AVERAGE FROBENIUS DISTRIBUTIONS FOR ELLIPTIC CURVES OVER ABELIAN EXTENSIONS

BRYAN FAULKNER AND KEVIN JAMES

Abstract. Let E be an elliptic curve defined over some Abelian number field K. For a prime $\mathfrak{p} \subset \mathcal{O}_K$ of degree f, we consider E over the finite field $\mathcal{O}_K/\mathfrak{p}$ and let $a_{\mathfrak{p}}(E)$ be the trace of the Frobenius morphism. A generalization of the Lang-Trotter conjecture asserts that for $r \in \mathbb{Z}$, there exists a positive real constant $C_{E,r,f}$ such that

$$\#\{\mathfrak{p} \subset \mathcal{O}_K : N(\mathfrak{p}) \leq x;\ \deg_K(\mathfrak{p}) = f;\ a_{\mathfrak{p}}(E) = r\} \sim C_{E,r,f} \begin{cases} \frac{\sqrt{x}}{\log x}, & \text{if } f = 1 \\ \log\log x, & \text{if } f = 2 \\ 1, & \text{otherwise.} \end{cases}$$

We prove that this conjecture holds on average when one averages over all elliptic curves defined over K.

1. Introduction and statement of results

Let E be an elliptic curve defined over a Galois number field K. Set $n = [K : \mathbb{Q}]$ and denote by $\mathcal{O}_K$ the ring of integers of K. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime of degree f which lies above the rational prime $p \in \mathbb{Z}$. We denote the degree of a prime $\mathfrak{p} \subset \mathcal{O}_K$ as $\deg_K(\mathfrak{p})$. If E has good reduction modulo $\mathfrak{p}$, then we consider E over the finite field $\mathcal{O}_K/\mathfrak{p}$. Let $a_{\mathfrak{p}}(E)$ be the trace of the Frobenius morphism. The number of points on E over $\mathcal{O}_K/\mathfrak{p}$ is

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

where the norm of $\mathfrak{p}$, $N(\mathfrak{p}) = p^f$ is the number of elements of $\mathcal{O}_K/\mathfrak{p}$, and $a_{\mathfrak{p}}(E)$ satisfies the Hasse bound

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

Let $r \in \mathbb{Z}$. If $f | [K : \mathbb{Q}]$, define

$$\begin{aligned} \pi_E^{r,f}(x) &= \#\{\mathfrak{p} \ :\ N(\mathfrak{p}) \leq x,\ \deg_K(\mathfrak{p}) = f, \text{ and } a_{\mathfrak{p}}(E) = r\}, \quad \text{and} \\ \pi_{1/2}(x) &= \int_2^x \frac{\mathrm{dt}}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}. \end{aligned}$$

Recall that in the case that $K = \mathbb{Q}$ Lang and Trotter [15] conjectured

Conjecture 1.1. *If E does not have complex multiplication or if $r \neq 0$, there is a constant $C_{E,r}$ such that*

$$\pi_E^{r,1}(x) \sim C_{E,r}\pi_{1/2}(x) \sim C_{E,r}\frac{\sqrt{x}}{\log x} \qquad \text{as } x \to \infty.$$

[1]This material is based upon work supported by the National Science Foundation under Grant No. 0552799.

Date: December 18, 2008.

Although the Lang-Trotter conjecture remains open, there are many partial results. Elkies [10] proved that for any elliptic curve $E/\mathbb{Q}$, there are infinitely many primes p such that $a_p(E) = 0$. There are several results which verify that the conjecture is true in an average sense, when one averages over a family of elliptic curves defined over $\mathbb{Q}$ (see [1], [3], [7], [11], [12], [13]). For $K \neq \mathbb{Q}$, less is known. David and Pappalardi [8] proved

Theorem 1.2. *Let $K = \mathbb{Q}(i)$ and $\mathcal{C}_x$ 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 $\max\{|a_1|, |a_2|, |b_1|, |b_2|\} \leq x \log x$. Then for $r \neq 0$,*

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

where

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

If $r = 0$, then

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

In this paper we generalize David and Pappalardi's results as follows. Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for $\mathcal{O}_K$. Then for any $A \in \mathcal{O}_K$ there exist $\vec{v} \in \mathbb{Z}^n$ such that $A = \sum_{i=1}^n \vec{v}[i]\alpha_i$. Put $\|\vec{v}\| := \max_{1 \leq i \leq n}\{\vec{v}[i]\}$, and for $\vec{v} \in \mathbb{Z}^n$, define $A'(\vec{v}) := \sum_{i=1}^n \vec{v}[i]\alpha_i \in \mathcal{O}_K$. For $\vec{v_1}, \vec{v_2} \in (\mathbb{Z}^n)^2$, we write $E_{\vec{v_1},\vec{v_2}}$ for the elliptic curve

$$E_{\vec{v_1},\vec{v_2}} : y^2 = x^3 + A'(\vec{v_1})x + A'(\vec{v_2}),$$

and for $t \in \mathbb{R}$ we let

$$\mathcal{C}_t = \{E_{\vec{v_1},\vec{v_2}} : \|\vec{v_1}\|, \|\vec{v_2}\| \leq t; \Delta_{E_{\vec{v_1},\vec{v_2}}} \neq 0\}$$

In this paper we prove the following theorem for odd r. The case of even r can be handled in a similar manner.

Theorem 1.3. *Suppose that $K/\mathbb{Q}$ is an abelian extension; that r is an odd integer and $\epsilon > 0$ is fixed. There are explicit constants $D_{r,1,K}$ and $D_{r,2,K}$ (see Section 2 for details) such that as $x \to \infty$,*

$$\frac{1}{|\mathcal{C}_t|} \sum_{E \in \mathcal{C}_t} \pi_E^{r,f}(x) \sim \begin{cases} D_{r,1,K}\pi_{1/2}(x) & \text{if } f = 1 \text{ and } t \gg x \log^{2+\epsilon} x, \\ D_{r,2,K} \log\log x & \text{if } f = 2 \text{ and } t \gg \sqrt{x} \log x, \end{cases}$$

and for $f \geq 3$,

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

provided that

$$t \gg \begin{cases} x^{1/6} \log x & \text{if } f = 3, \\ \log\log x \log^2 x & \text{if } f = 4, \\ \log^2 x & \text{if } f \geq 5. \end{cases}$$

The organization of the rest of this paper is as follows. In section 2, we state Theorem 2.2 which is a more precise version of Theorem 1.3. We then show that the proof of this theorem can be reduced to proving three key lemmas, namely Lemma 2.3, Lemma 2.4 and Lemma 2.5. Lemma 2.3 which is proved in section 4 relates the desired average of the main theorem to a weighted sum of the special values of L-series. Lemma 2.4 which is proved in section 6 gives an estimate for the weighted sums of L-series. Lemma 2.5 which is proved in section 8 gives an Euler product representation for the constant computed in Lemma 2.4. Sections 3, 5 and 7 contain various technical results which are essential to the proofs of the three key lemmas and are of sufficient interest to be presented separately.

2. Proof of Main Theorem

In this section we will prove a more precise version of Theorem 1.3 (see Theorem 2.2 below). Before giving the statement of this result, we need to introduce additional notation and recall an elementary fact concerning Abelian extensions.

Let $r \in \mathbb{Z}$ be odd and let $f \in \mathbb{Z}$ be as in the previous section and let $A, B \in \mathbb{Z}$ with $(A, B) = 1$. Define $\Delta^{r,A,f} = r^2 - 4A^f$, $\Delta_q^{r,A,f} = \mathrm{ord}_q(\Delta^{r,A,f})$, $\gamma_q = \left(\frac{\Delta^{r,A,f}/q^{\Delta_q^{r,A,f}}}{q}\right)$ and $B_q = \mathrm{ord}_q(B)$. Put

$$\begin{aligned}\mathfrak{Q}^{<}_{r,A,B,f} &= \{q > 2, \text{prime} : q|B; q \nmid r; 0 < \Delta_q^{r,A,f} < B_q\} \quad \text{and}\\ \mathfrak{Q}^{\geq}_{r,A,B,f} &= \{q > 2, \text{prime} : q|B; q \nmid r; \Delta_q^{r,A,f} \geq B_q\}\end{aligned}$$

For $q \in \mathfrak{Q}^{<}_{r,A,B,f}$, we let $\Gamma_q = \begin{cases}\gamma_q & \text{if } \Delta_q^{r,A,f} \text{ is even and finite,}\\ 0 & \text{otherwise.}\end{cases}$

Then we define constants for use in the cases $f = 1$ and $f = 2$ respectively as follows.

$$\begin{aligned}k_{r,A,B} = &\prod_{\substack{q,\text{odd}\\ q|B, q\nmid r\\ q\nmid \Delta^{r,A,1}}} \frac{q(q+\gamma_q)}{q^2-1} \prod_{q\in\mathfrak{Q}^{\geq}_{r,A,B,1}} \left(\frac{q^{\lfloor\frac{B_q+1}{2}\rfloor}-1}{q^{\lfloor\frac{B_q-1}{2}\rfloor}(q-1)} + \frac{q^{B_q+2}}{q^{3\lfloor\frac{B_q+1}{2}\rfloor}(q^2-1)}\right)\\ &\cdot \prod_{q\in\mathfrak{Q}^{<}_{r,A,B,1}} \left(1 + \frac{\Gamma_q(q+\Gamma_q)}{q^{\Delta_q^{r,A,1}/2}(q^2-1)} + \frac{(q^{\lfloor\frac{\Delta_q^{r,A,1}}{2}\rfloor}-1)}{q^{\lfloor\frac{\Delta_q^{r,A,1}}{2}\rfloor}(q-1)}\right) \prod_{\substack{q,\text{odd}\\ q|B, q|r}} \frac{q\,(q+\gamma_q)}{q^2-1},\end{aligned}$$

$$
\begin{aligned}
c_{r,A,B} \quad = \quad & \prod_{\substack{q,\text{odd}\\ q|B, q\nmid r\\ q\nmid \Delta^{r,A,2}}} \left(\frac{q^{2B_q+2} - \gamma_q q^{2B_q+1} + \gamma_q^{B_q+1} q - \gamma_q^{B_q+1}}{q^{2B_q-1}(q^2-\gamma_q)(q-\gamma_q)} \right) \prod_{\substack{q,\text{odd}\\ q\in\mathfrak{Q}^{<}_{r,A,B}\\ 2\nmid\Delta_q}} \left(\frac{q^3(q^{3\lceil \frac{\Delta_q^{r,A,2}}{2}\rceil}-1)}{q^{3\lceil \frac{\Delta_q^{r,A,2}}{2}\rceil}(q^3-1)} \right) \\
& \cdot \prod_{\substack{q,\text{odd}\\ q\in\mathfrak{Q}^{<}_{r,A,B}\\ 2|\Delta_q}} \left(\frac{q^{\frac{3\Delta_q^{r,A,2}}{2}+3}-1}{q^{3\frac{\Delta_q^{r,A,2}}{2}}(q^3-1)} + \frac{q^{2(B_q-\Delta_q)}\gamma_q - \gamma_q^{B_q-\Delta_q+1} - q^{2(B_q-\Delta_q)-1} + q\gamma_q^{B_q-\Delta_q+1}}{q^{2B_q-\Delta_q/2-1}(q^2-\gamma_q)(q-\gamma_q)} \right) \\
& \cdot \prod_{\substack{q,\text{odd}\\ q\in\mathfrak{Q}^{\geq}_{r,A,B}}} \left(\frac{q^{3\lceil\frac{B_q}{2}\rceil+2} + q^{3\lceil\frac{B_q}{2}\rceil+1} + q^{B_q}}{q^{3\lceil\frac{B_q}{2}\rceil-2}(q+1)(q^3-1)} \right)
\end{aligned}
$$

We recall the following useful characterization of Abelian extensions which is a corollary to [21, Theorem 3.7].

Fact 2.1. *Given a Galois extension $K/\mathbb{Q}$, there exists $B \in \mathbb{Z}$, such that for any rational prime $p \in \mathbb{Z}$, $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ depends only on the residue class of p modulo B if and only if $K/\mathbb{Q}$ is Abelian.*

For $f = 1$ or 2 we select $a_1, \ldots, a_l$ and $B \in \mathbb{Z}$ so that a prime $p \in \mathbb{Z}$ splits into degree f primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_g \subset \mathcal{O}_K$ if and only if $p \equiv a_1, \ldots, a_{l-1}$ or a_l modulo B. Then we define the constants mentioned in Theorem 1.3 for $f = 1, 2$ as follows.

$$
D_{r,1,K} = \frac{4n}{3\pi\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \frac{q^2}{q^2-1} \sum_{i=1}^{l} k_{r,a_i,B},
$$

and

$$
\begin{aligned}
D_{r,2,K} = \frac{2n}{3\pi\phi(B)} & \prod_{\substack{q,\text{odd}\\ q|B\\ q|r}} \left(\frac{q^{2B_q+2} - \gamma_q q^{2B_q+1} + \gamma_q^{B_q+1} q - \gamma_q^{B_q+1}}{q^{2B_q-1}(q^2-\gamma_q)(q-\gamma_q)} \right) \\
& \cdot \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q-\left(\frac{-1}{q}\right)} \right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(\frac{q\left(q^2-q-1-\left(\frac{-1}{q}\right)\right)}{(q-1)(q^2-1)} \right) \sum_{i=1}^{l} c_{r,a_i,B}
\end{aligned}
$$

Now we can state a more precise version of Theorem 1.3.

Theorem 2.2. *If $K/\mathbb{Q}$ is an abelian extension of degree n, then for any fixed $c > 1$ we have*

$$
\frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,1}(x) = D_{r,1,K}\pi_{1/2}(x) + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t} \right),
$$

and

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) = D_{r,2,K}\log\log x + \mathrm{O}\left(1+\frac{\sqrt{x}\log x}{t}\right).$$

If $f \geq 3$, then

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) = \begin{cases} \mathrm{O}\left(1+\frac{\log^2 x}{t}\right) & \text{for } f\geq 5,\\ \mathrm{O}\left(1+\frac{\log^2 x\log\log x}{t}\right) & \text{for } f=4,\\ \mathrm{O}\left(1+\frac{x^{1/6}\log x}{t}\right) & \text{for } f=3.\end{cases}$$

We utilize the following three lemmas in the proof of Theorem 2.2.

Lemma 2.3. *Let $K/\mathbb{Q}$ be an Abelian extension. Select $a_1,\dots a_l$ and B so that $deg_K(\mathfrak{p}) = f$ if and only if $p\equiv a_1,\dots,a_l \pmod B$, where $\mathfrak{p}$ is a prime above the rational prime p. Then*

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) = \frac{n}{\pi}\Bigg[\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{l}\sum_{\substack{k\leq 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\leq x^{1/f}\\k^2|r^2-4p^f\\p\equiv a_i \pmod B}} L(1,\chi_{d_k(p)})\log p$$

$$-\sum_{i=1}^{l}\int_{B(r)^f}\sum_{\substack{k\leq 2\sqrt{S}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\leq S^{1/f}\\k^2|r^2-4p^f\\p\equiv a_i \pmod B}} L(1,\chi_{d_k(p)})\log p\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{dS}\Bigg] + E(x,t),$$

where $B(r)$ is as in Lemma 2.4 and

$$E(x,t) \ll \begin{cases} 1+\frac{\log^2 x}{t} & \text{for } f\geq 5\\ 1+\frac{\log^2 x\log\log x}{t} & \text{for } f=4\\ 1+\frac{x^{1/6}\log x}{t} & \text{for } f=3\\ 1+\frac{\sqrt{x}\log x}{t} & \text{for } f=2\\ \log\log x+\frac{x^{3/2}\log x}{t} & \text{for } f=1.\end{cases}$$

We prove lemma 2.3 in section 4. Our next lemma combines a previous result of James [14, Proposition 2.1] with a straight forward generalization of a result of David and Pappalardi [8, Lemma 2.2]. In order to state this lemma, we require the following additional notation. Let

$$C_{r,A,B} = \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4nBk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k),$$

where

$$C_r(a,n,k) = \#\{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^* : b\equiv A \pmod B; 4b^2\equiv r^2-ak^2 \pmod{4nk^2}\}.$$

Also, let

$$K_{r,A,B} = \sum_{k=1}^{\infty}\frac{1}{k}\sum_{n=1}^{\infty}\frac{c_k^{r,A,B}(n)}{n\phi([B;nk^2])},$$

where

$$c_k^{r,A,B}(n) = \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})\\ a\equiv 0,1 \pmod 4\\ (r^2-ak^2,4nk^2)=4\\ 4A\equiv r^2-ak^2 \pmod{(4B,4nk^2)}}} \left(\frac{a}{n}\right).$$

Then we have the following evaluation of the sums of L-series appearing in Lemma 2.3.

Lemma 2.4. *Suppose that $r, A, B \in \mathbb{Z}$, with r odd and $(A, B) = 1$. Let $d_{k,f}(p) = (r^2 - 4p^f)/k^2$, if $k^2|(r^2 - 4p)$ and 0 otherwise. Let $B(r) = \max\{5, r, r^2/4, \Delta_K\}$ and let $\chi_{d_{k,f}(p)} = \left(\frac{d_{k,f}(p)}{\bullet}\right)$. Then for every $c > 0$,*

$$\sum_{k\le 2\sqrt{x}} \frac{1}{k} \sum_{\substack{B(r)<p\le x^{1/f}\\ p\equiv A \pmod B\\ 4p^f\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p = \begin{cases} K_{r,A,B}\cdot x + \mathrm{O}\left(\frac{x}{\log^c x}\right) & \text{if } f=1,\\ C_{r,A,B}\cdot\sqrt{x} + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right) & \text{if } f=2.\end{cases}$$

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

The third lemma gives an Euler product expansion for the constant appearing in Lemma 2.4 for the $f = 2$ case. For the $f = 1$ case, we use a result of James [14].

Lemma 2.5. *With the notation used in Theorem 2.2 and Lemma 2.4*

$$C_{r,A,B} = \prod_{\substack{q,\text{odd}\\ q|B\\ q|r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1} q^{-2\mathrm{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}\left(q - \left(\frac{-1}{q}\right)\right)}\right)$$

$$\cdot \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q-\left(\frac{-1}{q}\right)}\right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right)q+1}{(q-1)(q^2-1)}\right) c_{r,A,B}.$$

Proof of Thereom 2.2. Suppose $f = 1$. We combine Lemmas 2.3 and 2.4 (2) to obtain

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t} \pi_E^{r,1}(x) = \frac{n}{\pi}\Bigg[&\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{l}\left(K_{r,a_i,B}x + \mathrm{O}\left(\frac{x}{\log^c x}\right)\right)\\ &- \sum_{i=1}^{l}\int_{B(r)^f}^{x}\left(K_{r,a_i,B}S + \mathrm{O}\left(\frac{S}{\log^c S}\right)\right)\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS}\Bigg]\\ &+ \mathrm{O}\left(\log\log x + \frac{x^{3/2}\log x}{t}\right).\end{aligned}$$

In [14] James proved

$$K_{r,A,B} = \frac{2}{3\phi(B)}\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}}\frac{q^2}{q^2-1}k_{r,A,B}.$$

Thus, $\sum_{i=1}^{l} K_{r,a_i,B} = \frac{\pi D_{r,1,K}}{2n}$. Therefore,

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,1}(x) = \frac{D_{r,1,K}}{2}\left[\frac{\sqrt{x}}{\log x} - \int_2^x S\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS}\right] + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right)$$

Integrating $\pi_{1/2}(x)$ by parts one obtains

$$\frac{\sqrt{x}}{\log x} = \pi_{1/2}(x) - \int_2^x \frac{\mathrm{dS}}{\sqrt{S}\log^2 S}.$$

Therefore,

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,1}(x) &= \frac{D_{r,1,K}}{2}\left[\frac{\sqrt{x}}{\log x} + \int_2^x \frac{1}{2\sqrt{S}\log S}\,\mathrm{dS} + \int_2^x \frac{1}{\sqrt{S}\log^2 S}\,\mathrm{dS}\right] \\ &\quad + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right) \\ &= D_{r,1,K}\pi_{1/2}(x) + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x} + \frac{x^{3/2}\log x}{t}\right).\end{aligned}$$

This completes the proof for the $f = 1$ case.
Suppose $f = 2$. Combine Lemmas 2.3 and 2.4 (1) to obtain

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) = \frac{n}{\pi}\Bigg[&\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{l}\left(C_{r,a_i,B}\sqrt{x} + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)\right) \\ &- \sum_{i=1}^{l}\int_{B(r)^f}^{x}\left(C_{r,a_i,B}\sqrt{S} + \mathrm{O}\left(\frac{\sqrt{S}}{\log^c S}\right)\right)\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS}\Bigg] \\ &+ \mathrm{O}\left(1 + \frac{\sqrt{x}\log x}{t}\right).\end{aligned}$$

It is easy to see that the first term in the brackets is $\mathrm{O}(1)$. Integrating by parts we see that

$$\int_{B(r)^f}^{x}\sqrt{S}\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS} = -\log\log x + \mathrm{O}(1).$$

Also, note that integration by parts gives

$$\int_{B(r)^f}^{x}\frac{\sqrt{S}}{\log^c S}\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\mathrm{dS} = \mathrm{O}(1).$$

Therefore,

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) = \frac{n}{\pi}\left(\sum_{i=1}^{l}C_{r,a_i,B}\right)\log\log x + \mathrm{O}\left(1 + \frac{\sqrt{x}\log x}{t}\right).$$

By Lemma 2.5

$$C_{r,A,B} = \prod_{\substack{q,\text{odd}\\ q|B\\ q|r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{B_q+1} q^{-2B_q}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{B_q+1}}{q^{2B_q}\left(q - \left(\frac{-1}{q}\right)\right)}\right)$$

$$\cdot \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)}\right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right) q - 1}{(q-1)(q^2-1)}\right) c_{r,A,B},$$

which gives

$$\sum_{i=1}^{l} C_{r,a_i,B} = \frac{\pi D_{r,2,K}}{n}.$$

Therefore,

$$\frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,2}(x) = D_{r,2,K} \log\log x + \mathrm{O}\left(1 + \frac{\sqrt{x}\log x}{t}\right).$$

This completes the proof for the $f = 2$ case.

Suppose $f \geq 3$. By (10) and (11) from Section 4.

$$\frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,f}(x) = \frac{n}{2f} \sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=n/f}} \frac{H(4p^f - r^2)}{p^f} + E(x,t) \tag{1}$$

where

$$E(x,t) \ll \begin{cases} 1 + \frac{\log^2 x}{t} & \text{for } f \geq 5 \\ 1 + \frac{\log\log x \log^2 x}{t} & \text{for } f = 4 \\ 1 + \frac{x^{1/6}\log x}{t} & \text{for } f = 3. \end{cases}$$

We use $H(4p^f - r^2) \ll p^{f/2}\log^2 p$ (see pg. 10) to see that the main term of (1) is

$$\sum_{B(r)<p\leq x^{1/f}} \frac{H(4p^f - r^2)}{p^f} \ll \sum_{B(r)<p\leq x^{1/f}} \frac{\log^2(p)}{p^{f/2}} \ll 1.$$

Therefore,

$$\frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,f}(x) = \begin{cases} \mathrm{O}\left(1 + \frac{\log^2 x}{t}\right) & \text{for } f \geq 5 \\ \mathrm{O}\left(1 + \frac{\log\log x \log^2 x}{t}\right) & \text{for } f = 4 \\ \mathrm{O}\left(1 + \frac{x^{1/6}\log x}{t}\right) & \text{for } f = 3. \end{cases}$$

□

3. Counting Curves

First, we note that since

$$\#\{(\vec{v},\vec{w})\in(\mathbb{Z}^n)^2 : \|\vec{v}[i]\|,\|\vec{w}[i]\|\le t\ ;\ 1\le i\le n\} = (2t+\mathrm{O}(1))^{2n}$$

we have

$$|\mathcal{C}_t| = 4^n t^{2n} + \mathrm{O}(t^{2n-1}). \tag{2}$$

Next, let $\mathfrak{p}\subset\mathcal{O}_K$ be a prime which lies above an unramified ratoinal prime $p\nmid 6$. The model $E_{\vec{v_1},\vec{v_2}}$ from (1) is said to be *minimal at* $\mathfrak{p}$ if $\mathrm{ord}_{\mathfrak{p}}(\Delta(E_{\vec{v_1},\vec{v_2}}))$ is minimal among all models for E. We recall (see [19, pg. 172]) that for $\mathfrak{p}\nmid 6$, $E_{\vec{v_1},\vec{v_2}}$ is minimal if and only if $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_1}))<4$ or $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_2}))<6$. Let

$$E_{A,B} : y^2 = x^3 + Ax + B$$

be an elliptic curve defined over $\mathcal{O}_K/\mathfrak{p}$, and let $\mathcal{C}_t(E_{A,B})$ denote the set of elliptic curves $E\in\mathcal{C}_t$ which reduce to $E_{A,B}$ over $\mathcal{O}_K/\mathfrak{p}$. We recall that in order to reduce $E_{\vec{v_1},\vec{v_2}}$ modulo $\mathfrak{p}$ one should first obtain a model

$$E : y^2 = x^3 + u^4A'(\vec{v_1}) + u^6A'(\vec{v_2}) \quad (u\in(\mathcal{O}_K/\mathfrak{p})^*)$$

which is minimal at $\mathfrak{p}$, then reduce the coefficients of the minimal model (see [19, Chapter 7]). Denote by $E^{\mathfrak{p}}_{\vec{v_1},\vec{v_2}}$ the reduction of $E_{\vec{v_1},\vec{v_2}}$ modulo $\mathfrak{p}$.

We wish to estimate the size of $\mathcal{C}_t(E_{A,B})$. First, we note that

$$p^N\mathcal{O}_K \subseteq \mathfrak{p}^N \subseteq \mathcal{O}_K.$$

Thus by the third isomorphism theorem (for $\mathbb{Z}$-modules),

$$\frac{(\mathcal{O}_K)/(p^N\mathcal{O}_K)}{(\mathfrak{p}^N)/(p^N\mathcal{O}_K)} \cong \frac{\mathcal{O}_K}{\mathfrak{p}^N}$$

Therefore,

$$\left|\mathfrak{p}^N/p^N\mathcal{O}_K\right| = p^{N(n-f)}.$$

Set $s=p^{N(n-f)}$. Suppose $\{\rho_1,\dots\rho_s\}$ is a complete set of distinct coset representatives for $\mathfrak{p}^N/p^N\mathcal{O}_K$. Then for $A\in\mathcal{O}_K$, and $\vec{v}\in\mathbb{Z}^n$ we have

$$A'(\vec{v})\equiv A \pmod{\mathfrak{p}^N} \quad\Leftrightarrow\quad A'(\vec{v})-A\equiv\rho_i \pmod{p^N\mathcal{O}_K} \quad (\text{some } 1\le i\le s)$$

For $1\le i\le s$ set $A+\rho_i=\sum_{j=1}^n c_{i,j}\alpha_j$ where $c_{i,j}\in\mathbb{Z}$. Then

$$\begin{aligned}
&\#\{\vec{v}\in\mathbb{Z}^n | A'(\vec{v})\equiv A \pmod{\mathfrak{p}^N}; \|\vec{v}\|\le t\}\\
&= \sum_{i=1}^{s}\#\left\{(c_{i,1}+p^Nk_1, c_{i,2}+p^Nk_2,\dots,c_{i,n}+p^Nk_n)\ :\ \begin{matrix}|c_{i,j}+p^Nk_j|\le t;\\ 1\le j\le n\end{matrix}\right\}\\
&= \sum_{i=1}^{p^{N(n-f)}}\left(\frac{2t}{p^N}+\mathrm{O}(1)\right)^n = \frac{(2t)^n}{p^{Nf}} + \mathrm{O}\left(\frac{t^{n-1}}{p^{N(f-1)}}\right).
\end{aligned} \tag{3}$$

Therefore, for $A,B\in\mathcal{O}_K/\mathfrak{p}$,

$$\#\left\{(\vec{v_1},\vec{v_2})\in(\mathbb{Z}^n)^2\ :\ \begin{matrix}A'(\vec{v_1})\equiv A \pmod{\mathfrak{p}};\\ A'(\vec{v_1})\equiv A \pmod{\mathfrak{p}};\\ \|\vec{v_1}\|,\|\vec{v_2}\|\le t\end{matrix}\right\} = \left(\frac{2^nt^n}{p^f}\right)^2 + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}\right).$$

Thus the number of models in $\mathcal{C}_t(E_{A,B})$ which are not minimal at $\mathfrak{p}$ is

$$\#\{E_{\vec{v_1},\vec{v_2}} \in \mathcal{C}_t : A'(\vec{v_1}) \in \mathfrak{p}^4 \text{ and } A'(\vec{v_2}) \in \mathfrak{p}^6\} = \left(\frac{(2t)^n}{p^4 f} + \mathrm{O}\left(\frac{t^{n-1}}{p^{4(f-1)}}\right)\right)\left(\frac{(2t)^n}{p^6 f} + \mathrm{O}\left(\frac{t^{n-1}}{p^{6(f-1)}}\right)\right).$$

Thus

$$\begin{aligned} |\,\mathcal{C}_t(E_{A,B})| &= \#\left\{(\vec{v_1},\vec{v_2}) \in (\mathbb{Z}^n)^2 \mid E^{\mathfrak{p}}_{\vec{v_1},\vec{v_2}} = E_{A,B}\right\} \\ &= \#\left\{(\vec{v_1},\vec{v_2}) \in (\mathbb{Z}^n)^2 \ : \ \begin{array}{c} A'(\vec{v_1}) \equiv A \pmod{\mathfrak{p}}; A'(\vec{v_2}) \equiv B \pmod{\mathfrak{p}}; \\ \|\vec{v_1}\|, \|\vec{v_2}\| \le t \end{array}\right\} \\ &\quad + \mathrm{O}(\#\{E_{\vec{v_1},\vec{v_2}} \in \mathcal{C}_t : A'(\vec{v_1}) \in \mathfrak{p}^4 \text{ and } A'(\vec{v_2}) \in \mathfrak{p}^6\}) \\ &= \left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right) \end{aligned} \tag{4}$$

4. The Average in Terms of L-Series

First we recall the Hurwitz class number (see [16]) which is a weighted sum over the equivalence classes of binary quadratic forms $f = ax^2 + bxy + cy^2$ of a given discriminant. More precisely, if we let $\Delta_f = b^2 - 4ac$ denote the discriminant of the form f above, then for $\Delta > 0$,

$$H(\Delta) = \sum_{\substack{[f] \\ \Delta_f = -\Delta}} c_f \quad \text{where} \quad c_f = \begin{cases} \frac{1}{2} & \text{if } f \text{ is proportional to } x^2 + y^2, \\ \frac{1}{3} & \text{if } f \text{ is proportional to } x^2 + xy + y^2, \\ 1 & \text{otherwise.} \end{cases}$$

Some authors use instead the Kronecker class number $K(\Delta)$ which is the number of equivalence classes of binary quadratic forms of discriminant Δ each counted with weight 1. For our purposes, it will be more convenient to work with $H(\Delta)$. It is straight forward to check that $H(\Delta) = K(-\Delta) + \mathrm{O}(1)$. We recall the following useful formula for $H(\Delta)$ (see [8])

$$H(\Delta) = 2 \sum_{\substack{k^2 | \Delta \\ \frac{-\Delta}{k^2} \equiv 0,1 \pmod 4}} \frac{h(-\Delta/k^2)}{w(-\Delta/k^2)}, \tag{5}$$

where $h(d)$ and $w(d)$ denote respectively the Dirichlet class number and the number of units of the imaginary quadratic order of discriminant d. Recalling Dirichlet's class number formula

$$h(d) = \frac{w(d)|d|^{1/2}}{2\pi} L(1, \chi_d) \qquad \text{for } d < 0 \tag{6}$$

and the estimate $L(1, \chi_{\Delta_k}) \ll \log p$ (see [16, pg. 656]) and noting that r odd implies that $\frac{r^2 - 4p^f}{k^2} \equiv 1 \pmod 4$, we obtain the following useful estimate.

$$H(4p^f - r^2) = \sum_{k^2 | 4p^f - r^2} \frac{\sqrt{4p^f - r^2}}{\pi k} L(1, \chi_{(r^2 - 4p^f)/k^2}) \ll p^{f/2} \log^2 p. \tag{7}$$

For $p > 3$ and $f \ge 1$ any elliptic curve over $\mathbb{F}_{p^f}$ may be written as

$$E_{a,b} : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_{p^f}).$$

We recall that $E_{a',b'} \cong E_{a,b}$ if and only if there exists $u \in (\mathbb{F}_{p^f})^*$ such that $a' = u^4 a$ and $b' = u^6 b$. So, given $(a,b) \in \mathbb{F}_{p^f}^2$, the number of $(a',b') \in \mathbb{F}_{p^f}^2$ with $E_{a',b'} \cong E_{a,b}$ is

$$\begin{cases} \frac{p^f-1}{6} & \text{when } a = 0 \text{ and } p^f \equiv 1 \pmod 3 \\ \frac{p^f-1}{4} & \text{when } b = 0 \text{ and } p^f \equiv 1 \pmod 4 \\ \frac{p^f-1}{2} & \text{otherwise.} \end{cases}$$

Following Schoof [18] we define $N(r)$ to be the number of $\mathbb{F}_{p^f}$-isomorphism classes of elliptic curves with $p^f + 1 - r$ points defined over $\mathbb{F}_{p^f}$. Then by Deuring's Theorem (see [9] or [18, Theorem 4.6]) if $r^2 - 4p^f < 0$ and $p \nmid r$, then

$$N(r) = K(r^2 - 4p^f) = H(4p^f - r^2) + \mathrm{O}(1).$$

Let $T_{p^f}(r)$ be the number of models over $\mathbb{F}_{p^f}$ of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

with $p^f + 1 - r$ rational points. Then Deuring's theorem becomes

Theorem 4.1 (Deuring)**.** $T_{p^f}(r) = H(4p^f - r^2)\frac{p^f}{2} + \mathrm{O}(p^f)$.

Proof. Let $\tilde{E}$ denote an $\mathbb{F}_{p^f}$-isomorphism class of elliptic curves. Since there are at most 10 isomorphism classes with size different from $\frac{p^f-1}{2}$ we have

$$T_{p^f}(r) = \sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r}} \sum_{\substack{A,B \\ E_{A,B}\in\tilde{E}}} 1 = \sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r}} \left(\frac{p^f-1}{2}\right) + \mathrm{O}(p^f) = \frac{p^f-1}{2} H(4p^f - r^2) + \mathrm{O}(p^f).$$

□

Proof of Lemma 2.3. Noting that $N(\mathfrak{p}) = p^f$ and that there are $g = n/f$ primes in $\mathcal{O}_K$ which lie above each rational prime p, we have

$$\frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \pi_E^{r,f}(x) = \frac{1}{|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \sum_{\substack{N(\mathfrak{p})\le x \\ \deg_K \mathfrak{p}=f \\ a_{\mathfrak{p}}(E)=r}} 1 = \frac{n}{f|\mathcal{C}_t|} \sum_{E\in\mathcal{C}_t} \sum_{\substack{B(r)<p\le x^{1/f} \\ g(p)=n/f \\ a_{\mathfrak{p}}(E)=r}} 1 + \mathrm{O}(1)$$

where $g(p)$ is the number of primes of $\mathcal{O}_K$ lying above p and the O-term comes from the finite number of primes removed from the inner sum. We require $B(r) \ge \max\{(r^2/4)^{1/f}, r, 3, \Delta_K\}$, since for such $B(r)$, $p > B(r)$ implies that $|r| \le 2\sqrt{N(\mathfrak{p})}$, $p \nmid r$ (for Deuring's theorem), p does not ramify in $\mathcal{O}_K$ and all elliptic curves defined over K have Weierstrass equations of the form $y^2 = x^3 + ax + b$.

Now, reversing the order summation in the above estimate one obtains

$$\frac{n}{f|\mathcal{C}_t|} \sum_{\substack{B(r)<p\le x^{1/f} \\ g(p)=n/f}} \sum_{\substack{E\in\mathcal{C}_t \\ a_{\mathfrak{p}}(E)=r}} 1 + \mathrm{O}(1) \tag{8}$$

Given a rational prime p let $\mathfrak{p} \subset \mathcal{O}_K$ be any prime lying above p. The inner most sum of (8) becomes

$$\sum_{\substack{E_{A,B}/\mathbb{F}_{p^f} \\ \#E_{A,B}(\mathbb{F}_{p^f})=p^f+1-r}} |\mathcal{C}_t(E_{A,B})| + \mathrm{O}\left(\sum_{\substack{E\in\mathcal{C}_t \\ E^{\mathfrak{p}} \text{ is} \\ \text{singular}}} 1\right)$$

Note that

$$\sum_{\substack{E\in\mathcal{C}_t \\ E^{\mathfrak{p}} \text{ is} \\ \text{singular}}} 1 = \sum_{A\in\mathcal{O}_K/\mathfrak{p}} \sum_{\substack{B\in\mathcal{O}_K/\mathfrak{p} \\ 4A^3-27B^2\in\mathfrak{p}}} |\mathcal{C}_t(E_{A,B})| \ll \sum_{A\in\mathcal{O}_K/\mathfrak{p}} \frac{(2t)^{2n}}{p^{2f}} \ll \frac{t^{2n}}{p^f}.$$

Recalling (4), we have

$$\sum_{\substack{E\in\mathcal{C}_t \\ a_{\mathfrak{p}}(E)=r}} 1 = T_{p^f}(r)\left[\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right] + \mathrm{O}\left(\frac{t^{2n}}{p^f}\right)$$

Applying Theorem 4.1,

$$\sum_{\substack{E\in\mathcal{C}_t \\ a_{\mathfrak{p}}(E)=r}} 1 = \left(H(4p^f-r^2)\frac{p^f}{2} + \mathrm{O}(p^f)\right)\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right) + \mathrm{O}\left(\frac{t^{2n}}{p^f}\right)$$

Recalling (2), we have that

$$\begin{aligned}
(9)\qquad & \frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t} \pi_E^{r,f}(x) \\
&= \frac{n}{f}\sum_{\substack{B(r)<p\le x^{1/f} \\ g(p)=n/f}} \left[\left(\frac{1}{4^n t^{2n}} + \mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right)\left(\frac{(2t)^{2n}}{p^{2f}} + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right)\cdot\right. \\
&\qquad \left.\left(\frac{p^f}{2}H(4p^f-r^2) + \mathrm{O}(p^f)\right)\right] + \mathrm{O}\left(1 + \sum_{\substack{B(r)<p\le x^{1/f} \\ g(p)=n/f}} \frac{1}{p^f}\right)
\end{aligned}$$

Recalling (7), the summand of the main term of (9) becomes

$$\begin{aligned}
&\frac{H(4p^f-r^2)}{2p^f} + \mathrm{O}\left(\frac{1}{p^f} + \frac{p^f H(4p^f-r^2)}{t^{2n}}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right) + \frac{t^{2n}H(4p^f-r^2)}{p^f t^{2n+1}}\right) \\
&= \frac{H(4p^f-r^2)}{2p^f} + \mathrm{O}\left(\frac{1}{p^f} + \frac{\log^2 p}{p^{17f/2}} + \log^2 p\left(\frac{1}{tp^{f/2-1}} + \frac{1}{p^{f/2}t}\right)\right)
\end{aligned}$$

Combining this with (9), we may write

$$(10)\qquad \frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t} \pi_E^{r,f}(x) = \frac{n}{2f}\sum_{\substack{B(r)<p\le x^{1/f} \\ g(p)=n/f}} \frac{H(4p^f-r^2)}{p^f} + E(x,t),$$

where (using partial summation for $f=3$ and standard estimates)

$$E(x,t) \ll \sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}} \left(\frac{1}{p^f}+\frac{\log^2 p}{tp^{f/2-1}}\right) \ll \begin{cases} 1+\frac{\log^2 x}{t} & \text{for } f\ge 5\\ 1+\frac{\log^2 x\log\log x}{t} & \text{for } f=4\\ 1+\frac{x^{1/6}\log x}{t} & \text{for } f=3\\ 1+\frac{\sqrt{x}\log x}{t} & \text{for } f=2\\ \log\log x+\frac{x^{3/2}\log x}{t} & \text{for } f=1. \end{cases} \tag{11}$$

Letting $d_k(p)=\frac{r^2-4p^f}{k^2}$ and using (5) along with Dirichlet's class number formula (6), we may rewrite the main term of (10) as

$$\frac{n}{2f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}} \frac{H(4p^f-r^2)}{p^f} = \frac{n}{2\pi f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\sum_{k^2|r^2-4p^f} \frac{\sqrt{4p^f-r^2}}{kp^f}L(1,\chi_{d_k(p)}).$$

We approximate $\sqrt{4p^f-r^2}$ by $2\sqrt{p^f}+\mathrm{O}\left(\frac{1}{p^{f/2}}\right)$ and use $L(1,\chi_{d_k(p)})\ll \log p$ (see [16, pg. 656]). Then reversing the order of summation in the main term and noting that we only need consider $k\le 2\sqrt{x}$,we obtain

$$\frac{n}{\pi f}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}} \frac{L(1,\chi_{d_k(p)})}{p^{f/2}} + \mathrm{O}\left(\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\sum_{k^2|r^2-4p^f}\frac{\log p}{kp^{3f/2}}\right) \tag{12}$$

The error term is easily seen to be $\ll 1$ and thus can be absorbed into our estimate for $E(x,t)$. Using partial summation to estimate the inner sum, the main term in (12) becomes

$$\frac{n}{\pi\sqrt{x}\log x}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}} L(1,\chi_{d_k(p)})\log p$$
$$-\frac{n}{\pi f}\int_{B(r)}^{x^{1/f}}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{\substack{B(r)<p\le s\\ k^2|r^2-4p^f\\ g(p)=n/f}} L(1,\chi_{d_k(p)})\log p\frac{\mathrm{d}}{\mathrm{d}s}\left(\frac{1}{s^{f/2}\log s}\right)\,\mathrm{d}s.$$

Setting $s = S^{1/f}$, noting that $k^2|4p^f - r^2$ implies $k < 2\sqrt{S}$ and substituting into (10), we obtain

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) = \frac{n}{\pi}\Bigg[\frac{1}{\sqrt{x}\log x}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}} L(1,\chi_{d_k(p)})\log p$$

$$-\int_{B(r)^f}^{x}\sum_{k\le 2\sqrt{S}}\frac{1}{k}\sum_{\substack{B(r)<p\le S^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}} L(1,\chi_{d_k(p)})\log p\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{ds}\Bigg] + E(x,t)$$

□

5. Computing $C_r(a,n,k)$

In this section we give a formula for evaluating

$$C_r(a,n,k) = \#\{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^* : b\equiv A \pmod{B}; 4b^2\equiv r^2-ak^2 \pmod{4nk^2}\}.$$

First, we require the following lemma which is a straight forward application of Hensel's lemma.

Lemma 5.1. *Suppose A is odd, $2\le L\in\mathbb{Z}$, and $1\le k\in\mathbb{Z}$. Then for any $X\in\mathbb{Z}$,*

$$X\equiv MA + M^2 2^k \pmod{2^L}$$

has a unique solution M modulo 2^L.

By the Chinese Remainder Theorem

$$C_r(a,n,k) = \prod_{\substack{p|(4Bnk^2)\\ p \text{ prime}}} d_{p,a,k}(n)$$

where

$$d_{p,a,k}(n) = \sum_{\substack{b\in(\mathbb{Z}/p^l\mathbb{Z})^*\\ b\equiv A \pmod{p^{l_1}}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{l_2}}}} 1$$

with $l_1 = \mathrm{ord}_{p,a,k}(B)$, $l_2 = \mathrm{ord}_{p,a,k}(4nk^2)$ and $l = l_1 + l_2$.

Lemma 5.2. *Let p be an odd prime. Using the notation above we have*

(1) *Suppose $0\le l_2\le l_1$ and $l_1>0$. Then*

$$d_{p,a,k}(n) = \begin{cases} p^{l-l_1} & \text{if } 4A^2\equiv r^2-ak^2 \pmod{p^{l_2}}\\ 0 & \text{otherwise}\end{cases}$$

(2) *Suppose $l_1 = 0$. Then*

$$d_{p,a,k}(n) = \begin{cases} 1+\left(\frac{r^2-ak^2}{p}\right) & \text{if } (r^2-ak^2,p)=1\\ 0 & \text{otherwise}\end{cases}$$

(3) *Suppose* $1 \le l_1 < l_2$. *Then*

$$d_{p,a,k}(n) = \begin{cases} p^{l-l_2} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{p^{l_1}} \\ 0 & \text{otherwise} \end{cases}$$

(4) *Suppose* $l_1 = 0$ *or* $l_1 = 1$. *Then*

$$d_{2,a,k}(n) = \begin{cases} 2^{\min(l_1+4,l-1)} & \text{if } r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,l_2)}} \\ 0 & \text{if } r^2 - ak^2 \not\equiv 4 \pmod{2^{\min(5,l_2)}} \end{cases}$$

(5) *If* $l_1 \ge 2$ *and* $2 \le l_2 \le l_1 + 3$, *then*

$$d_{2,a,k}(n) = \begin{cases} 2^{l-l_1} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{2^{l-l_1}} \\ 0 & \text{if } 4A^2 \not\equiv r^2 - ak^2 \pmod{2^{l-l_1}} \end{cases}$$

(6) *If* $l_1 \ge 2$ *and* $l_2 \ge l_1 + 4$, *then*

$$d_{2,a,k}(n) = \begin{cases} 2^{l_1+3} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}} \\ 0 & \text{if } 4A^2 \not\equiv r^2 - ak^2 \pmod{2^{l_1+3}} \end{cases}$$

Proof. The proof is an exercise in carefully counting simultaneous solutions in $(\mathbb{Z}/p^l\mathbb{Z})^*$ to the equations $b \equiv A \pmod{p^{l_1}}$ and $4b^2 \equiv r^2 - ak^2 \pmod{p^{l_2}}$. For the sake of brevity, we prove only a few cases. The proofs of the other cases are similar.

(1) It is easy to see that if $l_2 = 0$ and $l_1 > 0$, then $d_{p,a,k}(n) = 1$. So suppose $0 < l_2 \le l_1$ and p is any odd prime. Then

$$\begin{aligned} & b \equiv A \pmod{p^{l_1}} \text{ and } 4b^2 \equiv r^2 - ak^2 \pmod{p^{l_2}} \\ & \Leftrightarrow \exists M \text{ such that } 4(A + Mp^{l_1})^2 \equiv r^2 - ak^2 \pmod{p^{l_2}} \\ & \Leftrightarrow 4A^2 \equiv r^2 - ak^2 \pmod{p^{l_2}}. \end{aligned}$$

Since $\#\{b \in (\mathbb{Z}/p^l\mathbb{Z})^* : b \equiv A \pmod{p^{l_1}}\} = p^{l-l_1}$, the result follows.

(5) Suppose $l_1 \ge 2$ and $2 \le l_2 \le l_1 + 3$. Observe

$$\begin{aligned} & \exists\, b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases} \\ & \Leftrightarrow \exists\, M \quad \text{such that} \quad 4(A + M2^{l_1})^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \\ & \Leftrightarrow 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}. \end{aligned}$$

The result follows from the fact that there are 2^{l-l_1} $b \in (\mathbb{Z}/2^l\mathbb{Z})^*$ such that $b \equiv A \pmod{2^{l_1}}$.
(6) We omit the cases $l_2 = l_1+4, l_1+5$. Suppose $l_1 \geq 2$ and $l_2 \geq l_1+6$. Then

$$\begin{aligned}
&\exists\, b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases} \\
&\Leftrightarrow \exists\, M \quad \text{such that} \quad (A+M2^{l_1})^2 \equiv \frac{r^2-ak^2}{4} \pmod{2^{l_2-2}} \ \text{ and } \ \frac{r^2-ak^2}{4} \in \mathbb{Z} \\
&\Leftrightarrow \left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv MA + M^2 2^{l_1-1} \pmod{2^{l_2-l_1-3}} \ \text{ and } \ 2^{l_1+1} \mid \left(\frac{r^2-ak^2}{4} - A^2\right).
\end{aligned} \tag{13}$$

In order for the left hand side of (13) to be an integer, we must have

$$r^2 - ak^2 \equiv 4A^2 \pmod{2^{l_1+3}}. \tag{14}$$

By Lemma 5.1, (14) is a sufficient condition for determining a unique solution M modulo $2^{l_2-l_1-3}$ for (13). Then we obtain a solution b modulo 2^{l_2-2}. Note that if b satisfies $4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}$, then so do $-b$, $b+2^{l_2-3}$, and $-b+2^{l_2-3}$. But, only two of these satisfy $b \equiv A \pmod{2^{l_1}}$. Thus, the number of solutions is $2^{l-l_2+2} \cdot 2$ □

6. Averaging Special Values of L-Series

In this section we prove the $f = 2$ case of Lemma 2.4. For the $f = 1$ case, see [14, Proposition 2.1]. In [8] David and Pappalardi present a proof of the $f = 2$ case of Lemma 2.4 for $A = 3$ and $B = 4$. In the proof that follows we use arguments similar to those of David and Pappalardi (see [8, proof of Lemma 2.2]).

Proof of Lemma 2.4 (for $f = 2$). Let U be a parameter to be determined later. We have the following identity (see [8, (4.2)])

$$L(1, \chi_{d_k(p)}) := \sum_{n\in\mathbb{N}} \left(\frac{d_k(p)}{n}\right)\frac{1}{n} = \sum_{n\in\mathbb{N}} \left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n} + \mathrm{O}\left(\frac{|d_k(p)|^{7/32}}{U^{1/2}}\right). \tag{15}$$

Thus, choosing $U > x^{7/16}\log^{2c} x$ we obtain

$$\begin{aligned}
&\sum_{\substack{k\leq 2\sqrt{x} \\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\leq\sqrt{x} \\ p\equiv A \pmod{B} \\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p \\
&= \sum_{\substack{k\leq 2\sqrt{x} \\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\leq\sqrt{x} \\ p\equiv A \pmod{B} \\ 4p^2\equiv r^2 \pmod{k^2}}} \left[\sum_{n\in\mathbb{N}} \left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n} + \mathrm{O}\left(\frac{p^{7/16}}{k^{7/16}U^{1/2}}\right)\right]\log p \\
&= \sum_{\substack{k\leq 2\sqrt{x} \\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\leq\sqrt{x} \\ p\equiv A \pmod{B} \\ 4p^2\equiv r^2 \pmod{k^2}}} \sum_{n\in\mathbb{N}} \left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n}\log p + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)
\end{aligned}$$

Let V be a parameter to be determined later. Note that

$$\sum_{\substack{V\le k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\pmod B\\4p^2\equiv r^2\pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p$$

$$\ll \log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{V\le k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{m\le\sqrt{x}\\4m^2\equiv r^2\pmod{k^2}}}1$$

$$\ll \log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{V\le k\le 2\sqrt{x}\\(k,2r)=1}}\frac{\#\{h\in\mathbb{Z}/k^2\mathbb{Z}:4h^2\equiv r^2\pmod{k^2}\}}{k}\frac{\sqrt{x}}{k^2}$$

In order to find $\#\{h\in\mathbb{Z}/k^2\mathbb{Z}:4h^2\equiv r^2 \pmod{k^2}\}$, suppose $k=p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}$ where the p_i's are distinct odd primes. Notice that $r^2\equiv(2x_i)^2 \pmod{p_i^{2a_i}}$ has two nonzero solutions whenever $(k,r)=1$. Now using the Chinese Remainder Theorem, we see that $4X^2\equiv r^2 \pmod{k^2}$ has at most $2^{\nu(k)}$ solutions X modulo k^2 when k is odd, where $\nu(k)$ is the number of distinct prime divisors of k. Therefore,

$$\sum_{\substack{V\le k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\pmod B\\4p^2\equiv r^2\pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p\ll\sqrt{x}\log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{V\le k\le 2\sqrt{x}}\frac{2^{\nu(k)}}{k^3}\tag{16}$$

To estimate $\sum_{V\le k\le 2\sqrt{x}}\frac{2^{\nu(k)}}{k^3}$ we use the following estimate [20, Exercise 2, pg 53]

$$\sum_{m\le T}2^{\nu(m)}=\frac{6}{\pi^2}T\log T+\mathrm{O}(T)$$

along with partial summation to obtain

$$\begin{aligned}\sum_{k=V}^{2x}\frac{2^{\nu(k)}}{k^3}&=\left(\frac{6}{\pi^2}2x\log(2x)+\mathrm{O}(2x)\right)\frac{1}{(2x)^3}+\int_V^{2x}\left(\frac{6}{\pi^2}y\log y+\mathrm{O}(y)\right)\frac{3}{y^2}\,\mathrm{dy}\\&\quad-\left(\frac{6}{\pi^2}(V-1)\log(V-1)+\mathrm{O}(V-1)\right)\frac{1}{V^3}\ll\frac{\log V}{V^2}.\end{aligned}\tag{17}$$

To estimate the sum $\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}$ we first note that

$$1-e^{-1/U}=1-\sum_{i=0}^{\infty}\frac{(-1)^i}{U^i i!}>\frac{1}{U}-\frac{1}{2U^2}.$$

Thus for $U>1$,

$$\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}=-\log(1-e^{-1/U})<\log U+\log\left(\frac{2U}{2U-1}\right)\le\log U+\log(2).\tag{18}$$

Choosing $V>(\log x)^{(c+3)/2}$ and using (17) and (18), (16) becomes

$$\sqrt{x}\log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{V\le k\le 2\sqrt{x}}\frac{2^{\nu(k)}}{k^3}\ll\frac{\sqrt{x}}{(\log x)^{c+2-\epsilon}}(\log U)\ll\frac{\sqrt{x}}{\log^c x}$$

if $U \ll \sqrt{x}/\log x$. Thus,

$$\begin{aligned}
&\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p \\
&\quad = \sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k}\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)
\end{aligned} \tag{19}$$

Now note that

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

and recall that we required $U > x^{7/16}\log^{2c} x$. Therefore,

$$\begin{aligned}
&\sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{n\ge U\log U} \frac{e^{-n/U}}{n} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p \\
&\quad \ll \frac{\log x}{U\log U}\sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{m\le\sqrt{x}\\ 4m^2\equiv r^2 \pmod{k^2}}} 1 \ll \frac{\sqrt{x}\log x}{U\log U} \ll \frac{\sqrt{x}}{\log^c x}.
\end{aligned}$$

Substituting this into (19) we obtain

$$\begin{aligned}
&\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p \\
&\quad = \sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k}\sum_{n<U\log U} \frac{e^{-n/U}}{n} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).
\end{aligned} \tag{20}$$

Since $\left(\frac{d_k(p)}{\bullet}\right)$ is periodic modulo $4n$, we can rewrite the inner sum as

$$\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}\\ d_k(p)=(r^2-4p^2)/k^2\equiv a \pmod{4n}}} \log p.$$

For positive coprime integers C and D define

$$\psi_1(X,C,D) := \sum_{\substack{2\le p\le X\\ p\equiv D \pmod C}} \log p.$$

Then our last sum becomes

$$\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}\psi_1(\sqrt{x},4Bnk^2,b)+\mathrm{O}\left(\frac{2^{\nu(nk)}}{k^2}\right)$$

where the O-term comes from the following estimates.

$$\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}\sum_{\substack{2\le p\le B(r)\\ p\equiv b \pmod{4Bnk^2}}}\log p$$
$$\ll \phi(4n)\cdot 2^{\nu(nk)}\cdot\frac{B(r)}{4Bnk^2}\log(B(r))\ll\frac{2^{\nu(nk)}}{Bk^2}.$$

Recall that $\psi_1(X,C,D)\sim\frac{X}{\phi(C)}$ (see [20, Chapter 2 §8.2 Theorem 5]) and define

$$E_1(X,C,D):=\psi_1(X,C,D)-\frac{X}{\phi(C)}.$$

Then,

$$\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}}\left(\frac{d_k(p)}{n}\right)\log p=$$
$$\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}$$
$$+\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}E_1(\sqrt{x},4Bnk^2,b)+\mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)$$

where as before

$$C_r(a,n,k)=\#\{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*: b\equiv A \pmod B; 4b^2\equiv r^2-ak^2 \pmod{4nk^2}\}.$$

Note that if we reverse the order of summation in the term involving $E_1(\sqrt{x},4Bnk^2,b)$, then the sum on a has at most one summand. Thus,

$$\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod B\\ 4b^2\equiv r^2-ak^2 \pmod{4nk^2}}}E_1(\sqrt{x},4Bnk^2,b)\ll\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\left|E_1(\sqrt{x},4Bnk^2,b)\right|.$$

Therefore, we may write (20) on page 18 as

$$\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}}L(1,\chi_{d_k(p)})\log p$$

$$(21)\qquad =\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n<U\log U}\frac{e^{-n/U}}{n}\Bigg[\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}$$

$$+\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\left|E_1(\sqrt{x},4Bnk^2,b)\right|+\mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)\Bigg]+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

Recall (see [17, Exercise 1.3.2]) that for $\epsilon>0$,

$$2^{\nu(m)}=\sum_{\substack{d|m\\d \text{ squarefree}}}1\le\sum_{d|m}1\ll(m)^{\epsilon}.$$

Thus,

$$\sum_{\substack{k\le V\\(k,2r)=1}}\sum_{n<U\log U}\frac{e^{-n/U}2^{\nu(nk)}}{nk^3}\ll\sum_{k\le V}\frac{1}{k^{3-\epsilon}}\sum_{n<U\log U}1\ll U\log U\ll\frac{\sqrt{x}}{\log^c x}$$

when

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

Therefore, (21) becomes

$$\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}}L(1,\chi_{d_k(p)})\log p$$

$$(22)\qquad =\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n<U\log U}\frac{e^{-n/U}}{n}\Bigg[\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}$$

$$+\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\left|E_1(\sqrt{x},4Bnk^2,b)\right|\Bigg]+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).$$

Applying the Cauchy-Schwarz inequality and using the identity $\phi(AB) = \phi(A)\phi(B)\frac{(A,B)}{\phi((A,B))}$, we obtain

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

$$\le \sum_{k\le V}\frac{1}{k}\left(\sum_{n\le U\log U}\frac{\phi(4Bnk^2)}{n^2}\right)^{1/2}\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2} \tag{23}$$

$$= \phi(B)\sum_{k\le V}\frac{\sqrt{\phi(k^2)}}{k}\left(\sum_{n\le U\log U}\frac{\phi(4n)}{n^2}\frac{(4n,B)}{\phi((4n,B))}\frac{(4Bn,k^2)}{\phi((4Bn,k^2))}\right)^{1/2}$$

$$\cdot\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}$$

Note that $\phi(4n)\le 4\phi(n)$, $\phi(k^2)=k\phi(k)$, $\phi(n)\le n$, and $\frac{(C,D)}{\phi((C,D))}=\prod_{p|(C,D)}\frac{p}{p-1}\le 2^{\nu(D)}\ll D^{\epsilon}$, for all $\epsilon>0$ (see [17, Exercise 1.3.2]). Therefore, the above estimate is

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

Substituting this into (23) and letting $m=4Bnk^2$, we obtain

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

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

The Barban-Davenport-Halberstam Theorem (see [2], [4, Chapter 29] or [5] and [6]) asserts that given any $l>0$ we have for $X>Q>X/\log^l X$

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

Therefore, if $\sqrt{x}>4BV^2U\log U>\sqrt{x}/\log^l(\sqrt{x})$, then

$$\sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\le U\log U\\ b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}} \frac{e^{-n/U}}{n}|E_1(\sqrt{x},4Bnk^2,b)|\ll(\log U)V^3\sqrt{U}\sqrt{\sqrt{x}\log x}\ll\frac{\sqrt{x}}{\log^c x}$$

when

$$U=\frac{\sqrt{x}}{\log^{5c+15}x}\quad\text{and}\quad V=\log^{(c+3)/2}x. \tag{24}$$

Combining this with (22) we obtain

$$
\begin{aligned}
&\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A \pmod B\\4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p\\
&=\sqrt{x}\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}\frac{e^{-n/U}}{n}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).
\end{aligned}
\tag{25}
$$

The proof of Lemma 2.4 (for $f=2$) now follows from the following lemma which also shows the convergence of the summation formula for $C_{r,A,B}$. □

Lemma 6.1.

$$
C_{r,A,B}=\sum_{\substack{k\le V\\n\le U\log U\\(k,2r)=1}}\frac{e^{-n/U}}{kn\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)+\mathrm{O}\left(\frac{1}{\log^c x}\right).
$$

Proof. Recall that $C_r(a,n,k)=\prod_{p|4Bnk^2}d_{p,a,k}(n)$, where the $d_{p,a,k}(n)$ are given in Lemma 5.2. In particluar, $d_{2,a,k}(n)$ is at most $2^{\mathrm{ord}_2(B)+3}$ by Lemma 5.2 (4)-(6). For $p|B$, $d_{p,a,k}(n)$ is at most $p^{\mathrm{ord}_p(B)}$ by Lemma 5.2 (1) and (3). For $p|nk$ and $p\nmid B$, $d_{p,a,k}(n)$ is at most 2. Therefore,

$$
C_r(a,n,k)\le 16B2^{\nu(k)}2^{\nu(n)-\nu((n,k))}=16B2^{\nu(nk)}
$$

Thus,

$$
\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)C_r(a,n,k)\ll\phi(n)2^{\nu(nk)}. \tag{26}
$$

Since $\phi(4Bnk^2)\ge 2\phi(B)\phi(n)\phi(k^2)$ and $2^{\nu(nk)}\le 2^{\nu(n)+\nu(k)}$,

$$
\sum_{\substack{k>V\\(k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}\frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{n\phi(4Bnk^2)}\ll\sum_{k>V}\frac{2^{\nu(k)}}{k^2\phi(k)}\sum_{n\le U\log U}\frac{e^{-n/U}2^{\nu(n)}}{n} \tag{27}
$$

Since, $\frac{2^{\nu(k)}}{\phi(k)}=\frac{1}{k}\prod_{p|k}\frac{2p}{p-1}\le\frac{12}{k}\prod_{\substack{p|k\\p>3}}3\ll\frac{3^{\nu(k)}}{k}$, we have that $\sum_{k>V}\frac{2^{\nu(k)}}{k^2\phi(k)}\ll\sum_{k>V}\frac{3^{\nu(k)}}{k^3}$. Recall [20, Excercise 4, pg 53] that $\sum_{n\le T}3^{\nu(n)}\ll T\log^2 T$, and using partial summation, we have $\sum_{k=V+1}^{X}\frac{3^{\nu(k)}}{k^3}\ll\frac{\log^2 V}{V^2}$. Thus,

$$
\sum_{k>V}\frac{2^{\nu(k)}}{k^2\phi(k)}\ll\frac{\log^2 V}{V^2}. \tag{28}
$$

Recalling that $\sum_{n\le T}2^{\nu(n)}\ll T\log T$ [20, Exercise 2, pg 53] and again using partial summation we have

$$
\sum_{n\le U\log U}\frac{e^{-n/U}2^{\nu(n)}}{n}\ll\frac{\log U}{U}+\int_1^{U\log U}\left(\frac{e^{-t/U}\log t}{t}+\frac{e^{-t/U}\log t}{U}\right)\,\mathrm{dt}\ll\log^2 U. \tag{29}
$$

Combining (27), (28) and (29) gives

$$\sum_{\substack{k\le V\\ n\le U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) \tag{30}$$

$$= \sum_{\substack{k\in\mathbb{N}\\ n\le U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) + \mathrm{O}\left(\frac{1}{\log^c x}\right)$$

whenever U and V are chosen as in (24).

Recall that for any $\epsilon > 0$, we have $2^{\nu(m)} \ll m^\epsilon$ (see pg. 20). Thus,

$$\sum_{k\in\mathbb{N}} \frac{2^{\nu(k)}}{k\phi(k^2)} \sum_{n>U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n} \ll \frac{1}{\sqrt{U\log U}} \int_{U\log U}^{\infty} e^{-t/U}\ \mathrm{dt} \ll \frac{1}{\log^c x}.$$

Combining this with (30), we have

$$\sum_{\substack{k\le V\\ n\le U\log U\\ (k,2r)=1}} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)$$

$$= \sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \sum_{n=1}^{\infty} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) + \mathrm{O}\left(\frac{1}{\log^c x}\right)$$

The proof of Lemma 6.1 now follows from the identity

$$\sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \sum_{n=1}^{\infty} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) \tag{31}$$

$$= \sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \sum_{n=1}^{\infty} \frac{1}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) + \mathrm{O}\left(\frac{1}{\log^c x}\right)$$

(see [8, pg. 15]). □

7. Constructing a Multiplicative Function

Let $e_{2,a,k}(n) = \frac{d_{2,a,k}(n)}{d_{2,a,k}(1)}$ if $d_{2,a,k}(1) \neq 0$ and 0 otherwise. Set $n = 2^{\mathrm{ord}_2 n} n'$. We define

$$c_k(n) := \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) e_{2,a,k}(n) \prod_{\substack{p|n\\ p\neq 2}} d_{p,a,k}(n).$$

Lemma 7.1. *Let q be an odd prime. For $\alpha > 0$,*

(1) *$c_k(n)$ is a multiplicative function in n and $c_k(1) = 1$.*
(2) *Suppose $q|B$ and write $k = q^\beta k_1$, where $\mathrm{ord}_q(k) = \beta$.*

(a) *If* $2\beta \geq \mathrm{ord}_q(B)$, *then*

$$c_k(q^\alpha) = \begin{cases} q^{\mathrm{ord}_q(B)}\phi(q^\alpha) & \text{if } r^2 \equiv 4A^2 \pmod{q^{\mathrm{ord}_q(B)}} \\ & \text{and } \alpha \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

(b) *If* $2\beta < \mathrm{ord}_q(B)$, *then*

$$c_k(q^\alpha) = \begin{cases} q^{\alpha - \min(\alpha, \mathrm{ord}_q(B) - 2\beta)} \left(\frac{(r^2-4A^2)/q^{2\beta}}{q}\right)^\alpha & \text{if } r^2 \equiv 4A^2 \pmod{q^{2\beta}} \\ 0 & \text{otherwise.} \end{cases}$$

(3) *Suppose* $q \nmid B$.

(a) *If* $q|k$, *then*

$$c_k(q^\alpha) = \begin{cases} 2q^{\alpha-1}(q-1) & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd.} \end{cases}$$

(b) *Suppose* $q \nmid k$.

$$c_k(q^\alpha) = \begin{cases} q^{\alpha-1}\left(\frac{-1}{q}\right)(q-1) & \text{if } q|r \text{ and } \alpha \text{ is odd} \\ -q^{\alpha-1}\left[\left(\frac{-1}{q}\right)+1\right] & \text{if } q \nmid r \text{ and } \alpha \text{ is odd} \\ q^{\alpha-1}(q-1) & \text{if } q|r \text{ and } \alpha \text{ is even} \\ q^{\alpha-1}\left[q-3\right] & \text{if } q \nmid r \text{ and } \alpha \text{ is even} \end{cases}$$

(4) $c_k(2^\alpha) = (-2)^\alpha$

(5) $c_k(q^\alpha) = c_{q^{\mathrm{ord}_q(k)}}(q^\alpha)$

Proof. For the proof of part (1), we refer the reader to [7, pg. 10] where a similar result is proved. In the proofs of parts (2) and (3) of the lemma, it will be convenient to note that if q is an odd prime and $\alpha > 0$, we have

$$c_k(q^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1 \\ q^{\min(l_1,l_2)} | (4A^2 - r^2 + ak^2)}} \left(\frac{a}{q}\right)^\alpha \sum_{\substack{b \in (\mathbb{Z}/q^l\mathbb{Z})^* \\ b \equiv A \pmod{q^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{q^{l_2}}}} 1$$

where, as before, $l_1 = \mathrm{ord}_q(B)$, $l_2 = \mathrm{ord}_q(q^\alpha k^2) = \alpha + 2\mathrm{ord}_q(k)$ and $l = l_1 + l_2$. Setting $\beta = \mathrm{ord}_q(k)$, we can use Lemma 5.2 to evaluate the inner sum and obtain

$$c_k(q^\alpha) = c_{q^\beta}(q^\alpha) = \begin{cases} q^{\min(l_1,l_2)} \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1 \\ ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(l_1,l_2)}}}} \left(\frac{a}{q}\right)^\alpha & \text{if } q|B \\ \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2-ak^2, q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha \left(1 + \left(\frac{r^2-ak^2}{q}\right)\right) & \text{if } q \nmid B \end{cases}$$

which implies part (5).

(2) Suppose $q|B$. Set $k = q^\beta k_1$. If $2\beta \geq l_1$, then

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(l_1,l_2)}} \iff r^2 \equiv 4A^2 \pmod{q^{l_1}},$$

which implies that

$$c_k(q^\alpha) = \begin{cases} q^{\min(l_1,l_2)} \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha & \text{if } r^2 \equiv 4A^2 \pmod{q^{l_1}} \\ 0 & \text{otherwise} \end{cases}$$

On the other hand, if $2\beta < l_1$, then

$$\begin{aligned} & ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(l_1,\alpha+2\beta)}} \\ \iff & ak_1^2 \equiv \frac{r^2-4A^2}{q^{2\beta}} \pmod{q^{\min(l_1-2\beta,\alpha)}} \quad \text{and } q^{2\beta}|(r^2-4A^2), \end{aligned}$$

which implies

$$\begin{aligned} c_k(q^\alpha) &= q^{\min(l_1,l_2)} \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ (r^2-ak^2,q^\alpha)=1 \\ a\equiv\frac{r^2-4A^2}{q^{2\beta}}k_1^{-2} \pmod{4q^{\min(l_1-2\beta,\alpha)}} \\ q^{2\beta}|(r^2-4A^2)}} \left(\frac{a}{q}\right)^\alpha \\ &= \begin{cases} q^{\alpha-\min(\alpha,l_1-2\beta)} \left(\frac{(r^2-4A^2)/q^{2\beta}}{q}\right)^\alpha & \text{if } r^2 \equiv 4A^2 \pmod{q^{2\beta}} \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

(3a) Suppose $q \nmid B$ and $q|k$. Since $(k, 2r) = 1$, $q \nmid r$. Therefore, by Lemma 5.2 (2)

$$c_k(q^\alpha) = 2 \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4}} \left(\frac{a}{q}\right)^\alpha = \begin{cases} 2\phi(q^\alpha) & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd} \end{cases}$$

(3b) Suppose $q \nmid B$ and $q \nmid k$. First, consider odd α. Then using Lemma 5.2 (2)

$$\begin{aligned} c_k(q^\alpha) &= \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha \left(1 + \left(\frac{r^2-ak^2}{q}\right)\right) \\ &= q^{\alpha-1}\left[-\left(\frac{r^2k^{-2}}{q}\right) + \sum_{a\in(\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a^{-1}}{q}\right)\left(\frac{r^2-ak^2}{q}\right)\right] = \begin{cases} q^{\alpha-1}\left(\frac{-1}{q}\right)(q-1) & \text{if } q|r \\ q^{\alpha-1}\left[-1-\left(\frac{-1}{q}\right)\right] & \text{if } q \nmid r \end{cases} \end{aligned}$$

If α is even, then

$$c_k(q^\alpha) = \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha \left(1 + \left(\frac{r^2-ak^2}{q}\right)\right) = \begin{cases} q^{\alpha-1}[q-2] - q^{\alpha-1} & \text{if } q \nmid r \\ q^{\alpha-1}[q-1] & \text{if } q|r \end{cases}$$

(4) By definition

$$d_{2,a,k}(1) = \begin{cases} 2 & \text{if } 2 \nmid B \text{ and } a \equiv 1 \pmod 4 \\ 4 & \text{if } 2|B \text{ and } a \equiv 1 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Set $l_2 = \mathrm{ord}_2(4 \cdot 2^\alpha k^2) = \alpha + 2$; $l_1 = \mathrm{ord}_2(B)$; $l = l_1 + l_2$. Suppose $l_1 = 0$. Since r and k are odd

$$r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,\alpha+2)}} \Rightarrow a \equiv 5 \pmod 8 \Rightarrow \left(\frac{a}{2}\right) = \left(\frac{2}{a}\right) = -1.$$

Thus, Lemma 5.2 (4) gives

$$c_k(2^\alpha) = \sum_{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^*} \left(\frac{a}{2}\right)^\alpha \frac{d_{2,a,k}(2^\alpha)}{d_{2,a,k}(1)} = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,\alpha+2)}}}} (-1)^\alpha \frac{2^{\min(4,\alpha+1)}}{2} = (-2)^\alpha.$$

The proof is similar when $l_1 > 0$. □

8. Computing the Constant

Let $r, A, B \in \mathbb{Z}$ with $(A, B) = 1$ and r odd. In this section we prove Lemma 2.5. First, we record several evaluations of $d_{p,a,k}$ which follow directly from Lemma 5.2(1-3) (see pg. 14).

Lemma 8.1. *Suppose $p \nmid 2n$,*

(1) *If $p|B$ and $p \nmid k$, then $d_{p,a,k}(1) = d_{p,a,k}(n) = 1$*
(2) *Suppose $p|k$.*
   (a) *If $p|B$, then*

$$d_{p,a,k}(n) = \begin{cases} p^{\min(\mathrm{ord}_p(B), \mathrm{ord}_p(k^2))} & \text{if } 4A^2 \equiv r^2 \pmod{p^{\min(\mathrm{ord}_p(B), \mathrm{ord}_p(k^2))}} \\ 0 & \text{otherwise} \end{cases}$$

   (b) *If $p \nmid B$ and $(r^2 - ak^2, p) = 1$, then $d_{p,a,k}(1) = d_{p,a,k}(n) = 2$*

If $a \equiv 3 \pmod 4$ or $(r^2 - ak^2, n') \neq 1$, then $C_r(a, n, k) = 0$. Therefore, we may write

$$C_{r,A,B} = \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, n')=1}} \left(\frac{a}{n}\right) \prod_{\substack{p, \text{prime} \\ p|4Bnk^2}} d_{p,a,k}(n).$$

If $p|B$ and $p \nmid 2nk$, Lemma 8.1 (1) implies that $d_{p,a,k}(n) = 1$. For primes p with $p|k$ and $p \nmid 2n$ Lemma 8.1 (2) gives $d_{p,a,k}(n) = d_{p,a,k}(1)$. Therefore,

$$C_{r,A,B} = \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \cdot \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, n')=1}} \left(\frac{a}{n}\right) d_{2,a,k}(n) \left(\prod_{\substack{p|n \\ p \neq 2}} d_{p,a,k}(n)\right) \left(\prod_{\substack{p|k \\ p \nmid 2n}} d_{p,a,k}(1)\right).$$

Note that if $d_{2,a,k}(1)=0$, then $4A^2 \not\equiv r^2-ak^2 \pmod{2^{\min(\mathrm{ord}_2(B),\mathrm{ord}_2(4k^2))}}$, which implies that $4A^2 \not\equiv r^2-ak^2 \pmod{2^{\min(\mathrm{ord}_2(B),\mathrm{ord}_2(4nk^2))}}$. Therefore, $d_{2,a,k}(1)=0 \Rightarrow d_{2,a,k}(n)=0$. Thus, $d_{2,a,k}(n)=d_{2,a,k}(1)e_{2,a,k}(n)$ and

$$C_{r,A,B}=\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)}\cdot\sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\a\equiv 1 \pmod 4\\(r^2-ak^2,n')=1}}\left(\frac{a}{n}\right)d_{2,a,k}(1)e_{2,a,k}(n)\left(\prod_{\substack{p|n\\p\neq 2}}d_{p,a,k}(n)\right)\left(\prod_{\substack{p|k\\p\nmid 2n}}d_{p,a,k}(1)\right).$$

For odd primes p, we see from the definition that $d_{p,a,k}(1)=d_{p,1,k}$. Also, since $a\equiv 1 \pmod 4$, $d_{2,a,k}(1)$ depends only on the parity of B. Thus we may write

$$C_{r,A,B}=d_{2,1,1}(1)\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)}\left(\prod_{\substack{p|(B,k)\\p\nmid 2n}}d_{p,1,k}(1)\right)\left(\prod_{\substack{p|k\\p\nmid 2Bn}}d_{p,1,k}(1)\right)c_k(n).$$

For integers x and y denote by $\nu(x,y)$ the number of distinct prime divisors of the $gcd(x,y)$. Then by Lemma 8.1, $\prod_{\substack{p|k\\p\nmid 2Bn}}d_{p,1,k}(1)=2^{\nu(k)-\nu(k,2Bn)}$. Using this along with the identity $\phi(AB)=\phi(A)\phi(B)\frac{(A,B)}{\phi((A,B))}$ allows us to write

$$C_{r,A,B}=d_{2,1,1}(1)\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\frac{2^{\nu(k)}}{k\phi(4Bk^2)}\cdot\sum_{n\in\mathbb{N}}\frac{\left[\prod_{\substack{p|(B,k)\\p\nmid 2n}}d_{p,1,k}(1)\right]\phi((n,4Bk^2))}{n\phi(n)(n,4Bk^2)2^{\nu(k,2Bn)}}c_k(n). \tag{32}$$

It is straightforward to check that

$$2^{\nu(k,2Bn)}=\frac{2^{\nu(k,B)}\cdot 2^{\nu\left(\frac{k}{(k,B)},n\right)}}{2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}. \tag{33}$$

Thus we may write (32) as

$$d_{2,1,1}(1)\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\frac{2^{\nu(k)}}{k2^{\nu(k,B)}\phi(4Bk^2)}\cdot\sum_{n\in\mathbb{N}}\frac{\left[\prod_{\substack{p|(B,k)\\p\nmid 2n}}d_{p,1,k}(1)\right]\phi((n,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{n\phi(n)(n,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},n\right)}}c_k(n). \tag{34}$$

For convenience we record the following fact as a lemma.

Lemma 8.2. *Suppose $p|(B,n,k)$. If $d_{p,1,k}(1)=0$, then $c_k(n)=0$.*

Proof. Let $\alpha=\mathrm{ord}_p(B)$ and $\beta=\mathrm{ord}_p(k)$. Recalling that $d_{p,a,k}(1)$ is independent of a, we have

$$\begin{aligned}d_{p,1,k}(1)=0 &\Rightarrow 4A^2\not\equiv r^2-ak^2 \pmod{p^{\min(\alpha,2\beta)}} \quad \text{for all } a\\ &\Rightarrow 4A^2\not\equiv r^2-ak^2 \pmod{p^{\min(\alpha,2\beta+\mathrm{ord}_p(n))}}\\ &\Rightarrow d_{p,a,k}(n)=0 \quad \text{for all } a \Rightarrow c_k(n)=0.\end{aligned}$$

□

For $p|(B,k,n)$, let $f_{p,k} = d_{p,1,k}(1)$ if $d_{p,1,k}(1) \neq 0$ and 1 otherwise. Then by Lemma 8.2,

$$\left(\prod_{\substack{p|(B,k)\\ p\nmid 2n}} d_{p,1,k}(1)\right) c_k(n) = \frac{\prod_{p|(B,k)} d_{p,1,k}(1)}{\prod_{p|(B,k,n)} f_{p,k}} c_k(n)$$

Note that if $d_{p,1,k}(1) = 0$ for some $p|(B,k)$, then both sides of the above equation are 0. Thus we may write $C_{r,A,B}$ as

(35)

$$\frac{d_{2,1,1}(1)}{\phi(4B)} \sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \frac{2^{\nu(k)}\phi((4B,k^2))\prod_{p|(B,k)} d_{p,1,k}(1)}{k2^{\nu(k,B)}\phi(k^2)(4B,k^2)} \sum_{n\in\mathbb{N}} \frac{\phi((n,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{\left[\prod_{p|(B,k,n)} f_{p,k}\right] n\phi(n)(n,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},n\right)}} c_k(n).$$

Upon noting that the summand of the inner sum is multiplicative and using Lemma 7.1(5) we may rewrite the inner sum as

(36)

$$\prod_{q,\ \text{prime}} \sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)} f_{p,k}\right] q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},q^\alpha\right)}} c_k(q^\alpha)$$

$$= \prod_{q\nmid k}\left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)\right) \prod_{q|k}\left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)} f_{p,k}\right] q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},q^\alpha\right)}} c_{q^{\mathrm{ord}_q(k)}}(q^\alpha)\right)$$

$$= \prod_{q,\text{prime}}\left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)\right) \prod_{q|k} \frac{\left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)} f_{p,k}\right]q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},q^\alpha\right)}} c_{q^{\mathrm{ord}_q(k)}}(q^\alpha)\right)}{\left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)\right)}$$

Substituting (36) into (35) we obtain

$$C_{r,A,B} = \frac{d_{2,1,1}(1)}{\phi(4B)} \prod_q \left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}\right) \sum_{\substack{k\in\mathbb{N}\\ (k,2r)=1}} \left(\frac{2^{\nu(k)}\left[\prod_{p|(B,k)} d_{p,1,k}(1)\right]\phi((4B,k^2))}{k2^{\nu(k,B)}\phi(k^2)(4B,k^2)}\right)$$

$$\cdot \prod_{\substack{q^\beta||k\\ \beta\geq 1}} \frac{\left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bq^{2\beta}))2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)},q^\alpha\right)} c_{q^\beta}(q^\alpha)}{\left[\prod_{p|(B,q)} f_{p,k}\right]q^\alpha\phi(q^\alpha)(q^\alpha,4Bq^{2\beta})2^{\nu\left(\frac{q^\beta}{(q^\beta,B)},q^\alpha\right)}}\right)}{\left(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}\right)} \tag{37}$$

Note that the powers of 2 in the innermost sum are the same regardless of the values of α and β. Also, note that the sum on k is a sum of multiplicative functions which allows us to

write this sum as

$$\prod_{\substack{q\\ q\nmid 2r}}\left[1+\sum_{\beta\geq 1}\left(\frac{\frac{2\left[\prod_{p|(B,q)} d_{p,1,q^\beta}(1)\right]\phi((4B,q^{2\beta}))}{q^\beta 2^{\nu(q^\beta,B)}\phi(q^{2\beta})(4B,q^{2\beta})}}{\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4B))c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}}\right)\cdot\left(\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,4Bq^{2\beta}))c_{q^\beta}(q^\alpha)}{\left[\prod_{p|(B,q)} f_{p,q^\beta}\right]q^\alpha\phi(q^\alpha)(q^\alpha,4Bq^{2\beta})}\right)\right] \tag{38}$$

Substituting (38) into (37) and noting that $\frac{\phi(q^j)}{q^j q^\alpha\phi(q^\alpha)}=\frac{1}{q^{2\alpha}}$ if $j>0$, we have

$$\begin{aligned} C_{r,A,B} = {} & \frac{d_{2,1,1}(1)}{\phi(4B)}\left(1+\sum_{\alpha\geq 1}\frac{c_1(2^\alpha)}{2^{2\alpha}}\right)\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}}\left(\sum_{\alpha\geq 0}\frac{c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)}\right)\prod_{\substack{q,\text{odd}\\ q|B\\ q|r}}\left(1+\sum_{\alpha\geq 1}\frac{c_1(q^\alpha)}{q^{2\alpha}}\right) \\ & \cdot\prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}}\left(\sum_{\alpha\geq 0}\frac{c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)}+\sum_{\beta\geq 1}\frac{2}{q^\beta\phi(q^{2\beta})}\left(1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{2q^{2\alpha}}\right)\right) \\ & \cdot\prod_{\substack{q,\text{odd}\\ q|B\\ q\nmid r}}\left(1+\sum_{\alpha\geq 1}\frac{c_1(q^\alpha)}{q^{2\alpha}}+\sum_{\beta\geq 1}\frac{d_{q,1,q^\beta}(1)}{f_{q,q^\beta}}\frac{1}{q^{3\beta}}\left(1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right)\right) \end{aligned} \tag{39}$$

Now using Lemma 7.1, and the formula for geometric series, Lemma 2.5 follows.

References

[1] S. Baier. The Lang-Trotter conjecture on average. *J. Ramanujan Math. Soc.*, 22(4):299–314, 2007.

[2] M.B. Barban. On the distribution of primes in arithmetic progressions "on average". *Dokl. Akad. NaukUzSSR*, 5:5–7, 1964. Russian.

[3] Jonathan Battista, Jonathan Bayless, Dmitriy Ivanov, and Kevin James. Average Frobenius distributions for elliptic curves with nontrivial rational torsion. *Acta Arith.*, 119(1):81–91, 2005.

[4] H. Davenport. *Multiplicative Number Theory.* Springer-Verlag, New York, 1980.

[5] H. Davenport and H. Halberstam. Primes in arithmetic progressions. *Michigan Math. J.*, 13:485–489, 1966.

[6] H. Davenport and H. Halberstam. Corrigendum: "primes in arithmetic progression". *Michigan Math. J.*, 15:505, 1968.

[7] Chantal David and Francesco Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, (4):165–183, 1999.

[8] Chantal David and Francesco Pappalardi. Average Frobenius distribution for inerts in $\mathbb{Q}(i)$. *J. Ramanujan Math. Soc.*, 19(3):181–201, 2004.

[9] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[10] Noam D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[11] É. Fouvry and M. Ram Murty. Supersingular primes common to two elliptic curves. In *Number theory (Paris, 1992–1993)*, volume 215 of *London Math. Soc. Lecture Note Ser.*, pages 91–102. Cambridge Univ. Press, Cambridge, 1995.

[12] Etienne Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[13] Kevin James. Average Frobenius distributions for elliptic curves with 3-torsion. *J. Number Theory*, 109(2):278–298, 2004.

[14] Kevin James. Averaging special values of Dirichlet L-series. *Ramanujan J.*, 10(1):75–87, 2005.

[15] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504.

[16] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

[17] M. Ram Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001. , Readings in Mathematics.

[18] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[19] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[20] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 46 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.

[21] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

Ferrum College, 80 Wiley Dr. Ferrum, VA 24088, USA

Department of Mathematical Sciences, Clemson University BOX 340975 Clemson, SC 29634-0975, USA

E-mail address: bfaulkner@ferrum.edu

E-mail address: kevja@clemson.edu

URL: <http://www.math.clemson.edu/∼kevja/>