ECM and the Elliott-Halberstam conjecture for quadratic fields

Razvan Barbulescu

RIGOROUS TIME BOUND FOR FACTORING WITH ELLIPTIC CURVES

RAZVAN BARBULESCU

Abstract. The complexity of the elliptic curve method of factorization (ECM) is proven under the celebrated conjecture of existence of smooth numbers in short intervals. In this work we tackle a different version of ECM which is actually much more studied and implemented, especially because it allows us to use ECM-friendly curves. In the case of curves with complex multiplication (CM) we replace the heuristics by rigorous results conditional to the Elliott-Halberstam (EH) conjecture. The proven results mirror recent theorems concerning the number of primes p such thar $p-1$ is smooth. To each CM elliptic curve we associate a value which measures how ECM-friendly it is. In the general case we explore consequences of a statement which translated EH in the case of elliptic curves.

1. Introduction

Many heuristics in cryptography assert that the proportion of primes (respectively smooth numbers) in an interval is unchanged when we restrict to a particular set of integers which is of interest. To be more precise, let $\Pi(x)$ be the set of primes less than x and, for a parameter y, let $\Psi(x,y)$ be the set of integers in $[1,x]$ which are y-smooth (or friable), i.e. such that all the prime factors are less than y. Then one studies if, for a set $A \subset \mathbb{N}$, the proportions $|A \bigcap \Pi(x)|/|A \bigcap [1,x]|$ (resp. $|A \bigcap \Psi(x,y)|/|A \bigcap [1,x]|$) is equivalent to the proportion $|\Pi(x)|/x$ (resp. $|\Psi(x,y)|/x$ uniformly on y). The most celebrated example is the precise version of the twin primes conjecture due to Hardy and Littlewood. Two other problems concern

- **P1:** the smoothness of $A_a = \{p+a : p \text{ prime}\}$, for a constant a; see [Wan18] and [LWX20] for the newest results, both of them are conditional on the Elliott-Halberstam conjecture;
- **P2:** the primality of $A_E = \{|E(\mathbb{F}_p)| : p \text{ prime }, p \nmid \Delta(E)\}$ where E is an elliptic curve with rational coefficients and $E(\mathbb{F}_p)$ is the reduction of E modulo p; see [Zyw11] for a review of the literature.

In this work we address a series of questions related to

- **P3:** the smoothness of the set A_E above.

We call

$$\psi_E(x,y) = |\{p \text{ prime} : |E(\mathbb{F}_p)| \text{ is } y\text{-smooth}\}|. \tag{1}$$

The main result of this work, Theorem 2, is a generalization of a theorem of Wu, Liu and Xi [LWX20], who studied problem **P1**, and it is conditional under the celebrated conjecture of Elliott and Halberstam (EH).

Conjecture 1 (parametric EH, [LWX20],[Pol16][1])**.** *Let $\delta(x)$ be a decreasing function such that*

$$(\log_2 x)/(2\log x) \leq \delta(x) < 1/2 \qquad (x \geq x_0).$$

Let K be either $\mathbb{Q}$ or an imaginary quadratic field of class number one and set

$$\Pi_K(x; c, a) = \{p \in \mathcal{O}_K, \ \textit{prime}, \| p \| \leq x, p \equiv a \pmod{c}\},$$

where $\| \cdot \|$ is the algebraic norm. Then for any fixed $a \in \mathbb{Z}$ and $A > 0$ we have

$$\sum_{\substack{q \leq x^{1-\delta(x)} \\ (q,a)=1}} \left| \pi_K(x; q, a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_A \frac{x}{(\log x)^A},$$

[1]Pollack stated the conjecture only in the case of constant δ

uniformly for $x \geq x_0$.

The technical conditions on δ have an interesting story : Halberstam formulated the conjecture for constant δ, H. L. Montgomery suggested that one could take $\delta(x) \to 0$ and finally Friedlander and Granville [FG92] showed that the conjecture fails if δ is less than a certain function of x. Our arguments show that the version of the conjecture with constant δ implies results with constant $(\log x)/(\log y)$. However for the cryptographic motivation explained in Section 2 we are interested in uniform results in x and y which allow to conduct numerical experiments and vary the two parameters independently.

Theorem 2. *Assume the parametric EH conjecture for a function $\delta(x)$. Let E be a elliptic curve with complex multiplication (CM) defined over Q. Set*

$$H = \left\{ (x,y) \in \mathbb{R}_+^2 : x^{\frac{\log_3 x}{\log_2 x}} \leq y \leq x \right\}.$$

For any $y \in [1,x]$ we set $u = \frac{\log x}{\log y}$. Then there exists a constant $\alpha(E)$ such that, as $x \to \infty$, we have the asymptotic development

$$\frac{\psi_E(x,y)}{\psi_E(x,\infty)} = \frac{\psi(xe^{\alpha(E)},y)}{\psi(xe^{\alpha(E)},\infty)} \left(1 + O\left(\frac{\log(u+1)^2}{(\log y)^2}\right)\right),$$

uniformly for $(x,y) \in H$, where $\alpha(E)$ is a constant.

This is a rigorous basis for a notion which is used in cryptography. Indeed, when changing the value of $\alpha(E)$ one obtains an error term which is larger than $O((\log(u+1))^2/(\log y)^2)$.

Corollary 3. *If E_1 and E_2 are two elliptic curves with $\alpha(E_1) < \alpha(E_2)$ then, for large enough x and y, uniformly for $(x,y) \in H$, we have*

$$\psi_{E_1}(x,y) > \psi_{E_2}(x,y),$$

In this case we say that E_1 is more ECM-friendly than E_2.

The second main question of this article concerns the proportion of smooth integers which contain at least one prime in a set whose density is known. In this work, the set of primes is one of the sets in problems **P1** and **P3**. For a set of primes Q and respectively $v > 0$ a parameter we set.

$$\begin{array}{rcl} \psi_Q(x,y) & = & \{n \in \psi(x,y) : \forall p \mid n, p \in Q\}. \\ \Psi_v(x,y) & = & \Psi_Q(x,y) \quad \text{for } Q = \{p \text{ prime } : P^-(p-1) < y^{1/v}\}. \end{array} \tag{2}$$

Here and in the sequel $P^-(n)$ and $P^+(n)$ are the smallest and largest prime factors of n.

Theorem 4. *Let K be a number field. Let (x,y,z) be three positive integers such that $u := \frac{\log x}{\log y}$ and $v := \frac{\log y}{\log z}$ are as in the domain*

$$\Delta : \quad u \leq \frac{x}{\log_2 x} \text{ and } v \leq \frac{\log_2 x}{\log_3 x}.$$

Then we have

$$\psi_v(x,y)/x \quad \geq \quad \rho(v)\rho(u)(1+o(1)),$$

uniformly on Δ.

The second part of the article is heuristic. In one direction, we prove that if one extends Theorem 4 to a wider domain then one can eliminate the heuristics in an algorithms which uses ECM as a building block. In a second direction, we prove that a heuristic assumption due to Pollack [Pol16] implies a statement similar to Theorem 2 for all elliptic curves.

The article is organized as follows. In Section 2 we give the cryptographic motivation and prove a complexity result under the assumption of a stronger version of Theorem 4. After the background in Section 3, we prove the main theorem in Section 4. In Section 5 we prove

Theorem 4. In these two sections the results are conditional under the EH conjecture. We then continue with heuristic results in Section 6 which treats the case of non-CM elliptic curves. In Section 7 we recognize $\alpha(E)$ as a quantity which is already known in cryptography.

2. Cryptographic motivation

The set A_E plays a key role in the elliptic curve method (ECM) of factorization [Len87]. Let E be an elliptic curve defined over $\mathbb{Q}$ and P a point $P = (x_P : y_P : z_P) \in E(\mathbb{Q})$. For an integer N we set $B(N) = \lfloor L_N(1/2, 1/\sqrt{2}) \rfloor$, where

$$L_N(\alpha, c) = \exp\left(c(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right). \tag{3}$$

Next we set $M(N) = (B!)^{\log_2 N}$. Note that for any integer N such that $\gcd(x_P, y_P, z_P, N) = 1$ and $\gcd(N, \Delta(E)) = 1$, E has good reduction modulo any unknown prime factor p of N and $\bar{P} := (x_P : y_P : z_P) \bmod p$ belongs to $E(\mathbb{F}_p)$. Running ECM for E and N consists in computing $Q = (x_Q, y_Q, z_Q) := [M]P \bmod N$, i.e. one uses the cord-and-tangent formulae and reduces the coordinates modulo N, if two points are different modulo N one uses the formula for adding two distinct points. We claim that, if the order $|E(\mathbb{F}_p)|$ is B-smooth for an unknown prime factor p, then $\gcd(z_Q, N)$ is a multiple of p. Indeed, if the points involved in the double-and-add method were all distinct not only modulo N but also modulo p, then Q is the neutral element, so $z_Q \equiv 0 \pmod p$. If one used a wrong formula because two points were distinct modulo N but equal modulo p, then $z_Q \equiv y_Q \equiv z_Q \equiv 0 \pmod p$. In both cases ECM finds a multiple of p and a carefull analysis shows that the probability that the result is exactly p is $1 - o(1)$ (see [Len87]). In case of failure one starts over with another curve.

Heuristically, running randomly chosen elliptic curves corresponds to doing independent trials and hence the expected number of trials is the inverse of the proportion studied in this work (see problem **P3**). The version of ECM presented above is a heuristic version of ECM, due to P. Montgomery, that is intensively studied since 1985 and made possible record computations and improvements [Mon87]. Two years after having presented the sketch of his algorithm, Lenstra [Len87] published the full proof in which he eliminated all the heuristics except for the one concerning the density of smooth numbers in short intervals (see [Gra08]), and this is the version which serves as a rigorous analysis of the algorithm. Lenstra's version differs from ours because it uses elliptic curves which are defined $\mathbb{F}_p$ but cannot be lifted over $\mathbb{Q}$. In this work we study rigorously P. Montgomery's version : E is defined over $\mathbb{Q}$ and is used to factor many integers[2] so that problem **P3** is relevant.

Since Theorem 2 eliminates the heuristics about $\Psi_E(x, y)$, it allows us to eliminate heuristics in the algorithms where ECM is used. A step of the number field sieve (NFS), called splitting, considers a prime q, a generator g of $(\mathbb{Z}/q\mathbb{Z})^*$ and a second element $h \in (\mathbb{Z}/q\mathbb{Z})^*$. One factors with ECM the integers $g^e h \bmod q$ for values of $e \in [1, q-1]$ which are uniformly randomly chosen until one of them is y-smooth for $y = L_x(\frac{2}{3}, c)$ for an absolute constant c (see Algorithm 1). Here we used the notation of Equation (3). The statement of the main theorem, if it remains true when the domain Δ is extended, eliminates the heuristics in the splitting step.

Theorem 5. *Assume that Theorem 2 can be extended to the domain* $(x, y = x^{1/u}, z = y^{1/v})$ *below :*

$$\Delta' : \quad u \le c_u \frac{(\log x)^{1/3}}{(\log_2 x)^{1/3}} \text{ and } v \le c_v \frac{(\log x)^{1/3}}{(\log_2 x)^{1/3}},$$

for two constants $c_u, c_v \ge 3^{1/3}$*. Then, with a constant probability, Algorithm 1 on input* ℓ *ends in a time* $L_\ell(1/3, 3^{1/3})^{1+o(1)}$.

[2]The record factorizations of RSA moduli done with CADO-NFS use ECM as a building block. For example, the default parameters use a dozen elliptic curves to factor billions of integers

Algorithm 1: Splitting step in discrete logarithm NFS: main part

Input: a prime q and two integers $g, h \in [1, q-1]$ such that g is a generator
Output: an integer e such that $P^-(g^e h \bmod q) < y$ with $y = L_q(\frac{2}{3}, \frac{1}{c_u})$

1: $E : y^2 = x^3 + x^2 - 3x + 1$, $P = (-1 : 2 : 1) \in E$
2: $B \leftarrow L_q(\frac{1}{3}, \frac{1}{c_u c_v})$; $m \leftarrow B!$
3: **repeat**
4: $\quad e \leftarrow$ random integer in $[1, q-1]$
5: $\quad N \leftarrow g^e h \bmod q$
6: $\quad Q(x_Q : y_Q : z_Q) \leftarrow [m]P \pmod N$
7: **until** $g := \gcd(z_Q, N) \neq 1$

Proof. We set the value of the constants : $c_v = c_u = 3^{1/3}$. The cost of line 6 is $O(\log_2 m)$ by double-and-add exponentiation. This is

$$\text{time(line 6)} = O(\log m) = O(B \log B) = B^{1+o(1)} = L_\ell(1/3, 1/(c_u c_v)).$$

Since e is randomly chosen with uniform probability, the number of executions of loop in lines 3-7 is with a constant probability less than a constant times the inverse of the success probability. We saw in this section that the condition in line 7 is satisfied if, for all prime factors p of N, the order $|E(\mathbb{F}_p)|$ is B-smooth. We set $u = c_u \frac{\log q}{\log y}$ and $v = c_v \frac{\log y}{\log B}$ and conclude that the number of executions of the loop is $q/\Psi_v(q, y)$.

Since u and v are in Δ', the assumption states that we have $q/\psi_v(q, y) \geq (\rho(v)\rho(u))(1+o(1))$. We inject the values of v and u:

$$\begin{aligned} \log(\rho(v)\rho(u)) &= (-1 + o(1)) \quad \cdot (u \log u + v \log v) \\ &= (-1 + o(1)) \quad \cdot \left(\tfrac{c_u + c_v}{3} (\log q)^{1/3} (\log_2 q)^{2/3}\right). \end{aligned}$$

Hence the loop is executed at most $L_q(1/3, \frac{c_u+c_v}{3})^{1+o(1)}$ times. When we multiply this by the cost $B^{1+o(1)} = L_q(1/3, \frac{1}{c_u c_v})^{1+o(1)}$, we find

$$\text{time(Algorithm 1)} = L_q(1/3, c),$$

where $c = \frac{1}{c_u c_v} + \frac{c_u + c_v}{3} = 3^{1/3}$.

□

Remark 6. *(i) Since Algorithm 1 uses a single curve E, with an explicitly given rational point P, we avoid heuristics about the rank of elliptic curves.*

(ii) At a heuristic level, the complexity remains the same if one searches for y-smooth integers. In that case, after line 7, one factors N/g with ECM and then goes back to line 3. Under the heuristic assumption that different elliptic curves are independent, the probability that $P^-(N/g) < y$ is negligible with respect to the probability that $P^-(N) < y$. Hence the full algorithm has a complexity equal to that of Algorithm 1 raised to the power $1 + o(1)$.

3. Background

In the case of an elliptic curve with CM, problem **P3** is a simple generalization of problem **P1** from $\mathbb{Q}$ to an imaginary quadratic field of class number one, as established by the following result.

We use the notation $\| \cdot \|$ for the number field norm. We also set

$$\psi_K(x, y; c, a) = |\{\pi \in \Pi_K(x; c, a), P^+(\| \pi - 1 \|) < y\}|. \tag{4}$$

Lemma 7 (CM theory, see [RS09] Th 1.1)**.** *For any elliptic curve E with CM by an order of K, there exists $a, c \in \mathcal{O}_K$ such that, for any prime ℓ split in K, $|E(\mathbb{F}_\ell)| = \| \pi - 1 \|$, where π is unique such that $\| \pi \| = \ell$ and $\pi \equiv a \pmod c$.*

In particular

$$\psi_E(x, y) = \psi_K(x, y; c, a)$$

for two constants a and c depending on E.

We follow the strategy of Wang [Wan18], so we assume Conjecture 1. Since classical EH conjecture is a strengthening of the statement of the Vinogradov-Bombieri (BV) theorem, the number field version of EH is the same strengthening of the number field BV, which due to Huxley. In the case of imaginary quadratic fields of class number one, the statement of Conjecture 1 can be found in [Pol16], but we allow δ to be non-constant.

An important ingredient of Wang's proof is the linear sieve. Let $\mathcal{A} \subset \mathcal{O}_K$ be a finite set, $\mathcal{P} \subset \mathcal{O}_K$ a set of primes, $z \geq 2$ a real and $d \in \mathcal{O}_K$ a square-free integer whose prime factors belong to $\mathcal{P}$. Call $\mathcal{A}_d = \mathcal{A} \bigcap d\mathcal{O}_K$ and $P_{\mathcal{P}}(z) = \prod_{\|p\|<z, p\in\mathcal{P}} \pi$. Let X be an approximation of $|\mathcal{A}|$ and w a multiplicative function such that $0 < w(p) < \| p \|$ and, for any $d \mid P_{\mathcal{P}}(z)$,

$$|\mathcal{A}_d| = \frac{w(d)}{\| d \|} X(1 + o(1)).$$

We set $r(\mathcal{A}, d) = |\mathcal{A}_d| - \frac{w(d)}{\|d\|} X$. We make some more notations.

$$\begin{aligned} S(\mathcal{A}; \mathcal{P}, z) &= |\{a \in \mathcal{A} : (a, P_{\mathcal{P}}(z)) = 1\}|, \\ V(z) &= \prod_{p\in\Pi_K(z)} (1 - \tfrac{w(p)}{\|p\|}). \end{aligned} \tag{5}$$

Lemma 8 (Rosser-Iwaniec [Iwa80])**.** *Assume that there exists $K \geq 2$ such that*

$$\prod_{u\leq\|p\|<v} \left(1 - \frac{w(p)}{p}\right)^{-1} \leq \frac{\log v}{\log u} \left(1 + \frac{K}{\log u}\right)$$

for all $v > u \geq 2$. For any $D \geq z \geq 2$ one has

$$S(\mathcal{A}; \mathcal{P}, z) \ll XV(z) + \sum_{\|d\|<D, d|P(z)} |r(\mathcal{A}, d)|.$$

We finish the section with a trilogy of results about asymptotic developments of the number of smooth elements in various sets of integers. The equivalent of $\psi_K(x, y)$ is known since Hildebrand's work but the error term was made explicit by Scourfield.

Theorem 9 ([Sco04])**.** *Let K be an imaginary quadratic field. Then, uniformly on H, one has*

$$\psi_K(x, y) = \lambda_K x \left(\rho(u) + \frac{\rho'(u)}{\log y}(\alpha_K + o(1))\right),$$

where λ_K is the residue of ζ_K and $\alpha_K = L'(1, \chi)/L(1, \chi)$ for χ the non-trivial character of K.

The result was generalized so that ζ_K was replaced by a large class of Dedekind series of the form $Z(s)G(s)$ where Z is a product of zeta functions with positive exponents and G a well behaved function (including holomorphic functions). The following particular case is sufficient for our applications.

Theorem 10 (Theorem 1.1 in [HTW08], case $Z = \zeta$, G holomorphic)**.** *Let h be an arithmetic function whose Dedekind series $\mathcal{H}(x) = \sum_n \frac{h(n)}{n^s}$ is meromorphic with a simple pole at 1. Let a_0 and a_1 be such that the Laurent expansion of $\mathcal{H}$ at 1 is $\mathcal{H}(s) = a_0/(s-1) + a_1 + O(s-1)$. Then*

$$\sum_{\substack{n\leq x \\ P^-(n)>y}} h(n) = x\rho(u) \left(a_0 + a_1 \frac{\log(u+1)}{\log y} + O\left(\frac{(\log(u+1))^2}{(\log y)^2}\right)\right),$$

uniformly on $(\log x)^{1+\epsilon} \leq y \leq x$ for any fixed $\epsilon > 0$.

Finally, one proved a similar result for $Z = \zeta^{-1}$, the Dedekind series of μ.

Lemma 11 ([LT15]). *Let μ be the Möbius function and let $P^-(n)$ denote the least prime factor of n with the convention $P^-(1)=\infty$. For any $\epsilon>0$, we have*

$$\sum_{\substack{n\leq x\\ P^-(n)>y}}\frac{\mu(n)}{n}=\left\{1+O_\epsilon\left(\frac{\log(u+1)}{\log y}\right)\right\}\rho(u)+O_\epsilon(\exp(-(\log y)^{\frac{3}{5}-\epsilon}))$$

uniformly in $x\geq 2$ and $\exp\{(\log x)^{\frac{2}{5}+\epsilon}\}\leq y\leq x$, where $u=(\log x)/\log y$.

See [dlBF20] for a results which eliminates the error term $O_\epsilon(\frac{\log(u+1)}{\log y})$.

4. Main theorem

Proof of Theorem 2. By Lemma 7 we have

$$\begin{aligned}\psi_E(x,y) &= |\{p \text{ split}, P^+(|E(\mathbb{F}_p)|)<y)\}|+|\{p \text{ inert}, P^+(|E(\mathbb{F}_p)|)<y)\}|+O(1)\\ &= \psi_K(x,y;c,a)+|\{p \text{ inert} : P^+(p+1)<y\}|+O(1),\end{aligned}$$

for two constants $a,c\in\mathcal{O}_K$ (see the notation (4)).

The second term of the right member is treated by Wang [Wan18]. His proof applies directly in the case of cyclotomic fields K and can be adapted in the other cases:

$$|\{p \text{ inert} : P^+(p+1)<y\}|=(1+o(1))\rho(u)\frac{\pi(x)}{2}.$$

Hence, it remains to prove an equivalent for $\psi_K(x;c,a)$.

We let $\delta(x)$ be as in Conjecture 1 and let y be such that $u=O(\frac{\log_2 x}{\log_3 x})$. This is such that

$$\frac{\mathrm{Li}(x)}{(\log x)^{1/2}}=\psi_E(x,y)\rho(u)\cdot o(\varepsilon(x,y)). \tag{6}$$

Hence, in the following the terms $O(\frac{1}{(\log x)^{1/2}})$ are negligible.

We use an inclusion-exclusion principle to write

$$\psi_K(x,y;c,a)=\sum_{\substack{q\in\mathcal{O}_K\\ P^-(\|q\|)>y}}\mu(q)\pi_K(x;qc,a)=S_1+S_2, \tag{7}$$

where

$$\begin{aligned}S_1 &= \sum_{\substack{q\in\mathcal{O}_K\\ \|q\|\leq x^{1-\delta(x)}\\ P^-(\|q\|)>y}}\mu(q)\pi_K(x;qc,a)\\ S_2 &= \sum_{\substack{q\in\mathcal{O}_K\\ \|q\|> x^{1-\delta(x)}\\ P^-(\|q\|)>y}}\mu(q)\pi_K(x;qc,a).\end{aligned}$$

We write $S_1=S_1'+S_1''$ with

$$\begin{aligned}S_1' &= \frac{\mathrm{Li}(x)}{\varphi(c)}\sum_{\substack{q\in\mathcal{O}_K\\ \|q\|\leq x^{1-\delta(x)}\\ p^-(\|q\|)>y}}\frac{\mu(q)}{\varphi(q)},\\ S_1'' &= \sum_{\substack{q\in\mathcal{O}_K\\ \|q\|\leq x^{1-\delta(x)}\\ p^-(\|q\|)>y}}\mu(q)r(x,qc)\qquad \text{where } r(x,qc)=(\pi_K(x;qc,a)-\tfrac{\mathrm{Li}(x)}{\varphi(cq)}).\end{aligned}$$

In step $1'$ we show that $S_1'=\frac{\mathrm{Li}(x)}{\varphi(c)}\frac{\psi_K(x,y)}{\psi_K(x,\infty)}(1+o(1/u))$. In step $1''$ we show that $S_1''=O(\frac{1}{\log x})$, which will be proven to be hidden in the $o(\varepsilon(x,y))$.

In the case of S_2 the main ingredient is the linear sieve, which was introduced in Section 3. We take $\mathcal{A}=\mathcal{A}(mc,a):=\{w\in\mathcal{A}: w\equiv a \pmod{cm}\}$ and note that we have

$$\mathcal{A}_d(mc,a)=\frac{1}{\varphi(d)}\cdot\frac{\mathrm{Li}(x)}{\varphi(cm)}+\left(\pi_K(x;dmc,a)-\frac{\mathrm{Li}(x)}{\varphi(dmc)}\right). \tag{8}$$

We apply Lemma 8 to $\mathcal{A}=\mathcal{A}(mc,a)$ with $X=\frac{\mathrm{Li}(x)}{\varphi(m)}$ and

$$w(p)=\begin{cases}0, & p\mid amc\\ \frac{1}{\|p\|-1}, & \text{otherwise.}\end{cases}$$

The inequality required to apply the lemma is verified because Mertens formula guarantees the case $w(p) = 1$ and we have the sandwich inequalities for all primes $p \in \mathcal{O}_K$ with $\| p \| > 2$

$$\left(1 - \frac{1}{\| p \|}\right) \leq \left(1 - \frac{1}{\| p \| - 1}\right) \leq \left(1 - \frac{1}{\| p \|}\right)\left(1 + \frac{1}{\| p \|^2}\right).$$

We conclude that $S_2 = S_2' + S_2''$ where

$$\begin{aligned} S_2' &= \sum_{\substack{m \leq x^\delta \\ (m,a)=1}} \frac{\pi(x)}{\varphi(m)} \prod_{\substack{p < z \\ p \nmid am}} \left(1 - \frac{1}{\|p\|-1}\right) \\ S_2'' &= \sum_{\substack{m \leq x^\delta \\ (m,a)=1}} \sum_{\substack{d < D \\ d \mid P_{am}(z)}} |r(\mathcal{A}(mc,a),d)|. \end{aligned}$$

In steps $2'$ and $2''$ we prove that $S_2' = O(u\delta)$ and respectively $S_2'' = O(\frac{1}{\log x})$, both of which will be proven to be hidden in the term $o(\varepsilon(x,y))$.

Step $1'$. By Lemma 11 we have

$$\begin{aligned} S_1' &= \frac{\pi_K(x)}{\varphi(c)} \rho\left(\frac{\log(x^{1-\delta(x)})}{\log y}\right)(1 + O(\tfrac{\log(u+1)}{\log y})) + O(-(\log y)^{\frac{3}{5}-\epsilon}) \\ &= \frac{\pi_K(x)}{\varphi(c)} \rho\left(\frac{\log(x^{1-\delta(x)})}{\log y}\right)(1 + O(\tfrac{\log(u+1)}{\log y})) \\ &= \pi_K(x)\rho(u)\left(1 + O(\tfrac{\delta(x)}{u}) + O(\tfrac{\log u}{\log y})\right) \\ &= \pi_K(x)\rho(u)(1 + o(\varepsilon(x,y))). \end{aligned} \tag{9}$$

Step $1''$. In the case of S_1'' we use the trivial inequality $\mu(q) \leq 1$ and use Conjecture 1 with $0 < \tilde{\delta}(x) < \delta(x)$ so that $cq \leq x^{1-\delta}$ whenever $\| q \| \leq x^{1-\tilde{\delta}}$.

$$\begin{aligned} S_1'' &\leq \sum_{\|m\| \leq x^{1-\tilde{\delta}}} \left|\pi_K(x; mc, a') - \tfrac{\mathrm{Li}(x)}{\varphi(q)}\right| \\ &\ll \mathrm{Li}(x)/\log(x)^{A_0}, \end{aligned} \tag{10}$$

where $A_0 > 0$ is an absolute constant. Here a' is such that $a' \equiv a \pmod{c}$ and $a' \equiv 1 \pmod{m}$.

Step $2'$. The terms of S_2' are all positive, so we get an upper bound if we delete the condition $(a,m) = 1$ under the σ sign. The parameters z and D are set as follows $z = D = y^{1-2\delta}$. Then we have

$$S_2' \ll \mathrm{Li}(x) \prod_{\|p\| < z} \left(1 - \tfrac{1}{\|p\|-1}\right) \sum_{m \leq x^\delta} \tfrac{f(m)}{\|m\|}\ , \tag{11}$$

where f is the multiplicative function such that, for all $p \in \mathcal{O}_K$, $f(p) = 1 + O(\frac{1}{\|p\|})$. We replace the sum $\sum \frac{f(m)}{\|m\|}$ by a partial Euler product and obtain

$$\begin{aligned} S_2' &\ll \pi(x) \prod_{\|p\| < z} \left(1 - \tfrac{1}{\|p\|}\right) \prod_{\|p\| < x^\delta} \left(1 - \tfrac{1}{\|p\|}\right)^{-1} \\ &\ll \mathrm{Li}(x)\delta(x)s(x)u. \end{aligned} \tag{12}$$

Step $2''$. To handle S_2'' note that if $\| m \| \leq x^\delta$ and $\| d \| \leq D = y^{1-2\delta} \leq x^{1-2\delta}$ then $q := md$ is such that $\| q \| \leq x^{1-\delta}$. Hence

$$\begin{aligned} S_2'' &\leq \sum_{\|q\| \leq x^{1-\delta}} \sum_{d \mid q} |r(\mathcal{A}; d, a)| \\ &\leq \sum_{\|q\| \leq x^{1-\delta}} \tau(q) |\pi_K(x; q, a) - \tfrac{\pi_K(x)}{\varphi(q)}| \\ &\leq (S_{2,*}'' S_{2,\dagger}'')^{\frac{1}{2}}, \end{aligned} \tag{13}$$

where

$$\begin{aligned} S_{2,\dagger}'' &= \sum_{\|q\| \leq x^{1-\delta}} |\pi_K(x; q, a) - \tfrac{\pi_K(x)}{\varphi(q)}| \\ S_{2,*}'' &= \sum_{\|q\| \leq x^{1-\delta}} \tau(q)^2 |\pi_K(x; q, a) - \tfrac{\pi_K(x)}{\varphi(q)}|. \end{aligned}$$

We recognize the expression of the EH conjecture, so

$$S_{2,\dagger}'' \leq x/(\log x)^A. \tag{14}$$

We upper bound $S''_{2,*}$ using the crude inequality

$$\left|\pi_K(x;q,a) - \frac{\pi_K(x)}{\varphi(q)}\right| \leq \pi_K(x;q,a) + \frac{\pi_K(x)}{\varphi(q)}\pi_K(x;q,a) \leq 2.1 \cdot \frac{x}{q},$$

so

$$\begin{aligned} S''_2 &\leq (x/(\log x)^A)^{\frac{1}{2}} \left(x \sum_{\|q\| \leq x^{1-\delta}} \frac{\tau(q)^2}{\|q\|}\right)^{\frac{1}{2}} \\ &\ll \pi_K(x)/(\log x)^{A/2-4}. \end{aligned} \tag{15}$$

Completion of the proof of an asymptotic development. When combining Equations 9, 10, 12 and 15 we obtain

$$\begin{aligned} \psi_K(x,y;a,c) &= \frac{\mathrm{Li}(x)}{\varphi(c)}\left(\rho(u) + O(\frac{\delta}{u} + \frac{\log_2 x}{\log y}) + O(\frac{1}{(\log x)^{A_0}}) + \alpha(E)\delta(x)s(x)u + O(\frac{1}{(\log x)^{A/2-4}})\right) \\ &= \frac{\rho(u)}{\varphi(c)}\mathrm{Li}(x)\left(1 + \alpha(E)\frac{\delta(x)s(x)u}{\rho(u)}(1 + O(\frac{1}{\log x}))\right). \end{aligned} \tag{16}$$

Since $\frac{\delta(x)s(x)u}{\rho(u)} \to 0$ we have completed the proof.

Putting the asymptotic development in the form of the statement. Based on Theorem 9, one can reproduce mutatis mutandis the arguments in the proof of Theorem 1.1 in [BL17] and obtain

$$\frac{\psi_K(x,y)}{\psi_K(x,\infty)} = \frac{\psi(xe^{\alpha(E)},y)}{\psi(xe^{\alpha(E)},\infty)}\left(1 + O\left(\frac{\log(u+1)^2}{(\log y)^2}\right)\right), \tag{17}$$

where $\alpha(E) = L'(1,\chi)/L(1,\chi)$ where χ is the non-trivial character of K. □

5. The set $\Psi_v(x,y)$

This section is devoted to proving the following result, which implies Theorem 4 in the introduction.

We prepare the proof with a lemma, which is a variation of the fact that a set of primes which has a natural density also has an analytic density (see for example Th III.1.3 in [Ten15]).

Lemma 12. *Let Q be a set of primes such that $|\frac{\pi_Q(x)}{\pi(x)} - \lambda(x)| = O(\frac{1}{(\log x)^A})$, $\lambda(x)$ is a positive decreasing function, $A > 0$ a constant and $\pi_Q(x)$ is the cardinality of $Q \bigcap [1,x]$. Then we have*

$$\sum_{\substack{p<x \\ p\in Q}} \frac{1}{p} / \sum_{p<x} \frac{1}{p} \geq \lambda(x)\left(1 + \frac{1}{\log x \log_2 x} + O(\frac{1}{(\log x)^A})\right).$$

Proof. With these notations we have

$$\sum_{\substack{p<x \\ p\in Q}} \frac{1}{p} = \sum_{n=1}^{\lfloor x \rfloor} \frac{\pi_Q(n) - \pi_Q(n-1)}{n}.$$

By an Abel summation we have

$$\sum_{n=1}^{\lfloor x \rfloor} \frac{\pi_Q(n) - \pi_Q(n-1)}{n} = \frac{\pi_Q(x)}{\lfloor x \rfloor} + \sum_{n=1}^{\lfloor x \rfloor} \frac{\pi_Q(n)}{n(n+1)}.$$

We use $\lambda(n) \geq \lambda(x)$ for all $n \leq n$ and have

$$\begin{aligned} &\textstyle\sum_{n=1}^{\lfloor x \rfloor} \frac{\pi_Q(n)}{n(n+1)} \\ &\quad= \textstyle\sum_{n\leq x} \lambda(n)\frac{1}{n\log n} + O(\sum_{n\leq x} \frac{1}{n(\log n)^{A+1}}) \\ &\quad\geq \lambda(x)\textstyle\sum_{n\leq x} \frac{1}{n\log n} + O(\sum_{n\leq x} \frac{1}{n(\log n)^{A+1}}) \\ &\quad\geq \lambda(x)\log\log x + O(\frac{1}{(\log x)^A}). \end{aligned}$$

Finally, the term $\pi_Q(x)/\lfloor x \rfloor$ has a contribution $\frac{\lambda}{\log x} + O(\frac{1}{(\log x)^A})$. □

Proof of Theorem 4.

$$\begin{aligned}\frac{\psi_v(x,y)}{\psi(x,y)} &= \left(\sum_{\substack{p\in Q\\ y^{1/v}<p\le y}} \psi(x/p,y,p)\right) / \left(\sum_{y^{1/v}<p\le y}\psi(x/p,y,p)\right)\\ &= \left(\sum_{\substack{p\in Q\\ y^{1/v}<p\le y}} x/p\rho(u)(1+\varepsilon(x,y,p))\right) / \left(\sum_{y^{1/v}<p\le y} x/p\rho(u)(1+\varepsilon(x,y,p))\right),\end{aligned}$$

where $\varepsilon(x,y,p) = (\psi(x/p,y,p) - x/p\rho(u))/\rho(u)$. Since $\varepsilon(x,y,p) = O(1/u)$ and using Lemma 12 we further have

$$\begin{aligned}\psi_v(x,y) &= \psi(x,y)(1+O(\tfrac{1}{u}))\left(\sum_{\substack{p\in Q\\ y^{1/v}<p\le y}} 1/p\right) / \left(\sum_{y^{1/v}<p\le y} 1/p\right)\\ &\ge x\rho(u)\rho(v)\cdot\left(1+o(1)+O(\tfrac{1}{u}+\tfrac{1}{\log y\log_2 x}+\tfrac{\log(u+1)}{\log y})\right)\\ &\ge x\rho(u)\rho(v)(1+o(1)).\end{aligned} \tag{18}$$

□

6. The case of non-CM elliptic curves

In the cryptographic applications one can test if a presumed formula for $\alpha(E)$ matches the numerical experiments. This section, based on a working hypothesis, is not a proof but an attempt to find a formula for $\alpha(E)$ in the case of curves without CM, and it continues in Section 7.2.

A key fact in the CM case was the asymptotc equivalent of $\pi_K(x;d,a)$ given in equation (8). The role of $\pi_K(x;d,a)$ in the CM case is played here by

$$\pi_E(x;d) = |\{p\in\Pi(x) : d \mid E(\mathbb{F}_p)\}|. \tag{19}$$

David and Wu [DW12b] give an asymptotic equivalent under GRH:

$$\pi_E(x;d) = \left(\prod_{q\mid d}\frac{q^2-2}{(q-1)(q^2-1)}\right)\mathrm{Li}(x) + O(d^3x^{1/2}\log(d\cdot N_E x)). \tag{20}$$

The error term is $O_x(d^3\log d)$, which is much smaller than given by the effective Chebotarev theorem in the case of a generic number field of degree d. One can sum the error terms up to $d \le x^{1/4}/(\log x)^2$ and obtain a Bombieri-Vinogradov statement for elliptic curves.

Theorem 13 (under GRH, Prop 5.3 in [Kow05][3].)**.** *For $X = x^{1/5}$,*

$$\sum_{q\le X}\left|\pi_E(x;q) - \frac{w(q)\,\mathrm{Li}(x)}{q}\right| \ll_{E,A} \frac{x}{(\log x)^3}, \tag{21}$$

where $0 < w_E(q) < q$ is a multiplicative function depending on E.

We follow Pollack [Pol16] and "pretend that this approximation is valid for d up to size $\approx x$, at least on average". For the moment, the following statement is only a hypothesis which is interesting to investigate and which allows us to derive the value of $\alpha(E)$.

Hypothesis 14. *Let $\delta(x)$ be a decreasing function such that*

$$(\log_2 x)/(2\log x) \le \delta(x) < 1 \qquad (x \ge x_0).$$

Then, for any fixed elliptic curve E defined over $\mathbb{Q}$ and any $A \ge 0$, Equation (21) holds for $X = x^{1-\delta(x)}$, where $w_E(q)$ is the multiplicative function of Theorem 13.

Theorem 15. *Assume Hypothesis 14 for an elliptic curve E and a function $\delta(x)$. Set*

$$H = \left\{(x,y)\in\mathbb{R}_+^2 : x^{\frac{\log_3 x}{\log_2 x}} \le y \le x\right\}.$$

[3]See also Equation (4.7) in [DW12a].

For any $y \in [1,x]$ we set $u = \frac{\log x}{\log y}$. Then there exists a constant $\alpha(E)$ such that, as $x \to \infty$, we have the asymptotic development

$$\frac{\psi_E(x,y)}{\psi_E(x,\infty)} = \frac{\psi(xe^{\alpha(E)},y)}{\psi(xe^{\alpha}(E),\infty)} \cdot \left(1 + O\left(\frac{\log(u+1)}{\log y}\right)\right),$$

uniformly for $(x,y) \in H$.

Proof. The argument is a verbatim translation of the proof of Theorem 2. The inclusion-exclusion principle yields

$$\psi_E(x,y) = S_1 + S_2, \tag{22}$$

where

$$\begin{aligned} S_1 &= \sum_{\substack{q \le x^{1-\delta(x)} \\ P^-(q) > y}} \mu(q)\pi_E(x;qc) \\ S_2 &= \sum_{\substack{q > x^{1-\delta(x)} \\ P^-(q) > y}} \mu(q)\pi_E(x;qc). \end{aligned}$$

We write $S_1 = S_1' + S_1'' + S_1^\dagger$ with

$$\begin{aligned} S_1' &= \mathrm{Li}(x) \sum_{\substack{q > x^{1-\delta(x)} \\ P^-(q) > y}} \frac{\mu(q)}{\varphi(q)} \\ S_1^\circ &= \mathrm{Li}(x) \sum_{\substack{q > x^{1-\delta(x)} \\ P^-(q) > y}} \mu(q)\left(\frac{1}{\varphi(q)} - \frac{w_E(q)}{q}\right) \\ S_1'' &= \sum_{\substack{q > x^{1-\delta(x)} \\ P^-(q) > y}} \mu(q) r(x,q) \qquad \text{where } r(x;q) = \pi_E(x;q) - \mathrm{Li}(x)\frac{w_E(q)}{q}. \end{aligned}$$

From Equation (20) we have $\frac{1}{\varphi(q)} - \frac{w_E(q)}{q} = O(\frac{1}{q^2})$ and then

$$\begin{aligned} S_1^\circ / \mathrm{Li}(x) &\ll \sum_q \tfrac{1}{q^2} \\ &\ll \prod_{p>y}(1-\tfrac{1}{p^2})^{-1} = O(\tfrac{1}{y}). \end{aligned}$$

The sum S_1' is identical to Theorem 2 so we can use Equation (9). As in step $1''$, we show that S_1'' is also hidden in the $o(\varepsilon(x,y))$ while replacing Conjecture 1 with Hypothesis 14.

For S_2 we apply Lemma 8 with $D = y^{1-\delta}$ and $z = D$. Then we can write $S_2 = S_2' + S_2''$, where

$$\begin{aligned} S_2' &\ll \left(\sum_{m \le x^\delta} \frac{\pi(x)}{\varphi(m)} \prod_{\substack{p<z \\ p \nmid m}} \left(1 - \frac{w_E(p)}{p}\right)\right) \\ S_2'' &\ll \sum_{m \le x^\delta} \sum_{\substack{d < D \\ d \mid P_m(z)}} |r_E(md)|, \end{aligned}$$

Again, Step $2''$ can be copied mutatis mutandis to prove that $S_2'' = o(\varepsilon(x,y))$. Finally, Equation (20) implies that $(1 - \frac{w_E(p)}{p})/(1-\frac{1}{p}) = 1 + O(\frac{1}{p^2})$, so, up to a multiplicative constant, S_2'' has the same value as in Equation (12), so $S_2' = o(\varepsilon(x,y))$.

□

7. A formula for $\alpha(E)$

7.1. Recognizing $\alpha(E)$ in the CM case.

Proposition 16. *Let E be an elliptic curve with CM and let $\alpha(E)$ be the constant in Theorem 2. For all rational primes ℓ we set*

$$\alpha_\ell(E) = \log \ell \left(\frac{1}{\ell - 1} - \mathbb{E}_p(\mathrm{val}_\ell(|E(\mathbb{F}_p)|))\right),$$

where $\mathbb{E}_p$ denotes the average value in the sense of Chebotarev density over random primes p. Then we have

$$\alpha(E) = \sum_\ell \alpha_\ell(E).$$

Proof. The proof of Theorem 2 implies that $\alpha(E) = L'(1,\chi)/L(1,\chi)$. Due to the uniforme convergence of the Euler product which divides $L(s,\chi)$, we can derivate term by term:

$$\begin{aligned}\alpha(E) &= -\sum_\ell \frac{\partial}{\partial s}\log(1-\tfrac{1+\chi(\ell)}{\ell^s})\Big|_{s=1}\\ &= -\sum_\ell \chi(\ell)\tfrac{\log\ell}{\ell-1}\\ &= \sum_\ell \log\ell\left(\tfrac{1}{\ell-1}-\tfrac{\chi(\ell)+1}{\ell-1}\right).\end{aligned}$$

By Dirichlet's theorem, inside the set of primes π such that $\pi \equiv a \pmod c$, the subset of these π such that $\| \pi - 1 \| \equiv 0 \pmod \ell^k$ is the density of random elements of K not divisible by inert primes whose norm is divisible by ℓ^k. This last density is $2/\ell^k$ if ℓ is split and 0 if ℓ is inert. We conclude that the average valuation in ℓ of $\#E(\mathbb{F}_p)$ is $\frac{\chi(\ell)+1}{\ell-1}$.

□

Remark 17. *In the study of smoothness of binary forms, Murphy* [Mur98] *associated a function to irreducible polynomials $f \in \mathbb{Z}[x]$ as follows*

$$\begin{aligned}\text{for a prime } \ell \quad \alpha_\ell(f) &= (\log\ell)\cdot(\mathbb{E}_n(\mathrm{val}_\ell\, n) - \mathbb{E}_{(a,b)=1}(\mathrm{val}_\ell\, b^{\deg(f)} f(a/b))),\\ \alpha(f) &= \textstyle\sum_{\ell \text{ prime}} \alpha_\ell(f),\end{aligned}$$

where $\mathbb{E}_{(a,b)=1}$ is the average (in the sense of Chebotarev density) for randomly chosen pairs of integers (a,b) which are relatively prime. Hence $\alpha(E)$ has a very similar expression to $\alpha(K)$, the difference being made by the condition $(a,b)=1$.

7.2. **Heuristics for non-CM elliptic curves.** From [DW12b], the function w_E is computed from Galois representations associated to E. Serre's open image theorem implies that for all but finitely many primes, which depend on E, $\alpha(E)$ is equal to the value in Theorem 15. A recent result [BS21] makes the list of all the infinite families of elliptic curves whose $\alpha(E)$ is different from the generic value, under Serre's uniformity conjecture.

Proposition 18. *Let E be an elliptic curve without CM. Let P_n be the multiplicative function such that $P_n = \mathrm{Prob}(n \mid \#E(\mathbb{F}_p))$ when n is a prime power. Let $h(n) = \mu(n)P_n$.*

Then there exists a constant $c(E)$ such that

$$\sum_{\substack{n\le x\\ P^-(n)>y}} h(n) = \tau(E)x\rho(u)\left(1+O\left(\frac{\log(u+1)}{\log y}\right)\right).$$

As a consequence, if one assumes Hypothesis 14, then

$$\psi_E(x,y)/x = \tau(E)\rho(u)\left(1+O\left(\frac{\log(u+1)}{(\log y)}\right)\right).$$

Proof. Let us show that Theorem 10 applies to $\mathcal{H}(s) = \sum_n \frac{P_n}{n^s}$ and let us compute the constants a_0 and a_1 in the statement of that theorem. By Equation (2.3) of [DW12b], Serre's open image theorem implies that there exists an integer $S(E)$ such that, for any two integers m and n such that $(mn, S_E) = 1$, we have $P_{mn} = P_m P_n$. By Lemma 2.3 of [DW12b] there exists a constant $M(E)$ such that, uniformly on ℓ and k, we have

$$\forall \ell \nmid S(E), \forall k \ge 0, \quad |P_{\ell^k} - \frac{1}{\ell^k}| \le \frac{M(E)}{\ell^{k+1}}.$$

Let us set

$$\tau(E) := (\sum_{n|S(E)^\infty} P_n n^{-s})\cdot \prod_{\ell|S(E)}(1-\ell^{-s}).$$

Then $\mathcal{H}(s) - \tau(E)\zeta(s)$ is holomorphic in a neighbourhood of 1 and Theorem 10 applies. We have directly that $\mathrm{ord}(\mathcal{H})_1 = 1$ and

$$a_0 = \mathrm{res}_1\,\mathcal{H} = \tau(E)\,\mathrm{res}_1\,\zeta = \tau(E).$$

Hence Theorem 10 applies and we have the asymptotic formula for $\sum h(n)$. Hypothesis 14 allows to replace $\sum h(n)$ by $\Psi_E(x,y)$ and obtain

$$\psi_E(x,y)/x = \tau(E)\rho(u)\left(1+O\left(\frac{\log(u+1)}{(\log y)}\right)\right). \tag{23}$$

□

The value of $\tau(E)$ can be made explicit for every family of elliptic curves. Recall that a Serre curve is an elliptic curve such that, for all primes ℓ, ρ_ℓ is surjective and $[\mathrm{GL}_2(\mathbb{Z}) : \mathrm{Im}(\rho_E)] = 2$.

Corollary 19. *If E is a Serre then $\tau(E)/\prod_{\ell|S(E)}(1-1/\ell) = \sum_{\substack{i,j,m,n \\ m \mid n \mid d^\infty}} P_{2^i m,2^j n}\frac{1}{2^{i+j}mn}$, where $P_{2^i m,2^j n}$ is given by Equations (26),(25) and (24).*

Proof. For any integers $a, b \geq 1$ such that $a \mid b$ we call $P_{a,b}$ the probability that $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \subset E(\mathbb{F}_p)$ when p is a random prime.

By Theorem 2.19 in [BBB+13], applied to a prime level ℓ, not necessarily odd, in the case $\mathrm{Im}(\rho_{E,\ell}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ we have

$$P_{\ell^i,\ell^j} = \begin{cases} c_3^{\max(j-i-1,0)} c_2^{\mathrm{sgn}(j-i)} P_{\ell,\ell} & \text{when } i \geq 1 \\ c_3^{\max(j-i-1,0)} P_{1,\ell} & \text{when } i = 0 < j, \end{cases} \tag{24}$$

where $c_1 = 1/\ell^4$, $c_2 = (\ell-1)(\ell+1)^2/\ell^4$, $c_3 = 1/\ell$, $P_{\ell,\ell} = 1/(\ell(\ell-1)^2(\ell+1))$ and $P_{1,\ell} = (\ell^3-2\ell-1)/(\ell(\ell+1)(\ell-1)^2)$.

Let $d := \mathrm{Disc}(E)$. Since $[\mathrm{GL}_2(\mathbb{Z}) : \mathrm{Im}(\rho_E)] = [\mathrm{GL}_2(\mathbb{Z}/2d\mathbb{Z}) : \mathrm{Im}(\rho_{E,2d})]$, for all odd integers m and n one has

$$P_{m,n} = \prod_{\ell|d,\ell\neq 2} P_{\ell^{\mathrm{val}_\ell(m)},\ell^{\mathrm{val}_\ell(n)}}. \tag{25}$$

For any integers $i, j \geq 0$ and odd integers n, m we have

$$P_{2^i m,2^j n} = \begin{cases} 2P_{2^i,2^j}P_{m,n} & \text{if } d \mid 2^i m \text{ and } i \geq 1 \\ P_{2^i,2^j}P_{m,n} & \text{otherwise} \end{cases} \tag{26}$$

Indeed, if $d \nmid 2^i m$ then the injection $\mathrm{Im}(\rho_{E,2^j n}) \to \mathrm{GL}_2(\mathbb{Z}/2^j n\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/2^j\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is surjective. Then one has directly $P_{2^i m,2^j n} = P_{2^i,2^j}P_{m,n}$.

Write $d = 2^{i_0}m_0$ and assume that $m_0 \mid m$ and $i_0 \leq i$ or equivalently $d \mid 2^i m$. Let H be the unique subgroup of index 2 in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$. Then the proportion of matrices having 1 as an eigenvalue is the same in H as in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$. This extends to the unique subgroup of index 2 of $\mathrm{GL}_2(\mathbb{Z}/2_0^i\mathbb{Z})$. Hence one has $P_{2^i m,2^j n} = P_{1,2^{j-i}n/m}P_{m/m_0,m/m_0}P_{2^i m_0,2^i m_0}$.

Finally, we have $P_{2^i m_0,2^i m_0} = P_{m_0,m_0}$ if $i = 0$. If $i \geq 1$ we have a different equation

$$P_{2^i m_0,2^i m_0} = 1/|\mathrm{Im}\rho_{E,2^i m_0}| = 2/(|\mathrm{Im}\rho_{E,2^i}| \cdot |\mathrm{Im}\rho_{E,m_0}|) = 2P_{2^i,2^i}P_{m_0,m_0},$$

which implies Equation (26). □

Remark 20. *ECM-friendly curves without CM have $\tau(E) \neq 1$ in general. Hence they keep their advantage asymptotically compared to random integers of the same bit size.*

References

[BBB+13] Razvan Barbulescu, Joppe Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter Montgomery. Finding ECM-friendly curves through a study of Galois properties. *The Open Book Series*, 1(1):63–86, 2013.

[BL17] Razvan Barbulescu and Armand Lachand. Some mathematical remarks on the polynomial selection in NFS. *Mathematics of Computation*, 86(303):397–418, 2017.

[BS21] Razvan Barbulescu and Sudarshan Shinde. A classification of ECM-friendly families using modular curves. *Mathematics of Computation*, to appear, 2021.

[dlBF20] Régis de la Bretèche and Daniel Fiorilli. Entiers friables dans des progressions arithmétiques de grand module. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 169, pages 75–102. Cambridge University Press, 2020.

[DW12a] C. David and J. Wu. Pseudoprime reductions of elliptic curves. *Canadian Journal of Mathematics*, 64(1):81–101, 2012.

[DW12b] Chantal David and Jie Wu. Almost prime values of the order of elliptic curves over finite fields. In *Forum Mathematicum*, volume 24, pages 99–119. Walter de Gruyter GmbH & Co. KG, 2012.

[FG92] John Friedlander and Andrew Granville. Limitations to the equi-distribution of primes iii. *Compositio Mathematica*, 81(1):19–32, 1992.

[Gra08] Andrew Granville. Smooth numbers: computational number theory and beyond. *Algorithmic number theory: lattices, number fields, curves and cryptography*, 44:267–323, 2008.

[HTW08] Guillaume Hanrot, Gérald Tenenbaum, and Jie Wu. Moyennes de certaines fonctions multiplicatives sur les entiers friables, 2. *Proceedings of the London Mathematical Society*, 96(1):107–135, 2008.

[Iwa80] Henryk Iwaniec. A new form of the error term in the linear sieve. *Acta Arithmetica*, 37(1):307–320, 1980.

[Kow05] Emmanuel Kowalski. Analytic problems for elliptic curves. ArXiv preprint math/0510197, 2005.

[Len87] Hendrik W Jr Lenstra. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[LT15] Armand Lachand and Gerald Tenenbaum. Note sur les valeurs moyennes criblées de certaines fonctions arithmétiques. *The Quarterly Journal of Mathematics*, 66(1):245–250, 2015.

[LWX20] Jianya Liu, Jie Wu, and Ping Xi. Primes in arithmetic progressions with friable indices. *Science China Mathematics*, 63(1):23–38, 2020.

[Mon87] Peter L Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.

[Mur98] Brian Murphy. Modelling the yield of number field sieve polynomials. In *Algorithmic Number Theory–ANTS III*, volume 1423 of *Lecture Notes in Computer Science*, pages 137–150, 1998.

[Pol16] Paul Pollack. A titchmarsh divisor problem for elliptic curves. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 160, pages 167–189. Cambridge University Press, 2016.

[RS09] Karl Rubin and Alice Silverberg. Point counting on reductions of CM elliptic curves. *Journal of Number Theory*, 129(12):2903–2923, 2009.

[Sco04] Eira J Scourfield. On ideals free of large prime factors. *Journal de théorie des nombres de Bordeaux*, 16(3):733–772, 2004.

[Ten15] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163. American Mathematical Soc., 2015.

[Wan18] Zhiwei Wang. Autour des plus grands facteurs premiers d'entiers consécutifs voisins d'un entier criblé. *The Quarterly Journal of Mathematics*, 69(3):995–1013, 2018.

[Zyw11] David Zywina. A refinement of Koblitz's conjecture. *International Journal of Number Theory*, 7(03):739–769, 2011.