Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 80 (2005)

Artikel: A prime analogue of the Erdös-Pomerance conjecture for elliptic curves
Autor: Liu, Yu-Ru
DOI: https://doi.org/10.5169/seals-60462

Comment. Math. Helv. 80 (2005), 755–769

Commentarii Mathematici Helvetici

A prime analogue of the Erdös–Pomerance conjecture for elliptic curves

Yu-Ru Liu*

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve of rank ≥ 1 and $b \in E(\mathbb{Q})$ a rational point of infinite order. For a prime p of good reduction, let $g_b(p)$ be the order of the cyclic group generated by the reduction $\bar{b}$ of b modulo p. We denote by $\omega(g_b(p))$ the number of distinct prime divisors of $g_b(p)$. Assuming the GRH, we show that the normal order of $\omega(g_b(p))$ is $\log\log p$. We also prove conditionally that there exists a normal distribution for the quantity

$$\frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}}.$$

The latter result can be viewed as an elliptic analogue of a conjecture of Erdös and Pomerance about the distribution of $\omega(f_a(n))$, where a is a natural number > 1 and $f_a(n)$ the order of a modulo n.

Mathematics Subject Classification (2000). 11N37, 11G20.

Keywords. Prime divisors, order of cyclic groups, elliptic curves.

1. Introduction

For $n \in \mathbb{N} := \{1, 2, 3, \dots\}$, let $\omega(n)$ denote the number of distinct prime divisors of n. The Turán Theorem is about the second moment of $\omega(n)$ [23]; it states that for $x \in \mathbb{R}$, $x > 1$,

$$\sum_{n \leq x} (\omega(n) - \log\log x)^2 \ll x \log\log x.$$

Turán's result implies an earlier theorem of Hardy and Ramanujan [8], which states that for any $\varepsilon > 0$

$$\#\{n \leq x \mid n \text{ satisfies } |\omega(n) - \log\log n| > \varepsilon \log\log n\}$$

is $o(x)$ as $x \to \infty$. In other words, the normal order of $\omega(n)$ is $\log\log n$. The significance of the '$\log\log n$' term is that it is about $\sum_{p \leq n} \frac{\omega(p)}{p}$ where p runs over primes.

*Research partially supported by an NSERC discovery grant.

The idea behind Turán's proof was essentially probabilistic. Further development of probabilistic ideas led Erdös and Kac [5] to prove a remarkable refinement of the Turán Theorem, namely, the existence of a normal distribution for $\omega(n)$. More precisely, they proved that for $\gamma \in \mathbb{R}$,

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x \,\middle|\, n \text{ satisfies } \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \le \gamma \right\} = G(\gamma) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{\frac{-t^2}{2}} dt.$$

The theorem of Erdös and Kac opened a door to the study of probabilistic number theory. In the early 1960s and subsequently the 1970s, the theory was refined by many authors, culminating in a generalized Erdös–Kac theorem proved independently by Kubilius [10] and Shapiro [20]. Their result is applicable to what are called 'strongly additive functions'. The interested reader can find a comprehensive treatment of it in the monograph of Elliott [3].

We can also consider functions that are not strongly additive, say the Euler's φ-function. Using the same principle of the work of Kubilius and Shapiro, the issue of $\omega(\varphi(n))$ devolves upon the estimation of the sums

$$\sum_{p\le x} \omega(p-1) \quad \text{and} \quad \sum_{p\le x} \omega^2(p-1),$$

where p denotes a rational prime. Sums of this type were estimated by Haselgrove [9] and Erdös and Pomerance [6]. They proved that

$$\sum_{p\le x} \omega(p-1) = \pi(x)\log\log x + O\big(\pi(x)\big)$$

and

$$\sum_{p\le x} \omega^2(p-1) = \pi(x)(\log\log x)^2 + O\big(\pi(x)\log\log x\big),$$

where $\pi(x)$ is the number of rational primes $\le x$. Applying partial summation, we can derive from the above equalities that

$$\sum_{p\le n} \frac{\omega(p-1)}{p} = \frac{1}{2}(\log\log n)^2 + O\big(\log\log n\big)$$

and

$$\sum_{p\le n} \frac{\omega^2(p-1)}{p} = \frac{1}{3}(\log\log n)^3 + O\big((\log\log n)^2\big).$$

As a consequence we have the following result of Erdös and Pomerance [6], which states that

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x \,\middle|\, n \text{ satisfies } \frac{\omega(\varphi(n)) - \frac{1}{2}(\log\log n)^2}{\frac{1}{\sqrt{3}}(\log\log n)^{3/2}} \le \gamma \right\} = G(\gamma).$$

In [6], Erdös and Pomerance also proposed the following question. Let a be a positive integer > 1. For any natural number n coprime to a, let $f_a(n)$ denote the order of a modulo n. Thus $f_a(n)$ is a divisor of $\varphi(n)$. Based on the belief that the difference between $\omega(\varphi(n))$ and $\omega(f_a(n))$ is 'small on average', Erdös and Pomerance conjectured that

$$\begin{aligned}\lim_{x\to\infty}\frac{1}{x}\#\Big\{n\le x \,\Big|\, n \text{ satisfies } (a,n)=1 \text{ and } \frac{\omega(f_a(n))-\frac{1}{2}(\log\log n)^2}{\frac{1}{\sqrt{3}}(\log\log n)^{3/2}}\le\gamma\Big\}\\ =\frac{\varphi(a)}{a}G(\gamma).\end{aligned}$$

The conjecture remains open until today. Even a conditional result was only obtained recently by Murty and Saidak [17] under the assumption of the GRH (i.e., the Riemann Hypothesis for all Dedekind zeta functions of number fields). Later Li and Pomerance [13] also provided an alternative proof of the same result. The difficulty of this conjecture lies in the intervention of the distribution of primes in the non-abelian extensions $\mathbb{Q}(\zeta_q, \sqrt[q]{a})$ where q varies over rational primes and ζ_q is a primitive q-th root of unity.

Let us recall that $f_a(n)$ is the least common multiple of $\{f_a(p^\gamma) \mid p^\gamma \parallel n\}$ where p^γ is the exact power of p which divides n. Also $f_a(p^\gamma)$ divides $p^{\gamma-1}f_a(p)$. Thus similarly to the case of $\omega(\varphi(n))$, to study the conjecture of Erdös and Pomerance, it is sufficient to estimate the sums

$$\sum_{p\le x}\omega(f_a(p)) \quad\text{and}\quad \sum_{p\le x}\omega^2(f_a(p)).$$

Under the assumption of the GRH, Murty and Saidak proved that

$$\sum_{p\le x}\omega(f_a(p)) = \pi(x)\log\log x + O\big(\pi(x)\big)$$

and

$$\sum_{p\le x}\omega^2(f_a(p)) = \pi(x)(\log\log x)^2 + O\big(\pi(x)\log\log x\big).$$

A conditional result of the conjecture follows.

In [17], Murty and Saidak also proved the following 'prime analogue' of the Erdös–Pomerance conjecture:

$$\begin{aligned}\lim_{x\to\infty}\frac{1}{\pi(x)}\#\Big\{p\le x \,\Big|\, p \text{ satisfies } (a,p)=1 \text{ and } \frac{\omega(f_a(p))-\log\log p}{\sqrt{\log\log p}}\le\gamma\Big\}\\ = G(\gamma).\end{aligned}$$

In a sense, as we see from [17, §5, §7], there is not much difference between the study of $\omega(f_a(n))$ and $\omega(f_a(p))$, as the main technical difficulty of both problems depends on the study of $\omega(i_a(p))$, where $i_a(p) = (p-1)/f_a(p)$.

The purpose of this paper is to formulate an analogous Erdös–Pomerance conjecture for elliptic curves and provide a conditional proof of it. Let $E/\mathbb{Q}$ be an elliptic curve of rank ≥ 1. Let $b \in E(\mathbb{Q})$ be a rational point of infinite order. For a prime p of good reduction, let $g_b(p)$ be the order of $\langle \bar{b} \rangle$, the cyclic group generated by the reduction $\bar{b}$ of b modulo p. The function $g_b(p)$ can be viewed as an elliptic analogue of $f_a(p)$. Thus, an analogous formulation of the conjecture of Erdös and Pomerance for elliptic curves is that there exists a normal distribution for the quantity

$$\frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}}.$$

We prove the following result.

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve of rank ≥ 1 and $b \in E(\mathbb{Q})$ a rational point of infinite order. For a prime p of good reduction, let $\langle \bar{b} \rangle$ be the cyclic group generated by the reduction $\bar{b}$ of b modulo p and $g_b(p)$ its order. Assuming the* GRH, *we have*

$$\sum_{\substack{p \leq x \\ p \text{ of good reduction}}} \big(\omega(g_b(p)) - \log\log x\big)^2 \ll \pi(x) \log\log x.$$

As a direct consequence of Theorem 1 we have

Corollary 2. *Assuming the* GRH, *the normal order of $\omega(g_b(p))$ is* $\log\log p$.

The following theorem is an analogous result of Murty and Saidak for elliptic curves.

Theorem 3. *Let $E/\mathbb{Q}$, b, and $g_b(p)$ be defined as in Theorem* 1. *Let $\gamma \in \mathbb{R}$. Assuming the* GRH, *we have*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \#\Big\{ p \leq x \;\Big|\; p \text{ is of good reduction and } \frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}} \leq \gamma \Big\}$$
$$= G(\gamma).$$

Thus, we obtain an elliptic analogue of a conjecture of Erdös and Pomerance in terms of primes.

Acknowledgment. I would like to thank W. Kuo and R. Murty for many helpful discussions related to this work. I also would like to thank D. Mckinnon for his comments about this paper. Special thanks go to the referee for the careful reading of the paper and many valuable suggestions.

Notation. For $x \in \mathbb{R}, x > 0$, let $f(x)$ and $g(x)$ be two functions of x. If $g(x)$ is positive and there exists a constant $C > 0$ such that $|f(x)| \leq Cg(x)$, we write either $f(x) \ll g(x)$ or $f(x) = O(g(x))$. If both $f(x)$ and $g(x)$ are positive, we use $f(x) \asymp g(x)$ to denote that $f(x) = O(g(x))$ and $g(x) = O(f(x))$. If $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$, we write $f(x) = o(g(x))$. Also, we use $\bar{\mathbb{Q}}$ and $\bar{\mathbb{F}}_p$ to denote some fixed algebraic closures of $\mathbb{Q}$ and $\mathbb{F}_p$ respectively.

2. Preliminaries

We first recall some theorems about elliptic curves that will be needed later. Let $E/\mathbb{Q}$ be an elliptic curve of rank ≥ 1. For a prime $l \in \mathbb{N}$, we denote by $E[l]$ the l-torsion points. By adjoining to $\mathbb{Q}$ the coordinates of the l-torsion points, we obtain $\mathbb{Q}(E[l])$, a finite Galois extension of $\mathbb{Q}$. Since

$$E[l] \cong (\mathbb{Z}/l\mathbb{Z}) \times (\mathbb{Z}/l\mathbb{Z})$$

(see [21, Corollary 6.4]), by choosing a basis, we have a natural injection

$$\Phi_l : \mathrm{Gal}\big(\mathbb{Q}(E[l])/\mathbb{Q}\big) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}).$$

In the following discussion we will abuse our notation by identifying an element $\gamma \in \mathrm{Gal}\big(\mathbb{Q}(E[l])/\mathbb{Q}\big)$ with its image $\Phi_l(\gamma) \in \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$.

Let $b \in E(\mathbb{Q})$ be a rational point of infinite order. We denote by $l^{-1}b$ the set of elements $v \in E(\bar{\mathbb{Q}})$ such that

$$[l]\,v = \underbrace{v + v + \cdots + v}_{l \text{ times}} = b.$$

Define $L_l = \mathbb{Q}(E[l], l^{-1}b)$, which is a finite extension of $\mathbb{Q}(E[l])$. We have the following theorem.

Theorem 4 (Bachmakov [1]). *For a prime l, the Galois group $\mathrm{Gal}(L_l/\mathbb{Q}(E[l]))$ can be identified with a subgroup of $E[l]$ and is equal to $E[l]$ for all but finitely many l.*

The group $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ acts naturally on $E[l]$ by matrix multiplication. We denote this action by $*$ and we see that it induces a semidirect product $E[l] \rtimes \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$. Let G_l be the Galois group $\mathrm{Gal}(L_l/\mathbb{Q})$. From Theorem 4, for all but finitely many l, we have

$$G_l \cong E[l] \rtimes \mathrm{Gal}\big(\mathbb{Q}(E[l])/\mathbb{Q}\big),$$

which is a subgroup of $E[l] \rtimes \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$.

An element $(\tau, \gamma) \in G_l$ acts on $E[l]$ and $l^{-1}b$ as follows: let $v_0 \in l^{-1}b$ be a fixed element; for $u \in E[l]$ and $v \in l^{-1}b$ we have

- $(\tau, \gamma) \cdot u := \gamma * u$.
- $(\tau, \gamma) \cdot v := v_0 + \gamma * (v - v_0) + \tau$.

Notice that since $[l]v = [l]v_0 = b$, $(v - v_0) \in E[l]$. Thus, $\gamma * (v - v_0)$ is well defined. Also, since both $(v - v_0)$ and τ are in $E[l]$, for $v \in l^{-1}b$, we have

$$[l]\big((\tau, \gamma) \cdot v\big) = [l]v_0 = b.$$

Thus, (τ, γ) is a well-defined action on the set $l^{-1}b$. Moreover, for $v \in l^{-1}b$, we have

$$(\tau, \gamma) \cdot v = v \quad \text{if and only if} \quad (\gamma - I) * (v_0 - v) = \tau,$$

where I is the 2×2 identity matrix.

Let p be a prime of good reduction. We denote by $\overline{E}$ the reduction of E modulo p. Let $\overline{E}(\mathbb{F}_p)$ be the set of rational points of $\overline{E}$ defined over the finite field $\mathbb{F}_p$. Let $b \in E(\mathbb{Q})$ be a rational point of infinite order and $\bar{b} \in \overline{E}(\mathbb{F}_p)$ the reduction of b modulo p. Let $\langle \bar{b} \rangle$ be the cyclic group generated by $\bar{b}$, which is a subgroup of $\overline{E}(\mathbb{F}_p)$. We denote by $g_b(p)$ the order of $\langle \bar{b} \rangle$. Thus $g_b(p)$ is a divisor of $\#\overline{E}(\mathbb{F}_p)$. We write

$$\#\overline{E}(\mathbb{F}_p) = g_b(p) \cdot i_b(p),$$

where $i_b(p)$ is the index of $\langle \bar{b} \rangle$ in $\overline{E}(\mathbb{F}_p)$. Let Δ be the discriminant of E. For $p \nmid l\Delta$, Lang and Trotter [12] gave a condition on the Frobenius element $(\tau_p, \gamma_p) \in G_l$ in order that $l \mid i_b(p)$. We review their arguments below.

Notice that $l \mid i_b(p)$ implies that $l \mid \#\overline{E}(\mathbb{F}_p)$. Since

$$\operatorname{tr} \gamma_p \equiv p + 1 - \#\overline{E}(\mathbb{F}_p) \pmod{l}$$

and

$$\det \gamma_p \equiv p \pmod{l}$$

(see [22, p. 172]), if $l \mid \#\overline{E}(\mathbb{F}_p)$, we have

$$1 - \operatorname{tr} \gamma_p + \det \gamma_p \equiv 0 \pmod{l}.$$

Thus $\gamma_p \in \operatorname{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) \subseteq \operatorname{GL}_2(\mathbb{Z}/l\mathbb{Z})$ has an eigenvalue 1.

We consider first the case when $\gamma_p = I$. We recall that the cyclic group generated by $\pi_p \colon x \mapsto x^p$ is dense in $\operatorname{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. The group $\operatorname{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ acts on $w \in \overline{E}(\bar{\mathbb{F}}_p)$ coordinatewise. Thus for $w \in \overline{E}(\bar{\mathbb{F}}_p)$ we have

$$\pi_p \cdot w = w \quad \text{if and only if} \quad w \in \overline{E}(\mathbb{F}_p).$$

Let $w_1 \in E(\mathbb{Q}(E[l]))$. The Frobenius element $\gamma_p \in \mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q})$ acts on w_1 coordinatewise. This action is compatible with π_p in the following sense: let $\bar{w}_1 \in \bar{E}(\mathbb{F}_p)$ be the reduction of w_1 modulo p; we have

$$\overline{\gamma_p \cdot w_1} = \pi_p \cdot \bar{w}_1.$$

Thus for $\gamma_p = I$ we have

$$\bar{w}_1 = \overline{\gamma_p \cdot w_1} = \pi_p \cdot \bar{w}_1.$$

It follows that $\bar{w}_1 \in \bar{E}(\mathbb{F}_p)$. Let $\bar{E}[l]$ denote the reduction of $E[l]$ modulo p. Since $E[l] \subseteq E(\mathbb{Q}(E[l]))$, the above argument shows that

$$\bar{E}(\mathbb{F}_p) \supseteq \bar{E}[l] \cong (\mathbb{Z}/l\mathbb{Z}) \times (\mathbb{Z}/l\mathbb{Z}), \quad \text{provided that } p \nmid l\Delta$$

(see [21, Corollary 6.4]). Consider the subgroup $\langle \bar{b} \rangle$ in $\bar{E}(\mathbb{F}_p)$. Since $\langle \bar{b} \rangle$ is cyclic, it can not contain two $(\mathbb{Z}/l\mathbb{Z})$ factors. Thus, at least one of $(\mathbb{Z}/l\mathbb{Z})$ factors of $\bar{E}(\mathbb{F}_p)$ is contained in $\bar{E}(\mathbb{F}_p)/\langle \bar{b} \rangle$. Since $i_b(p)$ is the order of $\bar{E}(\mathbb{F}_p)/\langle \bar{b} \rangle$, we have $l \mid i_b(p)$. We conclude that for $\gamma_p = I$, l is a divisor of $i_b(p)$.

On the other hand, if γ_p has an eigenvalue 1 and $\gamma_p \neq I$, $\bar{E}(\mathbb{F}_p)$ can not contain a $(\mathbb{Z}/l\mathbb{Z}) \times (\mathbb{Z}/l\mathbb{Z})$ factor. Hence, the l-torsion points of $\bar{E}(\mathbb{F}_p)$, which is the kernel of the map $\gamma_p - I \colon E[l] \to E[l]$, form a cyclic subgroup. In other words, the l-primary part of $\bar{E}(\mathbb{F}_p)$ is of the form $\mathbb{Z}/l^\alpha\mathbb{Z}$ for some $\alpha \in \mathbb{N}$. Write

$$\bar{E}(\mathbb{F}_p) \cong \mathbb{Z}/l^\alpha\mathbb{Z} \times H,$$

where H is an abelian group with $(|H|, l) = 1$. We will abuse our notation by identifying an element in $\bar{E}(\mathbb{F}_p)$ with its image in $\mathbb{Z}/l^\alpha\mathbb{Z} \times H$. For $\bar{b} \in \bar{E}(\mathbb{F}_p)$, without loss of generality, we can assume that either $\bar{b} = (0, h)$ or $\bar{b} = (l^\beta, h)$ where $h \in H$ and $\beta \geq 0$.

Case 1. Suppose $\bar{b} = (0, h)$. Since $(|H|, l) = 1$, the element $\bar{b}_l = (0, l^{-1}h) \in \bar{E}(\mathbb{F}_p)$ is well defined and $[l]\bar{b}_l = \bar{b}$.

Case 2. Suppose $\bar{b} = (l^\beta, h)$. If $\beta = 0$, the order of the cyclic group $\langle b \rangle$ is divisible by l^α, i.e., $l \nmid i_b(p)$. Hence, if $l \mid i_b(p)$, it implies that $\beta \geq 1$. Choosing $\bar{b}_l = (l^{\beta-1}, l^{-1}h) \in \bar{E}(\mathbb{F}_p)$, we have $[l]\bar{b}_l = \bar{b}$.

We conclude that if γ_p has an eigenvalue 1, $\gamma_p \neq 1$ and $l \mid i_b(p)$, there exists $\bar{b}_l \in \bar{E}(\mathbb{F}_p)$ such that $[l]\bar{b}_l = \bar{b}$. Let $b_l \in \bar{E}(\bar{\mathbb{Q}})$ such that the reduction of b_l modulo p is $\bar{b}_l$. Since $[l]\bar{b}_l = \bar{b}$, it follows that $b_l \in l^{-1}b$. Moreover, since $\bar{b}_l \in E(\mathbb{F}_p)$, we have

$$(\tau_p, \gamma_p) \cdot b_l = b_l,$$

which is equivalent to

$$(\gamma_p - I) * (v_0 - b_l) = \tau_p,$$

i.e., $\tau_p \in \operatorname{Im}(\gamma_p - I)$.

Define a subset S_l of G_l as follows: an element (τ, γ) of G_l belongs to S_l if it satisfies one of the two following conditions:

(1) $\gamma = I$ or

(2) γ has an eigenvalue 1, $\ker((\gamma - I) : E[l] \to E[l])$ is cyclic, and $\tau \in \operatorname{Im}(\gamma - I)$.

Notice that S_l is a union of conjugacy classes of G_l. Combining all the above discussions, we obtain the following result of Lang and Trotter.

Theorem 5 (Lang and Trotter [12]). *Let $i_b(p)$ be the index of the cyclic group $\langle \bar{b} \rangle$ in $\overline{E}(\mathbb{F}_p)$. For a prime $l \in \mathbb{N}$, $p \nmid l\Delta$, the following two statements are equivalent:*

(1) $l \mid i_b(p)$.

(2) $(\tau_p, \gamma_p) \in S_l$.

Another important ingredient of the proof of Theorems 1 and 3 is the Chebotarev density theorem. Let $L/\mathbb{Q}$ be a finite Galois extension of degree n_L and discriminant d_L. We denote by G the Galois group of $L/\mathbb{Q}$ and C a union of conjugacy classes of G. Let $\sigma_p \in G$ be a Frobenius element. Define

$$\pi_C\big(x, L/\mathbb{Q}\big) = \#\big\{p \le x \mid p \text{ is an unramified prime in } L/\mathbb{Q} \text{ and } \sigma_p \subseteq C\big\}.$$

We have

Theorem 6 (Lagarias and Odlyzko [11], Serre [19]). *Assuming the* GRH *for the Dedekind zeta function of L, we have*

$$\pi_C\big(x, L/\mathbb{Q}\big) = \frac{|C|}{|G|} \operatorname{li} x + O\bigg(|C|\, x^{\frac{1}{2}} \Big(\frac{\log |d_L|}{n_L} + \log x\Big)\bigg),$$

where $\operatorname{li} x = \int_2^x \frac{dt}{\log t}$.

The following theorem is useful for estimating the error term in the Chebotarev density theorem.

Theorem 7 (Serre [19]). *Let $L/\mathbb{Q}$ be a finite Galois extension of degree n_L and discriminant d_L. We have*

$$\frac{n_L}{2} \sum_{q \text{ ramified}} \log q \le \log |d_L| \le (n_L - 1) \sum_{q \text{ ramified}} \log q + n_L \log n_L,$$

where the sum is over all primes q that are ramified in L.

3. Prime divisors of $i_b(p)$

We recall that $i_b(p)$ is the index of $\langle \bar{b} \rangle$ in $\bar{E}(\mathbb{F}_p)$. In this section, we consider the number of distinct prime divisors of $i_b(p)$. The following lemma is essential for the proof of Theorems 1 and 3. We use the notation $\sum'$ to denote the sum over primes of good reduction.

Lemma 8. *Assuming the* GRH, *we have*

$$\sum_{p \le x}{}' \omega^2(i_b(p)) \ll \pi(x).$$

Proof. Let $y = x^\delta$ with $0 < \delta < 1$ (a choice of δ will be made later). Define a truncation function ω_y of ω as follows:

$$\omega_y(i_b(p)) = \#\big\{l \le y \ \mid l \text{ is a prime and } \ l \mid i_b(p)\big\}.$$

For a prime $p \le x$, since

$$i_b(p) \le \#\bar{E}(\mathbb{F}_p) \le (p + 2\sqrt{p} + 1) \le 3x,$$

it follows that

$$\omega(i_b(p)) = \omega_y(i_b(p)) + O(1).$$

Hence we have

$$\begin{aligned}\sum_{p \le x}{}' \omega^2(i_b(p)) &= \sum_{p \le x}{}' \big(\omega_y(i_b(p)) + O(1)\big)^2 \ll \sum_{p \le x}{}' \omega_y^2(i_b(p)) + O\big(\pi(x)\big) \\ &= \sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2}} \sum_{\substack{p \le x \\ l_1 l_2 \mid i_b(p)}}{}' 1 + \sum_{l \le y} \sum_{\substack{p \le x \\ l \mid i_b(p)}}{}' 1 + O\big(\pi(x)\big),\end{aligned}$$

where l_1, l_2, and l are rational primes. Consider the sum

$$\sum_{l \le y} \sum_{\substack{p \le x \\ l \mid i_b(p)}}{}' 1.$$

Applying Theorems 5, 6 and 7 for all but finitely many primes l, under the GRH we have

$$\begin{aligned}&\#\big\{p \le x \mid p \text{ satisfies } \ l \mid i_b(p)\big\} \\ &\quad = \operatorname{li} x \cdot \frac{|S_l|}{|G_l|} + O\Big(|S_l| \cdot x^{\frac{1}{2}} \cdot \big(\sum_{q \text{ ramified}} \log q + + \log n_l + \log x\big)\Big),\end{aligned}$$

where the sum is over all primes q that are ramified in L_l and $n_l = |G_l|$.

In the case of elliptic curves without complex multiplication (non-CM) Serre [18] proved that for all but finitely many primes l,

$$\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}).$$

Hence, for all but finitely many l, we have

$$|G_l| \asymp l^6 \quad \text{and} \quad |S_l| \asymp l^4.$$

In the case of elliptic curves with complex multiplication (CM), from [7, p. 35–37], we have

$$|G_l| \asymp l^4 \quad \text{and} \quad |S_l| \asymp l^2.$$

It is well known that q is ramified in L_l if and only if $q \mid l\Delta$ (see [2]). Hence, assuming the GRH, we have

$$\sum_{l \le y} \sideset{}{'}\sum_{\substack{p \le x \\ l \mid i_b(p)}} 1 \ll \sum_{l \le y} \left(\frac{\pi(x)}{l^2} + O\big(l^4 x^{\frac{1}{2}} \log(l^6 x \Delta)\big) \right) \ll \pi(x) + O\big(x^{\frac{1}{2}+5\delta+\varepsilon}\big),$$

where $\varepsilon > 0$ is arbitrarily small. Choosing $\delta = \frac{1}{11}$, we have

$$\sum_{l \le y} \sideset{}{'}\sum_{\substack{p \le x \\ l \mid i_b(p)}} 1 \ll \pi(x).$$

Consider the sum

$$\sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2}} \sideset{}{'}\sum_{\substack{p \le x \\ l_1 l_2 \mid i_b(p)}} 1.$$

The group homomorphisms

$$E[l_1 l_2] \to E[l_1] \times E[l_2] \quad \text{and} \quad \mathrm{GL}_2(\mathbb{Z}/l_1 l_2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/l_1\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/l_2\mathbb{Z}),$$

which are induced by reduction modulo l_1 and l_2 respectively, are indeed isomorphisms. Moreover, these maps are compatible with the actions defined in Section 2. Since $|S_l|/|G_l| \asymp 1/l^2$, by Theorems 5, 6 and 7 we have

$$\begin{aligned} \sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2}} \sideset{}{'}\sum_{\substack{p \le x \\ l_1 l_2 \mid i_b(p)}} 1 &\ll \sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2}} \left(\frac{\pi(x)}{(l_1 l_2)^2} + O\big((l_1 l_2)^4 x^{\frac{1}{2}} \log(l_1^6 l_2^6 x \Delta)\big) \right) \\ &\ll \pi(x) + O\big(x^{\frac{1}{2}+10\delta+\varepsilon}\big), \end{aligned}$$

where $\varepsilon \to 0$ as $x \to \infty$. Choosing $\delta = \frac{1}{21}$, we have

$$\sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2}} \sideset{}{'}\sum_{\substack{p \le x \\ l_1 l_2 \mid i_b(p)}} 1 \ll \pi(x).$$

It follows that

$$\sum_{p\le x}{}' \omega^2(i_b(p)) \ll \pi(x).$$

This completes the proof of Lemma 8. □

4. A Turán analogue of $\omega(g_b(p))$

In this section, we provide a proof of Theorem 1 which states that under the GRH, we have

$$\sum_{p\le x}{}' \big(\omega(g_b(p)) - \log\log x\big)^2 \ll \pi(x)\log\log x.$$

Our proof is a combination of Lemma 8 with the following theorem.

Theorem 9 (Miri and Murty [16], Liu [14]). *Let $E/\mathbb{Q}$ be an elliptic curve. We have (assuming the GRH if E is non-CM)*

$$\sum_{p\le x}{}' \big(\omega(\#\bar{E}(\mathbb{F}_p)) - \log\log x\big)^2 \ll \pi(x)\log\log x.$$

Now we are ready to prove Theorem 1.

Proof of Theorem 1. Since

$$\#\bar{E}(\mathbb{F}_p) = g_b(p)\cdot i_b(p),$$

we have

$$\omega(\#\bar{E}(\mathbb{F}_p)) \ge \omega(g_b(p)) \ge \omega(\#\bar{E}(\mathbb{F}_p)) - \omega(i_b(p)).$$

It follows that

$$\begin{aligned}\sum_{p\le x}{}' \big(\omega(g_b(p)) - \log\log x\big)^2 &= \sum_{p\le x}{}' \big(\omega(\#\bar{E}(\mathbb{F}_p)) + O\big(\omega(i_b(p))\big) - \log\log x\big)^2\\ &\ll \sum_{p\le x}{}' \big(\omega(\#\bar{E}(\mathbb{F}_p)) - \log\log x\big)^2 + \sum_{p\le x}{}' \omega^2(i_b(p)).\end{aligned}$$

Combining Lemma 8 with Theorem 9 we obtain that under the GRH,

$$\sum_{p\le x}{}' \big(\omega(g_b(p)) - \log\log x\big)^2 \ll \pi(x)\log\log x.$$

This completes the proof of Theorem 1. □

5. An Erdös–Kac analogue of $\omega(g_b(p))$

In this section, we give a proof of Theorem 3. More precisely, under the GRH we prove that there exists a normal distribution for the quantity

$$\frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}}.$$

Our proof is dependent on the following theorem.

Theorem 10 (Liu [15]). *Let $E/\mathbb{Q}$ be an elliptic curve. We have (assuming the GRH if E is non-CM)*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \#\Big\{p \le x \;\Big|\; p \text{ is of good reduction and } \frac{\omega(\#\overline{E}(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma\Big\}$$
$$= G(\gamma).$$

Proof of Theorem 3. As in the proof of Theorem 1, we have

$$\begin{aligned}\frac{\omega(\#\overline{E}(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} &\ge \frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}} \\ &\ge \frac{\omega(\#\overline{E}(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} - \frac{\omega(i_b(p))}{\sqrt{\log\log p}}.\end{aligned}$$

For any $\varepsilon > 0$ and $\alpha, \beta \in \mathbb{R}$ with $\alpha < \beta$, define the set

$$S(\varepsilon, \alpha, \beta) = \Big\{p \;\Big|\; p \text{ is of good reduction, } \alpha < p \le \beta, \text{ and } \frac{\omega(i_b(p))}{\sqrt{\log\log p}} \ge \varepsilon\Big\}.$$

Let $N(\varepsilon, \alpha, \beta)$ be the cardinality of $S(\varepsilon, \alpha, \beta)$. We have

$$N(\varepsilon, 0, x) \le \pi(\sqrt{x}) + N(\varepsilon, \sqrt{x}, x).$$

Notice that

$$\sum_{p\le x}{}' \omega(i_b(p)) \ge \sum_{p\in S(\varepsilon,\sqrt{x},x)} \omega(i_b(p)) \ge N(\varepsilon, \sqrt{x}, x) \cdot \varepsilon\sqrt{\log\log x - \log 2}.$$

Since $\omega^2(i_b(p)) \ge \omega(i_b(p))$, Lemma 8 implies that

$$N(\varepsilon, \sqrt{x}, x) \ll \frac{\pi(x)}{\sqrt{\log\log x}} = o\big(\pi(x)\big).$$

It follows that

$$N(\varepsilon, 0, x) = o\big(\pi(x)\big).$$

Thus for $\gamma \in \mathbb{R}$ we obtain

$$\begin{aligned}
&\#\Big\{p \le x \;\Big|\; p \text{ is of good reduction and } \frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma\Big\}\\
&\quad\le \#\Big\{p \le x \;\Big|\; p \text{ is of good reduction and}\\
&\qquad\qquad \frac{\omega(\#\overline{E}(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} - \frac{\omega(i_b(p))}{\sqrt{\log\log p}} \le \gamma\Big\}\\
&\quad\le \#\Big\{p \le x \;\Big|\; p \text{ is of good reduction and}\\
&\qquad\qquad \frac{\omega(\#\overline{E}(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma + \varepsilon\Big\} + o\big(\pi(x)\big).
\end{aligned}$$

Also we have

$$\begin{aligned}
&\#\Big\{p \le x \;\Big|\; p \text{ is of good reduction and } \frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma\Big\}\\
&\quad\ge \#\Big\{p \le x \;\Big|\; p \text{ is of good reduction and } \frac{\omega(\#\overline{E}(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma\Big\}.
\end{aligned}$$

Combine all of the above results with Theorem 10. As $x \to \infty$, for all $\varepsilon > 0$ we obtain

$$\begin{aligned}
G(\gamma) \le \lim_{x\to\infty} \frac{1}{\pi(x)} \#\Big\{p \le x \;\Big|\; p &\text{ is of good reduction and}\\
&\frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma\Big\} \le G(\gamma + \varepsilon).
\end{aligned}$$

Since $G(\gamma)$ is a continuous function, for any $\varepsilon > 0$ we have

$$G(\gamma + \varepsilon) = G(\gamma) + O(\varepsilon).$$

Let $\varepsilon \to 0$. It follows that under the GRH,

$$\begin{aligned}
&\lim_{x\to\infty} \frac{1}{\pi(x)} \#\Big\{p \le x \;\Big|\; p \text{ is of good reduction and } \frac{\omega(g_b(p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma\Big\}\\
&\quad= G(\gamma).
\end{aligned}$$

This completes the proof of Theorem 3. □

References

[1] M. I. Bachmakov, Un théorème de finitude sur la cohomologie des courbes elliptiques. *C. R. Acad. Sci. Paris Sér.* A-B **270** (1970), A999–A1101. Zbl 0194.52303 MR 0269653

[2] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), 223–251. Zbl 0359.14009 MR 0463176

[3] P. D. T. A. Elliott, *Probabilistic number theory*. Vol. I and II, Grundlehren Math. Wiss. 239, 240, Springer-Verlag, New York, Berlin 1979. Zbl 0431.10029 MR 0551361 Zbl 0431.10030 MR 0560507

[4] P. Erdös, On the normal order of prime factors of $p-1$ and some related problems concerning Euler's ϕ-functions. *Quart. J. Math.* (*Oxford*) **6** (1935), 205–213. Zbl 0012.14905

[5] P. Erdös and M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions. *Amer. J. Math.* **62** (1940), 738–742. JFM 66.0172.02 MR 0002374

[6] P. Erdös and C. Pomerance, On the normal number of prime factors of $\varphi(n)$. *Rocky Mountain J. Math.* **15** (1985), 343–352. Zbl 0617.10037 MR 0823246

[7] R. Gupta and M. R. Murty, Primitive points on elliptic curves. *Compositio Math.* **58** (1986), 13–44. Zbl 0598.14018 MR 0834046

[8] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n. *Quart. J. Pure. Appl. Math.* **48** (1917), 76–97. JFM 46.0262.03

[9] C. B. Haselgrove, *Some theorems in the analytic theory of numbers*, *J. London Math. Soc.* 26 (1951), 273–277. Zbl 0043.04704 MR 0044564

[10] J. Kubilius, *Probabilistic methods in the theory of numbers*. Transl. Math. Monogr. 11, Amer. Math. Soc., Providence, R.I., 1964. Zbl 0133.30203 MR 0160745

[11] J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev density theorem. In *Algebraic number fields* (A. Fröhlich, ed.), Academic Press, New York 1977, 409–464. Zbl 0362.12011 MR 0447191

[12] S. Lang and H. Trotter, Primitive points on elliptic curves. *Bull. Amer. Math. Soc.* **83** (1977), 289–292. Zbl 0345.12008 MR 0427273

[13] S. Li and C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli. *J. Reine Angew. Math.* **556** (330), 205–224. Zbl 1022.11049 MR 1971146

[14] Y.-R. Liu, Prime divisors of number of rational points on elliptic curves with complex multiplication. To appear in *Bull. London Math. Soc.*

[15] Y.-R. Liu, Generalizations of the Turán and the Erdös-Kac theorems. Ph.D. thesis, Harvard 2003.

[16] S. A. Miri and V. K. Murty, An application of sieve methods to elliptic curves. In *Progress in Cryptology —INDOCRYPT*, Lecture Notes in Comput. Sci. 2247, Springer-Verlag, Berlin 2001, 91–98. Zbl 1011.94543 MR 1934487

[17] M. R. Murty and F. Saidak, Non-abelian generalizations of the Erdös-Kac theorem. *Canad. J. Math.* **56** (2004), 356–372. Zbl 1061.11052 MR 2040920

[18] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), 259–331. Zbl 0235.14012 MR 0387283

[19] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 123–201. Zbl 0496.12011 MR 0644559

[20] H. Shapiro, Distribution functions of additive arithmetic functions. *Proc. Nat. Acad. Sci. U.S.A.* **42** (1956), 426–430. Zbl 0071.04202 MR 0079609

[21] J. H. Silverman, *The arithmetic of elliptic curves*. Grad. Texts in Math. 106, Springer-Verlag, New York 1986. Zbl 0585.14026 MR 1329092

[22] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Grad. Texts in Math. 151, Springer-Verlag, New York 1994. Zbl 0911.14015 MR 1312368

[23] P. Turán, On a theorem of Hardy and Ramanujan. *J. London Math. Soc.* **9** (1934), 274–276. Zbl 0010.10401

Received March 23, 2004

Yu-Ru Liu, Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail: yrliu@math.uwaterloo.ca

Leere Seite
Blank page
Page vide