ACTA ARITHMETICA
149.3 (2011)

Average Frobenius distributions for elliptic curves over abelian extensions

by

Neil Calkin (Clemson, SC), Bryan Faulkner (Ferrum, VA),
Kevin James (Clemson, SC), Matt King,
and David Penniston (Oshkosh, WI)

This paper is dedicated to the memory of our coauthor Matt King

1. Introduction and statement of results. Let E be an elliptic curve defined over a number field K. Set $[K:\mathbb{Q}] = m$ and denote by $\mathcal{O}_K$ the ring of integers of K. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal which lies above the rational prime $p \in \mathbb{Z}$, and denote by $\deg_K(\mathfrak{p})$ the degree of $\mathfrak{p}$. If E has good reduction at $\mathfrak{p}$, then we may consider E over the finite field $\mathcal{O}_K/\mathfrak{p}$. If we denote by $a_\mathfrak{p}(E)$ the trace of the Frobenius morphism, then 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 $N(\mathfrak{p}) = p^{\deg_K(\mathfrak{p})}$ is the number of elements of $\mathcal{O}_K/\mathfrak{p}$. Moreover, we have the Hasse bound

$$|a_\mathfrak{p}(E)| \le 2\sqrt{N(\mathfrak{p})}.$$

Let $r, f \in \mathbb{Z}$ with $f > 0$. Define

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

and let

$$\pi_{1/2}(x) := \int_2^x \frac{dt}{2\sqrt{t}\log t}.$$

In the case that $K = \mathbb{Q}$, Lang and Trotter [12] made the following conjecture.

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11R20.
Key words and phrases: distribution of primes, Frobenius distributions, Lang–Trotter conjecture, abelian extensions.

DOI: 10.4064/aa149-3-2

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

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

Although the Lang–Trotter Conjecture remains open, there are many partial results. For example, Elkies [7] proved that for any elliptic curve $E/\mathbb{Q}$ there are infinitely many primes p such that $a_p(E) = 0$. Moreover, there are several results which verify that the conjecture is true in an average sense over families of elliptic curves defined over $\mathbb{Q}$ (see [1], [3], [4], [8], [9], [10]). For $K \neq \mathbb{Q}$, less is known. In [5] David and Pappalardi proved the following result.

THEOREM 1.2. *Let $K = \mathbb{Q}(i)$, and let $\mathcal{S}_x$ 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 $\max\{|a_1|, |a_2|, |b_1|, |b_2|\} \leq x \log x$. If $r \neq 0$, then*

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

where

$$c_r = \frac{1}{3\pi} \prod_{\substack{q \text{ prime} \\ q>2}} \frac{q\big(q - 1 - \big(\frac{-r^2}{q}\big)\big)}{(q-1)\big(q - \big(\frac{-1}{q}\big)\big)}.$$

If $r = 0$, then

$$\frac{1}{|\mathcal{S}_x|} \sum_{E \in \mathcal{S}_x} \pi_E^{0,2}(x) = O(1).$$

In this paper we generalize David and Pappalardi's result as follows. Let $\{\alpha_1, \ldots, \alpha_m\}$ be an integral basis for $\mathcal{O}_K$. Given $\vec{v} = (v_1, \ldots, v_m) \in \mathbb{Z}^m$, put $\|\vec{v}\| := \max_{1 \leq i \leq m} |v_i|$ and define $R(\vec{v}) := \sum_{i=1}^m v_i \alpha_i$. For $\vec{v}, \vec{w} \in \mathbb{Z}^m$ we write $E_{\vec{v},\vec{w}}$ for the curve

$$E_{\vec{v},\vec{w}} : y^2 = x^3 + R(\vec{v})x + R(\vec{w}) \tag{1}$$

with discriminant $\Delta_{\vec{v},\vec{w}} = -16[4R(\vec{v})^3 + 27R(\vec{w})^2]$, and for $t \in \mathbb{R}_{>0}$ we let

$$\mathcal{C}_t := \{(\vec{v}, \vec{w}) \in (\mathbb{Z}^m)^2 : \|\vec{v}\|, \|\vec{w}\| \leq t \text{ and } \Delta_{\vec{v},\vec{w}} \neq 0\}.$$

In this paper we prove the following theorem (the case of even r can be handled in a similar way).

THEOREM 1.3. *Suppose K is an abelian number field and r is an odd integer. Then there are explicit constants $D_{r,1,K}$ and $D_{r,2,K}$ (see Section 2 for details) such that for any $\epsilon > 0$,*

$$\frac{1}{|\mathcal{C}_t|}\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,f}_{E_{\vec{v},\vec{w}}}(x)$$
$$\sim\begin{cases} D_{r,1,K}\cdot\pi_{1/2}(x) & \text{if } f=1 \text{ and } t\gg x\log^{2+\epsilon}x,\\ D_{r,2,K}\log\log x & \text{if } f=2,\ m \text{ is even and } t\gg\sqrt{x}\log x.\end{cases}$$

Moreover, if $f\geq 3$, $f\,|\,m$ *and* $t\geq x^{1/f}$, *then*

$$\frac{1}{|\mathcal{C}_t|}\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,f}_{E_{\vec{v},\vec{w}}}(x)=O(1).$$

REMARK 1.4. While we have not pursued this, it would be interesting to have an explicit expression for the error term in the $f\geq 3$ case of Theorem 1.3.

The organization of the paper is as follows. In Section 2 we state Theorem 2.2, which is a more precise version of Theorem 1.3, and show that it follows from three key lemmas. Lemma 2.3, which is proved in Section 4, relates the desired average of the main theorem to a weighted sum of special values of L-series. Lemma 2.4, which is proved in Section 6, gives estimates for this weighted sum. Finally, Lemma 2.5, which is proved in Section 8, gives an Euler product representation for one of the constants appearing in Lemma 2.4. Sections 3, 5 and 7 contain various technical results which are essential to our proofs of the three key lemmas.

2. Proof of main theorem. In this section we prove a more precise version of Theorem 1.3. Let $r,f,A,B\in\mathbb{Z}$ with r odd, $f,A,B>0$ and $(A,B)=1$. Define $\Delta^{r,A,f}:=r^2-4A^f$, and for q prime let

$$\Delta_q=\Delta_q^{r,A,f}:=\operatorname{ord}_q(\Delta^{r,A,f}),\qquad B_q:=\operatorname{ord}_q(B)$$

and

$$\gamma_q=\gamma_{r,A,f,q}:=\left(\frac{\Delta^{r,A,f}/q^{\Delta_q}}{q}\right).$$

Put

$$\mathfrak{Q}^{<}_{r,A,B,f}:=\{q \text{ prime} : q\,|\,B,\ q\nmid 2r \text{ and } 0<\Delta_q<B_q\},$$
$$\mathfrak{Q}^{\geq}_{r,A,B,f}:=\{q \text{ prime} : q\,|\,B,\ q\nmid 2r \text{ and } \Delta_q\geq B_q\},$$

and for $q\in\mathfrak{Q}^{<}_{r,A,B,f}$ let

$$\Gamma_q:=\begin{cases}\gamma_q & \text{if } \Delta_q \text{ is even,}\\ 0 & \text{if } \Delta_q \text{ is odd.}\end{cases}$$

We define constants for use in the cases $f = 1$ and $f = 2$ respectively as follows:

$$\begin{aligned} k_{r,A,B} := & \prod_{\substack{q \mid B \\ q \nmid 2r\Delta^{r,A,1}}} \frac{q(q+\gamma_q)}{q^2-1} \\ & \times \prod_{q \in \mathfrak{Q}^{<}_{r,A,B,1}} \left(1 + \frac{\Gamma_q(q\Gamma_q+1)}{q^{\Delta_q/2-1}(q^2-1)} + \frac{\Gamma_q^2(q^{\Delta_q/2-1}-1)}{q^{\Delta_q/2-1}(q-1)}\right) \\ & \times \prod_{q \in \mathfrak{Q}^{\geq}_{r,A,B,1}} \left(\frac{q^{\lfloor (B_q+1)/2 \rfloor}-1}{q^{\lfloor (B_q-1)/2 \rfloor}(q-1)} + \frac{q^{B_q+2}}{q^{3\lfloor (B_q+1)/2 \rfloor}(q^2-1)}\right) \\ & \times \prod_{\substack{q \mid B \\ q \mid r}} \frac{q(q+\gamma_q)}{q^2-1}, \\ c_{r,A,B} := & \prod_{\substack{q \mid B \\ q \nmid 2r\Delta^{r,A,2}}} \left(\frac{q}{q-\gamma_q}\right) \prod_{\substack{q \in \mathfrak{Q}^{<}_{r,A,B} \\ 2 \nmid \Delta_q}} \left(\frac{q^{\lfloor \Delta_q/2 \rfloor+1}-1}{q^{\lfloor \Delta_q/2 \rfloor}(q-1)}\right) \\ & \times \prod_{\substack{q \in \mathfrak{Q}^{<}_{r,A,B} \\ 2 \mid \Delta_q}} \left(\frac{q^{\Delta_q/2}(q-\gamma_q)+\gamma_q-1}{q^{\Delta_q/2-1}(q-1)(q-\gamma_q)}\right) \\ & \times \prod_{q \in \mathfrak{Q}^{\geq}_{r,A,B}} \left(\frac{q^{2\lceil B_q/2 \rceil+1}(q+1)(q^{\lceil B_q/2 \rceil}-1)+q^{B_q+2}}{q^{3\lceil B_q/2 \rceil}(q^2-1)}\right) \\ & \times \prod_{\substack{q \mid B \\ q \mid r}} \left(\frac{q}{q-\gamma_q}\right). \end{aligned}$$

Next we recall a classical result which gives a useful characterization of abelian number fields.

FACT 2.1. *Let $K/\mathbb{Q}$ be a Galois number field. Then K is abelian if and only if there exists an integer B_K such that $\deg_K(\mathfrak{p})$ depends only on the residue class of p modulo B_K.*

Suppose from now on that K is abelian. For B_K as above and $f \mid m$, let $a_{f,1}, \ldots, a_{f,\ell_f}$ be positive integer representatives of the reduced residue classes modulo B_K that contain rational primes p which are unramified in K and split into degree f primes in $\mathcal{O}_K$. Define

$$D_{r,1,K} := \frac{4m}{3\pi\phi(B_K)} \prod_{\substack{q\nmid B_K \\ q\mid r}} \left(\frac{q^2}{q^2-1}\right) \prod_{q\nmid 2rB_K} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \sum_{i=1}^{\ell_1} k_{r,a_{1,i},B_K},$$

and if m is even let

$$D_{r,2,K} := \frac{m}{3\pi\phi(B_K)} \prod_{\substack{q\nmid B_K \\ q\mid r}} \left(\frac{q}{q-\left(\frac{-1}{q}\right)}\right) \times \prod_{q\nmid 2rB_K} \left(\frac{q\left(q^2-q-1-\left(\frac{-1}{q}\right)\right)}{(q-1)(q^2-1)}\right) \sum_{i=1}^{\ell_2} c_{r,a_{2,i},B_K}.$$

We now state our main result.

THEOREM 2.2. *Let K be an abelian number field, and suppose $t \geq x^{1/f}$. Then*

$$\frac{1}{|\mathcal{C}_t|} \sum_{(\vec{v},\vec{w})\in\mathcal{C}_t} \pi^{r,1}_{E_{\vec{v},\vec{w}}}(x) = D_{r,1,K}\cdot\pi_{1/2}(x) + O\left(\frac{\sqrt{x}}{\log^{c+1} x} + \frac{x^{3/2}\log x}{t}\right)$$

for any $c>0$, and if m is even,

$$\frac{1}{|\mathcal{C}_t|} \sum_{(\vec{v},\vec{w})\in\mathcal{C}_t} \pi^{r,2}_{E_{\vec{v},\vec{w}}}(x) = D_{r,2,K}\log\log x + O\left(1+\frac{\sqrt{x}\log x}{t}\right).$$

Moreover, if $f\geq 3$ and $f\mid m$, then

$$\frac{1}{|\mathcal{C}_t|} \sum_{(\vec{v},\vec{w})\in\mathcal{C}_t} \pi^{r,f}_{E_{\vec{v},\vec{w}}}(x) = O(1).$$

Recall that if χ is a Dirichlet character, we have the Dirichlet L-series

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Given an integer d we let χ_d be the Kronecker character $\chi_d(\bullet) = \left(\frac{d}{\bullet}\right)$. Set

$$B(r) := \max\{3, r^2/4, \Delta_K\},$$

where Δ_K is the discriminant of K, and for k any positive integer let

$$d_k(p) = d_{k,r,f}(p) := \begin{cases} (r^2-4p^f)/k^2 & \text{if } k^2 \mid r^2-4p^f, \\ 0 & \text{otherwise.} \end{cases}$$

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

LEMMA 2.3. *If $f \mid m$ and $t \ge x^{1/f}$, then*

$$\frac{1}{|\mathcal{C}_t|}\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,f}_{E_{\vec{v},\vec{w}}}(x)$$

$$= \frac{m}{\pi}\Bigg[\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{\ell_f}\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\p\equiv a_{f,i}\,(\mathrm{mod}\,B_K)\\k^2\mid r^2-4p^f}} L(1,\chi_{d_k(p)})\log p$$

$$-\sum_{i=1}^{\ell_f}\int_{B(r)^f}^{x}\sum_{\substack{k\le 2\sqrt{S}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le S^{1/f}\\p\equiv a_{f,i}\,(\mathrm{mod}\,B_K)\\k^2\mid r^2-4p^f}} L(1,\chi_{d_k(p)})$$

$$\times\log p\,\frac{d}{dS}\left(\frac{1}{\sqrt{S}\log S}\right)dS\Bigg] + \mathcal{E}(x,t),$$

where

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

The next lemma consists of a result of James [11, Proposition 2.1] and a straightforward generalization of a result of David and Pappalardi [5, Lemma 2.2]. Denote by $[C,D]$ the least common multiple of C and D, and let

$$K_{r,A,B} := \sum_{k\in\mathbb{N}}\frac{1}{k}\sum_{n\in\mathbb{N}}\frac{\kappa_k^{r,A,B}(n)}{n\phi([B,nk^2])},$$

where

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

Also, let

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

where

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

Then we have the following estimates for the weighted sums of L-series appearing in Lemma 2.3.

LEMMA 2.4. *For every $c > 0$,*

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

Our third lemma gives an Euler product expansion for the constant appearing in the $f = 2$ case of Lemma 2.4 (for the $f = 1$ case see [11, Theorem 1.1]).

LEMMA 2.5. *We have*

$$C_{r,A,B} = \frac{2}{3\phi(B)}\prod_{\substack{q\nmid B\\ q\mid r}}\left(\frac{q}{q-\left(\frac{-1}{q}\right)}\right)\prod_{q\nmid 2rB}\left(\frac{q\left(q^2-q-1-\left(\frac{-1}{q}\right)\right)}{(q-1)(q^2-1)}\right)c_{r,A,B}.$$

Proof of Theorem 2.2. First suppose $f = 1$. We combine Lemmas 2.3 and 2.4 to obtain

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}&\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,1}_{E_{\vec{v},\vec{w}}}(x)\\ &= \frac{m}{\pi}\left[\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{\ell_1}\left(K_{r,a_{1,i},B_K}\cdot x + O\left(\frac{x}{\log^c x}\right)\right)\right.\\ &\quad\left.-\sum_{i=1}^{\ell_1}\int_{B(r)}^{x}\left(K_{r,a_{1,i},B_K}\cdot S + O\left(\frac{S}{\log^c S}\right)\right)\frac{d}{dS}\left(\frac{1}{\sqrt{S}\log S}\right)dS\right]\\ &\quad + O\left(\log\log x + \frac{x^{3/2}\log x}{t}\right).\end{aligned}$$

In [11] James proved that

$$K_{r,A,B} = \frac{2}{3\phi(B)}\prod_{\substack{q\nmid B\\ q\mid r}}\left(\frac{q^2}{q^2-1}\right)\prod_{q\nmid 2rB}\frac{q(q^2-q-1)}{(q+1)(q-1)^2}\,k_{r,A,B},$$

and thus $\sum_{i=1}^{\ell_1} K_{r,a_{1,i},B_K} = \pi D_{r,1,K}/2m$. Moreover, one can show that

$$\int_{B(r)}^{x}\frac{S}{\log^c S}\cdot\frac{d}{dS}\left(\frac{1}{\sqrt{S}\log S}\right)dS = O\left(\frac{\sqrt{x}}{\log^{c+1} x}\right),$$

which yields

$$\frac{1}{|\mathcal{C}_t|}\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,1}_{E_{\vec{v},\vec{w}}}(x)=\frac{D_{r,1,K}}{2}\left[\frac{\sqrt{x}}{\log x}-\int_2^x S\,\frac{d}{dS}\left(\frac{1}{\sqrt{S}\log S}\right)dS\right]+O\left(\frac{\sqrt{x}}{\log^{c+1}x}+\frac{x^{3/2}\log x}{t}\right).$$

Integrating by parts gives

$$\int_2^x S\,\frac{d}{dS}\left(\frac{1}{\sqrt{S}\log S}\right)dS=\frac{\sqrt{x}}{\log x}-\frac{\sqrt{2}}{\log 2}-2\pi_{1/2}(x),$$

and our result follows.

Now suppose $f=2$. Here Lemmas 2.3 and 2.4 yield

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}&\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,2}_{E_{\vec{v},\vec{w}}}(x)\\&=\frac{m}{\pi}\left[\frac{1}{\sqrt{x}\log x}\sum_{i=1}^{\ell_2}\left(C_{r,a_{2,i},B_K}\cdot\sqrt{x}+O\left(\frac{\sqrt{x}}{\log^c x}\right)\right)\right.\\&\quad\left.-\sum_{i=1}^{\ell_2}\int_{B(r)^2}^{x}\left(C_{r,a_{2,i},B_K}\cdot\sqrt{S}+O\left(\frac{\sqrt{S}}{\log^c S}\right)\right)\frac{d}{dS}\left(\frac{1}{\sqrt{S}\log S}\right)dS\right]\\&\quad+O\left(1+\frac{\sqrt{x}\log x}{t}\right).\end{aligned}$$

It is easy to see that the first term in the brackets is $O(1)$. Moreover, integrating by parts gives

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

and

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

Therefore

$$\frac{1}{|\mathcal{C}_t|}\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,2}_{E_{\vec{v},\vec{w}}}(x)=\frac{m}{2\pi}\left(\sum_{i=1}^{\ell_2}C_{r,a_{2,i},B_K}\right)\log\log x+O\left(1+\frac{\sqrt{x}\log x}{t}\right),$$

and since Lemma 2.5 implies that

$$\sum_{i=1}^{\ell_2}C_{r,a_{2,i},B_K}=\frac{2\pi D_{r,2,K}}{m},$$

our result follows.

Finally, suppose $f \geq 3$. By (9) and (10) below, it suffices to show that the sum on the right hand side of (9) is $O(1)$; however, this follows easily from (7). ∎

3. Counting curves. In this section we gather results that will aid us in estimating the number of $(\vec{v}, \vec{w}) \in \mathcal{C}_t$ such that $E_{\vec{v},\vec{w}}$ reduces to a given elliptic curve.

Note first that $\#\{n \in \mathbb{Z} : |n| \leq t\} = 2t + O(1)$. Moreover, given $\vec{v} \in \mathbb{Z}^m$ there are at most two values of $\vec{w} \in \mathbb{Z}^m$ such that $\Delta_{\vec{v},\vec{w}} = 0$. It follows that

$$|\mathcal{C}_t| = 4^m t^{2m} + O(t^{2m-1}). \tag{3}$$

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal of degree f which lies above an unramified rational prime $p > 3$. Recall (see [16]) that in order to reduce an elliptic curve E/K modulo $\mathfrak{p}$ one first obtains a minimal model for the curve at $\mathfrak{p}$, and then reduces the coefficients of this model modulo $\mathfrak{p}$. We denote the resulting curve by $E^{\mathfrak{p}}$, and for $\gamma \in \mathcal{O}_K$ we denote by $\gamma^{\mathfrak{p}}$ its image in $\mathcal{O}_K/\mathfrak{p}$. In order to obtain our estimate we will use the fact that if $\mathrm{ord}_{\mathfrak{p}}(R(\vec{v})) < 4$ or $\mathrm{ord}_{\mathfrak{p}}(R(\vec{w})) < 6$, then the model (1) of $E_{\vec{v},\vec{w}}$ is minimal at $\mathfrak{p}$.

Next note that since

$$p\mathcal{O}_K \subseteq \mathfrak{p} \subseteq \mathcal{O}_K,$$

we have

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

and therefore

$$|\mathfrak{p}/p\mathcal{O}_K| = p^{m-f}.$$

Set $s = p^{m-f}$, and suppose $\{\rho_1, \ldots, \rho_s\}$ is a complete set of distinct coset representatives for $\mathfrak{p}/p\mathcal{O}_K$. Fix $\gamma \in \mathcal{O}_K$. Then for $\vec{v} \in \mathbb{Z}^m$ we have

$$R(\vec{v}) \equiv \gamma \pmod{\mathfrak{p}} \;\Leftrightarrow\; R(\vec{v}) - \gamma \equiv \rho_i \pmod{p\mathcal{O}_K} \text{ for some } 1 \leq i \leq s.$$

If we define, for each $1 \leq i \leq s$, integers $c_{i,j}$ $(1 \leq j \leq m)$ by $\gamma + \rho_i = \sum_{j=1}^{m} c_{i,j}\alpha_j$, then

$$\begin{aligned} \#\{\vec{v} \in \mathbb{Z}^m : \|\vec{v}\| \leq t \text{ and } R(\vec{v})^{\mathfrak{p}} = \gamma^{\mathfrak{p}}\} &= \sum_{i=1}^{s} \#\{(k_1, \ldots, k_m) \in \mathbb{Z}^m : |c_{i,j} + pk_j| \leq t \text{ for all } 1 \leq j \leq m\} \\ &= \frac{2^m t^m}{p^f} + O\left(\frac{t^{m-1}}{p^{f-1}}\right) \end{aligned} \tag{4}$$

when $t \geq p$.

4. The average in terms of L-series. In this section we prove Lemma 2.3. We begin by recalling the Hurwitz class number (see, for example, [13]), which is a weighted sum over the equivalence classes of binary quadratic forms $f(x,y) = ax^2 + bxy + cy^2$ of a given discriminant. More precisely, if we let $\Delta_f = b^2 - 4ac$ denote the discriminant of f, then for $\Delta > 0$,

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

where

$$c_f = \begin{cases} 1/2 & \text{if some } g \in [f] \text{ is proportional to } x^2 + y^2, \\ 1/3 & \text{if some } g \in [f] \text{ is proportional to } x^2 + xy + y^2, \\ 1 & \text{otherwise.} \end{cases}$$

The Kronecker class number $K(-\Delta)$, meanwhile, is simply the number of equivalence classes of binary quadratic forms of discriminant $-\Delta$. For our purposes it will be more convenient to work with $H(\Delta)$ (note that $H(\Delta) = K(-\Delta) + O(1)$). We recall (see [5]) that

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

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

$$h(d) = \frac{w(d)|d|^{1/2}}{2\pi} L(1, \chi_d). \tag{6}$$

Let $p > B(r)$ be prime. Then $4p^f - r^2 > 0$, and for a positive integer k with $k^2 \mid r^2 - 4p^f$ we have $L(1, \chi_{d_k(p)}) \ll \log p$ (see [13, p. 656]). Noting that $d_k(p) \equiv 1 \pmod 4$ since r is odd, we therefore obtain the following useful estimate:

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

Since $p > 3$, any elliptic curve over $\mathbb{F}_{p^f}$ may be written in the form

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

Recalling that $E_{a',b'} \cong E_{a,b}$ over $\mathbb{F}_{p^f}$ if and only if there exists $u \in \mathbb{F}_{p^f}^*$ such

that $a' = u^4 a$ and $b' = u^6 b$, it follows that

$$\#\{(a',b') \in \mathbb{F}_{p^f}^2 : E_{a',b'} \cong E_{a,b}\} = \begin{cases} (p^f-1)/6 & \text{if } a = 0 \text{ and } p^f \equiv 1 \pmod 3, \\ (p^f-1)/4 & \text{if } b = 0 \text{ and } p^f \equiv 1 \pmod 4, \\ (p^f-1)/2 & \text{otherwise.} \end{cases}$$

Following Schoof [15] 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 $\mathbb{F}_{p^f}$. Since $p \nmid r$, by Deuring's Theorem (see [6] or [15, Theorem 4.6]) we have

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

Letting

$$T_{p^f}(r) := \#\{(a,b) \in \mathbb{F}_{p^f}^2 : \#E_{a,b}(\mathbb{F}_{p^f}) = p^f + 1 - r\},$$

we get the following result.

THEOREM 4.1 (Deuring). $T_{p^f}(r) = (p^f/2) \cdot H(4p^f - r^2) + O(p^f)$.

Proof. Let $\tilde{E}$ denote an $\mathbb{F}_{p^f}$-isomorphism class of elliptic curves. Since there are at most ten isomorphism classes containing other than $(p^f-1)/2$ curves $E_{a,b}$, we have

$$T_{p^f}(r) = \sum_{a_{\mathfrak{p}}(\tilde{E})=r} \sum_{\substack{(a,b) \\ E_{a,b} \in \tilde{E}}} 1 = \frac{p^f - 1}{2} N(r) + O(p^f)$$

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

Our result now follows from (7). ∎

Proof of Lemma 2.3. Note first that

$$\frac{1}{|\mathcal{C}_t|} \sum_{(\vec{v},\vec{w}) \in \mathcal{C}_t} \pi^{r,f}_{E_{\vec{v},\vec{w}}}(x) = \frac{1}{|\mathcal{C}_t|} \sum_{(\vec{v},\vec{w}) \in \mathcal{C}_t} \sum_{\substack{N(\mathfrak{p}) \le x \\ \deg_K(\mathfrak{p}) = f \\ a_{\mathfrak{p}}(E_{\vec{v},\vec{w}}) = r}} 1$$

$$= \frac{1}{|\mathcal{C}_t|} \sum_{\substack{N(\mathfrak{p}) \le x \\ \deg_K(\mathfrak{p}) = f}} \sum_{\substack{(\vec{v},\vec{w}) \in \mathcal{C}_t \\ a_{\mathfrak{p}}(E_{\vec{v},\vec{w}}) = r}} 1.$$

For a prime ideal $\mathfrak{p}$ of degree f lying above a rational prime $p > B(r)$ we have

$$\sum_{\substack{(\vec{v},\vec{w}) \in \mathcal{C}_t \\ a_{\mathfrak{p}}(E_{\vec{v},\vec{w}}) = r}} 1 = \sum_{\substack{(a,b) \in \mathbb{F}_{p^f}^2 \\ \#E_{a,b}(\mathbb{F}_{p^f}) = p^f + 1 - r}} |\mathcal{C}_t(E_{a,b})|,$$

where

$$\mathcal{C}_t(E_{a,b}) := \{(\vec{v},\vec{w}) \in \mathcal{C}_t : E^{\mathfrak{p}}_{\vec{v},\vec{w}} = E_{a,b}\}.$$

If $E^{\mathfrak{p}}_{\vec{v},\vec{w}} = E_{a,b}$, then either $R(\vec{v})^{\mathfrak{p}} = a$ and $R(\vec{w})^{\mathfrak{p}} = b$, or the model (1) is not minimal at $\mathfrak{p}$. Since in the latter case we have $R(\vec{v})^{\mathfrak{p}} = R(\vec{w})^{\mathfrak{p}} = 0$, by (4) and Theorem 4.1 it follows that

$$\sum_{\substack{(\vec{v},\vec{w})\in\mathcal{C}_t \\ a_{\mathfrak{p}}(E_{\vec{v},\vec{w}})=r}} 1 = \left(\frac{4^m t^{2m}}{p^{2f}} + O\left(\frac{t^{2m-1}}{p^{2f-1}}\right)\right)\left(\frac{p^f}{2}H(4p^f - r^2) + O(p^f)\right)$$

for $t \geq p$.

Next note that the conditions $N(\mathfrak{p}) \leq x$ and $\deg_K(\mathfrak{p}) = f$ together imply that $p \leq x^{1/f}$. Then our assumption that $t \geq x^{1/f}$, along with (3) and the fact that the prime ideals $\mathfrak{p}$ lying above primes $p \leq B(r)$ do not affect our average, allows us to conclude that

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}&\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t} \pi^{r,f}_{E_{\vec{v},\vec{w}}}(x) \\ &= \sum_{\substack{B(r)^f < N(\mathfrak{p}) \leq x \\ \deg_K(\mathfrak{p})=f}} \left[\left(\frac{1}{4^m t^{2m}} + O\left(\frac{1}{t^{2m+1}}\right)\right)\left(\frac{4^m t^{2m}}{p^{2f}} + O\left(\frac{t^{2m-1}}{p^{2f-1}}\right)\right)\right. \\ &\qquad\qquad \left.\times \left(\frac{p^f}{2}H(4p^f - r^2) + O(p^f)\right)\right].\end{aligned}$$

If p is unramified in K, then $\deg_K(\mathfrak{p}) = f$ if and only if there are $g(p) = m/f$ primes in $\mathcal{O}_K$ which lie above p. It follows that

$$\begin{aligned}\frac{1}{|\mathcal{C}_t|}&\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t} \pi^{r,f}_{E_{\vec{v},\vec{w}}}(x) \\ &= \frac{m}{f}\sum_{\substack{B(r)<p\leq x^{1/f} \\ g(p)=m/f}} \left[\left(\frac{1}{4^m t^{2m}} + O\left(\frac{1}{t^{2m+1}}\right)\right)\left(\frac{4^m t^{2m}}{p^{2f}} + O\left(\frac{t^{2m-1}}{p^{2f-1}}\right)\right)\right. \\ &\qquad\qquad \left.\times \left(\frac{p^f}{2}H(4p^f - r^2) + O(p^f)\right)\right].\end{aligned} \tag{8}$$

Using the bound in (7), we find that the summand on the right hand side of (8) is

$$\frac{H(4p^f - r^2)}{2p^f} + O\left(\frac{1}{p^f} + \frac{\log^2 p}{tp^{f/2-1}}\right).$$

Since $t \geq x^{1/f}$, we may therefore write

$$\frac{1}{|\mathcal{C}_t|} \sum_{(\vec{v},\vec{w})\in\mathcal{C}_t} \pi_{E^{r,f}_{\vec{v},\vec{w}}}(x) = \frac{m}{2f} \sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=m/f}} \frac{H(4p^f - r^2)}{p^f} + \mathcal{E}(x,t) \tag{9}$$

where, by standard estimates,

$$\begin{aligned} \mathcal{E}(x,t) &\ll \sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=m/f}} \left(\frac{1}{p^f} + \frac{\log^2 p}{tp^{f/2-1}}\right) \\ &\ll \begin{cases} \log\log x + (x^{3/2}\log x)/t & \text{if } f=1,\\ 1 + (\sqrt{x}\log x)/t & \text{if } f=2,\\ 1 & \text{if } f\geq 3. \end{cases} \end{aligned} \tag{10}$$

Using the equality in (7) we may rewrite the main term on the right hand side of (9) as

$$\frac{m}{2\pi f} \sum_{\substack{B(r)<p\leq x^{1/f}\\ g(p)=m/f}} \sum_{k^2 | r^2-4p^f} \frac{\sqrt{4p^f - r^2}}{kp^f} L(1, \chi_{d_k(p)}). \tag{11}$$

Since $\sqrt{4p^f - r^2} = 2p^{f/2} + O(1/p^{f/2})$ and $L(1,\chi_{d_k(p)}) \ll \log p$, upon reversing the order of summation (and noting that we only need to consider $k \leq 2\sqrt{x}$) in (11) we obtain

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

The error term in (12) is easily seen to be $O(1)$, and thus can be absorbed into $\mathcal{E}(x,t)$. Moreover, partial summation allows us to replace the main term of (12) with

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

Setting $s = S^{1/f}$, and noting that $k^2 \mid r^2 - 4p^f$ implies $k \le 2\sqrt{S}$, we obtain

$$\frac{1}{|\mathcal{C}_t|}\sum_{(\vec{v},\vec{w})\in\mathcal{C}_t}\pi^{r,f}_{E_{\vec{v},\vec{w}}}(x) = \frac{m}{\pi}\Bigg[\frac{1}{\sqrt{x}\log x}\sum_{k\le 2\sqrt{x}}\frac{1}{k}\sum_{\substack{B(r)<p\le x^{1/f}\\ g(p)=m/f\\ k^2\mid r^2-4p^f}} L(1,\chi_{d_k(p)})\log p$$

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

Observe that if $p > B(r)$, then $p \nmid r$. It follows that if $k^2 \mid r^2 - 4p^f$, then $(k, 2r) = 1$. Our result now follows from the definition of $a_{f,1}, \dots, a_{f,\ell_f}$. ∎

5. Computing $C_r(a,n,k)$. Let $a, n, k \in \mathbb{Z}$ with $n, k > 0$. In this section we give formulae for evaluating

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

We utilize the following straightforward consequence of Hensel's lemma.

LEMMA 5.1. *Suppose $N, s, L \in \mathbb{Z}$ with N odd and $s, L > 0$. Then for any $X \in \mathbb{Z}$,*

$$2^s M^2 + NM \equiv X \pmod{2^L}$$

has a unique solution M modulo 2^L.

By the Chinese Remainder Theorem

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

where

$$d_{p,a,k}(n) := \sum_{\substack{b\in(\mathbb{Z}/p^\ell\mathbb{Z})^*\\ b\equiv A \,(\mathrm{mod}\, p^{\ell_1})\\ 4b^2\equiv r^2-ak^2 \,(\mathrm{mod}\, p^{\ell_2})}} 1 \tag{13}$$

with $\ell_1 = \mathrm{ord}_p(B)$, $\ell_2 = \mathrm{ord}_p(4nk^2)$ and $\ell = \ell_1 + \ell_2$.

LEMMA 5.2. *Let p be a prime such that $p \mid 4Bnk^2$.*

(1) *If p is odd and $\ell_1 = 0$, then*

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

(2) *If p is odd and $\ell_1 > 0$, then*

$$d_{p,a,k}(n) = \begin{cases} p^{\min(\ell_1,\ell_2)} & \text{if } r^2 - ak^2 \equiv 4A^2 \pmod{p^{\min(\ell_1,\ell_2)}}, \\ 0 & \text{otherwise.} \end{cases}$$

(3) *If $p = 2$ and $\ell_1 \le 1$, then*

$$d_{2,a,k}(n) = \begin{cases} 2^{\min(\ell_1+4,\ell-1)} & \text{if } r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,\ell_2)}}, \\ 0 & \text{otherwise.} \end{cases}$$

(4) *If $p = 2$ and $\ell_1 \ge 2$, then*

$$d_{2,a,k}(n) = \begin{cases} 2^{\min(\ell_1+3,\ell_2)} & \text{if } r^2 - ak^2 \equiv 4A^2 \pmod{2^{\min(\ell_1+3,\ell_2)}}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For the sake of brevity we only prove (4) (the other cases can be handled similarly).

Let $u = \min(\ell_1 + 3, \ell_2)$. First suppose that there exists an odd integer b such that

$$b \equiv A \pmod{2^{\ell_1}} \quad \text{and} \quad 4b^2 \equiv r^2 - ak^2 \pmod{2^{\ell_2}}. \tag{14}$$

Then $b^2 \equiv A^2 \pmod{2^{\ell_1+1}}$, and therefore $4A^2 \equiv r^2 - ak^2 \pmod{2^u}$.

Now suppose $r^2 - ak^2 - 4A^2 = 2^u \cdot s$ for some integer s, and let $b \in \mathbb{Z}$ be odd. Then b satisfies (14) if and only if there is an integer M such that $b = A + 2^{\ell_1} M$ and

$$4A^2 + 2^{\ell_1+3} AM + 2^{2\ell_1+2} M^2 \equiv r^2 - ak^2 \pmod{2^{\ell_2}}, \tag{15}$$

i.e., $2^{\ell_1+3-u} AM + 2^{2\ell_1+2-u} M^2 \equiv s \pmod{2^{\ell_2-u}}$. If $\ell_2 > \ell_1 + 3$, then by Lemma 5.1 this congruence has a unique solution M modulo 2^{ℓ_2-u}, and thus (14) has exactly $2^{\ell-(\ell_1+\ell_2-u)} = 2^u$ solutions modulo 2^ℓ. On the other hand, if $\ell_2 \le \ell_1 + 3$, then the congruence in question holds trivially, and so (14) has exactly $2^{\ell-\ell_1} = 2^u$ solutions modulo 2^ℓ. ∎

6. Averaging special values of L-series. In this section we prove the $f = 2$ case of Lemma 2.4 (for the $f = 1$ case see [11, Proposition 2.1]). In [5] David and Pappalardi present a proof of the $f = 2$ case of Lemma 2.4 when $K = \mathbb{Q}(i)$, $A = 3$ and $B = 4$, and our proof uses similar arguments.

Proof of Lemma 2.4 (for $f = 2$). Let U be a parameter to be determined later. By [5, (4.2)] we have

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

Assume $U \geq x^{7/16}\log^{2c} x$. Using $|d_k(p)| \leq 4p^2/k^2$, we obtain

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

We first show that the part of the sum on the right side of (16) with k sufficiently large can be absorbed into the error term. Let V be a parameter to be determined later. Then

$$\begin{aligned}&\sum_{\substack{V<k\leq 2\sqrt{x}\\(k,2r)=1\\ n\in\mathbb{N}}} \frac{e^{-n/U}}{kn} \sum_{\substack{B(r)<p\leq\sqrt{x}\\ p\equiv A \,(\mathrm{mod}\, B)\\ 4p^2\equiv r^2 \,(\mathrm{mod}\, k^2)}} \left(\frac{d_k(p)}{n}\right)\log p\\ &\ll (\log x)\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{V<k\leq 2\sqrt{x}\\(k,2r)=1} \frac{1}{k} \sum_{\substack{m\leq\sqrt{x}\\ 4m^2\equiv r^2 \,(\mathrm{mod}\, k^2)}} 1\\ &\ll (\log x)\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{\substack{V<k\leq 2\sqrt{x}\\(k,2r)=1}} \frac{\#\{h\in(\mathbb{Z}/k^2\mathbb{Z}) : 4h^2\equiv r^2 \ (\mathrm{mod}\ k^2)\}}{k}\cdot\frac{\sqrt{x}}{k^2}.\end{aligned}$$

Denote by $\nu(k)$ the number of distinct prime divisors of k. Then by the Chinese Remainder Theorem $4h^2 \equiv r^2 \pmod{k^2}$ has at most $2^{\nu(k)}$ solutions h when $(k, 2r) = 1$, and therefore

$$\begin{aligned}(17)\qquad &\sum_{\substack{V<k\leq 2\sqrt{x}\\(k,2r)=1\\ n\in\mathbb{N}}} \frac{e^{-n/U}}{kn} \sum_{\substack{B(r)<p\leq\sqrt{x}\\ p\equiv A \,(\mathrm{mod}\, B)\\ 4p^2\equiv r^2 \,(\mathrm{mod}\, k^2)}} \left(\frac{d_k(p)}{n}\right)\log p\\ &\ll (\sqrt{x}\log x)\sum_{n\in\mathbb{N}} \frac{e^{-n/U}}{n} \sum_{V<k\leq 2\sqrt{x}} \frac{2^{\nu(k)}}{k^3}.\end{aligned}$$

Since $2^{\nu(k)} \ll k^\epsilon$ for any $0 < \epsilon < 1$ (see [14, Exercise 1.3.2]), it follows that

$$(18)\qquad \sum_{V<k\leq 2\sqrt{x}} \frac{2^{\nu(k)}}{k^3} \ll \int_V^\infty \frac{1}{y^{3-\epsilon}}\,dy \ll \frac{1}{V^{2-\epsilon}}.$$

To estimate the sum $\sum_{n\in\mathbb{N}}(e^{-n/U}/n)$ we first note that if $U>1$, then

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

and hence

$$\sum_{n\in\mathbb{N}}\frac{e^{-n/U}}{n}=-\log(1-e^{-1/U})<\log U+\log\left(\frac{2U}{2U-1}\right)\leq\log U+\log 2. \tag{19}$$

Upon supposing $V\geq\log^{(c+3)/2}x$ and $U\ll\sqrt{x}$, (18) and (19) yield

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

Then by (16) and (17) we conclude that

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

Next we show that the portion of the sum on the right hand side of (20) with n large can be absorbed into the error term. Note first that

$$\sum_{n>U\log U}\frac{e^{-n/U}}{n}\ll\frac{1}{U\log U}\int_{U\log U}^{\infty}e^{-t/U}\,dt=\frac{1}{U\log U}.$$

Recalling that $U\geq x^{7/16}\log^{2c}x$ and $V\leq 2\sqrt{x}$, we obtain

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

and combining this with (20) yields

$$\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\,(\mathrm{mod}\,B)\\k^2\mid r^2-4p^2}}L(1,\chi_{d_k(p)})\log p \tag{21}$$

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

Since $(\frac{\bullet}{n})$ is periodic modulo $4n$, we can rewrite the innermost sum on the right hand side of (21) as

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

which may be further rewritten as

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

where

$$\psi_1(X,C,D):=\sum_{\substack{p\le X\\p\equiv D\,(\mathrm{mod}\,C)}}\log p$$

and the O-term comes from the primes $\le B(r)$ and the prime divisors of n (recall that in the outer sum we have the condition $(k,2r)=1$).

If $(C,D)=1$, then $\psi_1(X,C,D)\sim X/\phi(C)$ (see [17, Part 2, §8.2, Theorem 5]). Defining

$$\mathcal{E}_1(X,C,D):=\psi_1(X,C,D)-\frac{X}{\phi(C)},$$

by our work above we find that

$$\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\,(\mathrm{mod}\,B)\\4p^2\equiv r^2\,(\mathrm{mod}\,k^2)}}\left(\frac{d_k(p)}{n}\right)\log p=\sqrt{x}\left(\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\frac{C_r(a,n,k)}{\phi(4Bnk^2)}\right) \tag{22}$$

$$+\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*\\b\equiv A\,(\mathrm{mod}\,B)\\4b^2\equiv r^2-ak^2\,(\mathrm{mod}\,4nk^2)}}\mathcal{E}_1(\sqrt{x},4Bnk^2,b)+O(\log n).$$

We now show that the contribution of the last two summands on the right hand side of (22) to the sum on the right hand side of (21) can be absorbed into the error term. Since

$$\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}\frac{e^{-n/U}}{n}\cdot\log n \ll \sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}e^{-n/U}$$
$$\ll U\log U\log V,$$

the contribution of the O-term is $\ll \sqrt{x}/\log^c x$ when $U \ll \sqrt{x}/\log^{c+2} x$. Next note that if we reverse the order of summation involving $\mathcal{E}_1(\sqrt{x}, 4Bnk^2, b)$ in (22), then the sum on a has at most one summand. Thus

$$\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*\\ b\equiv A\,(\mathrm{mod}\,B)\\ 4b^2\equiv r^2-ak^2\,(\mathrm{mod}\,4nk^2)}}\mathcal{E}_1(\sqrt{x},4Bnk^2,b) \ll \sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}|\mathcal{E}_1(\sqrt{x},4Bnk^2,b)|. \tag{23}$$

Applying the Cauchy–Schwarz inequality and the identity

$$\phi(CD)=\phi(C)\phi(D)\frac{(C,D)}{\phi((C,D))} \tag{24}$$

we obtain

$$\begin{aligned}\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\frac{e^{-n/U}}{n}|\mathcal{E}_1(\sqrt{x},4Bnk^2,b)| \qquad (25)\\ \le \sum_{k\le V}\frac{1}{k}\Big(\sum_{n\le U\log U}\frac{\phi(4Bnk^2)}{n^2}\Big)^{1/2}\\ \times\Big(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\mathcal{E}_1(\sqrt{x},4Bnk^2,b)^2\Big)^{1/2}\\ =\sum_{k\le V}\frac{\sqrt{\phi(k^2)}}{k}\Big(\sum_{n\le U\log U}\frac{\phi(4Bn)}{n^2}\frac{(4Bn,k^2)}{\phi((4Bn,k^2))}\Big)^{1/2}\\ \times\Big(\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\mathcal{E}_1(\sqrt{x},4Bnk^2,b)^2\Big)^{1/2}.\end{aligned}$$

Clearly

$$\sum_{n\le U\log U}\sum_{b\in(\mathbb{Z}/4Bnk^2\mathbb{Z})^*}\mathcal{E}_1(\sqrt{x},4Bnk^2,b)^2 \le \sum_{n\le 4Bk^2U\log U}\sum_{b\in(\mathbb{Z}/n\mathbb{Z})^*}\mathcal{E}_1(\sqrt{x},n,b)^2,$$

and the Barban–Davenport–Halberstam Theorem [2] asserts that if $X > Q > X/\log^\ell X$ for some $\ell > 0$, then

$$\sum_{s\le Q}\sum_{b\in(\mathbb{Z}/s\mathbb{Z})^*}\mathcal{E}_1(X,s,b)^2 \ll QX\log X.$$

Assume from now on that

$$U = \frac{\sqrt{x}}{\log^{5c+15}x} \quad\text{and}\quad V = \log^{(c+3)/2}x. \tag{26}$$

It follows that

$$\sum_{n\le 4Bk^2U\log U}\sum_{b\in(\mathbb{Z}/n\mathbb{Z})^*}\mathcal{E}_1(\sqrt{x},n,b)^2 \ll (k^2U\log U)\sqrt{x}\log x$$

for $k \le V$, and this, along with the inequalities $\phi(k^2) \le k^2$ and $\phi(CD) \le C\phi(D)$, implies that the right side of (25) is

$$\ll x^{1/4}\sqrt{U\log U\log x}\Big(\sum_{k\le V}k\Big)\Big(\sum_{n\le U\log U}\frac{1}{n}\Big)^{1/2}.$$

This quantity is $\ll x^{1/4}V^2\log U\sqrt{U\log x}$, which in turn is $\ll \sqrt{x}/\log^c x$ for our choice of U and V. Combining this with (21)–(23) we obtain

$$\sum_{\substack{k\le 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{B(r)<p\le\sqrt{x}\\p\equiv A\,(\mathrm{mod}\,B)\\k^2\mid r^2-4p^2}}L(1,\chi_{d_k(p)})\log p$$
$$= \sqrt{x}\Bigg(\sum_{\substack{k\le V\\(k,2r)=1}}\frac{1}{k}\sum_{n\le U\log U}\frac{e^{-n/U}}{n\phi(4Bnk^2)}\sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\Big(\frac{a}{n}\Big)C_r(a,n,k)\Bigg) + O\Big(\frac{\sqrt{x}}{\log^c x}\Big).$$

Our result therefore follows from the proposition below, which also implies the convergence of the summation formula (2) for $C_{r,A,B}$. ∎

PROPOSITION 6.1. *For any $c > 0$,*

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

when U and V are chosen as in (26).

Proof. We begin with the identity

$$\sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n \in \mathbb{N}} \frac{e^{-n/U}}{n\phi(4Bnk^2)} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) = \sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n \in \mathbb{N}} \frac{1}{n\phi(4Bnk^2)} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) + O\left(\frac{1}{\log^c x}\right) \tag{27}$$

(see [5, p. 198]). Our first aim is to show that the terms in the sum on the left hand side of (27) with n large can be absorbed into the error term.

Recall that $C_r(a,n,k) = \prod_{p \mid 4Bnk^2} d_{p,a,k}(n)$. By Lemma 5.2, $d_{2,a,k}(n) \le 2^{\mathrm{ord}_2(B)+4}$ and for odd p, $d_{p,a,k}(n)$ is at most $p^{\mathrm{ord}_p(B)}$ if $p \mid B$, and is at most 2 if $p \mid nk$ and $p \nmid B$. It follows that

$$C_r(a,n,k) \le 2^{\nu(nk)+4} \cdot B,$$

and thus

$$\left| \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) \right| \le 64B\phi(n)2^{\nu(nk)}. \tag{28}$$

Since $\phi(4Bnk^2) \ge \phi(4B)\phi(n)\phi(k^2)$, $\phi(k^2) = k\phi(k)$ and $2^{\nu(nk)} \le 2^{\nu(n)+\nu(k)}$, by (28) we have

$$\sum_{\substack{k \in \mathbb{N} \\ (k,2r)=1}} \frac{1}{k} \sum_{n > U \log U} \frac{e^{-n/U}}{n\phi(4Bnk^2)} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) \ll \sum_{k \in \mathbb{N}} \frac{2^{\nu(k)}}{k^2\phi(k)} \sum_{n > U \log U} \frac{e^{-n/U}2^{\nu(n)}}{n}. \tag{29}$$

As $2^{\nu(k)} \ll k^{1/2}$, the first factor on the right hand side of (29) is a convergent series, while

$$\sum_{n > U \log U} \frac{e^{-n/U}2^{\nu(n)}}{n} \ll \frac{1}{\sqrt{U \log U}} \int_{U \log U}^{\infty} e^{-t/U}\, dt = \frac{1}{\sqrt{U \log U}} \ll \frac{1}{\log^c x}.$$

We conclude that

$$\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{1}{k} \sum_{n>U\log U} \frac{e^{-n/U}}{n\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) \ll \frac{1}{\log^c x}. \tag{30}$$

Next we show that the terms in the sum on the left hand side of (27) with n small and k large can be absorbed into our error term. By our arguments above we have

$$\begin{aligned}\sum_{\substack{k>V\\(k,2r)=1}} \frac{1}{k} \sum_{n\le U\log U} \frac{e^{-n/U}}{n\phi(4Bnk^2)} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) C_r(a,n,k) \\ \ll \sum_{k>V} \frac{2^{\nu(k)}}{k^2\phi(k)} \sum_{n\le U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n}.\end{aligned} \tag{31}$$

Since

$$\frac{2^{\nu(k)}}{\phi(k)} = \frac{1}{k}\prod_{p\mid k}\left(\frac{2p}{p-1}\right) \le \frac{12}{k}\prod_{\substack{p\mid k\\p>3}} 3 \ll \frac{3^{\nu(k)}}{k},$$

we have

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

Using $3^{\nu(k)} \ll k^\epsilon$, we see that

$$\sum_{k>V} \frac{2^{\nu(k)}}{k^2\phi(k)} \ll \frac{1}{V^{2-\epsilon}}. \tag{32}$$

Moreover, using partial summation and the fact that $\sum_{n\le T} 2^{\nu(n)} \ll T\log T$ [17, Exercise 2, p. 53], we find that

$$\begin{aligned}\sum_{n\le U\log U} \frac{e^{-n/U}2^{\nu(n)}}{n} &\ll \frac{\log U}{U} + \int_1^{U\log U} \left(\frac{e^{-t/U}\log t}{t} + \frac{e^{-t/U}\log t}{U}\right) dt \\ &\ll \log^2 U.\end{aligned} \tag{33}$$

Now (31)–(33) imply that

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

and combining this with (30) yields

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

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

Our result now follows from (27) and the definition of $C_{r,A,B}$. ∎

7. Constructing a multiplicative function. In this section we construct a function for use in the proof of Lemma 2.5. Let n and k be positive integers, and suppose $(k,2r)=1$. Define n' by $n = 2^{\mathrm{ord}_2(n)}n'$, let

$$e_{2,a,k}(n) = \begin{cases} \dfrac{d_{2,a,k}(n)}{d_{2,a,k}(1)} & \text{if } d_{2,a,k}(1)\neq 0,\\ 0 & \text{otherwise,}\end{cases}$$

and define

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

LEMMA 7.1. *Let q be an odd prime and α a positive integer, and moreover let $\beta = \mathrm{ord}_q(k)$.*

(1) *$c_k(n)$ is a multiplicative function, and $c_k(1)=1$.*

(2) *Suppose $q \mid B$.*

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

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

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

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

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

(a) *If $q \mid k$, 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) *If $q \nmid k$, then*

$$c_k(q^\alpha) = \begin{cases} q^{\alpha-1}\left(\dfrac{-1}{q}\right)(q-1) & \text{if } q \mid r \text{ and } \alpha \text{ is odd,} \\ -q^{\alpha-1}\left(\left(\dfrac{-1}{q}\right)+1\right) & \text{if } q \nmid r \text{ and } \alpha \text{ is odd,} \\ q^{\alpha-1}(q-1) & \text{if } q \mid r \text{ and } \alpha \text{ is even,} \\ q^{\alpha-1}(q-3) & \text{if } q \nmid r \text{ and } \alpha \text{ is even.} \end{cases}$$

(4) $c_k(2^\alpha) = (-2)^\alpha$.
(5) $c_k(q^\alpha) = c_{q^\beta}(q^\alpha)$.

Proof. For (1) we refer the reader to [4, pp. 173–174], where a similar result is proved. Also, note that (5) follows immediately from (2) and (3).

For the remainder it will be convenient to note that by Lemma 5.2,

$$c_k(q^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, q) = 1 \\ ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(\ell_1,\ell_2)}}}} \left(\frac{a}{q}\right)^\alpha \sum_{\substack{b \in (\mathbb{Z}/q^\ell\mathbb{Z})^* \\ b \equiv A \pmod{q^{\ell_1}} \\ 4b^2 \equiv r^2 - ak^2 \pmod{q^{\ell_2}}}} 1,$$

where, as before, $\ell_1 = \operatorname{ord}_q(B)$, $\ell_2 = \operatorname{ord}_q(4q^\alpha k^2) = \alpha + 2\beta$ and $\ell = \ell_1 + \ell_2$. Using Lemma 5.2 again to evaluate the inner sum, we obtain

$$c_k(q^\alpha) = \begin{cases} q^{\min(\ell_1,\ell_2)} \displaystyle\sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, q) = 1 \\ ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(\ell_1,\ell_2)}}}} \left(\frac{a}{q}\right)^\alpha & \text{if } q \mid B, \\ \displaystyle\sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4 \\ (r^2 - ak^2, q) = 1}} \left(\frac{a}{q}\right)^\alpha \left(1 + \left(\frac{r^2 - ak^2}{q}\right)\right) & \text{if } q \nmid B. \end{cases} \tag{34}$$

(2) If $2\beta \geq \ell_1$, then

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(\ell_1,\ell_2)}} \;\Leftrightarrow\; r^2 \equiv 4A^2 \pmod{q^{\ell_1}}.$$

Since $q \mid k$ and $(k, 2r) = 1$, by (34) this implies that

$$c_k(q^\alpha) = \begin{cases} q^{\min(\ell_1,\ell_2)} \displaystyle\sum_{\substack{a \in (\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ a \equiv 1 \pmod 4}} \left(\frac{a}{q}\right)^\alpha & \text{if } r^2 \equiv 4A^2 \pmod{q^{\ell_1}}, \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand, if $2\beta < \ell_1$ and we write $k = q^\beta k_1$, then

$$ak^2 \equiv r^2 - 4A^2 \pmod{q^{\min(\ell_1,\ell_2)}}$$
$$\Leftrightarrow\ r^2 \equiv 4A^2 \pmod{q^{2\beta}} \text{ and } ak_1^2 \equiv \frac{r^2-4A^2}{q^{2\beta}} \pmod{q^{\min(\alpha,\ell_1-2\beta)}}.$$

Hence if $r^2 \equiv 4A^2 \pmod{q^{2\beta}}$, then

$$c_k(q^\alpha) = q^{\min(\ell_1,\ell_2)} \sum_{\substack{a\in(\mathbb{Z}/4q^\alpha\mathbb{Z})^* \\ ak_1^2\equiv(r^2-4A^2)/q^{2\beta} \,(\mathrm{mod}\, 4q^{\min(\alpha,\ell_1-2\beta)})}} \left(\frac{a}{q}\right)^\alpha$$

by (34), and our result follows.

(3a) Suppose $q \nmid B$ and $q \mid k$. Then $q \nmid r$ as $(k, 2r) = 1$, and so (34) yields

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

(3b) Suppose $q \nmid B$ and $q \nmid k$. First consider odd α. Then by (34),

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

On the other hand, if α is even, then

$$c_k(q^\alpha) = \begin{cases} q^{\alpha-1}(q-1) & \text{if } q \mid r, \\ q^{\alpha-1}(q-2) - q^{\alpha-1} & \text{if } q \nmid r. \end{cases}$$

(4) By definition

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

Set $\ell_1 = \mathrm{ord}_2(B)$, $\ell_2 = \mathrm{ord}_2(4 \cdot 2^\alpha k^2) = \alpha + 2$ and $\ell = \ell_1 + \ell_2$. Suppose $\ell_1 \le 1$. Since r and k are odd,

$$r^2 - ak^2 \equiv 4 \pmod{2^{\min(5,\alpha+2)}} \ \Rightarrow\ a \equiv 5 \pmod 8,$$

and hence by Lemma 5.2(3),

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

The proof is similar when $\ell_1 > 1$. ∎

8. Computing the constant. In this section we prove Lemma 2.5. We begin by recording several evaluations of $d_{p,a,k}(n)$ which follow directly from Lemma 5.2.

LEMMA 8.1. *Suppose p is a prime such that $p \nmid 2n$.*

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

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

   (b) *If $p \nmid Br$, then $d_{p,a,k}(n) = 2$.*

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

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

If $p \mid B$ and $p \nmid 2nk$, then $d_{p,a,k}(n) = 1$ by Lemma 8.1(1). Moreover, if $p \mid k$ and $p \nmid 2n$, then Lemma 8.1(2) implies that $d_{p,a,k}(n) = d_{p,a,k}(1)$. Hence

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

Next note that if p is prime, $n \in \mathbb{N}$ and $d_{p,a,k}(1) = 0$, then since $\mathrm{ord}_p(4k^2) \leq \mathrm{ord}_p(4nk^2)$, by (13) we have $d_{p,a,k}(n) = 0$. It follows that we may rewrite our last expression for $C_{r,A,B}$ as

$$\sum_{\substack{k\in\mathbb{N}\\(k,2r)=1\\n\in\mathbb{N}}} \frac{1}{kn\phi(4Bnk^2)} \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\a\equiv 1 \pmod 4\\(r^2-ak^2,n')=1}} \left(\frac{a}{n}\right) d_{2,a,k}(1)e_{2,a,k}(n) \times \Big(\prod_{\substack{p \text{ odd}\\p\mid n}} d_{p,a,k}(n)\Big)\Big(\prod_{\substack{p\mid k\\p\nmid 2n}} d_{p,a,k}(1)\Big).$$

For odd primes p we see from (13) that $d_{p,a,k}(1) = d_{p,1,k}(1)$. Moreover, when $(k, 2r) = 1$ and $a \equiv 1 \pmod 4$, then $d_{2,a,k}(1)$ is independent of k and a.

Thus we may write

$$C_{r,A,B} = d_{2,1,1}(1) \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1\\n\in\mathbb{N}}} \frac{1}{kn\phi(4Bnk^2)} \times \Big(\prod_{\substack{p\mid(B,k)\\p\nmid 2n}} d_{p,1,k}(1)\Big)\Big(\prod_{\substack{p\mid k\\p\nmid 2Bn}} d_{p,1,k}(1)\Big)c_k(n). \tag{35}$$

For ease of notation write $\nu(C,D)$ for the number of distinct common prime divisors of C and D. If $(k,2r)=1$, then by Lemma 8.1(2b) we have that $\prod_{p\mid k,\,p\nmid 2Bn} d_{p,1,k}(1) = 2^{\nu(k)-\nu(k,2Bn)}$. Moreover, it is straightforward to check that

$$2^{\nu(k,2Bn)} = \frac{2^{\nu(k,B)}\cdot 2^{\nu(k/(k,B),n)}}{2^{\nu((k,B^2)/(k,B),n)}}$$

for odd k. This, together with (24), allows us to rewrite the expression for $C_{r,A,B}$ in (35) as

$$d_{2,1,1}(1) \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{2^{\nu(k)}}{2^{\nu(k,B)}k\phi(4Bk^2)} \times \sum_{n\in\mathbb{N}} \frac{[\prod_{p\mid(B,k),\,p\nmid 2n} d_{p,1,k}(1)]\phi((n,4Bk^2))2^{\nu((k,B^2)/(k,B),n)}}{n\phi(n)(n,4Bk^2)2^{\nu(k/(k,B),n)}}\, c_k(n). \tag{36}$$

Recall that if p is prime, $n\in\mathbb{N}$ and $d_{p,a,k}(1)=0$, then $d_{p,a,k}(n)=0$. Combining this with the fact that $d_{p,a,k}(1) = d_{p,1,k}(1)$ for odd primes p yields the following useful lemma.

LEMMA 8.2. *Suppose $d_{p,1,k}(1)=0$ for some odd prime divisor p of n. Then $c_k(n)=0$.*

For primes p such that $p\mid(B,k,n)$ let

$$f_{p,k} = \begin{cases} d_{p,1,k}(1) & \text{if } d_{p,1,k}(1)\neq 0,\\ 1 & \text{otherwise.}\end{cases}$$

By Lemma 8.2, if $(k,2r)=1$, then

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

and combining this with (24) and (36) yields

$$C_{r,A,B} = \frac{d_{2,1,1}(1)}{\phi(4B)} \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{2^{\nu(k)}\phi((4B,k^2))\prod_{p|(B,k)} d_{p,1,k}(1)}{2^{\nu(k,B)}k\phi(k^2)(4B,k^2)} \times \sum_{n\in\mathbb{N}} \frac{\phi((n,4Bk^2))2^{\nu((k,B^2)/(k,B),n)}}{[\prod_{p|(B,k,n)} f_{p,k}]n\phi(n)(n,4Bk^2)2^{\nu(k/(k,B),n)}} c_k(n). \tag{37}$$

Noting that the summand of the inner sum in (37) is multiplicative in n, we deduce that Lemma 7.1(5) allows us to rewrite this sum as

$$\begin{aligned}
&\prod_{q\,\text{prime}} \sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2))2^{\nu((k,B^2)/(k,B),q^\alpha)}}{[\prod_{p|(B,k,q^\alpha)} f_{p,k}]q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu(k/(k,B),q^\alpha)}} c_k(q^\alpha) \qquad (38)\\
&= \prod_{q\nmid k}\Bigg(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)\Bigg)\\
&\quad\times\prod_{q|k}\Bigg(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2))2^{\nu((k,B^2)/(k,B),q^\alpha)}}{[\prod_{p|(B,k,q^\alpha)} f_{p,k}]q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu(k/(k,B),q^\alpha)}} c_{q^{\operatorname{ord}_q(k)}}(q^\alpha)\Bigg)\\
&= \prod_{q}\Bigg(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)\Bigg)\\
&\quad\times\prod_{q|k}\frac{\displaystyle\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bk^2))2^{\nu((k,B^2)/(k,B),q^\alpha)}}{[\prod_{p|(B,k,q^\alpha)} f_{p,k}]q^\alpha\phi(q^\alpha)(q^\alpha,4Bk^2)2^{\nu(k/(k,B),q^\alpha)}} c_{q^{\operatorname{ord}_q(k)}}(q^\alpha)}{\displaystyle\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)}.
\end{aligned}$$

Substituting (38) into (37), we make our expression for $C_{r,A,B}$ become

$$\begin{aligned}
&\frac{d_{2,1,1}(1)}{\phi(4B)}\prod_{q}\Bigg(\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)\Bigg) \qquad (39)\\
&\quad\times \sum_{\substack{k\in\mathbb{N}\\(k,2r)=1}} \frac{2^{\nu(k)}\phi((4B,k^2))\prod_{p|(B,k)} d_{p,1,k}(1)}{2^{\nu(k,B)}k\phi(k^2)(4B,k^2)}\\
&\quad\times\prod_{\substack{q^\beta\|k\\\beta\geq 1}}\frac{\displaystyle\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4Bq^{2\beta}))2^{\nu((q^\beta,B^2)/(q^\beta,B),q^\alpha)}}{[\prod_{p|(B,q^\alpha)} f_{p,k}]q^\alpha\phi(q^\alpha)(q^\alpha,4Bq^{2\beta})2^{\nu(q^\beta/(q^\beta,B),q^\alpha)}} c_{q^\beta}(q^\alpha)}{\displaystyle\sum_{\alpha\geq 0} \frac{\phi((q^\alpha,4B))}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)} c_1(q^\alpha)}.
\end{aligned}$$

Since the sum on k in (39) is a sum of multiplicative functions, we may

rewrite it as

$$\prod_{q\nmid 2r}\Bigg[1+\sum_{\beta\ge 1}\frac{\dfrac{2[\prod_{p|(B,q)}d_{p,1,q^\beta}(1)]\phi((4B,q^{2\beta}))}{q^\beta 2^{\nu(q,B)}\phi(q^{2\beta})(4B,q^{2\beta})}}{\displaystyle\sum_{\alpha\ge 0}\frac{\phi((q^\alpha,4B))c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)(q^\alpha,4B)}}\times\sum_{\alpha\ge 0}\frac{\phi((q^\alpha,4Bq^{2\beta}))\delta_{\alpha,B}c_{q^\beta}(q^\alpha)}{[\prod_{p|(B,q^\alpha)}f_{p,q^\beta}]q^\alpha\phi(q^\alpha)(q^\alpha,4Bq^{2\beta})}\Bigg],\tag{40}$$

where $\delta_{\alpha,B}$ is equal to $1/2$ if $\alpha>0$ and $q\nmid B$, and equal to 1 otherwise. Substituting (40) into (39), and noting that $\phi(q^j)/q^jq^\alpha\phi(q^\alpha)=1/q^{2\alpha}$ if $\alpha,j>0$, we obtain

$$\begin{aligned}C_{r,A,B}=\frac{d_{2,1,1}(1)}{\phi(4B)}&\Big(\sum_{\alpha\ge 0}\frac{c_1(2^\alpha)}{2^{2\alpha}}\Big)\prod_{\substack{q\nmid B\\ q|r}}\Big(\sum_{\alpha\ge 0}\frac{c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)}\Big)\prod_{\substack{q|B\\ q|r}}\Big(\sum_{\alpha\ge 0}\frac{c_1(q^\alpha)}{q^{2\alpha}}\Big)\\&\times\prod_{q\nmid 2rB}\Big[\sum_{\alpha\ge 0}\frac{c_1(q^\alpha)}{q^\alpha\phi(q^\alpha)}+\sum_{\beta\ge 1}\frac{2}{q^\beta\phi(q^{2\beta})}\Big(1+\sum_{\alpha\ge 1}\frac{c_{q^\beta}(q^\alpha)}{2q^{2\alpha}}\Big)\Big]\\&\times\prod_{\substack{q|B\\ q\nmid 2r}}\Big[\sum_{\alpha\ge 0}\frac{c_1(q^\alpha)}{q^{2\alpha}}+\sum_{\beta\ge 1}\frac{d_{q,1,q^\beta}(1)}{q^{3\beta}}\Big(1+\sum_{\alpha\ge 1}\frac{c_{q^\beta}(q^\alpha)}{q^{2\alpha}f_{q,q^\beta}}\Big)\Big].\end{aligned}$$

Our result now follows from Lemma 7.1 and the formula for the sum of a geometric series. ∎

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

The authors also wish to thank Todd Molnar and Kenny Stauffer for their contributions to this work.

References

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

[2] M. B. Barban, *On the distribution of primes in arithmetic progressions "on average"*, Dokl. Akad. Nauk UzSSR 1964, no. 5, 5–7 (in Russian).

[3] J. Battista, J. Bayless, D. Ivanov, and K. James, *Average Frobenius distributions for elliptic curves with nontrivial rational torsion*, Acta Arith. 119 (2005), 81–91.

[4] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Int. Math. Res. Notices 1999, 165–183.

[5] —, —, *Average Frobenius distribution for inerts in* $\mathbb{Q}(i)$, J. Ramanujan Math. Soc. 19 (2004), 181–201.

[6] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197–272.
[7] N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. 89 (1987), 561–567.
[8] É. Fouvry and M. R. Murty, *Supersingular primes common to two elliptic curves*, in: Number Theory (Paris, 1992–1993), London Math. Soc. Lecture Note Ser. 215, Cambridge Univ. Press, Cambridge, 1995, 91–102.
[9] —, —, *On the distribution of supersingular primes*, Canad. J. Math. 48 (1996), 81–104.
[10] K. James, *Average Frobenius distributions for elliptic curves with 3-torsion*, J. Number Theory 109 (2004), 278–298.
[11] —, *Averaging special values of Dirichlet L-series*, Ramanujan J. 10 (2005), 75–87.
[12] S. Lang and H. Trotter, *Frobenius Distributions in* GL_2*-extensions*, Lecture Notes in Math. 504, Springer, Berlin, 1976.
[13] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) 126 (1987), 649–673.
[14] M. R. Murty, *Problems in Analytic Number Theory*, Grad. Texts in Math. 206, Springer, New York, 2001.
[15] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A 46 (1987), 183–211.
[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.
[17] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Stud. Adv. Math. 46, Cambridge Univ. Press, Cambridge, 1995.

Neil Calkin
Department of Mathematical Sciences
Clemson University
Box 341907
Clemson, SC 29634-1907, U.S.A.
E-mail: calkin@clemson.edu

Kevin James
Department of Mathematical Sciences
Clemson University
Box 340975
Clemson, SC 29634-0975, U.S.A.
E-mail: kevja@clemson.edu
URL: http://www.math.clemson.edu/~kevja/

Bryan Faulkner
Ferrum College
80 Wiley Dr.
Ferrum, VA 24088, U.S.A.
E-mail: bfaulkner@ferrum.edu

David Penniston
Department of Mathematics
University of Wisconsin Oshkosh
Oshkosh, WI 54901-8631, U.S.A.
E-mail: pennistd@uwosh.edu

Received on 6.1.2009
and in revised form on 5.7.2010 (5908)