PSEUDOPRIME REDUCTIONS OF ELLIPTIC CURVES

C. DAVID & J. WU

Abstract. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication, and for each prime p of good reduction, let $n_E(p) = |E(\mathbb{F}_p)|$. For any integer b, we are studying in this paper elliptic pseudoprimes to the base b. More precisely, let $Q_{E,b}(x)$ be the number of primes $p \leqslant x$ such that $b^{n_E(p)} \equiv b \,(\mathrm{mod}\, n_E(p))$, and $\pi_{E,b}^{\mathrm{pseu}}(x)$ be the number of *compositive* $n_E(p)$ such that $b^{n_E(p)} \equiv b \,(\mathrm{mod}\, n_E(p))$ (also called elliptic curve pseudoprimes). Motivated by cryptography applications, we address in this paper the problem of finding upper bounds for $Q_{E,b}(x)$ and $\pi_{E,b}^{\mathrm{pseu}}(x)$, generalising some of the literature for the classical pseudoprimes [6, 17] to this new setting.

1. Introduction

The study of the structure and size of the group of points of elliptic curves over finite fields has received much attention since Koblitz and Miller independently proposed in 1985 elliptic curve cryptography, an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Those cryptosystems guarantee, in general, a high level of security with less cost in the size of the keys, whenever the order of the group has a big prime divisor.

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N_E and without complex multiplication (CM), and denote by $E(\mathbb{F}_p)$ the reduction of E modulo p. Writing $n_E(p) := |E(\mathbb{F}_p)|$, it is an interesting problem to study the asymptotic behavior of

$$\pi_E^{\mathrm{twin}}(x) := \big|\big\{p \leqslant x \,:\, n_E(p) \text{ is prime}\big\}\big|. \tag{1.1}$$

Here and in the sequel, the letters p, q and ℓ denote prime numbers. Koblitz [11] conjectured that as $x \to \infty$,

$$\pi_E^{\mathrm{twin}}(x) \sim \frac{C_E^{\mathrm{twin}} x}{(\log x)^2}, \tag{1.2}$$

with an explicit constant C_E^{twin} depending only on E (see [5, (2.5)] for its precise definition). It is easy to see that if $C_E^{\mathrm{twin}} = 0$, then $\pi_E^{\mathrm{twin}}(x) \ll_E 1$ for all $x \geqslant 1$. The asymptotic formula (1.2) can be regarded as the analogue of the twin prime conjecture for elliptic curves. As in the classical case, Koblitz's conjecture is still open, but was shown to be true on average over all elliptic curves [1]. One can also apply sieve methods to get unconditional or conditional upper bounds for $\pi_E^{\mathrm{twin}}(x)$. The best unconditional upper bound is due to Zywina [22, Theorem 1.3], and the

Date: December 14, 2010.

2000 *Mathematics Subject Classification.* 11N36, 14H52.

Key words and phrases. Rosser-Iwaniec's sieve, group order of elliptic curves over finite fields, pseudoprimes.

best bound under the Generalised Riemann Hypothesis (GRH) is due to David & Wu [5, Theorem 2]. For E an elliptic curve over $\mathbb{Q}$ without CM, and for any $\varepsilon > 0$, those bounds are

$$\pi_E^{\mathrm{twin}}(x) \leqslant \begin{cases} (24C_E^{\mathrm{twin}} + \varepsilon)\dfrac{x}{(\log x)\log_2 x} & \text{(unconditionally)}, \\ (10C_E^{\mathrm{twin}} + \varepsilon)\dfrac{x}{(\log x)^2} & \text{(under the GRH)}, \end{cases} \tag{1.3}$$

where $\log_k$ denotes the k-fold logarithm function.

Let $b \geqslant 2$ be an integer. We say that a composite positive integer n is a pseudoprime to base b if the congruence

$$b^n \equiv b \,(\mathrm{mod}\, n) \tag{1.4}$$

holds. In practice, primality testing algorithms are not fast when one wants to test many numbers in a short amount of time, and pseudoprime testing can provide a quick pre-selection procedure to get rid of most of the pretenders. The distribution of pseudoprimes was studied by many authors, including [6, 17]. Motivated by applications in cryptography, the question of the distribution of pseudoprimes in certain sequences of positive integers has received some interest (see [3, 7, 14, 15, 18]). In particular Cojocaru, Luca & Shparlinski [3] have investigated distribution of pseudoprimes in $\{n_E(p)\}_{p\,\mathrm{primes}}$. Define

$$Q_{E,b}(x) := \big|\big\{p \leqslant x \,:\, b^{n_E(p)} \equiv b \,(\mathrm{mod}\, n_E(p))\big\}\big|.$$

According to Fermat's little theorem, if $n_E(p)$ is a prime such that $n_E(p) \nmid b$, then (1.4) holds with $n = n_E(p)$. Thus

$$\pi_E^{\mathrm{twin}}(x) \leqslant Q_{E,b}(x) \tag{1.5}$$

for all $x \geqslant 2$. Cojocaru, Luca & Shparlinski [3, Theorems 1 and 2] proved that for any fixed base $b \geqslant 2$ and elliptic curve E without CM, the estimates

$$Q_{E,b}(x) \ll_{E,b} \begin{cases} \dfrac{x(\log_3 x)^2}{(\log x)\log_2 x} & \text{(unconditionally)} \\ \dfrac{x(\log_2 x)^2}{(\log x)^2} & \text{(under the GRH)} \end{cases} \tag{1.6}$$

hold for all $x \geqslant 10$, where the implied constant depends on E and b. *

The first aim of this paper is to improve (1.6).

*We noticed that there are two inaccuracies in Cojocaru, Luca & Shparlinski's proof of (1.6): With the notation of [3], we have $t_b(\ell) \mid (n_E(p) - 1)$ instead of $t_b(\ell) \mid n_E(p)$ (see [3, page 519]). Thus the inequality (see [3, page 520])

$$\#\mathcal{T} \leqslant \sum_{y < \ell \leqslant z} \Pi(x; \ell\rho(t_b(\ell)))$$

does not hold. Secondly the statements of Lemmas 3, 4, 6 and 7 of [3] are not true when $(m, M_E) \neq 1$ (see Section 2 for the definition of M_E). Then, the proofs of Lemma 9 and 10 hold only for $(m, M_E) = 1$. This is not sufficient for the proof bounding $\#\mathcal{T}$ since $t_b(\ell)$ is not necessarily coprime with M_E.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$ without CM and $b \geqslant 2$ be an integer. For any $\varepsilon > 0$, we have*

$$Q_{E,b}(x) \leqslant \begin{cases} (48\mathrm{e}^{\gamma} + \varepsilon)\dfrac{x \log_3 x}{(\log x)\log_2 x} & (\textit{unconditionally}) \\ (28\mathrm{e}^{\gamma} + \varepsilon)\dfrac{x \log_2 x}{(\log x)^2} & (\textit{under the GRH}) \end{cases} \tag{1.7}$$

for all $x \geqslant x_0(E, b, \varepsilon)$, where γ is the Euler constant.

Denoting by $\pi(x)$ the number of primes not exceeding x, and by $\pi_b^{\mathrm{pseu}}(x)$ the number of pseudoprimes to base b not exceeding x, then it is known that (see [6, 17])

$$\pi_b^{\mathrm{pseu}}(x) = o(\pi(x)) \tag{1.8}$$

as $x \to \infty$. Precisely Pomerance [17, Theorem 2] proved that [†]

$$\pi_b^{\mathrm{pseu}}(x) \leqslant \frac{x}{\sqrt{L(x)}} \tag{1.9}$$

for $x \geqslant x_0(b)$, where

$$L(x) := \mathrm{e}^{(\log x)(\log_3 x)/\log_2 x}. \tag{1.10}$$

As analogue of $\pi_b^{\mathrm{pseu}}(x)$ for elliptic curve, we introduce

$$\pi_{E,b}^{\mathrm{pseu}}(x) := \big|\big\{p \leqslant x \,:\, n_E(p) \text{ is pseudoprime to base } b\big\}\big|.$$

Clearly

$$Q_{E,b}(x) = \pi_E^{\mathrm{twin}}(x) + \pi_{E,b}^{\mathrm{pseu}}(x).$$

In view of (1.8), it seems reasonable to conjecture

$$\pi_{E,b}^{\mathrm{pseu}}(x) = o\big(\pi_E^{\mathrm{twin}}(x)\big) \tag{1.11}$$

as $x \to \infty$.

In order to establish analogue of (1.9) for $\pi_{E,b}^{\mathrm{pseu}}(x)$, we need a supplementary hypothesis.

Hypothesis 1.2. *Let E be an elliptic curve over $\mathbb{Q}$. There is a positive constant δ such that*

$$M_E(n) := \#\{p \,:\, n_E(p) = n\} \ll_E n^{\delta} \tag{1.12}$$

holds uniformly for $n \geqslant 1$, where the implied constant can depend on the elliptic curve E.

By the Hasse bound $|p + 1 - n_E(p)| \leqslant 2\sqrt{p}$, it is easy to see that

$$n_E(p)/16 \leqslant p \leqslant 16 n_E(p) \tag{1.13}$$

for all p. Thus the relation $n_E(p) = n$ and the Hasse bound imply that $|p - n| \leqslant 9\sqrt{n}$. Therefore (1.12) holds trivially with $\delta = \frac{1}{2}$ and an absolute implicit constant. It is conjectured that (1.12) should hold for any $\delta > 0$ (see [12, Question 4.11]). Kowalski

[†]In [17], the definition of pseudoprime to base b is slightly stronger: $b^{n-1} \equiv 1 \pmod n$ in place of $b^n \equiv b \pmod n$. It is easy to adapt Pomerance's proof of [17, Theorem 2] to obtain (1.9), as we do in this paper for the context of elliptic curves pseudoprimes. See Section 5 for more details.

proved that this conjecture is true for elliptic curves with CM [12, Proposition 5.3] and on average for elliptic curves without CM [12, Lemma 4.10].

The next theorem shows that we can obtain a better conditional upper bound for $\pi_{E,b}^{\mathrm{pseu}}(x)$ than $\pi_E^{\mathrm{twin}}(x)$, which can be regarded as analogue of (1.9) for elliptic curves without CM.

Theorem 1.3. *Let E be an elliptic curve over $\mathbb{Q}$ without CM and $b \geqslant 2$ be an integer. If we assume the GRH and Hypothesis 1.2 with $\delta < \frac{1}{24}$, we have*

$$\pi_{E,b}^{\mathrm{pseu}}(x) \leqslant \frac{x}{L(x)^{1/38}} \tag{1.14}$$

for all $x \geqslant x_0(E, b, \delta)$.

In view of Koblitz's conjecture (1.2), the result of Theorem 1.3 then encourages our belief in Conjecture (1.11).

By combining (1.14) and the second part of (1.3), we immediately get the following result.

Corollary 1.4. *Let E be an elliptic curve over $\mathbb{Q}$ without CM and $b \geqslant 2$ be an integer. If we assume the GRH and hypothesis 1.2 with $\delta < \frac{1}{24}$, for any $\varepsilon > 0$ we have*

$$Q_{E,b}(x) \leqslant (10C_E^{\mathrm{twin}} + \varepsilon)\frac{x}{(\log x)^2} \tag{1.15}$$

for all $x \geqslant x_0(E, b, \delta, \varepsilon)$.

We can also consider the same problem for elliptic curves with CM. In this case, we easily obtain an unconditional result by using the bound (1.9) of Pomerance for pseudoprimes and a result of Kowalski [12] about the second moment of $M_E(n)$ for elliptic curves with CM.

Theorem 1.5. *Let E be an elliptic curve over $\mathbb{Q}$ with CM and $b \geqslant 2$ be an integer. Then we have*

$$\pi_{E,b}^{\mathrm{pseu}}(x) \leqslant \frac{x}{L(x)^{1/4}} \tag{1.16}$$

for all $x \geqslant x_0(E, b)$.

It seems be interesting to prove that

$$\pi_{E,b}^{\mathrm{pseu}}(x) \to \infty, \quad \text{as } x \to \infty. \tag{1.17}$$

We hope to come back to this question in the future.

Acknowledgments. This first author was supported by the Natural Sciences and Engineering Research Council of Canada (Discovery Grant 155635-2008) and by a grant to the Institute for Advanced Study from the Minerva Research Foundation during the academic year 2009-2010. The second author wishes to thank the Centre de Recherches Mathématiques (CRM) in Montréal for hospitality and support during the preparation of this article.

2. Chebotarev density theorem

In order to prove Theorems 1.1 and 1.3, we need to know some information on the distribution of the sequence $\{n_E(p)\}_{p\,\text{primes}}$ in arithmetic progressions. The aim of this section is to give such results with the help of the Chebotarev density theorem. Our main result of this section is Theorem 2.3 below.

We conserve all notation of [5, Sections 2 and 3]. In particular, for an elliptic curve E without complex multiplication defined over the rationals, let $E[n]$ be the group of n-torsion points of E, and let L_n be the field extension obtained from $\mathbb{Q}$ by adding the coordinates of the n-torsion points of E. This is a Galois extension of $\mathbb{Q}$, and we denote $G(n) := \mathrm{Gal}(L_n/\mathbb{Q})$. Since $E[n](\bar{\mathbb{Q}}) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, choosing a basis for the n-torsion and looking at the action of the Galois automorphisms on the n-torsion, we get an injective homomorphism

$$\rho_n : G(n) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

If $p \nmid nN_E$, then p is unramified in $L_n/\mathbb{Q}$. Let p be an unramified prime, and let σ_p be the Artin symbol of $L_n/\mathbb{Q}$ at the prime p. For such a prime p, $\rho_n(\sigma_p)$ is a conjugacy class of matrices of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Since the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ of E over $\mathbb{F}_p$ satisfies the polynomial $x^2 - a_E(p)x + p$, it is not difficult to see that

$$\mathrm{tr}(\rho_n(\sigma_p)) \equiv a_E(p) \,(\mathrm{mod}\, n) \qquad \text{and} \qquad \det(\rho_n(\sigma_p)) \equiv p \,(\mathrm{mod}\, n).$$

To study the sequence $\{n_E(p)\}_{p\,\text{primes}}$, we will use the Chebotarev Density Theorem to count the number of primes p such that

$$n_E(p) = p + 1 - a_E(p) \equiv \det(\rho_n(\sigma_p)) + 1 - \mathrm{tr}(\rho_n(\sigma_p)) \equiv r \,(\mathrm{mod}\, n)$$

for integers r, n with $n \geqslant 2$. We then define

$$C_r(n) = \{g \in G(n) \,:\, \det(g) + 1 - \mathrm{tr}(g) \equiv r \,(\mathrm{mod}\, n)\}\,.$$

Then, the $C_r(n)$ are unions of conjugacy classes in $G(n)$. We also denote $C(n) := C_0(n)$. For any prime ℓ such that $(\ell, M_E) = 1$, $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and it is easy to compute that

$$|C_r(\ell)| = \begin{cases} \ell(\ell^2 - 2) & \text{for } r \equiv 0 \,(\mathrm{mod}\, \ell) \\ \ell(\ell^2 - \ell - 1) & \text{for } r \equiv 1 \,(\mathrm{mod}\, \ell) \\ \ell(\ell^2 - \ell - 2) & \text{for } r \not\equiv 0, 1 \,(\mathrm{mod}\, \ell) \end{cases} \tag{2.1}$$

and then

$$\frac{|C_r(\ell)|}{|G(\ell)|} = \begin{cases} \dfrac{\ell^2 - 2}{(\ell-1)^2(\ell+1)} & \text{for } r \equiv 0 \,(\mathrm{mod}\, \ell) \\ \dfrac{\ell^2 - \ell - 1}{(\ell-1)^2(\ell+1)} & \text{for } r \equiv 1 \,(\mathrm{mod}\, \ell) \\ \dfrac{\ell^2 - \ell - 2}{(\ell-1)^2(\ell+1)} & \text{for } r \not\equiv 0, 1 \,(\mathrm{mod}\, \ell). \end{cases} \tag{2.2}$$

It was shown by Serre [19] that the Galois groups $G(n) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ are large, and that there exists a positive integer M_E depending only on the elliptic curve E such that

(2.3) If $(n, M_E) = 1$, then $G(n) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$;

(2.4) If $(n, M_E) = (n, m) = 1$, then $G(mn) \simeq G(m) \times G(n)$;

(2.5) If $M_E \mid m$, then $G(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the full inverse image of $G(M_E) \subseteq \mathrm{GL}_2(\mathbb{Z}/M_E\mathbb{Z})$ under the projection map.

Let

$$\pi_{C_r(n)}(x, L_n/\mathbb{Q}) := |\{p \leqslant x : p \nmid nN_E \text{ and } \rho_n(\sigma_p) \in C_r(n)\}|.$$

The following proposition (with a better error term) was proved in [5, Theorem 3.9] for the conjugacy class $C(n) = C_0(n) \subseteq G(n)$ when n is squarefree, and can be easily generalised to general n and r.

Proposition 2.1. *Let E be an elliptic curve over $\mathbb{Q}$ without CM. Let $r \geqslant 0$ be an integer, and let $n = dm$ be any positive integer with $(d, M_E) = 1$ and $m \mid {M_E}^{\infty}$.* [‡]

(i) *Then,*

$$\pi_{C_r(n)}(x, L_n/\mathbb{Q}) = \frac{|C_r(m)|}{|G(m)|}\Big(\prod_{\ell^k \| d} \frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|}\Big)\mathrm{Li}(x) + O_E\Big(x \exp\Big\{-An^{-2}\sqrt{\log x}\Big\}\Big)$$

uniformly for $\log x \gg n^{12} \log n$, where the implied constants depend only on the elliptic curve E and A is a positive absolute constant.

(ii) *Assuming the GRH for the Dedekind zeta functions of the number fields $L_n/\mathbb{Q}$, we have*

$$\pi_{C_r(n)}(x, L_n/\mathbb{Q}) = \frac{|C_r(m)|}{|G(m)|}\Big(\prod_{\ell^k \| d} \frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|}\Big)\mathrm{Li}(x) + O_E\left(n^3 x^{1/2} \log(nx)\right).$$

Proof. To prove (i) and (ii), one applies the effective Cheboratev Density Theorem due to Lagarias and Odlyzko [13] and slightly improved by Serre in [20], as stated in [5, Theorem 3.1] with the appropriate bounds for the discriminants of number fields [20, Proposition 6], and the bound of Stark [21] for the exceptional zero of Dedekind L-functions for (i). We refer the reader to [5] for more details. □

Remark 1. There are many cases where we can improve the error term in Proposition 2.1 (ii) by applying a strategy first used in [20] and [16] to reduce to the case of an extension where Artin's conjecture holds. The error term then becomes

$$O_E\big(n^{3/2} x^{1/2} \log(nx)\big).$$

This can be done if $r = 0$ (as in [5, Theorem 3.9]), or if $(n, M_E) = 1$ for any r. To apply the strategy of [20] and [16] and obtain this improved error term, one needs to insure that $C_r(n) \cap B(n) \neq \emptyset$, where $B(n)$ is the Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For example, this is the case if E is a Serre curve, and most elliptic curves are Serre curves as it was shown by Jones [10].

[‡]The notation $d \mid n^{\infty}$ means that $p \mid d \Rightarrow p \mid n$ and the notation $p^k \| n$ means that $p^k \mid n$ and $p^{k+1} \nmid n$.

We now need upper and lower bounds on the size of the main term of Proposition 2.1, which are computed in the next lemma.

Lemma 2.2. *Let E be an elliptic curve over $\mathbb{Q}$ without CM. For all primes $\ell \nmid M_E$ and integers $k \geqslant 1$, we have the bounds*

$$\frac{1}{\varphi(\ell^k)} \cdot \frac{\ell-2}{\ell-1} \leqslant \frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|} \leqslant \frac{1}{\varphi(\ell^k)} \tag{2.6}$$

when $r \not\equiv 0 \pmod{\ell}$, and the bounds

$$\frac{1}{\varphi(\ell^k)} \cdot \frac{\ell-2}{\ell-1} \leqslant \frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|} \leqslant \frac{1}{\varphi(\ell^k)}\left(1 + \frac{1}{(\ell^3-1)(\ell^2-1)}\right) \tag{2.7}$$

when $r \equiv 0 \pmod{\ell}$.

Furthermore, for $m \mid {M_E}^\infty$ such that $|C_r(m)| \neq 0$, we have that

$$\frac{1}{\varphi(m)} \ll_E \frac{|C_r(m)|}{|G(m)|} \ll_E \frac{1}{\varphi(m)} \tag{2.8}$$

with constants depending only on the elliptic curve E. In particular, the upper bound in (2.8) holds without the hypothesis $|C_r(m)| \neq 0$.

Proof. Fix $\ell \nmid M_E$ and $k \geqslant 1$. To count the number of elements in $C_r(\ell^k)$, we count the matrices $\tilde{g} \in \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ which are the inverse images of a matrix $g \in C_r(\ell)$ under the projection map from $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and which satisfy

$$\det(\tilde{g}) + 1 - \mathrm{tr}\,(\tilde{g}) \equiv r \pmod{\ell^k}.$$

Let

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \tilde{g} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}.$$

If $b \not\equiv 0 \pmod{\ell}$, then $\tilde{b}$ is invertible, and we have to count the number of $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}$ lifting a, b, c, d such that $\tilde{c} \equiv \tilde{b}^{-1}(\tilde{a}\tilde{d} - (\tilde{a}+\tilde{d}) - r + 1) \pmod{\ell^k}$, and there are $\ell^{3(k-1)}$ such lifts. A similar argument shows that there are also $\ell^{3(k-1)}$ lifts if $c \not\equiv 0 \pmod{\ell}$, or $a \not\equiv 1 \pmod{\ell}$ or $d \not\equiv 1 \pmod{\ell}$. This proves (2.6) as the identity matrix does not belong to $C_r(\ell)$ when $r \not\equiv 0 \pmod{\ell}$. Then, the number of lifts of any matrix from $C_r(\ell)$ to $C_r(\ell^k)$ is $\ell^{3(k-1)}$, and the number of lifts from $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ is $\ell^{4(k-1)}$, which gives

$$\frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|} = \frac{\ell^{3(k-1)}|C_r(\ell)|}{\ell^{4(k-1)}|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|},$$

and the result follows by using (2.2).

Finally, we have to count the number of lifts

$$\begin{pmatrix} 1+k_1\ell & k_2\ell \\ k_3\ell & 1+k_4\ell \end{pmatrix}$$

of the identity matrix such that $\ell^2(k_1k_4 - k_2k_3) \equiv r \pmod{\ell^k}$, where $0 \leqslant k_i < \ell^{k-1}$. We assume that $k \geqslant 2$. If $r \not\equiv 0 \pmod{\ell^2}$, there are no lifts, and we assume that $r \equiv 0 \pmod{\ell^2}$. Let $v = \min_i v_\ell(k_i)$, where $v_\ell(n)$ is the ℓ-adic evaluation of n, and write $k_i = \ell^v k_i'$ with $0 \leqslant k_i' < \ell^{k-1-v}$. If $r \not\equiv 0 \pmod{\ell^{2+v}}$, there is no solution with

k_1, k_2, k_3, k_4 such that $v = \min_i v_\ell(k_i)$. Suppose that $r \equiv 0 \pmod{\ell^{2+v}}$. Then we need to solve

$$\ell^{2+v}(k_1'k_4' - k_2'k_3') \equiv \ell^{2+v} r' \pmod{\ell^k} \iff (k_1'k_4' - k_2'k_3') \equiv r' \pmod{\ell^{k-2-v}},$$

and there are $\ell\ell^{3(k-1-v)}$ solutions k_1', k_2', k_3', k_4'. The number of lifts of the identity matrix is then bounded by

$$\ell \sum_{v=0}^{k-2} \ell^{3(k-1-v)} = \ell\ell^{3(k-1)} \sum_{v=0}^{k-2} \ell^{-3v} \leqslant \ell\ell^{3(k-1)} \frac{\ell^3}{\ell^3 - 1}. \tag{2.9}$$

We now prove (2.7). Using (2.9) and the first formula of (2.1), it follows that

$$\frac{\ell^{k-1}|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|} \leqslant \frac{|C_r(\ell)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} + \frac{\ell^4/(\ell^3-1)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} = \frac{(\ell^3-1)(\ell^2-1)+1}{(\ell-1)(\ell^2-1)(\ell^3-1)}.$$

For the lower bound, we have

$$\frac{\ell^{k-1}|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|} \geqslant \frac{|C_r(\ell)|-1}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} = \frac{\ell(\ell^2-2)-1}{\ell(\ell-1)(\ell^2-1)} \geqslant \frac{\ell-2}{(\ell-1)^2}.$$

We now prove (2.8). Let $m' = \prod_{p|m} p^{\min(v_p(m), v_p(M_E))}$. By (2.5), $G(m)$ is the full inverse image of $G(m')$ under the projection map from $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ to $\mathrm{GL}_2(\mathbb{Z}/m'\mathbb{Z})$. Fix $g \in C_r(m')$, and we now count the number of lifts $\tilde{g}$ in $C_r(m)$. By the Chinese Remainder Theorem, it suffices to count the number of lifts from $C_r(p^{v_p(m')})$ to $C_r(p^{v_p(m)})$ for each $p \mid m$. In general, fix $1 \leqslant e \leqslant k$, fix $g \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ such that $\det(g) + 1 - \mathrm{tr}(g) \equiv r \pmod{p^e}$, and we count the number of lifts $\tilde{g} \in \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ such that $\det(\tilde{g}) + 1 - \mathrm{tr}(\tilde{g}) \equiv r \pmod{p^k}$. If g is not congruent to the identity matrix modulo p, then the same argument as above shows that there are $p^{3(k-e)}$ lifts of g. If g is congruent to the identity matrix modulo p, we have to count the number of matrices

$$\tilde{g} = \begin{pmatrix} 1 + k_1 p^e & k_2 p^e \\ k_3 p^e & 1 + k_4 p^e \end{pmatrix}$$

such that

$$p^{2e}(k_1k_4 - k_2k_3) \equiv r \pmod{p^k},$$

where $0 \leqslant k_i < p^{k-e}$. If $r \not\equiv 0 \pmod{\min(p^k, p^{2e})}$, there are no lifts, and we suppose that $r \equiv 0 \pmod{\min(p^k, p^{2e})}$. Let $v = \min_i v_p(k_i)$, and write $k_i = p^v k_i'$ where $0 \leqslant v < k - e$ and $0 \leqslant k_i' < p^{k-e-v}$. The congruence above rewrites as

$$p^{2e+v}(k_1'k_4' - k_2'k_3') \equiv r \pmod{p^k}. \tag{2.10}$$

If $2e + v \geqslant k$, (2.10) has $p^{4(k-e-v)}$ solutions when $r \equiv 0 \pmod{p^k}$ and no solutions otherwise. If $2e + v < k$, assume that $r \equiv 0 \pmod{(p^{2e+v})}$ (otherwise (2.10) has no solutions). Writing $r = r'p^{2e+v}$, (2.10) rewrites as $k_1'k_4' - k_2'k_3' \equiv r' \pmod{p^{k-2e-v}}$ and this leads to $p^e p^{3(k-e-v)}$ solutions k_1', k_2', k_3', k_4'. Then, the number of lifts of the identity matrix from $C_r(p^e)$ to $C_r(p^k)$ is bounded by

$$\sum_{\substack{v=0 \\ 2e+v<k}}^{k-e-1} p^e p^{3(k-e-v)} + \sum_{\substack{v=0 \\ 2e+v\geqslant k}}^{k-e-1} p^{4(k-e-v)} \leqslant p^{3(k-e)} p^{4e+1}. \tag{2.11}$$

Then, applying (2.11), we have that

$$\frac{|C_r(m)|}{|G(m)|} \leqslant \frac{|C_r(m')|}{|G(m')|} \prod_{p\mid m} \frac{p^{3(v_p(m)-v_p(m'))}p^{4v_p(m')+1}}{p^{4(v_p(m)-v_p(m'))}}$$
$$= \frac{|C_r(m')|}{|G(m')|}\frac{1}{\varphi(m)} \prod_{p\mid m} p^{v_p(m')-1}p^{4v_p(m')+1}(p-1) \ll_E \frac{|C_r(m')|}{|G(m')|}\frac{1}{\varphi(m)}.$$

Finally we suppose that $|C_r(m)| \neq 0$ and prove the lower bound in (2.8). Denoting by $C_r(m')_{\not\equiv}$ the subset of $C_r(m')$ consisting of matrices not equivalent to the identity matrix modulo p (notice that $C_r(m')_{\not\equiv}$ is not empty since $|C_r(m)| \neq 0$), we have that

$$\frac{|C_r(m)|}{|G(m)|} \geqslant \frac{|C_r(m')_{\not\equiv}|}{|G(m')|} \prod_{p\mid m} \frac{p^{3(v_p(m)-v_p(m'))}}{p^{4(v_p(m)-v_p(m'))}}$$
$$= \prod_{p^k\| m} \frac{1}{p^{k-1}(p-1)} \prod_{p\mid m} \frac{(p-1)p^{v_p(m')}}{p} \frac{|C_r(m')_{\not\equiv}|}{|G(m')|} \gg_E \frac{1}{\varphi(m)},$$

and the lower bound in (2.8) follows from the last two inequalities. □

Theorem 2.3. *Let E be an elliptic curve over $\mathbb{Q}$ without CM. Let $r \geqslant 0$ be an integer, and let $n = dm$ be any positive integer with $(d, M_E) = 1$ and $m \mid {M_E}^\infty$.*

(i) *We have that*

$$|\{p \leqslant x \,:\, n_E(p) \equiv r \,(\mathrm{mod}\, n)\}| \ll_E \frac{\mathrm{Li}(x)}{\varphi(n)} + x\exp\Big\{-An^{-2}\sqrt{\log x}\Big\}$$

uniformly for $\log x \gg n^{12}\log n$, where the implied constants depend only on the elliptic curve E and A is a positive absolute constant.

(ii) *Assuming the GRH for the Dedekind zeta functions of the number fields $L_n/\mathbb{Q}$, we have that*

$$|\{p \leqslant x \,:\, n_E(p) \equiv r \,(\mathrm{mod}\, n)\}| \ll_E \frac{\mathrm{Li}(x)}{\varphi(n)} + n^3x^{1/2}\log(nx).$$

(iii) *Assuming the GRH for the Dedekind zeta functions of the number fields $L_n/\mathbb{Q}$, we have that*

$$|\{p \leqslant x \,:\, n_E(p) \equiv r \,(\mathrm{mod}\, n)\}| \ll_E \frac{\mathrm{Li}(x)}{\varphi(n)}$$

holds uniformly for $n \leqslant x^{1/8}/\log x$, where the implied constant depends only on the elliptic curve E.

Further if $r = 0$ or $(n, M_E) = 1$, then the condition $n \leqslant x^{1/8}/\log x$ in the third assertion can be relaxed to $n \leqslant x^{1/5}/\log x$ and the term $n^3x^{1/2}\log(nx)$ in the second can be replaced by $n^{3/2}x^{1/2}\log(nx)$.

Proof. It follows from the estimates of Lemma 2.2 that

$$\frac{|C_r(m)|}{|G(m)|}\Big(\prod_{\ell^k\| d} \frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|}\Big) \ll_E \frac{1}{\varphi(d)}\frac{1}{\varphi(m)} = \frac{1}{\varphi(n)},$$

and first two statements are obtained by using this upper bound in the estimates of Proposition 2.1 for

$$\pi_{C_r(n)}(x, L_n/\mathbb{Q}) = |\{p \leqslant x \,:\, n_E(p) = p + 1 - a_E(p) \equiv r \,(\mathrm{mod}\, n)\}|\,.$$

We now prove (iii). If $|C_r(m)| = 0$, Proposition 2.1 implies trivially the required inequality, and we suppose that $|C_r(m)| \neq 0$. Clearly, it is sufficient to show that

$$\frac{1}{\varphi(n)\log_2 n} \ll_E \frac{|C_r(m)|}{|G(m)|}\Big(\prod_{\ell^k \| d} \frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|}\Big) \ll_E \frac{1}{\varphi(n)}. \tag{2.12}$$

It follows from Lemma 2.2 that

$$\frac{1}{\varphi(d)}\prod_{\ell \mid d}\frac{\ell-2}{\ell-1} \leqslant \prod_{\ell^k \| d} \frac{|C_r(\ell^k)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})|} \ll \frac{1}{\varphi(d)}, \tag{2.13}$$

and the lower bound of (2.12) follows from (2.13), (2.8) and the estimate

$$\prod_{\ell \mid d}\frac{\ell-2}{\ell-1} \geqslant \prod_{\ell \mid n}\frac{\ell-2}{\ell-1} \gg \frac{1}{\log_2 n}.$$

This completes the proof of the Theorem. □

3. Rosser-Iwaniec's linear sieve formulas

We state in this section the Rosser-Iwaniec linear sieve [9, Theorem 1], which will be used in the proof of Theorem 1.1. It is worth indicating that the Selberg linear sieve [8, Theorem 8.4] cannot be applied for our purpose since the condition $(\Omega_2(1, L))$ of Selberg's linear sieve (see [8, page 228]) is not satisfied by the function $w_y(\ell)$. But the corresponding condition (Ω_1) of the Rosser-Iwaniec's sieve is satisfied by the $w_y(\ell)$ (see (4.5) below).

Let $\mathcal{A}$ be a finite sequence of integers and $\mathcal{P}$ a set of prime numbers. As usual, we write the sieve function

$$S(\mathcal{A}, \mathcal{P}, z) := |\{a \in \mathcal{A} : (a, P(z)) = 1\}|,$$

where

$$P(z) := \prod_{p<z,\, p\in\mathcal{P}} p. \tag{3.1}$$

Let $\mathcal{B} = \mathcal{B}(\mathcal{P})$ denote the set of all positive squarefree integers supported on the primes of $\mathcal{P}$. For each $d \in \mathcal{B}$, define

$$\mathcal{A}_d := \{a \in \mathcal{A} : a \equiv 0 \,(\mathrm{mod}\, d)\}.$$

We assume that $\mathcal{A}$ is well distributed over arithmetic progressions $0 \,(\mathrm{mod}\, d)$ in the following sense: There are a convenient approximation X to $|\mathcal{A}|$ and a multiplicative function $w(d)$ on $\mathcal{B}$ verifying [§]

$$0 < w(p) < p \qquad (p \in \mathcal{P}) \tag{A_0}$$

[§]Since we need (3.2) below only for $d \mid P(z)$, we are freely to define $w(p) = 0$ for $p \notin \mathcal{P}$.

such that

(i) the "remainders"

$$r(\mathcal{A}, d) := |\mathcal{A}_d| - \frac{w(d)}{d}X \qquad (d \in \mathcal{B}) \tag{3.2}$$

are small on average over the divisors d of $P(z)$;

(ii) there exists a constant $K \geqslant 1$ such that

$$\frac{V(z_1)}{V(z_2)} \leqslant \frac{\log z_2}{\log z_1}\left(1 + \frac{K}{\log z_1}\right) \qquad (2 \leqslant z_1 < z_2), \tag{Ω_1}$$

where

$$V(z) := \prod_{p<z}\left(1 - \frac{w(p)}{d}\right).$$

The next result is the well known theorem of Iwaniec [9, Theorem 1].

Lemma 3.1. *Under the hypotheses* (A_0), (3.2) *and* (Ω_1), *we have*

$$S(\mathcal{A}, \mathcal{P}, z) \leqslant XV(z)\{F(s) + E\} + 2^{\varepsilon^{-\gamma}}R(\mathcal{A}, M, N),$$

where $0 < \varepsilon < \frac{1}{8}$, $s := (\log MN)/\log z$, $E \ll \varepsilon s^2 \mathrm{e}^K + \varepsilon^{-8}\mathrm{e}^{K-s}(\log MN)^{-1/3}$ *and*

$$F(s) = \frac{2\mathrm{e}^\gamma}{s} \quad (0 < s \leqslant 3), \qquad V(z) := \prod_{p<z}\left(1 - \frac{w(p)}{d}\right).$$

The second error term $R(\mathcal{A}, M, N)$ *has the form*

$$R(\mathcal{A}, M, N) := \sum_{\substack{m<M, n<N \\ mn|P(z)}} a_m b_n r(\mathcal{A}, mn),$$

where the coefficients a_m, b_n *are bounded by 1 in absolute value and depend at most on* M, N, z *and* ε.

4. Proof of Theorem 1.1

As in [3], introduce

$$L := \prod_{y \leqslant \ell < z} \ell$$

and

$$\mathcal{S}(x, y, z) := \{p \leqslant x \,:\, (n_E(p), L) = 1\},$$
$$\mathcal{T}(x, y, z) := \{p \leqslant x \,:\, (n_E(p), L) > 1,\ b^{n_E(p)} \equiv b \,(\mathrm{mod}\, n_E(p))\}.$$

Clearly

$$Q_{E,b}(x) \leqslant |\mathcal{S}(x, y, z)| + |\mathcal{T}(x, y, z)|. \tag{4.1}$$

First we estimate $|\mathcal{S}(x, y, z)|$.

Lemma 4.1. *Let E be an elliptic curve over $\mathbb{Q}$ without CM and $b \geqslant 2$ be an integer. For any ε, there is a constant $y_0 = y_0(E, b, \varepsilon)$ such that*

(i) *We have*

$$|\mathcal{S}(x, y, z)| \leqslant (\mathrm{e}^\gamma + \varepsilon)\frac{x \log y}{(\log x) \log z} \tag{4.2}$$

uniformly for $y_0 \leqslant y \leqslant z \leqslant (\log x)^{1/24}/\log_2 x$.

(ii) *If we assume the GRH, we have*

$$|\mathcal{S}(x, y, z)| \leqslant (\mathrm{e}^\gamma + \varepsilon)\frac{x \log y}{(\log x) \log z} \tag{4.3}$$

uniformly for $y_0 \leqslant y \leqslant z \leqslant x^{1/10}/(\log x)^4$.

Proof. We shall sieve

$$\mathscr{A} := \{n_E(p) \,:\, p \leqslant x\}$$

by

$$\mathscr{P}_y := \{p \,:\, p \geqslant y\}.$$

By definition, $|\mathcal{S}(x, y, z)| = S(\mathscr{A}, \mathscr{P}_y, z)$ for all $1 \leqslant y \leqslant z \leqslant x$.

Without loss of generality, we can suppose that $y_0 \geqslant M_E + b$. Thus we have $(d, M_E) = 1$ for all $d \in \mathcal{B}(\mathscr{P}_y)$. Using Proposition 2.1 (with the improved error term discussed in the remark following the proposition under the GRH) and (2.2), we get that

$$|\mathscr{A}_d| = \frac{w_y(d)}{d}X + r(\mathscr{A}, d) \tag{4.4}$$

for all $d \in \mathcal{B}(\mathscr{P}_y)$, with

$$\begin{aligned} X &= \mathrm{Li}(x), \\ w_y(\ell) &= \frac{\ell(\ell^2 - 2)}{(\ell - 1)(\ell^2 - 1)} \quad (\ell \in \mathscr{P}_y), \\ |r(\mathscr{A}, d)| &\ll_E \begin{cases} x\,\mathrm{e}^{-Ad^{-2}\sqrt{\log x}} & (d \leqslant (\log x)^{1/12}/\log_2 x), \\ d^{3/2}x^{1/2}\log(dx) & (\text{under the GRH}), \end{cases} \end{aligned} \tag{4.5}$$

where $A > 0$ is a positive absolute constant.

In order to apply Lemma 3.1, we must show that $w_y(\ell)$ satisfies conditions (A_0) and (Ω_1). The former is obvious, and we now check the latter. Writing

$$V_y(z) := \prod_{p<z}\left(1 - \frac{w_y(p)}{p}\right)^{-1}, \tag{4.6}$$

then

$$\frac{V_y(z_1)}{V_y(z_2)} \leqslant \frac{V_1(z_1)}{V_1(z_2)}$$

for all $z_2 > z_1 \geqslant 2$. On the other hand, by using the prime number theorem, it follows that

$$\begin{aligned} V_1(z) &= \prod_{p<z}\left(1-\frac{w_1(p)}{p}\right) \\ &= \prod_{p<z}\left(1-\frac{1}{p}\right)\prod_{p<z}\left(1-\frac{p^2-p-1}{(p-1)^3(p+1)}\right) \\ &= \left\{1+O\left(\frac{1}{\log z}\right)\right\}\frac{C\mathrm{e}^{-\gamma}}{\log z}, \end{aligned} \tag{4.7}$$

where γ is the Euler constant and

$$C := \prod_{p}\left(1-\frac{p^2-p-1}{(p-1)^3(p+1)}\right).$$

Clearly this implies that for any $2 \leqslant z_1 < z_2$

$$\frac{V_1(z_1)}{V_1(z_2)} = \frac{\log z_2}{\log z_1}\left\{1+O\left(\frac{1}{\log z_1}\right)\right\}, \tag{4.8}$$

and (4.6) and (4.8) show that the condition (Ω_1) is satisfied. Therefore we can apply Lemma 3.1 to write

$$S(\mathscr{A}, \mathscr{P}_y, z) \leqslant (\mathrm{e}^{\gamma}+\varepsilon)XV_y(z) + R_{\mathcal{S}}, \tag{4.9}$$

where

$$R_{\mathcal{S}} := \sum_{\substack{d<z^2\\ d\mid P(z)}} 2^{\omega(d)}|r(\mathscr{A}, d)|.$$

In view of the bounds for $|r(\mathscr{A}, d)|$ of (4.5), we can deduce that

$$R_{\mathcal{S}} \ll x/(\log x)^3 \tag{4.10}$$

for all

$$z \leqslant \begin{cases} (\log x)^{1/24}/\log_2 x & \text{(unconditionally)},\\ x^{1/10}/(\log x)^4 & \text{(under GRH)}. \end{cases} \tag{4.11}$$

On the other hand, in view of (4.7), we have for any $z > y$,

$$V_y(z) = \frac{V_1(z)}{V_1(y)} = \left\{1+O\left(\frac{1}{\log y}\right)\right\}\frac{\log y}{\log z}. \tag{4.12}$$

Inserting (4.10) and (4.12) into (4.9), we obtain the required results. □

In order to estimate $|\mathcal{T}(x, y, z)|$, we need to prove a preliminary result. For integers $b \geqslant 2$ and $d \geqslant 1$, denote by $\mathrm{ord}_d(b)$ the multiplicative order of b modulo d (i.e. the smallest positive integer k with $b^k \equiv 1 \,(\mathrm{mod}\, d)$).

Lemma 4.2. *For all $t \geqslant 1$, we have*

$$\sum_{\ell \geqslant t} \frac{1}{\ell \mathrm{ord}_\ell(b)} \ll_b \frac{1}{t^{1/2}}, \tag{4.13}$$

$$\sum_{\ell \mathrm{ord}_\ell(b) \geqslant t} \frac{1}{\ell \mathrm{ord}_\ell(b)} \ll_b \frac{1}{t^{1/3}}. \tag{4.14}$$

Proof. Let $0 < \eta < 1$ be a parameter to be choosen later. We have

$$\sum_{\substack{\ell \\ \mathrm{ord}_\ell(b) = m}} 1 \leqslant \sum_{\ell | (b^m - 1)} 1 \leqslant \frac{\log(b^m - 1)}{\log 2} \leqslant \frac{\log b}{\log 2} m. \tag{4.15}$$

Thus

$$\sum_{\substack{\ell \leqslant u \\ \mathrm{ord}_\ell(b) < \ell^\eta}} \frac{1}{\mathrm{ord}_\ell(b)} = \sum_{m \leqslant u^\eta} \frac{1}{m} \sum_{\substack{\ell \leqslant u \\ \mathrm{ord}_\ell(b) = m}} 1 \leqslant \sum_{m \leqslant u^\eta} \frac{\log b}{\log 2} \ll_{b,\eta} u^\eta.$$

A simple partial summation leads to

$$\sum_{\substack{\ell \geqslant t \\ \mathrm{ord}_\ell(b) < \ell^\eta}} \frac{1}{\ell \mathrm{ord}_\ell(b)} = \int_t^\infty \frac{1}{u} \mathrm{d}\Big(\sum_{\substack{\ell \leqslant u \\ \mathrm{ord}_\ell(b) < \ell^\eta}} \frac{1}{\mathrm{ord}_\ell(b)} \Big) \ll_{b,\eta} \frac{1}{t^{1-\eta}}.$$

On the other hand, we have trivially

$$\sum_{\substack{\ell \geqslant t \\ \mathrm{ord}_\ell(b) \geqslant \ell^\eta}} \frac{1}{\ell \mathrm{ord}_\ell(b)} \ll \sum_{\ell \geqslant t} \frac{1}{\ell^{1+\eta}} \ll_\eta \frac{1}{t^\eta}.$$

Combining these estimates and taking $\eta = \frac{1}{2}$, we obtain (4.13).

Similarly we have

$$\sum_{\substack{\ell \mathrm{ord}_\ell(b) \geqslant t \\ \mathrm{ord}_\ell(b) < \ell^\eta}} \frac{1}{\ell \mathrm{ord}_\ell(b)} \leqslant \sum_{\substack{\ell \geqslant t^{1/(1+\eta)} \\ \mathrm{ord}_\ell(b) < \ell^\eta}} \frac{1}{\ell \mathrm{ord}_\ell(b)} \ll_{b,\eta} \frac{1}{t^{(1-\eta)/(1+\eta)}},$$

$$\begin{aligned}
\sum_{\substack{\ell \mathrm{ord}_\ell(b) \geqslant t \\ \mathrm{ord}_\ell(b) \geqslant \ell^\eta}} \frac{1}{\ell \mathrm{ord}_\ell(b)} &= \sum_{k \geqslant 1} \sum_{\substack{\ell \mathrm{ord}_\ell(b) \geqslant t \\ 2^{k-1} \ell^\eta \leqslant \mathrm{ord}_\ell(b) < 2^k \ell^\eta}} \frac{1}{\ell \mathrm{ord}_\ell(b)} \\
&\ll \sum_{k \geqslant 1} \frac{1}{2^k} \sum_{\ell \geqslant (2^{-k} t)^{1/(1+\eta)}} \frac{1}{\ell^{1+\eta}} \\
&\ll_\eta \frac{1}{t^{\eta/(1+\eta)}}.
\end{aligned}$$

The inequality (4.14) follows from these estimates with the choice of $\eta = \frac{1}{2}$. □

We now estimate $|\mathcal{T}(x, y, z)|$.

Lemma 4.3. *Let E be an elliptic curve over $\mathbb{Q}$ without CM and $b \geqslant 2$ be an integer. Then there is a constant $y_0 = y_0(E, b)$ and a positive absolute constant A such that*

(i) *We have*

$$|\mathcal{T}(x,y,z)| \ll_{E,b} \mathrm{Li}(x)\frac{\log_2 z}{y^{1/2}} + x\exp\Big\{-Az^{-4}\sqrt{\log x}\Big\} \tag{4.16}$$

uniformly for

$$y_0 \leqslant y < z \leqslant (\log x)^{1/24}/\log_2 x. \tag{4.17}$$

(ii) *If we assume the GRH, we have*

$$|\mathcal{T}(x,y,z)| \ll_{E,b} \mathrm{Li}(x)\frac{\log_2 z}{y^{1/2}} + z^7 x^{1/2} \tag{4.18}$$

uniformly for

$$y_0 \leqslant y < z. \tag{4.19}$$

The implied constants depend on E and b only.

Proof. If $n_E(p)$ is a pseudoprime to base b and $d \mid n_E(p)$ with $(d,b)=1$, then

$$d \mid n_E(p) \mid b(b^{n_E(p)-1}-1) \;\Rightarrow\; d \mid (b^{n_E(p)-1}-1) \;\Rightarrow\; b^{n_E(p)-1} \equiv 1 \,(\mathrm{mod}\, d).$$

Using Fermat's little theorem, it follows that

$$n_E(p) \equiv 0 \,(\mathrm{mod}\, d), \quad n_E(p) \equiv 1 \,(\mathrm{mod}\, \mathrm{ord}_d(b)), \quad (d, \mathrm{ord}_d(b)) = 1. \tag{4.20}$$

By the Chinese remainder theorem, there is an integer $r_{b,d} \in \{1,\dots,d\mathrm{ord}_d(b)\}$ such that $n_E(p) \equiv r_{b,d} \,(\mathrm{mod}\, d\mathrm{ord}_d(b))$.

Clearly for each $p \in \mathcal{T}(x,y,z)$, there is a prime ℓ such that

$$y \leqslant \ell < z, \qquad \ell \mid (L, n_E(p)) \qquad \text{and} \qquad n_E(p) \mid b^{n_E(p)} - b. \tag{4.21}$$

Applying (4.20) with $d=\ell$, we have

$$\begin{aligned} |\mathcal{T}(x,y,z)| &\leqslant \sum_{y<\ell\leqslant z} \sum_{\substack{p\leqslant x \\ n_E(p)\equiv r_{b,\ell} (\mathrm{mod}\, \ell\mathrm{ord}_\ell(b))}} 1 \\ &= \sum_{y<\ell\leqslant z} \pi_{C_{r_{b,\ell}}}(x, L_{\ell\mathrm{ord}_\ell(b)}/\mathbb{Q}). \end{aligned}$$

Then, using (i) and (ii) of Theorem 2.3 with the bound $\varphi(n) \gg n/\log_2 n$, we have that

$$|\mathcal{T}(x,y,z)| \ll_E \mathrm{Li}(x)(\log_2 z) \sum_{y<\ell\leqslant z} \frac{1}{\ell\mathrm{ord}_\ell(b)} + R_{\mathcal{T}}, \tag{4.22}$$

where

$$\begin{aligned} R_{\mathcal{T}} &:= \begin{cases} \displaystyle\sum_{y<\ell\leqslant z} x\exp\Big\{-A\ell^{-4}\sqrt{\log x}\Big\} & (z \leqslant (\log x)^{1/24}/\log_2 x) \\ \displaystyle\sum_{y<\ell\leqslant z} \ell^6 x^{1/2}\log(\ell^2 x) & \text{(under the GRH)} \end{cases} \\ &\ll \begin{cases} x\exp\Big\{-Az^{-4}\sqrt{\log x}\Big\} & (z \leqslant (\log x)^{1/24}/\log_2 x), \\ z^7 x^{1/2} & \text{(under the GRH)}. \end{cases} \end{aligned} \tag{4.23}$$

The required results follow from (4.22), (4.23) and (4.13) of Lemma 4.2. □

Taking, in Lemmas 4.1 and 4.3

$$y = \begin{cases} (\log_2 x)^2 \log_3 x & \text{(unconditionally)}, \\ (\log x)^2 \log_2 x & \text{(under the GRH)}, \end{cases}$$
$$z = \begin{cases} (\log x)^{1/24}/\log_2 x & \text{(unconditionally)}, \\ x^{1/14}/\log x & \text{(under the GRH)}, \end{cases}$$

which satisfy (4.11) and (4.17), and using the bounds of those lemmas in (4.1), this proves Theorem 1.1.

5. Proof of Theorem 1.3

We shall adapt Pomerance's method [17] to prove Theorem 1.3.

We split the primes $p \leqslant x$ such that $n_E(p)$ is pseudoprimes to base b into four possibly overlapping classes:

- $n_E(p) \leqslant x/L(x)$;
- there is $\ell \mid n_E(p)$ with $\mathrm{ord}_\ell(b) \leqslant L(x)$ and $\ell > L(x)^3$;
- there is $\ell \mid n_E(p)$ with $\mathrm{ord}_\ell(b) > L(x)$;
- $n_E(p) > x/L(x)$, for all $\ell \mid n_E(p)$, we have $\ell \leqslant L(x)^3$;

and denote by $S_1, \dots, S_4$ the corresponding contribution to $\pi^{\mathrm{pseu}}_{E,b}(x)$, respectively.

A. *Estimate for* S_1

In view of (1.13), it follows that

$$S_1 \leqslant \sum_{p \leqslant 16x/L(x)} 1 \ll \frac{x}{L(x)}. \tag{5.1}$$

B. *Estimate for* S_2

Clearly

$$S_2 \leqslant \sum_{\substack{\ell > L(x)^3 \\ \mathrm{ord}_\ell(b) \leqslant L(x)}} \sum_{\substack{p \leqslant x \\ \ell \mid n_E(p)}} 1.$$

Using (iii) of Theorem 2.3 with $r = 0$ and (4.15), we deduce that the contribution of $L(x)^3 < \ell \leqslant x^{1/5}/\log x$ to S_2 is

$$\ll_E \sum_{\substack{L(x)^3 < \ell \leqslant x^{1/5}/\log x \\ \mathrm{ord}_\ell(b) \leqslant L(x)}} \frac{\mathrm{Li}(x)}{\varphi(\ell)} \ll_E \frac{x}{L(x)^3} \sum_{\mathrm{ord}_\ell(b) \leqslant L(x)} 1 \ll_{E,b} \frac{x}{L(x)}.$$

Furthermore, using Hypothesis 1.2 with $\delta < \frac{1}{5}$, we have

$$\begin{aligned}\sum_{\substack{x^{1/5}/\log x<\ell\\ \mathrm{ord}_\ell(b)\leqslant L(x)}}\sum_{\substack{p\leqslant x\\ \ell\mid n_E(p)}} 1 &\leqslant \sum_{\substack{x^{1/5}/\log x<\ell\leqslant 2x\\ \mathrm{ord}_\ell(b)\leqslant L(x)}}\sum_{m\leqslant 2x/\ell}\sum_{\substack{p\leqslant x\\ n_E(p)=m\ell}} 1\\ &\ll_E \sum_{\substack{x^{1/5}/\log x<\ell\leqslant 2x\\ \mathrm{ord}_\ell(b)\leqslant L(x)}}\sum_{m\leqslant 2x/\ell}(m\ell)^\delta\\ &\ll_E \sum_{\substack{x^{1/5}/\log x<\ell\leqslant 2x\\ \mathrm{ord}_\ell(b)\leqslant L(x)}}\frac{x^{1+\delta}}{\ell}\\ &\ll_{E,b} x^{4/5+\delta}L(x)^3,\end{aligned}$$

using (4.15).

Combining these estimates yields

$$S_2 \ll_{E,b} \frac{x}{L(x)}. \tag{5.2}$$

C. *Estimate for* S_3

Clearly

$$S_3 \leqslant \sum_{\substack{n\leqslant 4x,\, \exists \ell\mid n \text{ with } \mathrm{ord}_\ell(b)>L(x)\\ n \text{ pseudoprime}}}\sum_{\substack{p\leqslant x\\ n_E(p)=n}} 1.$$

If n is a pseudoprime and $d \mid n$, then

$$n \equiv 0 \,(\mathrm{mod}\, d), \quad n \equiv 1 \,(\mathrm{mod}\, \mathrm{ord}_d(b)), \quad (d, \mathrm{ord}_d(b)) = 1. \tag{5.3}$$

Thus the number of pseudoprimes $n \leqslant 4x$ with $d \mid n$ at most $1 + 4x/(d\mathrm{ord}_d(b))$. If $d = \ell$, a prime, then we throw out the solution $n = \ell$ to (5.3), so that in this case there are at most $4x/(\ell\mathrm{ord}_\ell(b))$ solutions in pseudoprimes n. Then, if $\ell\mathrm{ord}_\ell(b) > 4x$, there are no solution in pseudoprimes n and no contribution to S_3, and we can suppose that $\ell\mathrm{ord}_\ell(b) \leqslant 4x$. Thus

$$\begin{aligned}S_3 &\leqslant \sum_{\substack{\ell\mathrm{ord}_\ell(b)\leqslant 4x\\ \mathrm{ord}_\ell(b)>L(x)}}\sum_{\substack{n\leqslant 4x,\, \ell\mid n\\ n \text{ pseudoprime}}}\sum_{\substack{p\leqslant x\\ n_E(p)=n}} 1\\ &\leqslant \sum_{\substack{\ell\mathrm{ord}_\ell(b)\leqslant 4x\\ \mathrm{ord}_\ell(b)>L(x)}}\sum_{\substack{p\leqslant 4x,\, \ell\mid n_E(p)\\ n_E(p) \text{ pseudoprime}}} 1.\end{aligned}$$

Applying (4.20) with $d = \ell$, there is an integer $r_{b,\ell} \in \{1, \dots, \ell\mathrm{ord}_\ell(b)\}$ such that $n_E(p) \equiv r_{b,\ell} \,(\mathrm{mod}\, d\mathrm{ord}_d(b))$. Thus

$$S_3 \leqslant \sum_{\substack{\ell\mathrm{ord}_\ell(b)\leqslant 4x\\ \mathrm{ord}_\ell(b)>L(x)}}\sum_{\substack{p\leqslant x\\ n_E(p)\equiv r_{b,\ell}(\mathrm{mod}\, \ell\mathrm{ord}_\ell(b))}} 1. \tag{5.4}$$

If $\ell\mathrm{ord}_\ell(b) \leqslant x^{1/8}/\log x$, then by Theorem 2.3(iii)

$$\sum_{\substack{p\leqslant x\\ n_E(p)\equiv r_{b,\ell}(\mathrm{mod}\,\ell\mathrm{ord}_\ell(b))}} 1 \ll_E \frac{\mathrm{Li}(x)}{\varphi(\ell\mathrm{ord}_\ell(b))},$$

and using again the bound $\varphi(n) \gg n/\log_2 n$, the contribution of those ℓ to S_3 is bounded by

$$\begin{aligned}\sum_{\substack{\ell\mathrm{ord}_\ell(b)\leqslant x^{1/8}/\log x\\ \mathrm{ord}_\ell(b)>L(x)}} \frac{\mathrm{Li}(x)}{\varphi(\ell\mathrm{ord}_\ell(b))} &\ll_E \frac{\mathrm{Li}(x)\log_2 x}{L(x)} \sum_{\ell\mathrm{ord}_\ell(b)\leqslant x^{1/8}/\log x} \frac{1}{\ell}\\ &\ll_E \frac{\mathrm{Li}(x)(\log_2 x)^2}{L(x)}.\end{aligned}$$

With the help of Hypothesis 1.2 with $\delta < \frac{1}{24}$ and (4.14) of Lemma 4.2, the contribution of $x^{1/8}/\log x < \ell\mathrm{ord}_\ell(b) \leqslant 4x$ to S_3 is bounded by

$$\begin{aligned}&\sum_{x^{1/8}/\log x<\ell\mathrm{ord}_\ell(b)\leqslant 4x}\ \sum_{0\leqslant m\leqslant 4x/\ell\mathrm{ord}_\ell(b)}\ \sum_{\substack{p\leqslant x\\ n_E(p)=r_{b,\ell}+m\ell\mathrm{ord}_\ell(b)}} 1\\ &\ll_E \sum_{x^{1/8}/\log x<\ell\mathrm{ord}_\ell(b)\leqslant 4x}\ \sum_{0\leqslant m\leqslant 4x/\ell\mathrm{ord}_\ell(b)} (r_{b,\ell}+m\ell\mathrm{ord}_\ell(b))^\delta\\ &\ll_E \sum_{x^{1/8}/\log x<\ell\mathrm{ord}_\ell(b)\leqslant 4x} \frac{x^{1+\delta}}{\ell\mathrm{ord}_\ell(b)}\\ &\ll_E x^{1+\delta-1/24}\log x.\end{aligned}$$

Inserting these estimates into (5.4), we find that

$$S_3 \ll_E \frac{x}{L(x)}. \tag{5.5}$$

D. *Estimate for S_4*

In order to adapt the proof of [17] to the more general definition (1.4) of pseudoprimes (which includes the case where b and n are not coprime), we write $n_E(p) = n'_E(p)n''_E(p)$ with $n'_E(p) \mid b^\infty$ and $(n''_E(p), b) = 1$. Denote by S'_4 and S''_4 the contribution of $n'_E(p) > x^{2/3}$ and $n'_E(p) \leqslant x^{2/3}$ to S_4, respectively.

By the Hasse bound (formulated as the statement of Hypothesis 1.2 with $\delta = \frac{1}{2}$), we have

$$\begin{aligned} S_4' &\leqslant \sum_{\substack{x^{2/3}<d\leqslant 4x\\ d\mid b^\infty}} \sum_{\substack{m\leqslant 4x/d\\ (m,b)=1}} \sum_{\substack{p\leqslant x\\ n_E'(p)=d,\, n_E''(p)=m}} 1 \\ &\ll_E \sum_{\substack{x^{2/3}<d\leqslant 4x\\ d\mid b^\infty}} \sum_{m\leqslant 4x/d} (dm)^{1/2} \\ &\leqslant \sum_{\substack{x^{2/3}<d\leqslant 4x\\ d\mid b^\infty}} \frac{x^{3/2}}{d} \\ &\leqslant x^{5/6}(\log x)^b. \end{aligned}$$

If p is counted in S_4'', then $n_E''(p) > x^{1/3}/L(x)$ and all prime factors of $n_E''(p)$ are $\leqslant L(x)^3$. Thus $n_E''(p)$ must have a divisor d with $x^{1/18} < d \leqslant x^{1/17}$ and $(d,b)=1$. Thus, by the comment following (4.20), $n_E(p) \equiv r_{b,d} \pmod{d\mathrm{ord}_d(b)}$ for some residue $r_{b,d}$, and by Theorem 2.3, we have

$$\begin{aligned} S_4'' &\leqslant \sum_{\substack{x^{1/18}<d\leqslant x^{1/17}\\ (d,b)=1}} \sum_{\substack{p\leqslant x\\ n_E(p)\equiv r_{b,d} (\mathrm{mod}\, d\mathrm{ord}_d(b))}} 1 \\ &\ll_E \sum_{x^{1/18}<d\leqslant x^{1/17}} \frac{x}{d\mathrm{ord}_d(b)} \\ &\leqslant x \sum_{m\leqslant x^{1/17}} \frac{1}{m} \sum_{\substack{x^{1/18}<d\leqslant x^{1/17}\\ \mathrm{ord}_d(b)=m}} \frac{1}{d}. \end{aligned}$$

With the help of the following inequality (see [17, Theorem 1])

$$\sum_{\substack{d\leqslant t\\ \mathrm{ord}_d(b)=m}} 1 \leqslant \frac{t}{\sqrt{L(t)}} \quad (t \geqslant t_0(b),\, m \geqslant 1),$$

a simple partial integration allows us to deduce that

$$\sum_{\substack{x^{1/18}<d\leqslant x^{1/17}\\ \mathrm{ord}_d(b)=m}} \frac{1}{d} = \int_{x^{1/18}}^{x^{1/17}} \frac{1}{t}\,\mathrm{d}\Big(\sum_{\substack{d\leqslant t\\ \mathrm{ord}_d(b)=m}} 1\Big) \ll \frac{1}{L(x)^{1/37}},$$

and $S_4'' \ll_E x(\log x)L(x)^{-1/37}$. Thus

$$S_4 = S_4' + S_4'' \ll_{E,b} \frac{x}{L(x)} + \frac{x\log x}{L(x)^{1/37}} \leqslant \frac{x}{L(x)^{1/38}}. \tag{5.6}$$

The statement of Theorem 1.3 then follows from (5.1), (5.2), (5.5) and (5.6).

6. Proof of Theorem 1.5

First write

$$\pi_{E,b}^{\mathrm{pseu}}(x) = \sum_{\substack{p\leqslant x\\ n_E(p) \text{ is pseudoprime to base } b}} 1 \leqslant \sum_{\substack{n\leqslant 4x\\ n \text{ is pseudoprime to base } b}} M_E(n).$$

By using the Cauchy-Schwarz inequality, it follows that

$$\pi_{E,b}^{\mathrm{pseu}}(x) \leqslant \Big(\pi_b^{\mathrm{pseu}}(4x)\Big)^{1/2}\Big(\sum_{n\leqslant 4x} M_E(n)^2\Big)^{1/2}. \tag{6.1}$$

To bound the second sum on the right-hand side of (6.1), we use a result of Kowalski [12] who proved that for a curve E with complex multiplication and for any $\varepsilon > 0$,

$$\sum_{n\leqslant 4x} M_E(n)^2 \ll \frac{x}{(\log x)^{1-\varepsilon}}. \tag{6.2}$$

We remark that in [12], there are no curves with complex multiplication defined over $\mathbb{Q}$ as the field of complex multiplication must be included in the field of definition of the elliptic curve. Then, (6.2) is first proven for the sequence $\{n_E(\mathfrak{p}) = \#E(\mathbb{F}_{\mathfrak{p}})\}$ associated to E, where $\mathfrak{p}$ runs over the primes of the CM field [12, Theorem 5.4]. This first result can then be used to deduce the upper bound (6.2) by separating the rational primes into ordinary and supersingular primes of E, and by using [12, Theorem 5.4] to obtain (6.2) (see [12, Proposition 7.4]).

Theorem 1.5 then follows by replacing (6.2) and (1.9) in (6.1).

References

[1] A. Balog, A. C. Cojocaru & C. David, *Average twin prime conjecture for elliptic curves*, Amer. J. of Math., to appear.

[2] A. C. Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289.

[3] A. C. Cojocaru, F. Luca & I. E. Shparlinski, *Pseudoprime reductions of elliptic curves*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 3, 513–522.

[4] R. Crandall & C. Pomerance, *Prime numbers. A computational perspective*, Second edition. Springer, New York, 2005. xvi+597 pp.

[5] C. David & J. Wu, *Almost prime values of the order of elliptic curves over finite fields*, Forum Math., to appear.

[6] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206.

[7] D.M. Gordon and C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), 825–838.

[8] H. Halberstam & H.-E. Richert, *Sieve Methods*, Academic Press, London 1974.

[9] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith. **37** (1980), 307–320.

[10] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. of the Amer. Math. Soc. **362** (2010), 1547–1570.

[11] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), No. 1, 157–165.
[12] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. **21** (2006), no. 1, 19–114.
[13] J. Lagarias & A. Odlyzko, *Effective versions of the Chebotarev Density Theorem*, in: Algebraic Number Fields (A. Fröhlich edit.), New York, Academic Press (1977), 409-464.
[14] F. Luca & Igor E. Shparlinski, *Pseudoprime values of the Fibonacci sequence, polynomials and the Euler function*, Indag. Math. (N.S.) **17** (2006), no. 4, 611–625.
[15] F. Luca & Igor E. Shparlinski, *Pseudoprime Cullen and Woodall numbers*, Colloq. Math. **107** (2007), no. 1, 35–43.
[16] M.-R. Murty, V.-K. Murty & N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), 253–281.
[17] C. Pomerance, *On the distribution of pseudoprimes*, Math. Computation **37** (1981), no. 156, 587–593.
[18] A. J. van der Poorten & A. Rotkiewicz, *On strong pseudoprimes in arithmetic progressions*, J. Austral. Math. Soc. Ser. A **29** (1980), no. 3, 316–321.
[19] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
[20] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Etudes Sci. Publ. Math. **54** (1981), 123–201.
[21] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152.
[22] D. Zywina, *The large sieve and Galois representations*, preprint. arXiv:0812.2222.

Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montréal, QC, H3G 1M8, Canada
E-mail address: cdavid@mathstat.concordia.ca

Institut Elie Cartan Nancy, CNRS, Université Henri Poincaré (Nancy 1), INRIA, Boulevard des Aiguillettes, B.P. 239, 54506 Vandœuvre-lès-Nancy, France
E-mail address: wujie@iecn.u-nancy.fr