*The Quarterly Journal of Mathematics*, 2024, **75**, 757–777
doi:https://doi.org/10.1093/qmath/haae029
Advance Access published on 24 May 2024
**Article**

OXFORD

# CYCLICITY AND EXPONENT OF ELLIPTIC CURVES MODULO $p$ IN ARITHMETIC PROGRESSIONS

by PENG-JIE WONG[*,†]

Department of Applied Mathematics, National Sun Yat-Sen University, No. 70 Lienhai Road, Kaohsiung City 804, Taiwan

[†]Corresponding author. E-mail: pjwong@math.nsysu.edu.tw
Dedicated to Professor Ram Murty on the occasion of his seventieth birthday.

**ABSTRACT**

In this article, we study the cyclicity problem of elliptic curves $E/\mathbb{Q}$ modulo primes in a given arithmetic progression. We extend the recent work of Akbal and Güloğlu by proving an unconditional asymptotic for such a cyclicity problem over arithmetic progressions for elliptic curves $E$, which also presents a generalization of the previous works of Akbary, Cojocaru, M.R. Murty, V.K. Murty and Serre. In addition, we refine the conditional estimates of Akbal and Güloğlu, which gives log-power savings (for small moduli) and consequently improves the work of Cojocaru and M.R. Murty. Moreover, we study the average exponent of $E$ modulo primes in a given arithmetic progression and obtain several conditional and unconditional estimates, extending the previous works of Freiberg, Kim, Kurlberg and Wu.

## 1. INTRODUCTION

Let $E$ be an elliptic curve, defined over $\mathbb{Q}$, of conductor $N_E$. For a prime $p$ of good reduction, we let $\tilde{E}$ denote the reduction of $E$ modulo $p$ and $\tilde{E}(\mathbb{F}_p)$ be the group of rational points of $\tilde{E}$ over $\mathbb{F}_p$. The study of $\tilde{E}(\mathbb{F}_p)$, as $p$ varies, manifests as part of the 'analytic theory' of elliptic curves. Most profoundly, Lang and Trotter [17] formulated an elliptic curve analogue of Artin's primitive root conjecture, and Serre [25] considered the cyclicity problem of estimating

$$\pi_c(x,E) = \#\{p \leq x \mid p \nmid N_E \text{ and } \tilde{E}(\mathbb{F}_p)\text{is cyclic }\}.$$

For each $m \in \mathbb{N}$, let $E[m]$ denote the group of $m$-torsion points of $E$, and let $\mathbb{Q}(E[m])$ be the $m$th division field of $E$. In light of Hooley's conditional resolution of Artin's primitive root conjecture, Serre proved that assuming the generalized Riemann hypothesis (GRH), if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, then one has

$$\pi_c(x,E) = \mathfrak{c}_E \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right),$$

**Received** 25 September 2023; **Revised** 11 March 2024
© The Author(s) 2024. Published by Oxford University Press. All rights reserved. For commercial re-use, please contact reprints@oup.com for reprints and translation rights for reprints. All other permissions can be obtained through our RightsLink service via the Permissions link on the article page on our site–for further information please contact journals.permissions@oup.com.

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

where $\mathrm{Li}(x)$ is the usual logarithmic integral,

$$\mathfrak{c}_E = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]},$$

and $\mu(m)$ is the Möbius function. This was improved by M.R. Murty [20, pp. 160–161], who showed that under GRH, one has

$$\pi_c(x,E) = \mathfrak{c}_E \mathrm{Li}(x) + O\left(\frac{x(\log\log x)}{(\log x)^2}\right).$$

Moreover, the error term above was sharpened considerably by Cojocaru and M.R. Murty [5]. They proved under GRH that for any elliptic curve $E/\mathbb{Q}$ of conductor $N_E$, if $E$ is with complex multiplication (CM) by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K$, one has

$$\pi_c(x,E) = \mathfrak{c}_E \mathrm{Li}(x) + O(x^{3/4}(\log(N_E x))^{1/2}), \tag{1}$$

and if $E$ is non-CM, one has

$$\pi_c(x,E) = \mathfrak{c}_E \mathrm{Li}(x) + O(x^{5/6}(\log(N_E x))^{2/3}) + O\left(\frac{(\log\log x)(\log(N_E x))}{\log x} A(E)^3\right), \tag{2}$$

where $A(E)$ is the Serre's constant associated with $E$. (Recall that for each $m$, there is a natural injective representation $\rho_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ associated with $E$. Serre [24] proved that if $E$ is non-CM, then there exists a finite set $S_E$ of primes such that $\rho_\ell$ is surjective whenever $\ell \notin S_E$. Furthermore, setting

$$A(E) = 2 \cdot 3 \cdot 5 \cdot \prod_{\ell \in S_E \setminus \{2,3,5\}} \ell, \tag{3}$$

Serre's constant associated to $E$, $\rho_m$ is surjective when $(m, A(E)) = 1$ (see [4, Appendix]).)

There are several unconditional results regarding $\pi_c(x,E)$. For any elliptic curve $E/\mathbb{Q}$, Gupta and M.R. Murty [10] showed that $\pi_c(x,E) \gg x/(\log x)^2$. Moreover, for CM elliptic curves, the assumption of GRH was removed by M.R. Murty in [20] (where Wilson's Bombieri–Vinogradov theorem for number fields [26] was used, and no error terms were given). Furthermore, by the sieve of Eratosthenes and the effective version of the Chebotarev density theorem due to Lagarias and Odlyzko [16] (instead of using Wilson's theorem), Cojocaru [3] proved that for any CM elliptic curve $E/\mathbb{Q}$ of conductor $N_E$,

$$\pi_c(x,E) = \mathfrak{c}_E \mathrm{Li}(x) + O\left(\frac{x}{(\log x)(\log\log((\log x)/N_E^2))} \frac{\log\log x}{\log((\log x)/N_E^2)}\right).$$

Moreover, adapting M.R. Murty's argument and applying the Bombieri–Vinogradov theorem for number fields established by Huxley [12], Akbary and V.K. Murty [2] obtained the improvement that given any CM elliptic curve $E/\mathbb{Q}$ of conductor $N_E$, for any $A, B > 0$, one has

$$\pi_c(x,E) = \mathfrak{c}_E \mathrm{Li}(x) + O_{A,B}\left(\frac{x}{(\log x)^A}\right) \tag{4}$$

uniformly in $N_E \leq (\log x)^B$, where the implied constant only depends on $A$ and $B$.

Recently, Akbal and Güloğlu [1] proposed the cyclicity problem over arithmetic progressions, asking for estimates of

$$\pi_c(x,E,q,a) = \#\{p \leq x \mid p \nmid N_E, p \equiv a \,(\mathrm{mod}\, q), \text{and } \tilde{E}(\mathbb{F}_p) \text{is cyclic }\}$$

when $(a,q) = 1$. By extending the argument of Gupta and M.R. Murty [10], they proved the following theorem.

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

THEOREM 1.1 ([1, Theorem 1]) *Let $E/\mathbb{Q}$ be an elliptic curve, and let $a$ and $q$ be coprime natural numbers such that $(a-1,q)$ has no odd prime divisors. Assume that $[\mathbb{Q}(E[2]):\mathbb{Q}]=3$. Then, for any fixed $A\geq 0$ and sufficiently large $x$, when $q\ll(\log x)^A$, one has $\pi_c(x,E,q,a)\gg x/(\log x)^{2+A}$ unless $\mathbb{Q}(E[2])\subseteq\mathbb{Q}(\zeta_q)$ and $\sigma_a$ fixes $\mathbb{Q}(E[2])$. (Here, as later, $\mathbb{Q}(\zeta_q)$ is the $q$th cyclotomic extension of the rationals formed by adjoining a primitive $q$th root of unity $\zeta_q$, and $\sigma_a$ denotes the automorphism $\zeta_q\mapsto\zeta_q^a$.)*

Furthermore, under GRH, by generalizing the work of Cojocaru and M.R. Murty [5], Akbal and Güloğlu [1] determined the asymptotics for $\pi_c(x,E,q,a)$ as follows.

THEOREM 1.2 ([1, Theorems 3 and 5]) *Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N_E$, and let $a$ and $q$ be coprime natural numbers. Assume that GRH is valid for the Dedekind zeta function of $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)$ for every square-free $m$. Define*

$$\mathfrak{c}_E(q,a)=\sum_{m=1}^{\infty}\frac{\gamma_{E,m}(q,a)\mu(m)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]},$$

*where $\gamma_{E,m}(q,a)=1$ if the automorphism $\sigma_a$, defined as in Theorem 1.1, fixes $\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_q)$, and it is 0 otherwise. Then, one has*

$$\pi_c(x,E,q,a)=\mathfrak{c}_E(q,a)Li(x)+\mathcal{E}_c(x),$$

*where if $E$ is with CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K=\mathbb{Q}(\sqrt{-D})$, $\mathcal{E}_c(x)$ satisfies*

$$\mathcal{E}_c(x)\ll x^{3/4}\left(\frac{\log(qN_Ex)G_D(a,q)}{q^3}\right)^{1/2}+x^{3/4}\left(\frac{\log(qN_Ex)}{\log x}\right)^{1/2}$$
$$+x^{1/2}q\log(qN_Ex)+x^{1/2}\left(\frac{1}{q}+\frac{\log x}{q^2}\right)G_D(a,q)$$

*with $G_D(a,q)<c\cdot 4^{\omega(q)}\tau_2(q)q^2$, (here, $c=2$ if $D\equiv 1,2 \pmod 4$, or $D\equiv 3 \pmod 4$ and $q$ is odd; $c=49$ otherwise), and if $E$ is non-CM, one has*

$$\mathcal{E}_c(x)\ll x^{5/6}\left(\frac{H(q)(\log(qN_Ex))^2}{q}\right)^{1/3}+x^{5/8}\left(\frac{\tau_2(q_2)(\log(qN_Ex))^3}{\phi(q)\log x}M_E^3\right)^{1/4}$$
$$+x^{1/2}q\log(qN_Ex)+\frac{\tau_2(q_2)}{\phi(q)x^{1/2}\log x}M_E^3, \tag{5}$$

*where $q_2$ denotes the largest divisor of $q$ that is coprime to $M_E$ defined in (6) below.*

Here, as later, $\omega(n)$ denotes the number of prime divisors of $n$, and $\tau_2(n)$ is the number of (positive) divisors of $n$. In addition, $\phi(n)$ is Euler's totient function, and the arithmetic function $H(n)$ is defined by

$$H(n)=\sum_{d|n}\sum_{\substack{1\leq k\leq d\\ d|k^2}}1.$$

Also, $G_D(a,q)$ is the cardinality of the set defined in [1, Equation (23)], and its bound is given in [1, Equation (11)]. Last but not least, $M_E\in\mathbb{N}$ is defined by

$$M_E=\prod_{\ell|A(E)N_E}\ell, \tag{6}$$

where $A(E)$ is the Serre's constant defined in (3).

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

One of the main objectives of this article is to prove the following unconditional asymptotic of $\pi_c(x,E,q,a)$ for CM elliptic curves $E$.

THEOREM 1.3 *Let $E/\mathbb{Q}$ be a CM elliptic curve of conductor $N_E$, and let $a$ and $q$ be coprime natural numbers. Then, for any $A,B>0$, we have*

$$\pi_c(x,E,q,a)=\mathfrak{c}_E(q,a)Li(x)+O_{A,B}\left(\frac{x}{(\log x)^A}\right), \tag{7}$$

*uniformly in $qN_E\leq(\log x)^B$, where the implied constant only depends on $A$ and $B$.*

In addition, we have the following refinement of Theorem 1.2, which notably improves the estimates (1) and (2) of Cojocaru and M.R. Murty by factors of $(\log x)^{1/2}$ and $(\log x)^{1/3}$, respectively.

THEOREM 1.4 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N_E$, and let $a$ and $q$ be coprime natural numbers. Assume GRH. If $E$ has CM, then we have*

$$\pi_c(x,E,q,a)=\mathfrak{c}_E(q,a)Li(x)+O\left(x^{3/4}\frac{(\log(qN_Ex))^{1/2}}{(\log x)^{1/2}}+x^{1/4}\log N_E\right). \tag{8}$$

*In particular, we have*

$$\pi_c(x,E)=\mathfrak{c}_ELi(x)+O\left(x^{3/4}\frac{(\log(N_Ex))^{1/2}}{(\log x)^{1/2}}+x^{1/4}\log N_E\right).$$

*Furthermore, if $E$ is non-CM, we have*

$$\begin{aligned}&\pi_c(x,E,q,a)\\&=\mathfrak{c}_E(q,a)Li(x)+O\left(x^{5/6}\frac{(\log(qN_Ex))^{2/3}}{(\log x)^{1/3}}+\frac{\tau_2(q_2)\log(qN_Ex)}{\phi(q)}R_{E,q_1}\right),\end{aligned} \tag{9}$$

*where $q_1=\frac{q}{q_2}$, $q_2$ denotes the largest divisor of $q$ that is coprime to $M_E$, and*

$$R_{E,q_1}=\sum_{d|M_E}\frac{\phi((d,q_1))d^3}{\phi(d)}. \tag{10}$$

*Consequently, we have*

$$\pi_c(x,E)=\mathfrak{c}_ELi(x)+O\left(x^{5/6}\frac{(\log(N_Ex))^{2/3}}{(\log x)^{1/3}}+\log(N_Ex)\sum_{d|M_E}\frac{d^3}{\phi(d)}\right).$$

*In addition, both factors $M_E^3$ in (5) can be replaced by $R_{E,q_1}$.*

To obtain the improved asymptotic (8), we invoke the work of Hinz and Lodemann [**11**] on the Brun–Titchmarsh inequality for number fields, which allows us to deduce a refined bound (31) (cf. (21) and (22)). This is our key new observation. For the non-CM case, our results rely on an alternative bound for the 'middle range' $\Sigma_2'$ in (36) and a refined bound for the 'tail' $\Sigma_3$ in (37) arising from the sieving argument of Akbal and Güloğlu [**1**, Section 3.2]. When $H(q)/q$ is of a constant size, our result reduces the leading term of (5) by a factor of $(\log x)^{1/3}$. (It shall be noted that, in general, the leading error term in (9) is smaller than the one in (5) only if $\frac{q}{H(q)}\ll(\log x)^{1/3}$. So, our result does

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

*not* yield a consistent improvement but relies on $q$. It is worth further noting that the reason why we were not able to give a uniform description for the range of $q$, where the improvement is granted, mainly came from the irregular behaviour of $H(q)$ as discussed in [1, Remark 1].) Such a 'log-saving' is due to the insert of the Burn–Titchmarsh theorem when estimating $\Sigma_2'$. Also, when $q$ and $M_E$ do not have too many common divisors, $R_{E,q_1}$ gives a better estimate than $M_E^3$. For instance, if $(q, M_E) = 1$, $R_{E,q_1} = \sum_{d|M_E} d^3/\phi(d)$ presents a power-saving for the factors $M_E^3$ in (5).

**Remark**. (i) Note that $\pi_c(x, E, q, a) \le \pi(x, q, a) = \#\{p \le x \mid p \equiv a \pmod q\}$ and that under GRH for Dirichlet $L$-functions, for $(a, q) = 1$, one has

$$\pi(x, q, a) = \frac{1}{\phi(q)}\mathrm{Li}(x) + O(x^{1/2}\log(qx)).$$

Hence, when $\sqrt{x} \le q \le x$, assuming GRH, we have $\pi_c(x, E, q, a) \ll x^{1/2}\log x$, which provides a superior estimate than (8) and (9).

(ii) As may be noticed, applying Theorems 1.1 and 1.3, for coprime $a, q \in \mathbb{N}$ such that $(a-1, q)$ has no odd prime divisors, if $E/\mathbb{Q}$ has CM and satisfies $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 3$, then $\mathfrak{c}_E(q, a)$ is positive unless $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_q)$ and $\sigma_a$ fixes $\mathbb{Q}(E[2])$. (Under these assumptions, suppose, on the contrary, that $\mathfrak{c}_E(q, a) = 0$. Then, Theorem 1.3 gives $\pi_c(x, E, q, a) \ll x/(\log x)^3$, which contradicts the estimate $\pi_c(x, E, q, a) \gg x/(\log x)^{2+\varepsilon}$ given by Theorem 1.1 (with $A = \varepsilon \in (0, 1)$).) In general, determining necessary and sufficient conditions for the positivity of $\mathfrak{c}_E(q, a)$ appears as an interesting question. For example, there is an observation of Serre that $\mathfrak{c}_E \ne 0$ if and only if $E$ has an irrational 2-torsion point (see [5, p. 619] for a proof). Also, in [1, Theorems 4 and 6], Akbal and Güloğlu gave some sufficient conditions for the positivity of $\mathfrak{c}_E(q, a)$. More recently, Jones and Lee [13] systemically studied the question of which arithmetic progressions $a \pmod q$ admit the property that for all but finitely many primes $p \equiv a \pmod q$, $\tilde{E}(\mathbb{F}_p)$ is not cyclic. In particular, they gave a criterion for $\mathfrak{c}_E(q, a) = 0$ in [13, Section 3.2].

In a slightly different vein, knowing that for any prime $p$ of good reduction, there are natural numbers $d_p$ and $e_p$ such that $d_p \mid e_p$ and

$$\tilde{E}(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z},$$

one may also study the behaviours of $d_p$ and $e_p$ as $p$ varies. As the exponent $e_p$ is the largest possible order of points on $\tilde{E}(\mathbb{F}_p)$, determining the asymptotic for

$$\pi_e(x, E) = \sum_{p \le x} e_p$$

presents an interesting problem. Freiberg and Kurlberg [7] investigated this problem and showed that under GRH,

$$\sum_{p \le x} e_p = \mathfrak{e}_E\mathrm{Li}(x^2) + O(x^{19/10}(\log x)^{6/5}),$$

where

$$\mathfrak{e}_E = \sum_{m=1}^{\infty} \frac{1}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} \sum_{d|m} \frac{\mu(d)}{e};$$

they also showed that

$$\sum_{p \le x} e_p = \mathfrak{e}_E\mathrm{Li}(x^2) + O\left(\frac{x^2(\log\log\log x)}{(\log x)(\log\log x)}\right),$$

unconditionally, if $E/\mathbb{Q}$ is a CM elliptic curve. The errors in these two estimates were improved by Wu [28] to $O(x^{11/6}(\log x)^{1/3})$ and $O(x^2/(\log x)^{15/14})$, respectively. Furthermore, adapting the work

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

of Akbary and V.K. Murty [2], Kim [11] used Huxley's Bombieri–Vinogradov theorem for number fields [12] to show that if $E/\mathbb{Q}$ has CM, then for any $A, B > 0$, one has

$$\pi_e(x,E) = \mathfrak{e}_E \mathrm{Li}(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^A}\right) \tag{11}$$

uniformly in $N_E \leq (\log x)^B$, where the implied constant only depends on $A$ and $B$.

Inspired by the previously mentioned work of Akbal and Güloğlu [1], we consider the average of exponents over arithmetic progressions:

$$\pi_e(x,E,q,a) = \sum_{\substack{p\leq x \\ p\equiv a(\mathrm{mod}\, q)}} e_p$$

and prove the following generalization of Kim's work [11]. (Note that when $q = 1$, our result recovers Kim's estimate (11).)

THEOREM 1.5 *Let $E/\mathbb{Q}$ be a CM elliptic curve of conductor $N_E$, and let $a$ and $q$ be coprime natural numbers. Then setting*

$$\mathfrak{e}_E(q,a) = \sum_{m=1}^{\infty}\sum_{de|m} \frac{\mu(d)}{e} \frac{\gamma_{E,m}(q,a)\mu(m)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]},$$

*for any $A, B > 0$, we have*

$$\pi_e(x,E,q,a) = \mathfrak{e}_E(q,a)Li(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^A}\right) \tag{12}$$

*uniformly in $qN_E \leq (\log x)^B$, where the implied constant only depends on $A$ and $B$.*

Moreover, we have the following extension of the works of Freiberg–Kurlberg and Wu mentioned earlier, which particularly presents refinements of their results by taking $q = 1$.

THEOREM 1.6 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N_E$, and let $a$ and $q$ be coprime natural numbers. Assume that GRH is valid for the Dedekind zeta function of $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)$ for every square-free $m$. Then*

$$\pi_e(x,E,q,a) = \mathfrak{e}_E(q,a)Li(x^2) + x\mathcal{E}_e(x),$$

*where if $E$ is with CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, $\mathcal{E}_e(x)$ satisfies both bounds*

$$\mathcal{E}_e(x) \ll x^{3/4}\frac{(\log(qN_Ex))^{1/2}}{(\log x)^{1/2}} + x^{1/4}\log N_E$$

*and*

$$\begin{aligned}\mathcal{E}_e(x) \ll{}& x^{3/4}\left(\frac{\log(qN_Ex)G_D(a,q)}{q^3}\right)^{1/2} + x^{3/4}\left(\frac{\log(qN_Ex)}{\log x}\right)^{1/2} \\ &+ x^{1/2}q\log(qN_Ex) + x^{1/2}\left(\frac{1}{q}+\frac{\log x}{q^2}\right)G_D(a,q),\end{aligned} \tag{13}$$

*with the same $G_D(a,q)$ as in Theorem 1.2, and if $E$ is non-CM, $\mathcal{E}_e(x)$ satisfies both estimates*

$$\mathcal{E}_e(x) \ll x^{5/6}\frac{(\log(qN_Ex))^{2/3}}{(\log x)^{1/3}} + \frac{x^{1/2}}{q} \tag{14}$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

*and*

$$\mathcal{E}_e(x) \ll x^{5/6}\left(\frac{H(q)(\log(qN_Ex))^2}{q}\right)^{1/3} + x^{5/8}\left(\frac{\tau_2(q_2)(\log(qN_Ex))^3}{\phi(q_2)\log x}S_E\right)^{1/4} + x^{1/2}q\log(qN_Ex) + \frac{\tau_2(q_2)}{\phi(q_2)x^{1/2}\log x}S_E, \tag{15}$$

*where* $S_E = \sum_{d|M_E^\infty}\frac{B_E}{d\phi(d)}$, *and* $B_E$ *is the constant, depending only on E, as in [7, Proposition 3.2], such that* $B_E\cdot[\mathbb{Q}(E[m]):\mathbb{Q}] \geq |GL_2(\mathbb{Z}/m\mathbb{Z})|$ *for every m. (The existence of* $B_E$ *is due to Serre's open image theorem. It may be possible to determine* $B_E$ *in terms of* $N_E$ *by an effective version of Serre's open image theorem (see [19] and references therein) or the index bound for the image of the 'adelic' representation attached to E (see [18]). However, as it seemingly requires a delicate algebraic and representation-theoretic argument that appears beyond this article's scope, we shall reserve it as a future project.)*

**Remark**. (i) It is worthwhile noting that our unconditional estimates (7) and (12) come from the effective version of the Chebotarev density theorem established by V.K. Murty [23]. This is the main observation in the proofs of Theorems 1.3 and 1.5 that verifying Artin's (holomorphy) conjecture for the Galois extensions $L/\mathbb{Q}$ involved (see Lemma 2.5) allows us to remove $n_L$, the degree of $L$, in the error term of the effective version of the Chebotarev density theorem (26) due to Lagarias and Odlyzko [16].

(ii) Compared to the works [2, 11], our argument does not rely on Huxley's Bombieri–Vinogradov theorem for number fields. Still, it obtains results of the same strength (which also particularly gives an improvement of Cojocaru's work [3]). Moreover, our method allows us to express the errors in terms of the location of the possible Landau–Siegel zeros of Dirichlet $L$-functions. This feature could not be seen from the method relying on the Bombieri–Vinogradov theorem for number fields, and it leads to a conditional resolution of a question of Akbary and V.K. Murty on improving the error term in their estimate (4) as discussed below.

Akbary and V.K. Murty [2] remarked that their theorem can be viewed as an elliptic analogue of the following weak form of the classical Siegel-Walfisz theorem: for any $(a,q)=1$, one has

$$\pi(x,q,a) = \frac{1}{\phi(q)}\mathrm{Li}(x) + O_{A,B}\left(\frac{x}{(\log x)^A}\right),$$

uniformly for $q \leq (\log x)^B$, for any given $A, B > 0$. Moreover, recalling that the Siegel–Walfisz theorem, in fact, states that for any $B > 0$, there exists $c_0 = c_{0,B}$ such that

$$\pi(x,q,a) = \frac{1}{\phi(q)}\mathrm{Li}(x) + O\left(x\exp(-c_0\sqrt{\log x})\right)$$

uniformly in $q \leq (\log x)^B$, Akbary and V.K. Murty noted that it seems quite unclear how to extend this to their setting (i.e., to the cyclicity problem). In Section 7, we shall show that such an expected stronger estimate follows from the non-existence of the Landau–Siegel zeros of Dirichlet $L$-functions. Indeed, we have the following conditional result.

THEOREM 1.7 *Let* $E/\mathbb{Q}$ *be a CM elliptic curve of conductor* $N_E$, *and let a and q be coprime natural numbers. Assume that there exists a constant* $S \geq -1$ *such that for any* $Q \in \mathbb{N}$ *and any real primitive character* $\chi$ *modulo Q,*

$$L(1,\chi) \gg (\log Q)^{-S}, \tag{16}$$

*where* $L(s,\chi)$ *is the Dirichlet L-function attached to* $\chi$, *and the implied constant is absolute. Then, there is an absolute constant* $c_1 > 0$ *so that uniformly for* $\log(qN_E) \ll (\log x)^{1/(2S+4)}$, *(such*

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

*uniformity can be precisely written as* $qN_E \leq \exp\left(\frac{1}{2\kappa}(\log x)^{1/(2S+4)}\right)$ *with the same* $\kappa$ *as in (24)), we have*

$$\pi_c(x,E,q,a) = \mathfrak{c}_E(q,a)Li(x) + O\left(x\exp\left(-c_1(\log x)^{1/(2S+4)}\right)\right)$$

*and*

$$\pi_e(x,E,q,a) = \mathfrak{e}_E(q,a)Li(x^2) + O\left(x^2\exp\left(-c_1(\log x)^{1/(2S+4)}\right)\right).$$

**Remark**. It is well known that the non-existence of the Landau-Siegel zeros implies that (16) holds with $S=-1$ (see [**8**, Section 1]). In his recent preprint [**29**], Zhang announced that $S=2022$ is admissible; however, as [**29**] is still unpublished, Theorem 1.7 shall be treated with caution as a conditional result.

The rest of the article is organized as follows. In the next section, we will collect the necessary preliminaries to prove our results (particularly, we will discuss the effective version of the Chebotarev density theorem established by V.K. Murty). Theorems 1.3, 1.4, 1.5 and 1.6 will be proved in Sections 3, 4, 5 and 6, respectively. In the last section, we will prove Theorem 1.7.

## 2. PRELIMINARIES

### 2.1. Artin's (holomorphy) conjecture and the Chebotarev density theorem

In this section, we shall recall the effective version of the Chebotarev density theorem established by V.K. Murty. To state his result, we require the following notation. For a number field $F$, we let $d_F$ and $n_F$ denote the absolute discriminant and degree of $F$, respectively. Let $L/K$ be a Galois extension of number fields with Galois group $G$. The set of irreducible characters of $G$ will be denoted by $\mathrm{Irr}(G)$, and the biggest character degree of $G$ is defined by $b(G)=\max_{\chi\in\mathrm{Irr}(G)}\chi(1)$. Also, for each $\chi\in\mathrm{Irr}(G)$, we let $\mathfrak{f}_\chi$ stand for the (global) Artin conductor of $\chi$, and we set

$$\mathcal{A}=\mathcal{A}(L/K)=\max_{\chi\in\mathrm{Irr}(G)}A_\chi,$$

where $A_\chi = d_K^{\chi(1)}\mathrm{N}(\mathfrak{f}_\chi)$. Moreover, we recall from [**22**, Proposition 2.5] that

$$\log \mathrm{N}(\mathfrak{f}_\chi) \leq 2\chi(1)n_K\left(\sum_{p\in P(L/K)}\log p + \log(n_L/n_K)\right), \tag{17}$$

where $P(L/K)$ denotes the set of rational primes $p$ for which there is a prime $\mathfrak{p}\mid p$ of $K$ such that $\mathfrak{p}$ is ramified in $L$. Following [**23**, Section 4], we further put

$$\log\mathcal{M}=\log\mathcal{M}(L/K)=\frac{1}{n_K}\log d_K + 2\sum_{p\in P(L/K)}\log p + 2\log(n_L/n_K). \tag{18}$$

Let $C$ be a conjugacy class of $G=\mathrm{Gal}(L/K)$, and let $\pi_C(x)$ denote the number of primes $\mathfrak{p}$ of $K$, with $\mathrm{N}(\mathfrak{p})\leq x$, whose Artin symbol equals $C$. In [**23**], V.K. Murty proved the following effective version of the Chebotarev density theorem under Artin's conjecture.

THEOREM 2.1 ([**23**, Theorem 4.1]) *If Artin's conjecture holds for* $L/K$*, then there is an absolute* $c_2>0$ *such that for any conjugacy class* $C$ *in* $G$*, one has*

$$\begin{aligned}\pi_C(x) = {}& \frac{|C|}{|G|}Li(x) - \frac{|C|}{|G|}\chi_1(C)Li(x^{\beta_1}) \\ & + O\left(|C|^{\frac{1}{2}}n_K x(\log(\mathcal{M}x))^2\exp\left(\frac{-c_2\log x}{b(G)^{\frac{3}{2}}\sqrt{b(G)^3(\log\mathcal{A})^2+n_K\log x}}\right)\right)\end{aligned} \tag{19}$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

*provided that* $\log x \gg b(G)^4 n_K \log \mathcal{M}$. *Here,* $\beta_1$ *is the possible exceptional zero of* $\zeta_L(s)$, *the Dedekind zeta function of* $L$. *If* $\beta_1$ *exists, then it must arise from* $L(s, \chi_1, L/K)$, *the Artin L-function attached to* $\chi_1$, *for some character* $\chi_1$ *that is real and abelian (i.e one-dimensional).*

When $K = \mathbb{Q}$, we know that $\chi_1$ corresponds to a real (quadratic) Dirichlet character modulo $Q_1$ (say). By (17), we have

$$\log Q_1 \ll \sum_{p \in P(L/\mathbb{Q})} \log p + \log n_L, \tag{20}$$

which will allow us to apply the following theorem of Siegel later.

THEOREM 2.2 (Siegel) *With the same notation as above, for any* $\varepsilon > 0$, *there is an absolute (ineffective) constant* $c_3(\varepsilon) > 0$ *such that*

$$\beta_1 < 1 - \frac{c_3(\varepsilon)}{Q_1^{\varepsilon}}.$$

### 2.2. Elliptic curves and associated prime-counting functions

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N_E$, and let $E[m]$ denote the set of $m$-torsion points of $E$. It is well known that $\mathbb{Q}(E[m])/\mathbb{Q}$ forms a Galois extension. Also, the ramified primes of $\mathbb{Q}(E[m])/\mathbb{Q}$ are divisors of $mN_E$ (see [5, Proposition 3.5]). Consequently, as $\mathbb{Q}(\zeta_q) \subset \mathbb{Q}(E[q])$, we know that $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) \subset \mathbb{Q}(E[mq])$, and thus the ramified primes of $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)$ must divide $mqN_E$.

We shall require the following handy lemmata (see [5, Lemma 2.1] and [11, Lemma 2.2]).

LEMMA 2.3 *Assume that* $p \nmid N_E$. *Then* $\tilde{E}(\mathbb{F}_p)$ *is cyclic if and only if* $p$ *does not split completely in* $\mathbb{Q}(E[m])$ *for any square-free* $m > 1$.

LEMMA 2.4 *Let* $E/\mathbb{Q}$ *be an elliptic curve and* $p$ *be a prime of good reduction. Then,* $p$ *splits completely in* $\mathbb{Q}(E[m])$ *if and only if* $m \mid d_p$.

We set $\pi_{E,1}(x, q, a) = \#\{p \le x \mid p \nmid N_E, p \equiv a \pmod q\}$, and for integers $m > 1$, we define

$$\pi_{E,m}(x, q, a) = \#\{p \le x \mid p \nmid N_E \text{ splits completely in } \mathbb{Q}(E[m]), p \equiv a \pmod q\}.$$

In the remaining part of this section, we shall further assume that $E$ has CM by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K$. Recall that for any $3 \le m \le \sqrt{x} + 1$, one has

$$\pi_{E,m}(x, q, a) \le \#\{p \le x \mid p \nmid N_E \text{splits completely in } \mathbb{Q}(E[m])\} \ll \frac{x}{m^2}, \tag{21}$$

where the implied constant is absolute (see [11, Lemma 2.3] or [20, Lemma 5]). In addition, the argument used in [1, Sectioon 4.1] yields

$$\sum_{y < m \le \sqrt{x}+1} \pi_{E,m}(x, q, a) \ll \left( \frac{\sqrt{x}}{q} + \frac{\sqrt{x}\log x}{q^2} + \frac{x}{yq^3} \right) G_D(a, q), \tag{22}$$

for $2q \le y \le \sqrt{x}$, where $G_D(a, q)$ is the same as in Theorem 1.2.

**Remark**. It may be noticed that in (21), the dependence of $q$ is dropped. It is undoubtedly desirable to obtain a uniform upper bound for $\pi_{E,m}(x, q, a)$ with explicit dependence of $q$ (whenever $E$ is with CM or not). In general, it manifests as a Brun–Titchmarsh type inequality for the Chebotarev density theorem. The known results usually require $x$ significantly greater than a power of the absolute discriminant of $\mathbb{Q}(E[m])$, (see [15, Theorem 1.4]), which is often too large for our purpose. On

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

the other hand, for CM curves, the proof of (21) translates the original estimate to a lattice-counting problem over quadratic fields (see [20, Lemma 5]). However, tracing the involving mod $q$ condition appears to be unclear during the translating procedure. To a certain degree, this reflects the fact that the degrees of the composite fields $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)$ do not behave uniformly but depend on the common prime factors of $m$, $q$ and $M_E$.

It can be shown that if $E$ is with CM by $\mathcal{O}_K$, then $\mathbb{Q}(E[m])/\mathbb{Q}$ is a meta-abelian extension, and thus Artin's conjecture holds for $\mathbb{Q}(E[m])/\mathbb{Q}$. (By a meta-abelian extension $L/K$, we mean that $L/K$ is a Galois extension with Galois group $G$, and $G$ admits an abelian normal subgroup $N$ such that $G/N$ is also abelian. For such an instance, all the irreducible representations of $G$ are monomial (namely, induced from one-dimensional representations of subgroups of $G$), and thus Artin's conjecture is known. In fact, it can be further shown that Langlands reciprocity holds for such $L/K$ (see [27, Theorem 2.5]).) In what follows, we shall extend this result to $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}$.

LEMMA 2.5 *In the notation as above, if $E$ is with CM by $\mathcal{O}_K$, then Artin's conjecture holds for $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}$. In addition, the biggest character degree $b(Gal(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}))$ of the Galois group of $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is at most 2.*

*Proof.* In [20, Lemma 4], M.R. Murty proved that there exists an integral ideal $\mathfrak{f} = \mathfrak{f}_E$ of $K$ such that

$$K_{\mathfrak{m}} \subseteq K(E[m]) \subseteq K_{\mathfrak{f}\mathfrak{m}},$$

where $K_{\mathfrak{m}}$ and $K_{\mathfrak{f}\mathfrak{m}}$ are ray class fields of $K$ of levels $\mathfrak{m} = m\mathcal{O}_K$ and $\mathfrak{f}\mathfrak{m}$, respectively. In addition, he showed that if $m \geq 3$, then $\mathbb{Q}(E[m]) = K(E[m])$. Consequently, for $m \geq 3$, $\mathrm{Gal}(\mathbb{Q}(E[m])/K)$ is abelian, and so there is an abelian normal subgroup $N$ of $G = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ such that the fixed field of $N$ in $\mathbb{Q}(E[m])/\mathbb{Q}$ is $K$. As $[K : \mathbb{Q}] = 2$, $G/N$ is of order two and thus a nilpotent group. Therefore, by [12, Proposition 2.7], when $m \geq 3$, for any $\chi \in \mathrm{Irr}(\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}))$, we have $\chi(1) \leq 2$. On the other hand, since $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, $|\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})|$ is either 1, 2, 3 or 6, which means that $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is an abelian group or $S_3$. Thus, $b(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})) \leq 2$.

Now, since $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is abelian, it then follows that for $m \geq 2$, every irreducible character of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is of degree at most 2. Furthermore, recalling that the map $\sigma \mapsto (\sigma|_{\mathbb{Q}(E[m])}, \sigma|_{\mathbb{Q}(\zeta_q)})$ defines an injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, from the above discussion, we conclude that

$$b(\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q})) \leq b(\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})) \leq 2.$$

In other words, the set

$$\mathrm{cd}(\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q})) := \{\chi(1) \mid \chi \in \mathrm{Irr}(\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}))\}$$

is either $\{1\}$ or $\{1, 2\}$, where the former instance implies that $\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is abelian. Hence, applying Artin reciprocity and [27, Corollary 5.2], Artin's conjecture holds for $\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}$. □

Now, we shall consider $L/K = \mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}$. By (18) and the fact that $[\mathbb{Q}(E[m]) : \mathbb{Q}] \ll m^2$, we deduce

$$\log \mathcal{M}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q}) \ll \sum_{p \mid mqN_E} \log p + \log(m^2 q) \ll \log(mqN_E).$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

Hence, when $(\log(mqN_E))^2 \ll \log x$, as $(\log \mathcal{A})^2 \ll \log x$ in this case, (19) implies that

$$\pi_C(x) = \frac{|C|}{|G|}\mathrm{Li}(x) - \frac{|C|}{|G|}\chi_1(C)\mathrm{Li}(x^{\beta_1}) + O\left(|C|^{\frac{1}{2}} x \exp(-c_2'\sqrt{\log x})\right), \tag{23}$$

for some $c_2' \in (0, c_2)$ with $c_2$ given in Theorem 2.1, where $\beta_1$ is the possible exceptional zero of the Artin $L$-function $L(s, \chi_1, \mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q})$. As $\chi_1$ is abelian, Artin reciprocity tells us that $\chi_1$ can be regarded as a Dirichlet character, (by a slight abuse of notation, we shall denote such a Dirichlet character by $\chi_1$), and $L(s, \chi_1, \mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)/\mathbb{Q})$ corresponds to the Dirichlet $L$-function attached to $\chi_1$. Moreover, by (20), the modulus $Q_1$ of $\chi_1$ satisfies

$$\log Q_1 \ll \sum_{p \mid mqN_E} \log p + \log(m^2 q) \ll \log(mqN_E)$$

which means that

$$\log Q_1 \leq \kappa \log(mqN_E) \tag{24}$$

for some absolute $\kappa > 0$. Thus, by Theorem 2.2, for any $\varepsilon > 0$, we have

$$\mathrm{Li}(x^{\beta_1}) \ll \frac{x^{\beta_1}}{\log x} \ll \frac{x}{\log x} \exp\left(\log x \frac{-c_3(\varepsilon)}{Q_1^{\varepsilon}}\right) \leq \frac{x}{\log x} \exp\left(\log x \frac{-c_3(\varepsilon)}{e^{\varepsilon\kappa \log(mqN_E)}}\right).$$

Assume that $m \leq (\log x)^A$ and $qN_E \leq (\log x)^B$. Note that under this assumption, we have

$$\log(mqN_E) \leq (A+B)\log\log x,$$

which particularly gives

$$(\log mqN_E)^2 \ll_{A,B} \log x.$$

Hence, choosing $\varepsilon = 1/(2\kappa(A+B))$, we arrive at

$$\pi_C(x) = \frac{|C|}{|G|}\mathrm{Li}(x) + O\left(\frac{x}{\log x}\exp(-c_3\sqrt{\log x}) + |C|^{\frac{1}{2}} x \exp(-c_2'\sqrt{\log x})\right)$$

with $c_3 = c_3(1/(2\kappa(A+B)))$. Thus, for any $A, B > 0$, we have

$$\pi_{E,m}(x, q, a) = \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]}\mathrm{Li}(x) + O\left(x \exp(-c_{5,A,B}\sqrt{\log x})\right), \tag{25}$$

for some positive constant $c_{5,A,B}$ depending only on $A, B$, provided $m \leq (\log x)^A$ and $qN_E \leq (\log x)^B$. Here, the factor $\gamma_{E,m}(q,a)$ is defined as in Theorem 1.2 (for the rationale of the appearance of $\gamma_{E,m}(q,a)$, see [**1**, Section 3.2.1]).

**Remark**. (i) The effective version of the Chebotarev density theorem due to Lagarias and Odlyzko [**16**] gives

$$\pi_C(x) = \frac{|C|}{|G|}\mathrm{Li}(x) + O\left(|C| x \exp(-c_5'\sqrt{(\log x)/n_L})\right) \tag{26}$$

with some absolute $c_5' > 0$. (See also [**21**, Lemma 2]. It is worth noting that as Artin's conjecture is known for abelian extensions, one may improve [**21**, Theorem 1] on an analogue of Artin's primitive root conjecture for abelian extensions by utilizing (19) instead of [**21**, Lemma 2].) So, without Artin's conjecture, to have an estimate of similar strength as (23) (and its consequence (25)) for $L = \mathbb{Q}(E[m])\mathbb{Q}(\zeta_q)$, one would have to work over a much more restricted range of $m$ (which is roughly

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

at most $\ll \sqrt{\log x}$ since $\phi(m) \ll [\mathbb{Q}(E[m]) : \mathbb{Q}] \ll m^2$). However, to prove (7) and (12) for any given $A > 0$, it is crucial to the uniformity of the estimate (25) for $m \leq (\log x)^A$.
(ii) The Siegel–Walfisz type estimate (25) can be improved significantly under GRH. Indeed, assuming GRH, by the work of Lagarias–Odlyzko [16], for any elliptic curve $E/\mathbb{Q}$ (not necessarily with CM), one has

$$\pi_{E,m}(x,q,a) = \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]}\mathrm{Li}(x) + O\left(x^{\frac{1}{2}}\log([\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]mqN_E)\right),$$

(see also [5, Theorem 3.1 and Lemma 3.4]). If $E$ has CM, $[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}] \ll m^2 q$; otherwise, $[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}] \ll m^4 q$. Therefore, the above estimate becomes

$$\pi_{E,m}(x,q,a) = \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]}\mathrm{Li}(x) + O\left(x^{\frac{1}{2}}\log(mqN_E)\right), \tag{27}$$

where the implied constant is absolute. As shall be seen in the proofs of Theorems 1.4 and 1.6, (27) plays a crucial role in helping us to obtain the power-savings for the estimates involved.

## 3. PROOF OF THEOREM 1.3

Let $E$ be an elliptic curve over $\mathbb{Q}$. Recall that the order of $\tilde{E}(\mathbb{F}_p)$ can be written as $|\tilde{E}(\mathbb{F}_p)| = p + 1 - a_p$ for some $a_p \in \mathbb{Z}$ satisfying Hasse's bound $|a_p| \leq 2\sqrt{p}$. Also, by Lemma 2.4, if $p \nmid N_E$ splits completely in $\mathbb{Q}(E[m])$, then $m^2$ divides $|\tilde{E}(\mathbb{F}_p)|$. Consequently, for such an instance, we must have $m^2 \leq p + 1 + 2\sqrt{p} = (\sqrt{p}+1)^2 \leq (\sqrt{x}+1)^2$ if $p \leq x$.

In the remaining part of this section, we shall further assume that $E$ is with CM by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K$. Now, an application of the inclusion–exclusion principle, Lemma 2.3, and the above discussion give

$$\begin{aligned}\pi_c(x,E,q,a) &= \#\{p \leq x \mid p \nmid N_E, p \equiv a \,(\mathrm{mod}\, q), \text{and } \tilde{E}(\mathbb{F}_p) \text{is cyclic }\} \\ &= \sum_{m \leq y}\mu(m)\pi_{E,m}(x,q,a) + O\left(\frac{x}{y}\right),\end{aligned} \tag{28}$$

for any $3 \leq y \leq \sqrt{x}+1$, where $\pi_{E,m}(x,q,a)$ is defined as in Section 2.2, and the big-O term follows from (21) and the elementary bound

$$\sum_{m>y}\frac{x}{m^2} \ll \frac{x}{y}.$$

From (25), it follows that the sum in (28) equals

$$\sum_{m \leq y}\frac{\gamma_{E,m}(q,a)\mu(m)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]}\mathrm{Li}(x) + O\left(yx\exp(-c_{S,A,B}\sqrt{\log x})\right), \tag{29}$$

provided that $3 \leq y \leq (\log x)^A$ and $qN_E \leq (\log x)^B$, where $\gamma_{E,m}(q,a)$ is defined as before. By the fact that $[\mathbb{Q}(E[m]) : \mathbb{Q}] \gg \phi(m)^2$, it has been shown in the first displayed estimate of [1, Section 4.1] that

$$\sum_{m>y}\frac{\mu(m)^2}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]} \ll \frac{1}{y},$$

and thus

$$\sum_{m>y}\frac{\gamma_{E,m}(q,a)\mu(m)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]}\mathrm{Li}(x) \ll \frac{x}{y\log x}. \tag{30}$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

Finally, choosing $y = (\log x)^A$ and combining (28), (29) and (30), we establish

$$\begin{aligned}\pi_c(x,E,q,a) &= \sum_{m\le(\log x)^A} \frac{\gamma_{E,m}(q,a)\mu(m)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x)\\ &\quad + O\left(x(\log x)^A \exp(-c_{5,A,B}\sqrt{\log x}) + \frac{x}{(\log x)^A}\right)\\ &= \sum_{m=1}^{\infty} \frac{\gamma_{E,m}(q,a)\mu(m)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x) + O_{A,B}\left(\frac{x}{(\log x)^A}\right),\end{aligned}$$

whenever $qN_E \le (\log x)^B$, as desired.

## 4. PROOF OF THEOREM 1.4

In this section, we will prove Theorem 1.4. As shall be seen, the key new input is the Brun-Titchmarsh theorem and its variant for number fields.

### 4.1. A CM refinement

We begin by recalling the work of Hinz and Lodemann on the Brun–Titchmarsh inequality for number fields. Given a number filed $F$, for any coprime integral ideals $\mathfrak{a}, \mathfrak{q}$ of $F$, we set

$$\pi(x,\mathfrak{q},\mathfrak{a}) = \#\{\mathfrak{p}\subset\mathcal{O}_F \mid \mathrm{N}(\mathfrak{p})\le x \text{ and } \mathfrak{p}\sim\mathfrak{a} \pmod{\mathfrak{q}}\},$$

where $\mathfrak{p}$ stands for a prime of $F$, and $\mathfrak{p}\sim\mathfrak{a} \pmod{\mathfrak{q}}$ means that $\mathfrak{p}$ and $\mathfrak{a}$ are in the same ray class of the ray class group modulo $\mathfrak{q}$. By [11, Theorem 4] of Hinz and Lodemann, it is known that for any $(\mathfrak{a},\mathfrak{q}) = 1$, if $N(\mathfrak{q}) < x$, then

$$\pi(x,\mathfrak{q},\mathfrak{a}) \le \frac{2x}{h(\mathfrak{q})\log(x/N(\mathfrak{q}))}\cdot\left(1+O\left(\frac{\log\log(3x/N(\mathfrak{q}))}{\log(x/N(\mathfrak{q}))}\right)\right),$$

where $h(\mathfrak{q})$ denotes the cardinality of the ray class group modulo $\mathfrak{q}$.

Let $h_F$ denote the class number of $F$ and $r_1$ be the number of real embeddings of $F$. Recall that $h(\mathfrak{q})$ can be expressed as

$$h(\mathfrak{q}) = \frac{h_F 2^{r_1}\Phi(\mathfrak{q})}{T(\mathfrak{q})},$$

where $T(\mathfrak{q})$ is the number of residue classes $(\mathrm{mod}\,\mathfrak{q})$ that contain a unit, and $\Phi(\mathfrak{q})$ is the number field analogue of Euler's totient function for $F$. Moreover, if $F$ is an imaginary quadratic field, then $T(\mathfrak{q}) \le 6$. Therefore, if $F$ is an imaginary quadratic field of class number 1, one has

$$\frac{1}{h(\mathfrak{q})} \le \frac{6}{\Phi(\mathfrak{q})}.$$

For an elliptic curve $E$ with CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K$, $K$ must be of class number 1. As discussed in the proof of Lemma 2.5, by the work of M.R. Murty [20], we know that $K_{\mathfrak{m}} \subseteq K(E[m]) = \mathbb{Q}(E[m])$ for $m \ge 3$, where $K_{\mathfrak{m}}$ is the ray class field of $K$ of level $\mathfrak{m} = m\mathcal{O}_K$. Hence, if a rational prime $p$ splits completely in $\mathbb{Q}(E[m])$, then for any $\mathfrak{p}$ of $K$ that is above $p$, $\mathfrak{p}$ must splits completely in $K(E[m])$ and thus in $K_{\mathfrak{m}}$. Consequently, for $m \ge 3$, we have

$$\pi_{E,m}(x) \le \pi(x,\mathfrak{m},1) + \log N_E,$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

where $\mathbf{1} = 1 \cdot \mathcal{O}_K = \mathcal{O}_K$, and $N_E$ is the conductor of $E$. Therefore, from the above discussion, it follows that for any fixed $\theta \in (0, \frac{1}{2})$, if $3 \leq y \leq x^\theta$, then

$$\begin{aligned}\sum_{y<m\leq x^\theta} \pi_{E,m}(x,q,a) &\ll \sum_{y<m\leq x^\theta} \frac{x}{\Phi(\mathfrak{m})\log(x/\mathrm{N}(\mathfrak{m}))} + x^\theta \log N_E \\ &\ll_\theta \sum_{y<m\leq x^\theta} \frac{x}{\phi(m)^2 \log x} + x^\theta \log N_E.\end{aligned} \tag{31}$$

This bound, together with the estimate

$$\sum_{m>X} \frac{1}{\phi(m)^2} \ll \frac{1}{X} \tag{32}$$

(see [1, Lemma 11]) and (21), then gives

$$\sum_{y<m\leq\sqrt{x}+1} \pi_{E,m}(x,q,a) \ll \frac{x}{y\log x} + x^\theta \log N_E + \frac{x}{x^\theta}. \tag{33}$$

Thus, by an argument similar to the one leading to (28) and the above bound, we have

$$\pi_c(x,E,q,a) = \sum_{m\leq y} \mu(m)\pi_{E,m}(x,q,a) + O\left(\frac{x}{y\log x} + x^\theta \log N_E + \frac{x}{x^\theta}\right).$$

Hence, using (27) and (30), we obtain

$$\begin{aligned}\pi_c(x,E,q,a) = \sum_{m=1}^{\infty} \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x) + O\left(yx^{1/2}\log(qN_E x)\right) \\ + O\left(\frac{x}{y\log x} + x^\theta \log N_E + x^{1-\theta}\right).\end{aligned} \tag{34}$$

Finally, choosing

$$y = \frac{x^{1/4}}{(\log x)^{1/2}(\log(qN_E x))^{1/2}}$$

and $\theta = \frac{1}{4}$ in (34), we establish (8).

### 4.2. A non-CM refinement

Recall that in [1, Section 3.2] (see, particularly, [1, Equations (15)–(18)]), it has been shown that under GRH, one has

$$\pi_c(x,E,q,a) = \mathfrak{c}_E(q,a)\mathrm{Li}(x) + O(yx^{1/2}\log(qN_E x)) + O(\Sigma_2' + \Sigma_3\mathrm{Li}(x)), \tag{35}$$

where

$$\Sigma_2' := \sum_{y<m\leq\sqrt{x}+1} \pi_{E,m}(x,q,a) \ll x^{1/2}\log x + \frac{x^{3/2}}{y^2 q}H(q), \tag{36}$$

and

$$\Sigma_3 := \sum_{m>y} \frac{\mu(m)^2}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]} \ll \frac{\tau_2(q_2)}{y^3\phi(q)}M_E^3. \tag{37}$$

In this section, we shall refine the estimates for $\Sigma_2$ (for 'small' $q$) and $\Sigma_3$ (when $q$ and $M_E$ do not have many common prime factors) as follows.

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

First, by using Hasse's bound $|a_p| \le 2\sqrt{p} \le 2\sqrt{x}$ for $p \le x$, we have

$$\begin{aligned}\pi_{E,m}(x,q,a) &\le \#\{p \le x \mid p \nmid 2N_E, p \equiv a \,(\mathrm{mod}\, q), p \equiv 1 \,(\mathrm{mod}\, m), m^2 \mid |\tilde{E}(\mathbb{F}_p)|\} + 1 \\ &\le \sum_{|b| \le 2\sqrt{x}} \#\{p \le x \mid p \nmid 2N_E, m \mid p-1, m^2 \mid p+1-b, a_p = b\} + 1 \\ &\le \sum_{\substack{|b| \le 2\sqrt{x}, b \ne 2 \\ m \mid b-2}} \sum_{\substack{p \le x \\ m^2 \mid p+1-b}} 1 + \sum_{\substack{p \le x \\ m^2 \mid p-1}} 1 \\ &\ll \sum_{\substack{|b| \le 2\sqrt{x}, b \ne 2 \\ m \mid b-2}} \frac{x}{\phi(m^2)\log(9x/m^2)} + \frac{x}{m^2},\end{aligned}$$

where the last estimate follows from the Burn–Titchmarsh theorem, provided that $m \le \sqrt{x}+1$. (We shall note that this argument is inspired by the argument of Cojocaru and M.R. Murty [**5**, Section 4], and our new input is the use of the Burn–Titchmarsh theorem in the last estimate.) Note that $t\log(9x/t^2)$ is increasing for $0 < t \le \sqrt{x}+1$, as its derivative is $\log(9x/t^2) + t(-2/t) \ge (\log 8) - 2 > 0$, when $x$ is sufficiently large. Thus, we obtain

$$\begin{aligned}\sum_{y < m \le \sqrt{x}+1} \pi_{E,m}(x,q,a) &\ll \sum_{y < m \le \sqrt{x}+1} \frac{\sqrt{x}}{m} \frac{x}{m\phi(m)\log(9x/m^2)} + \frac{x}{y} \\ &\le \frac{x^{3/2}}{y\log(9x/y^2)} \sum_{y < m \le \sqrt{x}+1} \frac{1}{m\phi(m)} + \frac{x}{y}.\end{aligned}$$

By Abel's summation and the elementary estimate $\sum_{m \le t} \frac{1}{\phi(m)} = \gamma \log t + O(1)$ for some constant $\gamma > 0$, the last sum above is $\ll \frac{1}{y}$ (see also [**1**, Lemma 10]). Hence, we derive

$$\Sigma_2' \ll \frac{x^{3/2}}{y^2\log(3x/y^2)} + \frac{x}{y}. \tag{38}$$

To estimate the tail $\Sigma_3$, we shall closely follow the argument of [**1**, p. 1294]. For each $q$, we set $q_1 = \frac{q}{q_2}$ where $q_2$ denotes the largest divisor of $q$ that is coprime to $M_E$. As $\mu(m)^2 = 1$ if and only if $m$ is square-free, recalling that $M_E$ is square-free by its definition (6), we can write

$$\Sigma_3 = \sum_{\substack{m > y \\ m \text{ square-free}}} \frac{1}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q) : \mathbb{Q}]} = \sum_{\substack{de > y \\ d \mid M_E^\infty, (e, M_E) = 1}} \frac{1}{[\mathbb{Q}(E[de])\mathbb{Q}(\zeta_q) : \mathbb{Q}]},$$

which, by the decomposition $q = q_1q_2$, is

$$\begin{aligned}&\sum_{d \mid M_E} \frac{1}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_{q_1}) : \mathbb{Q}]} \sum_{\substack{e > y/d \\ (e, M_E) = 1}} \frac{1}{[\mathbb{Q}(E[e])\mathbb{Q}(\zeta_{q_2}) : \mathbb{Q}]} \\ &\le \sum_{d \mid M_E} \frac{1}{\phi([d, q_1])} \sum_{\substack{e > y/d \\ (e, M_E) = 1}} \frac{[\mathbb{Q}(E[e]) \cap \mathbb{Q}(\zeta_{q_2}) : \mathbb{Q}]}{[\mathbb{Q}(E[e]) : \mathbb{Q}][\mathbb{Q}(\zeta_{q_2}) : \mathbb{Q}]}.\end{aligned}$$

(Here, we used the fact that the $d$th cyclotomic field is contained in $\mathbb{Q}(E[d])$.) Moreover, it follows from the facts

$$[\mathbb{Q}(E[e]) : \mathbb{Q}] \gg e^3\phi(e) \text{ and } [\mathbb{Q}(E[e]) \cap \mathbb{Q}(\zeta_{q_2}) : \mathbb{Q}] = \phi((e, q_2))$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

(see [1, p. 1294]) that the last sum above is

$$\ll \frac{1}{\phi(q_2)}\sum_{k|q_2}\phi(k)\sum_{\substack{e>y/d\\(e,q_2)=k}}\frac{1}{e^3\phi(e)} \leq \frac{1}{\phi(q_2)}\sum_{k|q_2}\phi(k)\sum_{kr>y/d}\frac{1}{(kr)^3\phi(kr)}.$$

By the inequality $\phi(k)\phi(r)\leq\phi(kr)$ and the estimate $\sum_{r>X}\frac{1}{r^3\phi(r)}\ll X^{-3}$ (see [1, Lemma 10]), we see that the last quantity is

$$\leq \frac{1}{\phi(q_2)}\sum_{k|q_2}\frac{1}{k^3}\sum_{r>y/(dk)}\frac{1}{r^3\phi(r)} \ll \frac{1}{\phi(q_2)}\sum_{k|q_2}\frac{1}{k^3}\frac{(dk)^3}{y^3}.$$

Thus, recalling that $\phi([d,q_1])\phi((d,q_1))=\phi(d)\phi(q_1)$, we derive

$$\Sigma_3 \ll \frac{\tau_2(q_2)}{y^3}\sum_{d|M_E}\frac{1}{\phi([d,q_1])}\frac{1}{\phi(q_2)}d^3 = \frac{\tau_2(q_2)}{y^3\phi(q)}\sum_{d|M_E}\frac{\phi((d,q_1))d^3}{\phi(d)} = \frac{\tau_2(q_2)}{y^3\phi(q)}R_{E,q_1}, \tag{39}$$

where $R_{E,q_1}$ is defined as in (10). Thus, inserting (39) into the argument of [1, Section 3.2] (instead of using the bound given in (37)) yields the last assertion of the theorem.

Furthermore, by (35), (38) and (39), we can choose

$$y = \frac{x^{1/3}}{(\log x)^{1/3}(\log(qN_Ex))^{1/3}} \tag{40}$$

to deduce (9), which completes the proof.

## 5. PROOF OF THEOREM 1.5

Throughout this section, $p$ will denote a (rational) prime coprime to $N_E$. We start by observing $d_pe_p = |\tilde{E}(\mathbb{F}_p)| = p+1-a_p$ and writing

$$\pi_e(x,E,q,a) = \sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)}} e_p = \sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)}}\frac{p}{d_p} + \sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)}}\frac{1}{d_p}(1-a_p),$$

where by Hasse's bound, the last sum is

$$\ll \sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)}}(1+|a_p|) \ll \sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)}}\sqrt{p} \ll \frac{x^{3/2}}{q}.$$

For the main term, as done in [7] and [28], it follows from the identity

$$\frac{1}{m} = \sum_{de|m}\frac{\mu(d)}{e} \tag{41}$$

(see, e.g., the formula below [28, Equation (3.2)]) that

$$\sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)}}\frac{p}{d_p} = \sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)}} p\sum_{de|d_p}\frac{\mu(d)}{e} = \sum_{m\leq\sqrt{x}+1}\sum_{de|m}\frac{\mu(d)}{e}\sum_{\substack{p\leq x\\p\equiv a(\mathrm{mod}\,q)\\m|d_p}} p.$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

Therefore, we can consider the splitting

$$\pi_e(x,E,q,a) = \sum_{m\le y}\sum_{de|m}\frac{\mu(d)}{e}\sum_{\substack{p\le x\\ p\equiv a(\mathrm{mod}\,q)\\ m|d_p}} p + \sum_{y<m\le\sqrt{x}+1}\sum_{de|m}\frac{\mu(d)}{e}\sum_{\substack{p\le x\\ p\equiv a(\mathrm{mod}\,q)\\ m|d_p}} p + O\left(\frac{x^{3/2}}{q}\right), \tag{42}$$

where $y = y(x) \le \sqrt{x}+1$ is a parameter to be chosen later. Since

$$\left|\sum_{de|m}\frac{\mu(d)}{e}\right| \le \frac{1}{m} \le 1$$

(cf. [**28**, Equation (3.6)]), Lemma 2.4, together with (21), yields that the last triple sum in (42) is

$$\ll \sum_{y\le m\le\sqrt{x}+1} x\pi_{E,m}(x,q,a) \ll \sum_{y\le m\le\sqrt{x}+1}\frac{x^2}{m^2} \ll \frac{x^2}{y}.$$

Now, applying Abel's summation, we deduce

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv a(\mathrm{mod}\,q)\\ m|d_p}} p &= x\pi_{E,m}(x,q,a) - \int_2^x \pi_{E,m}(t,q,a)\,\mathrm{d}t\\ &= x\frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x) + x\mathcal{E}_{E,m}(x,q,a)\\ &\quad - \int_2^x \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(t)dt - \int_2^x \mathcal{E}_{E,m}(t,q,a)\,\mathrm{d}t,\end{aligned}$$

where $\mathcal{E}_{E,m}(x,q,a) = \pi_{E,m}(x,q,a) - \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x)$. Hence, by the expression

$$\mathrm{Li}(x^2) = x\mathrm{Li}(x) - \int_2^x \mathrm{Li}(t)dt + O(1),$$

we have

$$\sum_{\substack{p\le x\\ p\equiv a(\mathrm{mod}\,q)\\ m|d_p}} p = \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x^2) + O\left(x\max_{t\le x}|\mathcal{E}_{E,m}(t,q,a)| + 1\right). \tag{43}$$

Again, by (25), we obtain

$$\sum_{m\le(\log x)^A}\max_{t\le x}|\mathcal{E}_{E,m}(t,q,a)| \ll x(\log x)^A\exp(-c_{5,A,B}\sqrt{\log x}). \tag{44}$$

Therefore, by (42), (43) and (44), choosing $y = (\log x)^A$, we conclude that

$$\begin{aligned}\pi_e(x,E,q,a) &= \sum_{1\le m\le(\log x)^A}\sum_{de|m}\frac{\mu(d)}{e}\frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x^2)\\ &\quad + O\left(x^2(\log x)^A\exp(-c_{5,A,B}\sqrt{\log x}) + \frac{x^2}{(\log x)^A} + \frac{x^{3/2}}{q}\right).\end{aligned}$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

Note that

$$\sum_{m>y}\sum_{d e|m}\frac{\mu(d)}{e}\frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x^2)\ll\sum_{m>y}\frac{1}{\phi(m)^2}\frac{x^2}{\log x}\ll\frac{1}{y}\frac{x^2}{\log x}, \tag{45}$$

where the last estimate follows from (32). Hence, we finally arrive at

$$\pi_e(x,E,q,a)=\mathfrak{e}_E(q,a)\mathrm{Li}(x^2)+O_{A,B}\left(\frac{x^2}{(\log x)^A}\right)$$

whenever $qN_E\le(\log x)^B$.

## 6. CONDITIONAL ESTIMATES FOR $\pi_e(x,E,q,a)$

Throughout this section, we shall assume GRH and apply (27). More precisely, by (27) and (43), under GRH, we have

$$\sum_{\substack{p\le x\\ p\equiv a(\mathrm{mod}\,q)\\ m|d_p}}p=\frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x^2)+O\left(x^{3/2}\log(mqN_E)\right). \tag{46}$$

Also, bounding each $p$ trivially by $x$ and using Lemma 2.4, we have

$$\sum_{y\le m\le\sqrt{x}+1}\sum_{d e|m}\frac{\mu(d)}{e}\sum_{\substack{p\le x\\ p\equiv a(\mathrm{mod}\,q)\\ m|d_p}}p\ll x\sum_{y<m\le\sqrt{x}+1}\pi_{E,m}(x,q,a). \tag{47}$$

### 6.1. Elliptic curves with CM

We begin by noting that if $E$ has CM, (22) and (33) tell us that the right of (47) is $\ll x\mathcal{E}_1(x)$ with

$$\mathcal{E}_1(x):=\min\left\{\left(\frac{\sqrt{x}}{q}+\frac{\sqrt{x}\log x}{q^2}+\frac{x}{yq^3}\right)G_D(a,q),\frac{x}{y\log x}+x^\theta\log N_E+\frac{x}{x^\theta}\right\}.$$

Putting (42), (45) and (46), and this bound together then yields

$$\begin{aligned}\pi_e(x,E,q,a)=&\sum_{m=1}^{\infty}\sum_{d e|m}\frac{\mu(d)}{e}\frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x^2)+O\left(yx^{3/2}\log(qN_Ex)\right)\\&+O\left(x\mathcal{E}_1(x)+\frac{x^2}{y\log x}+\frac{x^{3/2}}{q}\right).\end{aligned} \tag{48}$$

Finally, as done in [**1**, p. 1301], applying [**9**, Lemma 2.4] to find $y\in[2q,x^{1/2}]$ to balance the error terms in (48), we deduce (13).

### 6.2. Non-CM elliptic curves

Assume that $E$ is non-CM. As discussed in Section 4.2, by (36) and (38), the last sum in (47) is

$$\ll\mathcal{E}_2(x):=\min\left\{x^{1/2}\log x+\frac{x^{3/2}}{y^2q}H(q),\frac{x^{3/2}}{y^2\log(3x/y^2)}+\frac{x}{y}\right\}$$

provided that $2q\le y\le\sqrt{x}$, and thus the triple sum on the left of (47) is $\ll x\mathcal{E}_2(x)$.

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

By (41), we have

$$\sum_{m>y}\sum_{de|m}\frac{\mu(d)}{e}\frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\ll\sum_{m>y}\frac{1}{m}\frac{1}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}. \tag{49}$$

From an argument analogous to the one leading to (39), it follows that the right of (49) is

$$\ll\sum_{d|M_E^\infty}\frac{1}{d[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_{q_1}):\mathbb{Q}]}\frac{1}{\phi(q_2)}\sum_{k|q_2}\frac{1}{k^3}\frac{(dk)^3}{y^3}.$$

Unfortunately, if we used the bound $[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_{q_1}):\mathbb{Q}]\geq\phi([d,q_1])$ as before, the above sum over $d$ would not converge. To resolve this issue, we recall that by Serre's open image theorem, Freiberg and Kurlberg [7, Proposition 3.2] showed that there exists a constant $B_E$, depending only on $E$, such that $B_E\cdot[\mathbb{Q}(E[m]):\mathbb{Q}]\geq|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})|\gg m^3\phi(m)$, for any $m\in\mathbb{N}$, whenever $E$ is non-CM. From which, we derive the upper bound

$$\ll\sum_{d|M_E^\infty}\frac{B_E}{d^4\phi(d)}\frac{1}{\phi(q_2)}\sum_{k|q_2}\frac{1}{k^3}\frac{(dk)^3}{y^3}=\frac{\tau_2(q_2)}{y^3\phi(q_2)}\sum_{d|M_E^\infty}\frac{B_E}{d\phi(d)}.$$

Thus, by (42), (46) and the above discussion, we obtain

$$\begin{aligned}\pi_e(x,E,q,a)=&\sum_{m=1}^{\infty}\sum_{de|m}\frac{\mu(d)}{e}\frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x^2)+O\left(yx^{3/2}\log(qN_Ex)\right)\\&+O\left(x\mathcal{E}_2(x)+\frac{\tau_2(q_2)}{\phi(q_2)}\sum_{d|M_E^\infty}\frac{B_E}{d\phi(d)}\frac{x^2}{y^3\log x}+\frac{x^{3/2}}{q}\right).\end{aligned}$$

Hence, balancing the errors as in [1, Section 3.2.3] gives the desired estimate (15).

Finally, to derive (14), we instead use the bound $[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]\geq\phi(m)$ in (49) so that the resulting error is $\ll y^{-1}$. Consequently, the last big-O term above can be replaced by $O(x\mathcal{E}_2(x)+\frac{x^2}{y\log x}+\frac{x^{3/2}}{q})$, and choosing $y$ as in (40) yields (14).

## 7. WHEN THE LANDAU-SIEGEL ZERO IS NOT TOO CLOSE TO 1

In this section, we shall assume (16). Suppose that there is an exceptional Dirichlet character $\chi_1$ modulo $Q_1$ such that $L(s,\chi_1)$ admits a Landau–Siegel zero $\beta_1$. Arguing classically, by the mean value theorem, we have

$$1-\beta_1=\frac{L(1,\chi_1)}{L'(\sigma_1,\chi_1)}$$

for some $\sigma_1\in(\beta_1,1)$. This, combined with (16) and the well-known estimate $L'(\sigma_1,\chi_1)=O((\log Q_1)^2)$, yields

$$1-\beta_1>\frac{c_6}{(\log Q_1)^{S+2}}$$

for some $c_6>0$. From this lower bound, one has

$$x^{\beta_1}\ll x\exp\left(-c_6(\log x)(\log Q_1)^{-S-2}\right)\ll x\exp(-c_6\sqrt{\log x}) \tag{50}$$

whenever $(\log Q_1)^{S+2}\leq\sqrt{\log x}$ or, equivalently, $Q_1\leq\exp\left((\log x)^{1/(2S+4)}\right)$, which leads to the following improvement of the Siegel–Walfisz theorem:

$$\pi(x,q,a)=\frac{1}{\phi(q)}\mathrm{Li}(x)+O\left(x\exp(-c_6'\sqrt{\log x})\right)$$

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

uniformly in $q \leq \exp\left((\log x)^{1/(2S+4)}\right)$ for some abosulte $c_6' \in (0, c_6)$ (cf. [6, Sections 21–22].)

Now, in the same notation of Section 2.2, for any CM elliptic curve $E$ of conductor $N_E$, assuming that $\log m \leq \frac{1}{2\kappa}(\log x)^{1/(2S+4)}$ and $\log(qN_E) \leq \frac{1}{2\kappa}(\log x)^{1/(2S+4)}$, by (24), we know that

$$\log Q_1 \leq \kappa \log(mqN_E) \leq (\log x)^{1/(2S+4)}.$$

Therefore, by (23) and (50), we arrive at

$$\pi_C(x) = \frac{|C|}{|G|}\mathrm{Li}(x) + O\left(|C|^{\frac{1}{2}} x \exp(-c_2'\sqrt{\log x}) + x\exp(-c_6\sqrt{\log x})\right).$$

Hence, under the assumption of (16), the estimate (25) can be improved as

$$\pi_{E,m}(x,q,a) = \frac{\gamma_{E,m}(q,a)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x) + O\left(x\exp(-c_7\sqrt{\log x})\right), \tag{51}$$

uniformly in $\log m \leq \frac{1}{2\kappa}(\log x)^{1/(2S+4)}$ and $\log(qN_E) \leq \frac{1}{2\kappa}(\log x)^{1/(2S+4)}$, for some $c_7 > 0$.

Thus, gathering (28), (30) and (51) (instead of (29)), we get

$$\pi_c(x,E,q,a) = \sum_{m=1}^{\infty} \frac{\gamma_{E,m}(q,a)\mu(m)}{[\mathbb{Q}(E[m])\mathbb{Q}(\zeta_q):\mathbb{Q}]}\mathrm{Li}(x) + O\left(yx\exp(-c_7\sqrt{\log x}) + \frac{x}{y}\right)$$

whenever $\log(qN_E) \leq \frac{1}{2\kappa}(\log x)^{1/(2S+4)}$. This, together with the choice

$$y = \exp\left(\min\left\{\frac{1}{2\kappa}, \frac{c_7}{2}\right\}(\log x)^{1/(2S+4)}\right),$$

then yields the first claimed estimate of Theorem 1.7. Finally, we conclude this section by noting that the last estimate of Theorem 1.7 follows similarly while using (51) (instead of (29)) in the argument starting from (43).

## ACKNOWLEDGEMENTS

The author thanks Professors Amir Akbary, Wen-Ching Winnie Li and Ram Murty for their encouragement as well as helpful comments and suggestions. He is also grateful to the referee for the careful reading and insightful comments.

## FUNDING

This research was partially supported by grant 111-2115-M-110-005-MY3 from the National Science and Technology Council (Taiwan).

## REFERENCES

1. Y. Akbal and A.M. Güloğlu, Cyclicity of elliptic curves modulo primes in arithmetic progressions, *Canad. J. Math.* **74** no. 5 (2022), 1277–1309. 10.4153/S0008414X21000237
2. A. Akbary and V.K. Murty, An analogue of the Siegel-Walfisz theorem for the cyclicity of CM elliptic curves mod p, *Indian J. Pure Appl. Math.* **41** no. 1 (2010), 25–37. 10.1007/s13226-010-0002-4
3. A.C. Cojocaru, Cyclicity of CM elliptic curves mod $p$, *Trans. Amer. Math. Soc.* **355** no. 7 (2003), 2651–2662. 10.1090/S0002-9947-03-03283-5
4. A.C. Cojocaru and E., Kani, On the surjectivity of the Galois representations associated to non-CM elliptic curve; with an appendix by E. Kani, *Canad. Math. Bull.* **48** no. 1 (2005), 16–31. 10.4153/CMB-2005-002-x
5. A.C. Cojocaru and M.R. Murty, Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem, *Math. Ann.* **330** no. 3 (2004), 601–625. 10.1007/s00208-004-0562-x

Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024

6. H. Davenport, *Multiplicative Number Theory*, **vol 74**, 3rd edn, revised and with a preface by Hugh L. Montgomery, Graduate Texts in Mathematics, Springer, Germany, 2000.
7. T. Freiberg and P. Kurlberg, On the average exponent of elliptic curves modulo p, *Int. Math. Res. Not.* **2014** no. 8 (2014), 2265–2293. 10.1093/imrn/rns280
8. D. Goldfeld, An asymptotic formula relating the Siegel zero and the class number of quadratic fields, *Annali della Scuola Normale Superiore di Pisa—Classe di Scienze, Serie 4*, **2** (1975), 611–615.
9. S.W. Graham and G. Van der Kolesnik, *Corput's Method of Exponential Sums*, London Mathematical Society Lecture Note Series 126, Cambridge University Press, United Kingdom, 1991.
10. R. Gupta and M.R. Murty, Cyclicity and generation of points modp on elliptic curves, *Invent. Math.* **101** no. 1 (1990), 225–235. 10.1007/BF01231502
11. J. Hinz and M. Lodemann, On Siegel zeros of Hecke-Landau zeta-functions, *Mh. Math.* **118** no. 3–4 (1994), 231–248. 10.1007/BF01301691
12. M.N. Huxley, The large sieve inequality for algebraic number fields III. Zero-density results, *J. Lond. Math. Soc.* **2** no. 2 (1971), 233–240. 10.1112/jlms/s2-3.2.233
13. N. Jones and S.M. Lee, *On the acyclicity of reductions of elliptic curves modulo primes in arithmetic progressions*, preprint, https://arxiv.org/abs/2206.00872.
14. S. Kim, Average behaviors of invariant factors in Mordell-Weil groups of CM elliptic curves modulo *p*, *Finite Fields Appl.* **30** (2014), 178–190.
15. J.C. Lagarias, H.L. Montgomery and A.M. Odlyzko, A bound for the least prime ideal in the Chebotarev density theorem, *Invent. Math.* **54** no. 3 (1979), 271–296. 10.1007/BF01390234
16. J.C. Lagarias and A.M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields: *L*-functions and Galois Properties (Durham, 1975), Academic Press, United States of America, 1977, 409–464.
17. S. Lang and H. Trotter, Primitive points on elliptic curves, *Bull. Am. Math. Soc.* **83** no. 2 (1977), 289–292. 10.1090/S0002-9904-1977-14310-3
18. D. Lombardo, Bounds for Serre's open image theorem for elliptic curves over number fields, *Algebra Number Theory* **9** no. 10 (2015), 2347–2395. 10.2140/ant.2015.9.2347
19. J. Mayle and T. Wang, *On the effective version of Serre's open image theorem*, preprint, https://arxiv.org/abs/2109.08656.
20. M.R. Murty, On Artin's conjecture, *J. Number Theory* **16** no. 2 (1983), 147–168. 10.1016/0022-314X(83)90039-2
21. M.R. Murty, An analogue of Artin's conjecture for abelian extensions, *J. Number Theory* **18** no. 3 (1984), 241–248. 10.1016/0022-314X(84)90059-3
22. M.R. Murty, V.K. Murty and N., Saradha, Modular forms and the Chebotarev density theorem, *Am. J. Math.* **110** no. 2 (1988), 253–281. 10.2307/2374502
23. V.K. Murty, Modular forms and the Chebotarev density theorem II, *Analytic Number Theory (London Mathematical Society Lecture Note Series)*, Y. Motohashi (ed.), Cambridge University Press, 1997, 287–308.
24. J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
25. J.-P. Serre, *Résumé des cours de l'année scolaire 1977-1978*, Annuaire du Collège de France, 1978, 67–70, in Collected Papers, volume III, Springer, Germany, 1985.
26. R.J. Wilson, The large sieve in algebraic number fields, *Mathematika* **16** no. 2 (1969), 189—204. 10.1112/S0025579300008160
27. P.-J. Wong, Langlands reciprocity for certain Galois extensions, *J. Number Theory* **178** (2017), 126–145. 10.1016/j.jnt.2017.02.003
28. J. Wu, The average exponent of elliptic curves modulo p, *J. Number Theory* **135** (2014), 28–35. 10.1016/j.jnt.2013.08.009
29. Y. Zhang, *Discrete mean estimates and the Landau-Siegel zero*, preprint, https://arxiv.org/abs/2211.02515.


Downloaded from https://academic.oup.com/qjmath/article/75/2/757/7681831 by guest on 01 July 2024