Bull. London Math. Soc. 37 (2005) 658–664
doi:10.1112/S0024609305004558

PRIME DIVISORS OF THE NUMBER OF RATIONAL POINTS ON ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

YU-RU LIU

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime p of good reduction, let $E(\mathbb{F}_p)$ be the set of rational points defined over the finite field $\mathbb{F}_p$. Denote by $\omega(\#E(\mathbb{F}_p))$ the number of distinct prime divisors of $\#E(\mathbb{F}_p)$. For an elliptic curve with complex multiplication, the normal order of $\omega(\#E(\mathbb{F}_p))$ is shown to be $\log\log p$. The normal order of the number of distinct prime factors of the exponent of $E(\mathbb{F}_p)$ is also studied.

1. *Introduction*

For $n \in \mathbb{N}$, define $\omega(n)$ to be the number of distinct prime divisors of n. The Turán theorem is concerned with the second moment of $\omega(n)$ (see [**14**]); it states that

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

This result implies a theorem of Hardy and Ramanujan [**6**], namely that

$$\#\{n \leqslant x \mid |\omega(n) - \log\log n| > \epsilon \log\log n\} = \mathrm{o}(x).$$

In other words, the normal order of $\omega(n)$ is $\log\log n$.

Instead of all $n \in \mathbb{N}$, we consider only the set of primes. Since $\omega(p) = 1$ for each prime p, the normal order of $\omega(p)$ is not $\log\log p$. However, an analogue of the Turán theorem holds for $\omega(p-1)$. It was proved by Erdős [**5**] in 1935 that

$$\sum_{p \leqslant x} (\omega(p-1) - \log\log x)^2 \ll \pi(x) \log\log x,$$

where $\pi(x)$ is the number of primes $p \leqslant x$. An immediate corollary of the Erdős theorem is that the normal order of $\omega(p-1)$ is $\log\log p$.

Another 'prime analogue' of the Turán theorem which can be described as 'non-abelian' was discovered by Murty and Murty [**12**] in 1984. Assuming that the GRH (that is, the Riemann hypothesis for all Dedekind zeta functions of number fields) holds, they proved that

$$\sum_{\substack{p \leqslant x \\ \tau(p) \neq 0}} (\omega(\tau(p)) - \log\log x)^2 \ll \pi(x) \log\log x,$$

where $\tau(p)$ is the Ramanujan τ-function. Thus (conditionally) the normal order of $\omega(\tau(p))$ is $\log\log p$. Their method is indeed applicable to a wider class of functions arising as Fourier coefficients of modular forms.

Received 3 March 2004, revised 12 August 2004.

2000 *Mathematics Subject Classification* 11N37, 11G20.

Research partially supported by an NSERC discovery grant.

Let E be an elliptic curve defined over $\mathbb{Q}$. For a prime p of good reduction, we denote by $E(\mathbb{F}_p)$ the set of rational points defined over the finite field $\mathbb{F}_p$. It was proved by Miri and Murty [**11**] that if E is an elliptic curve without complex multiplication (non-CM), assuming the GRH, we have

$$\sum_{\substack{p \leqslant x \\ p\,:\,\text{good reduction}}} (\omega(\#E(\mathbb{F}_p)) - \log\log x)^2 \ll \pi(x) \log\log x.$$

The same result was also obtained independently by the author in her Ph.D. thesis; see [**8**].

The purpose of this paper is to investigate the case of elliptic curves with complex multiplication (CM). We prove that the same result holds unconditionally.

THEOREM 1.1. *Let $E/\mathbb{Q}$ be a* CM *elliptic curve. We have*

$$\sum_{\substack{p \leqslant x \\ p\,:\,\text{good reduction}}} (\omega(\#E(\mathbb{F}_p)) - \log\log x)^2 \ll \pi(x) \log\log x.$$

This theorem is the first 'non-abelian' prime analogue of the Turán theorem that can be proved unconditionally. The following corollary follows directly from Theorem 1.1.

COROLLARY 1.2. *If $E/\mathbb{Q}$ is a* CM *elliptic curve, then for a prime p of good reduction, the normal order of $\omega(\#E(\mathbb{F}_p))$ is $\log\log p$.*

It is well known that the group of $\mathbb{F}_p$-rational points $E(\mathbb{F}_p)$ is isomorphic to

$$E(\mathbb{F}_p) \cong (\mathbb{Z}/f_p\mathbb{Z}) \times (\mathbb{Z}/m_p\mathbb{Z}),$$

for unique integers f_p and m_p with $m_p \mid f_p$. The number f_p is called the *exponent* of $E(\mathbb{F}_p)$, and is the largest possible order of points on $E(\mathbb{F}_p)$. Since $\#E(\mathbb{F}_p) = f_p \cdot m_p$ and $m_p \mid f_p$, we have

$$\omega(f_p) = \omega(\#E(\mathbb{F}_p)).$$

Hence, as a direct consequence of Theorem 1.1 and the result of Miri and Murty [**11**], the next statement holds.

THEOREM 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve. We have (assuming that the* GRH *holds if E is* non-CM)

$$\sum_{\substack{p \leqslant x \\ p\,:\,\text{good reduction}}} (\omega(f_p) - \log\log x)^2 \ll \pi(x) \log\log x.$$

As usual, Theorem 1.3 implies a prime analogue of the Hardy–Ramanujan theorem, as follows.

COROLLARY 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve, and p a prime of good reduction. We find (assuming that the* GRH *holds if E is* non-CM) *that the normal order of $\omega(f_p)$ is $\log\log p$.*

2. *Preliminaries*

The most important ingredients in our proof are theorems of Bombieri and Vinogradov [**1**, **3**, **15**] and Wilson [**16**]. For $m \in \mathbb{N}$ and $a \in \mathbb{Z}$, define

$$\pi(x, a, m) = \#\{p \leqslant x \mid p\text{: prime, } p \equiv a \bmod m\}.$$

We have the following theorem.

THEOREM 2.1 (Bombieri and Vinogradov [**1**, **3**, **15**]). *For any positive constant A, there exists a positive constant B such that*

$$\sum_{m \leqslant Z} \max_{(a,m)=1} \max_{y \leqslant x} \left| \pi(y, a, m) - \frac{\operatorname{li} y}{\phi(m)} \right| \ll x(\log x)^{-A},$$

where $Z = x^{1/2}(\log x)^{-B}$ and $\phi(m)$ is the Euler ϕ-function.

An analogue of the Bombieri–Vinogradov theorem in algebraic number fields has been proved by Wilson. Let $L/\mathbb{Q}$ be a number field of degree n_L with r_1 real embeddings. Let $\mathcal{O}_L$ be its ring of integers with the class number h. Let $\mathfrak{a}$ and $\mathfrak{m}$ be ideals of $\mathcal{O}_L$ and $N(\mathfrak{m}) = |\mathcal{O}_L/\mathfrak{m}|$. Define

$$\pi(x, \mathfrak{a}, \mathfrak{m}) = \#\{N(\mathfrak{p}) \leqslant x \mid \mathfrak{p}\text{: prime ideal, } \mathfrak{p} \sim \mathfrak{a} \bmod \mathfrak{m}\},$$

where '$\sim$' denotes an equivalence relation for ideals, following Landau [**7**]. The order of the $\mathfrak{m}$-ideal class group $h(\mathfrak{m})$ is equal to

$$h(\mathfrak{m}) = \frac{h 2^{r_1} \phi(\mathfrak{m})}{T(\mathfrak{m})},$$

where $\phi(\mathfrak{m})$ is the number of invertible residue classes (of elements in $\mathcal{O}_L$) mod $\mathfrak{m}$ (that is, $\phi(\mathfrak{m}) = |(\mathcal{O}_L/\mathfrak{m})^*|$) and $T(\mathfrak{m})$ is the number of residue classes mod $\mathfrak{m}$ containing a unit. We have the following theorem.

THEOREM 2.2 (Wilson [**16**]). *For any positive constant A, there exists a positive constant B such that*

$$\sum_{N(\mathfrak{m}) \leqslant Z} \max_{(\mathfrak{a},\mathfrak{m})=1} \max_{y \leqslant x} \frac{1}{T(\mathfrak{m})} \left| \pi(y, \mathfrak{a}, \mathfrak{m}) - \frac{\operatorname{li} y}{h(\mathfrak{m})} \right| \ll x(\log x)^{-A},$$

where $Z = x^{1/(n_L+1)}(\log x)^{-B}$.

We also need a result of Mertens, in connection with Dirichlet's work on primes in an arithmetic progression.

THEOREM 2.3 (Mertens [**10**]; see also [**3**, Chapter 7]).

$$\sum_{\substack{p \leqslant x \\ p \equiv a \ (\mathrm{mod}\ m)}} \frac{1}{p} = \frac{1}{\phi(m)} \log\log x + \mathrm{O}(1).$$

3. *Proof of Theorem* 1.1

We now prove Theorem 1.1. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$. Let $\mathcal{O}_K$ be the ring of integers of K. For a prime p of good reduction, $E(\mathbb{F}_p)$ is the set of $\mathbb{F}_p$-rational points of E. We use the notation $\sum'$ for the sum over primes of good reduction.

We consider

$$\sum_{p\leqslant x}{}' (\omega(\#E(\mathbb{F}_p)) - \log\log x)^2 = \sum_{p\leqslant x}{}' \omega^2(\#E(\mathbb{F}_p)) - 2\log\log x \sum_{p\leqslant x}{}' \omega(\#E(\mathbb{F}_p)) + (\log\log x)^2 \sum_{p\leqslant x}{}' 1.$$

The third term above is

$$\pi(x)(\log\log x)^2 + \mathrm{O}((\log\log x)^2).$$

Let $\delta \in \mathbb{R}$ with $0 < \delta < 1$ (a choice of δ will be made later). The sum in the second term can be written as

$$\begin{aligned}\sum_{p\leqslant x}{}' \omega(\#E(\mathbb{F}_p)) &= \sum_{p\leqslant x}{}' \sum_{\substack{l\mid\#E(\mathbb{F}_p)\\ l\leqslant x^{\delta}}} 1 + \sum_{p\leqslant x}{}' \sum_{\substack{l\mid\#E(\mathbb{F}_p)\\ l> x^{\delta}}} 1\\ &= \sum_{l\leqslant x^{\delta}} \sum_{\substack{p\leqslant x\\ l\mid\#E(\mathbb{F}_p)}}{}' 1 + \mathrm{O}(\pi(x)).\end{aligned}$$

The last inequality holds since $\#E(\mathbb{F}_p) \leqslant (p + 2\sqrt{p} + 1) \leqslant 3x$.

We now estimate the quantity

$$\sum_{l\leqslant x^{\delta}} \sum_{\substack{p\leqslant x\\ l\mid\#E(\mathbb{F}_p)}}{}' 1.$$

We divide the primes p into two cases: p is *supersingular* (ss), or p is *ordinary* (ord). Notice that p is supersingular if and only if p is ramified or inert in K; see [**4**]. Since there are only finitely many primes ramified in K, it suffices to consider only primes that are inert in K. This corresponds to the case where the Legendre symbol $(\frac{-D}{p}) = -1$ if p is odd [**9**]. Moreover, p is a supersingular prime if and only if $\#E(\mathbb{F}_p) = p+1$; see [**13**]. Let $a_1, a_2, \dots, a_{r_l} \in (\mathbb{Z}/lD\mathbb{Z})^*$ be such that $a_i \equiv -1 \bmod l$ and $(\frac{-D}{a_i}) = -1$. Applying Theorem 2.1, we have

$$\begin{aligned}\sum_{l\leqslant x^{\delta}} \sum_{\substack{p\leqslant x,\ \mathrm{ss}\\ l\mid\#E(\mathbb{F}_p)}}{}' 1 &= \sum_{l\leqslant x^{\delta}} \sum_{i=1}^{r_l} \sum_{\substack{p\leqslant x\\ p\equiv a_i \bmod lD}} 1 + \mathrm{O}(x^{\delta})\\ &= \sum_{l\leqslant x^{\delta}} \sum_{i=1}^{r_l} \pi(x, a_i, lD) + \mathrm{O}(x^{\delta})\\ &= \sum_{l\leqslant x^{\delta}} \frac{r_l}{\phi(lD)} \operatorname{li} x + \mathrm{O}(x(\log x)^{-A}),\end{aligned}$$

for any positive constant A, provided that $\delta < 1/2$. Notice that $r_l/\phi(lD) = 1/2(l-1)$. We have

$$\sum_{l\leqslant x^{\delta}} \sum_{\substack{p\leqslant x,\ \mathrm{ss}\\ l\mid\#E(\mathbb{F}_p)}}{}' 1 = \frac{1}{2}\pi(x)\log\log x + \mathrm{O}(\pi(x)).$$

Now we consider ordinary primes p of good reduction. Let π_p and $\overline{\pi}_p$ be roots of $x^2 - a_p x + p$, where $a_p = (p + 1 - \#E(\mathbb{F}_p))$. We have [**2**, Lemma 5.1.2]

$$\mathbb{Q}(\pi_p) = K.$$

Since there are only finitely many primes l ramified in K, we consider l in only the following two cases: l is inert or l is split. We consider first the primes l that are inert in K. Let (l) be the ideal $l\mathcal{O}_K$. Since

$$\#E(\mathbb{F}_p) = (\pi_p - 1)(\overline{\pi}_p - 1),$$

$l \mid \#E(\mathbb{F}_p)$ implies that $\pi_p \equiv 1 \bmod (l)$. Notice see there are at most six units in K. By Theorem 2.2, we have

$$\sum_{\substack{l \leqslant x^\delta \\ l:\ \text{inert}}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ l \mid \#E(\mathbb{F}_p)}} 1 \ll \sum_{\substack{N_{K/\mathbb{Q}}((l)) = l^2 \leqslant x^{2\delta} \\ l:\ \text{inert}}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ (\pi_p) \sim (1) \bmod (l)}} 1$$
$$\ll \sum_{\substack{N_{K/\mathbb{Q}}((l)) = l^2 \leqslant x^{2\delta} \\ l:\ \text{inert}}} \frac{\operatorname{li} x}{h((l))} + \mathrm{O}(x(\log x)^{-A}),$$

provided that $2\delta < \frac{1}{3}$. Since K has class number 1 and $r_1 = 0$, we have

$$h((l)) \geqslant \frac{\phi(l^2)}{6}.$$

It follows that

$$\sum_{\substack{l \leqslant x^\delta \\ l:\ \text{inert}}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ l \mid \#E(\mathbb{F}_p)}} 1 \ll \pi(x).$$

Now we consider

$$\sum_{\substack{l \leqslant x^\delta \\ l:\ \text{split}}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ l \mid \#E(\mathbb{F}_p)}} 1.$$

For l split, we write $(l) = \mathfrak{l}_1 \mathfrak{l}_2$. Hence $l \mid \#E(\mathbb{F}_p)$ implies that

$$\pi_p \equiv 1 \bmod \mathfrak{l}_1 \qquad \text{or} \qquad \pi_p \equiv 1 \bmod \mathfrak{l}_2.$$

We have

$$\sum_{\substack{l \leqslant x^\delta \\ l:\ \text{split}}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ l \mid \#E(\mathbb{F}_p)}} 1 = \frac{1}{2} \sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{l}) = l \leqslant x^\delta \\ l:\ \text{split}}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ \pi_p \equiv 1 \bmod \mathfrak{l}}} 1$$
$$= \frac{1}{2} \sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{l}) = l \leqslant x^\delta \\ l:\ \text{split}}} \frac{1}{T(\mathfrak{l})} \sideset{}{'}\sum_{\substack{N_{K/\mathbb{Q}}((\pi_p)) = p \leqslant x,\ \text{ord} \\ (\pi_p) \sim (1) \bmod \mathfrak{l}}} 1$$
$$= \frac{1}{2} \sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{l}) = l \leqslant x^\delta \\ l:\ \text{split}}} \frac{1}{\phi(\mathfrak{l})} \operatorname{li} x + \mathrm{O}(x(\log x)^{-A}).$$

The last equality follows from Theorem 2.2, provided that $\delta < \frac{1}{3}$.

Since $(l) = \mathfrak{l}_1\mathfrak{l}_2$, it follows that

$$\sum_{\substack{l \leqslant x^\delta \\ l:\,\text{split}}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ l \mid \#E(\mathbb{F}_p)}} 1 = \frac{1}{2} \cdot 2 \sum_{\substack{l \leqslant x^\delta \\ l:\,\text{split}}} \frac{1}{\phi(l)} \operatorname{li} x + \mathrm{O}(x(\log x)^{-A})$$

$$= \frac{1}{2}\pi(x) \log\log x + \mathrm{O}(\pi(x)).$$

The last inequality follows from Theorem 2.3, combined with the fact that an odd prime l splits if and only if the Legendre symbol $(\frac{-D}{l}) = 1$ (see [**4**]). Combine all the above calculations. Choosing $\delta = 1/7$, we obtain

$$\sideset{}{'}\sum_{p \leqslant x} \omega(\#E(\mathbb{F}_p)) = \pi(x) \log\log x + \mathrm{O}(\pi(x)).$$

Using the same arguments as above, we have

$$\sum_{\substack{l_1, l_2 \leqslant x^\delta \\ l_1 \neq l_2}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ss} \\ l_1 l_2 \mid \#E(\mathbb{F}_p)}} 1 = \frac{1}{2}\pi(x)(\log\log x)^2 + \mathrm{O}(\pi(x) \log\log x)$$

and

$$\sum_{\substack{l_1, l_2 \leqslant x^\delta \\ l_1 \neq l_2}} \sideset{}{'}\sum_{\substack{p \leqslant x,\ \text{ord} \\ l_1 l_2 \mid \#E(\mathbb{F}_p)}} 1 = \frac{1}{2}\pi(x)(\log\log x)^2 + \mathrm{O}(\pi(x) \log\log x),$$

provided that $4\delta < \frac{1}{3}$. Choosing $\delta = \frac{1}{13}$, it follows that

$$\sideset{}{'}\sum_{p \leqslant x} \omega^2(\#E(\mathbb{F}_p)) = \pi(x)(\log\log x)^2 + \mathrm{O}(\pi(x) \log\log x).$$

Combining all the above results, we obtain

$$\sum_{\substack{p \leqslant x \\ p:\,\text{good reduction}}} (\omega(\#E(\mathbb{F}_p)) - \log\log x)^2 \ll \pi(x) \log\log x.$$

This completes the proof of Theorem 1.1.

Acknowledgements. This paper is part of my PhD thesis [**8**]. I would like to thank my thesis advisor, Prof. B. Mazur, for many important comments about my work. I would also like to thank Prof. R. Murty for many useful discussions during the completion of this paper. Finally, I wish to express my gratitude to the referee for his/her valuable suggestions.

References

1. E. Bombieri, 'On the large sieve', *Mathematika* 12 (1965) 201–225.
2. A. C. Cojocaru, 'Cyclicity of elliptic curves modulo p', Ph.D. thesis, Queen's University, Canada, 2002.
3. H. Davenport, *Multiplicative number theory* (Springer, 2000).
4. M. Deuring, 'Die typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hansischen Univ.* 14 (1941) 197–272.
5. P. Erdős, 'On the normal order of prime factors of $p-1$ and some related problems concerning Euler's ϕ-functions', *Q. J. Math.* (*Oxford*) 6 (1935) 205–213.
6. 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.
7. E. Landau, 'Über Ideale und Primideale in Idealklassen', *Math. Zeit.* 2 (1918) 52–154.

8. Y.-R. Liu, 'Generalizations of the Turán and the Erdős–Kac theorems', Ph.D. Thesis, Harvard, 2003.
9. D. A. Marcus, *Number fields* (Springer, 1977) 74–75.
10. F. Mertens, 'Ein beitrag zur analytischen zahlentheorie', *J. Reine Angew. Math.* 78 (1874) 46–62.
11. S. A. Miri and V. K. Murty, 'An application of sieve methods to elliptic curves', *Progress in Cryptology – INDOCRYPT*, Lecture Notes in Comput. Sci. 2247 (Springer, Berlin, 2001) 91–98.
12. M. R. Murty and V. K. Murty, 'Prime divisors of Fourier coefficients of modular forms', *Duke. Math. J.* 51 (1984) 57–76.
13. J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. 106 (Springer, 1986) 179.
14. P. Turán, 'On a theorem of Hardy and Ramanujan', *J. London Math. Soc.* 9 (1934) 274–276.
15. A. I. Vinogradov, 'On the density hypothesis for Dirichlet L-functions', *Izv. Akad. Nauk SSSR Ser. Math.* 29 (1965) 903–934; 30 (1966) 719–720.
16. R. J. Wilson, 'The large sieve in algebraic number fields', *Mathematika* 16 (1969) 189–204.

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

yrliu@math.uwaterloo.ca