J. Math. Kyoto Univ. (JMKYAZ)
48-4 (2008), 725–746

Study of group orders of elliptic curves

By

Hidemi Sakagawa

1. Introduction

In this paper, we study the group of points modulo p of elliptic curves defined over $\mathbb{Q}$. In particular, we are interested in the frequency with which this group is cyclic. Let E be an elliptic curve over $\mathbb{Q}$ and for each prime p where E has good reduction, let $E_p(\mathbb{F}_p)$ be the group of rational points on the reduction of E modulo p. J.-P.Serre raised the question of how often this group becomes cyclic. Assuming the Generalized Riemann Hypothesis (GRH), he ([16]) showed that, for some constant C_E depending only on E, we have $f(x,E) \sim C_E \mathrm{Li}\, x$, where $f(x,E)$ denotes the number of primes $p \leq x$ such that E has good reduction at p and $E_p(\mathbb{F}_p)$ is cyclic, and Li x is the logarithmic integral. In 1980 ([10]), Ram Murty removed the GRH in the case for an elliptic curves over $\mathbb{Q}$ and with complex multiplication. In 1990 ([5]), Rajiv Gupta and Ram Murty proved unconditionally that for an elliptic curve E defined over $\mathbb{Q}$, the group $E_p(\mathbb{F}_p)$ is cyclic for infinitely many primes p if and only if E has an irrational 2-division points. By the fundamental theorem of finite abelian group, if the group order of $E_p(\mathbb{F}_p)$ is square-free, then the group becomes cyclic. Here, a natural question arises. Namely, how often the group $E_p(\mathbb{F}_p)$ becomes cyclic with non-square-free order? For this question, we will show the following result.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$. We assume that the isomorphism $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ holds for any prime q. Then, under the GRH, the primes $p \leq x$ such that $E_p(\mathbb{F}_p)$ is a cyclic group with non-square-free order have positive density in the set of rational primes.*

By the way, the group which has the prime order clearly becomes cyclic. So another natural question is as follows. Namely, how often the group $E_p(\mathbb{F}_p)$ has prime order? As to this problem, Koblitz ([7]) conjectured the number of primes $p \leq x$ such that $E_p(\mathbb{F}_p)$ has prime order becomes $\sim C_E \frac{x}{(\log x)^2}$, where C_E is the constant depending only on E. In 2001, assuming the GRH, Ali Miri and Kumar Murty ([13]) showed that, for an elliptic curve E over $\mathbb{Q}$ without complex multiplication, the number of primes $p \leq x$ such that $\sharp E_p(\mathbb{F}_p)$ has at most 16 prime divisors (counting multiplicity) is $\gg \frac{x}{(\log x)^2}$. However, it seems

Received January 17, 2007

that the above estimate is not best possible. Because, the numerical results listed at the end of this paper, suggest that the following conjecture holds.

Conjecture 1.2. *Let E be a torsion-free elliptic curve over $\mathbb{Q}$ without complex multiplication. Then, the number of primes $p \leq x$ such that $\sharp E_p(\mathbb{F}_p)$ is a product of exactly k different prime numbers is*

$$\sim C_{E,k} \frac{x(\log\log x)^{k-1}}{(\log x)^2},$$

where $C_{E,k}$ is the positive constant depending only on E and k.

So the numbers of primes $p \leq x$ such that $\sharp E_p(\mathbb{F}_p)$ has at most 16 prime divisors (counting multiplicity) should have the magnitude $\frac{x(\log\log x)^{15}}{(\log x)^2}$. In this paper, we consider the following meek functions. Namely, let $\pi^{\alpha}(x, E)$ be the number of primes $p \leq x$ such that E has good reduction at p and $\sharp E_p(\mathbb{F}_p)$ is not divisible by the primes q less than x^{α}. By a classical result due to Hasse and Weil, we know $\pi(x, E) \sim \pi^{\frac{1}{2}}(x, E)$, where $\pi(x, E)$ denotes the number of primes $p \leq x$ such that $E_p(\mathbb{F}_p)$ has prime order. Under the notation above, we will show the following result.

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Then, under the GRH, there exists the constant A_E and B_E depending only on E such that the following inequality holds*:

$$A_E \frac{x}{(\log x)^2} \leq \pi^{\frac{1}{22}}(x, E) \leq B_E \frac{x}{(\log x)^2}.$$

Finally, we will show the following unconditional result by using a similar technics given in [2].

Theorem 1.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Then, the natural density of primes $p \leq x$ such that $E_p(\mathbb{F}_p)$ has prime order is zero. That is, we have unconditionally*

$$\lim_{x\to\infty} \frac{\pi(x, E)}{\mathrm{Li}(x)} = 0.$$

2. Preliminaries

Let E be an elliptic curve defined over the field $\mathbb{Q}$, and $E[m]$ be a group consisting of the m-division points of E. Then, $\mathbb{Q}(E[m])$ is a Galois extension of $\mathbb{Q}$, and the elements of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ naturally act $\mathbb{Z}$-lineally on $E[m]$. As is well known, $E[m]$ is isomorphic to the group $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$. Now we fix two elements P and Q of $E[m]$ such that P and Q correspond to the vectors $(1, 0)$ and $(0, 1)$ respectively. Then, we have the natural group homomorphisms ρ_m from $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ to $\mathrm{GL}_2(m)$, where $\mathrm{GL}_2(m)$ denotes the two-dimensional general linear group over the ring $\mathbb{Z}/m\mathbb{Z}$.

Proposition 2.1 (Serre [14]). *Under the notation above, let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N without complex multiplication. Then, there exists a positive absolute constant a such that for any prime $q \geq aN(\log\log N)^{1/2}$, the map ρ_q becomes an isomorphism. In particular, by the chinese remainder theorem, for the square-free integers k composed of primes $\geq aN(\log\log N)^{1/2}$, the map ρ_k becomes an isomorphism.*

Throughout this paper, we denote by a the absolute positive constant stated above proposition. Now let p be a good prime of E. Then we are interested in the prime factors of $\sharp E_p(\mathbb{F}_p)$. From a classical result of algebraic number theory, we easily know the following lemma which is often used throughout this paper.

Lemma 2.2. *Assume that the square-free integer k is composed of primes equal or greater than $aN(\log\log N)^{1/2}$. Then, for good primes p of E, the next two statements are equivalent.*

(1) *$\sharp E_p(\mathbb{F}_p)$ is divisible by k*

(2) $\left(\dfrac{\mathbb{Q}(E[k])/\mathbb{Q}}{p}\right) \subseteq M(k)$,

where $\left(\frac{\mathbb{Q}(E[k])/\mathbb{Q}}{p}\right)$ denotes the Artin symbol of the prime p by the extension $\mathbb{Q}(E[k])/\mathbb{Q}$ and $M(k)$ is the subset of $\mathrm{GL}_2(k)$ defined as follows:

$$M(k) = \left\{ C \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} C^{-1} \middle| C \in \mathrm{GL}_2(k), a \in (\mathbb{Z}/k\mathbb{Z})^*, b \in \mathbb{Z}/k\mathbb{Z} \right\}.$$

One of the main tool used in this paper is the Chebotarev density thorem which we recall now. Let $K/\mathbb{Q}$ be a finite Galois extension of Galois group G of degree n_K and discriminant d_K. For each conjugacy class C of G, we define

$$\pi_C(x, K) = \sharp \left\{ p \leq x \;\middle|\; p \text{ is unramified in } K, \ \left(\frac{K/\mathbb{Q}}{p}\right) = C \right\}.$$

The classical Chebotarev density theorem asserts that

$$\pi_C(x, K) \sim \frac{|C|}{|G|} \mathrm{Li}\ x.$$

In [8], Lagarias and Odlyzko proved the effective versions of this theorem. Here, we recall their results.

Proposition 2.3. *Assuming the GRH for the Dedekind zeta function of K, we have*

$$\pi_C(x, K) = \frac{|C|}{|G|} \mathrm{Li}\ x + O\left(\frac{|C|}{|G|} \sqrt{x} \log(|d_K| x^{n_K}) \right),$$

where the implied constant is absolute.

Proposition 2.4. *There exists an positive constant A and there exists an absolute positive constant c such that if*

$$\sqrt{\frac{\log x}{n_K}} \geq c \max(\log |d_K|, |d_K|^{1/n_K}),$$

then

$$\pi_C(x, K) = \frac{|C|}{|G|} \mathrm{Li}\ x + O\left(x \exp\left(-A\sqrt{\frac{\log x}{n_K}} \right) \right),$$

where the implied constant is absolute.

Now we apply the Chebotarev density theorem to $M(k)$, and get the following estimate.

Proposition 2.5. *Let k be a square-free integer whose prime divisors are equal or greater than $aN(\log\log N)^{1/2}$. Put*

$$\pi_k(x, E) = \sharp \left\{ p \leq x \;\middle|\; p\text{: good prime of } E,\ k | \sharp E_p(\mathbb{F}_p) \right\}.$$

Then, assuming the GRH of $\mathbb{Q}(E[k])/\mathbb{Q}$, we have

$$\pi_k(x, E) = \frac{\sharp M(k)}{\sharp \mathrm{GL}_2(k)} \frac{x}{\log x} + O\left(\frac{\sharp M(k)}{\sharp \mathrm{GL}_2(k)} \sqrt{x} (\log d(k) + n(k) \log x) \right),$$

where $n(k)$(resp. $d(k)$) denotes the extension degree (resp. the discriminant) of the number field $\mathbb{Q}(E[k])/\mathbb{Q}$.

Finally we quote the next result due to Hensel which is used frequently in this paper (see [15, p.130]).

Proposition 2.6. *Let $K/\mathbb{Q}$ be a finite Galois extension which is ramified only at the primes $p_1, p_2, \cdots, p_m$. Then we have*

$$\frac{1}{n_k} \log |d_k| \leq \log n_k + \sum_{i=1}^{m} \log p_i,$$

where n_k(resp. d_k) denotes the degree (resp. the discriminant) of $K/\mathbb{Q}$.

3. The orders of $M(p)$ and $M(p^2)$

In this section, we compute the explicit orders of $M(p)$ and $M(p^2)$ respectively.

Proposition 3.1. $\sharp M(p) = p(p^2 - 2)$.

Proof. In this proof, we identify the elements of $\mathbb{Z}/p\mathbb{Z}$ with the integers k $(0 \leq k \leq p-1)$. First of all, assume that $a \neq 1$. Then two matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}$ are conjugate to each other in $\mathrm{GL}_2(p)$ if and only if $a = a'$. For, if two matrices are conjugate, then considering the determinants, we know $a = a'$. Conversely, if $a = a' \neq 1$, then we have

$$\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{b'-b}{1-a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{b'-b}{1-a} \\ 0 & 1 \end{pmatrix}^{-1}.$$

Next we consider the matrices of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. If $b \neq 0$, then we have the relation

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & 1 \end{pmatrix}^{-1}.$$

From the above, we easily know that $M(p)$ can be represented as the direct sum of conjugacy classes, and we can take the next elements as the perfect representatives;

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \cdots, \begin{pmatrix} p-1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

By easy calculations, we know the order of the stabilizer of $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ $\left(\textit{resp.} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)$ is $(p-1)^2 (\textit{resp. } p(p-1))$, where a is an integer belonging to $\{2, 3, \cdots, p-1\}$. So we have

$$\sharp M(p) = \frac{\sharp \mathrm{GL}_2(p)}{(p-1)^2} + \frac{\sharp \mathrm{GL}_2(p)}{p(p-1)} + 1 = p(p^2-2),$$

which is the desired result. □

Proposition 3.2. $\sharp M(p^2) = p^6 + p^4 - 2p^2 + 1.$

Proof. In this proof, we identify the elements of $\mathbb{Z}/p^2\mathbb{Z}$ with the integers k $(0 \leq k \leq p^2-1)$. If $a \not\equiv 1 \bmod p$, then we know the two matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}$ are conjugate to each other in $\mathrm{GL}_2(p^2)$ if and only if $a = a'$. For, if two matrices are conjugate, then considering the determinants, we see $a = a'$. Conversely, if $a = a'$, then we have

$$\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{b'-b}{1-a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{b'-b}{1-a} \\ 0 & 1 \end{pmatrix}^{-1}.$$

Next, if $a = kp+1(k = 1, 2, \cdots, p-1)$ and $\mathrm{ord}_p(b) = \mathrm{ord}_p(b')$, then two matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a & b' \\ 0 & 1 \end{pmatrix}$ are conjugate. Because if $\mathrm{ord}_p(b) = \mathrm{ord}_p(b') = 0$, then we have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p \\ 0 & \frac{b'}{b} \end{pmatrix} \begin{pmatrix} a & b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & \frac{b'}{b} \end{pmatrix}^{-1},$$

and if $\mathrm{ord}_p(b) = \mathrm{ord}_p(b') = 1$, then from $\frac{b}{p}, \frac{b}{p'} \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$, we have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p \\ 0 & \frac{b'}{p}/\frac{b}{p} \end{pmatrix} \begin{pmatrix} a & b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & \frac{b'}{p}/\frac{b}{p} \end{pmatrix}^{-1}.$$

When $a = kp + 1(k = 1, 2, \cdots, p-1)$, we have

$$\begin{pmatrix} a & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{k} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{k} \\ 0 & 1 \end{pmatrix}^{-1}.$$

So two matrices $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a & p \\ 0 & 1 \end{pmatrix}$ are conjugate. Finally, by easy calculations, we know the matrices of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ are conjugate to either $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. From the above, we know that $M(p^2)$ can be represented as the direct sum of conjugacy classes, and we can take next elements as the perfect representatives;

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| a \not\equiv 1 \mathrm{mod}\ p \right\} \sqcup \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix} \middle| a \equiv 1 \mathrm{mod}\ p \right\}.$$

By easy calculations, if $a \not\equiv 1 \bmod p$, then we know that the order of the stabilizer of $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ is $p^2(p-1)^2$. And, if $a \equiv 1 \bmod p$, we know the order of the stabilizer of $\begin{pmatrix} kp+1 & 0 \\ 0 & 1 \end{pmatrix} \left(resp. \begin{pmatrix} kp+1 & 1 \\ 0 & 1 \end{pmatrix}, resp. \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)$ is $p^4(p-1)^2(resp.\ p^4(p-1),\ resp.\ p^3(p-1))$, where k is an integer belonging to $\{1, 2, \cdots, p-1\}$. So we conclude that

$$\begin{aligned} \sharp M(p^2) &= \phi(p^2)\frac{\sharp \mathrm{GL}_2(p^2)}{p^2(p-1)^2} + (p-1)\frac{\sharp \mathrm{GL}_2(p^2)}{p^4(p-1)^2} \\ &\quad + (p-1)\frac{\sharp \mathrm{GL}_2(p^2)}{p^4(p-1)} + \frac{\sharp \mathrm{GL}_2(p^2)}{p^3(p-1)} + 1 \\ &= p^6 + p^4 - 2p^2 + 1. \end{aligned}$$

□

From the above, we get the following result.

Proposition 3.3. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Further more, we assume* $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ *for any prime q. Then, for any square-free integer k, we have*

$$\pi_k(x, E) = \prod_{p|k} \frac{p^2 - 2}{(p-1)^2(p+1)} \mathrm{Li}(x) + O\left(k^3 \sqrt{x} \log kNx\right).$$

Proof. Since the ramified primes of $\mathbb{Q}(E[k])/\mathbb{Q}$ are exactly the prime divisors of kN, applying Hensel's theorem to the field extensions $\mathbb{Q}(E[k])/\mathbb{Q}$, we know

$$\begin{aligned} &O\left(\frac{\sharp M(k)}{\sharp \mathrm{GL}_2(k)} \sqrt{x}(\log d_k + n_k \log x)\right) \\ &= O\left(\sharp M(k) \sqrt{x}(\log n_k + \log kN + \log x)\right) \\ &= O\left(k^3 \sqrt{x} \log kNx\right). \end{aligned}$$

□

4. Selberg's sieve method

We follow the notation of [4]. We first recall a theorem which is used to show the upper bound of Theorem 5.1. Let A be any finite set of elements and let P be a set of primes. For each prime $p \in P$, let A_p be a set of A. Let $A_1 := A$ and for a square-free positive integers d composed of primes in P, let $A_d := \cap_{p|d} A_p$. Let z be a positive real number and set

$$P(z) := \prod_{\substack{p \in P \\ p < z}} p.$$

We denote by $S(A, P, z)$ the number of elements of

$$A \setminus \cup_{p|P(z)} A_p.$$

In 1947, Selberg proved the next theorem.

Theorem 4.1. *Under the notation above, assume that there exist a positive real number X and a multiplicative function $f(\cdot)$ satisfying $f(p) > 1$ for any prime $p \in P$, such that for any square-free integer d composed of primes in P we have*

$$\sharp A_d = \frac{X}{f(d)} + R_d$$

for some real number R_d. We write

$$f(n) = \sum_{d|n} f_1(d)$$

for some multiplicative function $f_1(\cdot)$ *that is uniquely determined by* f *by using the Möbius inversion formula*; *that is,*

$$f_1(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Also, we set

$$V(z) \ := \sum_{\substack{d<z \\ d|P(z)}} \frac{\mu^2(d)}{f_1(d)}.$$

Then, we have

$$S(A,P,z) \leq \frac{X}{V(z)} + O\left(\sum_{\substack{d_1,d_2\leq z \\ d_1,d_2|P(z)}} \left|R_{[d_1,d_2]}\right|\right).$$

In a sense, the first lower bound sieve was derived by Viggo Brun in the year 1919. Selberg indicated how his method can be developed into a lower bound sieve. The next treatment is due to Bombieri [1]. For more details, see [4].

Theorem 4.2. *Under the notation above, assume that there exist a positive real number* X *and a multiplicative function* $f(\cdot)$ *such that, for any positive square-free integer* d *composed of primes in* P,

$$\sharp A_d = \frac{X}{f(d)} + R_d$$

for some real number R_d. *We write*

$$f(n) = \sum_{d|n} f_1(d)$$

for some multiplicative function $f_1(\cdot)$ *that is uniquely determined by* f. *Then, for any* $y, z > 0$ *and for any sequences of real numbers* (ω_t),(λ_d) *that are supported only at positive square-free integers* $t \leq y$, $d \leq z$ *composed of primes in* P, *we have*

$$\sum_{a\in A}\left(\sum_{\substack{t \\ a\in A_t}} \omega_t\right)\left(\sum_{\substack{d \\ a\in A_d}} \lambda_d\right)^2 = \Delta X + E,$$

where

$$E \ := \ O\left(\sum_{\substack{m\leq yz^2 \\ m|P(yz)}}\left(\sum_{\substack{t\leq y \\ t|m}} |\omega_t|\right)\left(\sum_{\substack{d\leq z \\ d|m}} |\lambda_d|\right)^2 |R_m|\right)$$

and

$$\Delta = \sum_{\substack{\delta < z \\ \delta | P(z) \\ (t,\delta)=1}} \sum_{\substack{t<y \\ t|P(y)}} \frac{w_t}{f(t)} \frac{1}{f_1(\delta)} \left(\sum_{\substack{r \le \frac{z}{\delta} \\ r|P(z) \\ r|t}} \mu(r) z_{\delta r} \right)^2 ,$$

with

$$z_r \ := \ \mu(r) f_1(r) \sum_{\substack{s \le z/r \\ s|P(z)}} \frac{\lambda_{sr}}{f(sr)}$$

for any positive square-free integers r *composed of primes in* P.

5. Asymptotic behavior of $\pi^{\frac{1}{22}}(x, E)$

In this section, we prove the following result by using a methods given in [13].

Theorem 5.1. *Let* E *be an elliptic curve defined over* $\mathbb{Q}$ *without complex multiplication. Then, under the GRH, there exist the constants* A_E *and* B_E *depending only on* E *such that the following inequality holds*:

$$A_E \frac{x}{(\log x)^2} \le \pi^{\frac{1}{22}}(x, E) \le B_E \frac{x}{(\log x)^2}.$$

Proof. We first show the upper bound. Without loss of generality, we can assume the isomorphism $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ holds for any prime q, since the number of primes which don't satisfy the isomorphism is finite, and such finite primes don't verify the asymptotic nature. Put

$$\begin{aligned} A &= \left\{ p \le x \;\middle|\; p : \text{good primes of } E \right\}, \\ A_d &= \left\{ p < x \;\middle|\; p \in A \text{ and } \sharp E_p(\mathbb{F}_p) \text{ is be divisible by } d \right\}, \\ P &= \left\{ p < x \;\middle|\; p : \text{prime} \right\}, \\ P(z) &= \prod_{\substack{p<z \\ p \in P}} p. \end{aligned}$$

Then, by Proposition 3.3, we know

$$\sharp A_d = \frac{X}{f(d)} + R_d,$$

with $X = \mathrm{Li}(x)$, $f(d) \sim d$, and $R_d = O\left(k^3\sqrt{x}\log kNx\right)$. By Theorem 4.1, we have

$$S(A,P,z) \le \frac{X}{V(z)} + O\left(\sum_{\substack{d_1,d_2\le z\\ d_1,d_2|P(z)}} \left|R_{[d_1,d_2]}\right|\right),$$

where we set

$$V(z) = \sum_{d\le z}\frac{\mu^2(d)}{f_1(d)},$$

and

$$R_d = d^3\sqrt{x}\log(dNx).$$

Put $r_d := d^3\log(dNx)$, then for any positive real number ϵ, we have

$$\begin{aligned}\sum_{\substack{d_1,d_2\le z\\ d_1,d_2|P(z)}} \left|R_{[d_1,d_2]}\right| &= \sqrt{x}\sum_{\substack{d_1,d_2\le z\\ d_1,d_2|P(z)}}\left|r_{\frac{d_1d_2}{(d_1,d_2)}}\right|\\ &\ll \sqrt{x}\sum_{\substack{d_1,d_2\le z\\ d_1,d_2|P(z)}}|r_{d_1}|\,|r_{d_2}|\\ &\le \sqrt{x}\left(\sum_{d\le z}|r_d|\right)^2\\ &\le x^{\frac{1}{2}+\epsilon}z^{10}\\ &= O\left(x^{1-\epsilon}\right),\end{aligned}$$

provided that $z = x^{\frac{1}{22}}$. Next, we estimate the term $V(z) = \sum_{d\le z}\frac{\mu^2(d)}{f_1(d)}$. Using the equality,

$$\sum_{d^2|n}\mu(d) = \mu^2(n),$$

we have

$$\begin{aligned}V(z) &= \sum_{n\le z}\frac{\mu^2(n)}{f_1(n)}\\ &= \sum_{n\le z}\frac{1}{f_1(n)}\sum_{d^2|n}\mu(d)\\ &= \sum_{d^2\le z}\mu(d)\sum_{\substack{n\le z\\ d^2|n}}\frac{1}{f_1(n)}\\ &= \sum_{d\le z^{\frac{1}{2}}}\frac{\mu(d)}{f_1(d)^2}\sum_{n\le\frac{z}{d^2}}\frac{1}{f_1(n)}.\end{aligned}$$

Then, from

$$\sum_{d\le z^{\frac{1}{2}}}\frac{\mu(d)}{f_1(d)^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{f_1(d)^2}+O\left(\sum_{d>z^{\frac{1}{2}}}\frac{1}{d^2}\right)$$
$$=\prod_{p:\text{prime}}\left(1-\frac{1}{f_1(p)^2}\right)+O\left(z^{-\frac{1}{2}}\right),$$

we have

$$V(z)=A\prod_{p}\left(1-\frac{1}{f_1(p)^2}\right)\log(z)+B+O\left(\frac{1}{z}\right)$$
$$=A'\log(x)+B'+O\left(\frac{1}{x}\right),$$

where A, B, A', and B' are the some real numbers. From the above, we conclude that there exists a positive real number B_E such that for all $x(\ge 1)$, we have the following inequality:

$$\pi^{\frac{1}{22}}(x,E)\le B_E\frac{x}{(\log x)^2}.$$

Secondly, we show the existence of the lower bound. To do so, we apply Theorem 4.2 to two cases. The one is as follows:

$$w_t=\begin{cases}1 & \text{if } t=1\\ 0 & \text{otherwise,}\end{cases}$$

and

$$z_d=\begin{cases}\frac{1}{V(z)} & \text{if } d<z \text{ and } d \text{ is square-free}\\ 0 & \text{otherwise.}\end{cases}$$

By this choice, we have

$$E=O\left(\sum_{\substack{m\le yz^2\\ m|P(z)}}d(m)^3|R_m|\right)$$
$$=O\left(\sum_{m\le yz^2}\frac{d(m)^3}{\sqrt{m}}m^{\frac{7}{2}}\sqrt{x}\log(mNx)\right)$$
$$\ll (yz^2)^{\frac{7}{2}}x^{\frac{1}{2}+\epsilon}\log(xN)$$
$$\ll x^{1-\epsilon}$$

provided that $yz^2\ll x^{\frac{1}{7}-\epsilon}$, where $d(m)$ denotes the number of positive divisors of m. By the way, from

$$\Delta=\sum_{\substack{\delta<z\\ \delta|P(z)}}\frac{1}{f_1(\delta)}{z_1}^2,$$

we have finally

$$\sum_{p\le x}\left(\sum_{\substack{d\\ d|\sharp E_p(\mathbb{F}_p)}}\lambda_d\right)^2 = {z_1}^2\left(\sum_{\substack{\delta<z\\ \delta|P(z)}}\frac{1}{f_1(\delta)}\right)\mathrm{Li}(x)+O\left(x^{1-\epsilon}\right)$$

$$= {z_1}^2\left(\sum_{\delta<z}\frac{\mu^2(\delta)}{f_1(\delta)}\right)\mathrm{Li}(x)+O\left(x^{1-\epsilon}\right).$$

Now, we apply seive methods for another case. In other words, we select (w_t) and (z_d) as follows:

$$w_t=\begin{cases}1 & \text{if } t \text{ is a prime less than } y\\ 0 & \text{otherwise,}\end{cases}$$

and

$$z_d=\begin{cases}\frac{1}{V(z)} & \text{if } d<z \text{ and } d \text{ is square-free}\\ 0 & \text{otherwise.}\end{cases}$$

Then, we have

$$\Delta=\sum_{\substack{\delta<z\\ \delta|P(z)\\ (t,\delta)=1}}\sum_{\substack{t<y\\ t|P(y)}}\frac{w_t}{f(t)}\frac{1}{f_1(\delta)}\left(\sum_{\substack{r\le\frac{z}{\delta}\\ r|P(z)\\ r|t}}\mu(r)z_{\delta r}\right)^2$$

$$=\sum_{\delta<z}\sum_{\substack{l<y\\ l:\text{prime}\\ l\nmid\delta}}\frac{\mu^2(\delta)}{f_1(\delta)}\frac{1}{f(l)}\left(\sum_{\substack{r\le\frac{z}{\delta}\\ r|l}}\mu(r)z_{\delta r}\right)^2$$

$$={z_1}^2\sum_{\delta<z}\frac{\mu^2(\delta)}{f_1(\delta)}\left(\sum_{\substack{\frac{z}{\delta}<l<y\\ l\nmid\delta}}\frac{1}{f(l)}\right).$$

From the above, we know

$$\sum_{p\le x}\left(\sum_{\substack{t\\ p\in A_t}}w_t\right)\left(\sum_{\substack{d\\ p\in A_d}}\lambda_d\right)^2=\sum_{p\le x}\left(\sum_{\substack{l<y\\ l:\text{prime}\\ l|\sharp E_p(\mathbb{F}_p)}}1\right)\left(\sum_{\substack{d\\ d|\sharp E_p(\mathbb{F}_p)}}\lambda_d\right)^2$$

$$=\Delta X+O\left(x^{1-\epsilon}\right)$$

$$\sim\mathrm{Li}(x)\left\{1+\log\left(\frac{\log y}{\log z}\right)\right\}\left(\sum_{\delta<z}\frac{\mu^2(\delta)}{f_1(\delta)}\right){z_1}^2.$$

Combining the two equations derived from the sieve method, we know the following estimation:

$$\sum_{p\le x}\left(1-\sum_{\substack{l:\text{prime}\\ l<y\\ l\mid\sharp E_p(\mathbb{F}_p)}}1\right)\left(\sum_{\substack{d\\ d\mid\sharp E_p(\mathbb{F}_p)}}\lambda_d\right)^2$$
$$={z_1}^2\left(\sum_{\delta<z}\frac{\mu^2(\delta)}{f_1(\delta)}\right)\left\{\log\left(\frac{\log z}{\log y}\right)\right\}\mathrm{Li}(x)+O\left(x^{1-\epsilon}\right).$$

Now we choose y and z so that

$$y=x^{\frac{1}{21}-\epsilon},$$

and

$$z=x^{\frac{1}{21}+\epsilon}.$$

Then we have

$$\log\left(\frac{\log z}{\log y}\right)>0.$$

Hence, for many primes p, we have

$$1-\sum_{\substack{l:\text{prime}\\ l<y\\ l\mid\sharp E_p(\mathbb{F}_p)}}1>0.$$

This means that for many p, the number $\sharp E_p(\mathbb{F}_p)$ has no prime divisors less than $y=x^{\frac{1}{21}-\epsilon}$. By easy estimations, we know the number of such primes is

$$\gg\frac{x}{(\log x)^2},$$

which is the desired result. □

6. Unconditional result of prime density

In this section, removing GRH, we show unconditionally the following result.

Theorem 6.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Then, we have unconditionally*

$$\pi(x,E)=O\left(\frac{x}{\log x}\frac{1}{\log\log\log x}\right).$$

In particular, the natural density of such primes is zero. That is, we have unconditionally

$$\lim_{x\to\infty}\frac{\pi(x,E)}{\mathrm{Li}(x)}=0.$$

Proof. Without loss of generality, we can assume the isomorphism $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ holds for any prime q, since the primes which don't satisfy the isomorphism is finite, and such finite primes don't verify the asymptotic nature. At first, we consider the following quantity:

$$N(x,y) = \sharp \left\{ p < x \middle| \sharp E_p(\mathbb{F}_p) \text{ is not divisible by primes less than } y \right\}.$$

By the inclusion-exclusion principle, we have

$$N(x,y) = {\sum}' \mu(k)\pi_k(x,E),$$

where $\sum'$ means the sum over k which are square-free integers whose prime divisors are less than y. Clearly, the following inequality holds asymptotically;

$$\pi(x,E) \leq N(x,y).$$

Then, by Proposition 2.4, there exists positive absolute constants A and c such that if

$$\sqrt{\frac{\log x}{n(q)}} \geq c \max(\log|d(q)|, |d(q)|^{\frac{1}{n(q)}}),$$

then we have

$$\pi_q(x,E) = \frac{\sharp M(q)}{\sharp \mathrm{GL}_2(q)} \mathrm{Li}(x) + O\left(x \exp\left(-A\sqrt{\frac{\log x}{n(q)}} \right) \right),$$

where the implied constant is absolute. By Proposition 2.6, we know

$$|d(k)|^{\frac{2}{n(k)}} \leq (kNk^4)^2 \ll k^{10}.$$

So we have

$$n(k)|d(k)|^{\frac{2}{n(k)}} \ll k^{14},$$

and

$$n(k)(\log|d(k)|)^2 \ll k^{14}.$$

From the above, if we choose y so that

$$k^{14} \ll \log x,$$

then L-O conditions are all satisfied. By the way, we have

$$k \leq \prod_{p \leq y} p = \exp\left(\sum_{p \leq y} \log p \right) \leq \exp(2y).$$

So if we choose y of the form $d\log\log x$ for some d, then all L-O conditions are satisfied. By this choice, we have

$$\frac{n(k)}{m(k)} \ll k \ll (\log x)^{\frac{1}{14}}.$$

Since the number of the square-free positive integers whose all divisors are less than y is at most $2^y \asymp (\log x)^d$, for any positive real number B sufficiently large, we have

$$\begin{aligned} O\left(\sum{}' x\exp\left(-A\sqrt{\frac{\log x}{n(k)}}\right)\right) &\ll (\log x)^d x\exp(-A(\log x)^{\frac{5}{14}}) \\ &= O\left(\frac{x}{(\log x)^B}\right). \end{aligned}$$

Combining the above results, for some C_E, we have

$$\begin{aligned} \pi(x,E) &\le \left(\sum{}' \frac{m(k)}{n(k)}\mu(k)\right)\mathrm{Li}(x) + O\left(\frac{x}{(\log x)^B}\right) \\ &= \prod_{p<y}\left(1-\frac{m(p)}{n(p)}\right)\mathrm{Li}(x) + O\left(\frac{x}{(\log x)^B}\right) \\ &= C_E\frac{x}{\log x}\frac{1}{\log\log\log x} + O\left(\frac{x}{(\log x)^B}\right), \end{aligned}$$

which is the desired result. Here, the last equality follows from the following result due to Mertense:

$$\prod_{p<z}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right).$$

□

7. Estimation of the square-free order

Theorem 7.1. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. We assume that the isomorphism $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ holds for any prime q. Then we have unconditionally*

$$\begin{aligned} \sharp\left\{p<x \,\middle|\, \sharp E_p(\mathbb{F}_p) \text{ is square free}\right\} &\ll \sum_{k=1}^{\infty}\frac{\sharp M(k^2)}{\sharp\mathrm{GL}_2(k^2)}\mu(k)\mathrm{Li}(x) \\ &= \prod_{p:\mathrm{prime}}\left(1-\frac{\sharp M(p^2)}{\sharp\mathrm{GL}_2(p^2)}\right)\mathrm{Li}(x). \end{aligned}$$

In particular, under the GRH, the primes $p \le x$ such that $E_p(\mathbb{F}_p)$ is a cyclic group with non-square-free order have positive density in the set of rational primes.

Proof. Put

$$N(x,y) = \sharp\left\{ p < x \,\middle|\, \left(\frac{\mathbb{Q}(E[q^2])/\mathbb{Q}}{p}\right) \not\subset M(q^2) \text{ for any prime } q \text{ less than } y \right\}.$$

Then, by the inclusion-exclusion principle, we have

$$N(x,y) = \sum{}' \mu(k)\pi_{M(k^2)}(x, \mathbb{Q}(E[k^2])),$$

where $\sum'$ means the sum over k which are square-free integers whose prime divisors are less than y. Clearly, we have

$$f(x,E) {:=} \sharp\left\{ p < x \,\middle|\, \sharp E_p(\mathbb{F}_p) \text{ is square free} \right\} \leq N(x,y)$$

Then, by Proposition 2.4, there exist positive absolute constants A and c such that if

$$\sqrt{\frac{\log x}{\sharp \mathrm{GL}_2(q^2)}} \geq c \max(\log|d(q^2)|, |d(q^2)|^{\frac{1}{n(q^2)}}),$$

then

$$\pi_{M(q^2)}(x, \mathbb{Q}(E[q^2])) = \frac{\sharp M(q^2)}{\sharp \mathrm{GL}_2(q^2)} \mathrm{Li}(x) + O\left(x \exp\left(-A\sqrt{\frac{\log x}{n(q^2)}} \right) \right),$$

where the implied constant is absolute. By Proposition 2.6, we know

$$|d(k^2)|^{\frac{2}{n(k^2)}} \leq (kNk^8)^2 \ll k^{18}.$$

So we have

$$n(k^2)|d(k^2)|^{\frac{2}{n(k^2)}} \ll k^{26},$$

and

$$n(k^2)(\log|d(k^2)|)^2 \ll k^{26}.$$

From the above, if we choose y so that

$$k^{26} \ll \log x,$$

then L-O conditions are all satisfied. On the other hand, we have

$$k \leq \prod_{p \leq y} p = \exp\left(\sum_{p \leq y} \log p \right) \leq \exp(2y),$$

so if we choose y of the form $d \log\log x$ for some d, then all conditions are satisfied. Then, by this choice, we have

$$\frac{n(k^2)}{m(k^2)} \ll k^2 \ll (\log x)^{\frac{1}{13}}.$$

Since the numbers of square-free integers whose all divisors are less than y is at most $2^y \asymp (\log x)^d$, for any positive real number B sufficiently large, we have

$$O\left(\sum{}' x \exp\left(-A\sqrt{\frac{\log x}{n(k^2)}}\right)\right) \ll (\log x)^d x \exp(-A(\log x)^{\frac{9}{26}}) = O\left(\frac{x}{(\log x)^B}\right).$$

From the above, we know

$$N(x,y) = \left(\sum{}' \frac{m(k^2)}{n(k^2)}\mu(k)\right) \mathrm{Li}(x) + O\left(\frac{x}{(\log x)^B}\right).$$

Finally we estimate the term

$$\sum{}' \frac{m(k^2)}{n(k^2)}\mu(k).$$

By

$$\sum_k{}' \frac{m(k^2)}{n(k^2)}\mu(k) = \sum_{k=1}^{\infty} \frac{m(k^2)}{n(k^2)}\mu(k) - \sum_k{}'' \frac{m(k^2)}{n(k^2)}\mu(k),$$

where $\sum''$ means the sum over the square-free integers k which have at least one prime divisor greater than y. By

$$\left|\sum_k{}'' \frac{m(k^2)}{n(k^2)}\mu(k)\right| \le \sum_k{}'' \frac{m(k^2)}{n(k^2)} \ll \sum_{\substack{q:\text{prime} \\ q>y}} \frac{1}{q^2} \ll \frac{1}{y},$$

we have

$$\sum{}' \frac{m(k^2)}{n(k^2)}\mu(k) = \sum_{k=1}^{\infty} \frac{m(k^2)}{n(k^2)}\mu(k) + O\left(\frac{1}{\log\log x}\right).$$

So we get the following estimation:

$$f(x,E) \le \left(\sum_{k=1}^{\infty} \frac{m(k^2)}{n(k^2)}\mu(k)\right) \mathrm{Li}(x) + O\left(\frac{1}{\log\log x}\mathrm{Li}(x)\right).$$

□

8. Numerical result

The curve E used here is $y^2+y=x^3-x$ (Serre curve) over $\mathbb{Q}$ of conductor 37. This curve satisfies $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ for any prime q. In the following tables, $\mathbb{P}_k$ denotes the number of primes $p \le x$ for which $\sharp E_p(\mathbb{F}_p)$ is the product of the exactly k different prime numbers. We compare these numbers with the function $\mathbb{L}_k := \frac{x(\log\log x)^{k-1}}{(\log x)^2}$.

x ($\times 10^8$)	$\mathbb{P}_1$	$\mathbb{P}_1/\mathbb{L}_1$
1	168514	0.5718041972410603279051447358
2	311287	0.5686255005075590360393390800
3	446389	0.5669181970313549098703904788
4	577219	0.5661310022615735102660467897
5	704052	0.5649392853595534408971988272
6	828986	0.5644603522342226091855410509
7	951752	0.5639783564458440852123348302
8	1072351	0.5633261052799434317993091122
9	1192178	0.5631027856599714526730239605
10	1310343	0.5627317111380662342326258552
11	1427375	0.5624027582958578735849156431
12	1543478	0.5621392978109860822921191535
13	1659057	0.5620332149154404283053194568
14	1773656	0.5618848048749182199908873398
15	1886335	0.5614025610394570707803232740
16	1999226	0.5612260597613554655364794131
17	2111180	0.5609877343496769420885828236
18	2222977	0.5608829808718263754350696880
19	2333712	0.5606661286872861638654080597
20	2444517	0.5606044405874796741477110615

x ($\times 10^8$)	$\mathbb{P}_2$	$\mathbb{P}_2/\mathbb{L}_2$	$\mathbb{P}_2/\mathbb{L}_1$
1	602709	0.7019527555309573659338995665	2.0451210932917278633904712887
2	1125132	0.6966043015733853173537504680	2.0552697242000819608175531119
3	1624139	0.6941742468113585345308047581	2.0626716913013262691553468842
4	2109021	0.6927275395435837484998529356	2.0685080922850876810964439926
5	2582112	0.6912752689538097431700303525	2.0719158641667479879070691662
6	3047569	0.6902520847405876681657956184	2.0751036461388944600427150221
7	3506708	0.6894614717303222172105245869	2.0779650732286278572220244485
8	3961177	0.6889350296665867403549412273	2.0808806181320206568040612366
9	4409772	0.6882890139206528988478641562	2.0828726057059798392495300333
10	4856197	0.6880023640467681057754322298	2.0855119975712800636793381143
11	5297574	0.6875538187665899773190055020	2.0873072807611321333207712788
12	5735545	0.6871352988206966235000545795	2.0889026204865324736472774800
13	6170826	0.6867876106245743051539006968	2.0904701739987158948954745003
14	6603730	0.6865038916091230332763587253	2.0920266063411640683990708755
15	7033544	0.6861826007186939798946465792	2.0932918144357746865983603555
16	7460196	0.6858073432700444391082313668	2.0942386734303300370110140488
17	7885329	0.6855163521895320775035119812	2.0953082400893356947690025004
18	8308249	0.6852282488835809476874187102	2.0962679618121872659420418200
19	8729792	0.6849988750010400151873712663	2.0973019313802394018726082555
20	9149221	0.6847570184011227722910839194	2.0982034162643259882362835466

x ($\times 10^8$)	$\mathbb{P}_3$	$\mathbb{P}_3/\mathbb{L}_3$	$\mathbb{P}_3/\mathbb{L}_1$
1	857191	0.3426625672208730654459638451	2.9086331796602166202056738838
2	1633132	0.3427056709127766737210294538	2.9832293057368630994708995557
3	2381821	0.3426043021380603182487722011	3.0249349042458904291602242000
4	3113666	0.3424986018126301309794734403	3.0538545219193833630148017366
5	3833492	0.3424123413273721304709211047	3.0760373252424043099826213500
6	4543366	0.3422944337883338181170683131	3.0935986526780802558847494443
7	5245405	0.3421851689417991855589595653	3.1082623317763585406631214644
8	5940592	0.3420698894103868076214319740	3.1207044656247718437335548888
9	6630628	0.3419932188997791072410176920	3.1318520367554217518645936440
10	7314844	0.3418817675970901589770416615	3.1413871641455839921906843022
11	7997698	0.3419124995725326520267598798	3.1511883108624334346995937778
12	8673772	0.3418217036050786668551817618	3.1590136700701871830859130700
13	9347950	0.3418015348828134558328953745	3.1667738910530448030276904339
14	10017014	0.3417179369534202229929918120	3.1733368572143211865794710788
15	10683618	0.3416597120532694525318786779	3.1796104649318611336883086991
16	11348378	0.3416344375825035522803404071	3.1857356144940349991816538884
17	12009702	0.3415860528472074676777068257	3.1912463717896076463187114885
18	12669894	0.3415758816573803497344948667	3.1967617811835515001579129388
19	13327074	0.3415463690492884575265860413	3.2017828190920668724377383555
20	13981671	0.3415075859461948349915192571	3.2064358110142770629619272229

x ($\times 10^8$)	$\mathbb{P}_4$	$\mathbb{P}_4/\mathbb{L}_4$	$\mathbb{P}_4/\mathbb{L}_1$
1	619240	0.08496438513213545825374308286	2.101214326996891637798532028
2	1210774	0.08611531924855926407868836904	2.211711288140973713330446614
3	1793243	0.08680829490529152930804571770	2.277435349883393122681581834
4	2367866	0.08722663712370130777485304449	2.322380849904634153518202186
5	2937390	0.08753774687392337111883393940	2.356994948416166251579461266
6	3502767	0.08778115608746893233342224977	2.385050042599526682126127667
7	4066041	0.08800871266882075624180346164	2.409408249650556374014288517
8	4625948	0.08818951824700412872834275747	2.430097300293974415508681755
9	5182573	0.08833165942729013272212326348	2.447890577737682822023214491
10	5737407	0.08846342891262073240111894474	2.463950933919988261661188872
11	6289860	0.08857502156478358193356988978	2.478279788629326284085694023
12	6841534	0.08868888325557084124275711013	2.491707117762602936697724957
13	7391722	0.08879361329259857002623026751	2.504069046103412452732999858
14	7939847	0.08888273885361775697327014332	2.515301378808351114443830637
15	8487048	0.08896967502233675706421300564	2.525877154834534721378758853
16	9032025	0.08904077589591013825893579842	2.535485133954868833544642012
17	9576632	0.08911495573275305689960011720	2.544725266618959725493642940
18	10120673	0.08918915951357333616537365596	2.553563640410588889832676201
19	10663146	0.08925429431709721487608870247	2.561783453762641109561407101
20	11203909	0.08930993056754813255022393572	2.569407836942033460393446759

x ($\times 10^8$)	$\mathbb{P}_5$	$\mathbb{P}_5/\mathbb{L}_5$	$\mathbb{P}_5/\mathbb{L}_1$
1	239022	0.01125653297927349909468395788	0.8110529857041712955395011990
2	485766	0.01171013146781239815738662232	0.8873449096157402098407115862
3	734115	0.01195981795464472634372112381	0.9323329029471450005701343589
4	984281	0.01214273001103811334424137260	0.9653736086944882899872921721
5	1235951	0.01228892544677182325443326980	0.9917410570233809929242922224
6	1488256	0.01240610985131790079886787018	1.013360305209853005305320695
7	1740309	0.01249833150173208883301492187	1.031252479141531064911650530
8	1993881	0.01258480703840945913956051478	1.047423108778449304135901632
9	2247128	0.01265630411867556659457806917	1.061388514579635197514319997
10	2501031	0.01272167869790342135985154798	1.074077134184979758634997458
11	2754364	0.01277650095420640892484289326	1.085252236413564953932107953
12	3007785	0.01282586163715235824387120933	1.095444280946289337150903095
13	3260761	0.01286866658296171615170223094	1.104637145017251635381594349
14	3514928	0.01291211924406621502269982867	1.113510530468922129858399630
15	3769430	0.01295301757895958594186157785	1.121840847812801366836470700
16	4023387	0.01298887594150013216488885466	1.129451914343381229745121010
17	4277894	0.01302379985859796757307148621	1.136732094301801311351517127
18	4531765	0.01305444825261590020196020526	1.143417076204842539654485217
19	4785874	0.01308380090856853019308419055	1.149789454724977624575438585
20	5040132	0.01311176002586187941990095104	1.155860393013039019577876221

References

[1] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Second edition, Asterisque **18** (1987), 103.

[2] A. C. Cojocaru, *On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves*, J. Number Theory **96**-2 (2002), 335–350.

[3] ———, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc. **355**-7 (2003), 2651–2662.

[4] A. C. Cojocaru and M. R. Murty, *An introduction to sieve methods and their applications*, London Math. Soc. Stud. Texts **66**, Cambridge University Press, Cambridge, 2006.

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

[6] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Math. **70**, Cambridge University Press, Cambridge-New York-Melbourne, 1976.

[7] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131**-1 (1988), 157–165.

[8] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464, Academic Press, London, 1977.

[9] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83**-2 (1977), 289–292.

[10] M. R. Murty, *On Artin's conjecture*, J. Number Theory **16**-2 (1983), 147–168.

[11] ———, *An analogue of Artin's conjecture for abelian extensions*, J. Number Theory **18**-3 (1984), 241–248.

[12] ———, *Problems in analytic number theory*, Grad. Texts in Math. **206**, Springer Verlag, 2001.

[13] S. A. Miri and V. K. Murty, *An application of sieve methods to elliptic curves*, Progress in cryptology—INDOCRYPT 2001 (Chennai), 91–98, Lecture Notes in Comput. Sci. **2247**, Springer, Berlin, 2001.

[14] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15**-4 (1972), 259–331.

[15] ———, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. I. H. E. S. **54** (1981), 123–201.

[16] ———, *Résumé des cours de 1977-1978*, Annuaire du Collège de France, 1978, pp. 67–70, in Collected Papers, volume III, Springer Verlag, 1986, pp. 465–468.

[17] J. H. Silverman, *The arithmetic of elliptic curves*, Corrected reprint of the 1986 original, Grad. Texts in Math. **106**, Springer-Verlag, New York, 1992.