AVERAGE FROBENIUS DISTRIBUTIONS FOR ELLIPTIC CURVES OVER ABELIAN EXTENSIONS

BRYAN FAULKNER, KEVIN JAMES, MATTHEW KING, TODD MOLNAR, AND KENNY STAUFFER

Abstract. Let E be an elliptic curve defined over some Abelian number field K with ring of integers $\mathcal{O}_K$. For a prime $\mathfrak{p}$ of degree f in $\mathcal{O}_K$ let $a_{\mathfrak{p}}(E)$ be the trace of the Frobenius morphism. Let p be a rational prime such that $\mathfrak{p}$ lies above p. By Hasse's theorem, we know that $a_{\mathfrak{p}}(E)$ satisfies the inequality $|a_{\mathfrak{p}}(E)| \leq 2p^{f/2}$. For a fixed integer r we define

$$\pi_E^{r,f}(x) = \#\{\mathfrak{p} \ : \ N(\mathfrak{p}) \leq x, \deg_K(\mathfrak{p}) = f, \text{ and } a_{\mathfrak{p}}(E) = r\}.$$

A generalization of the Lang-Trotter conjecture for elliptic curves over number fields asserts that there exists a positive real constant $C_{E,r,f}$ such that

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

We prove an average version of the above conjecture. For the $f = 1$ and $f = 2$ cases we calculate an explicit constant.

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 $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ of degree f which lies above the rational prime p in $\mathbb{Z}$. We denote the degree of a prime in $\mathcal{O}_K$ 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

$$\pi_E^{r,f}(x) = \#\{\mathfrak{p} \ : \ N(\mathfrak{p}) \leq x, \, deg_K(\mathfrak{p}) = f, \text{ and } a_{\mathfrak{p}}(E) = r\}.$$

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

Conjecture 0.1. *Except for the case where $r = 0$ and E has complex mulitplication, there is a constant $C_{E,r}$ such that*

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

Very little is known about the Lang-Trotter conjecture. In [?] Elkies found that for any elliptic curve E over $\mathbb{Q}$, there are infinitely many primes p such that $a_p(E) = 0$, but there are no other results of this type with $a_p(E) \neq 0$. There are several average results (see [?], [?], [?], [?], [?], [?]). In [?] David and Pappalardi prove

Theorem 0.2. *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 to include number fields other than $\mathbb{Q}(i)$ and we allow f to be any positive integer such that $f | [K : \mathbb{Q}]$. Let $[\alpha_1, \ldots, \alpha_n]$ be an integral basis for $\mathcal{O}_K$. By an integral basis we mean that

$$\mathcal{O}_K \cong \bigoplus_{1 \leq i \leq n} \mathbb{Z}\alpha_i.$$

Then for any $A \in \mathcal{O}_K$ there exist $\vec{v} \in \mathbb{Z}^n$ such that $A = \sum_{i=1}^n \vec{v}[i]\alpha_i$. Define

$$\|\vec{v}\| := \max_{1 \leq i \leq n} \{\vec{v}[i]\}.$$

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

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

Definition 0.3. *For a parameter $t \in \mathbb{R}$ let $\mathcal{C}_t$ be the set of elliptic curves defined over $\mathcal{O}_K$ which have Weierstrass equations*

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

where $\|\vec{v_1}\|, \|\vec{v_2}\| \leq t$.

Brett Tangedal points out the following fact which is a corollary to [**?**, Chapter 3, Theorem 3.7].

Fact 0.4. *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.*

In this chapter we prove

Theorem 0.5. *If $K/\mathbb{Q}$ is an abelian extension of degree n, then*

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

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

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

where $D_{r,f,k}$ is defined as follows for $f = 1, 2$. Select $a_1, \ldots a_l$ and B so that $deg_K(\mathfrak{p}) = f$ if and only if $p \equiv a_1, \ldots a_l \pmod{B}$ (This can be done since K/Q is Abelian.), where $\mathfrak{p}$ is a prime above the rational prime p. Then,

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

and

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

$$\cdot \frac{2n}{3\pi\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)}\right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right)q - 1}{(q-1)(q^2-1)}\right) \sum_{i=1}^{l} c_{r,a_i,B}$$

where $k_{r,a_i,B}$ *and* $c_{r,a_i,B}$ *are defined as follows. Let* $r, A, B \in \mathbb{Z}$ *with* $(A,B) = 1$ *and* r *odd. Let* $\Delta^{r,A} = r^2 - 4A$ *and put*

$$\mathfrak{Q}^{<}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \operatorname{ord}_q(\Delta^{r,A}) < \operatorname{ord}_q(B)\} \quad \textit{and}$$
$$\mathfrak{Q}^{\geq}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \operatorname{ord}_q(\Delta^{r,A}) \geq \operatorname{ord}_q(B)\}$$

For $q \in \mathfrak{Q}^{<}_{r,A,B}$, *we let*

$$\Gamma_q = \begin{cases} \left(\frac{(\Delta^{r,A})/q^{\operatorname{ord}_q(\Delta^{r,A})}}{q}\right) & \textit{if } \operatorname{ord}_q(\Delta^{r,A}) \textit{ is even, positive and finite,} \\ 0 & \textit{otherwise.} \end{cases}$$

then

$$k_{r,A,B} = \prod_{\substack{q,\text{odd}\\ q|B\\ q|r}} \frac{q\left(q + \left(\frac{-A}{q}\right)\right)}{q_2 - 1} \prod_{q \in \mathfrak{Q}^{\geq}_{r,A,B}} \left(\frac{q^{\lfloor\frac{\operatorname{ord}_q(B)+1}{2}\rfloor} - 1}{q^{\lfloor\frac{\operatorname{ord}_q(B)-1}{2}\rfloor}(q-1)} + \frac{q^{\operatorname{ord}_q(B)+2}}{q^{3\lfloor\frac{\operatorname{ord}_q(B)+1}{2}\rfloor}(q^2-1)}\right)$$

$$\cdot \prod_{q \in \mathfrak{Q}^{<}_{r,A,B}} \left(1 + \frac{q\left(\frac{\Delta^{r,A}}{q}\right) + \left(\frac{\Delta^{r,A}}{q}\right)^2 + q^{-\operatorname{ord}_q(\Delta^{r,A}/2)}(q\Gamma_q + q^2\Gamma_q^2)}{q^2 - 1} + \frac{\Gamma_q^2(q^{\lfloor\frac{\operatorname{ord}_q(\Delta^{r,A})-1}{2}\rfloor} - 1)}{q^{\lfloor\frac{\operatorname{ord}_q(\Delta^{r,A})-1}{2}\rfloor}(q-1)}\right)$$

for $c_{r,A,B}$ *set* $\Delta_q = \operatorname{ord}_q(r^2 - 4A^2)$, $L_q = \left(\frac{r^2-4A^2}{q}\right)$ *and put*

$$\mathfrak{P}^{\leq}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \operatorname{ord}_q(B) \leq \Delta_q\} \quad \textit{and}$$
$$\mathfrak{P}^{>}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \operatorname{ord}_q(B) > \Delta_q > 0\}.$$

Let

$$\gamma_q = \left(\frac{\Delta/q^{\Delta_q}}{q}\right)$$

then

$$c_{r,A,B} = \prod_{\substack{q,\text{odd} \\ q \mid B \\ q \nmid r \\ \Delta_q = 0}} \left(1 + \frac{L_q q^{2\mathrm{ord}_q(B)} - L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)+2} - L_q q^{2\mathrm{ord}_q(B)}} + \frac{L_q^{\mathrm{ord}_q(B)+1}}{q - L_q} \right)$$

$$\cdot \prod_{\substack{q,\text{odd} \\ q \in \mathfrak{P}^{\leq}_{r,A,B}}} \left(1 + \frac{1 - q^{-3\left\lceil \frac{\mathrm{ord}_q(B)}{2} - 1 \right\rceil}}{q^3 - 1} + \frac{(q^2 + q + q^{\mathrm{ord}_q(B)}) q^{2 - 2\left\lceil \frac{\mathrm{ord}_q(B)}{2} \right\rceil}}{(q+1)(q^3-1)} \right)$$

$$\prod_{\substack{q,\text{odd} \\ q \in \mathfrak{P}^{>}_{r,A,B} \\ \Delta_q \equiv 1 \pmod 2}} \left(\frac{1 - q^{-3\lceil \Delta_q/2 - 1 \rceil}}{q^3 - 1} \right) \prod_{\substack{q,\text{odd} \\ q \in \mathfrak{P}^{>}_{r,A,B} \\ \Delta_q \equiv 0 \pmod 2}} \left(\frac{1 - q^{-3(\Delta_q/2 - 1)}}{q^3 - 1} + \right.$$

$$\left. \frac{1}{q^{3\Delta_q/2}} \left[1 + \gamma_q \left[\frac{(q^{2(\mathrm{ord}_q(B) - \Delta_q)} - \gamma_q^{\mathrm{ord}_q(B) - \Delta_q})(q - \gamma_q) + \gamma_q^{\mathrm{ord}_q(B) - \Delta_q}(q^2 - \gamma_q)}{q^{2(\mathrm{ord}_q(B) - \Delta_q)}(q - \gamma_q)(q^2 - \gamma_q)} \right] \right] \right).$$

An immediate corollary is

Corollary 0.6. *With the notation from above*

(1) *For* $t \gg x^{3/2}\log x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,1}(x) \sim D_{r,1,K}\frac{\sqrt{x}}{\log x}.$$

(2) *For* $t \gg \sqrt{x}\log x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,2}(x) \sim D_{r,2,K}\log\log x.$$

(3) *For* $t \gg x^{1/6}\log x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,3}(x) = \mathrm{O}(1).$$

(4) *For* $t \gg \log\log x\log^2 x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,4}(x) = \mathrm{O}(1).$$

(5) *For* $f \geq 5$ *and* $t \gg \log^2 x$,
$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) = \mathrm{O}(1).$$

In order to prove Theorem 0.5 we employ the following three lemmas.

Lemma 0.7. *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*

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

$$= \frac{n}{\pi}\left[\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{l}\sum_{\substack{k\le 2x^{f/2}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\k^2|r^2-4p^f\\p\equiv a_i \pmod B}} L(1,\chi_{d_k(p)})\log p\right.$$

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

where

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

Lemma 0.8. *Suppose that $r, A, B \in \mathbb{Z}$, with r odd.*

(1) *($f = 1$) Set $d_k(p) = (r^2 - 4p)/k^2$, if $k^2 | (r^2 - 4p)$ and 0 otherwise. Let $B(r) = \max\{5, r^2/4\}$. and $\chi_{d_k(p)} = \left(\frac{d_k(p)}{\bullet}\right)$. For every $c > 0$,*

$$\sum_{k \leq 2\sqrt{x}} \frac{1}{k} \sum_{\substack{B(r) < p \leq x \\ p \equiv A \pmod{B} \\ 4p \equiv r^2 \pmod{k^2}}} L(1, \chi_{d_k(p)}) \log p = K_{r,A,B}\, x + \mathrm{O}\left(\frac{x}{\log^c x}\right)$$

(2) *($f = 2$) Set $d_k(p) = (r^2 - 4p^2)/k^2$, if $k^2 | (r^2 - 4p^2)$ and 0 otherwise. Let $B(r) = \max\{3, r, r^2/4\}$. and $\chi_{d_k(p)} = \left(\frac{d_k(p)}{\bullet}\right)$. For every $c > 0$,*

$$\sum_{\substack{k \leq 2x \\ (k, 2r) = 1}} \frac{1}{k} \sum_{\substack{B(r) < p \leq x^{1/2} \\ p \equiv A \pmod{B} \\ 4p^2 \equiv r^2 \pmod{k^2}}} L(1, \chi_{d_k(p)}) \log p = C_{r,A,B} \sqrt{x} + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

where $L(s, \chi_{d_k(p)})$ is the Dirichlet L-function of $\chi_{d_k(p)}$.
We define $C_{r,A,B}$ by

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

where

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

We define $K_{r,A,B}$ by

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

where

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

Lemma 0.9. *With the notation used in Theorem 0.5 and Lemma 0.8*

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

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

The organization of the rest of this paper is as follows. Using the above three lemmas we prove Theorem 0.5 in section 1. Let $E_{A,B}$ be a curve defined over $\mathcal{O}_K/\mathfrak{p}$. After determining the number of elliptic curves in $\mathcal{C}_t$ which reduce to $E_{A,B}$ over $\mathcal{O}_K/\mathfrak{p}$ in section 2 we give the average in terms of Hurwitz class numbers by using Deuring's theorem in section 3. Then using the class formula we obtain a result in terms of L-series and prove Lemma 0.7. Section 4 is devoted to computing $C_r(a, n, k)$ defined in Lemma 0.8. In section 5 we use arguments similar to those of David and Pappalardi [**?**, lemma 2.2] to prove part *1* of Lemma 0.8. We construct a multiplicative function in section 6 which is a necessary tool in section 7 where we manipulate the double sum, $C_{r,A,B}$ defined in Lemma 0.8 and prove Lemma 0.9.

1. Proof of Main Theorem

In this section we prove Theorem 0.5. Suppose $f = 1$. We combine Lemmas 0.7 and 0.8 (2) to obtain

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

Recall the expression for $D_{r,1,K}$

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

In [**?**] James proved

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

We make two observations:

(1)

$$\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{l}\left(K_{r,a_i,B}x+\mathrm{O}\left(\frac{x}{\log^c x}\right)\right)=\frac{\sqrt{x}}{\log x}\sum_{i=1}^{l}K_{r,a_i,B}+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

(2)

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

Therefore, we may write

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

Note that $\frac{\mathrm{d}}{\mathrm{dS}}\frac{1}{\sqrt{S}\log S}=-\left[\frac{1}{2S^{3/2}\log S}+\frac{1}{S^{3/2}\log^2 S}\right]$. For the O-term inside the integral we have

$$\begin{aligned}\int_2^x\left(\frac{S}{\log^c S}\right)\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{dS}&=-\int_2^x\frac{S}{\log^c S}\left[\frac{1}{2S^{3/2}\log S}+\frac{1}{S^{3/2}\log^2 S}\right]\,\mathrm{dS}\\&\ll\frac{1}{\log^c x}.\end{aligned}$$

Therefore,

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

Recall the definition for $\pi_{1/2}(X)$

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

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,

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

This completes the proof for the $f = 1$ case.
Suppose $f = 2$. Combine Lemmas 0.7 and 0.8 (1) to obtain

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

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

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

For the O-term note that

$$\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{\sqrt{S}}{\log^c S}\right) = \frac{1}{2\sqrt{S}\log^c S} - \frac{c}{\sqrt{S}\log^{c+1} S}.$$

Integrating by parts gives

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

Therefore,

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

Recall the expression for $D_{r,2,K}$

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

$$\cdot \frac{2n}{3\pi\phi(B)} \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q|r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)}\right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right) q - 1}{(q-1)(q^2-1)}\right) \sum_{i=1}^{l} c_{r,a_i,B}.$$

By Lemma 0.9

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

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

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 (8) and (9) from Section 3.

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

and

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

We use $H(4p^f - r^2) \ll p^{f/2} \log^2 p$ (see pg. 17) 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,

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

This concludes the proof of Theorem 0.5.

2. Counting Curves

Let $K/\mathbb{Q}$ be a Galois extension of degree n. Choose $\alpha_1,\ldots,\alpha_n$ so that $[\alpha_1,\ldots,\alpha_n]$ is a $\mathbb{Q}$-basis for K and $[\alpha_1,\ldots,\alpha_n]$ is an integral basis for $\mathcal{O}_K$. Let $p\in\mathbb{Z}$ be a rational prime, and $\mathfrak{p}_1,\ldots\mathfrak{p}_g$ be the distinct primes in $\mathcal{O}_K$ above p. Suppose that p does not ramify in $\mathcal{O}_K$, so that

$$p\mathcal{O}_K=\mathfrak{p}_1\cdots\mathfrak{p}_g.$$

Since K is Galois over $\mathbb{Q}$, there exist a positive integer f, so that $[\mathcal{O}_K/\mathfrak{p}_i:\mathbb{Z}/p\mathbb{Z}]=f$ for all i, $1\leq i\leq g$. The ring, $\mathcal{O}_K$ may be thought of as a $\mathbb{Z}$-module generated by α_i, $1\leq i\leq n$. For a parameter $t\in\mathbb{R}$ to be chosen later recall the notation given in definition 0.3. For $\vec{v}\in\mathbb{Z}^n$ define

$$\|\vec{v}\|:=\max_{1\leq i\leq n}\{\vec{v}[i]\}$$

and

$$A'(\vec{v}):=\sum_{i=1}^{n}\vec{v}[i]\alpha_i.$$

Recall for $\vec{v_1},\vec{v_2}\in(\mathbb{Z}^n)^2$, we denote by $E_{\vec{v_1},\vec{v_2}}$ the elliptic curve

$$y^2=x^3+A'(\vec{v_1})x+A'(\vec{v_2}). \tag{2}$$

Recall the definition of $\mathcal{C}_t$

$$\mathcal{C}_t=\{E_{\vec{v_1},\vec{v_2}}:\|\vec{v_1}\|,\|\vec{v_2}\|\leq t\}.$$

Since

$$\begin{aligned}&\#\{(\vec{v},\vec{w})\in(\mathbb{Z}^n)^2\mid|\vec{v}[i]|,|\vec{w}[i]|\leq t\ ;\ 1\leq i\leq n\}\\&=(2t+\mathrm{O}(1))^{2n}\end{aligned}$$

we have

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

Therefore,

$$\frac{1}{|\mathcal{C}_t|}=\frac{1}{4^nt^{2n}}+\mathrm{O}\left(\frac{1}{t^{2n+1}}\right). \tag{3}$$

Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. The curve $E_{\vec{v_1},\vec{v_2}}$ from (2) is said to be *minimal* whenever the highest power of $\mathfrak{p}$ dividing the discriminant is minimized, that is whenever $\mathrm{ord}_\mathfrak{p}(\Delta(E_{\vec{v_1},\vec{v_2}}))$ is minimized. According to Silverman [**?**, pg. 172] if $\mathfrak{p}\nmid 6$, then $E_{\vec{v_1},\vec{v_2}}$ 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 $E_{A,B}$ 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 $\mathcal{O}_K/\mathfrak{p}$. To reduce $E_{\vec{v_1},\vec{v_2}}$ modulo $\mathfrak{p}$ we mean that one should first obtain a model

$$E : y^2 = x^3 + u^4 A'(\vec{v_1}) + u^6 A'(\vec{v_2})$$

which is minimal at $\mathfrak{p}$, then reduce the coefficients of the minimal model (see [**?**, 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 find asymptotics for the size of the set $\mathcal{C}_t(E_{A,B})$ by thinking of $p^N\mathcal{O}_K$ and $\mathfrak{p}^N$ as $\mathbb{Z}$-modules, where $N \geq 1$. We start with the following inclusions,

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

Since $p^N\mathcal{O}_K$ and $\mathfrak{p}^N$ are $\mathbb{Z}$-submodules of $\mathcal{O}_K$ the third isomorphism theorem for modules gives

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

Therefore,

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

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

$$\begin{aligned}
&A'(\vec{v}) \equiv A \pmod{\mathfrak{p}^N} \\
\Leftrightarrow\ & A'(\vec{v}) - A \in \mathfrak{p}^N \\
\Leftrightarrow\ & A'(\vec{v}) - A \equiv \rho_i \pmod{p^N\mathcal{O}_K} \quad (\text{some } 1 \leq i \leq s) \\
\Leftrightarrow\ & A'(\vec{v}) \equiv A + \rho_i \pmod{p^N\mathcal{O}_K} \quad (\text{some } 1 \leq i \leq s).
\end{aligned}$$

For $1 \leq i \leq s$ set

$$A + \rho_i = \sum_{j=1}^{n} c_{i,j}\alpha_j \qquad c_{i,j} \in \mathbb{Z}.$$

Then

$$\begin{aligned}
&\#\{\vec{v} \in \mathbb{Z}^n | A'(\vec{v}) \equiv A \pmod{\mathfrak{p}^N}; \|\vec{v}\| \leq t\} \\
&= \sum_{i=1}^{s} \#\left\{(c_{i,1} + p^N k_1, c_{i,2} + p^N k_2, \ldots, c_{i,n} + p^N k_n) \ :\ \begin{matrix} |c_{i,j} + p^N k_j| \leq t; \\ 1 \leq j \leq n \end{matrix}\right\} \\
&= \sum_{i=1}^{s} \left(\frac{2t}{p^N} + \mathrm{O}(1)\right)^n \qquad (4) \\
&= p^{N(n-f)}\left[\left(\frac{2t}{p^N}\right)^n + \mathrm{O}\left(\frac{t^{n-1}}{p^{Nn-N}}\right)\right] \\
&= \frac{(2t)^n}{p^{Nf}} + \mathrm{O}\left(\frac{t^{n-1}}{p^{N(f-1)}}\right).
\end{aligned}$$

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

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

Considering non-minimal models we see that

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

Recall that if $\mathfrak{p} \nmid 6$, then $E_{\vec{v_1},\vec{v_2}}$ is minimal if and only if $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_1})) < 4$ and $\mathrm{ord}_{\mathfrak{p}}(A'(\vec{v_2})) < 6$. Therefore, we estimate $\#\{$non - minimal models$\}$ as follows.

$$\#\{\text{non-minimal models}\} = \#\{E_{\vec{v_1},\vec{v_2}} \in \mathcal{C}_t : A'(\vec{v_1}) \in \mathfrak{p}^4 \text{ and } A'(\vec{v_2}) \in \mathfrak{p}^6\}.$$

Using the estimates from (4) we have

$$\left(\frac{(2t)^n}{p^4 f} + \mathrm{O}\left(\frac{t^{n-1}}{p^{4(f-1)}}\right)\right)\left(\frac{(2t)^n}{p^6 f} + \mathrm{O}\left(\frac{t^{n-1}}{p^{6(f-1)}}\right)\right).$$

Hence, accounting for non-minimal models we have

$$
\begin{aligned}
|\mathcal{C}_t(E_{A,B})| &= \#\{E_{\vec{v_1},\vec{v_2}} \in \mathcal{C}_t | E^{\mathfrak{p}}_{\vec{v_1},\vec{v_2}} = E_{A,B}\} \\
&= \left(\frac{2^n t^n}{p^f}\right)^2 + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}\right) + \mathrm{O}\left(\frac{t^n}{p^4 f} \cdot \frac{t^n}{p^6 f}\right) \\
&= \left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)
\end{aligned}
$$

3. The Average in Terms of L-Series

Before proving Lemma 0.7 we discuss the Kronecker class number and the Hurwitz class number. In [?] Schoof defines the Kronecker class number as follows. For $a, b, c \in \mathbb{Z}$ with $a > 0$ let $\Delta_f = b^2 - 4ac$ be the discriminant of the binary quadratic form $f = ax^2 + bxy + cy^2$. For $\Delta < 0$, Schoof defines

$$K(\Delta) = \sum_{\substack{[f] \\ \Delta_f = \Delta}} 1$$

where the sum runs over classes of binary quadratic forms of discriminant Δ.
A definition of the Hurwitz class number used by Lenstra in [?] and the definition we use is as follows. For $\Delta > 0$, we define

$$H(\Delta) = \sum_{\substack{[f] \\ \Delta_f = -\Delta}} c_f$$

where

$$c_f = \begin{cases} \frac{1}{2} & \text{if } f \text{ is proportional to } x^2 + y^2, \\ \frac{1}{3} & \text{if } f \text{ is proportional to } x^2 + xy + y^2, \\ 1 & \text{otherwise.} \end{cases}$$

Since among forms of discriminant Δ there cannot be forms proportional to x^2+y^2 and forms proportional to x^2+xy+y^2, we cannot have both a $1/2$ and a $1/3$ show up in the sum above. Consider the form $f = ax^2+bxy+cy^2$. f is proportional to x^2+y^2[resp. x^2+xy+y^2] means there exists $\alpha \in \mathbb{Z}$[resp. $\beta \in \mathbb{Z}$] such that $f = \alpha(x^2+y^2)$[resp. $f = \beta(x^2+xy+y^2)$]. The discriminants of these forms are $\Delta_f = b^2 - 4ac$, $\Delta_{\alpha(x^2+y^2)} = -4\alpha^2$, and $\Delta_{\beta(x^2+xy+y^2)} = -3\beta^2$. Since $4\alpha^2 \neq 3\beta^2$ for any $\alpha, \beta \in \mathbb{Z}$, the sum above has one summand which differs from one. Therefore, $H(\Delta) = K(\Delta) + \mathrm{O}(1)$. In [?] David and Pappalardi state the following well-known formula for the Hurwitz class number. Let $D > 0$ be the discriminant of a quadratic imaginary order then

$$H(D) = 2 \sum_{\substack{k^2 \mid D \\ \frac{D}{k^2} \equiv 0,1 \pmod 4}} \frac{h(D/k^2)}{w(D/k^2)},$$

where $h(d)$ and $w(d)$ denote respectively the Dirichlet class number and the number of units of the order of discriminant d. For $p > 3$ and $f \geq 1$ any elliptic curve over $\mathbb{F}_{p^f}$ may be written as

$$E_{a,b} : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_{p^f}$. According to [?, Lenstra] the elliptic curves $E_{a',b'}$ over $\mathbb{F}_{p^f}$ which are $\mathbb{F}_{p^f}$-isomorphic to $E_{a,b}$ are given by all choices

$$a' = u^4 a \text{ and } b' = u^6 b$$

with $u \in \mathbb{F}_{p^f}^*$. The number of such $E_{a',b'}$ 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 [?] 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 [?] or [?, Theorem 4.6]) if $r^2 - 4p^f < 0$ and $p \nmid r$, then

$$N(r) = K(r^2 - 4p^f).$$

Therefore,

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

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 using Deuring's theorem we have

Theorem 3.1.

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

Proof.
Let $\tilde{E}$ denote an $\mathbb{F}_{p^f}$-isomorphism class. Then

$$T_{p^f}(r) = \sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r}} \sum_{\substack{A,B \\ E_{A,B}\in\tilde{E}}} 1$$

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

Since there are at most 10 classes with size different from $\frac{p^f-1}{2}$ we have

$$T_{p^f}(r) = \sum_{\substack{\tilde{E}/\mathbb{F}_{p^f} \\ a_{\mathfrak{p}}(\tilde{E})=r}} \frac{p^f-1}{2} + \mathrm{O}\left(p^f\right)$$

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

Using the class number formula

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

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

$$H(4p^f - r^2) = 2 \sum_{k^2|4p^f-r^2} \frac{h((r^2-4p^f)/k^2)}{w((r^2-4p^f)/k^2)}$$

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

$$\ll \sum_{k^2|4p^f-r^2} \frac{p^{f/2}}{k} \log p$$

$$\ll p^{f/2} \log^2 p.$$

The result follows.

$\square$

Proof of Lemma 0.7.
We begin by writing $\pi_E^{r,f}(x)$ as a sum.

$$\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x) = \frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{N(\mathfrak{p})\le x\\ \deg_K\mathfrak{p}=f\\ a_\mathfrak{p}(E)=r}} 1$$

Using $N(\mathfrak{p}) = p^f$ we rewrite the inner sum as a sum on p. There are $g = n/f$ primes in $\mathcal{O}_K$ which lie above each rational prime p. Therefore

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

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 set $B(r) = \max\{(r^2/4)^{1/f}, r, 3\}$ for several reasons. First, to ensure that $|r| \le 2\sqrt{N(\mathfrak{p})}$, which is a necessary condition in Hasse's theorem. Secondly, we need $r < p$ to ensure that $p \nmid r$ (for Deuring's theorem). Recall that an elliptic curve defined over a field K has Weierstrass equation $y^2 = x^3 + ax + b$ if the characteristic of K is not 2 or 3. Hence, we require $p > 3$.
Reversing summation we have

$$\begin{aligned}
&\frac{n}{f|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f\\ a_\mathfrak{p}(E)=r}} 1 + \mathrm{O}(1)\\
&= \frac{n}{f|\mathcal{C}_t|}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\ \sum_{\substack{E\in\mathcal{C}_t\\ a_\mathfrak{p}(E)=r}} 1 + \mathrm{O}(1)
\end{aligned}\tag{5}$$

Given a rational prime p let $\mathfrak{p}$ be any prime of $\mathcal{O}_K$ lying above p. Then the inner most sum of (5) becomes

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

We estimate the O-term as follows

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

$$\ll \sum_{A\in\mathcal{O}_K/\mathfrak{p}} \frac{(2t)^{2n}}{p^{2f}}$$

$$\ll \frac{t^{2n}}{p^f}.$$

Recall from the previous section that given $E/\mathbb{F}_{p^f}$,

$$|\mathcal{C}_t(E)| = \left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right). \tag{6}$$

Therefore, the main term is

$$\sum_{\substack{E_{A,B}/\mathbb{F}_{p^f}\\ \#E_{A,B}(\mathbb{F}_{p^f})=p^f+1-r}} |\mathcal{C}_t(E_{A,B})| = T_{p^f}(r)\left[\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right]$$

Applying Theorem 3.1 we have

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

$$= \left(H(4p^f-r^2)\frac{p^f}{2} + \mathrm{O}(p^f)\right)\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right) + \mathrm{O}\left(\frac{t^{2n}}{p^f}\right)$$

Recall (3)

$$\frac{1}{|\mathcal{C}_t|} = \left(\frac{1}{4^n t^{2n}} + \mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right)$$

then

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

$$= \frac{n}{f}\left(\frac{1}{4^n t^{2n}} + \mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right) \sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=n/f}} \left[\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right) + \mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}} + \frac{t^{2n}}{p^{10f}}\right)\right)\cdot\right.$$

$$\left.\left(\frac{p^f}{2}H(4p^f-r^2) + \mathrm{O}(p^f)\right) + \mathrm{O}\left(\frac{t^{2n}}{p^f}\right)\right] + \mathrm{O}(1)$$

Rearranging we may write

$$\tag{7} \begin{aligned} &\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)\\ &=\frac{n}{f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\left[\left(\frac{1}{4^nt^{2n}}+\mathrm{O}\left(\frac{1}{t^{2n+1}}\right)\right)\left(\left(\frac{(2t)^{2n}}{p^{2f}}\right)+\mathrm{O}\left(\frac{t^{2n-1}}{p^{2f-1}}+\frac{t^{2n}}{p^{10f}}\right)\right)\cdot\right.\\ &\qquad\left.\left(\frac{p^f}{2}H(4p^f-r^2)+\mathrm{O}(p^f)\right)\right]+\mathrm{O}\left(\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\frac{1}{p^f}\right)+\mathrm{O}(1) \end{aligned}$$

Recall $H(4p^f-r^2)\ll p^{f/2}\log^2 p$ (see 17). Therefore, the expression within the brackets in (7) becomes

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

Substituting into (7) we have

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

Write

$$\tag{8} \frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)=\frac{n}{2f}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=n/f}}\frac{H(4p^f-r^2)}{p^f}+E(x,t).$$

First we deal with the O-term in (8). For $f = 1$ we use the estimates

$$\sum_{p<x} \frac{1}{p} \ll \log\log x,$$

$$\sum_{p<x} \frac{\sqrt{p}\log^2 p}{t} \ll \frac{x}{t\log x}\sqrt{x}\log^2 x = \frac{x^{3/2}\log x}{t}.$$

For $f = 2$ we use

$$\sum_{p<\sqrt{x}} \frac{\log^2 p}{t} \ll \frac{\sqrt{x}}{\log\sqrt{x}}\frac{\log^2\sqrt{x}}{t} \ll \frac{\sqrt{x}\log x}{t}.$$

For $f = 3$ we recall the partial summation formula. Let $\{a_n\}$ be a sequence of complex numbers. Set

$$A(y) = \sum_{n\leq y} a_n \qquad (y > 0).$$

Let $f(y)$ be a continously differentiable function on the interval $[m, X]$. Then we have

$$\sum_{m\leq n\leq X} a_n f(n) = A(X)f(X) - \int_1^X A(y)f'(y)\ \mathrm{dy} - A(m-1)f(m)$$

where $A(-1) = 0$. A proof of the partial summation formula follows directly from Murty's proof found in [**?**, Theorem 2.2].
Suppose $f = 3$. Set $f(y) = y^{-1/2}$ and set

$$a_n = \begin{cases} \log^2 n & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Then partial summation gives

$$\sum_{p<x^{1/3}} \frac{\log^2 p}{tp^{1/2}} \ll \frac{x^{1/6}\log x}{t}.$$

Suppose $f = 4$. Then using $\sum_{p<x}\frac{1}{p} \ll \log\log x$ we have

$$\sum_{p<x^{1/4}} \frac{\log^2 p}{tp} \ll \frac{\log^2 x}{t}\sum_{p<x}\frac{1}{p} \ll \frac{\log^2 x\log\log x}{t}.$$

For $f \geq 5$ use

$$\sum_{p<x^{1/f}} \frac{\log^2 p}{tp^{f/2-1}} \ll \frac{\log^2 x}{t}\sum_{p<x^{1/f}}\frac{1}{p^{3/2}} \ll \frac{\log^2 x}{t}\sum_{n=1}^{x^{1/f}}\frac{1}{n^{3/2}} \ll \frac{\log^2 x}{t}$$

Therefore, we have

$$E(x,t) \ll \begin{cases} 1+\frac{\log^2 x}{t} & \text{for } f \geq 5 \\ 1+\frac{\log^2 x \log\log x}{t} & \text{for } f = 4 \\ 1+\frac{x^{1/6}\log x}{t} & \text{for } f = 3 \\ 1+\frac{\sqrt{x}\log x}{t} & \text{for } f = 2 \\ \log\log x + \frac{x^{3/2}\log x}{t} & \text{for } f = 1. \end{cases} \tag{9}$$

Now we deal with the main term in (8). Let $d_k(p) = \frac{r^2-4p^f}{k^2}$. From the formula for the Hurwitz class number

$$H(4p^f - r^2) = \sum_{k^2 | 4p^f - r^2} \frac{h(d_k(p))}{w(d_k(p))}$$

and by the class number formula

$$h(d_k(p)) = \frac{w(d_k(p))|d_k(p)|^{1/2}}{2\pi} L(1, \chi_{d_k(p)})$$

we have

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

Switching the order of summation and noticing that we need only consider $k \leq 2x^{f/2}$, we have

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

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

Approximate $\sqrt{4p^f - r^2}$ by $2\sqrt{p^f} + \mathrm{O}\left(\frac{1}{p^{f/2}}\right)$ and use the fact that $L(1, \chi_{d_k(p)}) \ll \log p$ (see [**?**, pg. 656]) to obtain

$$\frac{n}{\pi f} \sum_{k \leq 2x^{f/2}} \frac{1}{k} \left[\sum_{\substack{B(r)<p\leq x^{1/f} \\ k^2 | r^2 - 4p^f \\ g(p)=n/f}} \frac{L(1, \chi_{d_k(p)})}{p^{f/2}} + \mathrm{O}\left(\sum_{\substack{B(r)<p\leq x^{1/f} \\ k^2 | r^2 - 4p^f \\ g(p)=n/f}} \frac{\log p}{p^{3f/2}} \right) \right] \tag{10}$$

for the O-term we use the fact that for any integer m

$$\sum_{k|m} 1 \ll m^{\epsilon} \qquad \text{for all } \epsilon > 0$$

(see [**?**, Exercise 1.3.2]) to see that

$$\sum_{k\le 2x^{f/2}} \frac{1}{k} \sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}} \frac{\log p}{p^{3f/2}} \ll \sum_{p\le x^{1/f}} \left(\sum_{k^2|r^2-4p^f} \frac{1}{k}\right) \frac{\log p}{p^{3f/2}} \ll \sum_{p\le x^{1/f}} \frac{p^{\epsilon}\log p}{p^{3f/2}} \ll 1$$

Set $f(y) = (y^{f/2}\log y)^{-1}$ and set

$$a_n = \begin{cases} L(1,\chi_{d_k(p)})\log p & \text{if } n \text{ is prime and } n > B(r),\\ 0 & \text{otherwise.}\end{cases}$$

Using partial summation (see pg. 21) the main term in (10) becomes

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

Set $s = S^{1/f}$ and note that $k^2|4p^f - r^2$ implies $k < 2S^{f/2}$ to obtain

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

since

$$\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{f}{S^{1/2}\log S}\right)\,\mathrm{dS} = \frac{\mathrm{d}}{\mathrm{ds}}\left(\frac{1}{s^{f/2}\log s}\right)\,\mathrm{ds}.$$

Therefore,

$$\begin{aligned}
&\frac{1}{|\mathcal{C}_t|}\sum_{E\in\mathcal{C}_t}\pi_E^{r,f}(x)\\
&=\frac{n}{\pi}\Bigg[\frac{1}{\sqrt{x}\log x}\sum_{k\le 2x^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}} L(1,\chi_{d_k(p)})\log p\\
&\quad-\int_{B(r)^f}^{x}\sum_{k\le 2S^{f/2}}\frac{1}{k}\sum_{\substack{B(r)<p\le S^{1/f}\\ k^2|r^2-4p^f\\ g(p)=n/f}} L(1,\chi_{d_k(p)})\log p\frac{\mathrm{d}}{\mathrm{dS}}\left(\frac{1}{S^{1/2}\log S}\right)\,\mathrm{ds}\Bigg]+E(x,t)
\end{aligned}$$

□

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

Recall that in the statement of Lemma 0.8 (1) we defined

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

where

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

In section 5 we require an upper bound on

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

in order to prove Lemma 0.8. In this section we provide a formula for $C_r(a,n,k)$ which will provide the requisite upper bound. The lemma proved in this section will also enable us to construct a multiplicative function in section 6 which will in turn allow us to prove a product formula for $C_{r,A,B}$ in section 7. For the main result in this section we require the following lemma.

Lemma 4.1. *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.

Proof. It is easy to check the $L=2$ case. We proceed by induction on L. To that end assume $X=MA+M^2 2^k \pmod{2^{L-1}}$ has a unique solution $M_0 \pmod{2^{L-1}}$ for $L\ge 3$. Given $A\equiv 1 \pmod 2$ and $1\le k\le L-1$ ($k\ge L$ is obvious) consider $X\equiv MA+M^2 2^k \pmod{2^L}$. By our assumption there exists a unique M such that $X=MA+M^2 2^k \pmod{2^{L-1}}$, say $M=M_0$.

We write $X - M_0A - M_0^2 2^k = 2^{L-1}N$ for some $N \in \mathbb{Z}$. Set $M_1 = M_0 + 2^{L-1}Q$, where $Q \in \mathbb{Z}$. Then

$$\begin{aligned}
&X \equiv M_1A + 2^k M_1^2 \pmod{2^L} \\
\Leftrightarrow\ & 2^{L-1}N = X - M_0A - 2^k M_0^2 \equiv 2^{L-1}[AQ + QM_0 2^{k+1} + Q^2 2^{k+L-1}] \pmod{2^L} \\
\Leftrightarrow\ & N \equiv AQ + QM_0 2^{k+1} + Q^2 2^{k+L-1} \pmod{2} \\
\Leftrightarrow\ & N \equiv AQ + QM_0 2^{k+1} \pmod{2} \\
\Leftrightarrow\ & N \equiv Q \pmod{2}
\end{aligned}$$

Therefore, choosing $Q \equiv N \pmod{2}$ M_1 is the unique solution to $X \equiv MA + M^2 2^k \pmod{2^L}$
$\square$

Let $p \in \mathbb{Z}$ be any prime. In order to compute $C_r(a, n, k)$, we note that by the Chinese Remainder Theorem

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

where

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

with $l = \mathrm{ord}_p(4Bnk^2),\ l_1 = \mathrm{ord}_p(B),\ l_2 = \mathrm{ord}_p(4nk^2)$.
Note that $l = l_1 + l_2$ and $ord_2(4nk^2) \geq 2$.

Lemma 4.2. *Let p be an odd prime. Using the notation above we have*

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

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

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

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

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

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

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

$$d_2(n) = \begin{cases} 2^{\min(l_1+4, l-1)} & \text{if } r^2 - ak^2 \equiv 4 \pmod{2^{\min(5, l_2)}} \\ 0 & \text{if } r^2 - ak^2 \not\equiv 4 \pmod{2^{\min(5, l_2)}} \end{cases}$$

(5) *If $l_1 \geq 2$ and $2 \leq l_2 \leq l_1 + 3$, then*

$$d_2(n) = \begin{cases} 2^{l-l_1} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{2^{l-l_1}} \\ 0 & \text{if } 4A^2 \not\equiv r^2 - ak^2 \pmod{2^{l-l_1}} \end{cases}$$

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

$$d_2(n) = \begin{cases} 2^{l_1+3} & \text{if } 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}} \\ 0 & \text{if } 4A^2 \not\equiv r^2 - ak^2 \pmod{2^{l_1+3}} \end{cases}$$

Proof.
(1) It is easy to see that if $l_2 = 0$ and $l_1 > 0$, then $d_p(n) = 1$. So suppose $0 < l_2 \leq l_1$ and p is any odd prime. Then

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

Since $\#\{b \in (\mathbb{Z}/p^l\mathbb{Z})^* : b \equiv A \pmod{p^{l_1}}\} = p^{l-l_1}$, the result follows.
(2) If $l_1 = 0$, then $d_p(n)$ becomes

$$d_p(n) = \sum_{\substack{b \in (\mathbb{Z}/p^l\mathbb{Z})^* \\ 4b^2 \equiv r^2 - ak^2 \pmod{p^l}}} 1.$$

If $p|(r^2 - ak^2)$, then there are no solutions in $(\mathbb{Z}/p^l\mathbb{Z})^*$ to $4b^2 \equiv r^2 - ak^2 \pmod{p}$. If $(r^2 - ak^2, p) = 1$, then there are two or zero solutions to $4b^2 \equiv r^2 - ak^2 \pmod{p^l}$. If $r^2 - ak^2$ is a square modulo p then there are two solutions modulo p which lift to two solutions modulo p^l. On the other hand, if $r^2 - ak^2$ is not a square modulo p, then there are no solutions modulo p, hence there are no solutions modulo p^l.
(3) Suppose $l_2 > l_1 \geq 1$ and p is odd. If $b = A$ is a solution to $4b^2 \equiv r^2 - ak^2 \pmod{p^{l_1}}$, then $b \equiv A \pmod{p^{l_1}}$ lifts uniquely to a solution modulo p^{l_2}. Since $\#\{b \in (\mathbb{Z}/p^l\mathbb{Z})^* : b \equiv A \pmod{p^{l_2}}\} = p^{l-l_2}$, the result follows.
(4) Suppose $l_1 = 0$. Then

$$d_2(n) = \sum_{\substack{b \in (\mathbb{Z}/2^{l_2})^* \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}}} 1.$$

The cases $l_2 = 2, 3$ and 4 may be checked directly. For $l_2 \geq 5$ the number of solutions to $b^2 \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2 - 2}}$ are 4 if $\frac{r^2 - ak^2}{4} \equiv 1 \pmod{8}$ and 0 otherwise (see [?, pg. 98]). These four solutions lift to 16 solutions modulo 2^{l_2}.
Suppose $l_1 = 1$. Since B is even and $(A, B) = 1$ we see that A is odd. Thus,

$$d_p(n) = \sum_{\substack{b \in (\mathbb{Z}/2^{l_2+1})^* \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}}} 1.$$

The cases $l_2 = 2, 3$ and 4 may be checked directly. For $l_2 \geq 5$ the number of solutions to $b^2 \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2 - 2}}$ are 4 if $\frac{r^2 - ak^2}{4} \equiv 1 \pmod{8}$ and 0 otherwise (see [?, pg. 98]). These four solutions lift to 32 solutions modulo 2^{l_2+1}.

(5) Suppose $l_1 \geq 2$ and $2 \leq l_2 \leq l_1 + 3$. Observe

$$\begin{aligned}
&\exists\, b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases} \\
&\Leftrightarrow \exists\, M \quad \text{such that} \quad 4(A + M2^{l_1})^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \\
&\Leftrightarrow 4(A^2 + 2^{l_1+1}MA + M^2 2^{2l_1}) \equiv r^2 - ak^2 \pmod{2^{l_2}} \\
&\Leftrightarrow 4A^2 + 2^{l_1+3}MA + M^2 2^{2l_1+2} \equiv r^2 - ak^2 \pmod{2^{l_2}} \\
&\Leftrightarrow 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}.
\end{aligned}$$

The result follows from the fact that there are 2^{l-l_1} $b \in (\mathbb{Z}/p^l\mathbb{Z})^*$ such that $b \equiv A \pmod{2^{l_1}}$.
(6) We consider three cases.
Case 1: Suppose $l_1 \geq 2$ and $l_2 = l_1 + 4$. Then

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

We require

$$\left(\frac{\frac{r^2-ak^2}{4} - A^2}{2^{l_1+1}}\right)$$

to be an integer. This requirement may be written as $4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}}$. Under this condition we have a unique M modulo 2 which gives a solution b modulo 2^{l_1+2}. Note if b satisfies $4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}}$, then so do $-b$, $b + 2^{l_1+1}$, and $-b + 2^{l_1+1}$. But only two of these four satisfy $b \equiv A \pmod{2^{l_1}}$. Therefore, the number of solutions is $2 \cdot 2^{l-(l_1+2)}$.

Case 2: Suppose $l_1 \geq 2$ and $l_2 = l_1 + 5$. Then

$$\exists\, b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases}$$

$$\Leftrightarrow \exists\, M \quad \text{such that} \quad (A + M2^{l_1})^2 \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2 - 2}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow A^2 + 2^{l_1+1}MA + M^2 2^{2l_1} \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_1+3}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow \frac{r^2 - ak^2}{4} - A^2 \equiv 2^{l_1+1}MA + M^2 2^{2l_1} \pmod{2^{l_1+3}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow \frac{1}{2^{l_1+1}}\left[\frac{r^2 - ak^2}{4} - A^2\right] \equiv MA + M^2 2^{l_1 - 1} \pmod{4} \text{ and } 2^{l_1+1} | \left(\frac{r^2 - ak^2}{4} - A^2\right)$$

$$\Leftrightarrow \left(\frac{\frac{r^2 - ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv_4 \begin{cases} AM & \text{if } l_1 \geq 3 \\ AM + 2M^2 & \text{if } l_1 = 2 \end{cases}$$

We require $r^2 - ak^2 \equiv 4A^2 \pmod{2^{l_1+3}}$ so that the left hand side of the above equation is an integer. If $l_1 = 2$ we use Lemma 4.1 and see that we can find a *unique* M modulo 4 which satisfies

$$\left(\frac{\frac{r^2 - ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv AM + 2M^2 \pmod{4}$$

which gives a unique b modulo 2^5. Note if b satisfies $b \equiv A \pmod{2^2}$ and $4b^2 \equiv r^2 - ak^2 \pmod{2^7}$, then so does $b + 2^4$. Therefore the number of solutions is $2 \cdot 2^{9-5} = 32$

If $l_1 \geq 3$, then it is easy to see that we have a unique M modulo 4 such that to

$$\left(\frac{\frac{r^2 - ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv AM \pmod{4}.$$

which gives a unique b modulo 2^{l_1+3}. Note that if b satisfies $4b^2 \equiv r^2 - ak^2 \pmod{2^{l_1+5}}$, then so do $-b$, $b + 2^{l_1+2}$, and $-b + 2^{l_1+2}$. But, only two of these satisfy $b \equiv A \pmod{2^{l_1}}$. Thus, the number of solutions is $2 \cdot 2^{l-(l_1+3)} = 2^{l_1+3}$.

Case 3: Suppose $l_1 \geq 2$ and $l_2 \geq l_1 + 6$. Then

$$\exists\, b \quad \text{such that} \quad \begin{cases} b \equiv A \pmod{2^{l_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{l_2}} \end{cases}$$

$$\Leftrightarrow \exists\, M \quad \text{such that} \quad (A + M2^{l_1})^2 \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2 - 2}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow A^2 + 2^{l_1+1}MA + M^2 2^{2l_1} \equiv \frac{r^2 - ak^2}{4} \pmod{2^{l_2-2}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

$$\Leftrightarrow \frac{r^2 - ak^2}{4} - A^2 \equiv 2^{l_1+1}MA + M^2 2^{2l_1} \pmod{2^{l_2-2}} \text{ and } \frac{r^2 - ak^2}{4} \in \mathbb{Z}$$

(11)

$$\Leftrightarrow \left(\frac{\frac{r^2 - ak^2}{4} - A^2}{2^{l_1+1}}\right) \equiv MA + M^2 2^{l_1 - 1} \pmod{2^{l_2 - l_1 - 3}} \text{ and } 2^{l_1+1} | \left(\frac{r^2 - ak^2}{4} - A^2\right).$$

In order for the left hand side of (11) to be an integer, we must have

$$r^2 - ak^2 \equiv 4A^2 \pmod{2^{l_1+3}}. \tag{12}$$

By Lemma 4.1, (12) is a sufficient condition for determining a unique solution M modulo $2^{l_2-l_1-3}$ for (11). 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 $2^{l-l_2+2} \cdot 2$

$\square$

5. Averaging Special Values of L-Series

In this section we prove Lemma 0.8 (2). For a proof of Lemma 0.8 (1) see [**?**, Proposition 2.1]. In [**?**] David and Pappalardi present a proof of Lemma 0.8 for $A = 3$ and $B = 4$. We let A and B be any coprime positive integers and consider primes up to $\sqrt{x}$. In the proof that follows we use arguments similar to those of David and Pappalardi (see [**?**, proof of Lemma 2.2]).

Proof of Lemma 0.8 (1).
Throughout this section we will be concerned with the double sum

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

Let U be a parameter to be determined. We have the following identity (see [**?**, (4.2)])

$$L(1,\chi_{d_k(p)}) := \sum_{n\in\mathbb{N}}\left(\frac{d_k(p)}{n}\right)\frac{1}{n} = \sum_{n\in\mathbb{N}}\left(\frac{d_k(p)}{n}\right)\frac{e^{-n/U}}{n} + \mathrm{O}\left(\frac{|d_k(p)|^{7/32}}{U^{1/2}}\right). \tag{13}$$

Before using the identity above we make two observations:

(1) Since $d_k(p)=\frac{r^2-4p^2}{k^2}$,

$$|d_k(p)|^{7/32} \ll \left(\frac{p}{k}\right)^{7/16} \Rightarrow \frac{|d_k(p)|^{7/32}}{U^{1/2}} \ll \frac{p^{7/16}}{k^{7/16}U^{1/2}}.$$

(2)

$$\sum_{\substack{k\le 2x\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} \frac{p^{7/16}\log p}{k^{7/16}U^{1/2}} \ll \frac{1}{U^{1/2}}\sum_{p\le\sqrt{x}} p^{7/16}\log p$$

$$\ll \frac{1}{U^{1/2}}\sqrt{x^{7/16}}\log x\frac{\sqrt{x}}{\log x}$$

$$\ll \frac{x^{23/32}}{U^{1/2}}.$$

Therefore, substituting the identity (13) and choosing

$$U > x^{7/16}\log^{2c} x$$

we obtain

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

Throughout the next several pages we continue to make estimates involved with the double sum above. Since we have incurred an error of $\sqrt{x}/\log^c x$ we will choose any free parameters wisely so that our main term is bigger than $\sqrt{x}/\log^c x$. Next we show that we may neglect the larger values of k. Let V be a parameter to be determined. Note that

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

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

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

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 use the Chinese Remainder Theorem to solve

$$X=\begin{cases} x_1 & \pmod{p_1^{a_1}}\\ \vdots & \\ x_t & \pmod{p_t^{a_t}}.\end{cases}$$

Thus, $4X^2\equiv r^2 \pmod{k^2}$ 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,

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

$$\ll \sqrt{x}\log x\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}\sum_{V\le k\le 2x}\frac{2^{\nu(k)}}{k^3} \tag{14}$$

To estimate $\sum_{V\le k\le 2x}\frac{2^{\nu(k)}}{k^3}$ we use [**?**, Exercise 2, pg 53], which states

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

along with the partial summation formula (see pg. 21). Setting $a_n=2^{\nu(n)}$, $f(y)=\frac{1}{y^3}$ partial summation gives

$$\begin{aligned}\sum_{k=V}^{2x}\frac{2^{\nu(k)}}{k^3} &= \left(\frac{6}{\pi^2}2x\log(2x)+\mathrm{O}(2x)\right)\frac{1}{(2x)^3}+\int_V^{2x}\left(\frac{6}{\pi^2}y\log y+\mathrm{O}(y)\right)\frac{3}{y^2}\,\mathrm{dy}\\ &\quad -\left(\frac{6}{\pi^2}(V-1)\log(V-1)+\mathrm{O}(V-1)\right)\frac{1}{V^3}\ll\frac{\log V}{V^2}.\end{aligned} \tag{15}$$

To estimate the sum $\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n}$ we first use the Maclaurin series for e^z and the Alternating Series Estimation Theorem to see that

$$\begin{aligned}
1 - e^{-1/U} &= 1 - \sum_{i=0}^{\infty} \frac{(-1)^i}{U^i i!} \\
&= \frac{1}{U} - \sum_{i=2}^{\infty} \frac{(-1)^i}{U^i i!} \\
&= \frac{1}{U} - \frac{1}{2U^2} + \frac{1}{6U^3} - \frac{1}{24U^4} + \cdots \\
&> \frac{1}{U} - \frac{1}{2U^2}.
\end{aligned}$$

Then using the Maclaurin Series for $-\log(1-z)$ we write

$$\begin{aligned}
\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} &= -\log(1 - e^{-1/U}) \\
&\le -\log\left(\frac{1}{U} - \frac{1}{2U^2}\right) \\
&= -\log\left(\frac{1}{U}\left(1 - \frac{1}{2U}\right)\right) \\
&= \log U - \log\left(\frac{2U-1}{2U}\right) \\
&= \log U + \log\left(\frac{2U}{2U-1}\right) \\
&\le \log U + \log(2) \qquad \text{for } U > 1
\end{aligned} \tag{16}$$

Choose

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

and use (15) and (16), to see that (14) becomes

$$\begin{aligned}
\sqrt{x}\log x \sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{V\le k\le 2x} \frac{2^{\nu(k)}}{k^3} &\ll \sqrt{x}\log x(\log U)\left(\frac{\log V}{V^2}\right) \\
&\ll \sqrt{x}\log x(\log U)\left(\frac{1}{V^{2-\epsilon_1}}\right) \\
&\ll \sqrt{x}\log x(\log U)\left(\frac{1}{(\log x)^{c+3-\epsilon_2}}\right) \\
&\ll \frac{\sqrt{x}}{(\log x)^{c+2-\epsilon_2}}(\log U) \\
&\ll \frac{\sqrt{x}}{(\log x)^{c+1-\epsilon_2}} \\
&\ll \frac{\sqrt{x}}{\log^c x}
\end{aligned}$$

if $U \ll \sqrt{x}/\log x$. Note that requiring this upper bound on U will not be a problem since we will soon choose U to be a function of x which is $\ll \sqrt{x}/\log x$. We have shown that

$$
\begin{aligned}
&\sum_{\substack{k\le 2x\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p \\
&= \sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)
\end{aligned}
\tag{17}
$$

Now we concentrate of large values of n. Note that

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

and recall that U has been chosen so that

$$
U > x^{7/16}\log^{2c} x.
$$

Therefore,

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

Substituting this into (17) we obtain

$$
\begin{aligned}
&\sum_{\substack{k\le 2x\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p \\
&= \sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{n< U\log U} \frac{e^{-n/U}}{n} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).
\end{aligned}
\tag{18}
$$

For the inner sum

$$
\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p
$$

note that $\left(\frac{d_k(p)}{\bullet}\right)$ is periodic modulo $4n$. That is,

$$
d_1 \equiv d_2 \pmod{4n} \Rightarrow \left(\frac{d_1}{n}\right) = \left(\frac{d_2}{n}\right) \qquad \text{for all } n\in\mathbb{N}
$$

Thus

$$\sum_{\substack{B(r)<p\leq\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p$$

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

For positive coprime integers C and D define

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

Then

$$\sum_{\substack{B(r)<p\leq\sqrt{x}\\ p\equiv A \pmod B\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p$$

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

where the O-term comes from the following estimates.

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

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

$$\ll \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{2^{\nu(nk)}}{4Bnk^2}$$

$$\ll \frac{2^{\nu(nk)}}{Bk^2}\cdot\frac{\phi(4n)}{4n}$$

$$\ll \frac{2^{\nu(nk)}}{Bk^2}.$$

Since $\psi_1(X,C,D)\sim\frac{X}{\phi(C)}$ (see [**?**, Chapter 2 §8.2 Theorem 5]) we define

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

Therefore,

$$\sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} \left(\frac{d_k(p)}{n}\right)\log p$$

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

$$+\mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)$$

$$=\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}$$

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

where as before

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

If we interchange the sum on $a\in(\mathbb{Z}/4n\mathbb{Z})^*$ with the sum on $b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*$, then for a fixed b there is at most one value of $a\in(\mathbb{Z}/4n\mathbb{Z})^*$ such that $4b^2\equiv r^2-ak^2 \pmod{4nk^2}$. Therefore,

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

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

$$\le\sum_{\substack{b\in\left(\mathbb{Z}/4Bnk^2\mathbb{Z}\right)^*\\ b\equiv A \pmod{B}}}\left|E_1(\sqrt{x},4Bnk^2,b)\cdot 1\right|$$

$$\le\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\left|E_1(\sqrt{x},4Bnk^2,b)\right|.$$

Hence,

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

Therefore, we may write (18) on page 33 as

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

$$(19)\qquad = \sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n<U\log U}\frac{e^{-n/U}}{n}\Bigg[\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}$$
$$+\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\left|E_1(\sqrt{x},4Bnk^2,b)\right|+\mathrm{O}\left(\frac{2^{\nu(nk)}}{Bk^2}\right)\Bigg]+\mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

For the O-term inside the brackets note that for any $\epsilon>0$

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

(see pg. 22). With this fact we have for any $\epsilon>0$

$$\begin{aligned}\sum_{\substack{k\le V\\(k,2r)=1}}\sum_{n<U\log U}\frac{e^{-n/U}2^{\nu(nk)}}{nk^3}&\ll\sum_{k\le V}\frac{k^\epsilon}{k^3}\sum_{n<U\log U}\frac{e^{-n/U}n^\epsilon}{n}\\&\ll\sum_{k\le V}\frac{1}{k^{3-\epsilon}}\sum_{n<U\log U}\mathrm{O}(1)\\&\ll U\log U\end{aligned}$$

and

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

when

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

Therefore, (19) becomes

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

$$= \sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{n<U\log U} \frac{e^{-n/U}}{n}\left[\sqrt{x}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}\right. \tag{20}$$
$$\left. + \sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\left|E_1(\sqrt{x},4Bnk^2,b)\right|\right] + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).$$

Recall the Cauchy-Schwarz inequality. For two real valued sequences $\{a_n\}$ and $\{b_n\}$,

$$\sum_n a_nb_n \le \left(\sum_n a_n^2\right)^{1/2}\left(\sum_n b_n^2\right)^{1/2}.$$

We apply the Cauchy-Schwarz inequality to the middle term of (20) and obtain

$$\sum_{\substack{k\le V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\le U\log U\\ b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}} \frac{e^{-n/U}}{n}|E_1(\sqrt{x},4Bnk^2,b)| \tag{21}$$
$$\le \sum_{k\le V}\frac{1}{k}\left(\sum_{n\le U\log U}\frac{\phi(4Bnk^2)}{n^2}\right)^{1/2}\left(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}E_1(\sqrt{x},4Bnk^2,b)^2\right)^{1/2}$$

Using the identity $\phi(AB)=\phi(A)\phi(B)\frac{(A,B)}{\phi((A,B))}$ we can write,

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

Note that $\phi(4n) \leq 4\phi(n)$, $\phi(k^2) = k\phi(k)$, $\phi(n) \leq n$, and

$$\frac{(4Bn, k^2)}{\phi((4Bn, k^2))} = \prod_{p|(4Bn,k^2)} \frac{p}{p-1} \leq \prod_{p|(4Bn,k^2)} 2 = 2^{\nu((4Bn,k^2))} \leq 2^{\nu(k)}.$$

Similiarly,

$$\frac{(4n, B)}{\phi((4n, B))} \leq 2^{\nu(B)}.$$

Recall that for any $\epsilon > 0$, $2^{\nu(m)} \leq m^\epsilon$ (see pg. 22). Therefore,

$$\begin{aligned}
&\sum_{k\leq V} \frac{1}{k} \left(\sum_{n\leq U\log U} \frac{\phi(4Bnk^2)}{n^2} \right)^{1/2} \left(\sum_{n\leq U\log U} \sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*} E_1(\sqrt{x}, 4Bnk^2, b)^2 \right)^{1/2} \\
&\ll \sum_{k\leq V} \sqrt{2^{\nu(k)}2^{\nu(B)}} \left(\sum_{n\leq U\log U} \frac{1}{n} \right)^{1/2} \left(\sum_{n\leq U\log U} \sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*} E_1(\sqrt{x}, 4Bnk^2, b)^2 \right)^{1/2} \\
&\ll \sum_{k\leq V} \sqrt{k^\epsilon} (\log U)^{1/2} \left(\sum_{n\leq U\log U} \sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*} E_1(\sqrt{x}, 4Bnk^2, b)^2 \right)^{1/2}
\end{aligned}$$

Substituting $m = 4Bnk^2$ (21) may be written as

$$\begin{aligned}
&\sum_{\substack{k\leq V \\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{n\leq U\log U \\ b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}} \frac{e^{-n/U}}{n} |E_1(\sqrt{x}, 4Bnk^2, b)| \\
&\ll \sqrt{\log U} \sum_{k\leq V} \sqrt{k^\epsilon} \left(\sum_{m\leq 4BV^2U\log U} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} E_1(\sqrt{x}, m, b)^2 \right)^{1/2}
\end{aligned}$$

The Barban, Davenport, Halberstam Theorem asserts that given any $l > 0$ we have for $X > Q > X/\log^l X$

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

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

$$\begin{aligned}
&\sqrt{\log U} \sum_{k\leq V} \sqrt{kB} \left(\sum_{m\leq 4BV^2U\log U} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} E_1(\sqrt{x}, m, b)^2 \right)^{1/2} \\
&\ll \sqrt{\log U} \sum_{k\leq V} \sqrt{kB} \left(4BV^2U\log U\sqrt{x}\log x \right)^{1/2} \\
&\ll (\log U)V^3\sqrt{U}\sqrt{\sqrt{x}\log x} \\
&\ll \frac{\sqrt{x}}{\log^c x}
\end{aligned}$$

when

$$U = \frac{\sqrt{x}}{\log^{5c+15} x}, \quad V = \log^{(c+3)/2} x. \tag{22}$$

We have shown that (19) on page 36 becomes

$$\begin{aligned} &\sum_{\substack{k \le 2x \\ (k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r) < p \le \sqrt{x} \\ p \equiv A \pmod{B} \\ 4p^2 \equiv r^2 \pmod{k^2}}} L(1, \chi_{d_k(p)}) \log p \\ &= \sqrt{x} \sum_{\substack{k \le V \\ (k,2r)=1}} \frac{1}{k} \sum_{n \le U \log U} \frac{e^{-n/U}}{n} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \frac{C_r(a,n,k)}{\phi(4Bnk^2)} + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right). \end{aligned} \tag{23}$$

We now prove

Claim 5.1.

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

Recall that

$$C_r(a,n,k) = \prod_{p | 4Bnk^2} d_p(n)$$

where the $d_p(n)$ are given in Lemma 4.2. In particluar, $d_2(n)$ is at most $2^{\mathrm{ord}_2(B)+3}$ by Lemma 4.2 (4)-(6). For $p|B$, $d_p(n)$ is at most $p^{\mathrm{ord}_p(B)}$ by Lemma 4.2 (1) and (3). For $p|nk$ and $p \nmid B$, $d_p(n)$ is at most 2. Therefore,

$$\begin{aligned} C_r(a,n,k) &= d_2(n) \left(\prod_{\substack{p|B \\ p \neq 2}} d_p(n) \right) \left(\prod_{\substack{p|k \\ p \nmid 2B}} d_p(n) \right) \left(\prod_{\substack{p|n \\ p \nmid 2Bk}} d_p(n) \right) \\ &\le 16B 2^{\nu(k)} 2^{\nu(n) - \nu((n,k))} \\ &= 16B 2^{\nu(nk)} \end{aligned}$$

Since $C_r(a,n,k) = 0$ if $a \equiv 3 \pmod{4}$,

$$\begin{aligned} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) &= \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 1 \pmod{4}}} \left(\frac{a}{n}\right) C_r(a,n,k) \\ &\ll \phi(n) 2^{\nu(nk)}. \end{aligned} \tag{24}$$

Therefore,

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

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

$$+ \mathrm{O}\left(\sum_{\substack{k>V\\ n\le U\log U\\ (k,2r)=1}} \frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{kn\phi(4Bnk^2)} \right).$$

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

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

$$\ll \sum_{k>V} \frac{2^{\nu(k)}}{k^2\phi(k)} \sum_{n\le U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n} \tag{25}$$

We use partial summation (see pg. 21) to estimate the sums in (25). To that end, observe that

$$\phi(k) = \prod_{p^\alpha || k} p^{\alpha-1}(p-1) = k\prod_{p|k}\left(1-\frac{1}{p}\right)$$

and if $p>3$, then

$$\frac{2p}{p-1} < 3.$$

Therefore,

$$\frac{2^{\nu(k)}}{\phi(k)} = \frac{1}{k}\prod_{p|k}\frac{2}{1-p^{-1}} = \frac{1}{k}\prod_{p|k}\frac{2p}{p-1}$$

$$\le \frac{4}{k}\prod_{\substack{p|k\\ p>2}}\frac{2p}{p-1} \le \frac{12}{k}\prod_{\substack{p|k\\ p>3}}\frac{2p}{p-1} \le \frac{12}{k}\prod_{\substack{p|k\\ p>3}} 3 \ll \frac{3^{\nu(k)}}{k}.$$

Thus,

$$\sum_{k>V} \frac{2^{\nu(k)}}{k^2\phi(k)} \ll \sum_{k>V} \frac{3^{\nu(k)}}{k^3}. \tag{26}$$

Using [**?**, Excercise 4, pg 53]

$$\sum_{n\le T} 3^{\nu(n)} \ll T\log^2 T.$$

Set

$$a_n = 3^{\nu(n)};\ f(y) = \frac{1}{y^3}.$$

Then for $X > V+1$ partial summation (see pg. 21) gives

$$\sum_{k=V+1}^{X} \frac{3^{\nu(k)}}{k^3} \ll \frac{\log^2 V}{V^2}$$

Thus,

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

To estimate $\sum_{n\le U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n}$ we set

$$a_n = 2^{\nu(n)}; \qquad f(y) = \frac{e^{-y/U}}{y}$$

then using $\sum_{n\le T} 2^{\nu(n)} \ll T\log T$ from [**?**, Exercise 2, pg 53], partial summation (see pg. 21) gives

$$\begin{aligned}
&\sum_{n\le U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n} \\
&\ll \frac{e^{-U(\log U)/U}}{U\log U} \sum_{n\le U\log U} 2^{\nu(n)} + \int_1^{U\log U} (t\log t)\left[\frac{e^{-t/U}}{t^2} + \frac{e^{-t/U}}{tU}\right]\,\mathrm{dt} \\
&\ll \frac{\log U}{U} + \int_1^{U\log U} \frac{e^{-t/U}\log t}{t}\,\mathrm{dt} + \int_1^{U\log U} \frac{e^{-t/U}\log t}{U}\,\mathrm{dt} \qquad (27)\\
&\ll \frac{\log U}{U} + \int_1^{U\log U} \frac{\log t}{t}\,\mathrm{dt} + \frac{1}{U}\int_1^{U\log U} \log t\,\mathrm{dt} \\
&\ll \frac{\log U}{U} + \log^2 U + \frac{1}{U}\log U \int_1^{U\log U} 1\,\mathrm{dt} \\
&\ll \log^2 U.
\end{aligned}$$

Replacing the two sums in (25) with the estimates given in (26) and (27) gives

$$\begin{aligned}
\sum_{\substack{k>V \\ n\le U\log U \\ (k,2r)=1}} \frac{e^{-n/U}\phi(n)2^{\nu(nk)}}{n\phi(4Bnk^2)} &\ll \left(\frac{\log^2 V}{V^2}\right)\log^2 U \\
&\ll \frac{(\log\log x)^2}{\log^{c+3} x}\log^2 x \\
&\ll \frac{1}{\log^c x}
\end{aligned}$$

as U and V are given by (22). We have shown that

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

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

$$+\,\mathrm{O}\left(\frac{1}{\log^c x}\right)$$

whenever U and V are given by (22). Furthermore,

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

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

$$\mathrm{O}\left(\sum_{k\in\mathbb{N}} \frac{2^{\nu(k)}}{k\phi(k^2)} \sum_{n>U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n}\right)$$

Recall that for any $\epsilon>0$

$$2^{\nu(m)} \ll (m)^{\epsilon}$$

(see pg. 36). Thus the error term above is

$$\ll \frac{1}{\sqrt{U\log U}} \int_{U\log U}^{\infty} e^{-t/U}\ \mathrm{d}t \ll \frac{1}{\log^c x}.$$

Recall the statement of Claim 5.1

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

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

Use the identity

$$\text{(28)} \quad \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \sum_{n=1}^{\infty} \frac{e^{-n/U}}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)$$
$$= \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \sum_{n=1}^{\infty} \frac{1}{kn\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) + \mathrm{O}\left(\frac{1}{\log^c x}\right)$$

(see [**?**, pg. 15]). Claim 5.1 follows. Using (24) and $\phi(k^2) = k\phi(k)$ we may write

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

We make the following two observations:

1. For any $\epsilon > 0$, $2^{\nu(nk)} \ll (nk)^{\epsilon}$.
2. $\phi(4Bnk) \ge \phi(n)\phi(4Bk)$.

Therefore, for any $\epsilon > 0$

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

The double sum above is

$$\ll \left(\sum_{n\ge 1} \frac{e^{-n/U}}{n^{1-\epsilon}}\right)\left(\sum_{k\ge 1} \frac{1}{k^{2-\epsilon}\phi(4Bk)}\right) \ll \sum_{n\ge 1} \frac{e^{-n/U}}{n^{1-\epsilon}} \ll \sum_{n\ge 1} e^{-n/U} \ll 1$$

Therefore, using Claim 5.1 the double sum

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

converges. Thus, (23) from page 39 becomes

$$\sum_{\substack{k\le 2x\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{B(r)<p\le\sqrt{x}\\ p\equiv A \pmod{B}\\ 4p^2\equiv r^2 \pmod{k^2}}} L(1,\chi_{d_k(p)})\log p$$
$$= \sqrt{x}\left[\sum_{k=1}^{\infty}\frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k)\right] + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right).$$

□

6. Constructing a Multiplicative Function

Recall that

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

where

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

In this section we construct a multiplicative function which is a necessary tool used to prove a product formula for $C_{r,A,B}$ which in turn gives the constant in Theorem 0.5 (2). Recall that before we computed $C_r(a,n,k)$ in section 4 we used the Chinese Remainder Theorem (see pg. 25) to write

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

where

$$d_p(n) = \sum_{\substack{b\in(\mathbb{Z}/p^{\mathrm{ord}_p(4Bnk^2)}\mathbb{Z})^*\\ b\equiv A \pmod{p^{\mathrm{ord}_p(B)}}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{\mathrm{ord}_p(4nk^2)}}}} 1$$

Let

$$e_2(n) = \begin{cases}\frac{d_2(n)}{d_2(1)} & \text{if } d_2(1)\neq 0\\ 0 & \text{if } d_2(1)=0.\end{cases}$$

Definition 6.1. *Set* $n = 2^{\mathrm{ord}_2 n}n'$.

$$c_k(n) = \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,n')=1}}\left(\frac{a}{n}\right)e_2(n)\prod_{\substack{p|n\\ p\neq 2}} d_p(n)$$

Lemma 6.2. *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*

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

   (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) *$c_k(q^\alpha) = c_{q^{\mathrm{ord}_k(q)}}(q^\alpha)$*

Proof.
(1) We wish to show that for $(m,n) = 1$, $c_k(m)c_k(n) = c_k(mn)$. To that end, suppose $(m,n) = 1$ and $n \equiv 1 \pmod 2$. Note that $d_2(N) = d_2(2^{\mathrm{ord}_2(N)})$ for any $N \in \mathbb{N}$. Therefore, if

$d_2(1) \neq 0$ we have

$$\begin{aligned}
e_2(mn) &= \frac{d_2(mn)}{d_2(1)} \\
&= \frac{d_2(2^{\mathrm{ord}_2(m)} m_1 n)}{d_2(1)} \quad \text{where } m = 2^{\mathrm{ord}_2(m)} m_1 \\
&= \frac{d_2(2^{\mathrm{ord}_2(m)})}{d_2(1)} \\
&= \frac{d_2(2^{\mathrm{ord}_2(m)})}{d_2(1)} \left(\frac{d_2(n)}{d_2(1)} \right) \\
&= \frac{d_2(m) d_2(n)}{d_2(1) d_2(1)} \\
&= e_2(m) e_2(n).
\end{aligned}$$

Hence, $e_2(n)$ is multiplicative. To show $c_k(n)$ is multiplicative we follow David and Pappalardi's proof in [**?**, pg. 10]. Note the following two facts. First, there is a bijection between the invertible residues modulo $4n$ which are congruent to 1 modulo 4 and the invertible residues modulo n. Second, if a is congruent to 1 modulo 4, then $(r^2 - ak^2, N) = 1$ if and only if $(r^2 - ak^2, 4N) = 4$. Thus,

$$c_k(n) c_k(m) = \sum_{\substack{a_1 \in (\mathbb{Z}/n\mathbb{Z})^* \\ (r^2 - a_1 k^2, n') = 1}} \sum_{\substack{a_2 \in (\mathbb{Z}/4m\mathbb{Z})^* \\ a_2 \equiv 1 \pmod 4 \\ (r^2 - a_2 k^2, 4m') = 4}} \left(\frac{a_1}{n} \right) e_2(n) \left(\prod_{\substack{p \mid n \\ p \neq 2}} d_p(n) \right) \cdot \left(\frac{a_2}{m} \right) e_2(m) \left(\prod_{\substack{p \mid m \\ p \neq 2}} d_p(m) \right) \tag{29}$$

For any a_1 and a_2 in the above sums, we let a be the unique integer such that $1 \leq a \leq 4mn$, $(a, 4mn) = 1$, $a = a_1 + k_1 n = a_2 + k_2 4m$ for some integers k_1 and k_2. Then using the fact that

$$(r^2 - a_1 k^2, n) = 1 \text{ and } (r^2 - a_2 k^2, 4m) = 4 \iff (r^2 - ak^2, 4mn) = 4$$

(29) becomes

$$\begin{aligned}
&\sum_{\substack{a_1 \in (\mathbb{Z}/n\mathbb{Z})^* \\ a_2 \in (\mathbb{Z}/4m\mathbb{Z})^* \\ a_2 \equiv 1 \pmod 4 \\ (r^2 - ak^2, 4m'n') = 4}} \left(\frac{a}{n} \right) e_2(n) \prod_{\substack{p \mid n \\ p \neq 2}} d_p(n) \left(\frac{a}{m} \right) e_2(m) \prod_{\substack{p \mid m \\ p \neq 2}} d_p(m) \\
&= \sum_{\substack{a \in (\mathbb{Z}/4mn\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, 4m'n') = 1}} \left(\frac{a}{mn} \right) e_2(mn) \prod_{\substack{p \mid mn \\ p \neq 2}} d_p(mn) \\
&= c_k(mn).
\end{aligned}$$

To evaluate $c_k(q^\alpha)$ we first make the following simplification. Suppose q is an odd prime and $\alpha > 0$. Then using Lemma 4.2

$$\begin{aligned} c_k(q^\alpha) &= \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha e_2(q^\alpha)d_q(q^\alpha) \\ &= \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1 \\ q^{\min(l_1,l_2)}|(4A^2-r^2+ak^2)}} \left(\frac{a}{q}\right)^\alpha \sum_{\substack{b\in(\mathbb{Z}/q^l\mathbb{Z})^* \\ b\equiv A \pmod{q^{l_1}} \\ 4b^2\equiv r^2-ak^2 \pmod{q^{l_2}}}} 1 \end{aligned}$$

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 $l = l_1 + l_2$. In Lemma 4.2 we computed the inner sum above and obtained

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

Set $\beta = \mathrm{ord}_q(k)$. For an odd prime q and $\alpha > 0$ we have

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

(2) Suppose $q|B$. Set $k = q^\beta k_1$, where $\mathrm{ord}_q(k) = \beta$. We consider two cases.
Case 1: If $2\beta \geq l_1$, then the condition

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

becomes

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{l_1}}$$

as $\alpha > 0$ and $l_2 = \alpha + 2\beta$. Since $k = q^\beta k_1 \Rightarrow k^2 = q^{2\beta}k_1^2$, we have

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{l_1}} \Longleftrightarrow r^2 \equiv 4A^2 \pmod{q^{l_1}}$$

Therefore,

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

Case 2: If $2\beta < l_1$, then

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

Combining the two congruences

$$
a\equiv 1 \pmod 4 \ ; \ ak_1^2 \equiv \frac{r^2-4A^2}{q^{2\beta}} \pmod{q^{\min(l_1-2\beta,\alpha)}}
$$

we have

$$
\sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1 \\ ak_1^2\equiv \frac{r^2-4A^2}{q^{2\beta}} \pmod{q^{\min(l_1-2\beta,\alpha)}} \\ q^{2\beta}|(r^2-4A^2)}} \left(\frac{a}{q}\right)^\alpha = \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ (r^2-ak^2,q^\alpha)=1 \\ a\equiv \frac{r^2-4A^2}{q^{2\beta}}k_1^{-2} \pmod{4q^{\min(l_1-2\beta,\alpha)}} \\ q^{2\beta}|(r^2-4A^2)}} \left(\frac{a}{q}\right)^\alpha
$$

Thus,

$$
c_k(q^\alpha) = \begin{cases} q^{\alpha-\min(\alpha,l_1-2\beta)} \left(\frac{(r^2-4A^2)/q^{2\beta}}{q}\right)^\alpha & \text{if } r^2\equiv 4A^2 \pmod{q^{2\beta}} \\ 0 & \text{otherwise.} \end{cases}
$$

This concludes the proof of part (2).
For $q \nmid B$ we use Lemma 4.2 (see pg. 25) for the value of $d_q(q^\alpha)$.
(3a) Suppose $q\nmid B$ and $q|k$. Since $(k,2r)=1$, $q\nmid r$. Therefore, by Lemma 4.2 (2)

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

(3b) Suppose $q \nmid B$ and $q \nmid k$. First, consider odd α. Then using Lemma 4.2 (2)

$$\begin{aligned}
c_k(q^\alpha) &= \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, q^\alpha) = 1}} \left(\frac{a}{q}\right)^\alpha \left(1 + \left(\frac{r^2 - ak^2}{q}\right)\right) \\
&= \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, q^\alpha) = 1}} \left[\left(\frac{a}{q}\right) + \left(\frac{a}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
&= q^{\alpha-1} \sum_{\substack{a \in (\mathbb{Z}/q\mathbb{Z})^* \\ r^2 \not\equiv ak^2 \pmod q}} \left[\left(\frac{a}{q}\right) + \left(\frac{a}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
&= q^{\alpha-1} \left[\sum_{\substack{a \in (\mathbb{Z}/q\mathbb{Z})^* \\ r^2 \not\equiv ak^2 \pmod q}} \left(\frac{a}{q}\right) + \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
&= q^{\alpha-1} \left[-\left(\frac{r^2 k^{-2}}{q}\right) + \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a^{-1}}{q}\right)\left(\frac{r^2 - ak^2}{q}\right)\right] \\
&= q^{\alpha-1} \left[-\left(\frac{r^2}{q}\right) + \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a^{-1} r^2 - k^2}{q}\right)\right] \\
&= \begin{cases} q^{\alpha-1} \left(\frac{-1}{q}\right)(q-1) & \text{if } q \mid r \\ q^{\alpha-1}\left[-1 - \left(\frac{-1}{q}\right)\right] & \text{if } q \nmid r \end{cases}
\end{aligned}$$

If α is even, then

$$\begin{aligned}
c_k(q^\alpha) &= \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{a}{q}\right)^\alpha \left(1+\left(\frac{r^2-ak^2}{q}\right)\right) \\
&= \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a\equiv 1 \pmod 4 \\ (r^2-ak^2,q^\alpha)=1}} 1 + q^{\alpha-1} \sum_{\substack{a\in(\mathbb{Z}/q\mathbb{Z})^* \\ (r^2-ak^2,q^\alpha)=1}} \left(\frac{r^2-ak^2}{q}\right) \\
&= q^{\alpha-1} \sum_{\substack{a\in(\mathbb{Z}/q\mathbb{Z})^* \\ a\not\equiv r^2k^{-2} \pmod q}} 1 \\
&\quad + q^{\alpha-1}\left[\sum_{\substack{a\in(\mathbb{Z}/q\mathbb{Z})^* \\ a\not\equiv r^2k^{-2} \pmod q}} \left(\frac{r^2-ak^2}{q}\right) + \left(\frac{r^2}{q}\right) - \left(\frac{r^2}{q}\right)\right] \\
&= \begin{cases} q^{\alpha-1}[q-2] - q^{\alpha-1} & \text{if } q\nmid r \\ q^{\alpha-1}[q-1] & \text{if } q|r \end{cases}
\end{aligned}$$

(4) Throughout the proof of part (4) we will be using parts (4)-(6) of Lemma 4.2 from page 25. Note that by definition

$$d_2(1) = \sum_{\substack{b\in(\mathbb{Z}/2^{2+\mathrm{ord}_2(B)})^* \\ b\equiv A \pmod{2^{\mathrm{ord}_2(B)}} \\ 4b^2\equiv r^2-ak^2 \pmod{2^2}}} 1$$

therefore

$$d_2(1) = \begin{cases} 2 & \text{if } 2\nmid B \text{ and } a\equiv 1 \pmod 4 \\ 4 & \text{if } 2|B \text{ and } a\equiv 1 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Set $l_2 = \mathrm{ord}_2(4\cdot 2^\alpha k^2) = \alpha+2$; $l_1 = \mathrm{ord}_2(B)$; $l = \mathrm{ord}_2(4B2^\alpha k^2) = \alpha+2+l_1$. Suppose $l_1 = 0$. Note that since r and k are odd

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

Using Lemma 4.2 (4) with $l_1 = 0$ we have

$$
\begin{aligned}
c_k(2^\alpha) &= \sum_{a\in(\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^*} \left(\frac{a}{2}\right)^\alpha \frac{d_2(2^\alpha)}{d_2(1)} \\
&= \sum_{\substack{a\in(\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ r^2-ak^2\equiv 4 \pmod{2^{\min(5,\alpha+2)}}}} \left(\frac{a}{2}\right)^\alpha \frac{2^{\min(4,\alpha+1)}}{2} \\
&= \sum_{\substack{a\in(\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ r^2-ak^2\equiv 4 \pmod{2^{\min(5,\alpha+2)}}}} (-1)^\alpha \frac{2^{\min(4,\alpha+1)}}{2}
\end{aligned}
$$

If $\alpha = 1$, then

$$c_k(2) = \sum_{\substack{a\in(\mathbb{Z}/2^3\mathbb{Z})^* \\ r^2-ak^2\equiv 4 \pmod 8}} \left(\frac{a}{2}\right) \frac{2^2}{2} = \sum_{\substack{a\in(\mathbb{Z}/2^3\mathbb{Z})^* \\ a\equiv 5 \pmod 8}} \left(\frac{a}{2}\right) 2 = -2$$

If $\alpha = 2$, then

$$c_k(2^2) = \sum_{\substack{a\in(\mathbb{Z}/2^4\mathbb{Z})^* \\ r^2-ak^2\equiv 4 \pmod{2^4}}} \left(\frac{a}{2}\right)^2 \frac{2^3}{2} = 2^2$$

If $\alpha \geq 3$, then

$$c_k(2^\alpha) = \sum_{\substack{a\in(\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ r^2-ak^2\equiv 4 \pmod{2^5}}} \left(\frac{a}{2}\right)^\alpha \frac{2^4}{2} = 2^3 \cdot 2^{\alpha-3}(-1)^\alpha = (-2)^\alpha$$

Suppose $l_1 > 0$, we have three cases.
Case 1: $l_1 = 1$
Using Lemma 4.2 (4) $c_k(q^\alpha)$ is

$$c_k(2^\alpha) = \sum_{\substack{a\in(\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4\equiv r^2-ak^2 \pmod{2^{\min(5,l_2)}}}} \left(\frac{a}{2}\right)^\alpha \frac{2^{\min(5,l_2)}}{4}.$$

If $\alpha = 1$, then

$$c_k(2) = \sum_{\substack{a\in(\mathbb{Z}/2^3\mathbb{Z})^* \\ 4\equiv r^2-ak^2 \pmod{2^{\min(5,3)}}}} \left(\frac{a}{2}\right) \frac{2^{\min(5,3)}}{4} = \sum_{\substack{a\in(\mathbb{Z}/2^3\mathbb{Z})^* \\ 4\equiv r^2-ak^2 \pmod{2^3}}} (-2) = -2.$$

If $\alpha = 2$, then

$$c_k(2^2) = \sum_{\substack{a\in(\mathbb{Z}/2^4\mathbb{Z})^* \\ 4\equiv r^2-ak^2 \pmod{2^4}}} \left(\frac{a}{2}\right)^2 \frac{2^4}{4} = 2^2.$$

If $\alpha \geq 3$, then

$$c_k(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4 \equiv r^2 - ak^2 \pmod{2^5}}} \left(\frac{a}{2}\right)^\alpha \frac{2^5}{4} = (-1)^\alpha \cdot 2^3 \cdot 2^{\alpha+2-5} = (-2)^\alpha.$$

Case 2: $l_1 \geq 2$ and $l_2 \leq l_1 + 3$
Using Lemma 4.2 (5)

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

Case 3: $l_1 \geq 2$ and $l_2 \geq l_1 + 4$
Using Lemma 4.2 (6)

$$\begin{aligned} c_k(2^\alpha) &= \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}}}} \left(\frac{a}{2}\right)^\alpha \frac{2^{l_1+3}}{4} \\ &= (-1)^\alpha \frac{2^{l_1+3}}{4} \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ 4A^2 \equiv r^2 - ak^2 \pmod{2^{l_1+3}}}} 1 \\ &= (-1)^\alpha \cdot 2^{l_1+1} \cdot 2^{\alpha+2-(l_1+3)} = (-2)^\alpha. \end{aligned}$$

□

7. Computing the Constant

Let $r, A, B \in \mathbb{Z}$ with $(A, B) = 1$ and r odd. Recall the definition of $C_{r,A,B}$

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

where as before (see pg. 25)

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

and

$$d_p(n) = \sum_{\substack{b \in (\mathbb{Z}/p^{\mathrm{ord}_p(4Bnk^2)}\mathbb{Z})^* \\ b \equiv A \pmod{p^{\mathrm{ord}_p(B)}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{p^{\mathrm{ord}_p(4nk^2)}}}} 1.$$

In this section we show that

$$
\begin{aligned}
C_{r,A,B} = {} & c_{r,A,B} \\
& \cdot \prod_{\substack{q,\text{odd} \\ q|B \\ q|r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1} q^{-2\mathrm{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}\left(q - \left(\frac{-1}{q}\right)\right)} \right) \\
& \cdot \frac{2}{3\phi(B)} \prod_{\substack{q,\text{odd} \\ q\nmid B \\ q|r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)} \right) \prod_{\substack{q,\text{odd} \\ q\nmid B \\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right) q - 1}{(q-1)(q^2-1)} \right).
\end{aligned}
$$

First, we record several evaluations of d_p which follow directly from Lemma 4.2 (see pg. 25).

Lemma 7.1. *Suppose $p \nmid 2n$,*

(1) *If $p|B$ and $p \nmid k$, then $d_p(1) = d_p(n) = 1$*

(2) *Suppose $p|k$.*

  (a) *If $p|B$, then*

$$
\begin{aligned}
d_p(1) &= d_p(n) \\
&= \begin{cases} p^{\min(\mathrm{ord}_p(B), \mathrm{ord}_p(4nk^2))} & \text{if } 4A^2 \equiv r^2 \pmod{p^{\min(\mathrm{ord}_p(B), \mathrm{ord}_p(4nk^2))}} \\ 0 & \text{otherwise} \end{cases}
\end{aligned}
$$

  (b) *If $p \nmid B$ and $(r^2 - ak^2, p) = 1$, then $d_p(1) = d_p(n) = 2$*

Proof.
(1) By Lemma 4.2 (1).
(2a) By Lemma 4.2 (1) and (3).
(2b) By Lemma 4.2 (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

$$\begin{aligned}
C_{r,A,B} &= \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)} \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) \prod_{\substack{p,\text{prime}\\ p|4Bnk^2}} d_p(n)\\
&= \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)} \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right)\\
&\quad \cdot d_2(n)\left(\prod_{\substack{p|n\\ p\neq 2}} d_p(n)\right)\left(\prod_{\substack{p|k\\ p\nmid 2n}} d_p(n)\right)\left(\prod_{\substack{p|B\\ p\nmid 2nk}} d_p(n)\right)
\end{aligned}$$

If $p|B$ and $p \nmid 2nk$, Lemma 7.1 (1) implies that $d_p(n) = 1$. Therefore, $C_{r,A,B}$ simplifies to

$$\begin{aligned}
C_{r,A,B} = &\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)}\\
&\cdot \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) d_2(n)\left(\prod_{\substack{p|n\\ p\neq 2}} d_p(n)\right)\left(\prod_{\substack{p|k\\ p\nmid 2n}} d_p(n)\right)
\end{aligned}$$

For a prime p such that $p|k$ and $p \nmid 2n$ Lemma 7.1 (2) gives $d_p(n) = d_p(1)$. Therefore, we write $C_{r,A,B}$ as

$$\begin{aligned}
C_{r,A,B} = &\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k}\sum_{n=1}^{\infty}\frac{1}{n\phi(4Bnk^2)}\\
&\cdot \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4\\ (r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) d_2(n)\left(\prod_{\substack{p|n\\ p\neq 2}} d_p(n)\right)\left(\prod_{\substack{p|k\\ p\nmid 2n}} d_p(1)\right).
\end{aligned}$$

By definition,

$$d_2(1) = \sum_{\substack{b \in (\mathbb{Z}/2^{\mathrm{ord}_2(4Bk^2)}\mathbb{Z})^* \\ b \equiv A \pmod{2^{\mathrm{ord}_2(B)}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{\mathrm{ord}_2(4k^2)}}}} 1$$

and

$$d_2(n) = \sum_{\substack{b \in (\mathbb{Z}/2^{\mathrm{ord}_2(4Bnk^2)}\mathbb{Z})^* \\ b \equiv A \pmod{2^{\mathrm{ord}_2(B)}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{2^{\mathrm{ord}_2(4nk^2)}}}} 1.$$

If $d_2(1) = 0$, then $4A^2 \not\equiv r^2 - ak^2 \pmod{2^{\min(\mathrm{ord}_2(B), \mathrm{ord}_2(4k^2))}}$. Since $\min(\mathrm{ord}_2(B), \mathrm{ord}_2(4k^2)) \leq \min(\mathrm{ord}_2(B), \mathrm{ord}_2(4nk^2))$, we also have that $4A^2 \not\equiv r^2 - ak^2 \pmod{2^{\min(\mathrm{ord}_2(B), \mathrm{ord}_2(4nk^2))}}$. Therefore, $d_2(n) = 0$. Recall our definition of $e_2(n)$

$$e_2(n) = \begin{cases} \frac{d_2(n)}{d_2(1)} & \text{if } d_2(1) \neq 0 \\ 0 & \text{if } d_2(1) = 0. \end{cases}$$

Thus, $d_2(n) = d_2(1)e_2(n)$ and $C_{r,A,B}$ becomes

$$C_{r,A,B} = \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)}$$

$$\cdot \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, n')=1}} \left(\frac{a}{n}\right) d_2(1)e_2(n) \left(\prod_{\substack{p \mid n \\ p \neq 2}} d_p(n)\right) \left(\prod_{\substack{p \mid k \\ p \nmid 2n}} d_p(1)\right).$$

Suppose p is an odd prime, recall

$$d_p(1) := \sum_{\substack{b \in (\mathbb{Z}/p^{\mathrm{ord}_p(4Bk^2)}\mathbb{Z})^* \\ b \equiv A \pmod{p^{\mathrm{ord}_p(B)}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{p^{\mathrm{ord}_p(4k^2)}}}} .$$

Since p is an odd prime $\mathrm{ord}_p(4k^2) = \mathrm{ord}_p(k^2)$ and our last condition on the sum in the definition of $d_p(1)$ becomes $4b^2 \equiv r^2 \pmod{p^{\mathrm{ord}_p(4k^2)}}$. We have shown that for odd primes p $d_p(1)$ does not depend on a. Therefore, we write

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

$$\cdot \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, n')=1}} \left(\frac{a}{n}\right) d_2(1)e_2(n) \prod_{\substack{p \mid n \\ p \neq 2}} d_p(n).$$

Since $a \equiv 1 \pmod 4$, $d_2(1)$ *only* depends on B modulo 2 and our definition of $c_k(n)$ is

$$c_k(n) = \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, n')=1}} \left(\frac{a}{n}\right) e_2(n) \prod_{\substack{p|n \\ p \neq 2}} d_p(n).$$

We write $C_{r,A,B}$ as

$$\begin{aligned} C_{r,A,B} &= d_2(1) \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \left(\prod_{\substack{p|k \\ p \nmid 2n}} d_p(1) \right) c_k(n) \\ &= d_2(1) \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n=1}^{\infty} \frac{1}{n\phi(4Bnk^2)} \left(\prod_{\substack{p|(B,k) \\ p \nmid 2n}} d_p(1) \right) \left(\prod_{\substack{p|k \\ p \nmid 2Bn}} d_p(1) \right) c_k(n). \end{aligned}$$

For integers x and y denote by $\nu(x,y)$ the number of distinct prime divisors of the $gcd(x,y)$. Using Lemma 7.1

$$\prod_{\substack{p|k \\ p \nmid 2Bn}} d_p(1) = 2^{\nu(k) - \nu(k,2Bn)}.$$

Recall

$$\phi(AB) = \phi(A)\phi(B) \frac{(A,B)}{\phi((A,B))} \tag{30}$$

where (A,B) is the greatest common divisor of A and B. So, we can write

$$\begin{aligned} C_{r,A,B} = d_2(1) &\sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{2^{\nu(k)}}{k\phi(4Bk^2)} \\ &\cdot \sum_{n \in \mathbb{N}} \frac{\left[\prod_{\substack{p|(B,k) \\ p \nmid 2n}} d_p(1) \right] \phi((n, 4Bk^2))}{n\phi(n)(n, 4Bk^2) 2^{\nu(k,2Bn)}} c_k(n) \end{aligned} \tag{31}$$

For positive integers x, y, and z we have the identities:

(1)

$$(x,(y,z)) = (x,y,z) \tag{32}$$

(2)

$$(x,yz) = (x,y) \left(\frac{x}{(x,y)}, z \right). \tag{33}$$

Identity (33) along with the fact that ν is additive and k is odd implies that

$$\begin{aligned} 2^{\nu(k,2Bn)} &= 2^{\nu\left((k,B) \cdot \left(\frac{k}{(k,B)}, n\right)\right)} \\ &= 2^{\nu(k,B) + \nu\left(\frac{k}{(k,B)}, n\right) - \nu\left((k,B), \left(\frac{k}{(k,B)}, n\right)\right)} \end{aligned} \tag{34}$$

Observe that

$$\left((k,B),\left(\frac{k}{(k,B)},n\right)\right)=\left(\left(B,\left(k,\frac{k}{(k,B)}\right)\right),n\right)\qquad\text{by (32)}$$

$$=\left(\left(B,\frac{k}{(k,B)}\right),n\right)\qquad\text{by (33)}$$

$$=\left(\frac{(k,B^2)}{(k,B)},n\right)\qquad\text{by (33).}$$

Thus, (34) becomes

$$2^{\nu(k,2Bn)}=\frac{2^{\nu(k,B)}\cdot 2^{\nu\left(\frac{k}{(k,B)},n\right)}}{2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}. \tag{35}$$

Using (35) we may write (31) as

$$C_{r,A,B}=d_2(1)\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}}\frac{2^{\nu(k)}}{k2^{\nu(k,B)}\phi(4Bk^2)} \cdot\sum_{n\in\mathbb{N}}\frac{\left[\prod_{\substack{p|(B,k)\\p\nmid 2n}}d_p(1)\right]\phi((n,4Bk^2))2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{n\phi(n)(n,4Bk^2)2^{\nu\left(\frac{k}{(k,B)},n\right)}}c_k(n). \tag{36}$$

In order to make the inner sum multiplicative in n, we require the following lemma.

Lemma 7.2. *Suppose $p|(B,n,k)$. If $d_p(1)=0$, then $c_k(n)=0$.*

Proof.
Let $\alpha=\mathrm{ord}_p(B)$ and $\beta=\mathrm{ord}_p(k)$. By definition

$$d_p(1)=\sum_{\substack{b\in(\mathbb{Z}/p^{\alpha+2\beta}\mathbb{Z})^*\\ b\equiv A \pmod{p^\alpha}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{2\beta}}}}1$$

and

$$d_p(n)=\sum_{\substack{b\in(\mathbb{Z}/p^{\alpha+2\beta+\mathrm{ord}_p(n)}\mathbb{Z})^*\\ b\equiv A \pmod{p^\alpha}\\ 4b^2\equiv r^2-ak^2 \pmod{p^{2\beta+\mathrm{ord}_p(n)}}}}1$$

Recall from page 55 that $d_p(1)$ does not depend on a. Therefore, for any a one can see that if $d_p(1)=0$, then $4A^2\not\equiv r^2-ak^2 \pmod{p^{\min(\alpha,2\beta)}}$. Since $\min(\alpha,2\beta)\le\min(\alpha,2\beta+\mathrm{ord}_p(n))$,

$$4A^2\not\equiv r^2-ak^2 \pmod{p^{\min(\alpha,2\beta)}}\Rightarrow 4A^2\not\equiv r^2-ak^2 \pmod{p^{\min(\alpha,2\beta+\mathrm{ord}_p(n))}}$$
$$\Rightarrow d_p(n)=0$$

So, if $d_p(1)=0$, then $d_p(n)=0$ for all a. Thus, $c_k(n)=0$.

□

For $p|(B,k,n)$, define

$$f_p = \begin{cases} d_p(1) & \text{if } d_p(1) \neq 0 \\ 1 & \text{if } d_p(1) = 0. \end{cases}$$

Then by Lemma 7.2,

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

Note that if $d_p(1) = 0$ for some $p|(B,k)$, then both sides of the above equation are 0. Using Lemma 7.2, we write $C_{r,A,B}$ as

$$\begin{aligned} C_{r,A,B} = d_2(1) &\sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} \frac{2^{\nu(k)} \left[\prod_{p|(B,k)} d_p(1)\right]}{k 2^{\nu(k,B)} \phi(4Bk^2)} \\ &\cdot \sum_{n\in\mathbb{N}} \frac{\phi((n,4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{\left[\prod_{p|(B,k,n)} f_p\right] n\phi(n)(n,4Bk^2) 2^{\nu\left(\frac{k}{(k,B)},n\right)}} c_k(n). \end{aligned}$$

Another application of (30) yields

$$\begin{aligned} C_{r,A,B} = \frac{d_2(1)}{\phi(4B)} &\sum_{\substack{k\in\mathbb{N} \\ (k,2r)=1}} \frac{2^{\nu(k)} \left[\prod_{p|(B,k)} d_p(1)\right] \phi((4B,k^2))}{k 2^{\nu(k,B)} \phi(k^2)(4B,k^2)} \\ &\cdot \sum_{n\in\mathbb{N}} \frac{\phi((n,4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)},n\right)}}{\left[\prod_{p|(B,k,n)} f_p\right] n\phi(n)(n,4Bk^2) 2^{\nu\left(\frac{k}{(k,B)},n\right)}} c_k(n). \end{aligned} \tag{37}$$

Due to the multiplicativity of the functions in the inner sum above we may rewrite the inner sum as

$$\prod_{q,\ \text{prime}} \sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)},q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)} f_p\right] q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2) 2^{\nu\left(\frac{k}{(k,B)},q^\alpha\right)}} c_k(q^\alpha). \tag{38}$$

Since $c_k(q^\alpha) = c_{q^{\mathrm{ord}_q(k)}}(q^\alpha)$, the product above may be written as

$$\prod_{q \nmid k} \left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4B))}{q^\alpha \phi(q^\alpha)(q^\alpha, 4B)} c_1(q^\alpha) \right)$$

$$\cdot \prod_{q | k} \left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)}, q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)} f_p\right] q^\alpha \phi(q^\alpha)(q^\alpha, 4Bk^2) 2^{\nu\left(\frac{k}{(k,B)}, q^\alpha\right)}} c_{q^{\mathrm{ord}_q(k)}}(q^\alpha) \right)$$

$$= \prod_{q,\text{prime}} \left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4B))}{q^\alpha \phi(q^\alpha)(q^\alpha, 4B)} c_1(q^\alpha) \right)$$

$$\cdot \prod_{q|k} \frac{\left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4Bk^2)) 2^{\nu\left(\frac{(k,B^2)}{(k,B)}, q^\alpha\right)}}{\left[\prod_{p|(B,k,q^\alpha)} f_p\right] q^\alpha \phi(q^\alpha)(q^\alpha, 4Bk^2) 2^{\nu\left(\frac{k}{(k,B)}, q^\alpha\right)}} c_{q^{\mathrm{ord}_q(k)}}(q^\alpha) \right)}{\left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4B))}{q^\alpha \phi(q^\alpha)(q^\alpha, 4B)} c_1(q^\alpha) \right)} \tag{39}$$

Substituting (39) into (37) we obtain

$$C_{r,A,B} = \frac{d_2(1)}{\phi(4B)} \prod_q \left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4B)) c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, 4B)} \right)$$

$$\cdot \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \left(\frac{2^{\nu(k)} \left[\prod_{p|(B,k)} d_p(1)\right] \phi((4B, k^2))}{k 2^{\nu(k,B)} \phi(k^2)(4B, k^2)} \right)$$

$$\cdot \prod_{\substack{q^\beta || k \\ \beta \ge 1}} \frac{\left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4Bq^{2\beta})) 2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)}, q^\alpha\right)} c_{q^\beta}(q^\alpha)}{\left[\prod_{p|(B,q)} f_p\right] q^\alpha \phi(q^\alpha)(q^\alpha, 4Bq^{2\beta}) 2^{\nu\left(\frac{q^\beta}{(q^\beta,B)}, q^\alpha\right)}} \right)}{\left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4B)) c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, 4B)} \right)} \tag{40}$$

Again we have a sum of multiplicative functions which allows us to write the inner sum as

$$\prod_{\substack{q \\ q \nmid 2r}} \left[1 + \sum_{\beta \ge 1} \left(\frac{\frac{2^{\nu(q^\beta)}\left[\prod_{p|(B,q)} d_p(1)\right] \phi((4B, q^{2\beta}))}{q^\beta 2^{\nu(q^\beta,B)} \phi(q^{2\beta})(4B, q^{2\beta})}}{\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4B)) c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, 4B)}} \right) \right.$$
$$\left. \cdot \left(\sum_{\alpha \ge 0} \frac{\phi((q^\alpha, 4Bq^{2\beta})) 2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)}, q^\alpha\right)} c_{q^\beta}(q^\alpha)}{\left[\prod_{p|(B,q)} f_p\right] q^\alpha \phi(q^\alpha)(q^\alpha, 4Bq^{2\beta}) 2^{\nu\left(\frac{q^\beta}{(q^\beta,B)}, q^\alpha\right)}} \right) \right] \tag{41}$$

Putting (41) into (40) yields

$$
\begin{aligned}
C_{r,A,B} = \frac{d_2(1)}{\phi(4B)} \cdot &\left(1 + \sum_{\alpha \geq 1} \frac{\phi((2^\alpha, 4B))c_1(2^\alpha)}{2^\alpha \phi(2^\alpha)(2^\alpha, 4B)}\right) \\
&\cdot \prod_{\substack{q,\text{odd} \\ q \nmid B \\ q \mid r}} \left(\sum_{\alpha \geq 0} \frac{c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)}\right) \\
&\cdot \prod_{\substack{q,\text{odd} \\ q \nmid B \\ q \nmid r}} \left(\sum_{\alpha \geq 0} \frac{c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)} + \sum_{\beta \geq 1} \frac{2}{q^\beta \phi(q^{2\beta})} \sum_{\alpha \geq 0} \frac{\phi((q^\alpha, q^{2\beta}))c_{q^\beta}(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, q^{2\beta})2^{\nu(q^\beta, q^\alpha)}}\right) \\
&\cdot \prod_{\substack{q,\text{odd} \\ q \mid B \\ q \mid r}} \left(1 + \sum_{\alpha \geq 1} \frac{\phi((q^\alpha, B))c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, B)}\right) \\
&\cdot \prod_{\substack{q,\text{odd} \\ q \mid B \\ q \nmid r}} \left(1 + \sum_{\alpha \geq 1} \frac{\phi((q^\alpha, B))c_1(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, B)}\right. \\
&\quad \left. + \frac{d_q(1)}{f_q} \sum_{\beta \geq 1} \frac{\phi((B, q^{2\beta}))}{q^\beta \phi(q^{2\beta})(B, q^{2\beta})} \sum_{\alpha \geq 0} \frac{\phi((q^\alpha, Bq^{2\beta}))2^{\nu\left(\frac{(q^\beta, B^2)}{(q^\beta, B)}, q^\alpha\right)} c_{q^\beta}(q^\alpha)}{q^\alpha \phi(q^\alpha)(q^\alpha, 4Bq^{2\beta})2^{\nu\left(\frac{q^\beta}{(q^\beta, B)}, q^\alpha\right)}}\right)
\end{aligned}
\tag{42}
$$

Define $C(2)$ as

$$C(2) = 1 + \sum_{\alpha \geq 1} \frac{\phi((2^\alpha, 4B))c_1(2^\alpha)}{2^\alpha \phi(2^\alpha)(2^\alpha, 4B)}.$$

To compute $C(2)$ recall Lemma 6.2 (4),

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

We compute

$$1 + \sum_{\alpha \geq 1} \frac{\phi((2^\alpha, 4B))c_1(2^\alpha)}{2^\alpha \phi(2^\alpha)(2^\alpha, 4B)} = \frac{2}{3}$$

Using Lemma 6.2 the following two computations allow us to simplify the first and second products in (42). First we compute, for $q \nmid B$

$$\sum_{\alpha\geq 0}\frac{c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)} = \begin{cases} 1+\sum_{\substack{\alpha\geq 1\\ \alpha,\ \text{even}}}\frac{q^{\alpha-1}(q-3)}{q^\alpha q^{\alpha-1}(q-1)}+\sum_{\substack{\alpha\geq 1\\ \alpha,\ \text{odd}}}\frac{q^{\alpha-1}(-1-\left(\frac{-1}{q}\right))}{q^\alpha q^{\alpha-1}(q-1)} & \text{if } q\nmid r\\ 1+\sum_{\alpha\geq 1}\frac{\left(\frac{-1}{q}\right)^\alpha(\phi(q^\alpha))}{q^\alpha q^{\alpha-1}(q-1)} & \text{if } q|r\end{cases}$$

$$= \begin{cases} 1+\frac{(q-3)}{(q-1)(q^2-1)}+\frac{q\left(-1-\left(\frac{-1}{q}\right)\right)}{(q-1)(q^2-1)} & \text{if } q\nmid r\\ \frac{q^2+\left(\frac{-1}{q}\right)q}{q^2-1} & \text{if } q|r.\end{cases}$$

$$= \begin{cases} 1-\frac{\left(\frac{-1}{q}\right)q+3}{(q-1)(q^2-1)} & \text{if } q\nmid r\\ \frac{q}{q-\left(\frac{-1}{q}\right)} & \text{if } q|r.\end{cases}$$

Second, we compute for $q\nmid B$, $q\nmid r$

$$\sum_{\beta\geq 1}\frac{2}{q^\beta\phi(q^{2\beta})}\sum_{\alpha\geq 0}\frac{\phi((q^\alpha,q^{2\beta}))c_q(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,q^{2\beta})2^{\nu(q^\beta,q^\alpha)}}$$

$$=\sum_{\beta\geq 1}\frac{2}{q^\beta\phi(q^{2\beta})}\left[1+\frac{1}{2}\sum_{\alpha\geq 1}\frac{c_q(q^\alpha)}{q^\alpha q^\alpha}\right]$$

$$=\frac{2q}{q-1}\sum_{\beta\geq 1}\frac{1}{q^{3\beta}}\left[1+\frac{1}{q(q+1)}\right]$$

$$=\frac{2(q^2+q+1)}{q^2-1}\sum_{\beta\geq 1}\frac{1}{q^{3\beta}}$$

$$=\frac{2(q^2+q+1)}{(q^2-1)(q^3-1)}$$

$$=\frac{2}{(q^2-1)(q-1)}$$

For the third product in (42) note that $q|B$ and $q|r$. Since $(k,r)=1$, $q\nmid k=q^\beta$. Therefore using Lemma 6.2 with $\beta=0$

$$1+\sum_{\alpha\geq 1}\frac{\phi(q^{\min(\alpha,\text{ord}_q(B))})c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)q^{\min(\alpha,\text{ord}_q(B))}} = 1+\sum_{1\leq\alpha\leq\text{ord}_q(B)}\frac{c_1(q^\alpha)}{q^{2\alpha}}+\sum_{\text{ord}_q(B)<\alpha}\frac{c_1(q^\alpha)}{q^{2\alpha}}$$

$$=1+\sum_{1\leq\alpha\leq\text{ord}_q(B)}\frac{\left(\frac{-1}{q}\right)^\alpha}{q^{2\alpha}}+\sum_{\text{ord}_q(B)<\alpha}q^{\alpha-\text{ord}_q(B)}\left(\frac{-1}{q}\right)^\alpha\frac{1}{q^{2\alpha}}$$

$$=1+\frac{\left(\frac{-1}{q}\right)-\left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1}q^{-2\text{ord}_q(B)}}{q^2-\left(\frac{-1}{q}\right)}+\frac{\left(\frac{-1}{q}\right)^{\text{ord}_q(B)+1}}{q^{2\text{ord}_q(B)}\left(q-\left(\frac{-1}{q}\right)\right)}$$

(42) may now be written as

$$
\begin{aligned}
C_{r,A,B} = &\frac{d_2(1)}{\phi(4B)} \cdot \frac{2}{3} \\
&\cdot \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\mid r}} \left(\frac{q}{q - \left(\frac{-1}{q}\right)} \right) \prod_{\substack{q,\text{odd}\\ q\nmid B\\ q\nmid r}} \left(1 - \frac{\left(\frac{-1}{q}\right) q + 3}{(q-1)(q^2-1)} + \frac{2}{(q^2-1)(q-1)} \right) \\
&\cdot \prod_{\substack{q,\text{odd}\\ q\mid B\\ q\mid r}} \left(1 + \frac{\left(\frac{-1}{q}\right) - \left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1} q^{-2\mathrm{ord}_q(B)}}{q^2 - \left(\frac{-1}{q}\right)} + \frac{\left(\frac{-1}{q}\right)^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}(q - \left(\frac{-1}{q}\right))} \right) \\
&\cdot \prod_{\substack{q,\text{odd}\\ q\mid B\\ q\nmid r}} \left(1 + \sum_{\alpha\ge 1} \frac{c_1(q^\alpha)}{q^{2\alpha}} \right. \\
&\left. + \frac{d_q(1)}{f_q} \sum_{\beta\ge 1} \frac{1}{q^{3\beta}} \left(1 + \sum_{\alpha \ge 1} \frac{2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)}, q^\alpha\right)} c_{q^\beta}(q^\alpha)}{q^{2\alpha} 2^{\nu\left(\frac{q^\beta}{(q^\beta,B)}, q^\alpha\right)}} \right) \right)
\end{aligned}
\tag{43}
$$

For the computation of the last product we use the following notation.

$$
\Delta = r^2 - 4A^2 \qquad \Delta_q = \mathrm{ord}_q(\Delta) \qquad L_q = \left(\frac{r^2 - 4A^2}{q}\right)
$$

Using Lemma 6.2 for the value of $c_1(q^\alpha)$ we have,

$$
\begin{aligned}
&1 + \sum_{\alpha\ge 1} \frac{c_1(q^\alpha)}{q^{2\alpha}} \\
&= 1 + \sum_{1\le\alpha\le \mathrm{ord}_q(B)} \frac{c_1(q^\alpha)}{q^{2\alpha}} + \sum_{\mathrm{ord}_q(B)+1\le\alpha} \frac{c_1(q^\alpha)}{q^{2\alpha}} \\
&= 1 + \sum_{1\le\alpha\le \mathrm{ord}_q(B)} \frac{1}{q^{2\alpha}} L_q^\alpha + \sum_{\mathrm{ord}_q(B)+1\le\alpha} \frac{L_q^\alpha}{q^{\alpha+\mathrm{ord}_q(B)}} \\
&= \begin{cases} 1 + \frac{L_q q^{2\mathrm{ord}_q(B)} - L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)+2} - L_q q^{2\mathrm{ord}_q(B)}} + \frac{L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}(q-L_q)} & \text{if } \Delta_q = 0 \\ 1 & \text{if } \Delta_q > 0. \end{cases}
\end{aligned}
$$

We now deal with the remaining double sum in the fourth product. We first write the double sum as

$$
\frac{d_q(1)}{f_q} \sum_{\beta\ge 1} \frac{1}{q^{3\beta}} \left(1 + \sum_{\alpha\ge 1} \frac{2^{\nu\left(\frac{(q^\beta,B^2)}{(q^\beta,B)}, q^\alpha\right)} c_{q^\beta}(q^\alpha)}{q^{2\alpha} 2^{\nu\left(\frac{q^\beta}{(q^\beta,B)}, q^\alpha\right)}} \right) = \frac{d_q(1)}{f_q} \sum_{\beta\ge 1} \frac{1}{q^{3\beta}} \left(1 + \sum_{\alpha\ge 1} \frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}} \right)
$$

Now we split the sum on $\beta \geq 1$ according to Lemma 6.2 (2) and simplify. Then the double sum becomes

$$\begin{aligned}
&\frac{d_q(1)}{f_q} \sum_{\beta \geq 1} \frac{\phi((B, q^{2\beta}))}{q^{\beta}\phi(q^{2\beta})(B, q^{2\beta})} \sum_{\alpha \geq 0} \frac{\phi((q^{\alpha}, Bq^{2\beta}))c_{q^{\beta}}(q^{\alpha})}{q^{\alpha}\phi(q^{\alpha})(q^{\alpha}, 4Bq^{2\beta})} \\
&= \frac{d_q(1)}{f_q} \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)} \frac{1}{q^{3\beta}} \left[1 + \sum_{\alpha \geq 1} \frac{c_{q^{\beta}}(q^{\alpha})}{q^{2\alpha}}\right] \\
&+ \frac{d_q(1)}{f_q} \sum_{2\beta \geq \min(\mathrm{ord}_q(B),\Delta_q)} \frac{1}{q^{3\beta}} \left[1 + \sum_{\alpha \geq 1} \frac{c_{q^{\beta}}(q^{\alpha})}{q^{2\alpha}}\right]
\end{aligned} \tag{44}$$

To evaluate this double sum we first make the following two observations

(1) By the definition of f_q,

$$\frac{d_q(1)}{f_q} = \begin{cases} 0 & \text{if } d_q(1) = 0 \\ 1 & \text{if } d_q(1) \neq 0. \end{cases}$$

(2) Let $\mathrm{ord}_q(k) = \beta$. Note that since

$$d_q(1) = 0 \iff (B, q^{2\beta}) \nmid \Delta$$

we have

$$\frac{d_q(1)}{f_q} = 0 \iff \min(\mathrm{ord}_q(B), 2\beta) > \Delta_q.$$

Therefore, we examine three cases. Note that $\beta \geq 1$ and $\mathrm{ord}_q(B) \geq 1$.
Case 1: $\Delta_q = 0$
In this case $\frac{d_q(1)}{f_q} = 0$. Therefore the last product in (43) is

$$\prod_{\substack{q,\mathrm{odd} \\ q|B \\ q\nmid r}} \left(1 + \frac{L_q q^{2\mathrm{ord}_q(B)} - L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)+2} - L_q q^{2\mathrm{ord}_q(B)}} + \frac{L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)}(q - L_q)}\right).$$

Case 2: $1 \leq \mathrm{ord}_q(B) \leq \Delta_q$
In this case $\frac{d_q(1)}{f_q} = 1$. Since $c_{q^{\beta}}(q^{\alpha}) = 0$ whenever $2\beta < \Delta_q$, (44) becomes

$$\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}} [1 + 0] + \sum_{2\beta \geq \min(\mathrm{ord}_q(B),\Delta_q)=\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}} \left[1 + \sum_{\alpha \geq 1} \frac{c_{q^{\beta}}(q^{\alpha})}{q^{2\alpha}}\right].$$

The first sum is

$$\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\mathrm{ord}_q(B)} \frac{1}{q^{3\beta}} = \frac{1 - q^{-3\left\lceil \frac{\mathrm{ord}_q(B)}{2} - 1\right\rceil}}{q^3 - 1}.$$

Using Lemma 6.2 (2a) to obtain $c_{q^\beta}(q^\alpha)$ for $2\beta \geq \mathrm{ord}_q(B)$ the second sum is

$$\begin{aligned}
&\sum_{2\beta\geq \mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1+\sum_{\substack{\alpha\geq 1\\ \alpha \text{ even}}} \frac{q^{\mathrm{ord}_q(B)}\phi(q^\alpha)}{q^{2\alpha}}\right]\\
&= \sum_{2\beta\geq \mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1+\sum_{\substack{\alpha\geq 1\\ \alpha \text{ even}}} \frac{q-1}{q^{\alpha+1}} q^{\mathrm{ord}_q(B)}\right]\\
&= \sum_{2\beta\geq \mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\left[1+\frac{q^{\mathrm{ord}_q(B)}}{q(q+1)}\right]\\
&= \left(\frac{q(q+1)+q^{\mathrm{ord}_q(B)}}{q(q+1)}\right)\sum_{2\beta\geq \mathrm{ord}_q(B)} \frac{1}{q^{3\beta}}\\
&= \frac{(q^2+q+q^{\mathrm{ord}_q(B)})q^{2-2\left\lceil \frac{\mathrm{ord}_q(B)}{2}\right\rceil}}{(q+1)(q^3-1)}
\end{aligned}$$

Therefore, in the case that $1 \leq \mathrm{ord}_q(B) \leq \Delta_q$ we may write the last product in (43) as

$$\prod_{\substack{q,\text{odd}\\ q\mid B\\ q\nmid r}} \left(1+\frac{1-q^{-3\left\lceil \frac{\mathrm{ord}_q(B)}{2}-1\right\rceil}}{q^3-1}+\frac{(q^2+q+q^{\mathrm{ord}_q(B)})q^{2-2\left\lceil \frac{\mathrm{ord}_q(B)}{2}\right\rceil}}{(q+1)(q^3-1)}\right)$$

Case 3: $\mathrm{ord}_q(B) > \Delta_q > 0$

We examine carefully the two sums in (44). In order to determine $\frac{d_q(1)}{f_q}$, we examine $\min(\mathrm{ord}_q(B), 2\beta)$ by using observation 2 on page 63.

(1) In the first sum we sum over $1 < 2\beta < \min(\mathrm{ord}_q(B), \Delta_q) = \Delta_q$.

$$\frac{d_q(1)}{f_q} = \begin{cases} 1 & \text{if } \min(\mathrm{ord}_q(B), 2\beta) = 2\beta \\ 0 & \text{if } \min(\mathrm{ord}_q(B), 2\beta) = \mathrm{ord}_q(B). \end{cases}$$

By Lemma 6.2 2(b), $c_{q^\beta}(q^\alpha) = 0$, since $\Delta_q > 2\beta$. Therefore, the first sum becomes

$$\begin{aligned}
&\frac{d_q(1)}{f_q}\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q} \frac{1}{q^{3\beta}}[1+0]\\
&= \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q} \frac{1}{q^{3\beta}}
\end{aligned}$$

(2) In the second sum we sum over $2\beta \geq \min(\mathrm{ord}_q(B), \Delta_q) = \Delta_q$. If $\min(\mathrm{ord}_q(B), 2\beta) = \mathrm{ord}_q(B)$, then $d_q(1)/f_q = 0$. If $\min(\mathrm{ord}_q(B), 2\beta) = 2\beta$, then $d_q(1)/f_q = 1$ if and only if $2\beta = \Delta_q$, since $2\beta \geq \Delta_q$ For the second sum we also include the sum on $\alpha \geq 1$, since if $2\beta = \Delta_q$, then $c_{q^\beta}(q^\alpha) \neq 0$, by Lemma 6.2 2(b). Therefore, the second sum becomes

$$
\begin{aligned}
&\frac{d_q(1)}{f_q}\sum_{2\beta\geq\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q}\frac{1}{q^{3\beta}}\left[1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right]\\
&=\frac{d_q(1)}{f_q}\sum_{\beta=\lceil\frac{\Delta_q}{2}\rceil}^{\infty}\frac{1}{q^{3\beta}}\left[1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right]\\
&=\begin{cases}\frac{1}{q^{3\Delta_q/2}}\left[1+\sum_{\alpha\geq 1}\frac{q^{\alpha-\min(\alpha,\mathrm{ord}_q(B)-\Delta_q)}\gamma_q^\alpha}{q^{2\alpha}}\right] & \text{if } \Delta_q\equiv 0 \pmod 2\\ 0 & \text{otherwise.}\end{cases}
\end{aligned}
$$

where

$$
\gamma_q=\left(\frac{\Delta/q^{\Delta_q}}{q}\right).
$$

Therefore, (44) on page 63 becomes

$$
\begin{aligned}
&\frac{d_q(1)}{f_q}\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)}\frac{1}{q^{3\beta}}\left[1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right]\\
&\qquad\qquad+\frac{d_q(1)}{f_q}\sum_{2\beta\geq\min(\mathrm{ord}_q(B),\Delta_q)}\frac{1}{q^{3\beta}}\left[1+\sum_{\alpha\geq 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}}\right]\\
&=\begin{cases}\begin{array}{c}\sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q}\frac{1}{q^{3\beta}}\\ +q^{-3\Delta_q/2}\left[1+\sum_{\alpha\geq 1}q^{-\alpha-\min(\alpha,\mathrm{ord}_p(B)-\Delta_q)}\gamma_q^\alpha\right]\end{array} & \text{if } \Delta_q\equiv 0 \pmod 2\\ \sum_{1<2\beta<\min(\mathrm{ord}_q(B),\Delta_q)=\Delta_q}\frac{1}{q^{3\beta}} & \text{if } \Delta_q\equiv 1 \pmod 2.\end{cases}
\end{aligned}
$$

Therefore, if $\Delta_q\equiv 0 \pmod 2$ the double sum (44) simplifies to

$$
\frac{1-q^{-3(\Delta_q/2-1)}}{q^3-1}+\frac{1}{q^{3\Delta_q/2}}\left[1+\gamma_q\left[\frac{(q^{2(\mathrm{ord}_q(B)-\Delta_q)}-\gamma_q^{\mathrm{ord}_q(B)-\Delta_q})(q-\gamma_q)+\gamma_q^{\mathrm{ord}_q(B)-\Delta_q}(q^2-\gamma_q)}{q^{2(\mathrm{ord}_q(B)-\Delta_q)}(q-\gamma_q)(q^2-\gamma_q)}\right]\right].
$$

If $\Delta_q\equiv 1 \pmod 2$ the double sum (44) simplifies to

$$
\frac{1-q^{-3\lceil\Delta_q/2-1\rceil}}{q^3-1}.
$$

We have shown that

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

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

$$\cdot \prod_{\substack{q,\text{odd} \\ q|B \\ q\nmid r \\ \Delta_q=0}} \left(1 + \frac{L_q q^{2\mathrm{ord}_q(B)} - L_q^{\mathrm{ord}_q(B)+1}}{q^{2\mathrm{ord}_q(B)+2} - L_q q^{2\mathrm{ord}_q(B)}} + \frac{L_q^{\mathrm{ord}_q(B)+1}}{q - L_q} \right)$$

$$\cdot \prod_{\substack{q,\text{odd} \\ q\in\mathfrak{P}^{\leq}_{r,A,B}}} \left(1 + \frac{1 - q^{-3\left\lceil \frac{\mathrm{ord}_q(B)}{2} - 1 \right\rceil}}{q^3-1} + \frac{(q^2+q+q^{\mathrm{ord}_q(B)})q^{2-2\left\lceil \frac{\mathrm{ord}_q(B)}{2} \right\rceil}}{(q+1)(q^3-1)} \right)$$

$$\cdot \prod_{\substack{q,\text{odd} \\ q\in\mathfrak{P}^{>}_{r,A,B} \\ \Delta_q\equiv 1 \pmod 2}} \left(\frac{1 - q^{-3\lceil \Delta_q/2 - 1 \rceil}}{q^3-1} \right)$$

$$\cdot \prod_{\substack{q,\text{odd} \\ q\in\mathfrak{P}^{>}_{r,A,B} \\ \Delta_q\equiv 0 \pmod 2}} \left(\frac{1 - q^{-3(\Delta_q/2-1)}}{q^3-1} + \right.$$

$$\left. \frac{1}{q^{3\Delta_q/2}} \left[1 + \gamma_q \left[\frac{(q^{2(\mathrm{ord}_q(B)-\Delta_q)} - \gamma_q^{\mathrm{ord}_q(B)-\Delta_q})(q-\gamma_q) + \gamma_q^{\mathrm{ord}_q(B)-\Delta_q}(q^2-\gamma_q)}{q^{2(\mathrm{ord}_q(B)-\Delta_q)}(q-\gamma_q)(q^2-\gamma_q)} \right] \right] \right)$$

where

$$\mathfrak{P}^{\leq}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \mathrm{ord}_q(B) \leq \Delta_q\} \quad \text{and}$$
$$\mathfrak{P}^{>}_{r,A,B} = \{q > 2, \text{prime} : q|B; q \nmid r; \mathrm{ord}_q(B) > \Delta_q > 0\}.$$

This completes the proof of Lemma 0.9.

$\square$