AVERAGE FROBENIUS DISTRIBUTION FOR INERTS IN $\mathbb{Q}(i)$

CHANTAL DAVID AND FRANCESCO PAPPALARDI

Abstract. Given an integer r, we consider the problem of enumerating the inert prime ideals $\mathfrak{p}$ of $\mathbb{Q}(i)$ for which a given elliptic curve E has trace of Frobenius at $\mathfrak{p}$ equal to r. We prove that on average the number of such prime ideals up to x is asymptotic to $c_r \log\log x$ where c_r is an explicit constant computed in terms of an Euler product. This result is in accordance with the standard heuristics. This problem generalises naturally the classical Lang-Trotter conjecture for elliptic curves over $\mathbb{Q}$.

1. Introduction

Let E be an elliptic over a number field $K/\mathbb{Q}$ with a minimal model over the ring of integers $\mathcal{O}_K$. Let $\mathfrak{D}(E/K)$ be the discriminant of E/K, which is an ideal of $\mathcal{O}_K$. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ not dividing $\mathfrak{D}(E/K)$, E has good reduction modulo $\mathfrak{p}$, and we consider the elliptic curve $E_\mathfrak{p}$ over the finite field $\mathcal{O}_K/\mathfrak{p}$ with

$$|E_\mathfrak{p}(\mathcal{O}_K/\mathfrak{p})| = N(\mathfrak{p}) + 1 - a_\mathfrak{p}(E)$$

where the norm $N(\mathfrak{p}) = p^f$ is the number of elements of the finite field $\mathcal{O}_K/\mathfrak{p}$ and $\deg_K(\mathfrak{p}) = f$. The trace of Frobenius $a_\mathfrak{p}(E)$ verifies the Hasse bound

$$|a_\mathfrak{p}(E)| \leq 2\sqrt{N(\mathfrak{p})} = 2p^{f/2}.$$

Note that E has supersingular reduction at $\mathfrak{p}$ if and only if $p \mid a_\mathfrak{p}(E)$.

If f is a divisor of $[K:\mathbb{Q}]$, r is any integer, and

$$\pi_E^{r,f}(x) = \#\left\{\mathfrak{p} \;\mid\; N(\mathfrak{p}) \leq x,\ \deg_K(\mathfrak{p}) = f,\ \text{and } a_\mathfrak{p}(E) = r\right\},$$

the classical heuristic argument of Lang–Trotter [13] suggests the following conjecture

Conjecture 1.1. *Let K be a number field, and E be an elliptic curve defined over K without complex multiplication. Let f be a positive integer dividing $[K:\mathbb{Q}]$, and let r be any integer. Then, there exists a constant $c_{E,r,f} \in \mathbb{R}^{\geq 0}$ such that*

$$\pi_E^{r,f}(x) \sim c_{E,r,f} \begin{cases} \dfrac{\sqrt{x}}{\log x} & \textit{if } f = 1 \\ \log\log x & \textit{if } f = 2 \\ 1 & \textit{otherwise} \end{cases}.$$

The constant $c_{E,r,f}$ can be 0, and the asymptotic relation is then interpreted to mean that there are only finitely many such primes.

Date: July 11, 2003.

1991 *Mathematics Subject Classification.* 11F80 (11G05).

The first author is supported in part by NSERC, by GNSAGA from INDAM, and the second author is supported by INDAM.

To obtain evidence for this generalised Lang–Trotter conjecture, it is natural to consider average versions of the conjecture. One considers the function

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\pi_E^{r,f}(x)$$

where $\mathcal{C}$ is a suitable set of elliptic curves which may depend on x.

In this paper we will prove the following:

Theorem 1.2. *Let r be a non zero integer. Let $K=\mathbb{Q}(i)$ and let $\mathcal{C}_x$ denote the set of elliptic curves $E: Y^2=X^3+\alpha X+\beta$ with $\alpha=a_1+a_2i, \beta=b_1+b_2i\in\mathbb{Z}[i]$ and $\max\{|a_1|,|a_2|,|b_1|,|b_2|\}\le x\log x$. Then for $r\neq 0$,*

$$\frac{1}{|\mathcal{C}_x|}\sum_{E\in\mathcal{C}_x}\pi_E^{r,2}(x)\sim c_r\log\log x$$

where

$$c_r=\frac{1}{3\pi}\prod_{l>2}\frac{l(l-1-\left(\frac{-r^2}{l}\right))}{(l-1)(l-\left(\frac{-1}{l}\right))}.$$

If $r=0$, then

$$\frac{1}{|\mathcal{C}_x|}\sum_{E\in\mathcal{C}_x}\pi_E^{0,2}(x)<\infty.$$

It is easy to see that the product that defines c_r converges. Furthermore,

$$\prod_{l>2}\frac{l(l-1-\left(\frac{-1}{l}\right))}{(l-1)(l-\left(\frac{-1}{l}\right))}=\prod_{l>2}\left(1-\frac{\left(\frac{-1}{l}\right)}{(l-1)(l-\left(\frac{-1}{l}\right))}\right)\approx 1.07820$$

Let us review the classical case. Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. For all primes p of good reduction (*i.e.* $p\nmid N_E$), E reduces to an elliptic curve over $\mathbb{F}_p$ with $p+1-a_p(E)$ points where $|a_p(E)|\le 2\sqrt{p}$ by Hasse's Theorem. The case $a_p(E)=0$ corresponds to supersingular reduction. Fixing any $r\in\mathbb{Z}$, let

$$\pi_{E,r}(x)=\#\left\{p\le x : a_p(E)=r\right\}.$$

If E has complex multiplication, Deuring showed that $a_p(E)=0$ for half of the primes. For all other cases, Lang and Trotter [13] conjectured that

$$\pi_{E,r}(x)\sim C_{E,r}\frac{\sqrt{x}}{\log x} \tag{1.1}$$

for some $C_{E,r}\in\mathbb{R}^{\ge 0}$. To this date, no (non–trivial) case of the Lang–Trotter conjecture is known; in fact, it is not even known if $\pi_{E,r}(x)$ is unbounded, except for the case $r=0$ where Elkies [5] obtained lower bounds for $\pi_{E,0}(x)$. In [6], Elkies extends his proof to show that for any number field K which is not totally imaginary, any elliptic curve E/K has infinitely many supersingular primes. The result is also believed to be true for number fields which are totally imaginary, but the proof does not seem to generalise to this case.

To explain the obstruction from generalising his proof to totally imaginary fields, Elkies studies the following example. Let E be an elliptic curve over $K=\mathbb{Q}(\sqrt{-3})$ with K-rational 3-torsion. Let p be a rational prime which splits in K, say $p\mathcal{O}_K=\mathfrak{p}_1\mathfrak{p}_2$. Then, $p\equiv 1 \mod 3$, and for $i=1,2$, we have $3\mid p+1-a_{\mathfrak{p}_i}(E)$. Therefore, $a_{\mathfrak{p}_i}(E)$ cannot be 0, and there are no supersingular split primes. Let p be an inert prime in K, say $p\mathcal{O}_K=\mathfrak{p}$. Then, $|a_{\mathfrak{p}}(E)|\le 2p$, and $\mathfrak{p}$ is supersingular when

$a_{\mathfrak{p}}(E) = 0, \pm p, \pm 2p$. As $p \equiv 2 \mod 3$ and $3 \mid p^2 + 1 - a_{\mathfrak{p}}(E)$, the only possible values are $a_{\mathfrak{p}}(E) = p, -2p$. One then expects the number of supersingular primes to be proportional to

$$\sum_{p \leq x} \frac{1}{p} \sim \log \log x.$$

Then, the set of supersingular prime is much thinner than what is expected for elliptic curves over $\mathbb{Q}$ in (1.1). Similar obstructions also arise for elliptic curves over $\mathbb{Q}$ (for example, if $E/\mathbb{Q}$ has rational 3-torsion, then a similar argument shows that $a_p(E) = 1$ is impossible), but never for the supersingular case. This is one of our motivations for studying the densities $\pi_E^{r,2}(x)$ averaging over all elliptic curves defined over $\mathbb{Q}(i)$. The cases $r = 0, \pm p, \pm 2p$ which are particularly relevant to the example above are treated in Section 5.

Upper bounds were first obtained by Serre using the Cebotarev Density Theorem [18]. Further improvements and generalisations were later obtained by Elkies, Kaneko, K. Murty, R. Murty, Saradha and Wan [7, 15, 16, 22]. We refer the reader to a recent paper of K. Murty [17] for a complete account.

The average problem, for $K = \mathbb{Q}$ and $r = 0$ (the supersingular case) has been studied by Fouvry and Murty [8], and the general case ($K = \mathbb{Q}$ and $r \in \mathbb{Z}$) by the authors [4]. They proved that if $\mathcal{C}_x$ is the set of elliptic curves that admit a Weierstrass model $Y^2 = X^3 + aX + b$ with $|a| \leq x \log^2 x$, $|b| \leq x \log^2 x$, then

$$\frac{1}{|\mathcal{C}_x|} \sum_{E \in \mathcal{C}_x} \pi_E^{r,1}(x) \sim c_r \frac{\sqrt{x}}{\log x} \quad \text{as } x \to \infty \tag{1.2}$$

where

$$c_r = \frac{2}{\pi} \prod_{l \mid r} \left(1 - \frac{1}{l^2}\right)^{-1} \prod_{l \nmid r} \frac{l(l^2 - l - 1)}{(l-1)(l^2-1)} = \frac{2}{\pi} \prod_{l} \frac{l |\operatorname{GL}_2(\mathbb{F}_l)^{Tr=r}|}{|\operatorname{GL}_2(\mathbb{F}_l)|}, \tag{1.3}$$

and $G^{Tr=r}$ denotes the set of elements of G with trace equal to r for G any subgroup of $\operatorname{GL}_2(\mathbb{F}_l)$. Other averages were considered in [1, 9, 11].

It is natural to ask if the average constant of Theorem 1.2 has an interpretation in terms of local densities as does the constant (1.3) for the average Lang–Trotter conjecture over $\mathbb{Q}$. The authors have no such interpretation, but submit the following observation. Let

$$G_l = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{F}_l, a^2 + b^2 \neq 0 \right\} \subset \operatorname{GL}_2(\mathbb{F}_l).$$

Then

$$\prod_{l > 2} \frac{l \cdot |G_l^{Tr=r}|}{|G_l|} = \prod_{l > 2} \frac{l(l - 1 - \left(\frac{-r^2}{l}\right))}{(l-1)(l - \left(\frac{-1}{l}\right))} = 3\pi c_r.$$

Throughout the proof we will assume that r is odd and positive, since the other cases are analogous. The case $r = 0$ is easier, and is treated separately in Section 5.

We follow the framework of [4], with rapidly decreasing functions and contour integration as used in [1], where the authors also average over a “thin set”. The proof of Theorem 1.2 follows immediately from the following two results. In all the following, r is an odd positive integer.

Theorem 1.3 (Analytic). *With the above notations, we have*

$$\frac{1}{|\mathcal{C}_x|}\sum_{E\in\mathcal{C}_x}\pi_E^{r,2}(x)=\frac{1}{\pi}(k_r+o(1))\log\log x$$

where

$$k_r=\sum_{f=1}^{\infty}\frac{1}{f}\sum_{n=1}^{\infty}\frac{1}{n\varphi(4nf^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,f) \tag{1.4}$$

ia a convergent double series, and

$$C_r(a,n,f)=\#\{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*\mid b\equiv 3 \bmod 4, 4b^2\equiv r^2-af^2 \bmod 4nf^2\}.$$

Theorem 1.4 (Euler product). *With the above notations, we have*

$$k_r=\frac{1}{3}\prod_{l>2}\frac{l\left(l-1-\left(\frac{-r^2}{l}\right)\right)}{(l-1)(l-\left(\frac{-1}{l}\right))}.$$

2. Step one - The analytic number theory

The proof of Theorem 1.3 follows from two results. The average over all curves in the box C_x is related to an average of Kronecker class numbers of imaginary quadratic orders using Deuring's Theorem (Lemma 2.1), and this can be rewritten as an average of special values of L-functions which can be evaluated (Lemma 2.2).

Let $D<0$ be the discriminant of a quadratic imaginary order. Then, the Kronecker class number $H(D)$ is defined as

$$H(D)=2\sum_{f^2|D}\frac{h(D/f^2)}{w(D/f^2))}, \tag{2.1}$$

where $h(d)$ and $w(d)$ denote respectively the class number and the number of units of the order of discriminant d.

Lemma 2.1. *With the notation of Theorem 1.3*

$$\frac{1}{|\mathcal{C}_x|}\sum_{E\in\mathcal{C}_x}\pi_E^{r,2}(x)\quad\sim\quad\frac{1}{2}\sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4}}\frac{H(r^2-4p^2)}{p^2}+O(1).$$

Lemma 2.2. *With the notation above, suppose that $f^2\mid r^2-4p^2$, set $d=d_f(p)=(r^2-4p^2)/f^2$ and denote by $\chi_{d_f(p)}$ the Kronecker symbol modulo $d_f(p)$ (as r is odd, $d_f(p)\equiv 1 \bmod 4$). Then for every $c>0$,*

$$\sum_{\substack{f\le 2x\\ (f,2r)=1}}\frac{1}{f}\sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}}L(1,\chi_{d_f(p)})\log p=k_rx+O\left(\frac{x}{\log^c x}\right).$$

where $L(s,\chi_{d_f(p)})$ is the Dirichlet L–function of $\chi_{d_f(p)}$.

We will prove these lemmas in Section 4. We show here how to deduce the *analytic step* from Lemma 2.1 and Lemma 2.2.

Proof of Theorem 1.3. The definition of the Kronecker class number, the class number formula

$$h(d) = \frac{\omega(d)|d|^{1/2}}{2\pi} L(1,\chi_d) \qquad \text{for } d<0$$

and Lemma 2.1 imply that

$$\frac{1}{|\mathcal{C}_x|}\sum_{E\in\mathcal{C}_x} \pi_E^{r,2}(x) \sim \frac{1}{2\pi} \sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4}} \sum_{f^2|r^2-4p^2} \frac{1}{f}\frac{\sqrt{4p^2-r^2}}{p^2} L(1,\chi_{d_f(p)}).$$

Since $\sqrt{4p^2-r^2} = 2p + O(\frac{1}{p})$ and $L(1,\chi_{d_f(p)}) \ll \log p$, the above equals

$$\frac{1}{\pi}\sum_{\substack{f\le 2x\\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}} \frac{L(1,\chi_{d_f(p)})}{p} + O\left(\sum_{p\le x}\frac{\log p}{p^3}\sum_{f^2|r^2-4p^2} 1\right).$$

The sum in the error term is bounded since $\sum_{f^2|r^2-4p^2} 1 \ll p^\epsilon$. Now using partial integration and Lemma 2.2, we deduce

$$\sum_{\substack{f\le 2x\\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}} \frac{L(1,\chi_{d_f(p)})}{p} =$$

$$\frac{1}{x\log x}\sum_{\substack{f\le 2x\\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}} L(1,\chi_{d_f(p)})\log p$$

$$-\int_{3r}^{x} \sum_{\substack{f\le 2t\\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{3r<p\le t\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}} L(1,\chi_{d_f(p)})\log p \frac{d}{dt}\left(\frac{1}{t\log t}\right) dt =$$

$$-k_r\int_{3r}^{x} t\,\frac{d}{dt}\left(\frac{1}{t\log t}\right)\,dt + O\left(\int_{2}^{x}\frac{dt}{t\log^{c+1} t}\right) =$$

$$k_r\int_{3r}^{x}\frac{dt}{t\log t} + O\left(1\right) = k_r \log\log x + O(1).$$

This concludes the proof. □

3. Step two - computing the Euler product

Proof of Theorem 1.4. Let $\omega(k)$ be the number of distinct prime divisors of $k\in\mathbb{N}$.

Lemma 3.1. *If* $\gcd(f,2r)\neq 1$, *then* $C_r(a,n,f)=0$. *If* $\gcd(f,2r)=1$, *then*

$$C_r(a,n,f) = \begin{cases} d_2(n)2^{\omega(f)-\omega((n',f))}\prod_{l|n'}\left[1+\left(\frac{r^2-af^2}{l}\right)\right] & \textit{if } \gcd(n',r^2-af^2)=1\\ 0 & \textit{otherwise.}\end{cases}$$

Proof of Lemma 3.1. From the definition

$$C_r(a,n,f) = \#\{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^* \mid b\equiv 3 \bmod 4, 4b^2\equiv r^2-af^2 \bmod 4nf^2\},$$

it is clear that $C_r(a,n,f)=0$ when $\gcd(f,2r)\neq 1$. By the Chinese Remainder Theorem, all solutions modulo $4nf^2$ arise from solution modulo the prime power divisors of $4nf^2$. Furthermore, every solution modulo a prime l lift uniquely to a solution modulo l^α (see [10, Theorem 123]). We write $4n = 2^t n'$ with n' odd. Then

$$C_r(a,n,f) = d_2 \prod_{l^\alpha || n' f^2} d_l$$

where, if $d_l = d_l(n) = \{b \in (\mathbb{Z}/l\mathbb{Z})^* \mid b^2 \equiv (r^2 - af^2)/4 \bmod l\}$,

$$d_l = \begin{cases} 1 + \left(\frac{r^2-af^2}{l}\right) & \text{if } (l, r^2 - af^2) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

and if $d_2 = d_2(n) = \#\left\{ b \in (\mathbb{Z}/2^t\mathbb{Z})^* \;\middle|\; \substack{b \equiv 3 \bmod 4, \\ 4b^2 \equiv (r^2 - af^2) \bmod 2^t} \right\}$,

$$d_2 = \begin{cases} 2^{\min\{3,t-2\}} & \text{if } r^2 - af^2 \equiv 4 \bmod 2^{\min\{t,5\}} \\ 0 & \text{otherwise.} \end{cases}$$

The formula for d_2 is showns as follows. If $2 \le t < 5$ it can be verified directly. If $a \ge 3$, then the number of solutions of the quadratic equation $x^2 \equiv c \bmod 2^a$ are 4 if $c \equiv 1 \bmod 8$ and 0 otherwise (see [10, p. 98]). Let us write $b = -1 + 4u$, so that $4b^2 = 4 + 32(2u^2 - u) \equiv r^2 - af^2 \bmod 2^t$ implies $r^2 - af^2 \equiv 4 \bmod 32$. In such a case, the 4 solutions of $b^2 \equiv \frac{r^2-af^2}{4} \bmod 2^{t-2}$ lift to 16 solutions modulo 2^t and half of these are such that $b \equiv 3 \bmod 4$. The lemma now follows by observing that if $l \mid f$, then $d_l = 2$ as $(r, f) = 1$. □

Using the lemma, we rewrite (1.4) as

$$k_r = \sum_{\substack{f \in \mathbb{N}, \\ \gcd(f,2r)=1}} \frac{2^{\omega(f)}}{f\varphi(f^2)} \sum_{n \in \mathbb{N}} \frac{\varphi(\gcd(n,f))}{\gcd(n,f) 2^{\omega((n,f))}} \frac{1}{n\varphi(4n)} c_f(n) \tag{3.1}$$

where

$$c_f(n) = \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^*, \\ \gcd(r^2 - af^2, n')=1}} d_2(n) \left(\frac{a}{n}\right) \prod_{l \mid n'} \left(1 + \left(\frac{r^2 - af^2}{l}\right)\right).$$

Lemma 3.2. (i) *$c_f(n)$ is a multiplicative function of n.*

(ii) *Let l be an odd prime. Then $c_f(l^\alpha) = c_{\gcd(f,l)}(l^\alpha)$.*

(iii) *Let l be an odd prime not dividing f. Then*

$$c_1(l^\alpha) = \begin{cases} 1 & \text{if } \alpha = 0 \\ \left(\frac{-1}{l}\right)^\alpha \varphi(l^\alpha) & \text{if } l \mid r \\ l^{\alpha-1}(l-3) & \text{if } \alpha \text{ is even and } l \nmid r \\ l^{\alpha-1}(-1 - \left(\frac{-1}{l}\right)) & \text{if } \alpha \text{ is odd and } l \nmid r \end{cases} \tag{3.2}$$

(iv) *Let l be an odd prime such that $l \mid f$ and $l \nmid r$. Then*

$$c_l(l^\alpha) = \begin{cases} 1 & \text{if } \alpha = 0 \\ 2\varphi(l^\alpha) & \text{if } \alpha > 0 \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd.} \end{cases}$$

(v) $c_1(2^\alpha) = (-2)^\alpha$.

The proof of Lemma 3.2 will be done in Section 4. Using the lemma, we have

$$k_r = \left[\sum_{\substack{f\in\mathbb{N},\\ \gcd(f,2r)=1}} \frac{2^{\omega(f)}}{f\varphi(f^2)} \prod_{l>2}\sum_{\alpha\geq 0} \frac{\varphi(\gcd(l^\alpha,f))}{\gcd(l^\alpha,f)2^{\omega(\gcd(l^\alpha,f))}} \frac{1}{l^\alpha\varphi(l^\alpha)} c_f(l^\alpha)\right] \sum_{j\in\mathbb{N}} \frac{c_1(2^j)}{2^j\varphi(2^{j+2})}.$$

Using $c_f(l^\alpha) = c_{\gcd(l,f)}(l^\alpha)$ and

$$\sum_{j\in\mathbb{N}} \frac{c_1(2^j)}{2^j\varphi(2^{j+2})} = \sum_{j\in\mathbb{N}} \frac{(-2)^j}{2^{2j+1}} = 1/3,$$

we obtain

$$\begin{aligned} k_r &= \frac{1}{3}\left[\sum_{\substack{f\in\mathbb{N},\\ \gcd(f,2r)=1}} \frac{2^{\omega(f)}}{f\varphi(f^2)} \prod_{l\mid f} \frac{1+\frac{1}{2}\sum_{\alpha\geq 1}\frac{c_l(l^\alpha)}{l^{2\alpha}}}{\sum_{\alpha\geq 0}\frac{c_1(l^\alpha)}{l^\alpha\varphi(l^\alpha)}}\right] \prod_{l>2}\left(\sum_{\alpha\geq 0}\frac{c_1(l^\alpha)}{l^\alpha\varphi(l^\alpha)}\right) \\ &= \frac{1}{3}\prod_{l>2}\left(1+\left(\frac{r^2}{l}\right)\frac{1+\frac{1}{2}\sum_{\alpha\geq 1}\frac{c_l(l^\alpha)}{l^{2\alpha}}}{\sum_{\alpha\geq 0}\frac{c_1(l^\alpha)}{l^\alpha\varphi(l^\alpha)}} \sum_{\beta\geq 1}\frac{2}{l^{3\alpha-1}(l-1)}\right)\cdot\left(\sum_{\alpha\geq 0}\frac{c_1(l^\alpha)}{l^\alpha\varphi(l^\alpha)}\right). \end{aligned}$$

As $\sum_{\beta\geq 1}\frac{1}{l^{3\beta}} = \frac{1}{l^3-1}$, we obtain

$$k_r = \frac{1}{3}\prod_{l>2}\left[\sum_{\alpha\geq 0}\frac{c_1(l^\alpha)}{l^\alpha\varphi(l^\alpha)} + \left(\frac{r^2}{l}\right)\frac{2l}{(l-1)(l^3-1)}\left(1+\frac{1}{2}\sum_{\alpha\geq 1}\frac{c_l(l^\alpha)}{l^{2\alpha}}\right)\right],$$

and it follows from Lemma 3.2 that

$$1+\frac{1}{2}\sum_{\alpha\geq 1}\frac{c_l(l^\alpha)}{l^{2\alpha}} = \frac{l^2+l+1}{l^2+l}, \qquad \sum_{\alpha\geq 0}\frac{c_1(l^\alpha)}{l^\alpha\varphi(l^\alpha)} = \begin{cases} \frac{l}{(l-(\frac{-1}{l}))} & \text{if } l \mid r \\ -\frac{l(\frac{-1}{l})+3}{(l^2-1)(l-1)}+1 & \text{if } l\nmid r. \end{cases}$$

Therefore

$$\begin{aligned} k_r &= \frac{1}{3}\prod_{l\mid r,\ l>2}\frac{l}{(l-(\frac{-1}{l}))}\prod_{l\nmid r,\ l>2}\left(1-\frac{l\left(\frac{-1}{l}\right)+3}{(l-1)(l^2-1)}+\frac{2}{(l-1)(l^2-1)}\right) \\ &= \frac{1}{3}\prod_{l>2}\frac{l(l-1-(\frac{-1}{l}))}{(l-1)(l-(\frac{-1}{l}))} \end{aligned}$$

and this concludes the proof. □

4. Proofs of the Lemmas

Proof of Lemma 3.2. (i) It is easy to check that $c_f(n)$ is multiplicative using the Chinese Remainder Theorem.

(iii) Let l be an odd prime not dividing f. We also assume $\alpha \geq 1$ otherwise the statement is clear. Let f^* be the inverse of f modulo l. Then,

$$c_f(l^\alpha) = \sum_{\substack{a\in(\mathbb{Z}/4l^\alpha\mathbb{Z})^*,\\ \gcd(r^2-af^2,l^\alpha)=1}} d_2(1)\left(\frac{a}{l}\right)^\alpha\left(1+\left(\frac{r^2-af^2}{l}\right)\right)$$

and since $d_2(1)=1$ if $a \equiv (rf^*)^2 \equiv 1 \bmod 4$ and 0 otherwise, we have

$$c_f(l^\alpha) = l^{\alpha-1}\sum_{\substack{a\in(\mathbb{Z}/l\mathbb{Z})^*\\ a\not\equiv(rf^*)^2 \bmod l}} \left(\frac{a}{l}\right)^\alpha\left(1+\left(\frac{(rf^*)^2-a}{l}\right)\right).$$

If α is even, $\sum_{c\in(\mathbb{Z}/l\mathbb{Z})^*}\left(\frac{c}{l}\right)=0$ and therefore

$$c_f(l^\alpha) = l^{\alpha-1}\left(l-1-\left(\frac{r^2}{l}\right)+\sum_{\substack{c\in(\mathbb{Z}/l\mathbb{Z})^*,\\ c\not\equiv(rf^*)^2 \bmod l}}\left(\frac{c}{l}\right)\right) = l^{\alpha-1}\left(l-1-2\left(\frac{r^2}{l}\right)\right).$$

If α is odd, we have

$$\begin{aligned} c_f(l^\alpha) &= l^{\alpha-1}\sum_{\substack{a\in(\mathbb{Z}/l\mathbb{Z})^*\\ a\not\equiv(rf^*)^2 \bmod l}}\left(\left(\frac{a}{l}\right)+\left(\frac{(rf^*)^2a-a^2}{l}\right)\right)\\ &= l^{\alpha-1}\left(-\left(\frac{r^2}{l}\right)+\sum_{a\in\mathbb{Z}/l\mathbb{Z}}\left(\frac{(rf^*)^2a-a^2}{l}\right)\right).\end{aligned}$$

Since that affine conic $X^2+Y^2-(rf^*)^2X=0$ has $l-\left(\frac{-1}{l}\right)$ points, we deduce that

$$\sum_{a\in\mathbb{Z}/l\mathbb{Z}}\left(\frac{(rf^*)^2a-a^2}{l}\right) = -\left(\frac{-r^2}{l}\right)+\left(\frac{-1}{l}\right)(l-1)(1-\left(\frac{r^2}{l}\right)),$$

and therefore

$$c_f(l^\alpha) = l^{\alpha-1}\left(-\left(\frac{-r^2}{l}\right)-\left(\frac{r^2}{l}\right)+\left(\frac{-1}{l}\right)(l-1)(1-\left(\frac{r^2}{l}\right))\right).$$

Finally

$$c_f(l^\alpha) = c_1(l^\alpha) = \begin{cases} l^{\alpha-1}\left(l-1-2\left(\frac{r^2}{l}\right)\right) & \text{if } \alpha \text{ is even}\\ l^{\alpha-1}\left(\left(\frac{-1}{l}\right)(l-1)-\left(\frac{r^2}{l}\right)(\left(\frac{-1}{l}\right)l+1)\right) & \text{if } \alpha \text{ is odd.}\end{cases}$$

(iv) We now suppose that $l \mid f$ and $l \nmid r$. Then

$$\begin{aligned} c_f(l^\alpha) = \sum_{\substack{a\in(\mathbb{Z}/4l^\alpha\mathbb{Z})^*,\\ \gcd(r^2,l)=1}} d_2(1)\left(\frac{a}{l}\right)^\alpha\left(1+\left(\frac{r^2}{l}\right)\right) &= 2l^{\alpha-1}\sum_{a\in(\mathbb{Z}/l\mathbb{Z})^*}\left(\frac{a}{l}\right)^\alpha\\ &= l^{\alpha-1}(l-1)(1+(-1)^\alpha).\end{aligned}$$

(v) If $\alpha \geq 3$, then

$$c_f(2^\alpha) = 8 \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z}), \\ a \equiv r^2 - 4 \bmod 2^5}} \left(\frac{a}{2}\right)^\alpha = 8 \left(\frac{r^2-4}{2}\right)^\alpha \frac{2^{\alpha+2}}{2^5},$$

and $\left(\frac{r^2-4}{2}\right) = \left(\frac{-3}{2}\right) = -1$ since r is odd. The remaining cases $\alpha \leq 2$ are done in a similar way and this concludes the proof. □

Proof of Lemma 2.1. Let t be a parameter to be chosen later, and let $\mathcal{C}_t$ be the set of elliptic curves E over $\mathbb{Z}[i]$ that admit a Weierstrass equation of the form

$$E : Y^2 = X^3 + \alpha X + \beta.$$

with $\alpha = a_1 + a_2 i, \beta = b_1 + b_2 i \in \mathbb{Z}[i]$ and $\max\{|a_1|, |a_2|, |b_1|, |b_2|\} \leq t$. It is easy to see that

$$|\mathcal{C}_t| = 16t^4 + O(t^3),$$

so that

$$\frac{1}{|\mathcal{C}_t|} = \frac{1}{16t^4} + O\left(\frac{1}{t^5}\right).$$

For any prime $p \equiv 3 \bmod 4$, let us denote with $\mathbb{F}_{p^2}$ the field with p^2 elements. If $\tilde{E}$ is a curve defined over $\mathbb{F}_{p^2}$, let $\mathcal{C}_t(\tilde{E})$ denotes the set

$$\mathcal{C}_t(\tilde{E}) = \left\{ E \in \mathcal{C}_t \mid E_p = \tilde{E} \right\},$$

i.e. the set of elliptic curves E in $\mathcal{C}_t$ which reduce to $\tilde{E}$ over $\mathbb{F}_{p^2}$. If $t > p$, we have

$$|\mathcal{C}_t(\tilde{E})| = \frac{16t^4}{p^4} + O\left(\frac{t^3}{p^3}\right) + O\left(\frac{t^4}{p^{20}}\right) \tag{4.1}$$

since every element of $\mathbb{F}_{p^2}$ can be written as $A + B\theta$ where $A, B \in \mathbb{F}_p$ and $\theta^2 = 1$. The last term of (4.1) accounts for non-minimal models at p.

Let $T_{p^2}(r)$ denotes the number of elliptic curves over $\mathbb{F}_{p^2}$ with $p^2 + 1 - r$ rational points. We have the following classical result

Lemma 4.1 (Deuring's Theorem [14, 19]). *Let r be an integer such that $r^2 - 4p^2 < 0$. Then,*

$$T_{p^2}(r) = \begin{cases} H(r^2 - 4p^2)\dfrac{p^2-1}{2} & \text{when } p \nmid r; \\ O\left(p^2\right) & \text{when } r = 0; \\ O\left(p^2\right) & \text{when } r = \pm p; \\ \dfrac{p^3}{24} + O\left(p^2\right) & \text{when } r = \pm 2p. \end{cases}$$

Remark. There are several standard definitions for the Kronecker class number. We are using in this paper the "weighted" Kronecker class number defined by (2.1), as in [14], but unlike [19].

We now write

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x)=\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{p\le x\\ p\equiv 3 \bmod 4\\ a_p(E)=r}}1=\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4\\ a_p(E)=r}}1\;+\;O(1)$$

where the condition $3r<p\le x$ insures that $p>3$, that $r^2-4p^2<0$ and that $r\neq p, 2p$. Reversing summations, and using Deuring's Theorem with $r\neq 0,\pm p,\pm 2p$, we then have

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) &= \sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4}}\left[\frac{1}{16t^4}+O\left(\frac{1}{t^5}\right)\right]\left[\frac{16t^4}{p^4}+O\left(\frac{t^3}{p^3}+\frac{t^4}{p^{20}}\right)\right]\;T_{p^2}(r)\\ &\quad+O(1)\\ &= \sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4}}\left[\frac{H(r^2-4p^2)}{2p^2}+O\left(\frac{\log^2 p}{t}+\frac{1}{p^2}\right)\right]\;+\;O(1)\\ &= \frac{1}{2}\sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4}}\frac{H(r^2-4p^2)}{p^2}\;+\;O\left(1\right)\end{aligned}$$

if $t=x\log x$. This completes the proof. □

Proof of Lemma 2.2. Let us introduce a parameter U and start from the identity

$$L(1,\chi_{d_f(p)}) \;=\; \sum_{n\in\mathbb{N}}\left(\frac{d_f(p)}{n}\right)\frac{1}{n}=\sum_{n\in\mathbb{N}}\left(\frac{d_f(p)}{n}\right)\frac{e^{-n/U}}{n}+O\left(\frac{|d_f(p)|^{7/32}}{U^{1/2}}\right) \tag{4.2}$$

which follows from standard contour integration. More precisely, one starts from the integral identity

$$\sum_{n\in\mathbb{N}}\left(\frac{d_f(p)}{n}\right)\frac{e^{-n/U}}{n}=L(1,\chi_{d_f(p)})+\int_{\Re(s)=-1/2}L(s+1,\chi_{d_f(p)})\Gamma(s+1)\frac{U^s}{s}ds$$

and apply the Burgess' bound $L(1/2+it,\chi_{d_f(p)})\ll|t||d_f(p)|^{7/32}$ [2] to estimate the integral.

Summing (4.2) and noticing that $|d_f(p)|^{7/32}\ll\left(\frac{p}{f}\right)^{7/16}$, it follows that

$$\sum_{\substack{f\le 2x\\ (f,2r)=1}}\frac{1}{f}\sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}}L(1,\chi_{d_f(p)})\log p \tag{4.3}$$

$$=\sum_{\substack{f\le 2x\\ (f,2r)=1}}\frac{1}{f}\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{3r<p\le x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}}\left(\frac{d_f(p)}{n}\right)\log p+O\left(\frac{x^{23/16}}{U^{1/2}}\right).$$

Choosing

$$U>x^{7/8}\log^{2c}x, \tag{4.4}$$

the error term above is

$$O\left(\frac{x^{23/16}}{U^{1/2}}\right)=O\left(\frac{x}{\log^c x}\right).$$

We now deal with the values of f with $V \leq f \leq 2x$, and note that

$$\begin{aligned}\sum_{\substack{V\leq f\leq 2x\\(f,2r)=1}} \frac{1}{f}\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{3r<p\leq x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}}\left(\frac{d_f(p)}{n}\right)\log p &\ll\\ \log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{f\geq V\\(f,2)=1}}\frac{1}{f}\sum_{\substack{m\leq x\\4m^2\equiv r^2 \bmod f^2}}1 &\ll\\ \log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{f\geq V\\(f,2r)=1}}\frac{\#\{h\in\mathbb{Z}/f^2 \mid 4h^2\equiv r^2\ (f^2)\}}{f}\frac{x}{f^2} &\ll\end{aligned}$$

$$x\log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{f\geq V}\frac{2^{\omega(f)}}{f^3} \tag{4.5}$$

using the fact that $4X^2 \equiv r^2 \bmod f^2$ has at most $2^{\omega(f)}$ solutions X modulo f^2 when f is odd (this follows from [10, Theorem 123] and the Chinese Remainder Theorem). From the standard formula [21, Exercise 2, p.53]

$$\sum_{m\leq T}2^{\omega(m)} = \frac{6}{\pi^2}T\log T + O(T)$$

and partial summation, we obtain

$$\sum_{f\geq V}\frac{2^{\omega(f)}}{f^3} \ll \frac{\log V}{V^2}.$$

As $\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n} \ll \log U$, it follows that (4.5) is $O\left(\frac{x}{\log^c x}\right)$ when

$$V > (\log x)^{(c+3)/2}. \tag{4.6}$$

Therefore (4.3) equals

$$\sum_{\substack{f\leq V\\(f,2r)=1}} \frac{1}{f}\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{3r<p\leq x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}}\left(\frac{d_f(p)}{n}\right)\log p + O\left(\frac{x}{\log^c x}\right).$$

We estimate the terms with $n \geq U\log U$ by observing that since

$$\sum_{n\geq U\log U}\frac{e^{-n/U}}{n} \ll \frac{1}{U\log U}\int_{U\log U}^{\infty}e^{-x/U}dx \ll \frac{1}{U\log U},$$

we have

$$\begin{aligned}\sum_{\substack{f\le V\\(f,2r)=1}}\frac{1}{f}\sum_{n\ge U\log U}\frac{e^{-n/U}}{n}\sum_{\substack{3r<p\le x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}}\left(\frac{d_f(p)}{n}\right)\log p &\ll\\ \frac{\log x}{U\log U}\sum_{\substack{f\le V\\(f,2r)=1}}\frac{1}{f}\sum_{\substack{m\le x\\4m^2\equiv r^2 \bmod f^2}}1 &\ll\\ \frac{x\log x}{U\log U}\ll\frac{x}{\log^c x} \end{aligned}\tag{4.7}$$

as U is chosen according to (4.4).

We finally deal with the main term of (4.3). As the Kronecker symbol is periodic modulo $4n$, we write

$$\begin{aligned}\sum_{\substack{3r<p\le x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}}\left(\frac{d_f(p)}{n}\right)\log p &= \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{3r<p\le x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2\\(r^2-4p^2)/f^2\equiv a \bmod 4n}}\log p\\ &= \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*\\b\equiv 3 \bmod 4\\4b^2\equiv r^2-af^2 \bmod 4nf^2}}\psi_1(x,4nf^2,b)\\ &\quad +O\left(\frac{2^{\omega(nf)}}{f^2}\right)\end{aligned}\tag{4.8}$$

where as usual

$$\psi_1(x,4nf^2,b)=\sum_{\substack{2\le p\le x\\p\equiv b \bmod 4nf^2}}\log p$$

and the $O(2^{\omega(nf)}/f^2)$ term comes from the primes $p\le 3r$.

If we write

$$E_1(x,4nf^2,b)=\psi_1(x,4nf^2,b)-\frac{x}{\varphi(4nf^2)},$$

then (4.8) equals

$$x\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,f)}{\varphi(4nf^2)}+\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*\\b\equiv 3 \bmod 4\\4b^2\equiv r^2-af^2 \bmod 4nf^2}}E_1(x,4nf^2,b) +O\left(\frac{2^{\omega(nf)}}{f^2}\right)\tag{4.9}$$

with

$$C_r(a,n,f)=\#\{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*\mid b\equiv 3 \bmod 4, 4b^2\equiv r^2-af^2 \bmod 4nf^2\}.$$

Let us look at the middle term of (4.8) and note that if we interchange the summation over $b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*$ and that over $a\in(\mathbb{Z}/4n\mathbb{Z})^*$, for every fixed b

there is at most 1 value of $a \in (\mathbb{Z}/4n\mathbb{Z})^*$ with $f^2 a \equiv r^2 - 4b^2 \bmod 4nf^2$. Therefore

$$\sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \sum_{\substack{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^* \\ b \equiv 3 \bmod 4 \\ 4b^2 \equiv r^2 - af^2 \bmod 4nf^2}} E_1(x, 4nf^2, b) \ll \sum_{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^*} |E_1(x, 4nf^2, b)|. \tag{4.10}$$

Substituting (4.9), (4.10) and (4.7) in (4.3), we obtain

$$\sum_{\substack{f \le 2x \\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{3r < p \le x \\ p \equiv 3 \bmod 4 \\ 4p^2 \equiv r^2 \bmod f^2}} L(1, \chi_{d_f(p)}) \log p \quad = \tag{4.11}$$

$$\sum_{\substack{f \le V \\ n \le U \log U \\ (f,2r)=1}} \frac{e^{-n/U}}{nf} \left[x \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \frac{C_r(a,n,f)}{\varphi(4nf^2)} + \sum_{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^*} |E_1(x, 4nf^2, b)| \right]$$

$$+ O\left(\frac{x}{\log^c x}\right)$$

taking into account that

$$\sum_{\substack{f \le V \\ (f,2r)=1}} \sum_{n < U \log U} \frac{e^{-n/U} 2^{\omega(nf)}}{nf^3} \ll U \log U \ll \frac{x}{\log^c x}$$

when

$$U \ll \frac{x}{\log^{c+1} x}. \tag{4.12}$$

Now apply Cauchy–Schwarz to the middle term of (4.11) and obtain

$$\sum_{\substack{f \le V \\ (f,2r)=1}} \frac{1}{f} \sum_{n \le U \log U} \frac{e^{-n/U}}{n} \sum_{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^*} |E_1(x, 4nf^2, b)| \le \tag{4.13}$$

$$\le \sum_{f \le V} \frac{1}{f} \left(\sum_{n \le U \log U} \frac{\varphi(4nf^2)}{n^2} \right)^{1/2} \left(\sum_{n \le U \log U} \sum_{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^*} E_1(x, 4nf^2, b)^2 \right)^{1/2} \ll$$

$$\ll \sqrt{\log U} \sum_{f \le V} f \left(\sum_{m \le 4V^2 U \log U} \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^*} E_1(x, m, b)^2 \right)^{1/2}.$$

Now the Barban, Davenport, Halberstam Theorem (see [3, page 169]) asserts that for $x > Q \ge x/\log^k x$

$$\sum_{m \le Q} \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^*} E_1(x, m, b)^2 \ll Qx \log x.$$

Therefore if $x > 4V^2 U \log U > x/\log^k x$, (4.13) is $\ll V^3 \sqrt{U} \log U \sqrt{x \log x}$ which is $O(x/\log^c x)$ if U and V satisfy (4.4), (4.6) and (4.12). A possible choice is

$$U = \frac{x}{\log^{5c+15} x} \quad \text{and} \quad V = \log^{(c+3)/2} x. \tag{4.14}$$

Replacing in (4.11), we have proved that

$$\sum_{\substack{f\le 2x\\(f,2r)=1}}\frac{1}{f}\sum_{\substack{3r<p\le x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}}L(1,\chi_{d_f(p)})\log p \quad = \quad x\sum_{\substack{f\le V\\n\le U\log U\\(f,2r)=1}}\frac{e^{-n/U}c_f(n)}{nf\varphi(4nf^2)}+O\left(\frac{x}{\log^c x}\right)$$

where we set

$$c_f(n)=\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,f).$$

We claim that

$$\sum_{\substack{f\le V\\n\le U\log U\\(f,2r)=1}}\frac{e^{-n/U}c_f(n)}{nf\varphi(4nf^2)}=\sum_{\substack{f,n\in\mathbb{N}\\(f,2r)=1}}\frac{c_f(n)}{nf\varphi(4nf^2)}+O\left(\frac{1}{\log^c x}\right).$$

Using Lemma 3.1,

$$c_f(n) \quad \le \quad \phi(n)\#C_r(a,n,f)\le\phi(n)2^{\omega(nf)},$$

and therefore

$$\sum_{\substack{f\le V\\n\le U\log U\\(f,2r)=1}}\frac{e^{-n/U}c_f(n)}{nf\varphi(4nf^2)}=\sum_{\substack{f\in\mathbb{N}\\(f,2r)=1}}\sum_{n\le U\log U}\frac{e^{-n/U}c_f(n)}{nf\varphi(4nf^2)}+$$

$$O\left(\sum_{\substack{f>V\\n\le U\log U\\(f,2r)=1}}\frac{e^{-n/U}\varphi(n)2^{\omega(nf)}}{nf\varphi(4nf^2)}\right).$$

Since $\varphi(4nf^2)\ge 2\varphi(f^2)\varphi(n)$ and $\displaystyle\sum_{f>V}\frac{2^{\omega(f)}}{f\varphi(f^2)}\ll\frac{\log V}{V^2}$, the error term above is

$$\ll\frac{\log V}{V^2}\sum_{n\le U\log U}\frac{e^{-n/U}2^{\omega(n)}}{n}\ll\frac{\log V\log^2 U}{V^2}=O\left(\frac{1}{\log^c x}\right)$$

as U and V are chosen according to (4.14).

Furthermore

$$\sum_{\substack{f\in\mathbb{N}\\(f,2r)=1}}\sum_{n\le U\log U}\frac{e^{-n/U}c_f(n)}{nf\varphi(4nf^2)}=\sum_{\substack{f\in\mathbb{N}\\(f,2r)=1}}\sum_{n=1}^{\infty}\frac{e^{-n/U}c_f(n)}{nf\varphi(4nf^2)}+$$

$$O\left(\sum_{f\in\mathbb{N}}\frac{2^{\omega(f)}}{f\varphi(f^2)}\sum_{n>U\log U}\frac{e^{-n/U}2^{\omega(n)}}{n}\right)$$

and since $2^{\omega(n)}\ll\sqrt{n}$, the error term above is

$$\ll\frac{1}{\sqrt{U\log U}}\int_{U\log U}^{\infty}e^{-t/U}dt=O\left(\frac{1}{\log^c x}\right).$$

The last identity we need to conclude the proof is

$$\sum_{\substack{f\in\mathbb{N}\\(f,2r)=1}} \sum_{n=1}^{\infty} \frac{e^{-n/U}c_f(n)}{nf\varphi(4nf^2)} = \sum_{\substack{f\in\mathbb{N}\\(f,2r)=1}} \sum_{n=1}^{\infty} \frac{c_f(n)}{nf\varphi(4nf^2)} + O\left(\frac{1}{\log^c x}\right)$$

Consider the Dirichlet series

$$A_f(s) = \sum_{n=1}^{\infty} \frac{c_f(n)}{\varphi(4nf^2)n^s}$$

that converges for $\Re(s) > 0$. We have the identity

$$\sum_{n=1}^{\infty} \frac{c_f(n)e^{-n/U}}{n\varphi(4nf^2)} = A_f(1) + \int_{\Re(s)=-1/2} \Gamma(s+1)A_f(s+1)\frac{U^s}{s}ds.$$

Estimating the integral we obtain

$$\int_{\Re(s)=-1/2} \Gamma(s+1)A_f(s+1)\frac{U^s}{s}ds \ll \frac{1}{f\sqrt{U}}.$$

Summing over f we have the claim. □

5. Conclusion

We now study the average of $\pi_E^{0,2}(x)$ to complete the proof of Theorem 1.2. This is also related to the special curves which should have far fewer supersingular primes than general curves over $\mathbb{Q}(i)$ presented in the introduction. Consider an elliptic curve E over $K = \mathbb{Q}(i)$ with a K-rational 4 torsion point, or full 2-torsion defined over K. Let $\mathfrak{p}$ be a prime of good reduction not dividing 2. Then by hypothesis, $4 \mid N(\mathfrak{p}) + 1 - a_{\mathfrak{p}}(E)$. If $\mathfrak{p} \mid p$ is a split prime, $p \equiv 1 \mod 4$ and $4 \mid p + 1 - a_{\mathfrak{p}}(E)$, which implies that $a_{\mathfrak{p}}(E) \equiv 2 \mod 4$, and there are no supersingular split primes. If $\mathfrak{p} \mid p$ is a supersingular inert prime, then $a_{\mathfrak{p}}(E)$ is either $0, \pm p, \pm 2p$. We also have $p \equiv 3 \mod 4$ and $4 \mid p^2 + 1 - a_{\mathfrak{p}}(E)$, which implies that $a_{\mathfrak{p}}(E) \equiv 2 \mod 4$, and the supersingular inert primes are such that $a_{\mathfrak{p}}(E) = \pm 2p$.

We then define, for any elliptic curve E over $K = \mathbb{Q}(i)$,

$$\begin{aligned}
\pi'_E(x) &= \#\left\{\mathfrak{p} \mid N(\mathfrak{p}) \le x,\ \deg_K(\mathfrak{p}) = 2, \text{ and } a_{\mathfrak{p}}(E) = p \text{ or } a_{\mathfrak{p}}(E) = -p\right\} \\
\pi''_E(x) &= \#\left\{\mathfrak{p} \mid N(\mathfrak{p}) \le x,\ \deg_K(\mathfrak{p}) = 2, \text{ and } a_{\mathfrak{p}}(E) = 2p \text{ or } a_{\mathfrak{p}}(E) = -2p\right\} \\
\pi^{\mathrm{ss}}_E(x) &= \#\left\{\mathfrak{p} \mid N(\mathfrak{p}) \le x,\ \deg_K(\mathfrak{p}) = 2, \text{ and } \mathfrak{p} \text{ is a supersingular prime}\right\}.
\end{aligned}$$

We now compute the average of those densities over all elliptic curves E over $K = \mathbb{Q}(i)$. Unlike the average of Theorem 1.2 for $r \neq 0$ which requires delicate computations, those averages are trivial as Deuring's Theorem does not involve Kronecker class numbers in those cases. The curves of the example above are part of a special family, but there are reasons to believe that averages over families would lead to similar results as indicated in the recent work of James [11].

Theorem 5.1. *Let $K = \mathbb{Q}(i)$ and let $\mathcal{C}'_x$ (respectively $\mathcal{C}''_x$) denote the set of elliptic curves $E : Y^2 = X^3 + \alpha X + \beta$ with $\alpha = a_1 + a_2 i, \beta = b_1 + b_2 i \in \mathbb{Z}[i]$ and*

$\max\{|a_1|, |a_2|, |b_1|, |b_2|\} \leq \log\log x$ *(respectively $x/\log x$). Then,*

$$\begin{aligned}
\frac{1}{|\mathcal{C}'_x|}\sum_{E\in\mathcal{C}'_x}\pi_E^{0,2}(x) &< \infty\\
\frac{1}{|\mathcal{C}'_x|}\sum_{E\in\mathcal{C}'_x}\pi'_E(x) &< \infty\\
\frac{1}{|\mathcal{C}''_x|}\sum_{E\in\mathcal{C}''_x}\pi''_E(x) &\sim \frac{1}{24}\log\log x\\
\frac{1}{|\mathcal{C}''_x|}\sum_{E\in\mathcal{C}''_x}\pi^{\text{ss}}_E(x) &\sim \frac{1}{24}\log\log x
\end{aligned}$$

Proof of Theorem 5.1. Following the proof of Lemma 2.1, and using $T_{p^2}(0) = O(p^2)$, we have

$$\begin{aligned}
\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{0,2}(x) &= \frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{p\leq x\\ p\equiv 3 \bmod 4\\ a_p(E)=0}} 1\\
&= \sum_{\substack{p\leq x\\ p\equiv 3 \bmod 4}} \left[\frac{1}{16t^4} + O\left(\frac{1}{t^5}\right)\right]\left[\frac{16t^4}{p^4} + O\left(\frac{t^3}{p^3}+\frac{t^4}{p^{20}}\right)\right] T_{p^2}(0)\\
&= \sum_{\substack{p\leq x\\ p\equiv 3 \bmod 4}} O\left(\frac{1}{p^2}+\frac{1}{pt}\right)\\
&= O(1) \qquad \text{if } t = \log\log x.
\end{aligned}$$

The proof for $\pi'_E(x)$ is exactly the same. For $\pi''_E(x)$, we have $T_{p^2}(2p)+T_{p^2}(-2p) = p^3/12 + O(p^2)$ from Lemma 4.1, and working as above

$$\begin{aligned}
\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi''_E(x) &= \frac{1}{12}\sum_{\substack{p\leq x\\ p\equiv 3 \bmod 4}}\frac{1}{p} + O\left(\frac{1}{t}\sum_{\substack{p\leq x\\ p\equiv 3 \bmod 4}} 1\right)\\
&= \frac{1}{24}\log\log x + O(1) \qquad \text{if } t = \frac{x}{\log x}.
\end{aligned}$$

The average result for $\pi^{\text{ss}}_E(x)$ now follows by summing the first three estimates. □

References

1. A. Akbary, C. David and R. Juricevic, *Average distributions and product of L-series*, Acta Arithmetica, to appear.
2. D. A. Burgess, *On character sums and L-series II*, Proc. London Math. Soc. 3 **13** (1963), 524–536.
3. H. Davenport, *Multiplicative number theory*, Springer-Verlag, New York, 2000.
4. C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices (1999), 165–183.
5. N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (1987), 561–567.
6. N. D. Elkies, *Supersingular primes for elliptic curves over real number fields*, Compositio Math. **72** (1989), 165–172.

7. N. D. Elkies, *Distribution of supersingular primes*, Astérisque no. 198-200 (1991), 127–132.
8. E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), 81–104.
9. E. Fouvry and M. R. Murty, *Supersingular primes common to two elliptic curves*, Number theory (Paris, 1992–1993), 91–102, London Math. Soc. Lecture Note Ser., 215, Cambridge Univ. Press, Cambridge, 1995.
10. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, New York, 1979, Fifth Edition.
11. K. James, *Average Frobenius distributions for elliptic curves with 3-torsion*, preprint.
12. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.
13. S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Springer-Verlag, Berlin, 1976.
14. H. W. Lenstra, *Factoring integers with elliptic curves*, Ann. of Math. **126** (1987), 649–673.
15. M. R. Murty, V. Kumar Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), 253–281.
16. V. K. Murty, *Modular forms and the Chebotarev density theorem. II*, Analytic number theory (Kyoto, 1996), Cambridge Univ. Press, Cambridge, 1997, pp. 287–308.
17. V. K. Murty, *Frobenius distribution and Galois representations*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), 193–211, Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI, 1999.
18. J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.
19. R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), 183–211.
20. Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.
21. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, 46. Cambridge University Press, Cambridge, 1995.
22. Da Qing Wan, *On the Lang-Trotter conjecture*, J. Number Theory **35** (1990), 247–268.

(David) Department of Mathematics and Statistics, Concordia University 1455 de Maisonneuve West Montréal, Québec Canada H3G 1M8

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

(Pappalardi) Dipartimento di Matematica, Università Roma Tre, Largo S. L. Murialdo, 1, I–00191, Roma ITALIA

E-mail address: pappa@mat.uniroma3.it