mathbb{Z}/bf'_F t\mathbb{Z})^\times \cong (\mathbb{Z}/bf'_F\mathbb{Z})^\times \times (\mathbb{Z}/t\mathbb{Z})^\times$, our claim is correct. Next, suppose that $e > 1$. Then $\mathrm{lcm}(bf'_F, t) = bf'_F t'$. By similar way of proof of Lemma 8, if $e \mid (1 + c)$, we can find an unique element $\beta \in (\mathbb{Z}/bf'_F t'\mathbb{Z})^\times$ such that $\beta \equiv c \pmod{bf'_F}$ amd $\beta \equiv -1 \pmod{t}$. Moreover, there are $\varphi(t'')h$ ways to lift an element of $(\mathbb{Z}/bf'_F\mathbb{Z})^\times$ to an element of $(\mathbb{Z}/bf'_F t'\mathbb{Z})^\times$. Thus we have proved this lemma. □

Lemma 10. *Let b, f'_F, t' and e be the constants in Theorem 4 (ii). Let J be the subset of $(\mathbb{Z}/bf'_F\mathbb{Z})^\times$ in Theorem 4 (ii). Suppose that $e \mid (c + 1)$ for each $c \in J$. Then there is an integer α such that*

$$\begin{aligned}
&P\left(\ell \nmid \frac{p+1}{t} \,\middle|\, p \text{ is a prime, } t \mid (p+1),\ p \equiv c \pmod{bf'_F}\right) \\
&\qquad = P\left(\ell \nmid \frac{p+1}{t} \,\middle|\, p \text{ is a prime, } p \equiv \alpha \pmod{bf'_F t'}\right)
\end{aligned}$$

Proof. This is clear from the proof of Lemma 9. □

Lemma 11. *Let b, f'_F, f' and t' be the constants in Theorem 4. Let J be the subset of $(\mathbb{Z}/bf'_F\mathbb{Z})^\times$ in Theorem 4 (ii). Let α be the integer in Lemma 10.*

$$\begin{aligned}
&P\left(\ell \nmid \frac{p+1}{t} \,\middle|\, p \text{ is a prime, } p \equiv \alpha \pmod{bf'_F t'}\right) \\
&\qquad = \begin{cases} 1 - \frac{1}{\ell - 1} & \text{if } \ell \nmid bf'_F t', \\ 1 - \frac{1}{\ell} & \text{if } \ell \mid t,\ \ell \nmid f',\ t \mid (\alpha + 1), \\ 1 & \text{if } \ell \mid t,\ \ell \nmid f',\ t \nmid (\alpha + 1), \\ 1 & \text{if } \ell \mid f',\ t\ell \nmid (\alpha + 1), \\ 0 & \text{if } \ell \mid f',\ t\ell \mid (\alpha + 1). \end{cases}
\end{aligned}$$

Proof. First, suppose that $e = 1$. We have $\ell \mid \frac{p+1}{t}$ if and only if $p \equiv -1 \pmod{\ell t}$. Suppose that $\ell \nmid bf'_F t'$. In this case this is clear from the Chinese Remainder Theorem. Suppose that $\ell \mid t$, $\ell \nmid f'$. Then $\mathrm{lcm}(bf'_F t', \ell t) = bf'_F \ell t'$. By similar way of proof of Lemma 8, if $t \mid (\alpha + 1)$, we can find an unique element $\lambda \in (\mathbb{Z}/bf'_F \ell t'\mathbb{Z})^\times$ such that $\lambda \equiv \alpha \pmod{bf'_F t'}$ and $\lambda \equiv -1 \pmod{\ell t}$. Moreover, there are ℓ ways to lift an element of $(\mathbb{Z}/bf'_F t'\mathbb{Z})^\times$ to an element of $(\mathbb{Z}/bf'_F \ell t'\mathbb{Z})^\times$. Suppose that $\ell \mid f'$. Then $\ell t \mid bf'_F t'$. It implies that a prime number p satisfied $p \equiv \alpha \pmod{bf'_F t'}$, $p \equiv -1 \pmod{\ell t}$ if and only if $\alpha \equiv -1 \pmod{\ell t}$. Thus we have proved this lemma. □

Now, we describe our conjecture about $\pi_{t,c,bf'_F}(x)$ for each $c \in J$ where J is the subset of $(\mathbb{Z}/bf'_F\mathbb{Z})^\times$ in Theorem 4 (ii). First, we note that

$$\begin{aligned}
&P\left(\frac{p+1}{t} \colon \text{prime} \,\middle|\, p \colon \text{ prime, } p \equiv c \pmod{bf'_F}\right) \\
&= P\big(t \mid (p+1) \,\big|\, p \colon \text{ prime, } p \equiv c \pmod{bf'_F}\big) \\
&\qquad \times P\left(\frac{p+1}{t} \colon \text{prime} \,\middle|\, \begin{array}{l} p \colon \text{ prime, } t \mid (p+1), \\ p \equiv c \pmod{bf'_F} \end{array}\right).
\end{aligned}$$

By Lemma 10 and the arguments at the beginning of Section 2, we have

$$\begin{aligned}
&P\left(\frac{p+1}{t} \colon \text{prime} \,\middle|\, \begin{array}{l} p \colon \text{ prime, } t \mid (p+1), \\ p \equiv c \pmod{bf'_F} \end{array}\right) \\
&= P\left(\frac{p+1}{t} \colon \text{prime} \,\middle|\, p \colon \text{ prime, } p \equiv \alpha \pmod{bf'_F t'}\right) \\
&\approx P(n \colon \text{prime}) \\
&\qquad \times \prod_{\ell \geqq 2} \frac{P\big(\ell \nmid \frac{p+1}{t} \,\big|\, p \colon \text{ prime, } p \equiv \alpha \pmod{bf'_F t'}\big)}{P(\ell \nmid n)},
\end{aligned}$$

where α is the constant in Lemma 10. We define

$$\begin{aligned}
&C_{c,bf'_F,t} \\
&:= P\big(t \mid (p+1) \,\big|\, p \text{ is a prime, } p \equiv c \pmod{bf'_F}\big) \\
&\qquad \times \prod_{\ell \geqq 2} \frac{P\big(\ell \nmid \frac{p+1}{t} \,\big|\, p \text{ is a prime, } p \equiv \alpha \pmod{bf'_F t'}\big)}{P(\ell \nmid n)}.
\end{aligned}$$

We conjecture as follows:

Conjecture 3. *Let $\pi_{t,c,bf'_F}(x)$ be as in the Lemma 8. Then*

$$\pi_{t,c,bf'_F}(x) \sim \frac{C_{c,bf'_F,t}}{\varphi(bf'_F)} \frac{x}{(\log x)^2},$$

as $x \to \infty$, where $C_{c,bf'_F,t}$ is the constant which is defined as above.

(ii) of Theorem 4 follows from this conjecture, Lemma 8, Lemma 11 and $P(\ell \nmid n) = 1 - \frac{1}{\ell}$.

4. Numerical data

In this section we calculate the constant $C_{E,t,a,b}$ and give tables and graphs of $P_E(t,a,b,x)$ for three elliptic curves and x less than 10^{10}. Moreover, we also calculate $P_E(t,a,b,x)$ for twenty elliptic curves for which we could not calculate $C_{E,t}$ and $C_{E,t,a,b}$ for x less than 10^9 (in these case, we could not determine the set $\psi_t(m)$). The graphs of $P_E(t,a,b,x)$ for these elliptic curves can be found in [12]. To calculate $P_E(t,a,b,x)$, we use the computer algebra system Magma ([2]) and Sage.

Remark 2. When we calculate the expected values of $P_E(t,a,b,x)$, we use the following integral to calculate the value of $\pi_{E,t}(x)$

$$\pi_{E,t}(x) \sim C_{E,t} \int_{t+1}^{x} \frac{1}{\log(u+1) - \log t} \frac{du}{\log u} \quad \text{as } x \to \infty.$$

Zywina's heuristics suggests that this will be a better approximation of $\pi_{E,t}(x)$ than $C_{E,t}\frac{x}{(\log x)^2}$. For more detail see [16]. Thus we use the following expression to calculate $P_E(t,a,b,x)$.

$$P_E(t,a,b,x) \sim \frac{C_{E,t,a,b} C_{E,t} \int_{t+1}^{x} \frac{1}{\log(u+1)-\log t} \frac{du}{\log u}}{\pi(x)} \quad (10)$$

as $x \to \infty$.

4.1. Example 1. $E\colon y^2 = x^3 + 6x - 2$

For this elliptic curve, Zywina showed that $C_{E,1} = \frac{10}{9}\prod_{\ell}\left(1 - \frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right) \approx 0.561295742488261971297938 5$ and Theorem 2 holds with $M = 6$ (see [16]). Thus we can calculate $C_{E,1,a,\ell}$ for $\ell \neq 2, 3$ and all $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ by using Proposition 4. Here, we give the case where $\ell = 7, 5$.

$$C_{E,1,a,5} = \begin{cases} \frac{76}{73} & \text{if } a = 1, \\ \frac{72}{73} & \text{if } a \neq 1. \end{cases} \quad C_{E,1,a,7} = \begin{cases} \frac{246}{241} & \text{if } a = 1, \\ \frac{240}{241} & \text{if } a \neq 1. \end{cases}$$

Moreover, we can calculate $C_{E,1,1,3}$ and $C_{E,1,2,3}$. Because $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{-3})$ and $(\frac{-3}{p}) = -1$ when $p \equiv 2 \pmod 3$, by the proof of Theorem 1(i), if $p \equiv 2 \pmod 3$, then $2 \mid |E(\mathbb{F}_p)|$ except for $p = 2,\ 3$ which are the bad primes of E. Thus $|\psi_{1,2,3}(6)|$ is finite and so $C_{E,1,2,3} = 0$ and $C_{E,1,1,3} = 2$. Thus we can also calculate $C_{E,1,a,15}$ for all $a \in (\mathbb{Z}/15\mathbb{Z})^\times$ by definition of $C_{E,t,a,b}$.

$$C_{E,1,a,15} = \begin{cases} \frac{152}{73} & \text{if } a = 1, \\ \frac{144}{73} & \text{if } a = 4,\ 7,\ 13. \end{cases}$$

4.2. Example 2. $E\colon y^2 = x^3 - x$

This elliptic curve has complex multiplication by $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathbb{Z}[i]$. Then $F = \mathbb{Q}(i)$ and $f_F = 4$. The torsion subgroup $E(\mathbb{Q}(i))_{\mathrm{torsion}}$ has order 8 and is generated by $(i, 1-i)$ and $(1,0)$. Thus we consider the case where $t = 8$. Zywina showed that $M = 2$ and $C_{E_{\mathbb{Q}(i)},8} = \prod_{\ell\neq 2}\left(1 - \chi(\ell)\frac{\ell^2-\ell-1}{(\ell-\chi(\ell))(\ell-1)^2}\right) \approx 1.067350894\ldots$ where $\chi(\ell) = (-1)^{(\ell-1)/2}$ (see [16]). We have to calculate $C_{E,8}$, $C^{\mathrm{split}}_{E,8,a,b}$ and $C^{\mathrm{inert}}_{8,a,b}$ to calculate $C_{E,8,a,b}$. Here, we consider the case where $b = 3,\ 5$ and 7. First, we conjecture $C_{E,8}$. If $p \equiv 3 \pmod 4$, then p is inert in F and $|E(\mathbb{F}_p)| = p + 1$. Thus we conjecture

$$\pi_{E,8,3,4}(x) \sim C^{\mathrm{inert}}_{8,3,4}\frac{x}{(\log x)^2} = \frac{C_{3,4,8}}{\varphi(4)}\frac{x}{(\log x)^2},$$
$$C_{E,8} = \frac{1}{\varphi(4)}C_{3,4,8} + \frac{1}{2}C_{E_F,8} = \frac{1}{2}(C_{3,4,8} + C_{E_F,8})$$

as $x \to \infty$. From lemmas in §3.2.2, we have

$$C_{3,4,8} = \frac{1}{2}\prod_{\ell\geqq 3}\left(1 - \frac{1}{(\ell-1)^2}\right) \approx 0.3300809302948\ldots$$

and

$$C_{E,8} \approx 0.69871591214746\ldots.$$

Next, by Proposition 5, we have

$$C^{\mathrm{split}}_{E,8,a,3} = \begin{cases} \frac{3}{7} & \text{if } a = 1, \\ \frac{4}{7} & \text{if } a \neq 1, \end{cases} \quad C^{\mathrm{split}}_{E,8,a,5} = \begin{cases} \frac{1}{3} & \text{if } a = 1, \\ \frac{2}{9} & \text{if } a \neq 1, \end{cases}$$
$$C^{\mathrm{split}}_{E,8,a,7} = \begin{cases} \frac{7}{47} & \text{if } a = 1, \\ \frac{8}{47} & \text{if } a \neq 1, \end{cases}$$

and by lemmas in §3.2.2, we have

$$C^{\mathrm{inert}}_{8,a,3} = \begin{cases} \frac{1}{4}\prod_{\ell\geqq 3}\left(1 - \frac{1}{(\ell-1)^2}\right) & \text{if } a = 1, \\ 0 & \text{if } a \neq 1. \end{cases}$$
$$C^{\mathrm{inert}}_{8,a,5} = \begin{cases} \frac{1}{12}\prod_{\ell\geqq 3}\left(1 - \frac{1}{(\ell-1)^2}\right) & \text{if } a = 1,\ 2,\ 3, \\ 0 & \text{if } a = 4. \end{cases}$$
$$C^{\mathrm{inert}}_{8,a,7} = \begin{cases} \frac{1}{20}\prod_{\ell\geqq 3}\left(1 - \frac{1}{(\ell-1)^2}\right) & \text{if } a \neq 6, \\ 0 & \text{if } a = 6. \end{cases}$$

Thus we have

$$C_{E,8,a,3} \approx \begin{cases} 1.127091875298942\ldots & \text{if } a = 1, \\ 0.872908124701058\ldots & \text{if } a \neq 1, \end{cases}$$
$$C_{E,8,a,5} \approx \begin{cases} 1.333333333333333\ldots & \text{if } a = 1, \\ 0.993869062616255\ldots & \text{if } a = 2,\ 3, \\ 0.678928541434156\ldots & \text{if } a = 4, \end{cases}$$
$$C_{E,8,a,7} \approx \begin{cases} 0.965986332526847\ldots & \text{if } a = 1, \\ 1.063492027307284\ldots & \text{if } a \neq 1,\ 6, \\ 0.780045558243498\ldots & \text{if } a = 6, \end{cases}$$

4.3. Example 3. $E\colon y^2+y=x^3-x^2-10x-20$

For this elliptic curve, Lang and Trotter showed that $M = 2\cdot 5\cdot 11$ (see [8], Part I, §8). This curve have 5-torsion point (5, 5). Thus we consider $C_{E,5,a,b}$, i.e., $t=5$.
Zywina showed that $C_{E,5} = \frac{62208}{78913}\prod_{\ell}\left(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right)$ (see [16]). Here, we consider the case where $b = 3,\ 5$ and 7. Since $\gcd(3, Mt) = 1$, $C_{E,5,1,3} = \frac{10}{9}$ and $C_{E,5,2,3} = \frac{8}{9}$ by Proposition 4. Similarly, we can calculate $C_{E,5,a,7}$ for all $a \in (\mathbb{Z}/7\mathbb{Z})^{\times}$. Moreover, 5 divides M, but even so we can calculate $C_{E,5,a,5}$ because we know the structure of $\psi_5(2\cdot 5^2\cdot 11)$ (see proof of Lemma 8.2 in [16] and [8], Part I, §8). From this structure, $C_{E,5,a,5}$ is calculated as follows:

$$C_{E,5,a,5} = \begin{cases} 0 & \text{if } a = 1, \\ \frac{4}{3} & \text{if } a = 2,\ 3,\ 4. \end{cases}$$

4.4. Tables and graphs of $P_{E,t,a,b}$

Here, we give some tables and graphs of both actual and conjectural values of $P_{E,t,a,b}$ for the above three elliptic curves. In these tables and graphs, "Actual" means the actual values calculated by using the definition of $P_{E,t,a,b}$ and "Expected" means the values calculated by the right-hand side of (10).

Table 1: $P_E(1,a,b,x)$ for $E\colon y^2=x^3+6x-2$

$P_E(1,0,1,x)$		
x	Actual	Expected
1000000000	0.028640288	0.028637876
2000000000	0.02766305	0.027652581
3000000000	0.027102517	0.027107106
4000000000	0.026729141	0.026733024
5000000000	0.026445002	0.026450231
6000000000	0.026223783	0.026223329
7000000000	0.026035527	0.026034675
8000000000	0.025872841	0.025873494
9000000000	0.025731157	0.025732895
10000000000	0.025609361	0.025608326
$P_E(1,1,5,x)$		
x	Actual	Expected
1000000000	0.029683309	0.029814775
2000000000	0.028712855	0.028788988
3000000000	0.028161652	0.028221096
4000000000	0.027783831	0.027831641
5000000000	0.027502239	0.027537227
6000000000	0.027273820	0.027301000
7000000000	0.027080172	0.027104593
8000000000	0.026913190	0.026936789
9000000000	0.026758016	0.026790411
10000000000	0.026638621	0.026660723

$P_E(1,2,5,x)$		
x	Actual	Expected
1000000000	0.028270462	0.028245577
2000000000	0.027312707	0.027273778
3000000000	0.026738474	0.026735776
4000000000	0.026361056	0.026366818
5000000000	0.026076024	0.026087899
6000000000	0.025856804	0.025864105
7000000000	0.025679170	0.025678035
8000000000	0.025513050	0.025519063
9000000000	0.025377844	0.025380389
10000000000	0.025256671	0.025257527
$P_E(1,3,5,x)$		
x	Actual	Expected
1000000000	0.028324094	0.028245577
2000000000	0.027296193	0.027273778
3000000000	0.026725405	0.026735776
4000000000	0.026364419	0.026366818
5000000000	0.026086833	0.026087899
6000000000	0.025872954	0.025864105
7000000000	0.025675933	0.025678035
8000000000	0.025516022	0.025519063
9000000000	0.025377178	0.025380389
10000000000	0.025261585	0.025257527
$P_E(1,4,5,x)$		
x	Actual	Expected
1000000000	0.028283343	0.028245577
2000000000	0.027330484	0.027273778
3000000000	0.026784579	0.026735776
4000000000	0.026407275	0.026366818
5000000000	0.026114931	0.026087899
6000000000	0.025891566	0.025864105
7000000000	0.025706852	0.025678035
8000000000	0.025549114	0.025519063
9000000000	0.025411609	0.025380389
10000000000	0.025280586	0.025257527
$P_E(1,1,7,x)$		
x	Actual	Expected
1000000000	0.029252010	0.029232023
2000000000	0.028250240	0.028226286
3000000000	0.027710793	0.027669494
4000000000	0.027308621	0.027287651
5000000000	0.027018229	0.026998991
6000000000	0.026787093	0.026767381
7000000000	0.026589965	0.026574813
8000000000	0.026419677	0.026410289
9000000000	0.026278378	0.026266772
10000000000	0.026149671	0.026139620
$P_E(1,2,7,x)$		
x	Actual	Expected
1000000000	0.028456263	0.028519047
2000000000	0.027528390	0.027537840
3000000000	0.026969549	0.026994628
4000000000	0.026611260	0.026622099
5000000000	0.026327013	0.026340479
6000000000	0.026100654	0.026114518
7000000000	0.025933627	0.025926647
8000000000	0.025777114	0.025766136
9000000000	0.025639945	0.025626119
10000000000	0.025516608	0.025502068

$P_E(1,3,7,x)$		
x	Actual	Expected
1000000000	0.028584957	0.028519047
2000000000	0.027568842	0.027537840
3000000000	0.026976858	0.026994628
4000000000	0.026604671	0.026622099
5000000000	0.026322474	0.026340479
6000000000	0.026095088	0.026114518
7000000000	0.025904056	0.025926647
8000000000	0.025752377	0.025766136
9000000000	0.025617190	0.025626119
10000000000	0.025495139	0.025502068
$P_E(1,4,7,x)$		
x	Actual	Expected
1000000000	0.028549020	0.028519047
2000000000	0.027557762	0.027537840
3000000000	0.026993781	0.026994628
4000000000	0.026631773	0.026622099
5000000000	0.026350364	0.026340479
6000000000	0.026126800	0.026114518
7000000000	0.025927402	0.025926647
8000000000	0.025751858	0.025766136
9000000000	0.025594890	0.025626119
10000000000	0.025473708	0.025502068
$P_E(1,5,7,x)$		
x	Actual	Expected
1000000000	0.028475697	0.028519047
2000000000	0.027497563	0.027537840
3000000000	0.026957687	0.026994628
4000000000	0.026611717	0.026622099
5000000000	0.026322551	0.026340479
6000000000	0.026108358	0.026114518
7000000000	0.025918682	0.025926647
8000000000	0.025758791	0.025766136
9000000000	0.025617463	0.025626119
10000000000	0.025505215	0.025502068
$P_E(1,6,7,x)$		
x	Actual	Expected
1000000000	0.028523700	0.028519047
2000000000	0.027575445	0.027537840
3000000000	0.027006404	0.026994628
4000000000	0.026606784	0.026622099
5000000000	0.026329372	0.026340479
6000000000	0.026124689	0.026114518
7000000000	0.025939413	0.025926647
8000000000	0.025777223	0.025766136
9000000000	0.025639069	0.025626119
10000000000	0.025515821	0.025502068
$P_E(1,1,15,x)$		
x	Actual	Expected
1000000000	0.059371326	0.059629551
2000000000	0.057429260	0.057577977
3000000000	0.056326623	0.056442193
4000000000	0.055568311	0.055663283
5000000000	0.055004922	0.055074454
6000000000	0.054548205	0.054602000
7000000000	0.054161053	0.054209186
8000000000	0.053828214	0.053873578
9000000000	0.053517706	0.053580823
10000000000	0.053279207	0.053321447

$P_E(1,4,15,x)$		
x	Actual	Expected
1000000000	0.056572735	0.056491154
2000000000	0.054663939	0.054547557
3000000000	0.053569945	0.053471552
4000000000	0.052815552	0.052733637
5000000000	0.052230967	0.052175798
6000000000	0.051786600	0.051728211
7000000000	0.051415646	0.051356071
8000000000	0.051100429	0.051038127
9000000000	0.050824981	0.050760779
10000000000	0.050561930	0.050515055
$P_E(1,7,15,x)$		
x	Actual	Expected
1000000000	0.056538096	0.056491154
2000000000	0.054626427	0.054547557
3000000000	0.053477860	0.053471552
4000000000	0.052724464	0.052733637
5000000000	0.052151847	0.052175798
6000000000	0.051713658	0.051728211
7000000000	0.051357763	0.051356071
8000000000	0.051025443	0.051038127
9000000000	0.050754605	0.050760779
10000000000	0.050513846	0.050515055
$P_E(1,13,15,x)$		
x	Actual	Expected
1000000000	0.056649856	0.056491154
2000000000	0.054591432	0.054547557
3000000000	0.053449776	0.053471552
4000000000	0.052730033	0.052733637
5000000000	0.052174477	0.052175798
6000000000	0.051746302	0.051728211
7000000000	0.051351347	0.051356071
8000000000	0.051031741	0.051038127
9000000000	0.050754184	0.050760779
10000000000	0.050522826	0.050515055

Table 2: $P_E(1,a,b,x)$ for $E\colon y^2 = x^3 - x$

$P_E(8,0,1,x)$		
x	Actual	Expected
1000000000	0.039884962	0.039901509
2000000000	0.038335953	0.038369372
3000000000	0.037504973	0.037526748
4000000000	0.036942546	0.036951143
5000000000	0.036505217	0.036517181
6000000000	0.036156835	0.036169783
7000000000	0.035873168	0.035881428
8000000000	0.035631045	0.035635425
9000000000	0.035417906	0.035421119
10000000000	0.035228442	0.035231475

$P_E(8,1,3,x)$		
x	Actual	Expected
1000000000	0.044926912	0.044972693
2000000000	0.043197532	0.043245833
3000000000	0.042270214	0.042296118
4000000000	0.041631397	0.041647358
5000000000	0.041130211	0.041158243
6000000000	0.040741296	0.040766692
7000000000	0.040431756	0.040441690
8000000000	0.040155806	0.040164422
9000000000	0.039916747	0.039922879
10000000000	0.039706359	0.039709133
$P_E(8,2,3,x)$		
x	Actual	Expected
1000000000	0.034843433	0.034830324
2000000000	0.033474660	0.033492911
3000000000	0.032739902	0.032757378
4000000000	0.032253925	0.032254928
5000000000	0.031880318	0.031876120
6000000000	0.031572572	0.031572873
7000000000	0.031314647	0.031321166
8000000000	0.031106416	0.031106428
9000000000	0.030919158	0.030919359
10000000000	0.030750647	0.030753817
$P_E(8,1,5,x)$		
x	Actual	Expected
1000000000	0.053228105	0.053202012
2000000000	0.051117679	0.051159163
3000000000	0.049988729	0.050035664
4000000000	0.049247980	0.049268191
5000000000	0.048660480	0.048689575
6000000000	0.048187255	0.048226377
7000000000	0.047804421	0.047841904
8000000000	0.047485954	0.047513900
9000000000	0.047206575	0.047228159
10000000000	0.046958101	0.046975300
$P_E(8,2,5,x)$		
x	Actual	Expected
1000000000	0.039639518	0.039656885
2000000000	0.038140378	0.038134142
3000000000	0.037312561	0.037296684
4000000000	0.036741499	0.036724607
5000000000	0.036303592	0.036293306
6000000000	0.035965264	0.035948037
7000000000	0.035681467	0.035661451
8000000000	0.035434204	0.035416955
9000000000	0.035218889	0.035203964
10000000000	0.035024653	0.035015482
$P_E(8,3,5,x)$		
x	Actual	Expected
1000000000	0.039589226	0.039656885
2000000000	0.038072943	0.038134142
3000000000	0.037264892	0.037296684
4000000000	0.036709427	0.036724607
5000000000	0.036279298	0.036293306
6000000000	0.035937525	0.035948037
7000000000	0.035660325	0.035661451
8000000000	0.035422442	0.035416955
9000000000	0.035207751	0.035203964
10000000000	0.035021167	0.035015482

$P_E(8,4,5,x)$		
x	Actual	Expected
1000000000	0.027082997	0.027090252
2000000000	0.026013325	0.026050042
3000000000	0.025453846	0.025477961
4000000000	0.025071023	0.025087166
5000000000	0.024777438	0.024792537
6000000000	0.024537393	0.024556679
7000000000	0.024346385	0.024360907
8000000000	0.024181455	0.024193888
9000000000	0.024038474	0.024048390
10000000000	0.023909839	0.023919635
$P_E(8,1,7,x)$		
x	Actual	Expected
1000000000	0.038511268	0.038544281
2000000000	0.037015808	0.037064253
3000000000	0.036208409	0.036250292
4000000000	0.035673026	0.035694272
5000000000	0.035274622	0.035275065
6000000000	0.034934617	0.034939484
7000000000	0.034664333	0.034660938
8000000000	0.034437906	0.034423303
9000000000	0.034218907	0.034216287
10000000000	0.034035654	0.034033094
$P_E(8,2,7,x)$		
x	Actual	Expected
1000000000	0.042393945	0.042434902
2000000000	0.040747490	0.040805482
3000000000	0.039896884	0.039909360
4000000000	0.039283803	0.039297216
5000000000	0.038806989	0.038835695
6000000000	0.038449736	0.038466240
7000000000	0.038140537	0.038159578
8000000000	0.037885271	0.037897957
9000000000	0.037669209	0.037670045
10000000000	0.037471394	0.037468360
$P_E(8,3,7,x)$		
x	Actual	Expected
1000000000	0.042489766	0.042434902
2000000000	0.040839043	0.040805482
3000000000	0.039951119	0.039909360
4000000000	0.039342174	0.039297216
5000000000	0.038875829	0.038835695
6000000000	0.038496922	0.038466240
7000000000	0.038195669	0.038159578
8000000000	0.037929754	0.037897957
9000000000	0.037699978	0.037670045
10000000000	0.037491219	0.037468360
$P_E(8,4,7,x)$		
x	Actual	Expected
1000000000	0.042397935	0.042434902
2000000000	0.040741634	0.040805482
3000000000	0.039846378	0.039909360
4000000000	0.039254684	0.039297216
5000000000	0.038782045	0.038835695
6000000000	0.038413016	0.038466240
7000000000	0.038121209	0.038159578
8000000000	0.037862492	0.037897957
9000000000	0.037634084	0.037670045
10000000000	0.037433426	0.037468360

$P_E(8,5,7,x)$		
x	Actual	Expected
1000000000	0.042359961	0.042434902
2000000000	0.040723283	0.040805482
3000000000	0.039860842	0.039909360
4000000000	0.039284406	0.039297216
5000000000	0.038812677	0.038835695
6000000000	0.038440622	0.038466240
7000000000	0.038138995	0.038159578
8000000000	0.037878964	0.037897957
9000000000	0.037656674	0.037670045
10000000000	0.037456653	0.037468360
$P_E(8,6,7,x)$		
x	Actual	Expected
1000000000	0.031156936	0.031124970
2000000000	0.029948498	0.029929829
3000000000	0.029266142	0.029272545
4000000000	0.028817381	0.028823553
5000000000	0.028479174	0.028485038
6000000000	0.028206078	0.028214052
7000000000	0.027978517	0.027989123
8000000000	0.027792170	0.027797230
9000000000	0.027628804	0.027630062
10000000000	0.027482336	0.027482132

Table 3: $P_E(1,a,b,x)$ for $E\colon y^2+y=x^3-x^2-10x-20$

$P_E(5,0,1,x)$		
x	Actual	Expected
1000000000	0.022152893	0.022144232
2000000000	0.021336450	0.021315702
3000000000	0.020865162	0.020859291
4000000000	0.020548077	0.020547216
5000000000	0.020313097	0.020311776
6000000000	0.020123645	0.020123195
7000000000	0.019966167	0.019966600
8000000000	0.019831536	0.019832957
9000000000	0.019712679	0.019716496
10000000000	0.019610499	0.019613407
$P_E(5,1,3,x)$		
x	Actual	Expected
1000000000	0.024625027	0.024604703
2000000000	0.023714458	0.023684114
3000000000	0.023192720	0.023176990
4000000000	0.022842760	0.022830240
5000000000	0.022583294	0.022568641
6000000000	0.022374974	0.022359106
7000000000	0.022196851	0.022185111
8000000000	0.022046869	0.022036619
9000000000	0.021914528	0.021907324
10000000000	0.021800311	0.021792674

$P_E(5,2,3,x)$		
x	Actual	Expected
1000000000	0.019680966	0.019683762
2000000000	0.018958583	0.018947291
3000000000	0.018537686	0.018541592
4000000000	0.018253506	0.018264192
5000000000	0.018042947	0.018054912
6000000000	0.017872414	0.017887284
7000000000	0.017735517	0.017748089
8000000000	0.017616268	0.017629295
9000000000	0.017510876	0.017525859
10000000000	0.017420747	0.017434139
$P_E(5,2,5,x)$		
x	Actual	Expected
1000000000	0.029570302	0.029525643
2000000000	0.028443894	0.028420937
3000000000	0.027810500	0.027812388
4000000000	0.027396045	0.027396288
5000000000	0.027086294	0.027082369
6000000000	0.026822363	0.026830927
7000000000	0.026613928	0.026622134
8000000000	0.026434845	0.026443943
9000000000	0.026272390	0.026288789
10000000000	0.026140500	0.026151209
$P_E(5,3,5,x)$		
x	Actual	Expected
1000000000	0.029468792	0.029525643
2000000000	0.028407614	0.028420937
3000000000	0.027792564	0.027812388
4000000000	0.027385584	0.027396288
5000000000	0.027072018	0.027082369
6000000000	0.026820017	0.026830927
7000000000	0.026609925	0.026622134
8000000000	0.026435607	0.026443943
9000000000	0.026280147	0.026288789
10000000000	0.026148759	0.026151209
$P_E(5,4,5,x)$		
x	Actual	Expected
1000000000	0.029571249	0.029525643
2000000000	0.028493465	0.028420937
3000000000	0.027856753	0.027812388
4000000000	0.027410332	0.027396288
5000000000	0.027093743	0.027082369
6000000000	0.026851941	0.026830927
7000000000	0.026640448	0.026622134
8000000000	0.026455438	0.026443943
9000000000	0.026297808	0.024048390
10000000000	0.026152358	0.026151209
$P_E(5,1,7,x)$		
x	Actual	Expected
1000000000	0.022580600	0.022603656
2000000000	0.021764471	0.021757937
3000000000	0.021274153	0.021292056
4000000000	0.020947335	0.020973507
5000000000	0.020707965	0.020733183
6000000000	0.020518091	0.020540689
7000000000	0.020356586	0.020380845
8000000000	0.020221757	0.020244429
9000000000	0.020105229	0.020125552
10000000000	0.020009622	0.020020324

$P_E(5,2,7,x)$		
x	Actual	Expected
1000000000	0.022040766	0.022052348
2000000000	0.021196119	0.021227255
3000000000	0.020747154	0.020772737
4000000000	0.020442680	0.020461958
5000000000	0.020209998	0.020227495
6000000000	0.020014620	0.020039696
7000000000	0.019858458	0.019883751
8000000000	0.019723100	0.019750663
9000000000	0.019607517	0.019634685
10000000000	0.019509034	0.019532023
$P_E(5,3,7,x)$		
x	Actual	Expected
1000000000	0.022055137	0.022052348
2000000000	0.021268497	0.021227255
3000000000	0.020804856	0.020772737
4000000000	0.020490982	0.020461958
5000000000	0.020257906	0.020227495
6000000000	0.020067367	0.020039696
7000000000	0.019908478	0.019883751
8000000000	0.019776154	0.019750663
9000000000	0.019653258	0.019634685
10000000000	0.019546555	0.019532023
$P_E(5,4,7,x)$		
x	Actual	Expected
1000000000	0.022067684	0.022052348
2000000000	0.021270633	0.021227255
3000000000	0.020794840	0.020772737
4000000000	0.020456690	0.020461958
5000000000	0.020220788	0.020227495
6000000000	0.020037952	0.020039696
7000000000	0.019880798	0.019883751
8000000000	0.019747735	0.019750663
9000000000	0.019631755	0.019634685
10000000000	0.019519495	0.019532023
$P_E(5,5,7,x)$		
x	Actual	Expected
1000000000	0.022122145	0.022052348
2000000000	0.021271884	0.021227255
3000000000	0.020817422	0.020772737
4000000000	0.020494694	0.020461958
5000000000	0.020260184	0.020227495
6000000000	0.020072698	0.020039696
7000000000	0.019920629	0.019883751
8000000000	0.019784393	0.019750663
9000000000	0.019663395	0.019634685
10000000000	0.019562176	0.019532023
$P_E(5,6,7,x)$		
x	Actual	Expected
1000000000	0.022050936	0.022052348
2000000000	0.021247038	0.021227255
3000000000	0.020752510	0.020772737
4000000000	0.020456057	0.020461958
5000000000	0.020221723	0.020227495
6000000000	0.020031128	0.020039696
7000000000	0.019872037	0.019883751
8000000000	0.019736070	0.019750663
9000000000	0.019614913	0.019634685
10000000000	0.019516107	0.019532023

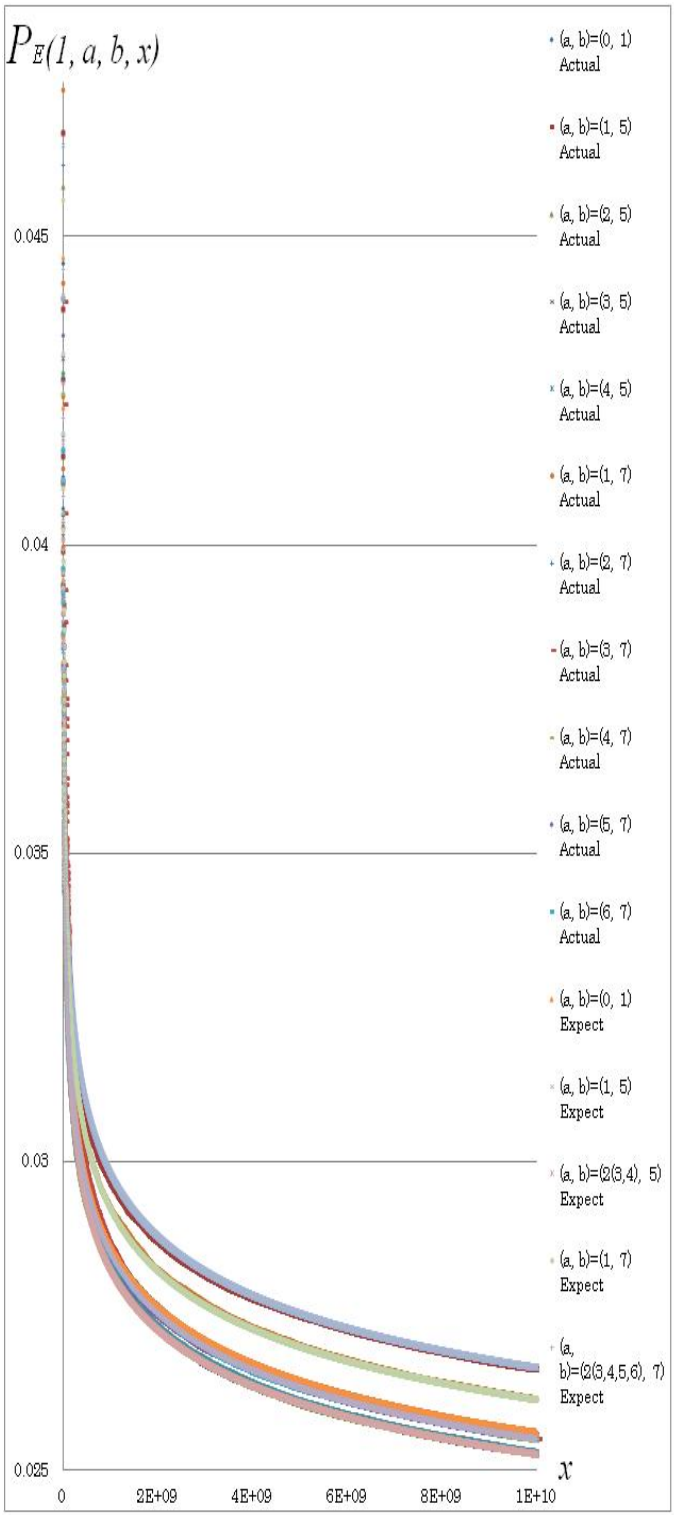

Figure 1: $P_E(1,a,b,x)$ for $E\colon y^2 = x^3 + 6x - 2$ and $b = 1, 5, 7$

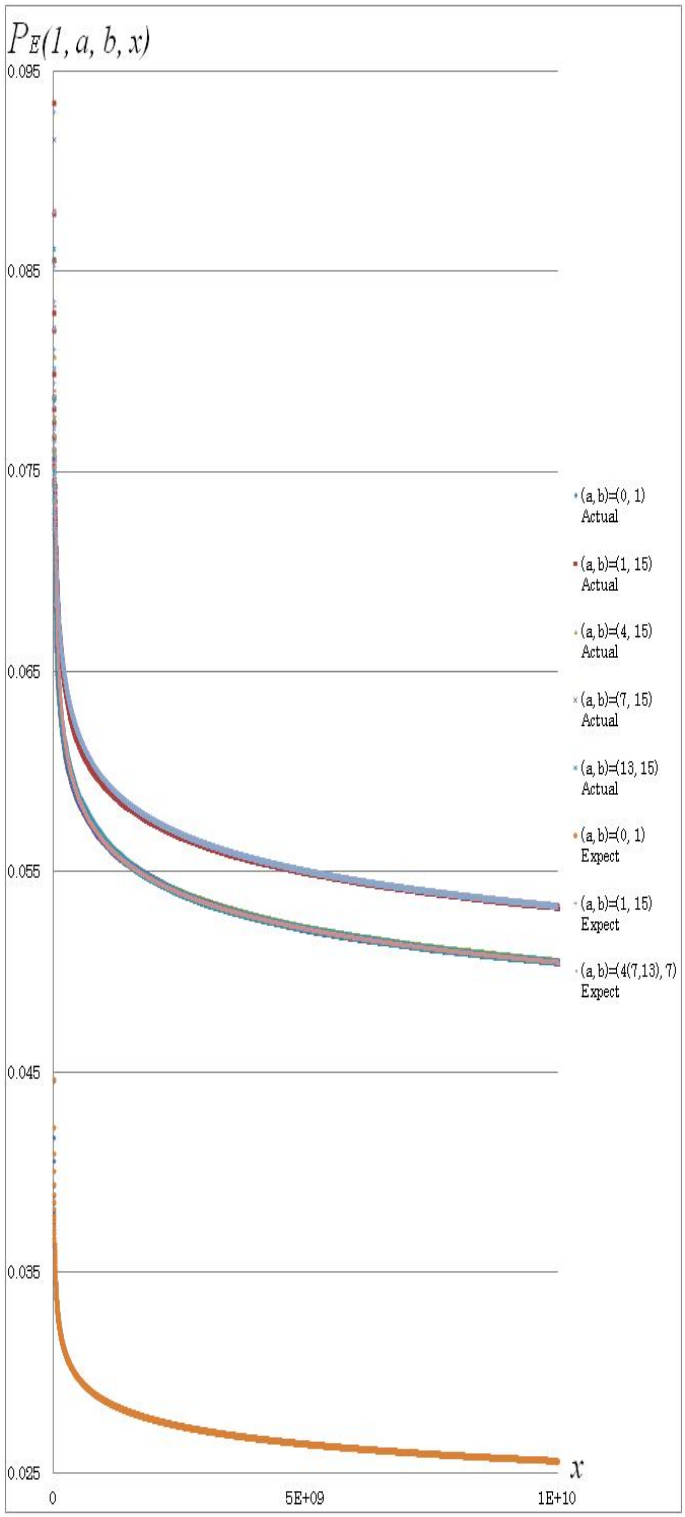

Figure 2: $P_E(1, a, b, x)$ for $E\colon y^2 = x^3+6x-2$ and $b = 1, 15$

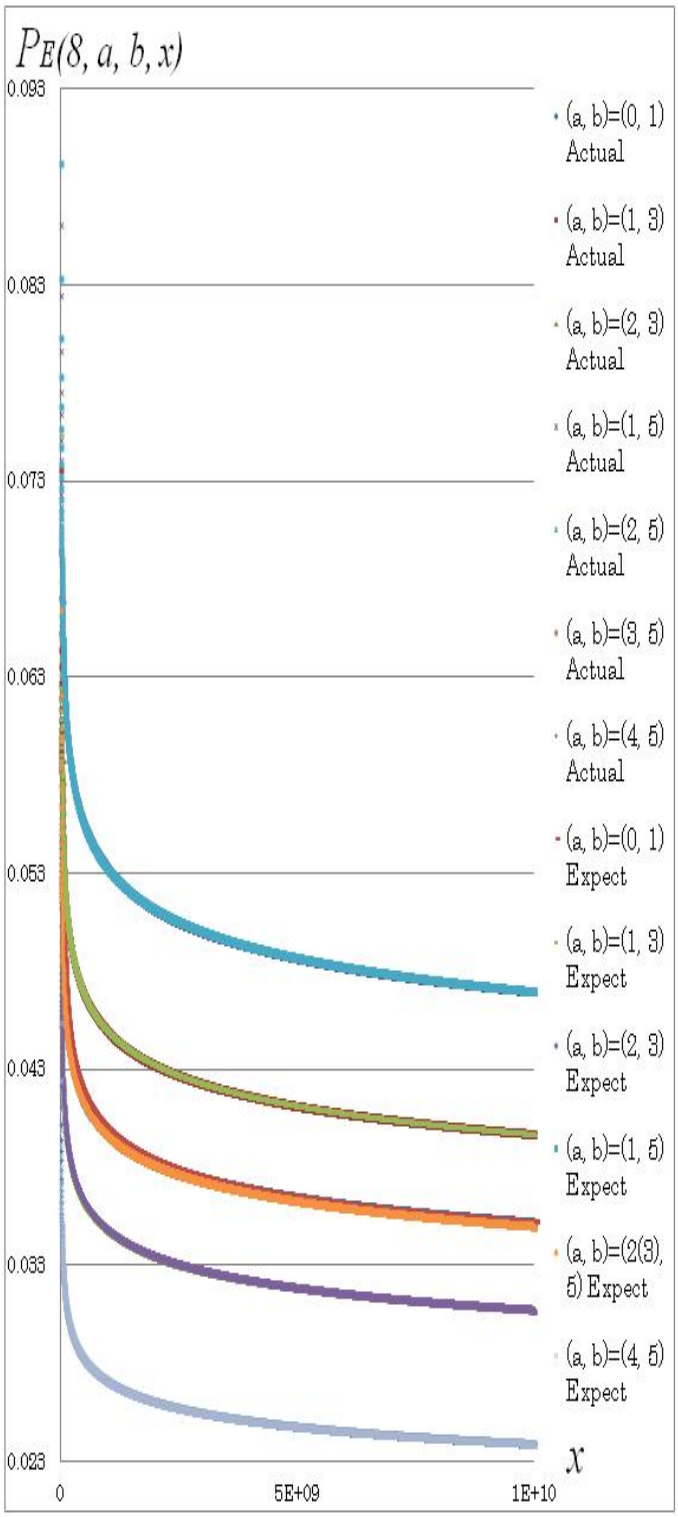

Figure 3: $P_E(8, a, b, x)$ for $E\colon y^2 = x^3 - x$ and $b = 1, 3, 5$

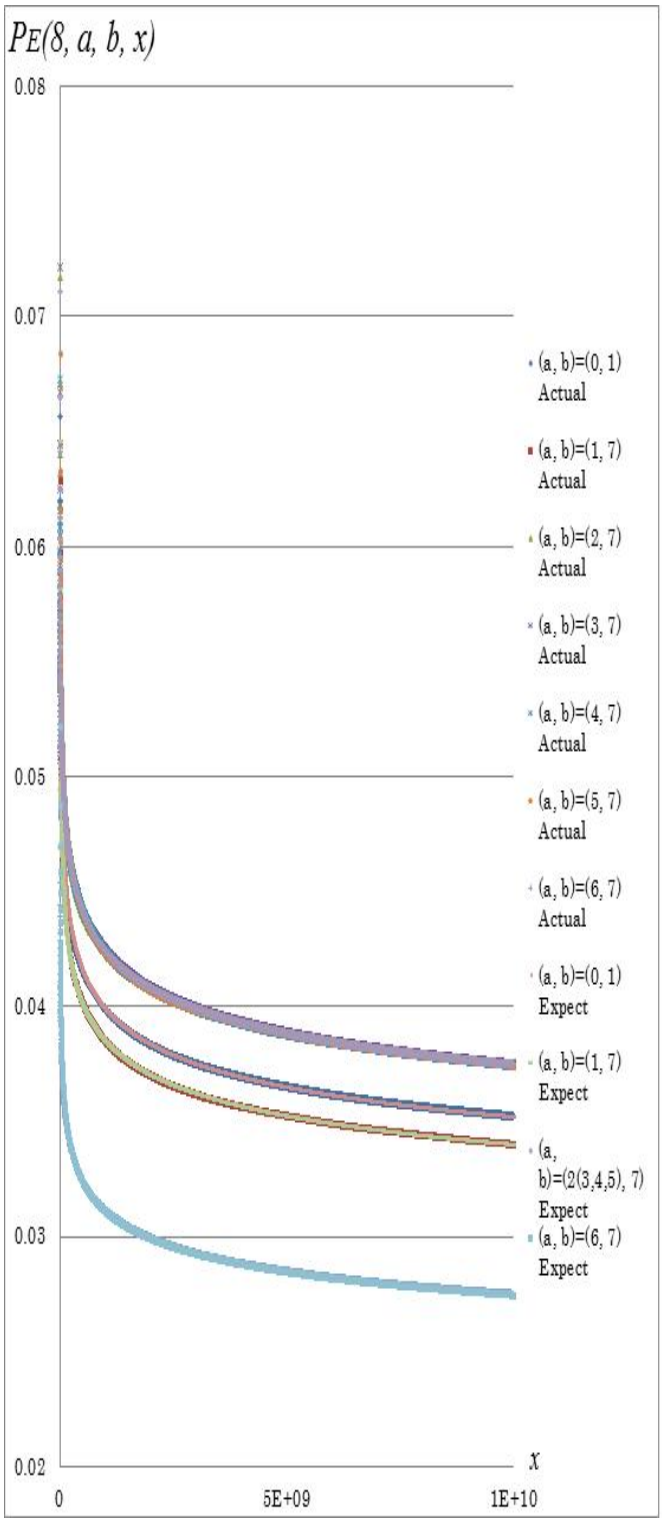

Figure 4: $P_E(8, a, b, x)$ for $E\colon y^2 = x^3 - x$ and $b = 7$

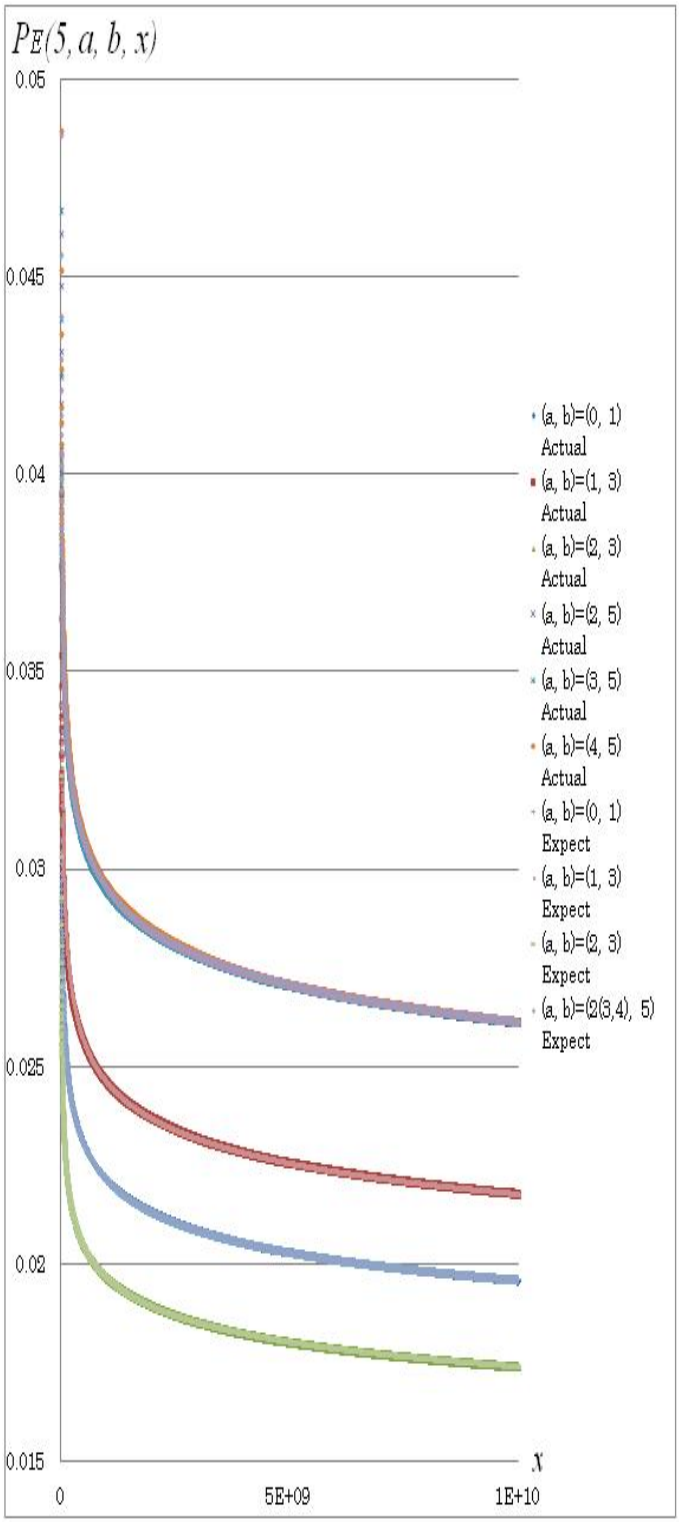

Figure 5: $P_E(5, a, b, x)$ for $E\colon y^2 + y = x^3 - x^2 - 10x - 20$ and $b = 1, 3, 5$

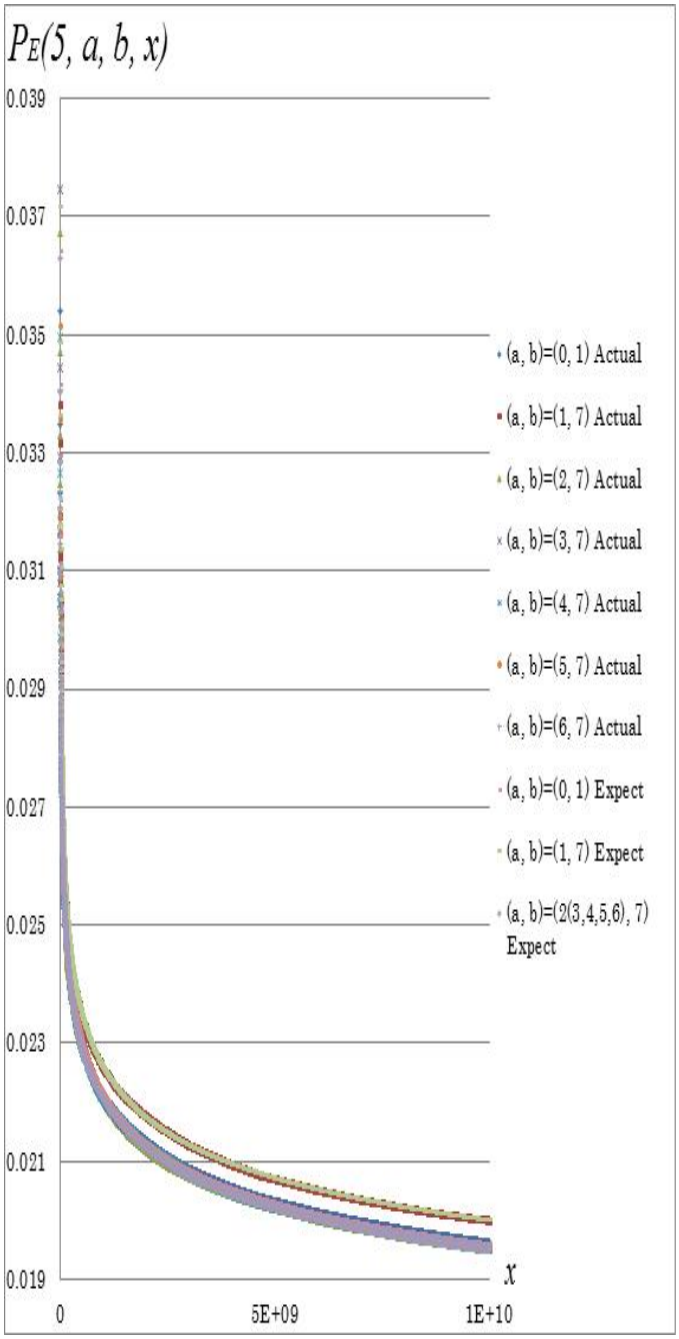

Figure 6: $P_E(5, a, b, x)$ for $E\colon y^2 + y = x^3 - x^2 - 10x - 20$ and $b = 1, 7$

References

[1] H. Baier and J. Buchmann, *Efficient Construction of Cryptographically Strong Elliptic curve*, In: INDOCRYPT 2000, Lecture Notes in Comp. Science, Vol. 1977, Springer, (2000), 191–202

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

[3] 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.

[4] M. E. Hellman and S. C. Pohlig, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*. IEEEE Transactions on Information Theory **24** (1978), 106–110.

[5] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), 157–165

[6] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Computation **48** (1987), 203–209.

[7] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, Vol. 211, Springer, New York, 2002.

[8] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions of the rational numbers*, Lecture Notes in Mathematics, Vol. 504 (Springer, Berlin, 1976).

[9] Ueli M. Maurer, *Some Number-theoretic Conjectures and Their Relation to the Generation of Cryptographic Primes*, Cryptography and Coding '92, Oxford University Press, (1992) 173–191

[10] V.S. Miller, *Use of elliptic curves in cryptography*, Abstracts for Crypto '85. Lecture Notes in Computer Science, **218** (1986), 417–426.

[11] V. Muller and S. Paulus, *On the Generation of Cryptography Strong Elliptic Curves*, Technical Report, Thchnical University of Darmstadt

[12] S. Okumura, *The full version of graphs of $P_E(t, a, b, x)$*, `http://www2.math.kyushu-u.ac.jp/~s-okumura/`

[13] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, Vol. 106, Springer 2009.

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

[15] N. Tschebotareff, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95** (1926), 191–228.

[16] D. Zywina, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011) 739–769.

A. Divisibility of $|E(\mathbb{F}_p)|$

In this appendix we consider whether or not for a given E, there is a triple $(a, b, \ell) \in \mathbb{Z}^3$ with $\gcd(a, b) = 1$ such that $|E(\mathbb{F}_p)|$ is divisible by the prime ℓ if $p \equiv a \pmod{b}$.

A.1. Theorem about divisibility of $|E(\mathbb{F}_p)|$

We obtain the next theorem on 2-divisibility of $|E(\mathbb{F}_p)|$.

Theorem A 1. *Let E be an elliptic curve over $\mathbb{Q}$. Suppose that E is not $\mathbb{Q}$-isogenous to an elliptic curve which has non-trivial $\mathbb{Q}$-torsion points. Let Δ_E be the discriminant of E and f_E the conductor of $\mathbb{Q}(\sqrt{\Delta_E})$.*

(i) *If $\sqrt{\Delta_E} \notin \mathbb{Q}$, then there are integers $a_1, a_2, \ldots, a_{\frac{\varphi(f_E)}{2}}$ with $a_i \not\equiv a_j \pmod{f_E}$ $(i \neq j)$ such that $|E(\mathbb{F}_p)|$ is divisible by 2 if $p \nmid \Delta_E f_E$ and $p \equiv a_i \pmod{f_E}$ for $i = 1, 2, \ldots, \frac{\varphi(f_E)}{2}$.*

(ii) *If $\sqrt{\Delta_E} \in \mathbb{Q}$, then there are an integer F_E and $\frac{\varphi(F_E)}{3}$ integers $a_1, a_2, \ldots, a_{\frac{\varphi(F_E)}{3}}$ with $a_i \not\equiv a_j \pmod{F_E}$ $(i \neq j)$ such that $|E(\mathbb{F}_p)|$ is divisible by 2 if $p \equiv a_i \pmod{F_E}$ for $i = 1, 2, \ldots, \frac{\varphi(F_E)}{3}$.*

Proof. First, we prove (i). Suppose that $\sqrt{\Delta_E} \notin \mathbb{Q}$ and

$$E[2] = \{\mathcal{O},\ (e_1, 0),\ (e_2, 0),\ (e_3, 0)\}.$$

Then $\sqrt{\Delta}_E = (e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$. Suppose that $p \nmid 2f_E$. Let $m_E := \mathrm{lcm}(f_E, 2)$ and $\sigma_p \in \mathrm{Frob}_p \subseteq \mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})$ a Frobenius automorphism at p. Then $\sigma_p(\sqrt{\Delta_E}) = -\sqrt{\Delta_E}$ means that there is an unique $i \in \{1, 2, 3\}$ such that $\sigma_p(e_i) = e_i$. Then there is an unique element $e_{i,p} \in \mathbb{F}_p$ such that $(e_{i,p}, 0) \in E(\mathbb{F}_p)[2]$. This means that $|E(\mathbb{F}_p)[2]| = 2$ and so $2 \mid |E(\mathbb{F}_p)|$. It is easy to see that $\sigma_p(\sqrt{\Delta_E}) = -\sqrt{\Delta_E}$ for a prime number p which belongs to one of a half of the congruence classes of $(\mathbb{Z}/m_E\mathbb{Z})^\times \cong (\mathbb{Z}/f_E\mathbb{Z})^\times$ (except for $p \mid 2f_E\Delta_E$ and bad prime for E). Thus we have proved (i). Next, we prove (ii). Suppose that $\sqrt{\Delta_E} \in \mathbb{Q}$. Then $\mathbb{Q}(E[2])/\mathbb{Q}$ is an abelian extension of degree 3 of $\mathbb{Q}$. Let F_E be the conductor of $\mathbb{Q}(E[2])$. We have $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathrm{C}_3 \subset \mathrm{S}_3 \cong GL_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathrm{C}_3 \cong \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}$. It implies that $\psi_1(2) = \{I_2\}$. Thus for $p \neq 2$ which is good prime for E, $|E(\mathbb{F}_p)|$ is divisible by 2 if and only if $\rho_2(\mathrm{Frob}_p) = I_2$. This means that for any Frobenius automorphism $\sigma_p \in \mathrm{Frob}_p \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_{F_E})/\mathbb{Q})$, $|E(\mathbb{F}_p)|$ is divisible by 2 if and only if $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_{F_E})/\mathbb{Q}(E[2]))$ except for $p \nmid 2F_E$ and the bad primes for E. Since order of $|\mathrm{Gal}(\mathbb{Q}(\zeta_{F_E})/\mathbb{Q}(E[2]))|$ is $\frac{\varphi(F_E)}{3}$, we see that $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_{F_E})/\mathbb{Q}(E[2]))$ for a prime number p which belongs to one of a third of the congruence classes of $(\mathbb{Z}/F_E\mathbb{Z})^\times$. Thus we have proved this theorem. □

A.2. Examples: 3-divisibility of $|E(\mathbb{F}_p)|$ for $p \equiv a \pmod{b}$

Proposition A 1. *Let E_i be an elliptic curve over $\mathbb{Q}$ defined by one of the following Weierstrass equations:*

$$E_1 \colon y^2 = x^3 + x^2 - 2x - 1.$$
$$E_2 \colon y^2 = x^3 + 12x + 8.$$
$$E_3 \colon y^2 = x^3 + 9x + 18.$$

(i) *If $p \equiv 2 \pmod 3$, then $3 \mid |E_1(\mathbb{F}_p)|$.*

(ii) *If $p \equiv 2 \pmod 3$ or $p \equiv \pm 1 \pmod 8$, then $3 \mid |E_2(\mathbb{F}_p)|$.*

(iii) *If $p \equiv 1 \pmod 4$ or $p \equiv 11 \pmod{12}$, then $3 \mid |E_3(\mathbb{F}_p)|$.*

Proof. First, we prove (i). Let $\psi_{E_1,3}(x)$ be the 3rd division polynomial of E. Then 2 is a root of $\psi_{E_1,3}(x)$ and

$$\psi_{E_1,3}(x) = (x - 2)(3x^3 + 10x^2 + 8x + 4).$$

Let $f(x) := 3x^3 + 10x^2 + 8x + 4$ and Δ_f the descriminant of f. Then $\mathbb{Q}(\sqrt{\Delta_f}) = \mathbb{Q}(\sqrt{-3})$. If $p \equiv 2 \pmod 3$, then $\left(\frac{-3}{p}\right) = -1$. Then from the proof of Theorem 1, $f \bmod p$ has a root in $\mathbb{F}_p$. Let a be this root. If $\sqrt{a^3 + a^2 - 2a - 1} \in \mathbb{F}_p$, then $(a, \pm\sqrt{a^3 + a^2 - 2a - 1}) \in E(\mathbb{F}_p)[3]$ and so $3 \mid |E(\mathbb{F}_p)|$. Since a is a root of $f \bmod p$, we have

$$3y^2|_{x=a} = 3y^2|_{x=a} - f(a) = -7(a + 1)^2.$$

Thus if $\left(\frac{-7\cdot 3^{-1}}{p}\right) = \left(\frac{-7\cdot 3}{p}\right) = 1$, then $\sqrt{a^3 + a^2 - 2a - 1} \in \mathbb{F}_p$. If $p \equiv 2 \pmod 3$ and $\left(\frac{7}{p}\right) = -1$, $\left(\frac{-7\cdot 3}{p}\right) = 1$. If $p \equiv 2 \pmod 3$ and $\left(\frac{7}{p}\right) = 1$, then $\left(\frac{-7\cdot 3}{p}\right) = -1$. However, since the point $(2, \pm\sqrt{7}) \in E[3]$, $\left(\frac{7}{p}\right) = 1$ implies that $(2, \pm\sqrt{7}) \in E(\mathbb{F}_p)[3]$. Thus we prove (i). Similarly, we can prove (ii) and (iii). □

Note that if $p \equiv 3 \pmod 4$, then $2 \mid |E_3(\mathbb{F}_p)|$ (see [16]). So if $p \equiv 11 \pmod{12}$, then $6 \mid |E_3(\mathbb{F}_p)|$.

Shinnya Okumura
Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
E-mail: s-okumura(at)math.kyushu-u.ac.jp