ECM And The Elliott-Halberstam Conjecture For Quadratic Fields

Razvan Barbulescu, Florent Jouve

ECM and the Elliott–Halberstam conjecture for quadratic fields

Razvan Barbulescu and Florent Jouve

Abstract

The complexity of the elliptic curve method of factorization (ECM) is proven under a strong conjectural form of existence of friable numbers in short intervals. In the present work we use friability to tackle a different version of ECM which is much more studied and implemented, especially because it enables the use of ECM-friendly curves. In the case of curves with complex multiplication (CM) we replace heuristic arguments by rigorous results conditional on the Elliott–Halberstam (EH) conjecture. The proven results mirror recent work concerning the count of primes p such that $p-1$ is friable. In the case of non CM curves, we explore consequences of a hypothetical statement that can be seen as an elliptic curve analogue of EH.

1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve that has good reduction precisely at every prime number not dividing an integer Δ_E. The main object of study of this paper is the prime counting function $\psi_E(x,y)$ which is defined as the cardinality of

$$\Psi_E(x,y) = \{p \leq x \colon p \text{ prime}, \, p \nmid \Delta_E, |E(\mathbb{F}_p)| \text{ is } y\text{-friable}\}. \tag{1}$$

Here we make the usual slight abuse of notation and write $E(\mathbb{F}_p)$ for the set of $\mathbb{F}_p$-points on the reduction of E modulo p and we also recall that an integer is *y-friable* (or *y-smooth*) if all its prime factors are less than y. For any integer n (or any algebraic integer of a number field K) we shall denote by $P^-(n)$ (resp $P^+(n)$) the smallest (resp. the largest) prime factor of the norm of n relative to $K/\mathbb{Q}$. By convention $P^-(1) = \infty$. The notation $\psi_E(x,y)$ is reminiscent of $\psi(x,y)$ which denotes the cardinality of

$$\Psi(x,y) = \{n \leq x \colon P^+(n) < y\}. \tag{2}$$

Our main motivation for studying $\Psi_E(x,y)$ comes from cryptography and more precisely from the method of factorization ECM. First recall the principle and purposes of ECM [Len87]. Let $P \in E(\mathbb{Q})$ be a rational point with homogeneous coordinates $P = (x_P : y_P : z_P) \in E(\mathbb{Q})$, relatively to a fixed projective embedding of E. Without loss of generality we can assume $x_P, y_P, z_P \in \mathbb{Z}$. Let N be a given positive integer for which one would like to find the prime factorization; set two parameters $u = u(N)$ and $v = v(N)$ in $(0,1)$ and define $B = N^{1/u}$, $C = B^{1/v}$. Note that if $\gcd(x_P, y_P, z_P, N) = 1$ and $\gcd(N, \Delta_E) = 1$ then 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 the multiple $Q = (x_Q : y_Q : z_Q) := [M]P \bmod N$ for $M = (\lfloor C \rfloor !)^{\lfloor \log N / \log 2 \rfloor}$, *i.e.* one uses the chord-and-tangent formulæ and reduces the coordinates modulo N (if two points have distinct coordinates modulo N then one uses the formula for adding two distinct points). We summarize this in Algorithm 1 below.

Claim 1. If $|E(\mathbb{F}_p)|$ is C-friable for some (unknown) prime factor p of N, then $g_N := \gcd(z_Q, N)$ is a multiple of p.

Algorithm 1: One curve subroutine of ECM

Input: parameters u, v, an integer N, an elliptic curve $E/\mathbb{Q}$ and $P \in E(\mathbb{Q})$.
Output: a prime factor p of N such that $p < B := \lfloor N^{1/u} \rfloor$ or FAIL.

1: $C \leftarrow \lfloor B^{1/v} \rfloor$
2: $M \leftarrow C!^{\lfloor \log N / \log 2 \rfloor}$
3: Q: $(x_Q : y_Q : z_Q) \leftarrow [M]P \bmod N$
4: $g \leftarrow \gcd(z_Q, N)$
5: **if** $g \neq 1$ **then**
6: **print** g
7: **end if**

Let us give the main ideas justifying the claim. If the points involved in the double-and-add method were all distinct not only modulo N but also modulo p, then Q would be 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 careful analysis shows that the probability that the result is exactly p is $1 - o_{p\to\infty}(1)$ (see [Len87]). If g_N is a prime factor of N we are done, otherwise we pick a different curve E and start over until a factor is found.

The ECM algorithm consists in repeating Algorithm 1 either once, or a given number of times, or until success, depending on the application. ECM is primarily used to completely factorize N, which is done by finding some proper divisor and then iterating. If one takes $u = 2$ so that we seek all prime factors less than $B = N^{1/2}$, these prime factors are enough to find a possible cofactor. Next the parameter v is chosen so as to minimize the average running time: $v = \sqrt{2}(\log N)^{1/2}/(\log\log N)^{1/2}$ or equivalently $C = \lfloor L_N(1/2, 1/\sqrt{2}) \rfloor$, where

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

and one runs Algorithm 1 with as many curves as needed in order to factorize N (note that there is no guarantee that the procedure terminates after testing finitely many curves). The expectation of the number of curves needed in this optimal choice of v is $C^{1+o(1)}$ (see [Len87]).

If one decides in advance to stop after $B/\psi(B, C)$ curves, then one finds all primes less than B with constant probability (under the heuristics asserting independence relatively to the choice of the elliptic curve). This allows a second application of ECM : given an integer, decide whether it is B-friable with no false positive and with a constant fraction of false negatives.

A third application is as follows : given a large number of integers less than a paremeter N and given a parameter $B = N^{1/u}$, find at least a prescribed proportion f of B-friable integers inside the set. This problem is solved by the Number Field Sieve (NFS) algorithm [LLJMP93], where ECM is used as a building block in the cofactorization step of the relation collection, also called sieving step, (see for example and [MBKL14, §3, page 337]) and in the splitting step of the discrete logarithm version of NFS (see for example [CS06, §4.1, point 1, page 181]). In the latter, one needs to find a single B-friable integer. To solve the problem, one uses a single elliptic curve or a finite number of them on a large number of integers. For example, the record factorizations of RSA moduli obtained with the CADO-NFS software [BGK+] use a dozen elliptic curves to test the friability of billions of integers. Also, in [MBKL14, Table 3, page 345] one uses 5 to 10 curves whereas the number of integers exceeds half a million per special-q and billions in total. The idea here is to set v so that one has $\psi(B, B^{1/v}) \geq f$ and then, in order to test B-friability, one is interested in how many primes up to B are found by Algorithm 1 with entries v and a particular elliptic curve E. We are hence interested in the quantity $\psi_E(x, y)$ for $(x, y) = (B^{1/u}, B^{1/uv})$.

In particular, the heuristics underlying the use of ECM as a friability test states that the larger $\psi_E(x,y)$ gets, the more y-friable integers will be found by ECM inside a given set. In other words, E is more ECM-friendly as $\psi_E(x,y)$ increases. We formalize this idea in the following definition.

Definition 1 (ECM-friendly curves)**.** Let $x > y$ be positive real numbers and let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be two elliptic curves. One says that E_1 is more ECM-friendly than E_2 with respect to (x,y) if

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

One says that E_1 is more ECM friendly than E_2 if there exists $x_0 \geq 2$ and a positive valued increasing function ϑ such that the above inequality holds for all pairs (x,y) such that $x \geq x_0$ and $\vartheta(x) \leq y \leq x$.

Our main result (Theorem 1.2) roughly states that the probability that the number of $\mathbb{F}_p$-points on a given elliptic curve is friable approaches asymptotically the probability for any integer to be friable. In the case of CM[1] elliptic curves our result is conditional on the Elliott–Halberstam conjecture (EH), an important analytic number theoretic statement about uniformity aspects in the distribution of primes in residue classes.

Conjecture 1.1 (Elliott–Halberstam, *e.g.* [Wan18, Hyp B] for $\mathbb{Q}$, extended to K quadratic in [Pol16, Prop. 2.2])**.** *Let K be either $\mathbb{Q}$ or an imaginary quadratic field of class number one and let $\delta > 0$. Let $\| \cdot \|$ denote the field norm relative to $K/\mathbb{Q}$. We define*

$$\Pi_K(x) = \{p \in \mathcal{O}_K, \text{prime}\colon \| p \| \leq x\}\,, \qquad \Pi_K(x;c,a) = \{p \in \Pi_K(x)\colon p \equiv a \bmod c\},$$

of cardinality denoted $\pi_K(x)$ and $\pi_K(x;c,a)$, respectively. Then for any fixed $a \in \mathcal{O}_K$ and $\omega > 0$ we have

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

for any $x \geq 2$ and where $q \in \mathcal{O}_K$ $\varphi(q) = |(\mathcal{O}_K/q\mathcal{O}_K)^*|$.

The Elliott–Halberstam conjecture is standard in analytic number theory. It is a far reaching generalization of the celebrated Bombieri–Vinogradov Theorem where $K = \mathbb{Q}$ and the bound on q in the index set of the summation cannot exceed $\sqrt{x}$. EH would have countless important applications in number theory. Suffice it to mention the EH bounds contained in [May15] on gaps between consecutive primes (or more generally on the length of intervals containing k-tuples of primes), as well as [Zha14] where, as a crucial step in the proof of the main result, Zhang establishes a bound towards EH (*i.e.* going beyond the $\sqrt{x}$ threshold) under some extra restrictions on the prime factorization of the moduli involved.

A quantitatively refined version of EH allows one to let δ depend on x as long as $\delta(x) \to 0$ as x tends to infinity. Indeed, Montgomery suggested that one could take $\delta(x) \to 0$ in Conjecture 1.1. Friedlander and Granville [FG92] showed that the conjecture fails if $\delta(x)$ is less than a certain function of x. However Liu, Wu and Xi [LWX20] used the conjecture for $\delta(x)$ large enough not to contradict the necessary constraints observed by Friedlander and Granville (Conjecture 4.1 below states this "parametrized" version of EH).

[1]For each number field K, there is a finite number of CM elliptic curves defined over K but there are overall infinitely many CM elliptic curves.

In order to state our main result, we first recall some classical facts about the counting function of friable integers. With notation as in (2), one has the well known asymptotics due to Dickman:

$$\lim_{x\to\infty} \frac{\psi(x, x^{\frac{1}{u}})}{x} = \varrho(u) \qquad \big(u = \frac{\log x}{\log y}\big)\,,$$

where ϱ is the unique continuous function on $\mathbb{R}_{\geq 0}$ that is differentiable on $(1,\infty)$ and satisfies $\varrho(u) \equiv 1$ on $[0,1]$ and $u\varrho'(u) = \varrho(u-1)$ on $(1,\infty)$. Hildebrand–Tenenbaum [HT86] have obtained the following asymptotics for ϱ:

$$\log \varrho(u) = -u\Big(\log u + \log_2(u+2) - 1 + O\big(\frac{\log_2(u+2)}{\log(u+2)}\big)\Big) \qquad (u \geq 1)\,. \tag{4}$$

We now state our main result. From Conjecture 1.1, it draws an asymptotic equivalent for $\psi_E(x,y)$. From a refined version of Conjecture 1.1 (Conjecture 4.1) we handle uniformity issues in these asymptotics, and finally, we state a non CM analogue (conjectural on Hypothesis 1) of our asymptotic estimates.

Theorem 1.2. *Let $x \geq 2$ and let y satisfy $2 \leq y \leq x$. Set $u := \frac{\log x}{\log y}$.*

- *Let $E/\mathbb{Q}$ be a CM elliptic curve.*

  1. *(Theorem 3.4) Assume Conjecture 1.1. If u is upper bounded by an absolute constant then one has*
  $$\psi_E(x,y) \sim \varrho(u)\,\mathrm{Li}(x) \qquad (x\to\infty)\,,$$
  where $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$.
  2. *(Corollary 4.3) Assume Conjecture 4.1. If $\delta(x)$ is a function satisfying for some $\eta > 0$ and $\beta > 0$:*
  $$\frac{\log_2 x}{\eta \log x} \leq \delta(x) \ll \frac{1}{(\log_2 x)^{1+\beta}}$$
  and $u \leq \frac{\log_3 x}{\log_4 x}$ then we have
  $$\psi_E(x,y) = \varrho(u)\,\mathrm{Li}(x)(1 + O(\delta(x)u/\varrho(u))).$$

- *Let $E/\mathbb{Q}$ be a non CM elliptic curve.*

  3. *(Theorem 6.2) Assume Hypothesis 1. If u is upper bounded by an absolute constant then one has*
  $$\psi_E(x,y) \sim \varrho(u)\,\mathrm{Li}(x), \qquad (x\to\infty)\,.$$

Note that the same asymptotics hold for $\psi_E(x,y)$ disregarding the endomorphism ring of E, provided the relevant assumption is made on E (Conjecture 1.1 if E has CM, and Hypothesis 1 otherwise). This uniform asymptotic behaviour of elliptic curves over $\mathbb{Q}$ suggests that ECM-friendliness is determined by the implicit error terms in Theorem 1.2. In Section 4.2, we discuss in detail these error terms. In particular, for CM elliptic curves, we show the relevance of introducing as in [BS21, Def. 5.1], the quantity

$$\alpha(E) = L'(1,\chi)/L(1,\chi),$$

where χ is the Kronecker character of the quadratic field associated to E.

We conclude by stating a strong form of Theorem 1.2(2) which is directly related to questions in cryptography, as we will discuss in Section 2.

Theorem 1.3. *Assume Conjecture 4.1. Let (x, y, z) be three positive integers such that $u := \frac{\log x}{\log y}$ and $v := \frac{\log y}{\log z}$ lie in the domain*

$$\Delta := \left\{(u, v) \in \mathbb{R}^2 \colon u \leq \frac{\log_2(x)}{\log_3(x)} \text{ and } v \leq \frac{\log_3 y}{\log_4 y}\right\}.$$

With notation as in (2) *we set*

$$\Psi_{E,z}(x, y) = \{n \in \Psi(x, y) \colon \exists p \mid n, |E(\mathbb{F}_p)| \text{ is } z\text{-friable}\}$$

and we let $\psi_{E,z}(x, y)$ denote its cardinality. Then we have, uniformly on Δ,

$$\frac{\psi_{E,z}(x, y)}{x} = \varrho(v)\varrho(u)(1 + o(1)) \qquad (x \to \infty,\, y \to \infty).$$

The paper is organized as follows. In Section 2 we come back to our cryptographic motivation and study the running time of the splitting step of NFS, which is ECM-based, as a consequence of Theorem 1.3. In Section 3 we prove Theorem 1.2(1) following work of Wang [Wan18]. In Section 4 we state a uniform version of the Elliott–Halberstam conjecture and, assuming it, we prove Theorem 1.2(2). The error terms implicit in Theorem 1.2 are then discussed and, in the CM case, we prove a computation oriented formula for $\alpha(E)$. Section 5 is devoted to the proof of Theorem 1.3. Finally in the last section, we investigate the implications, in the non CM case, of heuristics developed by Pollack and we prove Theorem 1.2(3).

2 Cryptographic motivation

In this section we put Theorem 1.3 in context and we give an example of algorithmic application. Precisely Theorem 1.3 enables us to perform a computational task (Problem 1 below), which is related to a classical problem in cryptography: the splitting step for discrete logarithms (Problem 2 below).

Problem 1. Consider a prime q, a generator g of $(\mathbb{Z}/q\mathbb{Z})^*$ and an auxiliary element $h \in (\mathbb{Z}/q\mathbb{Z})^*$. Let u and v be parameters and let $E/\mathbb{Q}$ be an elliptic curve. Find an integer $e \in [0, q-1]$ such that $n := g^e h \bmod q$ is $q^{1/u}$-friable and such that, for some prime divisor p of n, E has good reduction at p and $|E(\mathbb{F}_p)|$ is $q^{1/(uv)}$-friable.

Problem 2 (Splitting step of NFS)**.** Consider the same data as in the problem above. For a parameter k, consider $E_1, E_2, \ldots, E_k$, elliptic curves over $\mathbb{Q}$. Find an integer $e \in [0, q-1]$ such that $n := g^e h \bmod q$ is $q^{1/u}$-friable and, for all prime factors p of n, there exists $i \leq k$ such that $|E_i(\mathbb{F}_p)|$ is $q^{1/(uv)}$-friable.

To solve Problem 1, one runs ECM on the integers $g^e h \bmod q$ corresponding to values of $e \in [1, q-1]$ which are chosen uniformly at random until it is B-friable for $B = q^{1/u}$ (see Algorithm 2 for a precise description). Note that the algorithm uses a single CM elliptic curve $E/\mathbb{Q}$ that is required to have positive Mordell–Weil rank. To fix ideas, our description of Algorithm 2 uses, among the 13 possible j-invariants of CM elliptic curves defined over $\mathbb{Q}$, the case $j = 8000$ for which we selected one twist of positive rank given by the Weierstrass equation: $E \colon y^2 = x^3 + x^2 - 3x + 1$ (the point $P = (-1 : 2 : 1) \in E(\mathbb{Q})$ has infinite order).

The next statement asserts that Theorem 1.3 can be used to solve Problem 1.

Theorem 2.1. *1. Under Conjecture 1.1 (resp. Conjecture 4.1), Algorithm 2 solves Problem 1 in time $(q^{1/(uv)}/\varrho(u)\varrho(v))^{1+o(1)}$ (as $q \to \infty$) for bounded u (resp. for $u \leq \frac{\log_3 x}{\log_4 x}$).*

Algorithm 2: NFS splitting step

Input: a prime q and two integers $g, h \in [1, q-1]$ such that g is a generator of $\mathbb{F}_q^*$, and two parameters u and v

Output: an integer e such that $g^e h \bmod q$ has a factor less than $B = \lfloor q^{1/u} \rfloor$

1: $E\colon y^2 = x^3 + x^2 - 3x + 1$, $P = (-1 : 2 : 1) \in E(\mathbb{Q})$
2: **repeat**
3: $e \leftarrow$ an integer chosen uniformly at random in $[1, q-1]$
4: $n \leftarrow g^e h \bmod q$
5: run ECM for n and B on the curve E, with parameters u and v
6: **until** ECM finds a proper factor of n

2. Assume further that Theorem 1.3 can be extended to the domain $(x, y = x^{1/u}, z = y^{1/v})$ below :

$$\Delta' := \left\{(u,v) \in \mathbb{R}^2 \colon u \le c_u \frac{(\log x)^{1/3}}{(\log_2 x)^{1/3}} \text{ and } v \le c_v \frac{(\log x)^{1/3}}{(\log_2 x)^{1/3}}\right\},,$$

for two constants $c_u, c_v \ge 3^{1/3}$. Then, with a constant probability, Algorithm 2 on input q terminates in time $L_q(1/3, 3^{1/3})^{1+o(1)}$ and solves Problem 1 for $u = c_u(\log q/\log_2 q)^{1/3}$ and $v = c_v(\log q/\log_2 q)^{1/3}$.

Proof. 1. Recall that $B = \lfloor q^{1/u} \rfloor$ and $C = \lfloor B^{1/v} \rfloor = \lfloor q^{1/(uv)} \rfloor$. As input N of Algorithm 1, we take the ouput n of Algorithm 2. The cost of ECM (Algorithm 1) is essentially that of step 3, which is $O(\log M)$ by double-and-add exponentiation ($M = C!^{\lfloor \log n/\log 2 \rfloor}$ as defined in Algorithm 1). By Stirling's formula, this is

$$\text{time(Alg. 2: line 5)} = O(\log M) = O(C \log C \log n) = C^{1+o(1)} = q^{1/(uv)+o(1)} \ (q \to \infty). \quad (5)$$

Since e is uniformly chosen at random, the number of executions of the loop in lines 2-6 of Algorithm 2 is, with positive probability, less than a constant times the inverse of the probability of success. We saw earlier (*cf.* Claim 1) that the condition in line 6 of Algorithm 2 is satisfied if, for a prime factor p of n, the order $|E(\mathbb{F}_p)|$ is C-friable. We conclude that the number of executions of the loop is $q/\psi_{E,q^{1/(uv)}}(q, q^{1/(u)})$.

Since u and v are in the domain Δ defined in Theorem 1.3, we have $q/\psi_{E,q^{1/(uv)}}(q, q^{1/(u)}) \le (1/(\varrho(v)\varrho(u))(1+o(1))$. Combining this with (5), the cost of Algorithm 2 is $(q^{1/(uv)}/\varrho(u)\varrho(v))^{1+o(1)}$.

2. We set the value of the constants : $c_v = c_u = 3^{1/3}$. We inject in (4) the values of u and v:

$$\log(\varrho(v)\varrho(u)) = (-1+o(1)) \cdot (u \log u + v \log v) = (-1+o(1)) \cdot \left(\frac{c_u + c_v}{3} (\log q)^{1/3} (\log_2 q)^{2/3}\right).$$

Hence the loop is executed at most $L_q(1/3, \frac{c_u+c_v}{3})^{1+o(1)}$ times. Multiplying this by the cost computed in $(5), C^{1+o(1)} = L_q(1/3, \frac{1}{c_u c_v})^{1+o(1)}$, we find the running time of Algorithm 2

$$\text{time(Algorithm 2)} = L_q(1/3, c),$$

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

□

Remark 1. One can easily adapt Algorithm 2 to solve Problem 2 (hence the identical names): in line 5 apply ECM to all the curves E_i with $i = 1, \ldots, k$. If we set $k = 1/\varrho(v)^{1+o(1)}$, and if the outcome of ECM is independent of the input curve E_i, then with constant probability

we completely factorize n whenever it is B-friable. Then we execute the loop in lines 2-6 $q/\psi(q, q^{1/u}) = 1/\varrho(u)^{1+o(1)}$ times. Hence the total cost is $(C/\varrho(u)\varrho(v))^{1+o(1)}$, which is the same as for Problem 1. To the best of our knowledge, no rigorous argument proves the required "independence" property for the input curves at the present time even though a heuristic complexity to solve Problem 2 is well known ([CS06]).

3 Background and proof of Theorem 1.2(1)

Let K be either $\mathbb{Q}$ or an imaginary quadratic field of class number 1. Recall that $\| \cdot \|$ is the norm map relative to $K/\mathbb{Q}$ and that $P^-(n)$ and $P^+(n)$ respectively denote the smallest and largest prime factors of n. Let $a, c \in \mathcal{O}_K$ and let κ be a root of unity of K. We set (recall the notation of Conjecture 1.1)

$$\psi_K(x, y; c, a, \kappa) = |\{\pi \in \Pi_K(x; c, a) \colon P^+(\| \pi - \kappa \|) < y\}|. \tag{6}$$

We start by recalling a fundamental fact from the theory of CM elliptic curves that relates (1) with (6).

Lemma 3.1 (Deuring's CM theory, see *e.g.* [RS09, Th 1.1]). *For any elliptic curve $E/\mathbb{Q}$ with CM by an order of an imaginary quadratic field K, there exists $c \in \mathcal{O}_K$, a set $A \subset \{a \in \mathcal{O}_K \colon \gcd(a, c) = 1\}$ of cardinality $\varphi(c)/2$ and a root of unity $\mu_{c,a}$ such that, for any rational prime p which splits in K, $|E(\mathbb{F}_p)| = \| \pi - \mu_{c,a} \|$, where π is uniquely determined by the conditions $\| \pi \| = p$ and $\pi \equiv a \pmod{c}$. In particular*

$$\psi_E(x, y) = \#\{p \in \Psi_E(x, y) \colon p \text{ inert in } K\} + \sum_{a \in A} \psi_K(x, y; c, a, \mu_{c,a}) \, .$$

To prove Theorem 1.2(1), we follow the strategy of Wang [Wan18]. In particular we assume Conjecture 1.1 and we appeal to the linear sieve of Rosser–Iwaniec that we now recall.

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 number and $d \in \mathcal{O}_K$ a squarefree integer whose prime factors belong to $\mathcal{P}$. Let $\mathcal{A}_d = \mathcal{A} \bigcap d\mathcal{O}_K$ and $P(z) = \prod_{\|p\| < z, p \in \mathcal{P}} p$. Let X be a real number (that should be seen as an "approximation" of $|\mathcal{A}|$) and let w be a multiplicative function on $\mathcal{O}_K$ such that for $p \in \mathcal{P}$ one has $0 < w(p) < \| p \|$. We set $r(\mathcal{A}, d) = |\mathcal{A}_d| - \frac{w(d)}{\|d\|} X$ (which is expected to be small) and also:

$$S(\mathcal{A}; \mathcal{P}, z) = |\{a \in \mathcal{A} \colon (a, P(z)) = 1\}| \, , \qquad V(z) = \prod_{p \in \mathcal{P}, \, \|p\| \leq z} (1 - \frac{w(p)}{\| p \|}) \, .$$

Lemma 3.2 (Rosser–Iwaniec [Iwa80], see also [Wan18, Lemme 3.1]). *Assume that there exists $\alpha \geq 2$ such that*

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

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

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

Finally we recollect an estimate for the summatory function of $\mu(n)/\|n\|$ over integers less than x that are not divisible by primes $\leq y$. In the application of Wang's strategy, one of the base steps uses Möbius inversion, which explains why such summatory functions come into play.

Lemma 3.3 ([dlBF20, Lemma 7.2][2], generalized to imaginary quadratic fields[3]). *Let K be $\mathbb{Q}$ or an imaginary quadratic field of class number 1. Let μ be the Möbius function generalized to K. For any $\epsilon > 0$, we have*

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

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

We can now recall the statement and give the proof of Theorem 1.2(1).

Theorem 3.4. *Let $E/\mathbb{Q}$ be a CM elliptic curve and let K be the associated imaginary quadratic field of class number 1. Let $x \geq 2$ and let y be such that $2 \leq y \leq x$ and $u := \frac{\log x}{\log y}$ is upper bounded by an absolute constant. Then we have*

$$\psi_E(x, y) \sim \varrho(u) \operatorname{Li}(x) \qquad (x \to \infty).$$

Proof of Theorem 3.4. By Lemma 3.1 we have

$$\begin{aligned} \psi_E(x,y) =& |\{p \text{ split in } K,\, p \leq x \colon P^+(|E(\mathbb{F}_p)|) < y\}| \\ &+ |\{p \text{ inert in } K,\, p \leq x \colon P^+(|E(\mathbb{F}_p)|) < y\}| \\ =& \sum_{a \in A} \psi_K(x, y; c, a, \mu_{c,a}) + |\{p \text{ inert in } K,\, p \leq x \colon P^+(p+1) < y\}|, \end{aligned} \tag{7}$$

where A, c and μ are as in Lemma 3.1 (see the notation (6)). Note that for the purpose of this article one could have added a $O(1)$ term to account for ramified primes in K and for primes of bad reduction of E, but one can be more precise and erase the $O(1)$ term because the ramified primes correspond precisely to the primes of bad reduction.

The second term of the right hand side is the case $a = -1$ in [Wan18, Lemma 4.1]:

$$|\{p \text{ inert in } K,\, p \leq x \colon P^+(p+1) < y\}| \sim \varrho(u) \frac{\operatorname{Li}(x)}{2}. \tag{8}$$

We shall prove that $\psi_K(x, y; c, a, \mu) \sim \varrho(u) \operatorname{Li}(x)/\varphi(c)$ and, when summing over the $|A| = \varphi(c)/2$ values of a we obtain:

$$|\{p \text{ split in } K,\, p \leq x \colon P^+(|E(\mathbb{F}_p)|) < y\}| \sim \frac{1}{2} \varrho(u) \operatorname{Li}(x), \tag{9}$$

which, together with Equation (8) implies the equivalent of $\psi_E(x, y)$ and will complete the proof.

Hence, it remains to prove an equivalent for $\psi_K(x, y; c, a, \kappa)$ for constants c, $a \in \mathcal{O}_K$ and a constant $\kappa \in \mathcal{O}_K^\times$.

We note that for large enough y, more precisely $y > c$ (which we assume holds in the rest of the proof since $x \to \infty$ and u remains bounded), one has $\gcd(q, c) = 1$ as soon as $P^-(\| q \|) > y$.

[2] The first version of this lemma can be found in [LT15] where one has an additional error term $O_\epsilon(\frac{\log(u+1)}{\log y})$. The version of *loc. cit.* suffices for most of our computations, however our discussion of error terms in §4.2 requires the refinement in [dlBF20] .

[3] The generalization is direct, hence it is not reproduced here.

Therefore, by the Chinese Remainder Theorem, we can fix, for each such q an element $a' \in \mathcal{O}_K$ such that $a' \equiv a \pmod{c}$ and $a' \equiv \kappa \pmod{q}$. Combining this with Möbius' inversion we write

$$\begin{aligned}\psi_K(x,y;c,a,\kappa) &= |\{\pi \in \Pi_K(x;c,a)\colon P^+(\| \pi - \kappa \|) < y\}| \\ &= |\{\pi \in \Pi_K(x;c,a)\colon \gcd\Big(\pi-\kappa, \prod_{\ell \text{ prime}, \|\ell\|\geq y} \ell\Big) = 1\}| \\ &= \sum_{\substack{q\in\mathcal{O}_K,\, \|q\|\leq x+1 \\ P^-(\|q\|)>y}} \mu(q) |\Pi_K(x;c,a)\cap \Pi_K(x;q,\kappa)| = \sum_{\substack{q\in\mathcal{O}_K,\, \|q\|\leq x+1 \\ P^-(\|q\|)>y}} \mu(q)\pi_K(x;qc,a')\end{aligned} \tag{10}$$

where we have used the fact that the algebraic norm of a root of unity is 1.

In order to evaluate $\psi_K(x,y;c,a,\kappa)$ we follow closely Wang's method ([Wan18, Dém. du Lemme 4.1]). We highlight the necessary adaptations, omitting the details whenever they are straightforward form Wang's approach. Starting from (10) we fix an arbitrarily small $\delta > 0$ and split the counting function $\psi_K(x,y;c,a,\kappa) = S_1 + S_2$ where

$$S_1 = \sum_{\substack{q\in\mathcal{O}_K,\, \|q\|\leq x^{1-\delta} \\ P^-(\|q\|)>y}} \mu(q)\pi_K(x;qc,a')\,, \qquad S_2 = \sum_{\substack{q\in\mathcal{O}_K,\, x+1\geq\|q\|>x^{1-\delta} \\ P^-(\|q\|)>y}} \mu(q)\pi_K(x;qc,a')\,. \tag{11}$$

Next, using the multiplicativity of φ and our assumption $y > c$, we further decompose $S_1 = S_1' + S_1''$ where

$$S_1' = \frac{\mathrm{Li}(x)}{\varphi(c)} \sum_{\substack{q\in\mathcal{O}_K,\, \|q\|\leq x^{1-\delta} \\ P^-(\|q\|)>y}} \frac{\mu(q)}{\varphi(q)}, \qquad S_1'' = \sum_{\substack{q\in\mathcal{O}_K,\, \|q\|\leq x^{1-\delta} \\ P^-(\|q\|)>y}} \mu(q) r(x,qc,a') \tag{12}$$

and where $r(x,qc,a') = \pi_K(x;qc,a') - \frac{\mathrm{Li}(x)}{\varphi(cq)}$.

Step 1′. We show that $S_1' \sim \frac{\mathrm{Li}(x)}{\varphi(c)}\varrho(u)$ as $x\to\infty$ and u remains bounded (under these restrictions we deduce that S_1' is asymptotically larger than a constant times $\mathrm{Li}(x)$). For q satisfying $P^-(q) > y$, observe that

$$\frac{1}{\varphi(q)} - \frac{1}{q} = \frac{1}{q}\times O\Big(\big(1+\frac{1}{y}\big)^{\omega(q)} - 1\Big) = O\Big(\frac{1}{q}\times\frac{\omega(q)}{y}\Big)\,.$$

Since $\|q\| \leq x^{1-\delta}$, we use the upper bound $\omega(q) \ll \log x$ which we combine with the fact that $y \gg x^{\theta}$, for some $\theta > 0$ (recall that u remains bounded) to conclude that uniformly for any q in the index set of S_1' one has

$$\frac{1}{\varphi(q)} = \frac{1}{q}(1+o(x)) \qquad (x\to\infty)\,.$$

Using Lemma 3.3, Wang's computation [Wan18, (4.6)] immediately produces

$$S_1' = \frac{\mathrm{Li}(x)}{\varphi(c)}\varrho(u)\,(1+O(\delta)+o(x)) \sim \frac{\mathrm{Li}(x)}{\varphi(c)}\varrho(u) \qquad (x\to\infty, u\ll 1)\,. \tag{13}$$

Step 1″. We use Conjecture 1.1 with a fixed $\omega > 6$ to show that $S_1'' = O(\mathrm{Li}(x)/(\log x)^{\omega-1})$. Note that this is negligible compared to S_1'.

Let $0 < \tilde{\delta} < \delta$ be so that $\| cq \| \leq x^{1-\delta}$ whenever $\| q \| \leq x^{1-\tilde{\delta}}$. Using the triangle inequality and Conjecture 1.1 we have

$$\begin{aligned} S_1'' &= \sum_{\substack{q\in\mathcal{O}_K,\, \|q\|\leq x^{1-\delta}\\ P^-(\|q\|)>y}} \mu(q) r(x, qc, a') \leq \sum_{\|q\|\leq x^{1-\tilde{\delta}}} r(x, qc, a') \\ &\leq \sum_{\|q'\|\leq x^{1-\delta}} r(x, q', a') \ll_\omega \frac{x}{\log(x)^\omega}\,. \end{aligned} \tag{14}$$

We now handle the contribution of S_2 defined in (11). We first apply the triangle inequality and we observe that the primes $p \in \mathcal{O}_K$ that are counted satisfy $p - \kappa = qcm$ with $m \in \mathcal{O}_K$ of norm bounded by $\|m\| \leq x^\delta$. Therefore we have

$$|S_2| \leq \sum_{\substack{m\in\mathcal{O}_K\\ \|m\|\leq x^\delta}} |\{p \text{ prime},\, \|p\| \leq x \colon P^-\big(\frac{p-a'}{mc}\big) > y\}|\,.$$

To evaluate this upper bound, the main ingredient used by Wang is the linear sieve.

We apply Lemma 3.2 to

$$\mathcal{A} = \mathcal{A}(m, c, a') = \Big\{\frac{p-a'}{mc} \colon p \in \Pi_K(x; mc, a')\Big\}\,, \qquad \mathcal{P} = \{p \text{ prime} \colon p \nmid mca'\}\,, \qquad z \leq y\,.$$

Indeed for this choice of parameters, one has

$$|S_2| \leq \sum_{\substack{m\in\mathcal{O}_K\\ \|m\|\leq x^\delta}} S(\mathcal{A}(m, c, a'); \mathcal{P}, z)\,. \tag{15}$$

and therefore, for all squarefree $d \in \mathcal{O}_K$ having all its prime factors in $\mathcal{P}$, we have $\gcd(d, m) = 1$, and $\mathcal{A}_d$ is homothetic to the translate $\Pi_K(x; dmc, a') - a'$. In particular $|\mathcal{A}_d| = \pi_K(x; dmc, a')$. We set $X = \frac{\mathrm{Li}(x)}{\varphi(mc)}$ and fix a multiplicative function w on $\mathcal{O}_K$ satisfying

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

For any squarefree $d \in \mathcal{O}_K$ with all its prime factors in $\mathcal{P}$ we have therefore

$$\frac{w(d)}{\|d\|} X = \frac{w(d)}{\|d\|}\frac{\mathrm{Li}(x)}{\varphi(mc)} = \Big(\prod_{p\mid d} \frac{1}{\|p\|(1-\frac{1}{\|p\|})}\Big)\frac{\mathrm{Li}(x)}{\varphi(mc)} = \frac{\mathrm{Li}(x)}{\varphi(mcd)}$$

since d is coprime to mc, by definition of $\mathcal{P}$.

Finally note that the following inequalities hold for all primes $p \in \mathcal{O}_K$ with $\| p \| > 2$,

$$\left(1 - \frac{1}{\| p \|}\right) \geq \left(1 - \frac{1}{\| p \| - 1}\right) \geq \left(1 - \frac{1}{\| p \|}\right)\left(1 + \frac{1}{\| p \|^2}\right)\,, \tag{16}$$

therefore, combined with Mertens' formula (see *e.g.* [Ten15, Chap. I.6, Th. 1.12]), this shows that the hypotheses of Lemma 3.2 are satisfied. For any fixed $D \geq z$ we obtain

$$S(\mathcal{A}; \mathcal{P}, z) \ll X \prod_{\|p\|\leq z}\left(1 - \frac{w(p)}{\| p \|}\right) + \sum_{\|d\|<D,\, d\mid P(z)} \left||\mathcal{A}_d| - \frac{\mathrm{Li}(x)}{\varphi(dmc)}\right|\,.$$

From this upper bound, combined with (15), we deduce that $|S_2| \ll S_2' + S_2''$ where

$$S_2' = \sum_{\|m\| \le x^\delta} \frac{\mathrm{Li}(x)}{\varphi(cm)} \prod_{\substack{\|p\|<z \\ p \nmid mca'}} \Big(1 - \frac{1}{\| p \| - 1}\Big)\,, \qquad S_2'' = \sum_{\|m\| \le x^\delta} \sum_{\substack{\|d\|<D \\ d \mid P(z)}} |r(\mathcal{A}, d)|\,, \tag{17}$$

and where $|r(\mathcal{A}, d)| = |\pi_K(x; dmc, a') - \frac{\mathrm{Li}(x)}{\varphi(dmc)}|$.

We next set $z = D = y^{1-2\delta}$ and recall $\omega > 6$. Under these conditions we prove upper bounds for S_2' and S_2''.

Step 2′. We prove that $S_2' = O(\mathrm{Li}(x) u\delta)$. Since c and a' are constants we relax the condition $p \nmid mca'$ into $p \nmid m$ in the index set of the product appearing in S_2'. Then we have

$$\begin{aligned} S_2' &\ll_{c,a'} \sum_{\|m\| \le x^\delta} \frac{\mathrm{Li}(x)}{\varphi(m)} \prod_{\substack{\|p\|<z \\ p \nmid m}} \Big(1 - \frac{1}{\| p \| - 1}\Big) \\ &\ll \mathrm{Li}(x) \left(\prod_{\|p\|<z} \Big(1 - \frac{1}{\| p \| - 1}\Big) \right) \left(\sum_{\|m\| \le x^\delta} \frac{1}{\varphi(m)} \prod_{\substack{\|p\|<z \\ p \mid m}} \Big(1 - \frac{1}{\| p \| - 1}\Big)^{-1} \right) \end{aligned}$$

The first factor over primes on the right hand side is $\ll (\log z)^{-1} = ((1-2\delta)\log y)^{-1}$ by Mertens' formula combined with (16). For the right-most factor we write $\frac{\varphi(m)}{\|m\|} = \prod_{p \mid m}(1 - \frac{1}{\|p\|})$ and note that the function f defined on $\mathcal{O}_K$ by

$$f(m) = \prod_{p \mid m} \Big(1 - \frac{1}{\| p \| - 1}\Big)^{-v_p(m)} \Big(1 - \frac{1}{\| p \|}\Big)^{-v_p(m)}$$

(where $v_p(m)$ is the p-adic valuation of m) is completely multiplicative. Since in the product defining f, each factor at p is ≥ 1 we obtain:

$$\sum_{\|m\| \le x^\delta} \frac{1}{\varphi(m)} \prod_{\substack{\|p\|<z \\ p \mid m}} \Big(1 - \frac{1}{\| p \| - 1}\Big)^{-1} \le \sum_{\|m\| \le x^\delta} \frac{f(m)}{\| m \|}\,.$$

Here note that the general term of the product over primes on the left hand side is ≥ 1 and therefore the upper bound holds both in the case $z \ge x^\delta$ and $z < x^\delta$. Using a partial Euler product and Mertens' formula combined with (16) we deduce that

$$\sum_{\|m\| \le x^\delta} \frac{1}{\varphi(m)} \prod_{\substack{\|p\|<z \\ p \mid m}} \Big(1 - \frac{1}{\| p \| - 1}\Big)^{-1} \le \sum_{\|m\| \le x^\delta} \frac{f(m)}{\| m \|} \ll \prod_{\|p\| \le x^\delta} \Big(1 - \frac{1}{\| p \| - 2}\Big)^{-1} \ll \delta \log x\,,$$

This concludes step 2′:

$$S_2' = O\Big(\mathrm{Li}(x) u \frac{\delta}{1-2\delta} \Big) = O(\mathrm{Li}(x) u\delta)\,. \tag{18}$$

Step 2″. We prove that $S_2'' = O(\mathrm{Li}(x)/\log x^{\omega/2-3})$. Note that if $\| m \| \le x^\delta$ and $\| d \| \le D = y^{1-2\delta} \le x^{1-2\delta}$ then $n := md$ is such that $\| n \| \le x^{1-\delta}$. We denote by $\tau(n)$ the number of divisors of n. Hence we have, applying Cauchy–Schwarz in the last step,

$$S_2'' \le \sum_{\|n\| \le x^{1-\delta}} \sum_{d \mid n} |r(\mathcal{A}; cd, a')| \le \sum_{\|n\| \le x^{1-\delta}} \tau(q) |r(\mathcal{A}; nc, a')| \le (S_{2,\star}'' S_{2,\dagger}'')^{\frac{1}{2}}$$

where

$$S''_{2,\dagger} = \sum_{\|n\|\le x^{1-\delta}} |r(\mathcal{A}; nc, a')|\,, \qquad S''_{2,\star} = \sum_{\|n\|\le x^{1-\delta}} \tau(n)^2 |r(\mathcal{A}; nc, a')|\,.$$

For $S''_{2,\dagger}$ we recognize the expression of Conjecture 1.1 so, recalling that c is a constant (therefore for big enough x one has $\| c \| \le x^{\delta/2}$), we deduce

$$S''_{2,\dagger} \ll x/(\log x)^{\omega}.$$

As in [Wan18, (4.10)] we first use a trivial upper bound on $S''_{2,\star}$:

$$|r(\mathcal{A}; nc, a)| = \Big|\pi_K(x; nc, a) - \frac{\pi_K(x)}{\varphi(nc)}\Big| \ll \frac{x}{\| n \|},$$

to obtain the upper bound:

$$S''_{2,\star} \ll x \sum_{\|n\|\le x^{1-\delta}} \frac{\tau(n)^2}{\| n \|} \ll x(\log x)^4$$

where the last step uses summation by parts and knowledge of the average order of τ^2 (see *e.g.* [Wil23, (1.25)]). Note also that, invoking positivity for the general term of the sum, the implied constant is absolute (and in particular does not depend on δ). Overall we obtain

$$S''_2 \ll \Big(\frac{x}{(\log x)^{\omega}}\Big)^{\frac12} x^{\frac12} (\log x)^2 \ll \frac{\mathrm{Li}(x)}{(\log x)^{\frac{\omega}{2}-3}}\,. \tag{19}$$

Putting together (13), (14), (18), and (19), we see that the sums S''_1 and S''_2 are negligible compared to $\mathrm{Li}(x)$. Since $\varrho(u)$ is lower bounded by a constant, the proof of Theorem 3.4 is finished by letting $\delta \to 0$. □

4 Uniform version of the Elliott–Halberstam conjecture and proof of Theorem 1.2(2)

In this section we start by stating a refined version of Conjecture 1.1 and we prove Theorem 1.2(2) under this refined conjecture. We next discuss the error term implicit in Theorem 1.2(1) and (2).

4.1 Proof of Theorem 1.2(2)

The argument we provide is a consequence of [LWX20, Th. 1.5]. Let us first state the refined version of Conjecture 1.1 required in our analysis.

Conjecture 4.1 (parametric EH, [LWX20, Conj. 1] in the $K = \mathbb{Q}$, same $\delta(x)$ as in the rational case, with the same adjustments as in Conjecture 1.1 for the case of quadratic K)**.** *Let $\delta(x)$ be a decreasing function such that*

$$(\log_2 x)/(\eta \log x) \le \delta(x) < \eta \qquad (x \ge x_0(\eta)), \tag{20}$$

for any $\eta \in (0, 1/2]$ Let K be either $\mathbb{Q}$ or an imaginary quadratic field of class number one. For all $q \in K$ we set $\| q \| = |\mathcal{O}_K/q|$ the algebraic norm and $\varphi(q) = |(\mathcal{O}_K/q)^*|$ the Euler function. Let us consider

$$\pi_K(x) = \{p \in \mathcal{O}_K,\ \textit{prime}\colon \| p \| \le x\}\,,\ \pi_K(x; c, a) = \{p \in \mathcal{O}_K,\ \textit{prime}\colon \| p \| \le x,\ p \equiv a \bmod c\}.$$

Then for any fixed $a \in \mathcal{O}_K$, $a \neq 0$, and $\omega > 0$ we have

$$\sum_{\substack{q \in \mathcal{O}_K,\, (q,a)=1 \\ \|q\| \leq x^{1-\delta(x)}}} \left| \pi_K(x; q, a) - \frac{\pi_K(x)}{\varphi(q)} \right| \ll_\omega \frac{x}{(\log x)^\omega},$$

uniformly for $x \geq x_0(\eta)$.

The original EH conjecture is stated for $K = \mathbb{Q}$ and constant δ. As already mentioned it is a strengthening of the Bombieri–Vinogradov (BV) Theorem. Huxley [Hux71] proved a number field variant of the BV Theorem, so it was natural to make a number field EH conjecture which states Huxley's result for the same bound on q as in the original EH conjecture. Pollack [Pol16, Lemma 2.3] wrote Huxley's Theorem explicitly in the case of imaginary quadratic fields of class number one. Finally, Liu et al. [LWX20] extended EH by replacing δ with a decreasing function. In the present work we use the number field EH. If we only want to focus on non uniform results we can restrict to the original EH. However in order to prove uniform results, our analysis requires a new variant of EH (Conjecture 4.1) which combines the number field EH (extending [Pol16, Lemma 2.3]) with the parametric EH (see [LWX20]).

The proof of Theorem 1.2(2) will follow from a generalized form of [LWX20, Th. 1.5] that we now state.

Theorem 4.2 ([LWX20, Th. 1.5] generalized to imaginary quadratic fields)**.** *Let K be an imaginary quadratic field of class number 1. Let $a \in \mathcal{O}_K \setminus \{0\}$ and let μ denote a root of unity of K. Let $\omega > 0$ and let κ be a non-negative arithmetic function on $\mathcal{O}_K$. With notation as in* (6) *and assuming Conjecture 4.1 for a given function δ satisfying* (20)*, we have*

$$\sum_{\substack{q \in \mathcal{O}_K,\, \|q\| \leq Q \\ (q,a)=1}} \left| \psi_K(x, y; q, a, \mu) - \frac{\pi_K(x)}{\varphi(q)} \varrho\left(\frac{\log(x/\| q \|)}{\log y} \right) \right| \ll_{a,\omega} \frac{x \sqrt{\sum_{\|q\| \leq x} \kappa(q)^2 / \| q \|}}{(\log x)^\omega} + \pi_K(x) \delta(x) u \sum_{\|q\| \leq Q} \frac{\kappa(q)}{\varphi(q)}$$

For every $\epsilon > 0$ this upper bound is uniform for $x \geq 2$, $\exp((\log x)^{2/5+\epsilon}) \leq y \leq x$ and $Q \leq \min(y, \sqrt{x})$.

Note that the original statement [LWX20, Th. 1.5] is over $\mathbb{Q}$: in *loc. cit.* the prime counting function π_K is replaced by the usual prime counting function π and $\psi_K(x, y; q, a, \mu)$ is replaced by

$$\pi(x, y; q, a) = \#\{p \leq x \colon q \mid (p - a),\, P^+(\tfrac{p-a}{q}) \leq y\}.$$

Obtaining Theorem 4.2 from the original [LWX20, Th. 1.5] requires minor modifications only. As we will see below, Corollary 4.3 (and in turn Theorem 1.2(2)) will follow from Theorem 4.2. If one wants to dispense from generalizing [LWX20, Th. 1.5] to an imaginary quadratic field, one can instead consider the version of Corollary 4.3 proved in Appendix A, where the arguments used are similar to those of the proof of Theorem 1.2(1).

In [LWX20, Cor. 1.8 (p. 5)] a result is proven for $u \leq \frac{\log_2 x}{\log_3 x}$. We note here that a stronger consequence of Theorem 4.2 holds if one restricts to $u \leq \frac{\log_3 x}{\log_4 x}$, and implies in turn Theorem 1.2(2).

Corollary 4.3. *Let K be $\mathbb{Q}$ or an imaginary quadratic field of class number 1. Let $a, c \in \mathcal{O}_K$ with $a \neq 0$ and let μ be a unit of K. Finally let $\beta > 0$. Assuming Conjecture 4.1, we have*

$$\pi_K(x, y; c, a, \mu) = \frac{\mathrm{Li}(x)}{\varphi(c)} \varrho(u) \left(1 + O\left(\delta u \varrho(u)^{-1}\right)\right). \tag{21}$$

uniformly for $1 \leq u \leq \frac{\log_3 x}{\log_4 x}$ and for $\delta(x) \ll \frac{1}{(\log_2 x)^{1+\beta}}$. Consequently Theorem 1.2(2) holds.

Proof. First note that under the stated assumptions $(\delta(x)u/\varrho(u)) = o(1)$ as $x \to \infty$. Indeed, by (4), one has $\varrho(u) \gg \exp(-(1+\beta')u \log u)$ for $u \geq 1$ and any fixed β' satisfying $0 < \beta' < \beta$. Therefore we compute:

$$\begin{aligned}
\frac{u}{\varrho(u)} \ll u \mathrm{e}^{(1+\beta')u \log u} &\leq \frac{\log_3 x}{\log_4 x} \exp\Big((1+\beta')\frac{\log_3 x}{\log_4 x} \log\big(\frac{\log_3 x}{\log_4 x}\big)\Big) \\
&\leq \frac{\log_3 x}{\log_4 x} \exp\left((1+\beta')\log_3 x\Big(1 - \frac{\log_5 x}{\log_4 x}\Big)\right) \\
&\leq (\log_2 x)^{1+\beta'} \frac{\log_3 x}{\log_4 x} \exp\Big(-(1+\beta')\frac{\log_3 x}{\log_4 x}\Big) = o\big((\log_2 x)^{1+\beta}\big).
\end{aligned}$$

Next the assumption on the size of u implies that $\log y \geq \log x \log_4 x / \log_3 x$ and thus for big enough x one has $c \leq \min(y, \sqrt{x})$, since c is fixed. Setting $\kappa = \mathbf{1}_{\{c\}}$ in Theorem 4.2 we obtain:

$$\left|\psi_K(x, y; c, a, \mu) - \frac{\pi_K(x)}{\varphi(c)} \varrho\left(\frac{\log(x/\| c \|)}{\log y}\right)\right| \ll_{a,\omega} \frac{x}{\sqrt{\| c \|}(\log x)^{\omega}} + \frac{\pi_K(x)}{\varphi(c)} \delta(x) u. \tag{22}$$

The second summand on the right hand side of (22) is $\ll \mathrm{Li}(x)\delta(x)u$. Likewise, since $u \geq 1$, and since δ is lower bounded by assumption in Conjecture 4.1, we have for the first summand:

$$\frac{x}{(\log x)^{\omega}} \ll_{\eta} \mathrm{Li}(x)\delta(x)u \frac{\log x}{(\log x)^{\omega-1} \log_2 x}$$

which is $\ll \mathrm{Li}(x)\delta(x)u$ for any fixed $\omega \geq 2$.

Finally, since ϱ is smooth on $(1, \infty)$, c is fixed, and we may assume that y is big enough (recall that the assumptions imply that $\log y \geq \log x \log_4 x / \log_3 x$) there exists $\xi \in (u - \frac{\log \|c\|}{\log y}, u)$ such that

$$\left|\varrho\big(\frac{\log(x/\| c \|)}{\log y}\big) - \varrho(u)\right| = \left|\frac{\log \| c \|}{\log y} \varrho'(\xi)\right| \leq \left|\frac{\log \| c \|}{\log y} \frac{\varrho(\xi - 1)}{\xi}\right| \ll \left|\frac{\varrho(\xi - 1)}{\log x}\right|.$$

We deduce

$$\frac{1}{\mathrm{Li}(x)\delta(x)u} \left|\varrho\big(\frac{\log(x/\| c \|)}{\log y}\big) - \varrho(u)\right| \ll_{\eta} \frac{1}{x} \frac{\log x}{\log_2 x} = o(1).$$

This finishes the proof of (21).

To deduce Theorem 1.2(2), we combine (7) with (21), using again that c depends only on E.

□

4.2 Discussion on the implicit error terms in Theorem 1.2

The error term plays an important role in deciding whether an elliptic curve E_1 is more ECM-friendly than a second curve E_2. Indeed, let us recall [BS21, Problem 5.1].

Problem 3. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Decide whether there exists a real number $\beta(E)$ such that

$$\mathrm{Prob}(\#E(\mathbb{F}_p) \text{ is } B\text{-friable}\colon p \sim n) \sim_n \mathrm{Prob}(m \text{ is } B\text{-friable}\colon m \sim n\mathrm{e}^{\beta(E)}),$$

where $\sim_n$ denotes the asymptotic equivalent as $n \to \infty$, for positive numbers a, b we write $a \sim b$ as a shorthand for $a \in [b - \sqrt{b}, b + \sqrt{b}]$, and "Prob" on the left hand side denotes the natural density of a subset of primes, while "Prob" on the right hand side denotes the uniform probability on a finite set.

We mention two results that investigate the size of the error terms in approximations of the counting function of friable integers.

Theorem 4.4 ([Sco04, Cor. 1.2, Th. 1.3])**.** *Let K be an imaginary quadratic field. Then for a fixed $\varepsilon > 0$, for all x and y such that $(\log_2 x)^{5/3+\varepsilon} \leq \log y \leq \log x$, one has*

$$\psi_K(x, y) = \lambda_K x \left(\varrho(u) + \frac{\varrho'(u)}{\log y}(\alpha_K + o(1)) \right) \qquad (x \to \infty)\,.$$

Here $\psi_K(x, y) = |\{a \in \mathcal{O}_K\colon \|a\| \leq x,\ P^+(\|a\|) \leq y\}|$, λ_K is the residue at $s = 1$ of the Dedekind zeta function ζ_K of K and $\alpha_K = (L'/L)(1, \chi)/\zeta_K(1)$ for χ the Kronecker symbol of K.

The result was generalized from ζ_K to a large class of Dirichlet 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 (*e.g.* holomorphic functions). The following particular case is sufficient for our applications.

Theorem 4.5 ([HTW08, Theorem 1.1], case $Z = \zeta$, G holomorphic)**.** *Let h be an arithmetic function with Dirichlet series $\mathcal{H}(s) = \sum_{n \geq 1} \frac{h(n)}{n^s}$. We assume that $\mathcal{H}$ is meromorphic with a simple pole at $s = 1$ and we write $\mathcal{H}(s) = a_0/(s-1) + a_1 + O(s-1)$ in a neighborhood of 1. Then one has*

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

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

Let us add that a similar result holds for $Z = 1/\zeta$, the Dirichlet series of μ. A direct application of Theorem 4.5 yields

$$\psi(x\mathrm{e}^{\alpha(E)}, y) = \exp(u + \alpha(E)\frac{\log(u+1)}{\log y}(1 + o_x(1)))\,.$$

Note that Theorem 1.2(1) gives a positive answer to the problem in the CM case while Theorem 1.2(3) does so in the non CM case.

Finally, Theorem 1.2(2) raises the necessity of finding asymptotics for $\log(\psi_E(x, y)/\psi(x, y))$. The numerical statistics in Appendix B suggest that the following question is relevant.

Problem 4. Let E be a CM elliptic curve whose endomorphism ring is equal to $\mathcal{O}_K$ for an imaginary quadratic field K, and let χ be the nontrivial character associted to $\mathrm{Gal}(K/\mathbb{Q})$. Is it true that, when $\alpha(E) = L'(1, \chi)/L(1, \chi)$, the following formula holds:

$$\log(\psi_E(x, y)/\psi(x, y)) \sim \alpha(E)\frac{\log(u+1)}{\log y}\ ?$$

Remark 2. The result [LT15, Th. 1.1], which was used in [Wan18] and is sufficient for Theorem 1.2(1), is not enough here because the error term given is $O(\log(u+1)/\log y)$. We use instead the stronger Lemma 3.3 due to de la Bretèche and Fiorilli.

If Problem 4 receives a positive answer with the main term being $\alpha(E)\log(u+1)/\log y$ for a constant $\alpha(E)$, this constant will be used as a criterion to evaluate ECM-friendliness of elliptic curves. Given two elliptic curves E_1 and E_2, Peter Montgomery used without proof[4] ([Mon92, §6.3, pp. 75–76]) the constant $\sum_\ell \alpha_\ell(E)$ (see Proposition 4.6 below) for primes ℓ such that $\alpha_\ell(E_1) \neq \alpha_\ell(E_2)$ to compare $\psi_{E_1}(x,y)$ and $\psi_{E_2}(x,y)$.

Proposition 4.6 ([BS21, Th. 5.1])**.** *Let $E/\mathbb{Q}$ be any elliptic curve. For all rational primes ℓ we set*

$$\alpha_\ell(E) = \log \ell \left(\frac{1}{\ell - 1} - \mathbb{E}_p(\mathrm{val}_\ell(|E(\mathbb{F}_p)|)) \right), \tag{23}$$

where $\mathbb{E}_p$ is the operator $\lim_{x\to\infty} \pi(x)^{-1} \sum_{p\leq x}$ and val_ℓ denotes the ℓ-valuation. Then, the series $(\sum_\ell \alpha_\ell(E))$ converges to a limit $\alpha'(E)$.

In the case of CM curves, the definition of $\alpha(E)$ given in Problem 4 and the definition suggested by Peter Montgomery agree. The proog is similar to the proof of [BL17, th 4.1, p. 12].

Proposition 4.7. *If $E/\mathbb{Q}$ is a CM elliptic curve with endomorphism ring included in the quadratic field K, then*

$$2L'/L(1,\chi) = \alpha(E) + \sum_{\ell prime} \Big(\frac{1+\chi(\ell)}{(\ell-1)^2} + \frac{1-\chi(\ell)}{(\ell^2-1)^2} \Big)$$

where χ is the Kronecker character of K.

Proof. Fix $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 1$. We use the factorization $\zeta_K(s) = \zeta(s)L(s,\chi)$ of the Dedekind Zeta function ζ_K of K combined with the fact that the logarithmic derivative of ζ_K at s coincides, up to sign, with the Dirichlet series at s of the von Mangoldt function of K. We obtain

$$\begin{aligned} \frac{\zeta_K'(s)}{\zeta_K(s)} = \frac{L'(s,\chi)}{L(s,\chi)} + \frac{\zeta'(s)}{\zeta(s)} &= -\sum_{k\geq 1,\,\mathfrak{p}} \frac{\log(\mathcal{N}\mathfrak{p})}{(\mathcal{N}\mathfrak{p})^{ks}} \\ &= -\sum_{\ell \text{ prime}} \frac{(1+\chi(\ell))\log \ell}{\ell^s - 1} - \sum_{\ell \text{ prime}} \frac{(1-\chi(\ell))\log(\ell)}{\ell^{2s}-1}. \end{aligned}$$

Using the analogous link between the logarithmic derivative of ζ and the classical von Mangoldt function, we deduce that

$$\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\ell \text{ prime}} \log \ell \Big(\frac{1}{\ell^s - 1} - \frac{1+\chi(\ell)}{\ell^s - 1} \Big) - \sum_{\ell \text{ prime}} \log \ell \frac{1-\chi(\ell)}{\ell^{2s}-1}.$$

Since both sums on the right hand side converge at $s = 1$, we let $s \to 1$ and get

$$\frac{L'(1,\chi)}{L(1,\chi)} = \sum_{\ell \text{ prime}} \log \ell \Big(\frac{1}{\ell - 1} - \frac{1+\chi(\ell)}{\ell - 1} - \frac{1-\chi(\ell)}{\ell^2 - 1} \Big). \tag{24}$$

[4]Peter Montgomery is famous for having invented algorithms and concepts which are very effective in computer science but are not justified rigorously or are not presented as part of a broader theory. For instance the modern presentation [KVV10] of the Montgomery reduction is Barrett's reduction with $\mathbb{Q}_2$ replacing $\mathbb{R}$ whereas the use of Murphy's α to compare polynomials for NFS, originally used by Montgomery, was justified in [BL17].

To connect this expression to the average valuation of $\mathrm{val}_\ell\,|E(\mathbb{F}_p)|$ we recall that in a quadratic field the set of split primes is a finite union of primes in congruence classes. Moreover, the natural densities of all the congruence classes corresponding to split primes sum up to $1/2$, i.e. the natural density of split primes is $1/2$.

By Dirichlet's Theorem, the natural density of split primes is $1/2$.

Let ℓ be a rational prime and $l \in \mathcal{O}_K$ an irreducible algebraic integer above ℓ. Consider the expectancy of $\mathrm{val}\,\ell|E(\mathbb{F}_p)|$ conditional to the fact that p is split in K. Let $a, c \in \mathcal{O}_K$ be two algebraic integers and let $\mu_{a,c}$ be as in Lemma 3.1. We apply once again Dirichlet's Theorem and obtain that the subset of π's such that $\pi - \mu_{a,c} \equiv 0 \bmod l^k$ has natural density $\varphi(c)/\varphi(cl^k) = \frac{1}{(N(l)-1)N(l)^{k-1}}$. Hence, we obtain

$$\begin{aligned} 2\mathbb{E}\{\mathrm{val}_\ell\,|E(\mathbb{F}_p)| : p \text{ is split in- } K\} &= \tfrac{\chi(\ell)+1}{(\ell-1)}\big(\textstyle\sum_{k=1}^{\infty}\frac{1}{\ell^{k-1}}\big) + \tfrac{1-\chi(\ell)}{(\ell^2-1)}\big(\textstyle\sum_{k=1}^{\infty}\frac{1}{\ell^{2(k-1)}}\big) \\ &= \Big(\tfrac{\chi(\ell)+1}{\ell-1} + \tfrac{1-\chi(\ell)}{\ell^2-1}\Big) + \Big(\tfrac{\chi(\ell)+1}{(\ell-1)^2} + \tfrac{1-\chi(\ell)}{(\ell^2-1)^2}\Big). \end{aligned}$$

A similar result holds for the inert primes:

$$\begin{aligned} \mathbb{E}\{\mathrm{val}_\ell\,|E(\mathbb{F}_p)| : p \text{ is inert in- } K\} &= \tfrac{1}{\ell-1}\big(\textstyle\sum_{k=1}^{\infty}\frac{1}{\ell^{k-1}}\big) \\ &= \tfrac{1}{\ell-1} + \tfrac{1}{(\ell-1)^2}. \end{aligned}$$

When we combine with Equation (24) we have

$$2\frac{L'(1,\chi)}{L(1,\chi)} = \sum_{\ell \text{ prime}} \alpha_\ell(E) + \sum_{\ell \text{ prime}} \log \ell\Big(\frac{\chi(\ell)+1}{2}\frac{1}{(\ell-1)^2} + \frac{1-\chi(\ell)}{2}\frac{1}{(\ell^2-1)^2}\Big).$$

□

Example 1. Let us list the values of $\alpha(E)$ and $L'/L(1,\chi)$ for each CM field of class number 1.

d	1	2	3	7	11	19	43	67	163
$\alpha(E)$	4.09	3.96	3.76	4.16	3.69	3.73	3.94	4.15	4.94
$(L'/L)(1,\chi)$	2.13	2.15	2.28	2.46	2.39	2.33	2.37	2.45	2.84

Remark 3. The computation of $L'(1,\chi)/L(1,\chi)$ is slow if one uses a naive evaluation of each of the series $L'(s,\chi)$ and $L(s,\chi)$ (see [Lan22] for a recent algorithm). This gives a second purpose of the formula (23): quickly computing $(L'/L)(1,\chi)$. Note that [BL17] gives bounds on the convergence speed.

Remark 4. In the study of friability of binary forms, Murphy [Mur98] associated a function to irreducible polynomials $f \in \mathbb{Z}[x]$ as follows. For a prime ℓ,

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

where $\mathbb{E}_{(a,b)=1}$ corresponds to natural density for randomly chosen pairs of integers (a,b) which are relatively prime; the convergence of the series is proven in [BL17, §2.2]. Hence $\alpha(E)$ has a very similar expression to $\alpha(f)$ with f such that $K \simeq \mathbb{Q}[x]/(f)$, the difference residing in the condition $(a,b) = 1$.

5 The set $\Psi_{E,z}(x,y)$: proof of Theorem 1.3

This section is devoted to the proof of Theorem 1.3. We first state and prove a lemma, which is a variation on the fact that a set of primes which has a natural density also has an analytic (or logarithmic) density (see [Ten15, §III.1]).

Lemma 5.1. *Let Q be a set of primes and, for $x \geq 2$, let $\Pi_Q(x) = Q \cap [1,x]$. In the case where Q is the set of all primes, we will simply write $\Pi(x)$ for $\Pi_Q(x)$. Assume that there exists a positive non increasing function $\lambda(x)$ and a constant $\omega > 0$ such that for all $x \geq 2$,*

$$\frac{|\Pi_Q(x)|}{|\Pi(x)|} - \lambda(x) \ll \frac{1}{\big(\log_2 x\big)^{1+\omega}}\,.$$

Then we have

$$\frac{\sum_{p\in\Pi_Q(x)} p^{-1}}{\sum_{p\in\Pi(x)} p^{-1}} = \lambda(x)(1+o(1)) + O\Big(\frac{1}{(\log_2 x)^{1+\omega}}\Big)\,.$$

Proof. First note that

$$\sum_{p\in\Pi_Q(x)} p^{-1} = \sum_{n=1}^{\lfloor x\rfloor} \frac{|\Pi_Q(n)| - |\Pi_Q(n-1)|}{n}\,.$$

An Abel summation then yields

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

Now we use the Prime Number Theorem under the form $|\Pi(x)| = (x/\log x)(1+o(1))$. We obtain:

$$\sum_{n=1}^{\lfloor x\rfloor} \frac{|\Pi_Q(n)|}{n(n+1)} = \sum_{n\leq x} \lambda(n)\Big(\frac{1}{n\log n} + o(n^{-2})\Big) + O\Big(\sum_{n\leq x} \frac{1}{n\log n(\log_2 n)^{\omega+1}}\Big)\,. \tag{25}$$

To handle the error term we make use of Cauchy's condensation criterion. Precisely

$$\sum_{n\leq x} \frac{1}{n\log n(\log_2 n)^{\omega+1}} \ll \sum_{1\leq 2^k\leq x} \frac{2^k}{2^k\log(2^k)\log_2(2^k)^{\omega+1}} \ll \sum_{k\leq \log x} \frac{1}{k(\log k)^{\omega+1}} \ll (\log_2(x))^{-\omega}\,.$$

Plugging this into (25) and using the fact that $\lambda(n) \geq \lambda(x)$ for all $n \leq x$, one deduces that

$$\begin{aligned}\sum_{n=1}^{\lfloor x\rfloor} \frac{|\Pi_Q(n)|}{n(n+1)} &= \lambda(x)\Big(\sum_{n\leq x} \frac{1}{n\log n} + O(1)\Big) + O\big((\log_2 x)^{-\omega}\big)\\ &= \lambda(x)\log_2 x(1+o(1)) + O\big(\lambda(x) + (\log_2 x)^{-\omega}\big).\end{aligned}$$

Finally, the term $|\Pi_Q(x)|/\lfloor x\rfloor$ has size $\frac{\lambda(x)}{\log x}(1+o(1)) + O(\frac{1}{\log x(\log_2 x)^{1+\omega}})$, which is negligible compared to the left hand side of (25). The proof of the lemma is finished by using Dirichlet's estimate $\sum_{p\in\Pi(x)} p^{-1} = \log_2 x + O(1)$. □

Proof of Theorem 1.3. Let $Q = \{p \text{ prime} : |E(\mathbb{F}_p)| \text{ is } z\text{-friable}\}$ and recall that $z = y^{1/v}$.

$$\begin{aligned}\frac{\psi_{E,z}(x,y)}{\psi(x,y)} &= \Big(\sum_{p\in Q,\, p\le y} \psi(x/p,y)\Big)\cdot\Big(\sum_{p\le y}\psi(x/p,y)\Big)^{-1}\\ &= \Big(\sum_{p\in Q,\, p\le y} \frac{x}{p}\varrho(u)(1+\varepsilon(x,y,p))\Big)\cdot\Big(\sum_{p\le y}\frac{x}{p}\varrho(u)(1+\varepsilon(x,y,p))\Big)^{-1},\end{aligned}$$

where $\varepsilon(x,y,p) = (\psi(x/p,y) - (x/p)\varrho(u))/((x/p)\varrho(u))$. The case $h=1$, $a_0=1$, of Theorem 4.5 yields the well known estimate

$$\psi(x,y) = x\varrho(u)\left(1 + O\left(\frac{\log(u+1)}{\log y}\right)\right).$$

Moreover for any $u \in \Delta$, on has $\frac{\log(u+1)}{\log y} \ll \frac{\log_2 x}{\log x}$; in particular $\varepsilon(x,y,p) = O(\frac{\log(u+1)}{\log y}) = O(\frac{1}{(\log x)^{\omega}})$ for any fixed $0<\omega<1$ and for $u\in\Delta$. We obtain

$$\psi_{E,z}(x,y) = \psi(x,y)\big(1+O(\tfrac{\log(u+1)}{\log y})\big)\Big(\sum_{p\in Q,\, p\le y} 1/p\Big)\cdot\Big(\sum_{p\le y}1/p\Big)^{-1}.$$

In order to apply Lemma 5.1, we invoke Theorem 1.2(2) which asserts that

$$\frac{\psi_E(y,z)}{|\Pi(x)|} - \varrho(v) \ll \delta(y)v\,.$$

Here we fix $\beta>0$ such that $\delta(y)v \ll (\log_2 y)^{-1-\beta}\log_3 y(\log_4 y)^{-1}$. This is $\ll (\log_2 y)^{-1-\frac{\beta}{2}}$. Therefore, by Lemma 5.1 we have that

$$\Big(\sum_{p\in Q,\, p\le y} 1/p\Big)\cdot\Big(\sum_{p\le y}1/p\Big)^{-1} = \varrho(v)(1+o(1)) + O\big((\log_2 y)^{-1-\frac{\beta}{2}}\big).$$

Hence we infer

$$\begin{aligned}\psi_{E,z}(x,y) &= x\varrho(u)\Big(1+O(\frac{\log(u+1)}{\log y})\Big)\varrho(v)(1+o(1)) + O\big((\log_2 y)^{-1-\frac{\beta}{2}}\big)\\ &= x\varrho(u)\varrho(v)(1+o(1))\,.\end{aligned}$$

□

6 The case of non CM elliptic curves

It is interesting to investigate potential analogues of Theorem 3.4 in the non CM case. This section suggests such an analogue and highlights its theoretical limitations. Let $E/\mathbb{Q}$ be a non CM elliptic curve. Deuring's Theorem (Lemma 3.1) enabled us in the CM case to relate $\psi_E(x,y)$ to the count of primes in arithmetic progressions. In the non CM case a natural choice for the analogous prime counting function is the following:

$$\pi_E(x;d) = |\{p\le x\colon d \mid |E(\mathbb{F}_p)|\}|\,.$$

In celebrated work [Ser72], Serre shows the existence of an integer M_E depending only on E, such that for n coprime with M_E, the Galois group G_n of the n-torsion field extension $E[n](\overline{\mathbb{Q}})/\mathbb{Q}$ is isomorphic to the full group $\mathrm{GL}_2(\mathbb{Z}/\mathbb{Z})$. Moreover one has additional multiplicativity property

$G_{mn} \simeq G_m \times G_n$ for any m coprime with n. David and Wu [DW12, Proof of Lemma 4.1] give an asymptotic development under GRH for the Dedekind zeta function of $\mathbb{Q}(E[d](\overline{\mathbb{Q}}))$ when d is coprime to M_E and squarefree:

$$\pi_E(x;d) = \frac{w(d)}{d}\,\mathrm{Li}(x) + O_E(d^{3/2}x^{1/2}\log(dx))\,, \tag{26}$$
$$w_E(d) = \prod_{\substack{\ell \mid d \\ \ell \text{ prime}}} \frac{\ell^2(\ell^2-2)}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} = \prod_{\substack{\ell \mid d \\ \ell \text{ prime}}} \frac{\ell(\ell^2-2)}{(\ell-1)(\ell^2-1)}\,.$$

In the spirit of the Bombieri–Vinogradov Theorem and of its expected generalization Conjecture 1.1, it is tempting to expect some strong average version of (26) over d. The following results are evidence for the validity of this "Elliott–Halberstam phenomenon" that we next state (Hypothesis 1 below).

Theorem 6.1. *Let $E/\mathbb{Q}$ be a non CM elliptic curve and assume the GRH for Dedekind Zeta functions.*

1. *One has ([Kow06, Prop. 3.8]):*

$$\sum_{d \le x^{\frac{1}{4}}/(\log x)^2} \varphi(d)|\{p \le x\colon E[d](\overline{\mathbb{Q}}) \subset E(\mathbb{F}_p)\}| = \left(\sum_{d \ge 1} \frac{\varphi(d)}{|G_d|}\right)\mathrm{Li}(x) + O_E\Big(\frac{x}{(\log x)^3}\Big)$$

2. *One has ([DW12, (4.7)]):*

$$\sum_{\substack{d \le x^{\frac{1}{5}}/(\log x)^4 \\ p \mid d \Rightarrow M_E < p \le x^{1/10}/(\log x)^4}} 2^{\omega(d)}\mu(d)^2\Big|\pi_E(x;d) - \frac{w_E(d)}{d}\,\mathrm{Li}(x)\Big| \ll_E \frac{x}{(\log x)^3}\,.$$

Regarding point 2 of Theorem 6.1, we follow Pollack who studied the elliptic curve analogue of the Titchmarsh divisor problem ([Pol16, p.185]):

"We pretend that this approximation is valid for d up to size $\approx x$, at least on average".

This gives rise to the following hypothesis inspired by Conjecture 1.1.

Hypothesis 1. Let $E/\mathbb{Q}$ be a non CM elliptic curve. Then one has:

$$\sum_{d \le X}\Big|\pi_E(x;d) - \frac{w_E(d)}{d}\,\mathrm{Li}(x)\Big| \ll_{E,\omega} \frac{x}{(\log x)^\omega}\,,$$

for any $X \le x^{1-\delta}$, $x \ge 2$, for any constant $\omega > 0$, and where one extends w_E to a function on $\mathbb{N}$ satisfying $w_E(mn) = w_E(m)w_E(n)$ for any coprime integers m, n such that either m or n is coprime to M_E (see [DW12, §2]).

Note that Hypothesis 1 allows any exponent $\omega > 0$ on the denominator of the upper bound. This mimicks the upper bound appearing in the Elliott–Halberstam conjecture 1.1; moreover we believe that there was no attempt to optimize the exponent 3 appearing in the upper bounds of Theorem 6.1 in the works of Kowalski and David–Wu. Finally, as in the proof of Theorem 3.4, we need an exponent $\omega > 6$ to conclude the proof of Theorem 6.2.

Hypothesis 1 enables us to prove the following analogue of Theorem 3.4.

Theorem 6.2. *For any $x \geq 2$ and $y \in [1, x]$ we set $u = \frac{\log x}{\log y}$. Assume Hypothesis 1 for a non CM elliptic curve $E/\mathbb{Q}$. Then, as $x \to \infty$ and y is such that $u \leq u_0$, for some fixed constant u_0, we have*

$$\psi_E(x, y) \sim \mathrm{Li}(x)\varrho(u)\,.$$

Proof. The argument is a verbatim translation of the proof of Theorem 3.4. We fix $\delta > 0$. By Möbius inversion we split the studied prime counting function:

$$\psi_E(x, y) = \Big|\Big\{p \leq x \colon \gcd\big(|E(\mathbb{F}_p)|, \prod_{\substack{\ell \text{ prime} \\ \ell > y}} \ell\big) = 1\Big\}\Big| = S_1 + S_2,$$

where

$$S_1 = \sum_{\substack{q \leq x^{1-\delta} \\ P^-(q) > y}} \mu(q)\pi_E(x; q)\,, \qquad S_2 = \sum_{\substack{x + 2\sqrt{x} \geq q > x^{1-\delta} \\ P^-(q) > y}} \mu(q)\pi_E(x; q)\,.$$

Note that the upper bound on q in the index set of S_2 comes from the Hasse–Weil bound on $|E(\mathbb{F}_p)|$. We next decompose $S_1 = S_1' + S_1''$ where

$$S_1' = \mathrm{Li}(x) \sum_{\substack{q \leq x^{1-\delta} \\ P^-(q) > y}} \frac{\mu(q) w_E(q)}{q}\,, \qquad S_1'' = \sum_{\substack{q \leq x^{1-\delta} \\ P^-(q) > y}} \mu(q) r(x, q)\,,$$

and where $r(x, q) = \pi_E(x; q) - \mathrm{Li}(x)\frac{w_E(q)}{q}$. Since u remains bounded, we may assume that $M_E < y \leq x$, so that w_E is multiplicative on all integers q such that $P^-(q) > y$. If in addition q is squarefree, the formula (26) for $w_E(q)$ is valid and yields $w_E(q) = 1 + O((P^-(q))^{-1})$. We compute

$$\begin{aligned}\frac{S_1'}{\mathrm{Li}(x)} &= \sum_{\substack{q \leq x^{1-\delta} \\ P^-(q) > y\,, \gcd(q, M_E) = 1}} \frac{\mu(q) w_E(q)}{q} = \sum_{\substack{q \leq x^{1-\delta} \\ P^-(q) > y}} \frac{\mu(q)}{q} + O\Big(\sum_{\substack{q \leq x^{1-\delta} \\ P^-(q) > y}} \frac{1}{qP^-(q)}\Big) \\ &\sim \varrho(u) + O\Big(\frac{1}{y} \sum_{q \leq x^{1-\delta}} \frac{1}{q}\Big) \qquad (x \to \infty,\, u \ll 1)\,,\end{aligned}$$

where we have used Lemma 3.3. Finally, the fact that $u \ll 1$ implies that the error term is $O((\log y)/y) = o(1)$ as $x \to \infty$. This establishes $S_1' \sim \varrho(u)\,\mathrm{Li}(x)$ as $x \to \infty$ with $u \ll 1$.

As in the proof of Theorem 3.4 (step $1''$), we show that $S_1'' = O(x/(\log x)^\omega)$ by virtue of Hypothesis 1. In particular, for bounded u, one has $S_1'' = o(\mathrm{Li}(x)\varrho(u))$.

We turn to the evaluation of S_2. As in the proof of Theorem 3.4, we use Lemma 3.2 to obtain the following upper bound: $|S_2| \ll S_2' + S_2''$. Here we define

$$S_2' = \sum_{m \leq x^\delta} \mathrm{Li}(x) \frac{w_E(m)}{m} \prod_{\substack{p \in \mathcal{P},\, p < z \\ p \nmid m M_E}} \Big(1 - \frac{w_E(p)}{p}\Big)\,, \qquad S_2'' = \sum_{m \leq x^\delta} \sum_{\substack{d < D \\ d \mid P(z)}} |r(x, md)|\,,$$

where $z = D = 1 - 2\delta$, the parameter ca' has to be replaced by M_E to define the set of primes $\mathcal{P}$ and where, for $p \in \mathcal{P}$, we choose $w(p) = w_E(p)$ (which satisfies the hypotheses of Lemma 3.2 as shown in [DW12, Proof of Lemma 4.1]). We denote by $P(z)$ the product of primes in $\mathcal{P}$ that are less than z. The fact that $(1 - \frac{w_E(p)}{p})/(1 - \frac{1}{p}) = 1 + O(\frac{1}{p^2})$ for $p \in \mathcal{P}$ implies that the

method used in the proof of Theorem 3.4 to handle the contribution of S_2' also yields in the present case[5] that $S_2' = O(\delta \operatorname{Li}(x)u)$.

Finally, to obtain the bound for $S_2'' = o(\operatorname{Li}(x))$ we argue as in the proof of Theorem 3.4, invoking Hypothesis 1 for a fixed $\omega > 6$. We conclude by letting $\delta \to 0$.

□

A Alternative proof of Corollary 4.3

We prove the following form of Corollary 4.3, using the same method as for Theorem 3.4 (*i.e* an adaptation of Wang's approach [Wan18]).

Proposition A.1. *Let K be $\mathbb{Q}$ or an imaginary quadratic field of class number 1. Let $a, c \in \mathcal{O}_K$ be fixed and let $\mu \in \mathcal{O}_K^\times$. Let $C \in (0, \frac{1}{2})$ and $\beta \in (2C, 1)$. Assuming Conjecture 4.1, we have*

$$\psi_K(x, y; c, a, \mu) = \frac{\operatorname{Li}(x)}{\varphi(c)} \varrho(u) \left(1 + O\left(\delta(x)^{1-\beta} u \log u)\right)\right) \qquad (x \to \infty)$$

uniformly for $2 \le u := \log x/\log y \le C \log_2 x/\log_3 x$ and $\delta(x) \in (\frac{\log_2 x}{\eta \log x}, (\log x)^{-2C/\beta})$.

Proof. Let $\varepsilon(x, y) = \delta u \log u$. Recall that $\delta(x)$ satisfies the assumptions of Conjecture 4.1.

We follow through the steps of the proof of Theorem 3.4. We split $\psi_K(x, y; c, a, \mu) = S_1 + S_2$ with S_1 and S_2 as in Equation (11) (up to replacing δ by $\delta(x)$). We write $S_1 = S_1' + S_1''$ as in Equation (12) and we upper bound $|S_2| \le S_2' + S_2''$ as in Equation (17).

Step 1′. We show that $S_1' = \frac{\operatorname{Li}(x)}{\varphi(c)} \varrho(u)(1 + o(\varepsilon(x, y)))$. By Lemma 3.3 we have

$$S_1' = \frac{\operatorname{Li}(x)}{\varphi(c)} \sum_{\substack{q \in \mathcal{O}_K,\, \|q\| \le x^{1-\delta} \\ P^-(\|q\|) > y}} \frac{\mu(q)}{\varphi(q)} = \frac{\operatorname{Li}(x)}{\varphi(c)} \Big(\varrho\big(\frac{\log(x^{1-\delta(x)})}{\log y}\big) + O(\exp(-(\log y)^{\frac{3}{5}-\epsilon})) \Big). \qquad (27)$$

Note that $u \ll \log_2 x/\log_3 x$ implies that $\log y \gg \log x \log_3 x/\log_2 x$ (so that y lies in the range of validity for Lemma 3.3) In particular the error term in (27) is $o(\delta(x)\varrho(u)u \log u)$. Indeed one has

$$\begin{aligned} \frac{\mathrm{e}^{-(\log y)^{\frac{3}{5}-\epsilon}}}{\varrho(u)} &\ll \mathrm{e}^{-(\log y)^{\frac{3}{5}-\epsilon} + 2u \log u} \\ &\ll \exp\Big(- \big(\log x \frac{\log_3 x}{\log_2 x}\big)^{\frac{3}{5}-\epsilon} + O\big(\log_2 x (1 - \frac{\log_4 x}{\log_3 x})\big)\Big) \ll 1 \end{aligned}$$

where we have also used the lower bound $\varrho(u) \gg \exp(-2u \log u)$ coming from (4).

Finally, using (4) again, we compute (writing δ instead of $\delta(x)$, for simplicity):

$$\log\Big(\varrho\big(\frac{\log(x^{1-\delta})}{\log y}\big)\Big) - \log(\varrho(u))) = -u(1-\delta)(\log u + \log(1-\delta)) + u \log u + O(u \log_2 u)\,.$$

Hence $\varrho\left(\frac{\log(x^{1-\delta(x)})}{\log y}\right)/\varrho(u) = 1 + O(\delta(x) u \log u)$ which proves the stated estimate for S_1'.

Step 1″. We show that $S_1'' = o(\operatorname{Li}(x)\varrho(u)\varepsilon(x, y))$. To do so we apply Conjecture 4.1 in the same way we applied Conjecture 1.1 in the proof of Theorem 3.4. We fix $\omega > 2C - 2$ where C is an absolute constant such that we work undfer the restriction $u \le C \log_2 x/\log_3 x$. The exact

[5] Alternatively, one could appeal to [DW12, (4.3), (4.9)] to estimate the inner product over primes in the upper bound for S_2'.

same argument as the one used to obtain (14) yields $S_1'' = O(\mathrm{Li}(x)/(\log x)^{\omega-1})$. The point is that Conjecture 4.1 asserts that the implied constant in this upper bound is uniform in u. We now compute, using again the bound $\varrho(u) \gg \exp(-2u\log u)$ and the fact that $u\log u$ grows as $x \to \infty$,

$$\frac{S_1''}{\mathrm{Li}(x)\varrho(u)\varepsilon(x,y)} \ll \frac{\mathrm{e}^{2u\log u}}{(\log x)^{\omega-1}\delta(x)u\log u} \ll \frac{(\log_2 x)\mathrm{e}^{2u\log u}}{(\log x)^{\omega-2}u\log u} \ll \frac{(\log_2 x)\exp(2C\log_2 x)}{(\log x)^{\omega-2}} \ll \frac{\log_2 x}{(\log x)^{\omega-2C-2}}\,.$$

Step 2′. We prove that $S_2' = O\big(\mathrm{Li}(x)\frac{\delta(x)}{1-2\delta(x)}u\big)$ in the exact same way as for (18) (where the implied constant is absolute). From the bound $1-2\delta(x) \geq 1-2\eta \gg 1$ (recall Conjecture (4.1)), we conclude that

$$\frac{\delta(x)^\beta S_2'}{\varrho(u)\,\mathrm{Li}(x)\varepsilon(x,y)} \ll \frac{\delta(x)^\beta}{\varrho(u)} \ll \delta(x)^\beta \mathrm{e}^{2C\log_2 x} \ll 1\,.$$

Therefore we have $S_2' = O(\mathrm{Li}(x)\delta(x)^{1-\beta}\varrho(u)u\log u)$.

Step 2″. We prove that $S_2'' = o(\mathrm{Li}(x)\varrho(u)\varepsilon(x,y))$. As in the proof of (19), we have

$$S_2'' = O\Big(\frac{\mathrm{Li}(x)}{(\log x)^{\frac{\omega}{2}-3}}\Big)$$

with an implied constant depending only on ω. We then argue as in Step 1″ above by requiring this time that $\omega > 4C+4$. This concludes step 2″ and the proof of Proposition A.1. □

B Numerical illustration

We consider the examples $E_7\colon y^2+xy = x^3-x^2-2x-1$ and $E_{11}\colon y^2+y = x^3-x^2-7x+10$ which have endomorphism rings included in $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-11})$, respectively.

Our numerical experiment (see Figure 1) can be seen as a type of *Chebyshev race*[6] between E_7 and E_{11}: we compare $\psi_{E_7}(x,2^7)$ and $\psi_{E_{11}}(x,2^7)$ for various values of x. The data shows that E_7 is "always ahead", in other words, E_7 is more ECM-friendly than E_{11} for these values of x and y. We repeat this Chebyshev race for $y = 2^{25}$ and obtain the same conclusion. This suggests the following conjecture: E_7 is more ECM-friendly than E_{11} uniformly for x and y when y grows with x and is not too large compared to x.

In Figure 2 we search for an accurate expression for the error term in the asymptotic expansion of $\psi_E(x,y)$. First we plot the expression which is given by Scourfield's Theorem 4.4 $\varrho(u)+\frac{\log(u+1)}{\log y}\alpha_K$. The data corroborates the accuracy of this theoretical value. We also plot the expression $\alpha_K := \log(\frac{\frac{\psi_K(x,y)}{\psi_K(x,\infty)}\varrho(u)^{-1}-1}{\log(u+1)/\log y})$ which converges to a constant when $u = 1.5$. The data is consistent with the conjecture asserting that $\log(\psi_E(x,y)/\psi_E(x,\infty))$ has the same main error term as $\log(\psi(x,y)/\psi(x,\infty))$. The data suggests that α_E is a constant (it does not coincide with α_K since one takes into account both the split and inert primes).

[6] In an 1853 letter, Chebyshev observes that the count of primes up to x that are 3 modulo 4, almost always exceeds that of primes that are 1 modulo 4. Modern instances of what is now called a "prime number race" have been extensively studied in the recent years.

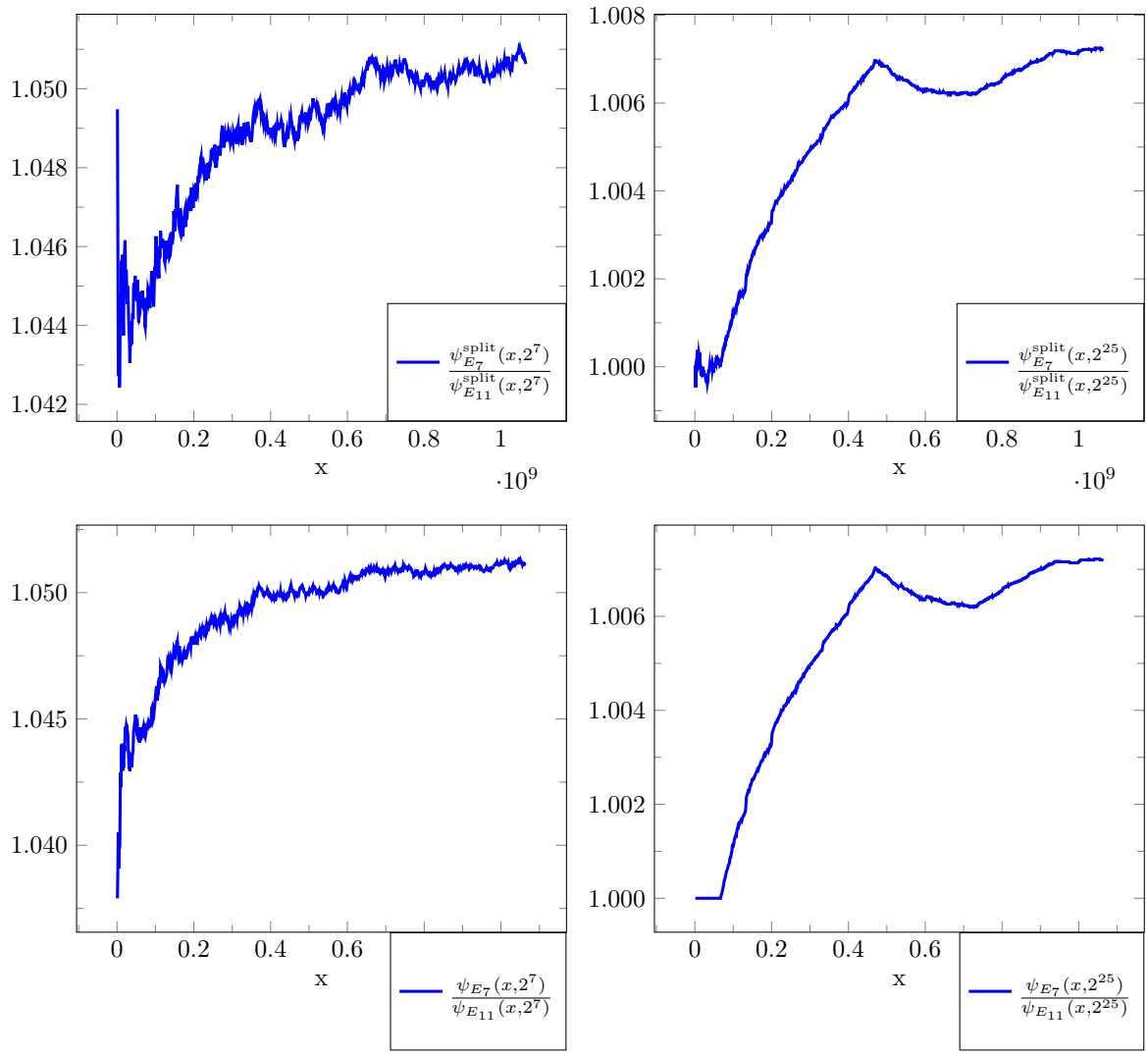

Figure 1: Comparison between $\psi_E(x, y)$ and $\psi_K(x, y)$ when E is CM and $K = \text{End}(E) \otimes \mathbb{Q}$.

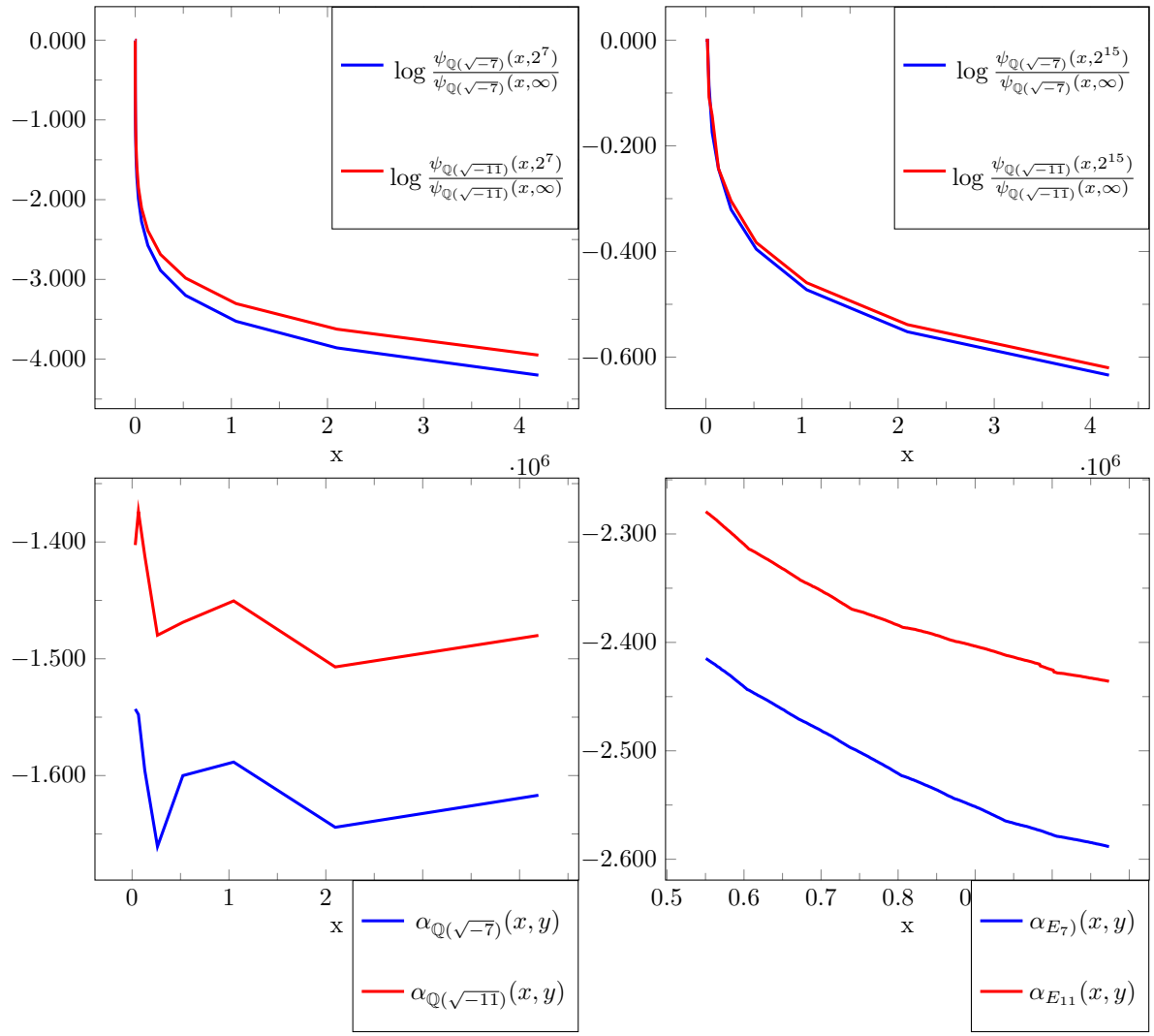

Figure 2: $\alpha_K(x,y) := \log(\frac{\frac{\psi_K(x,y)}{\psi_K(x,\infty)}\rho(u)^{-1}-1}{\log(u+1)/\log y})$ and $\alpha_E(x,y) := \log(\frac{\frac{\psi_E(x,y)}{\psi_E(x,\infty)}\rho(u)^{-1}-1}{\log(u+1)/\log y})$

References

[BGK+] Shi Bai, Pierrick Gaudry, Alexander Kruppa, François Morain, Emmanuel Thomé, and Paul Zimmermann. Crible algébrique: Distribution, optimisation—number field sieve (cado-nfs).

[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.

[CS06] An Commeine and Igor Semaev. An algorithm to solve the discrete logarithm problem with the number field sieve. In *Public Key Cryptography – PKC 2006*, volume 3958 of *Lecture Notes on Computer Science*, pages 174–190. Springer, 2006.

[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.

[DW12] C. David and J. Wu. Pseudoprime reductions of elliptic curves. *Canadian Journal of Mathematics*, 64(1):81–101, 2012.

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

[HT86] Adolf Hildebrand and Gérald Tenenbaum. On integers free of large prime factors. *Transactions of the American mathematical society*, 296(1):265–290, 1986.

[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.

[Hux71] MN Huxley. The large sieve inequality for algebraic number fields III. zero-density results. *Journal of the London Mathematical Society*, 2(2):233–233, 1971.

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

[Kow06] E. Kowalski. Analytic problems for elliptic curves. *J. Ramanujan Math. Soc.*, 21(1):19–114, 2006.

[KVV10] Miroslav Knezevic, Frederik Vercauteren, and Ingrid Verbauwhede. Faster interleaved modular multiplication based on barrett and montgomery reduction methods. *IEEE Transactions on Computers*, 59(12):1715–1721, 2010.

[Lan22] Alessandro Languasco. On computing $l'/l(1,\chi)$. In *Proceedings of the 5th Number Theory Meeting*, 2022.

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

[LLJMP93] Arjen K Lenstra, Hendrik W Lenstra Jr, Mark S Manasse, and John M Pollard. The number field sieve. In *The development of the number field sieve*, volume 1554 of *Lecture notes in mathematics*, pages 11–42. Springer, 1993.

[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.

[May15] James Maynard. Small gaps between primes. *Ann. of Math. (2)*, 181(1):383–413, 2015.

[MBKL14] Andrea Miele, Joppe W. Bos, Thorsten Kleinjung, and Arjen K. Lenstra. Cofactorization on graphics processing units. In *Cryptographic Hardware and Embedded Systems – CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 335–352, 2014.

[Mon92] Peter Lawrence Montgomery. *An FFT extension of the elliptic curve method of factorization*. PhD thesis, University of California, Los Angeles, 1992.

[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.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[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.

[Wil23] B. M. Wilson. Proofs of Some Formulae Enunciated by Ramanujan. *Proc. London Math. Soc. (2)*, 21:235–255, 1923.

[Zha14] Yitang Zhang. Bounded gaps between primes. *Ann. of Math. (2)*, 179(3):1121–1174, 2014.