ALMOST PRIME VALUES OF THE ORDER OF ELLIPTIC CURVES OVER FINITE FIELDS

C. DAVID & J. WU

ABSTRACT. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. For each prime p of good reduction, let $|E(\mathbb{F}_p)|$ be the order of the group of points of the reduced curve over $\mathbb{F}_p$. According to a conjecture of Koblitz, there should be infinitely many such primes p such that $|E(\mathbb{F}_p)|$ is prime, unless there are some local obstructions predicted by the conjecture. Suppose that E is a curve without local obstructions (which is the case for most elliptic curves over $\mathbb{Q}$). We prove in this paper that, under the GRH, there are at least $2.778 C_E^{\text{twin}} x/(\log x)^2$ primes p such that $|E(\mathbb{F}_p)|$ has at most 8 prime factors, counted with multiplicity. This improves previous results of Steuding & Weng [20] and Murty & Miri [15]. This is also the first result where the dependence on the conjectural constant C_E^{twin} appearing in Koblitz's conjecture (also called the twin prime conjecture for elliptic curves) is made explicit. This is achieved by sieving a slightly different sequence than the one of [20] and [15]. By sieving the same sequence and using Selberg's linear sieve, we can also improve the constant of Zywina [24] appearing in the upper bound for the number of primes p such that $|E(\mathbb{F}_p)|$ is prime. Finally, we remark that our results still hold under an hypothesis weaker than the GRH.

1. INTRODUCTION

The twin prime conjecture is one of the oldest questions in number theory, and can be stated as: there is an infinity of prime numbers p such that $p + 2$ is also prime. The best known result is due to Chen [3], who proved that

$$\big|\{p \leqslant x : p + 2 = P_2\}\big| \geqslant 0.335 \frac{C_{\text{twin}} x}{(\log x)^2} \tag{1.1}$$

for $x \geqslant x_0$, where P_r denotes an integer having at most r prime factors counted with multiplicity and

$$C_{\text{twin}} := 2 \prod_{\ell > 2} \bigg(1 - \frac{1}{(\ell - 1)^2}\bigg).$$

Here and in the sequel, the letters p and ℓ denote prime numbers. There are many generalisations of the twin prime conjecture, and in particular, an analogous conjecture for elliptic curves was formulated by Koblitz [13]. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N_E, and denote by $E(\mathbb{F}_p)$ the reduction of E modulo p. Koblitz [13] conjectured that as $x \to \infty$

$$\pi_E^{\text{twin}}(x) := \big|\{p \leqslant x : p \nmid N_E, |E(\mathbb{F}_p)| \text{ is prime}\}\big| \sim \frac{C_E^{\text{twin}} x}{(\log x)^2}, \tag{1.2}$$

Date: May 11, 2010.

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

Key words and phrases. linear sieve with weights, group order of elliptic curves.

where the constant C_E^{twin} can be explicitely written as an Euler product like the twin prime constant (see (2.5) below). The constant C_E^{twin} can be 0 when there are "congruence obstructions", and the conjecture is then interpreted to mean that there are finitely many primes p such that $|E(\mathbb{F}_p)|$ is prime (see Section 2 for more details). This conjecture has theoretical relevance to elliptic curve cryptosystems based the discrete logarithm problem in the group $E(\mathbb{F}_p)$.

As the twin prime conjecture, 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 lower bounds for the number of primes p such that $|E(\mathbb{F}_p)|$ is almost-prime. It is necessary to distinguish two cases: when E has complex multiplication (CM) or not. In the first case, Iwaniec & Jiménez Urroz [9, 10] have obtained an analogue of Chen's theorem (1.1). In the non-CM case, all results assume the generalized Riemann hypothesis (GRH) for Dedekind zeta-functions of some number fields. The first result of this type is due to Miri & Murty [15], who proved by using Selberg's sieve [2] that

$$\big|\big\{p \leqslant x : |E(\mathbb{F}_p)| = P_{16}\big\}\big| \gg \frac{x}{(\log x)^2} \tag{1.3}$$

for $x \geqslant x_0(E)$, where the implicit constant depends on the elliptic curve E. Recently Steuding and Weng [20, 21] have improved 16 to 9, by using Richert's logarithmic weighted sieve [7] and some improvements to the error term of the explicit Chebotarev Density Theorem due to Serre [18] and M.-R. Murty, V.-K. Murty & Saradha [16].

We prove in this paper a better result under a weaker hypothesis, namely we replace the GRH by the θ-hypothesis which states that there are no zeroes with $\Re e\, s > \theta$ for Dedekind zeta-functions and Artin L-functions. This is stated in Section 3 as Hypothesis 3.4. We also write explicitly the constant in terms of the twin prime constant C_E^{twin} by modifying slightly the set to sieve. In all the following, the primes $p \leqslant x$ always exclude the primes dividing the conductor of the elliptic curve E.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication such that $C_E^{\mathrm{twin}} \neq 0$. Assuming Hypothesis 3.4 for any $1/2 \leqslant \theta < 1$, we have*

$$\big|\big\{p \leqslant x : (|E(\mathbb{F}_p)|, M_E) = 1,\ |E(\mathbb{F}_p)| = P_r\big\}\big| \geqslant \frac{1.323}{1-\theta}\frac{C_E^{\mathrm{twin}} x}{(\log x)^2} \tag{1.4}$$

for $x \geqslant x_0(E, \theta)$, where M_E is an integer depending on E (which will be described explicitly in Section 2) and

$$r = r(\theta) := \left[\frac{18+2\theta}{5(1-\theta)}\right] + 1. \tag{1.5}$$

Here $[t]$ denotes the integral part of t.

Since $(18+2\theta)/(5-5\theta) < 8$ if and only if $\theta < 11/21$, we immediately obtain the following result, which improves, under a weaker hypothesis, the result of Steuding & Weng mentioned above.

Corollary 1.2. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication such that $C_E^{\text{twin}} \neq 0$. Assuming Hypothesis 3.4 for any $1/2 \leqslant \theta < 11/21$, we have*

$$\left|\left\{p \leqslant x : (|E(\mathbb{F}_p)|, M_E) = 1,\ |E(\mathbb{F}_p)| = P_8\right\}\right| \geqslant 2.778 \frac{C_E^{\text{twin}} x}{(\log x)^2} \tag{1.6}$$

for $x \geqslant x_0(E)$. In particular (1.6) holds if we assume GRH.

Of course, Theorem 1.1 and Corollary 1.2 imply the same lower bound for

$$\left|\left\{p \leqslant x : |E(\mathbb{F}_p)| = P_8\right\}\right|$$

since we are getting a lower bound for a smaller set. We will see in Section 2 that it is natural to count primes such that $(|E(\mathbb{F}_p)|, M_E) = 1$ when sieving to get the right constant in Theorem 1.1.

Upper bounds for $\pi_E^{\text{twin}}(x)$ were first studied by Cojocaru who showed in [4] that $\pi_E^{\text{twin}}(x) \ll x/(\log x)^2$ by using Selberg's linear sieve under the GRH. The implicit constant depends on the conductor of E, but the exact dependency was not worked out. Very recently, Zywina [24] applied an abstract form of the large sieve to obtain that

$$\pi_E^{\text{twin}}(x) \leqslant \{22 + o(1)\} \frac{C_E^{\text{twin}} x}{(\log x)^2} \tag{1.7}$$

as $x \to \infty$. His result applies to a more general form of Koblitz's conjecture, where the elliptic curve E can be defined over any number field.

The second aim of this paper is to show that Selberg's linear sieve allows us to obtain the correct twin prime constant C_E^{twin} with a better constant factor than (1.7) in the case of elliptic curves over $\mathbb{Q}$.

Theorem 1.3. *Under the condition of Theorem 1.1, for any $\varepsilon > 0$ we have*

$$\pi_E^{\text{twin}}(x) \leqslant \left(\frac{5}{1-\theta} + \varepsilon\right) \frac{C_E^{\text{twin}} x}{(\log x)^2}$$

for $x \geqslant x_0(E, \theta, \varepsilon)$.

Then, assuming GRH, Theorem 1.3 allows us to improve the constant in (1.7) from 22 to 10.

Acknowledgments. The authors wish to thank David Zywina for helpful comments and discussions. The first author also wishes to thank l'Institut Élie Cartan de Nancy-Université for hospitality and support during the preparation of this article.

2. Koblitz's Conjecture

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication with conductor N_E, and let $L_n := \mathbb{Q}(E[n])$ be the field extension obtained from $\mathbb{Q}$ by adding the coordinates of the points of n-torsion to $\mathbb{Q}$. This is a Galois extension of $\mathbb{Q}$, and in all this paper, we denote

$$G(n) = \text{Gal}(L_n/\mathbb{Q}).$$

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 $x^2 - a_p x + p$ where a_p is defined by the relation

$$|E(\mathbb{F}_p)| = p + 1 - a_p, \tag{2.1}$$

it is not difficult to see that

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

It was shown by Serre [17] that the Galois groups $G(n) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ are large, in the sense that there exists a positive integer M_E such that

$$\text{If } (n, M_E) = 1, \text{ then } G(n) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}); \tag{2.2}$$

$$\text{If } (n, M_E) = (n, m) = 1, \text{ then } G(mn) \simeq G(m) \times G(n). \tag{2.3}$$

For any integer n, let

$$C(n) = \{g \in G(n) \ : \ \det(g) + 1 - \mathrm{tr}(g) \equiv 0 \,(\mathrm{mod}\, n)\}.$$

The original Koblitz constant was defined in terms of the local probabilities for the event $\ell \nmid p+1-a_p(E)$, which can be evaluated by counting matrices g in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. More precisely, for each prime ℓ, the correcting probability factor is the quotient

$$E(\ell) = \frac{1 - |C(\ell)|/|G(\ell)|}{1 - 1/\ell} \tag{2.4}$$

where the numerator is the probability that $p + 1 - a_p(E)$ is not divisible by ℓ and the denominator is the probability that a random integer is not divisible by ℓ. If $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which happens for all but finitely many primes by (2.2), then

$$E(\ell) = \frac{1 - |C(\ell)|/|G(\ell)|}{1 - 1/\ell} \quad = \quad 1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}.$$

The constant C_E^{twin} of [13] was defined as the product over all primes ℓ of the Euler factors $E(\ell)$. In [23], Zywina made the observation that the probabilities are not multiplicative, as the events are not independent: the fields $\mathbb{Q}(E[\ell])$ are not necessarily linearly disjoint for all primes ℓ, as observed by Serre in [17]. For any integer m, let

$$\Omega(m) = \{g \in G(m) : (\det(g) + 1 - \mathrm{tr}(g), m) \neq 1\}.$$

According to the refinement of [23], the probability factor at M_E is defined as

$$\frac{1 - |\Omega(M_E)|/|G(M_E)|}{\prod_{\ell | M_E}(1 - 1/\ell)}.$$

The twin prime constant C_E^{twin} is then defined as

$$C_E^{\mathrm{twin}} := \frac{1 - |\Omega(M_E)|/|G(M_E)|}{\prod_{\ell | M_E}(1 - 1/\ell)} \prod_{\ell \nmid M_E} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right). \tag{2.5}$$

We remark that $C_E^{\rm twin}$ as defined by (2.5) can be 0, when $\Omega(M_E) = G(M_E)$, which means that $p+1-a_p(E) = |E(\mathbb{F}_p)|$ is never co-prime to M_E for any $p \nmid N_E M_E$. i.e there is a "congruence obstruction" modulo M_E. This happens for example when E has rational torsion of order t as $t \mid p+1-a_p(E)$ for all $p \nmid tN_E$ in that case, but not exclusively, and some other cases of congruence obstructions are exhibited in [12]. Elliptic curves with congruence obstructions are exceptional, and most elliptic curves over $\mathbb{Q}$ do not have congruence obstructions (for example, Serre curves do not have congruence obstructions, and most elliptic curves over $\mathbb{Q}$ are Serre curves [11]).

We also remark that if we assume Koblitz's conjecture, it follows immediately that

$$\left|\left\{p \leqslant x : (|E(\mathbb{F}_p)|, M_E) = 1,\ |E(\mathbb{F}_p)| \text{ is prime}\right\}\right| \sim \frac{C_E^{\rm twin} x}{(\log x)^2} \tag{2.6}$$

as $x \to \infty$. It is easy to see that (1.2) and (2.6) are equivalent, as we can write

$$\sum_{\substack{p\leqslant x\\ |E(\mathbb{F}_p)| \text{ is prime}}} 1 = \sum_{\substack{p\leqslant x\\ |E(\mathbb{F}_p)| \text{ is prime}\\ (|E(\mathbb{F}_p)|, M_E)=1}} 1 + \sum_{\substack{p\leqslant x\\ |E(\mathbb{F}_p)| \text{ is prime}\\ (|E(\mathbb{F}_p)|, M_E)>1}} 1. \tag{2.7}$$

The condition that $|E(\mathbb{F}_p)|$ is prime and $(|E(\mathbb{F}_p)|, M_E) > 1$ implies that $|E(\mathbb{F}_p)| = p'$ for some prime p' which divides M_E. On the other hand, the relation (2.1) and Hasse's bound $|a_p| \leqslant 2\sqrt{p}$ allow us to deduce that $|E(\mathbb{F}_p)| \geqslant p+1-2\sqrt{p} \geqslant p/16$. Thus $p \leqslant 16p' \leqslant 16M_E$. This shows that the second sum on the right-hand side of (2.7) is bounded by $16M_E$.

In this paper, we sieve the sequence

$$\{|E(\mathbb{F}_p)| : p \leqslant x,\ (|E(\mathbb{F}_p)|, M_E) = 1\} \tag{2.8}$$

instead of the sequence

$$\{|E(\mathbb{F}_p)| : p \leqslant x\} \tag{2.9}$$

suggested by (1.2) as in [16, 20, 21]. This will allow us to obtain the correct twin prime constant $C_E^{\rm twin}$ in our theorem.

We will need later the fact that

$$1 - \frac{|\Omega(M_E)|}{|G(M_E)|} = \sum_{d \mid M_E} \mu(d) \frac{|C(d)|}{|G(d)|}. \tag{2.10}$$

This can be proven by using the Chebotarev Density Theorem in the extension $L_{M_E}/\mathbb{Q}$. We are using here only the density result of the Chebotarev Density Theorem, and we refer the reader to Section 3 for versions of the Cheboratev Density Theorem with an explicit error term that will be needed to perform the sieve. Since $1 - |\Omega(M_E)|/|G(M_E)|$ is the proportion of matrices in $g \in G(M_E)$ with

$(\det g + 1 - \operatorname{tr} g, M_E) = 1$, we have that

$$\begin{aligned}\left(1 - \frac{|\Omega(M_E)|}{|G(M_E)|}\right)\pi(x) &\sim \sum_{\substack{p\leqslant x\\ (|E(\mathbb{F}_p)|, M_E)=1}} 1\\ &= \sum_{d\mid M_E} \mu(d) \sum_{\substack{p\leqslant x\\ d\mid |E(\mathbb{F}_p)|}} 1\\ &\sim \pi(x)\sum_{d\mid M_E}\mu(d)\frac{|C(d)|}{|G(d)|},\end{aligned}$$

as $x \to \infty$.

3. Chebotarev Density Theorem

We write in this section an explicit Chebotarev Density Theorem associated with the Galois extensions of $\mathbb{Q}$ obtained by adding the coordinates of the points of n-torsion to $\mathbb{Q}$.

We first need some notation and definitions. In all this section, let L/K be a finite Galois extension of number fields with Galois group G, and let C be a union of conjucacy classes in G. Let n_K and n_L be the degrees of K and L over $\mathbb{Q}$, and d_K and d_L their absolute discriminant. Let

$$M(L/K) := |G| d_K^{1/n_K} \prod_p p,$$

where the product is over the rational primes p which lie below the ramified primes of L/K. Let $\pi_C(x, L/K)$ be the number of prime ideals $\mathfrak{p} \in K$ such that $N\mathfrak{p} \leqslant x$ which are unramified in L/K and with $\sigma_{\mathfrak{p}} \in C$, where $\sigma_{\mathfrak{p}}$ is the Artin symbol at the prime ideal $\mathfrak{p}$.

The following Theorem is an effective version of the Chebotarev Density Theorem due to Lagarias and Odlyzko [14], with a slight refinement due to Serre [18].

Theorem 3.1 (Effective Chebotarev Density Theorem). (i) *Let β be the exceptional zero of the Dedekind zeta function of L (if any). Then, for all x such that $\log x \gg n_L(\log d_L)^2$,*

$$\pi_C(x, L/K) = \frac{|C|}{|G|}\mathrm{Li}(x) + O\left(\frac{|C|}{|G|}\mathrm{Li}(x^\beta) + |\tilde{C}| x \exp\left\{-c n_L^{-1/2} \log^{1/2} x\right\}\right),$$

where c is a positive absolute constant, and $|\tilde{C}|$ is the number of conjugacy classes in C.

(ii) *Assuming the GRH for the Dedekind zeta function of the number field L, we have that*

$$\pi_C(x, L/K) = \frac{|C|}{|G|}\mathrm{Li}(x) + O\left(x^{1/2}|C| n_K \log\left(M(L/K)x\right)\right).$$

We now apply Theorem 3.1 to the torsion fields of elliptic curves.

Theorem 3.2. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication, and let $L_n, C(n)$ and $G(n)$ be as defined above. Assuming the GRH for the Dedekind zeta function of the number fields L_n, we have that*

(i) *Let d be a square-free integer such that $(d, M_E) = 1$. Then,*

$$\pi_{C(d)}(x, L_d/\mathbb{Q}) = \left(\prod_{\ell | d} \frac{\ell^2 - 2}{(\ell - 1)(\ell^2 - 1)} \right) \mathrm{Li}(x) + O\left(d^3 x^{1/2} \log (d N_E x) \right).$$

(ii) *Let ℓ be a prime such that $\ell \nmid M_E$. Then,*

$$\pi_{C(\ell^2)}(x, L_{\ell^2}/\mathbb{Q}) = \frac{\ell^3 - \ell - 1}{\ell^2(\ell^2 - 1)(\ell - 1)} \mathrm{Li}(x) + O\left(\ell^6 x^{1/2} \log (\ell N_E x) \right).$$

It was noticed by Serre [18] that one can improve significantly the error term of Theorem 3.1.(ii) (basically replacing $|C|$ with $|C|^{1/2}$) by writing the characteristic functions of the conjucacy classes C in terms of the irreducible characters of G, and then working with the Artin's L-functions associated with those characters. Further applications can be found in [16], [5] and in [20] for the present application. For the convenience of the reader, we summarize in the next two theorems the main features of the approach, and how it can be applied in our case.

We first define some notation. For each character χ of G, let $L(s, \chi)$ be the Artin L-function associated to χ. If G is an abelian group, the Artin L-functions of L/K corresponds to Hecke L-functions, and are then analytic functions of the complex plane. In general, we have

Conjecture 3.3 (Artin's conjecture)**.** *Let χ be an irreducible non-trivial character of G. Then, $L(s, \chi)$ is analytic in the whole complex plane.*

We will write the improvement of Theorem 3.1 under the θ-hypothesis for the zeros of the L-functions in the critical strip, where $1/2 \leqslant \theta < 1$, and not the full Riemann Hypothesis, which allows us to obtain an improvement of the results of [20] under a weaker hypothesis.

Hypothesis 3.4 (θ-hypothesis)**.** *Let $L(s)$ be a Dedekind zeta function, or an Artin L-function satisfying Artin's conjecture. Let $1/2 \leqslant \theta < 1$. Then $L(s)$ is non-zero for $\Re\mathrm{e}\, s > \theta$.*

Let φ be a class function on G, i.e. a function which is invariant under conjugation. Define

$$\pi_\varphi(x, L/K) := \sum_{\substack{N\mathfrak{p} \leqslant x \\ \mathfrak{p} \text{ unramified}}} \varphi(\sigma_\mathfrak{p}).$$

If C is a conjugacy class (or a union of conjugacy classes) in G, and 1_C is its characteristic function, then $\pi_{1_C}(x, L/K) = \pi_C(x, L/K)$ as defined above.

To define $\tilde{\pi}_\varphi(x, L/K)$, we need to extend the definition of the Artin symbol $\sigma_\mathfrak{p}$ at the ramified primes $\mathfrak{p}$. This is done in [18, Section 2.5], and we refer the reader to this paper. Then,

$$\tilde{\pi}_\varphi(x, L/K) = \sum_{N\mathfrak{p}^m \leqslant x} \frac{1}{m} \varphi(\sigma_\mathfrak{p}^m),$$

where the sum runs over all pairs of primes $\mathfrak{p}$ of K and integers $m \geqslant 1$ such that $N\mathfrak{p}^m \leqslant x$. With this definition, if $\varphi = \chi$ is a character of G and $L(s, \chi)$ is the Artin L-function of χ with

$$\log L(s, \chi) = \sum_{n=1}^{\infty} a_n(\chi) n^{-s},$$

then

$$\tilde{\pi}_\chi(x, L/K) = \sum_{n \leqslant x} a_n(\chi).$$

Then, $\tilde{\pi}_\varphi(x, L/K)$ has the following two important properties.

Lemma 3.5. [18, Propostion 7] *Under the previous notation, we have*

$$\pi_\varphi(x, L/K) = \tilde{\pi}_\varphi(x, L/K) + O\left(\sup_{g \in G} |\varphi(g)| \left(\frac{1}{|G|} \log d_L + n_K x^{1/2}\right)\right).$$

Lemma 3.6. [18, Propostion 8] *Let H be a subgroup of G, φ_H a class function on H and $\varphi_G = \mathrm{Ind}_H^G(\varphi_H)$. Then*

$$\pi_{\varphi_G}(x, L/K) = \tilde{\pi}_{\varphi_H}(x, L/L^H).$$

Proof. This follows from the invariance of the Artin L-functions of induced characters. □

Using lemmas 3.5 and 3.6, we deduce that

Theorem 3.7. *Let L/K be a Galois extension of number fields with Galois group G. Let H be a subgroup of G and C a conjugacy class in G such that $C \cap H \neq \emptyset$. Let C_H be the union of conjucacy classes in H generated by $C \cap H$. Then*

$$\begin{aligned}\pi_C(x, L/K) = {} & \frac{|H|}{|G|}\frac{|C|}{|C_H|}\pi_{C_H}(x, L/L^H) \\ & + O\left(\frac{|C|}{|C_H||G|}\log d_L + \frac{|H|}{|G|}\frac{|C|}{|C_H|}[L^H : \mathbb{Q}]x^{1/2} + [K : \mathbb{Q}]x^{1/2}\right).\end{aligned}$$

Proof. Let φ be the class function on G induced from C_H. It is easy to see that

$$\varphi = \mathrm{Ind}_H^G(1_{C_H}) = \frac{|G|}{|H|}\frac{|C_H|}{|C|}1_C,$$

and by Lemma 3.6

$$\tilde{\pi}_{C_H}(x, L/L^H) = \frac{|G|}{|H|}\frac{|C_H|}{|C|}\pi_C(x, L/K).$$

Using Lemma 3.5 to bound the difference between π and $\tilde{\pi}$, we get the result. □

The second piece needed for the improved Chebotarev Density Theorem is an estimate for $\pi_C(x, L/K)$ in the case that G has a normal subgroup H with the property that the Artin L-functions of G/H satisfy Artin's conjecture and the θ-hypothesis. For $\theta = 1/2$, the following theorem is Proposition 3.12 from [16].

Theorem 3.8. *Let D be a non-empty union of conjugacy classes in G and let H be a normal subgroup of G such that for all Artin L-functions attached to characters of $G/H \simeq \mathrm{Gal}(L^H/K)$, the Artin conjecture and the θ-hypothesis hold. Suppose also that $HD \subseteq D$. Then,*

$$\pi_D(x, L/K) = \frac{|D|}{|G|}\mathrm{Li}(x) + O\bigg(\left(\frac{|D|}{|H|}\right)^{1/2} x^\theta n_K \log\big(M(L/K)x\big)\bigg).$$

We now apply the last two theorems to get an improvement to Theorem 3.2. Let E be an elliptic curve without complex multiplication, let $\ell \nmid M_E$, and let $L_\ell/\mathbb{Q}$, $G(\ell)$ and $C(\ell)$ be as defined above. Let $B(\ell) \subset G(\ell)$ be the subgroup of Borel matrices. Let $C_B(\ell)$ be the union of conjugacy classes generated by $B(\ell) \cap C(\ell)$. Applying Theorem 3.7, we get

$$\pi_{C(\ell)}(x, L_\ell/\mathbb{Q}) = \frac{|B(\ell)|}{|G(\ell)|}\frac{|C(\ell)|}{|C_B(\ell)|}\pi_{C_{B(\ell)}}\big(x, L_\ell/L_\ell^{B(\ell)}\big) + O\left(\ell \log\left(\ell N_E\right) + \ell x^{1/2}\right) \tag{3.1}$$

using the bounds of [18, Section 1.4] for $\log d_L$.

Let $U(\ell) \subset B(\ell)$ be the subgroup of unipotent matrices. It is easy to see that $U(\ell)$ is a normal subgroup of $B(\ell)$, and that $B(\ell)/U(\ell)$ is the abelian group of diagonal matrices over $\mathbb{F}_\ell$. Artin's conjecture then holds for all L-functions of $L_\ell^{U(\ell)}/L_\ell^{B(\ell)}$, and we apply Theorem 3.8 with $G = B(\ell)$, $H = U(\ell)$ and $D = C_B(\ell)$ under the θ-hypothesis for the appropriate L-functions. This gives

$$\pi_{C_{B(\ell)}}\big(x, L_\ell/L_\ell^{B(\ell)}\big) = \frac{|C_B(\ell)|}{|B(\ell)|}\mathrm{Li}(x) + O\left(\ell^{3/2} x^\theta \log\left(\ell N_E x\right)\right). \tag{3.2}$$

We are now ready to state the improvement to Theorem 3.2. In the next theorem, all error terms depend on the elliptic curve E. We remark that we need a version of the Cheboratev Density Theorem in the extension L_n where n is not necessarily co-prime to M_E in order to sieve the sequence of (2.8).

Theorem 3.9. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Assuming the θ-hypothesis for the Dedekind zeta functions of the number fields $L_n/\mathbb{Q}$, we have*

(i) *Let d, m be square-free integers such that $(d, M_E) = 1$ and $m \mid M_E$. Then,*

$$\pi_{C(dm)}(x, L_{dm}/\mathbb{Q}) = \frac{|C(m)|}{|G(m)|}\left(\prod_{\ell \mid d} \frac{\ell^2 - 2}{(\ell-1)(\ell^2-1)}\right)\mathrm{Li}(x) + O_E\left(d^{3/2} x^\theta \log\left(dx\right)\right).$$

(ii) *Let ℓ be a prime such that $\ell \nmid M_E$. Then,*

$$\pi_{C(\ell^2)}(x, L_{\ell^2}/\mathbb{Q}) = \frac{\ell^3 - \ell - 1}{\ell^2(\ell^2-1)(\ell-1)}\mathrm{Li}(x) + O_E\left(\ell^3 x^\theta \log\left(\ell x\right)\right).$$

Proof. The proof of (i) with $d = \ell$ and $m = 1$ follows directly by replacing (3.2) in (3.1), and the general case of (i) follows by applying the same reasoning as above to the extension $L_{dm}/\mathbb{Q}$ with Galois group $G(dm) \simeq G(m) \times \prod_{\ell \mid d} \mathrm{GL}_2(\mathbb{F}_\ell)$. The proof of (ii) follows similarly using $G(\ell^2) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$. □

4. Greaves' weighted sieve and proof of Theorem 1.1

We first recall the simplified version of Greaves' weighted sieve of dimension 1, i.e. taking $E = V$ and $T = U$ in [8, Theorem A].

Let $\mathcal{A}$ be a finite sequence of integers and $\mathcal{P}$ a set of prime numbers. Let $\mathcal{B} = \mathcal{B}(\mathcal{P})$ denote the set of all positive square-free 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

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

such that

(i) the "remainders"

$$r(\mathcal{A}, d) := |\mathcal{A}_d| - \frac{w(d)}{d} X \qquad (d \in \mathcal{B}) \tag{4.1}$$

are small on a average over the divisors d of

$$P(z) := \prod_{p<z,\, p\in\mathcal{P}} p; \tag{4.2}$$

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

$$(\Omega_1) \qquad \Bigg| \sum_{\substack{z_1 \leqslant p < z_2 \\ p \in \mathcal{P}}} \frac{w(d)}{d} \log p - \log \frac{z_2}{z_1} \Bigg| \leqslant A \qquad (2 \leqslant z_1 \leqslant z_2).$$

Let U and V be two constants verifying

$$V_0 \leqslant V \leqslant \tfrac{1}{4}, \qquad \tfrac{1}{2} \leqslant U < 1, \qquad U + 3V \geqslant 1, \tag{4.3}$$

where $V_0 := 0.074368\cdots$. The simplified version of Greaves' weighted sieve function is given by

$$H(\mathcal{A}, D^V, D^U) := \sum_{a\in\mathcal{A}} \mathscr{G}\big((a, P(D^U))\big), \tag{4.4}$$

where $D \geqslant 2$ is the basic parameter of considered problem,

$$\mathscr{G}(n) := \Big\{1 - \sum_{p|n,\, p\in\mathcal{P}} \big(1 - \mathscr{W}(p)\big)\Big\}^+,$$

with $\big(\{x\}^+ := \max\{0,\, x\}\big)$, and

$$\mathscr{W}(p) := \begin{cases} \dfrac{1}{U-V}\left(\dfrac{\log p}{\log D} - V\right) & \text{if } D^V \leqslant p < D^U, \\ 0 & \text{otherwise.} \end{cases}$$

It is clear that

$$\begin{aligned} H(\mathcal{A}, D^V, D^U) &= \sum_{\substack{a\in\mathcal{A}\\(a,P(D^V))=1}} \mathscr{G}\big((a,P(D^U))\big) \\ &\geqslant \sum_{\substack{a\in\mathcal{A}\\(a,P(D^V))=1}} \Big\{1 - \sum_{p\mid(a,P(D^U))} \big(1-\mathscr{W}(p)\big)\Big\} \\ &= \sum_{\substack{a\in\mathcal{A}\\(a,P(D^V))=1}} \Big\{1 - \frac{U}{U-V} \sum_{\substack{D^V\leqslant p<D^U\\p\mid a}} \Big(1 - \frac{1}{U}\frac{\log p}{\log D}\Big)\Big\}. \end{aligned}$$

The last quantity is the sum of weights of Richert's logarithmic weighted sieve [7, Chapter 9, (1.2)]. Therefore, Greaves' weighted sieve is always better than Richert's sieve. It is worth pointing out that Richert's logarithmic weighted sieve would have been sufficient for our propose. In fact, for our choice of parameters, these two sieves coincide in the main term (comparing [7, Lemma 9.1] and (4.12) below). The greatest advantage of Greaves' weighted sieve is the bilinear form error term. In many applications (for example P_2 in short intervals, [22]), this advantage allows to take a larger level of distribution D to obtain better results. The actual version of Chebotarev Density Theorem does not allows us to profit of this advantage for our problem.

As usual, let $\Omega(n)$ and $\omega(n)$ denote the number of prime factors of n counted with and without multiplicity, respectively. Define

$$\omega(a,z) := \omega(a) + \sum_{\substack{p\geqslant z,\,\nu\geqslant 2\\p^\nu\mid a}} 1,$$

where the sum is taken over all pairs of primes $p \geqslant z$ and integers $\nu \geqslant 2$ such that p^ν divides a.

The function H will be used to detect the integers in $\mathcal{A}$ having few of prime factors in the following way.

Lemma 4.1. *Let E be an elliptic curve over $\mathbb{Q}$ and let*

$$\begin{aligned} \mathscr{A} &:= \{|E(\mathbb{F}_p)| : p \leqslant x,\ (|E(\mathbb{F}_p)|, M_E) = 1\}, \\ \mathscr{P} &:= \{p : p \nmid M_E\}. \end{aligned}$$

If there are real positive constants $U, V, \xi, x_0(E), B$ and positive integer r such that (4.3) holds and for $x \geqslant x_0(E)$,

$$\max_{a\in\mathscr{A}} a \leqslant D^{rU+V}, \tag{4.5}$$

$$\sum_{D^V\leqslant p<D^U} |\mathscr{A}_{p^2}| \ll_E \frac{x}{(\log x)^3}, \tag{4.6}$$

$$H\big(\mathscr{A}, D^V, D^U\big) \geqslant B\frac{C_E^{\text{twin}} x}{(\log x)^2}, \tag{4.7}$$

where $D := x^{\xi}$, then we have

$$\big|\{p \leqslant x : (|E(\mathbb{F}_p)|, M_E) = 1,\ \Omega(|E(\mathbb{F}_p)|) \leqslant r\}\big| \geqslant \{B + o(1)\}\frac{C_E^{\mathrm{twin}}x}{(\log x)^2} \tag{4.8}$$

for $x \geqslant x_0(E)$.

Proof. Since $\mathscr{W}(p) \leqslant 1$, we have $0 \leqslant \mathscr{G}(n) \leqslant 1$ for all $n \in \mathbb{N}$. Thus hypothesis (4.7) allows us to write

$$\begin{aligned}\sum_{\substack{a\in\mathscr{A}\\ (a,P(D^V))=1, \mathscr{G}((a,P(D^U)))>0}} 1 &\geqslant \sum_{\substack{a\in\mathscr{A}\\ (a,P(D^V))=1}} \mathscr{G}\big((a,P(D^U))\big)\\ &= H\big(\mathscr{A}, D^V, D^U\big)\\ &\geqslant B\frac{C_E^{\mathrm{twin}}x}{(\log x)^2}\end{aligned} \tag{4.9}$$

for $x \geqslant x_0(E)$.

For each $a \in \mathscr{A}$ counted in the sum on the left-hand side of (4.9), we have $(a, P(D^V)) = 1$ and

$$\begin{aligned}0 &< \Big\{1 - \sum_{p|a,\ p<D^U} \big(1 - \mathscr{W}(p)\big)\Big\}^+\\ &= 1 - \frac{1}{U-V}\sum_{p|a,\ p<D^U}\bigg(U - \frac{\log p}{\log D}\bigg).\end{aligned}$$

This and hypothesis (4.5) imply

$$\begin{aligned}0 &< U - V - \sum_{p|a, p<D^U}\bigg(U - \frac{\log p}{\log D}\bigg)\\ &\leqslant U - V - \sum_{p|a}\bigg(U - \frac{\log p}{\log D}\bigg) - \sum_{p\geqslant D^U,\ \nu\geqslant 2,\ p^\nu|a}\bigg(U - \frac{\log p}{\log D}\bigg)\\ &\leqslant U - V - U\omega(a, D^U) + \frac{\log a}{\log D}\\ &\leqslant U - V - U\omega(a, D^U) + rU + V\\ &= U\big(r + 1 - \omega(a, D^U)\big).\end{aligned}$$

Hence for such a we have $(a, P(D^V)) = 1$ and $\omega(a, D^U) \leqslant r$. Combining this with (4.9), we obtain

$$\begin{aligned}&\big|\{p \leqslant x : (|E(\mathbb{F}_p)|, M_E) = (|E(\mathbb{F}_p)|, P(D^V)) = 1,\ \omega\big(|E(\mathbb{F}_p)|, D^U\big) \leqslant r\}\big|\\ &\geqslant B\frac{C_E^{\mathrm{twin}}x}{(\log x)^2}.\end{aligned} \tag{4.10}$$

When $(|E(\mathbb{F}_p)|, P(D^V)) = 1$, we have $\omega\big(|E(\mathbb{F}_p)|, D^U\big) = \Omega(|E(\mathbb{F}_p)|)$ unless a is divisible by the square of a prime p such that $D^V \leqslant p < D^U$ and the required result (4.8) now follows from (4.10) and hypothesis (4.6). □

Now we are ready to prove Theorem 1.1.

In Lemma 4.1, take

$$r = r(\theta) := \left[\frac{18+2\theta}{5(1-\theta)}\right] + 1, \quad \xi = \frac{2(1-\theta)}{5}(1-\varepsilon), \quad U = \frac{5}{8}, \quad V = \frac{1}{4}$$

where ε is an arbitrary small positive number. It is easy to see that condition (4.3) is satisfied. In order to verify (4.5), it is sufficient to show that $\xi(rU+V) > 1$, since a_p satisfies Hasse's bound $|a_p| < 2\sqrt{p}$. In view of the fact that ε is arbitrarily small, we have

$$\xi(rU+V) > \frac{2(1-\theta)}{5}(1-\varepsilon)\left(\left(\frac{18+2\theta}{5(1-\theta)} + \frac{8\varepsilon}{(1-\theta)(1-\varepsilon)}\right)\frac{5}{8} + \frac{1}{4}\right) = 1 + \varepsilon.$$

It remains to verify (4.6) and (4.7).

First Theorem 3.9(ii) allows us to deduce

$$\begin{aligned}\sum_{D^V \leqslant p < D^U} |\mathscr{A}_{p^2}| &\ll \sum_{D^V \leqslant p < D^U} \left(\frac{x}{p^2 \log x} + p^3 x^\theta \log x\right) \\ &\ll D^{-V} x + D^{4U} x^\theta \\ &\ll x^{1-\varepsilon(1-\theta)}\end{aligned}$$

for all $x \geqslant 3$. This shows that (4.6) is satisfied.

For d square-free with $(d, M_E) = 1$, we can write

$$\begin{aligned}|\mathscr{A}_d| &= \sum_{\substack{p \leqslant x \\ (|E(\mathbb{F}_p)|, M_E) = 1 \\ |E(\mathbb{F}_p)| \equiv 0 (\mathrm{mod}\ d)}} 1 \\ &= \sum_{m \mid M_E} \mu(m) \sum_{\substack{p \leqslant x \\ |E(\mathbb{F}_p)| \equiv 0 (\mathrm{mod}\ d) \\ |E(\mathbb{F}_p)| \equiv 0 (\mathrm{mod}\ m)}} 1 \\ &= \sum_{m \mid M_E} \mu(m) \sum_{\substack{p \leqslant x \\ |E(\mathbb{F}_p)| \equiv 0 (\mathrm{mod}\ dm)}} 1 \\ &= \sum_{m \mid M_E} \mu(m) \pi_{C(dm)}(x, L_{dm}/\mathbb{Q}).\end{aligned}$$

Using Theorem 3.9(i) and (2.10), we get that

$$\begin{aligned}|\mathscr{A}_d| &= \mathrm{Li}(x) \frac{|C(d)|}{|G(d)|} \sum_{m \mid M_E} \mu(m) \frac{|C(m)|}{|G(m)|} + O_E\left(|C(d)|^{1/2} x^\theta \log(dx)\right) \\ &= \mathrm{Li}(x) \frac{|C(d)|}{|G(d)|} \left(1 - \frac{|\Omega(M_E)|}{|G(M_E)|}\right) + O_E\left(d^{3/2} x^\theta \log(dx)\right).\end{aligned}$$

Thus we obtain

$$|\mathscr{A}_d| = \frac{w(d)}{d} X + r(\mathscr{A}, d) \tag{4.11}$$

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

$$w(d) = \frac{d|C(d)|}{|G(d)|} = \prod_{\ell | d} \frac{\ell(\ell^2 - 2)}{(\ell - 1)(\ell^2 - 1)}$$

and

$$X := \left(1 - \frac{|\Omega(M_E)|}{|G(M_E)|}\right) \mathrm{Li}(x), \qquad |r(\mathscr{A}, d)| \ll_E d^{3/2} x^{\theta} \log(dx).$$

Since

$$w(\ell) = 1 + \frac{\ell^2 - \ell - 1}{(\ell - 1)(\ell^2 - 1)},$$

conditions (A_0) and (Ω_1) are satisfied. Thus Theorem A of [8] is applicable. Denoting by γ the Euler constant and defining

$$V(D) := \prod_{\substack{p < D \\ p \in \mathscr{P}}} \left(1 - \frac{w(p)}{p}\right),$$

Theorem A of [8] allows us to write

$$\begin{aligned} H\big(\mathscr{A}, D^V, D^U\big) \geqslant \frac{2e^{\gamma} X V(D)}{U - V} \bigg\{ & U \log \frac{1}{U} + (1 - U) \log \frac{1}{1 - U} - \log \frac{4}{3} \\ & + \alpha(V) - V \log 3 - V\beta(V) + O\bigg(\frac{\log_3 D}{(\log_2 D)^{1/5}}\bigg)\bigg\} \\ & - (\log D)^{1/3} \bigg| \sum_{\substack{m < M \\ mn | P(D^U)}} \sum_{n < N} \alpha_m \beta_n r(\mathscr{A}, mn) \bigg| \end{aligned} \tag{4.12}$$

where M and N are any two real numbers satisfying

$$M > D^U, \qquad N > 1, \qquad MN = D$$

and α_m, β_n are certain real numbers satisfying $|\alpha_m| \leqslant 1, |\beta_n| \leqslant 1$. The functions $\alpha(V)$ and $\beta(V)$ are given by

$$\alpha(V) := \log \frac{1 - V}{(3/4)} - \int_4^{1/V} \left(\frac{2}{u} \log(2 - uV) + \log \frac{1 - 1/u}{1 - V}\right) \frac{\log(u - 3)}{u - 2} \, \mathrm{d}u,$$

$$\beta(V) := \log \frac{1 - V}{3V} - \int_4^{1/V} \left(\log(2 - uV) + \log \frac{1 - 1/u}{1 - V}\right) \frac{\log(u - 3)}{u - 2} \, \mathrm{d}u,$$

for $\frac{1}{6} \leqslant V \leqslant \frac{1}{4}$.

By using the prime number theorem, it follows that

$$\begin{aligned} V(D) &= \prod_{\ell \leqslant D,\, \ell \nmid M_E} \left(1 - \frac{|C(\ell)|}{|G(\ell)|}\right) \\ &= \prod_{\ell \leqslant D,\, \ell \nmid M_E} \left(1 - \frac{1}{\ell}\right) \prod_{\ell \leqslant D,\, \ell \nmid M_E} \left(1 - \frac{|C(\ell)|}{|G(\ell)|}\right)\left(1 - \frac{1}{\ell}\right)^{-1} \\ &= \prod_{\ell \leqslant D} \left(1 - \frac{1}{\ell}\right) \prod_{\ell \mid M_E} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell \leqslant D,\, \ell \nmid M_E} \left(1 - \frac{|C(\ell)|}{|G(\ell)|}\right)\left(1 - \frac{1}{\ell}\right)^{-1} \\ &\sim \frac{e^{-\gamma}}{\log D} \prod_{\ell \mid M_E} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell \nmid M_E} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right) \end{aligned} \tag{4.13}$$

as $D \to \infty$.

On the other hand, denoting by $\mu(d)$ the Möbius function, Theorem 3.9(ii) implies that

$$\begin{aligned} \Big| \sum_{\substack{m<M \\ mn \mid P(D^U)}} \sum_{n<N} \alpha_m \beta_n r(\mathscr{A}, mn) \Big| &\leqslant \sum_{d \leqslant D} \mu(d)^2 3^{\omega(d)} d^{3/2} x^\theta \log(dx) \\ &\ll x^\theta D^{5/2 + \varepsilon(1-\theta)/2} \\ &\ll x^{1 - \varepsilon(1-\theta)/2} \end{aligned} \tag{4.14}$$

since $D = x^\xi$ with $\xi = \frac{2}{5}(1-\theta)(1-\varepsilon)$.

Combining (4.12), (4.13), (4.14) and (2.5), we can find that

$$H\big(\mathscr{A}, D^V, D^U\big) \geqslant \big\{2J(\xi, U, V) + o(1)\big\} \frac{C_E^{\mathrm{twin}} x}{(\log x)^2}$$

with

$$J(\xi, U, V) := \frac{\alpha(V) - V\beta(V) - V\log 3 - U\log U - (1-U)\log(1-U) - \log(4/3)}{\xi(U - V)}.$$

Since $J(\xi, U, V)$ is continuous in (ξ, U) and $\alpha(\frac{1}{4}) = \beta(\frac{1}{4}) = 0$, a simple numerical computation shows that

$$\begin{aligned} 2J(\xi, U, V) &= 2J\bigg(\frac{2(1-\theta)}{5}, \frac{5}{8}, \frac{1}{4}\bigg) + O(\varepsilon) \\ &= \frac{1.32304\cdots}{1-\theta} + O(\varepsilon). \end{aligned}$$

This implies

$$H\big(\mathscr{A}, D^V, D^U\big) \geqslant \frac{1.32303}{1-\theta} \frac{C_E^{\mathrm{twin}} x}{(\log x)^2}$$

for $x \geqslant x_0(E, \theta)$. This completes the proof of Theorem 1.1. □

5. Selberg's linear sieve and proof of Theorem 1.3

We use the notation of Section 4. As usual, we write the sieve function

$$S(\mathscr{A}, \mathscr{P}, z) := |\{a \in \mathscr{A} : p \mid a \text{ and } p \in \mathscr{P} \Rightarrow p > z\}|.$$

Then in view of (2.7), we can write the following trivial inequality

$$\pi_E^{\mathrm{twin}}(x) \leqslant S(\mathscr{A}, \mathscr{P}, D^{1/2}) + O(D^{1/2}) \tag{5.1}$$

for all $x \geqslant 1$, where $D = x^{\xi}$ with $\xi = 2(1-\theta)(1-\varepsilon)/5$ as before, and the O-constant depends on the curve E.

Using Selberg's linear sieve [7, Theorem 8.3] with $q = 1$, it follows that

$$S(\mathscr{A}, \mathscr{P}, D^{1/2}) \leqslant XV(D^{1/2})\{F(2) + o(1)\} + \mathscr{R},$$

where

$$\begin{aligned} \mathscr{R} &:= \sum_{\substack{d<D \\ d \mid P(D^{1/2})}} 3^{\omega(d)} |r(\mathscr{A}, d)| \\ &\ll \sum_{d<D} \mu(d)^2 3^{\omega(d)} d^{3/2} x^{\theta} \log(dx) \\ &\ll x^{1-\varepsilon(1-\theta)/2}, \end{aligned}$$

using Theorem 3.9(i).

Since $F(2) = e^{\gamma}$, replacing D by $D^{1/2}$ in the asymptotic formula (4.13), we get that

$$\begin{aligned} XV(D^{1/2})F(2) &= C_E^{\mathrm{twin}} \frac{2\mathrm{Li}(x)}{\log x^{\xi}} \{1 + o(1)\} \\ &\leqslant \left(\frac{5}{1-\theta} + \varepsilon\right) \frac{C_E^{\mathrm{twin}} x}{(\log x)^2} \end{aligned}$$

for $x \geqslant x_0(E, \theta, \varepsilon)$.

Combining these estimates, we find that

$$S(\mathscr{A}, \mathscr{P}, D^{1/2}) \leqslant \left(\frac{5}{1-\theta} + \varepsilon\right) \frac{C_E^{\mathrm{twin}} x}{(\log x)^2} \tag{5.2}$$

for $x \geqslant x_0(E, \theta, \varepsilon)$. Theorem 1.3 now follows from (5.1) and (5.2). □

References

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

[2] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18** (1987), 2nd edition, 103pp.

[3] J.-R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176.

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

[5] A. C. Cojocaru & C. David, *Frobenius fields for Elliptic Curves*, American J. of Math. **130** (2008), no. 6, 1535–1560.

[6] F. Grupp & H.-E. Richert, *The functions of linear sieve*, J. Number Theory **22** (1986), no. 2, 208–239.

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

[8] H. Halberstam & H.-E. Richert, *A weighted sieve of Greaves' type, II*, in: Elementary and Analytic Theory of Numbers, Banach Center Publication **171** (1985), 183–215.

[9] H. Iwaniec & J. Jiménez Urroz, *Orders of CM elliptic curves modulo p with at most two primes*, preprint.

[10] J. Jiménez Urroz, *Almost Prime Orders of CM Elliptic Curves Modulo p*, in: Lecture Notes in Computer Science **5011**, Springer (2008), 74–87.

[11] N. Jones, *Almost all elliptic curves are Serre curves*, to appear, Transactions of the Amer. Math. Soc.

[12] N. Jones, *Primes p for which $\#E(\mathbb{F}_p)$ has only large prime factors.* Appendix to *Geometry and arithmetic of verbal dynamical systems on simple groups* by T. Bandman, F. Grunewald and B. Kunyavskii, preprint.

[13] 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.

[14] 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.

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

[16] M.-R. Murty, V.-K. Murty & N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), 253–281.

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

[18] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.

[19] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135-152.

[20] J. Steuding & A. Weng, *On the number of prime divisors of the order of elliptic modulo p*, Acta Arith. **117** (2005), no. 4, 341–352.

[21] J. Steuding & A. Weng, *Erratum: "On the number of prime divisors of the order of elliptic curves modulo p"* [Acta Arith. **117** (2005), no. 4, 341–352; MR2140162], Acta Arith. **119** (2005), no. 4, 407–408.

[22] J. Wu, *P_2 dans les petits intervalles*, in : Séminaire de Théorie des nombres, Paris 1989-1990 (D. Sinnou Ed.), Progress in Math. **102**, Birkhäuser (1992), 233–267.

[23] D. Zywina, *A refinement of Koblitz's conjecture*, preprint. arXiv:0909.5280.

[24] D. Zywina, *The large sieve and Galois representations*, preprint. arXiv:0812.2222.

[C. David] Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montréal, QC, H3G 1M8, Canada, and Institute for Advanced Study, Einstein Drive, Princeton, New Jersey, 08540, USA.

E-mail address: cdavid@mathstat.concordia.ca

[J. Wu] Institut Elie Cartan Nancy (IECN), Nancy-Université, CNRS, INRIA, Boulevard des Aiguillettes, B.P. 239, 54506 Vandœuvre-lès-Nancy, France, and School of Mathematical Sciences, Shandong Normal University, Jinan, Shandong 250100, China.

E-mail address: wujie@iecn.u-nancy.fr