The Lang-Trotter conjecture on average for elliptic curves with torsion

George J. Schaeffer, Cole T. South, Cinna J. Wu
Advisors: Neil J. Calkin, Kevin James, Timothy Flowers
REU for Computational Number Theory and Combinatorics

Clemson University, Summer 2005

1 Introduction

1.1 General theory

1.2 Purpose of this paper

The purpose of this paper is to show that the Lang-Trotter conjecture holds when one averages over those elliptic curves whose Mordell-Weil group over $\mathbb{Q}$ has a point of order m. That is to say, if $\mathcal{E}_m(\mathbf{p})$ is the set of all such elliptic curves with parameters bounded by $\mathbf{p}$, we will show that

$$\lim_{\mathbf{p}\to\infty} \frac{1}{\#\mathcal{E}_m(\mathbf{p})} \sum_{E\in\mathcal{E}_m(\mathbf{p})} \pi_E^r(x) \sim C^{r,m}\frac{\sqrt{x}}{\log x}, \tag{1}$$

for some constant $C^{r,m}$ which we will give explicitly.

2 The average and class numbers

In this section, we will show that for a fixed value of m, the argument of the limit in the left-hand side of (1) can be written in terms of class numbers of binary quadratic forms. Unfortunately, there is no way to avoid a significant case breakdown, and consequently the proof of the main results of this section have been divided into several parts.

The theory of this section is quite deep, so we begin with some preliminary facts about m-torsion subgroups, points of order m in $E(F)$, and counting certain parametrizations and subsets of elliptic curves over $\mathbb{F}_p$.

2.1 m-torsion subgroups

Fact 2.1 *Let F be a field, E/F be a nonsingular elliptic curve, and m be an integer. Define*

$$E(F)[m] = \{P \in E(F) : mP = \mathcal{O}\}. \tag{2}$$

$E(F)[m]$ is called the m-torsion subgroup of E over F.

Suppose that $E(\mathbb{Q})$ has a point of order m. Then for any prime p of good reduction,

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \leq E(\mathbb{F}_p)[m] \leq \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}. \tag{3}$$

The first of the above subgroup inclusions is a consequence of the fact that

$$E(\mathbb{Q})_{\text{tor}} \xrightarrow{\text{reduction modulo } p} E(\mathbb{F}_p) \tag{4}$$

is a monomorphism (as long as p is of good reduction). By hypothesis, $\mathbb{Z}/m\mathbb{Z} \leq E(\mathbb{Q})_{\text{tor}}$, so $\mathbb{Z}/m\mathbb{Z} \leq E(\mathbb{F}_p)$. The second subgroup inclusion is due to the fact that for any m, $E(\bar{\mathbb{F}}_p)[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, and also $E(\mathbb{F}_p) \leq E(\bar{\mathbb{F}}_p)[m]$.

Corollary 2.2 *For any m,*

$$E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{d\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}} \tag{5}$$

(where $d = 1, \ldots, m$ is any divisor of m). In particular, if m is prime, then either

$$E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}}, \quad \text{or} \quad E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}, \tag{6}$$

We say in the former of these cases that E has cyclic m-torsion*, and in the latter that E has* full m-torsion*.*

Lemma 2.3 *For any n, let $a \mid n$. There are $\varphi(a)$ points of order a in $\mathbb{Z}/n\mathbb{Z}$.*

Proof. The point $n_0 = n/a$ has order a in $\mathbb{Z}/n\mathbb{Z}$. Let n_1 be another point of order a. This means that for some integer k,

$$\begin{aligned} an_1 &= kn \\ n_1 &= k(n/a) = kn_0 \end{aligned} \tag{7}$$

Thus, a point of order a must be an integer multiple of n_0, where $1 \leq k \leq a$.

Let $\gcd(k, a) = d$, and suppose kn_0 has order a. This is true iff $akn_0 = 0$ and $\forall e \mid a, e \neq a$, we have $ekn_0 \neq 0$. This occurs iff $d = 1$, since otherwise, $(a/d)kn_0 = (k/d)an_0 = 0$ where $(a/d) < a$. Our lemma is now proved since the number of such k is $\varphi(a)$.□

Fact 2.4 *For any m, let $d \mid m$. Then the number of points of order m in $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ is*

$$\sum_{a|d} \varphi(a) \sum_{\substack{b|a \\ gcd(b, \frac{m}{a})=1}} \varphi(\frac{m}{b}) \tag{8}$$

Proof. A point (r, s) in $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ has order m iff $\text{lcm}(\text{ord}r, \text{ord}s) = m$. To construct our sum, consider the points of order $a \mid d$ in $\mathbb{Z}/d\mathbb{Z}$. By Lemma 2.3, there are $\varphi(a)$ such points. We can show that any point r of order a in $\mathbb{Z}/d\mathbb{Z}$ has

$$\sum_{\substack{b|a \\ \gcd(b, \frac{m}{a})=1}} \varphi(\frac{m}{b}) \tag{9}$$

corresponding points s in $\mathbb{Z}/m\mathbb{Z}$ such that the (r, s) have order m in $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

To see this, Let $1 \le c \le m$ be an integer such that $\mathrm{lcm}(a, c) = ac/\gcd(a, c) = m$. Since $a \mid m$, this means that for some e, $c = (m/a)e$. We have $\mathrm{lcm}(a, (m/a)e) = me/\gcd(a, (m/a)e) = m$ iff $e = \gcd(a, (m/a)e)$ which is true iff $e \mid a$ and $\gcd(a/e, m/a) = 1$. By Lemma 2.3, the number of points in $\mathbb{Z}/m\mathbb{Z}$ with order $(m/a)e$ is $\varphi(me/a)$. Setting $b = a/e$ gives us (9).

Putting all of the above together results in (9). □

2.2 Counting elliptic curves

Let F be a field and let E/F be a nonsingular elliptic curve. If $\mathcal{P}$ is a specified parametrization of elliptic curves, we write

$$\mathcal{P}(E/F) = \{\text{parametrizations of } E \text{ in } \mathcal{P} \text{ over } F\}, \tag{10}$$

and also

$$\mathcal{P}(\tilde{E}_0/F) = \bigcup_{E \cong E_0} \mathcal{P}(E/F). \tag{11}$$

Fact 2.5 *Let $p > 3$ be a prime. Then any curve E over $\mathbb{F}_p$ can be parametrized as*

$$E_{\mathcal{W}(a,b)} : Y^2 = X^2 + aX + b \tag{12}$$

with $a, b \in \mathbb{F}_p$. If $\mathcal{W}$ represents such parametrizations, we have

$$\#\mathcal{W}(\tilde{E}_{\mathcal{W}(a,b)}/\mathbb{F}_p) = \begin{cases} (p-1)/6 & \text{if } a = 0 \text{ and } p \equiv 1 \bmod 3, \\ (p-1)/4 & \text{if } b = 0 \text{ and } p \equiv 1 \bmod 4, \\ (p-1)/2 & \text{otherwise.} \end{cases} \tag{13}$$

Proof. We recall that $E_{\mathcal{W}(a,b)} \cong E_{\mathcal{W}(A,B)}$ if and only if there exists a $u \in \mathbb{F}_p^*$ such that $A = u^4 a$ and $B = u^6 b$. We must therefore count the number of elements in the images of the $\mathbb{F}_p^*$-maps $u \mapsto u^4$ and $u \mapsto u^6$.

Let $R_p(\alpha)$ be the image of $u \mapsto u^\alpha$ on $\mathbb{F}_p^*$; in particular, $R_p(2)$ is the set of quadratic residues modulo p, and of course, $\#R_p(2) = \frac{1}{2}(p-1)$. When $p \equiv 1 \bmod 4$, $u \in R_p(2)$ iff $-u \in R_p(2)$. It follows that

$$\#R_p(4) = \begin{cases} (p-1)/4 & \text{if } p \equiv 1 \bmod 4, \\ (p-1)/2 & \text{otherwise.} \end{cases} \tag{14}$$

We have $\#R_p(3) = p - 1$ unless $p \equiv 1 \bmod 3$, in which case $\#R_p(3) = \frac{1}{3}(p-1)$. If $u \in R_p(3)$, then there is a $v \in \mathbb{F}_p^*$ such that $u = v^3$, so $-u = (-v)^3$; therefore, $u \in R_p(3)$ iff $-u \in R_p(3)$. Consequently,

$$\#R_p(6) = \begin{cases} (p-1)/6 & \text{if } p \equiv 1 \bmod 3, \\ (p-1)/2 & \text{otherwise.} \end{cases} \tag{15}$$

The result follows from considering the different cases. □

Fact 2.6 *Let E be an elliptic curve and $p > 3$ be a prime of good reduction. Let $\mathcal{P}_m$ denote the parametrization of elliptic curves with a m-torsion point. Then*

$$\#\mathcal{P}_m(E/\mathbb{F}_p) = \left\{ \begin{array}{ll} 1 & \text{if } m = 2, \\ 1/2 & \text{otherwise.} \end{array} \right\} \#\{P \in E(\mathbb{F}_p) : \operatorname{ord} P = m\}. \tag{16}$$

Proof. If $E(\mathbb{F}_p)$ has no points of order m, then the claim follows trivially.

Suppose then that $E(\mathbb{F}_p)$ has at least one point of order m. To parametrize E over $\mathbb{F}_p$, we choose a point $P \in E(\mathbb{F}_p)$ with order m and translate the elliptic curve by an admissible change of variables so that the point analogous to P on the translated curve now lies at the origin (see [7] for more details). Choosing P and $-P$ give the same parametrization, so P is chosen up to its x-coordinate; recall that when $m = 2$, $P = -P$, but otherwise $P \neq -P$. The result follows. □

Fact 2.7 *We have*

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \begin{cases} \#\mathcal{P}_m(E/\mathbb{F}_p)\#\mathcal{W}(\tilde{E}_{\mathcal{W}(a,b)}/\mathbb{F}_p) & \text{if } m = 2, 3, \\ \#\mathcal{P}_m(E/\mathbb{F}_p) & \text{otherwise.} \end{cases} \tag{17}$$

Proof. In [7], pp. 145-148, Knapp discusses how to find the parametrizations of elliptic curves $E/\mathbb{Q}$ with points of some order m. Following this discussion, we start with a curve E and a point (x_0, y_0) of order m and make a few changes of variable to get the parametrization.

For $m = 2, 3$, the coefficients of the resulting parametrization depend on the coefficients of the original curve. Thus, each $E \in \mathcal{W}(\tilde{E}_{\mathcal{W}(a,b)}/\mathbb{F}_p)$ uniquely determines $\#\mathcal{P}_m(E/\mathbb{F}_p)$ parametrizations, and our result follows.

For all other cases, the resulting parametrization only depends on the x-coordinate of our chosen m-torsion point. More precisely, we obtain the same parametrizations from $E_{\mathcal{W}(A,B)}$ with a m-torsion point (x_0, y_0) and $E_{\mathcal{W}(u^4A,u^6B)}$ with a m-torsion point (u^2x_0, u^3y_0) with $u \in \mathbb{F}_p$. Thus, $\#\mathcal{P}_m(E/\mathbb{F}_p) = \#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p)$. □

2.3 Binary quadratic forms and class numbers

Definition 2.8 *A* binary quadratic form *is an expression of the form $Q(x, y) = ax^2 + bxy + cy^2$ (we take $a, b, c \in \mathbb{Z}$). We say that Q is* primitive *iff $(a, b, c) = 1$. The* discriminant *of Q is given by $b^2 - 4ac$.*

Let H, h be functions on the integers defined as

$$H(\Delta) = \#\{Q : Q \text{ is a binary quadratic form of discriminant } \Delta\}, \text{ and} \tag{18}$$

$$h(\Delta) = \#\{Q : Q \text{ is a primitive binary quadratic form of discriminant } \Delta\}. \tag{19}$$

H and h are called the Kronecker and Dirichlet class numbers, respectively.

Fact 2.9 *The Kronecker and Dirichlet class numbers are related by the identity*

$$H(\Delta) = 2 \sum_{\substack{f^2|\Delta \\ \Delta/f^2 \equiv 0,1 \bmod 4}} \frac{h(\Delta/f^2)}{\omega(\Delta/f^2)}, \tag{20}$$

where $\omega(\Delta)$ gives the number of units in the ring $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{\Delta})]$.

Fact 2.10 (Deuring, Schoof) *Fix $m \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ and $r \in \mathbb{Z}$. Let p be a prime such that $p \nmid r$ if $r \neq 0$, and $p > B(r)$ where $B(r) = \max\{3, r, r^2/4\}$. Define the following:*

$$N_{p,r}(m) = \#\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ m \mid \#E(\mathbb{F}_p)\},\ \text{and}$$
$$N'_{p,r}(m) = \#\left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}\right\}. \tag{21}$$

Then we have,

$$N_{p,r}(m) = \begin{cases} H(r^2 - 4p) & \text{if } p+1 \equiv r \bmod m \\ 0 & \text{if } p+1 \not\equiv r \bmod m, \end{cases} \tag{22}$$

and

$$N'_{p,r}(m) = \begin{cases} H\left(\frac{r^2-4p}{m^2}\right) & \text{if } p+1 \equiv r \bmod m^2, r \equiv 2 \bmod m, \text{and } r \neq 0, \\ h(-p) & \text{if } p+1 \equiv r \bmod m^2, r \equiv 2 \bmod m, r = 0, \text{and } m = 2 \\ 0 & \text{otherwise.} \end{cases} \tag{23}$$

Proof. These results easily follow from [10]. Assume m, p, r are given as in the hypothesis of our claim. The results for $N_{p,r}(m)$ follow immediately from Thm. 4.6 of [10].

Now suppose that $r \not\equiv 2 \bmod m$ or $r \not\equiv p+1 \bmod m^2$. Then $r \not\equiv 2 \bmod m$ gives $p \not\equiv 1 \bmod m$ since $p+1 \equiv r \bmod m$. By Prop. 3.7 of [10], $N'_{p,r}(m) = 0$.

If we have $r \equiv 2 \bmod m$ and $r \equiv p+1 \bmod m^2$, our result is stated in Thm. 4.9 of [10] for m odd and $r \neq 0$. The proof for this particular result is identical for when we allow m to be even and $r \neq 0$. Thus, $N'_{p,r}(m) = H\left(\frac{r^2-4p}{m^2}\right)$ if $r \neq 0$ for all m.

When $r = 0$, the assumptions $r \equiv 2 \bmod m$ and $r \equiv p+1 \bmod m^2$ give $p \equiv 1 \bmod m$ and $p \equiv -1 \bmod m$ which implies $m = 2$. Thus, $r = 0, m \neq 2$ gives $N'_{p,r}(m) = 0$. When $m = 2$, since $p \equiv -1 \bmod 4$, our claim follows from Lemma 4.8 (iii) of [10]. □

Definition 2.11 *Choose m, r, and p satisfying the hypothesis of Fact 2.10. Let $d \mid m$ and write*

$$N_{p,r}(d, m) = \#\left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{d\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}\right\}. \tag{24}$$

The following lemma gives $N_{p,r}(d, m)$ in terms of $N_{p,r}(m')$ and $N'_{p,r}(m'')$. We will later use this lemma to write $N_{p,r}(d, m)$ in terms of class numbers.

Lemma 2.12 *Let ℓ be a prime. We then have the following chart. (In each case, assume that $p+1 \equiv r \bmod m$.)*

m	d	$N_{p,r}(d,m)$
ℓ	1	$N_{p,r}(\ell) - N'_{p,r}(\ell)$
ℓ	ℓ	$N'_{p,r}(\ell)$
ℓ^2	1	$N_{p,r}(\ell^2) - N'_{p,r}(\ell)$
ℓ^2	ℓ	$N_{p,r}(\ell^3) - N_{p,r}(\ell^2) - N'_{p,r}(\ell^2) + N'_{p,r}(\ell)$
ℓ^2	ℓ^2	$N'_{p,r}(\ell^2)$
2ℓ	1	$N_{p,r}(2\ell) - N'_{p,r}(2) - N'_{p,r}(\ell) + N'_{p,r}(2\ell)$
2ℓ	2	$N'_{p,r}(2) - N'_{p,r}(2\ell)$
2ℓ	ℓ	$N'_{p,r}(\ell) - N'_{p,r}(2\ell)$
2ℓ	2ℓ	$N'_{p,r}(2\ell)$
ℓ^3	1	$N_{p,r}(\ell^3) - N'_{p,r}(\ell)$
ℓ^3	ℓ	$N_{p,r}(\ell^4) - N_{p,r}(\ell^3) - N'_{p,r}(\ell^2) + N'_{p,r}(\ell)$
ℓ^3	ℓ^2	$N'_{p,r}(\ell^2) - N'_{p,r}(\ell^3)$
ℓ^3	ℓ^3	$N'_{p,r}(\ell^3)$
4ℓ	1	$N_{p,r}(4) - N'_{p,r}(2) - N'_{p,r}(\ell) + N'_{p,r}(2\ell)$
4ℓ	2	$N_{p,r}(8\ell) - N_{p,r}(16\ell) + N'_{p,r}(2) - N'_{p,r}(4) - N'_{p,r}(2\ell) + N'_{p,r}(4\ell)$
4ℓ	4	$N'_{p,r}(4) - N'_{p,r}(4\ell)$
4ℓ	ℓ	$N'_{p,r}(\ell) - N'_{p,r}(2\ell)$
4ℓ	2ℓ	$N_{p,r}(16\ell) - N_{p,r}(4\ell) + N'_{p,r}(2\ell) - N'_{p,r}(4\ell)$
4ℓ	4ℓ	$N'_{p,r}(4\ell)$

Proof. In this proof, it will be understood that all elliptic curves E satisfy $a_p(E) = r$. Thus, $m \mid \#E(\mathbb{F}_p)$ and $E(\mathbb{F}_p)$ has a subgroup of order m. Consider the subgroups of $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ containing a subgroup of order m. Call the maximal such subgroup contained in $E(\mathbb{F}_p)$, the maximal full m-subgroup of $E(\mathbb{F}_p)$.

Consider the case where $m = \ell^2$. We have the following hierarchy of possible maximal full ℓ-subgroups:

$$\langle 0 \rangle < \frac{\mathbb{Z}}{l\mathbb{Z}} < \left\{ \begin{array}{c} \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z} \\ \\ \mathbb{Z}/l^2\mathbb{Z} \end{array} \right\} < \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}} < \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}}. \tag{25}$$

Since $E(\mathbb{F}_p)[l^2]$ must be one of

$$\frac{\mathbb{Z}}{l^2\mathbb{Z}}, \quad \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}}, \quad \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}},$$

it is helpful to identify the maximal full l^2-subgroup of $E(\mathbb{F}_p)$, as in these cases, the maximal full l^2-subgroup must be equivalent with the torsion subgroup $E(\mathbb{F}_p)[l^2]$.

Note that if $l^2 \mid \#E(\mathbb{F}_p)$, then either

$$\frac{\mathbb{Z}}{l^2\mathbb{Z}} \leq E(\mathbb{F}_p), \quad \text{or} \quad \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l\mathbb{Z}} \leq E(\mathbb{F}_p).$$

Thus, $N_{p,r}(l^2)$ counts those elliptic curves E having a maximal full l^2-subgroup lying in the restricted hierarchy

$$\left\{ \begin{array}{c} \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z} \\ \\ \mathbb{Z}/l^2\mathbb{Z} \end{array} \right\} < \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}} < \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}}.$$

On the other hand, $l^3 \mid \#E(\mathbb{F}_p)$ implies that either

$$\frac{\mathbb{Z}}{l^3\mathbb{Z}} \leq E(\mathbb{F}_p), \quad \text{or} \quad \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}} \leq E(\mathbb{F}_p).$$

(we do not admit the case wherein the triple direct sum of $\mathbb{Z}/l\mathbb{Z}$ is a subgroup of $E(\mathbb{F}_p)$, since then $E(\mathbb{F}_p)[l]$ would be larger than Theorem [] permits). Reducing, we find that $N_{p,r}(l^3)$ counts elliptic curves having a maximal full l^2-subgroup in the restricted hierarchy

$$\frac{\mathbb{Z}}{l^2\mathbb{Z}} < \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}} < \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}},$$

in particular, we note that if E is an element of the set counted by $N_{p,r}(l^3)$, then $\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z}$ is not the maximal full l^2-subgroup of $E(\mathbb{F}_p)$ (since $\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z}$ is not a subgroup of $\mathbb{Z}/l^2\mathbb{Z}$ and it is properly contained inside $\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l^2\mathbb{Z}$).

Likewise, we find that $N'_{p,r}(l)$ and $N'_{p,r}(l^2)$ count elliptic curves E with maximal full l^2-subgroups lying in the restricted hierarchies

$$\frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l\mathbb{Z}} < \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}} < \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}}, \quad \text{and} \quad \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}}$$

respectively.

We may now construct the following table, where the columns represent the possible maximal full ℓ^2-subgroups. A $*$ in column Y and row X indicates that Y counts the elliptic curves with maximal full ℓ^2-subgroup X.

	$\mathbb{Z}/l^2\mathbb{Z}$	$\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z}$	$\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l^2\mathbb{Z}$	$\mathbb{Z}/l^2\mathbb{Z} \oplus \mathbb{Z}/l^2\mathbb{Z}$
$N_{p,r}(l^2)$	$*$	$*$	$*$	$*$
$N_{p,r}(l^3)$	$*$		$*$	$*$
$N'_{p,r}(l)$		$*$	$*$	$*$
$N'_{p,r}(l^2)$				$*$

It should be clear at this point how we arrive at the claimed identities. For example, $N_{p,r}(l^2) - N'_{p,r}(l)$ counts all those elliptic curves E whose maximal full l^2-subgroup lies in the hierarchy

$$\left.\begin{matrix}\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z} \\ \\ \mathbb{Z}/l^2\mathbb{Z}\end{matrix}\right\} < \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}} < \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}}, \quad \text{but not in} \quad \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l\mathbb{Z}} < \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}} < \frac{\mathbb{Z}}{l^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^2\mathbb{Z}}.$$

That is, $N_{p,r}(l^2) - N'_{p,r}(l)$ counts those E for which $\mathbb{Z}/l^2\mathbb{Z}$ is the maximal full l^2-subgroup. Since this subgroup is the maximal subgroup under $\mathbb{Z}/l^2\mathbb{Z} \oplus \mathbb{Z}/l^2\mathbb{Z}$ in $E(\mathbb{F}_p)$, it follows that $E(\mathbb{F}_p)[l^2] \cong \mathbb{Z}/l^2\mathbb{Z}$. The second follows similarily, and the third identity is trivial.

For the other cases of m, we use construct similar tables using the same methods.
For $m = \ell$, we have:

	$\mathbb{Z}/m\mathbb{Z}$	$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$
$N_{p,r}(m)$	$*$	$*$
$N'_{p,r}(m)$		$*$

For $m = \ell^3$, we have:

	$\mathbb{Z}/l^3\mathbb{Z}$	$\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l^2\mathbb{Z}$	$\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l^3\mathbb{Z}$	$\mathbb{Z}/l^2\mathbb{Z} \oplus \mathbb{Z}/l^3\mathbb{Z}$	$\mathbb{Z}/l^3\mathbb{Z} \oplus \mathbb{Z}/l^3\mathbb{Z}$
$N_{p,r}(l^3)$	$*$	$*$	$*$	$*$	$*$
$N_{p,r}(l^4)$	$*$		$*$	$*$	$*$
$N'_{p,r}(l)$		$*$	$*$	$*$	$*$
$N'_{p,r}(l^2)$				$*$	$*$
$N'_{p,r}(l^3)$					$*$

For $m = 2\ell$, we have:

	$\mathbb{Z}/2l\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z}$	$\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z}$	$\mathbb{Z}/2l\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z}$
$N_{p,r}(2l)$	$*$	$*$	$*$	$*$
$N'_{p,r}(2)$		$*$		$*$
$N'_{p,r}(l)$			$*$	$*$
$N'_{p,r}(2l)$				$*$

For $m = 4\ell^3$, we have:

	$\frac{\mathbb{Z}}{4l\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2l\mathbb{Z}}$	$\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4l\mathbb{Z}}$	$\frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4l\mathbb{Z}}$	$\frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4l\mathbb{Z}}$	$\frac{\mathbb{Z}}{2l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2l\mathbb{Z}}$	$\frac{\mathbb{Z}}{2l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4l\mathbb{Z}}$	$\frac{\mathbb{Z}}{4l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4l\mathbb{Z}}$
$N_{p,r}(4l)$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$N_{p,r}(8l)$	$*$		$*$	$*$	$*$		$*$	$*$
$N_{p,r}(16l)$	$*$	$*$	$*$	$*$	$*$		$*$	$*$
$N'_{p,r}(2)$		$*$	$*$	$*$		$*$	$*$	$*$
$N'_{p,r}(4)$				$*$				$*$
$N'_{p,r}(l)$					$*$	$*$	$*$	$*$
$N'_{p,r}(2l)$						$*$	$*$	$*$
$N'_{p,r}(4l)$								$*$

Our identities then follow from simple combinatorial arguments.□

2.4 Main results

Of the main results we prove in this section of the paper, Lemma 2.13 (with which we reexpress our average in terms of sums over primes p and congruence classes modulo p) applies to all $m \in \{2, \ldots, 10, 12\}$. The remainder of the results (Lemmas **??**–**??**) are broken up by the prime factorization of m as well as the number of parameters in $\mathcal{P}_m$.

Lemma 2.13 *Let $B(r) = \max\{3, r, r^2/4\}$. We have*

$$\begin{aligned}
&\frac{1}{4ST}\sideset{}{'}\sum_{|s|\le S,|t|\le T}\pi^r_{E_{\mathfrak{P}_{m(s,t)}}}(x) = \\
&\qquad\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}}\left(\frac{1}{p^2}+\mathrm{O}\left(\frac{1}{Sp}+\frac{1}{Tp}+\frac{1}{ST}\right)\right)\sideset{}{'}\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathfrak{P}_{m(s,t)}})=r}} 1+\mathrm{O}(\log\log x),\ \textit{or}\\
&\frac{1}{2S}\sideset{}{'}\sum_{|s|\le S}\pi^r_{E_{\mathfrak{P}_{m(s)}}}(x) = \\
&\qquad\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}}\left(\frac{1}{p}+\mathrm{O}\left(\frac{1}{S}\right)\right)\sideset{}{'}\sum_{\substack{0\le s<p\\ a_p(E_{\mathfrak{P}_{m(s)}})=r}} 1+\mathrm{O}(\log\log x),
\end{aligned}\tag{26}$$

when $E_{\mathfrak{P}_m}$ has two parameters or one parameter, respectively.

Proof. We begin by considering the left-hand side of equations in (26) and replacing $\pi^r_{E_{\mathfrak{P}_m}}(x)$ by a summation:

$$\begin{aligned}
\frac{1}{4ST}\sideset{}{'}\sum_{|s|\le S,|t|\le T}\pi^r_{E_{\mathfrak{P}_{m(s,t)}}}(x) &= \frac{1}{4ST}\sideset{}{'}\sum_{|s|\le S,|t|\le T}\sum_{\substack{p\le x\\ a_p(E_{\mathfrak{P}_{m(s,t)}})=r}} 1,\\
\frac{1}{2S}\sideset{}{'}\sum_{|s|\le S}\pi^r_{E_{\mathfrak{P}_{m(s)}}}(x) &= \frac{1}{2S}\sideset{}{'}\sum_{|s|\le S}\sum_{\substack{p\le x\\ a_p(E_{\mathfrak{P}_{m(s)}})=r}} 1,
\end{aligned}\tag{27}$$

Recall that $m \mid \#E(\mathbb{F}_p)$. Therefore, $r = a_p(E) = p+1-\#E(\mathbb{F}_p)$ implies that $r \equiv p+1 \bmod m$. Also, if $p \le B(r)$, then $r \ge 2\sqrt{p}$ so that by Hasse's bound, we should restrict p to those primes satisfying $B(r) < p \le x$:

$$\begin{aligned}
\frac{1}{4ST}\sideset{}{'}\sum_{|s|\le S,|t|\le T}\pi^r_{E_{\mathfrak{P}_{m(s,t)}}}(x) &= \frac{1}{4ST}\sideset{}{'}\sum_{|s|\le S,|t|\le T}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m\\ a_p(E_{\mathfrak{P}_{m(s,t)}})=r}} 1,\\
\frac{1}{2S}\sideset{}{'}\sum_{|s|\le S,|t|\le T}\pi^r_{E_{\mathfrak{P}_{m(s)}}}(x) &= \frac{1}{2S}\sideset{}{'}\sum_{|s|\le S}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m\\ a_p(E_{\mathfrak{P}_{m(s)}})=r}} 1.
\end{aligned}\tag{28}$$

Switching the order of summation,

$$\begin{aligned}
\frac{1}{4ST}\sideset{}{'}\sum_{|s|\le S,|t|\le T}\pi^r_{E_{\mathfrak{P}_{m(s,t)}}}(x) &= \frac{1}{4ST}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}}\sideset{}{'}\sum_{\substack{|s|\le S,|t|\le T\\ a_p(E_{\mathfrak{P}_{m(s,t)}})=r}} 1+\mathrm{O}(\log\log x),\\
\frac{1}{2S}\sideset{}{'}\sum_{|s|\le S}\pi^r_{E_{\mathfrak{P}_{m(s)}}}(x) &= \frac{1}{2S}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}}\sideset{}{'}\sum_{\substack{|s|\le S\\ a_p(E_{\mathfrak{P}_{m(s)}})=r}} 1+\mathrm{O}(\log\log x),
\end{aligned}\tag{29}$$

with the error terms representing those curves which reduce to singular curves over $\mathbb{F}_p$.

Consider the inner summations above; in particular, note that the assumption $a_p(E) = r$ depends only on the congruence classes of the parameters of $E_{\mathcal{P}_m}$ modulo p. Thus we may estimate

$$\begin{aligned}\sideset{}{'}\sum_{\substack{|s|\le S,|t|\le T\\ a_p(E_{\mathcal{P}_m(s,t)})=r}} 1 &= \left(\frac{4ST}{p^2} + \mathrm{O}\left(\frac{S+T+p}{p}\right)\right) \sideset{}{'}\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m(s,t)})=r}} 1,\\ \sideset{}{'}\sum_{\substack{|s|\le S\\ a_p(E_{\mathcal{P}_m(s)})=r}} 1 &= \left(\frac{2S}{p} + \mathrm{O}(1)\right) \sideset{}{'}\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r}} 1.\end{aligned} \tag{30}$$

Substituting (30) into (29) and simplifying gives (26). □

By Corrollary 2.2, $E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{d\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}$ where $d \mid m$. We therefore write the inner summations of equation 26 as:

$$\sideset{}{'}\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m(s,t)})=r}} 1 = \sum_{d\mid m} \sideset{}{'}\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m(s,t)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/d\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}} 1 \tag{31}$$

and

$$\sideset{}{'}\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r}} 1 = \sum_{d\mid m} \sideset{}{'}\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/d\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}} 1. \tag{32}$$

The inner summations above can be written in terms of the number of certain isomorphism classes $E/\mathbb{F}_p$:

$$\begin{aligned}\sideset{}{'}\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/d\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}} 1 &= \#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p)\#\left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{d\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}\right\}\\ &= \#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p)N_{p,r}(d,m).\end{aligned} \tag{33}$$

Definition 2.14 *To simplify the following lemmas, let*

$$\begin{aligned}A_p &= \left(\frac{1}{p^2} + \mathrm{O}\left(\frac{1}{Sp} + \frac{1}{Tp} + \frac{1}{ST}\right)\right), \text{ and}\\ B_p &= \left(\frac{1}{p} + \mathrm{O}\left(\frac{1}{S}\right)\right).\end{aligned} \tag{34}$$

Lemma 2.15 *Fix $m \in \{2,3\}$ and $p \equiv r-1 \bmod m$. Then,*

$$\frac{1}{4ST}\sideset{}{'}\sum_{|s|\le S,|t|\le T} \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_p\left(\frac{p}{2}H(r^2-4p) + \mathrm{O}(p)\right) + \mathrm{O}(\log\log x) + S \tag{35}$$

Where

$$S = \begin{cases} \sum\limits_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod m^2}} \frac{mpA_p}{2} H\left(\frac{r^2-4p}{m^2}\right) & \text{if } r \equiv 2 \bmod m \text{ and } r \neq 0 \\ \sum\limits_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod m^2}} \frac{mpA_p}{2} h(-p) & \text{if } r \equiv 2 \bmod m, r = 0 \text{ and } m = 2 \\ 0 & \text{otherwise} \end{cases} \tag{36}$$

Proof. Combining Facts 2.4 and 2.6 we obtain

$$\#\mathcal{P}_m(E/\mathbb{F}_p) = \begin{cases} 1 & \text{if } E \text{ has cyclic 2- or 3-torsion,} \\ 3 & \text{if } E \text{ has full 2-torsion,} \\ 4 & \text{if } E \text{ has full 3-torsion.} \end{cases} \tag{37}$$

If we substitute the above into Equation (17) (see Fact 2.7),

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \left\{ \begin{array}{ll} 1/6 & \text{if } a = 0,\ p \equiv 1 \bmod 3, \text{ and } E \text{ has cyclic 2- or 3-torsion,} \\ 1/4 & \text{if } b = 0,\ p \equiv 1 \bmod 4, \text{ and } E \text{ has cyclic 2- or 3-torsion,} \\ 1/2 & \text{otherwise, if } E \text{ has cyclic 2- or 3-torsion,} \\ 1/2 & \text{if } a = 0,\ p \equiv 1 \bmod 3, \text{ and } E \text{ has full 2-torsion,} \\ 3/4 & \text{if } b = 0,\ p \equiv 1 \bmod 4, \text{ and } E \text{ has full 2-torsion,} \\ 3/2 & \text{otherwise, if } E \text{ has full 2-torsion,} \\ 2/3 & \text{if } a = 0,\ p \equiv 1 \bmod 3, \text{ and } E \text{ has full 3-torsion,} \\ 1 & \text{if } b = 0,\ p \equiv 1 \bmod 4, \text{ and } E \text{ has full 3-torsion,} \\ 2 & \text{otherwise, if } E \text{ has full 3-torsion.} \end{array} \right\} (p-1). \tag{38}$$

Note that the exceptional cases are very rare (there are at most 10) so we may estimate

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \left\{ \begin{array}{ll} 1/2 & \text{if } E \text{ has cyclic 2- or 3-torsion,} \\ 3/2 & \text{if } E \text{ has full 2-torsion,} \\ 2 & \text{if } E \text{ has full 3-torsion,} \end{array} \right\} (p-1). \tag{39}$$

By 2.12, we see that

$$\begin{aligned} N_{p,r}(1,m) &= N_{p,r}(m) - N'_{p,r}(m), \text{ and} \\ N_{p,r}(m,m) &= N'_{p,r}(m). \end{aligned} \tag{40}$$

Substituting the above into(33) gives us

$$\sum_{\substack{0\leq s,t<p \\ a_p(E_{\mathcal{P}_m(s,t)})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{1}{2} p N_{p,r}(m) - \frac{1}{2} p N'_{p,r}(m) + \mathrm{O}(p), \tag{41}$$

$$\sum_{\substack{0\leq s,t<p \\ a_p(E_{\mathcal{P}_m(s,t)})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \left\{ \begin{array}{ll} 3/2 & \text{if } m = 2, \\ 2 & \text{if } m = 3, \end{array} \right\} p N'_{p,r}(m) + \mathrm{O}(p), \tag{42}$$

with the error term representing the contribution from the exceptional curves in (39).

Combining (41) and (42) with (**??**) yields

$$\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m(s,t)})=r}}{}' 1 = \frac{1}{2}pN_{p,r}(m) + \frac{m}{2}pN'_{p,r}(m) + \mathrm{O}(p), \tag{43}$$

and plugging (43) into the right side of (26) gives

$$\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_p\frac{1}{2}pN_{p,r}(m) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_p\frac{m}{2}pN'_{p,r}(m) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_p\mathrm{O}(p) + \mathrm{O}(\log\log x). \tag{44}$$

Finally, we apply the results from **??** given in 2.10 to evaluate the above summations in terms of class numbers. Our claim then follows from considering each of the cases for when $N'_{p,r}(m)$ is nonzero.□

Lemma 2.16 *Fix $m \in \{5,7\}$ and $p \equiv r-1 \bmod m$. Then,*

$$\frac{1}{2S}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} B_p\frac{m-1}{2}H(r^2-4p) + \mathrm{O}(\log\log x) + S \tag{45}$$

Where

$$S = \begin{cases} \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m^2}} B_p\frac{m(m-1)}{2}H\left(\frac{r^2-4p}{m^2}\right) & \text{if } r\equiv 2 \bmod m \text{ and } r\neq 0\\ 0 & \text{otherwise} \end{cases} \tag{46}$$

Proof. Combining the results of Facts 2.4 and 2.6 and recalling that $\varphi(m) = m-1$ for m prime,

$$\#\mathcal{P}_m(E/\mathbb{F}_p) = \begin{cases} (m-1)/2 & \text{if } E \text{ has cyclic torsion,}\\ (m+1)(m-1)/2 & \text{if } E \text{ has full torsion.}\end{cases} \tag{47}$$

Again, the chart in Lemma 2.12 gives:

$$\begin{aligned} N_{p,r}(1,m) &= N_{p,r}(m) - N'_{p,r}(m), \text{ and}\\ N_{p,r}(m,m) &= N'_{p,r}(m).\end{aligned} \tag{48}$$

and since $m \notin \{2,3\}$ we have by Fact 2.7

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \#\mathcal{P}_m(E/\mathbb{F}_p). \tag{49}$$

We combine Equations (**??**–49) to get

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{m-1}{2}N_{p,r}(m) - \frac{m-1}{2}N'_{p,r}(m), \tag{50}$$

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{(m+1)(m-1)}{2}N'_{p,r}(m). \tag{51}$$

By substituting (50) and (51) into (**??**), we conclude

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r}}{}' \quad 1 = \frac{m-1}{2}N_{p,r}(m) + \frac{m(m-1)}{2}N'_{p,r}(m). \tag{52}$$

Plugging (43) into the right side of (26) gives

$$\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} B_p\frac{m-1}{2}N_{p,r}(m) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} B_p\frac{m(m-1)}{2}N'_{p,r}(m) + \mathrm{O}(\log\log x). \tag{53}$$

We apply the results from **??** given in 2.10, and our claim follows from considering each of the cases for when $N'_{p,r}(m)$ is nonzero.□

Lemma 2.17 *Fix $m \in \{6, 10\}$ and $p \equiv r-1 \bmod m$. Then $m = 2\ell$ for ℓ an odd prime. For simplicity, define the following:*

$$S_2 = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 2m}} B_p\varphi(m)H\left(\frac{r^2-4p}{4}\right), S_\ell = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod \ell m}} B_p\frac{\varphi(m)(\varphi(\ell)+1)}{2}H\left(\frac{r^2-4p}{\ell^2}\right)$$
$$S'_2 = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 2m}} B_p\varphi(m)h(-p), S_m = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m^2}} B_p\frac{m\varphi(m)}{2}H\left(\frac{r^2-4p}{m^2}\right) \tag{54}$$

We then have

$$\frac{1}{2S}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} B_p\frac{\varphi(m)}{2}H(r^2-4p) + \mathrm{O}(\log\log x) + S \tag{55}$$

where

$$S = \begin{cases} S_2+S_\ell+S_m & \text{if } r\equiv 2 \bmod m \text{ and } r\neq 0\\ S_2 & \text{if } r\equiv 2 \bmod 2, r\not\equiv 2 \bmod \ell, \text{and } r\neq 0\\ S_\ell & \text{if } r\equiv 2 \bmod \ell, r\not\equiv 2 \bmod 2, \text{and } r\neq 0\\ S'_2 & \text{if } r\equiv 2 \bmod 2 \text{ and } r=0\\ 0 & \text{otherwise}\end{cases} \tag{56}$$

Proof. By Corollary 2.2, Facts 2.6, 2.7, and 2.4, and the assumption that $m \notin \{2, 3\}$, we have

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \begin{cases} \varphi(m)/2 & \text{if } E \text{ has cyclic torsion,}\\ \varphi(m)(\varphi(q)+2)/2 & \text{if } E(\mathbb{F}_p)[m]\cong\mathbb{Z}/q\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}(q=2,\ell),\\ \varphi(m)(2(m+1)-\varphi(m))/2 & \text{if } E \text{ has full } m\text{-torsion.}\end{cases} \tag{57}$$

By the chart in Lemma 2.12 we have,

$$\begin{aligned} N_{p,r}(1,m) &= N_{p,r}(2\ell) - N'_{p,r}(2) - N'_{p,r}(\ell) + N'_{p,r}(2\ell) \\ N_{p,r}(2,m) &= N'_{p,r}(2) - N'_{p,r}(2\ell) \\ N_{p,r}(\ell,m) &= N'_{p,r}(\ell) - N'_{p,r}(2\ell) \\ N_{p,r}(m,m) &= N'_{p,r}(2\ell). \end{aligned} \tag{58}$$

Therefore, combining Equations (**??**–**??**) and Fact 2.10, we find for $r \neq 0$,

$$\sum_{\substack{0\leq s<p \\ a_p(E_{\mathcal{P}_{m(s)}})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{\varphi(m)}{2}\left(N_{p,r}(m) - N'_{p,r}(2) - N'_{p,r}(\ell) + N'_{p,r}(m)\right), \tag{59}$$

as well as

$$\sum_{\substack{0\leq s<p \\ a_p(E_{\mathcal{P}_{m(s)}})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/q\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{\varphi(m)}{2}(\varphi(q)+2)\left(N'_{p,r}(q) - N'_{p,r}(m)\right), \text{ and} \tag{60}$$

$$\sum_{\substack{0\leq s<p \\ a_p(E_{\mathcal{P}_{m(s)}})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{\varphi(m)}{2}\big(2(m+1) - \varphi(m)\big)N'_{p,r}(m). \tag{61}$$

Substituting (59–61) into (**??**) and collecting terms, we find

$$\begin{aligned} \sum_{\substack{0\leq s<p \\ a_p(E_{\mathcal{P}_{m(s)}})=r}}{}' 1 = \frac{\varphi(m)}{2}N_{p,r}(m) + \varphi(m)N'_{p,r}(2) + \frac{(\varphi(\ell)+1)\varphi(m)}{2}N'_{p,r}(\ell) \\ + \frac{\varphi(m)}{2}\big(2(m-1) - \varphi(m) - \varphi(\ell)\big)N'_{p,r}(m). \end{aligned} \tag{62}$$

Also note that $2(m-1) - \varphi(m) - \varphi(\ell) = m$. Plugging (62) into the right side of (26), simplifying as usual, and applying the results from **??** as usual proves our claim.□

Lemma 2.18 *Fix $m \in \{4, 9\}$ and $p \equiv r - 1 \bmod m$. Then $m = \ell^2$ for ℓ a prime. For simplicity, define the following:*

$$S_\ell = \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod m}} B_p \frac{\varphi(\ell)\varphi(m)}{2} H\left(\frac{r^2-4p}{m}\right), S_m = \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod m^2}} B_p \frac{\varphi(m)}{2}\left(1+\varphi(\ell)+\varphi(m)\right) H\left(\frac{r^2-4p}{m^2}\right)$$

$$S'_\ell = \begin{cases} \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 4}} B_p \frac{\varphi(\ell)\varphi(m)}{2} h(-p) & \text{if } m = 4 \\ 0 & \text{if } m = 9 \end{cases} \tag{63}$$

We then have

$$\frac{1}{2S}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} B_p\frac{\varphi(\ell)\varphi(m)}{2}H(r^2-4p) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod \ell m}} B_p\frac{\varphi(m)}{2}(\varphi(\ell)+1)H(r^2-4p) + \mathrm{O}(\log\log x) + S \tag{64}$$

where

$$S = \begin{cases} S_\ell + S_m & \text{if } r\equiv 2 \bmod m \text{ and } r\neq 0\\ S_\ell & \text{if } r\equiv 2 \bmod \ell, r\not\equiv 2 \bmod m, \text{and } r\neq 0\\ S'_\ell & \text{if } r\equiv 2 \bmod \ell \text{ and } r=0\\ 0 & \text{otherwise}\end{cases} \tag{65}$$

Proof. By Corollary 2.2, Facts 2.6, 2.7, and 2.4, and the assumption that $m\notin\{2,3\}$, we have

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \begin{cases} \varphi(m)/2 & \text{if } E \text{ has cyclic torsion,}\\ \varphi(m)(\varphi(\ell)+1)/2 & \text{if } E(\mathbb{F}_p)[m]\cong\mathbb{Z}/\ell\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z},\\ \varphi(m)(2+2\varphi(\ell)+\varphi(m))/2 & \text{if } E \text{ has full } m\text{-torsion.}\end{cases} \tag{66}$$

By the chart in Lemma 2.12 we have,

$$\begin{aligned} N_{p,r}(1,m) &= N_{p,r}(\ell^2) - N'_{p,r}(\ell)\\ N_{p,r}(\ell,m) &= N_{p,r}(\ell^3) - N_{p,r}(\ell^2) - N'_{p,r}(\ell^2) + N'_{p,r}(\ell)\\ N_{p,r}(m,m) &= N'_{p,r}(\ell^2).\end{aligned} \tag{67}$$

The rest of the proof is identical to the previous cases so it will not be repeated.□
The proofs for the cases where $m = 8, 12$ use the same methods as the previous cases, thus only the statements of the lemmas will be given.

Lemma 2.19 *Let $m = 8$ and $p\equiv r-1 \bmod 8$. For simplicity, define the following:*

$$\begin{aligned} S_2 &= \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 8}} 2B_pH\left(\frac{r^2-4p}{4}\right), S_4 = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 16}} 4B_pH\left(\frac{r^2-4p}{16}\right)\\ S'_2 &= \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 8}} 2B_p\varphi(m)h(-p), S_m = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 64}} 32B_pH\left(\frac{r^2-4p}{64}\right)\end{aligned} \tag{68}$$

We then have

$$\frac{1}{2S}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 8}} (-2)B_pH(r^2-4p) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod 16}} 4B_pH(r^2-4p) + \mathrm{O}(\log\log x) + S \tag{69}$$

where

$$S = \begin{cases} S_2 + S_4 + S_8 & \text{if } r \equiv 2 \bmod 8 \text{ and } r \neq 0 \\ S_2 + S_4 & \text{if } r \equiv 2 \bmod 4, r \not\equiv 2 \bmod 8, \text{and } r \neq 0 \\ S_2 & \text{if } r \equiv 2 \bmod 2, r \not\equiv 2 \bmod 4, \text{and } r \neq 0 \\ S_2' & \text{if } r \equiv 2 \bmod 2 \text{ and } r = 0 \\ 0 & \text{otherwise} \end{cases} \tag{70}$$

Lemma 2.20 *Let $m = 12$ and $p \equiv r - 1 \bmod 12$. For simplicity, define the following:*

$$\begin{aligned} S_2 &= \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 12}} 2B_p H\left(\frac{r^2-4p}{4}\right), S_3 = \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 36}} 6B_p H\left(\frac{r^2-4p}{9}\right), \\ S_6 &= \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 36}} 14B_p H\left(\frac{r^2-4p}{36}\right), S_2' = \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 12}} 2B_p h(-p) \\ S_4 &= \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 48}} 8B_p \varphi(m) H\left(\frac{r^2-4p}{16}\right), S_1 2 = \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 144}} 24B_p H\left(\frac{r^2-4p}{144}\right) \end{aligned} \tag{71}$$

We then have

$$\begin{aligned} \frac{1}{2S}\sum_{|s|\leq S,|t|\leq T}{}' \pi^r_{E_{\mathfrak{P}_m(s,t)}}(x) = &\sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 12}} (-14)B_p H(r^2-4p) + \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 24}} 4B_p H(r^2-4p) \\ &+ \sum_{\substack{B(r)<p\leq x \\ p\equiv r-1 \bmod 48}} 12B_p H(r^2-4p) + \mathrm{O}(\log\log x) + S \end{aligned} \tag{72}$$

where

$$S = \begin{cases} S_2 + S_3 + S_4 + S_6 + S_{12} & \text{if } r \equiv 2 \bmod 12 \text{ and } r \neq 0 \\ S_2 + S_3 + S_6 & \text{if } r \equiv 2 \bmod 6, r \not\equiv 2 \bmod 4, \text{and } r \neq 0 \\ S_2 + S_4 & \text{if } r \equiv 2 \bmod 4, r \not\equiv 2 \bmod 3, \text{and } r \neq 0 \\ S_2 & \text{if } r \equiv 2 \bmod 2, r \not\equiv 2 \bmod 4, r \not\equiv 2 \bmod 3, \text{and } r \neq 0 \\ S_3 & \text{if } r \equiv 2 \bmod 3, r \not\equiv 2 \bmod 2, \text{and } r \neq 0 \\ S_2' & \text{if } r \equiv 2 \bmod 2 \text{ and } r = 0 \\ 0 & \text{otherwise} \end{cases} \tag{73}$$

3 Averaging special values of Dirichlet L-series

We now turn our efforts towards estimating terms of the form

$$H\left(\frac{r^2-4p}{d^2}\right), \tag{74}$$

where r, m are fixed integers, d is a divisor of m, p is a prime, and H is the Kronecker class number. Our estimate depends crucially on averaging values of certain L-series.

3.1 Working with class numbers

Definition 3.1 *Set*

$$\Delta_f^r(p) = \frac{r^2-4p}{f^2}, \tag{75}$$

$$\begin{aligned}\mathcal{S}_f^{r,m} = \{&B(r) < p \le x : p \equiv r-1 \bmod m,\\ &4p \equiv r^2 \bmod f^2,\ \Delta_f^r(p) \equiv 0,1 \bmod 4\}.\end{aligned} \tag{76}$$

Where convenient, we will write Δ without some of its arguments and parameters. In particular, we will abbreviate $\Delta_f^r(p)$ by Δ.

Fact 3.2 (Class number formula) *If $\Delta < 0$, then we have*

$$h(\Delta) = \frac{\omega(\Delta)\sqrt{-\Delta}}{2\pi} L(1,\chi_\Delta). \tag{77}$$

Lemma 3.3 *Fix x, r, m and let p be a prime with $B(r) < p \le x$. We have*

$$H\left(\frac{r^2-4p}{d^2}\right) = \frac{1}{\pi} \sum_{\substack{d\mid f\\ f^2\mid r^2-4p\\ \Delta\equiv 0,1 \bmod 4}} L(1,\chi_\Delta)\sqrt{-\Delta}. \tag{78}$$

In particular, we may write

$$\begin{aligned}\frac{1}{2} \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} \frac{1}{p} H\left(\frac{r^2-4p}{d^2}\right) &= \frac{1}{\pi\sqrt{x}\log x} \sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}} \frac{1}{f} \sum_{p\in \mathcal{S}_f^{r,m}(x)} L(1,\chi_\Delta)\log p\\ &- \frac{1}{\pi}\int_2^x \sum_{\substack{f\le 2\sqrt{t}\\ d\mid f}} \left(\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(t)} L(1,\chi_\Delta)\log p\right) \frac{d}{dt}\left(\frac{1}{\sqrt{t}\log t}\right) dt + \mathrm{O}(\log^2 x).\end{aligned} \tag{79}$$

Proof. By Fact 2.9, we have

$$H\left(\frac{r^2-4p}{d^2}\right) = 2 \sum_{\substack{f^2\mid (r^2-4p)/d^2\\ \Delta_{df}\equiv 0,1 \bmod 4}} \frac{h(\Delta_{df})}{\omega(\Delta_{df})}. \tag{80}$$

It is clear that $f^2 \mid (r^2-4p)/d^2$ iff $(df)^2 \mid r^2-4p$. Replace df by f with the additional condition that $d \mid f$:

$$H\left(\frac{r^2-4p}{d^2}\right) = 2 \sum_{\substack{d\mid f\\ f^2\mid r^2-4p\\ \Delta\equiv 0,1 \bmod 4}} \frac{h(\Delta)}{\omega(\Delta)}. \tag{81}$$

Because $p > B(r)$, $r^2-4p < 0$ and $\Delta < 0$, so the class number formula gives

$$h(\Delta) = \frac{\omega(\Delta)\sqrt{-\Delta}}{2\pi} L(1,\chi_\Delta), \tag{82}$$

and (78) now follows from combining (82) and (81).

Substitute to obtain

$$\frac{1}{2}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}}\frac{1}{p}H\left(\frac{r^2-4p}{d^2}\right)=\frac{1}{2\pi}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}}\frac{1}{p}\sum_{\substack{d|f\\ f^2|r^2-4p\\ \Delta\equiv 0,1 \bmod 4}}\frac{L(1,\chi_\Delta)\sqrt{4p-r^2}}{f}. \tag{83}$$

Switching the order of summation and then approximating $\sqrt{4p-r^2}=2\sqrt{p}+\mathrm{O}(1)$ yields

$$\begin{aligned}\frac{1}{2}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}}\frac{1}{p}H\left(\frac{r^2-4p}{d^2}\right)&=\frac{1}{2\pi}\sum_{\substack{f\le 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}\frac{\sqrt{4p-r^2}}{p}L(1,\chi_\Delta),\\ &=\frac{1}{\pi}\sum_{\substack{f\le 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}\frac{L(1,\chi_\Delta)}{\sqrt{p}}+\mathrm{O}(\log^2 x),\end{aligned} \tag{84}$$

and partial summation gives

$$\begin{aligned}\sum_{\substack{f\le 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}\frac{L(1,\chi_\Delta)}{\sqrt{p}}&=\frac{1}{\sqrt{x}\log x}\sum_{\substack{f\le 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}L(1,\chi_\Delta)\log p\\ &\quad-\int_2^x\sum_{\substack{f\le 2\sqrt{t}\\ d|f}}\left(\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(t)}L(1,\chi_\Delta)\log p\right)\frac{d}{dt}\left(\frac{1}{\sqrt{t}\log t}\right)\,dt.\end{aligned} \tag{85}$$

The result follows. □

3.2 Analytic results

We now state some analytic results which will be used in the proof of the main theorem in this section.

Fact 3.4 (Polyá-Vinogradov inequality) *For any nonprincipal Dirichlet character χ modulo q, we have*

$$\sum_{n>N}\chi(n)\ll\sqrt{q}\log q, \tag{86}$$

and in particular, for $\Delta<0$,

$$\sum_{n>N}\left(\frac{\Delta}{n}\right)=\sqrt{-\Delta}\log(-\Delta). \tag{87}$$

Fact 3.5 (Barban, Davenport, and Halberstam) *Let $(a,n)=1$ and define*

$$\psi_1(x;n,a)=\sum_{\substack{p\le x\\ p\equiv a \bmod n}}\log p, \tag{88}$$

$$E_1(x;n,a)=\psi_1(x;n,a)-\frac{x}{\varphi(n)}. \tag{89}$$

Using the notation above, for any $c > 0$ and Q satisfying $x \log^{-c} x \le Q \le x$, we have

$$\sum_{n \le Q} \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} E_1^2(x; n, a) \ll Qx \log x. \tag{90}$$

Fact 3.6 (David and Pappalardi) *Define*

$$L = \prod_{\ell} \left(1 + \frac{1}{\ell(\sqrt{\ell} - 1)}\right). \tag{91}$$

Then

$$\sum_{n > U} \frac{1}{\kappa(n)\varphi(n)} \sim \frac{L}{\sqrt{U}}, \tag{92}$$

and in particular, $\displaystyle\sum_{n=1}^{\infty} \frac{1}{\kappa(n)\varphi(n)}$ *converges.*

(References here.)

Lemma 3.7 *Let x, m, r, f be fixed. Then*

$$\sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ (a,n)=1}} \left(\frac{a}{n}\right) \sum_{\substack{p \in \mathcal{S}_f^{r,m}(x) \\ \Delta \equiv a \bmod 4n}} \left(\frac{\Delta}{n}\right) \log p$$

$$= \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ (a,n)=1,\, a \equiv 0,1 \bmod 4 \\ 4(r-1) \equiv r^2 - af^2 \bmod 4(nf^2, m) \\ (r-1,m)=1,\, (r^2-af^2, 4nf^2)=4}} \left(\frac{a}{n}\right) \psi_1(x; [nf^2, m], b) + \mathrm{O}(n), \tag{93}$$

where each $b \in \mathbb{Z}/[nf^2, m]\mathbb{Z}$ is determined uniquely by m, r, f, a.

Proof. The conditions under the inner sum on the left hand side hold iff $B(r) < p \le x$ and the following congruences hold:

$$p \equiv r - 1 \bmod m, \tag{94}$$
$$4p \equiv r^2 \bmod f^2, \tag{95}$$
$$4p \equiv r^2, r^2 - f^2 \bmod 4f^2, \text{ and} \tag{96}$$
$$4p \equiv r^2 - af^2 \bmod 4nf^2. \tag{97}$$

Congruence (96) implies (95), so we can ignore (95) altogether. Congruences (96) and (97) are compatible only if

$$r^2 - af^2 \equiv r^2, r^2 - f^2 \bmod 4f^2, \tag{98}$$

or equivalently, only if $a \equiv 0, 1 \bmod 4$. In such a case, (97) implies (96), so we are left with the congruences

$$p \equiv r - 1 \bmod m, \tag{99}$$
$$4p \equiv r^2 - af^2 \bmod 4nf^2, \tag{100}$$

and the preliminary assumption that $a \equiv 0, 1 \bmod 4$. Congruences (99) and (100) are compatible only if

$$4(r-1) \equiv r^2 - af^2 \bmod 4(nf^2, m). \tag{101}$$

By the Chinese remainder theorem, if the congruences are compatible there exists a unique $b \in \mathbb{Z}/[nf^2, m]\mathbb{Z}$ such that

$$b \equiv r - 1 \bmod m, \quad \text{and} \quad b \equiv \tfrac{1}{4}(r^2 - af^2) \bmod nf^2. \tag{102}$$

We may therefore write

$$\sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ (a,n)=1}} \left(\frac{a}{n}\right) \sum_{\substack{p \in \mathcal{S}_f^{r,m}(x) \\ \Delta \equiv a \bmod 4n}} \log p = \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ (a,n)=1,\ a \equiv 0,1 \bmod 4 \\ 4(r-1) \equiv r^2 - af^2 \bmod 4(nf^2, m)}} \left(\frac{a}{n}\right) \sum_{\substack{B(r) < p \leq x \\ p \equiv b \bmod [nf^2, m]}} \log p. \tag{103}$$

Note that $(b, [nf^2, m]) = 1$ iff $(r-1, m) = 1$ and $(4nf^2, r^2 - af^2) = 4$; with these assumptions,

$$\sum_{\substack{B(r) < p \leq x \\ p \equiv b \bmod [nf^2, m]}} \log p = \psi_1(x; [nf^2, m], b) + \mathrm{O}(1), \tag{104}$$

where the error term represents those primes less than $B(r)$. In the case where our coprimality conditions do not hold there is at most one prime which satisifies the congruence (as opposed to infinitely many) and these cases do not contribute an appreciable error.

Substituting (104) into (103) establishes (93). □

3.3 Statement and proof of the theorem

Theorem 3.8 *Let x, m, r be fixed and let d be a divisor of m. For any $c > 0$,*

$$\sum_{\substack{f \leq 2\sqrt{x} \\ d | f}} \frac{1}{f} \sum_{p \in \mathcal{S}_f^{r,m}(x)} L(1, \chi_\Delta) \log p = K^{r,m,d} x + \mathrm{O}\left(\frac{x}{\log^c x}\right), \tag{105}$$

where $K^{r,m,d}$ is a constant given by $K^{r,m,d} = 0$ if $(r-1, m) \neq 1$ and by

$$K^{r,m,d} = \sum_{\substack{f=1 \\ d|f}}^{\infty} \sum_{n=1}^{\infty} \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} \quad \textit{with} \quad c_f^{r,m}(n) = \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ (a,n)=1,\ a \equiv 0,1 \bmod 4 \\ 4(r-1) \equiv r^2 - af^2 \bmod 4(nf^2, m) \\ (r^2 - af^2, 4nf^2) = 4}} \left(\frac{a}{n}\right), \tag{106}$$

otherwise.

Proof. Fix a parameter $U > 0$ to be chosen later; we write

$$L(1, \chi_\Delta) = \sum_{n \geq 1} \left(\frac{\Delta}{n}\right) \frac{1}{n} = \sum_{n \leq U} \left(\frac{\Delta}{n}\right) \frac{1}{n} + \sum_{n > U} \left(\frac{\Delta}{n}\right) \frac{1}{n}. \tag{107}$$

Note that

$$\sum_{n>U}\left(\frac{\Delta}{n}\right)\frac{1}{n}<\sum_{n>U}\left(\frac{\Delta}{n}\right)\frac{1}{U}, \tag{108}$$

so that by the Polyá-Vinogradov inequality, we have

$$\sum_{n>U}\left(\frac{\Delta}{n}\right)\ll\sqrt{-\Delta}\log(-\Delta), \tag{109}$$

$$L(1,\chi_\Delta)=\sum_{n\geq 1}\left(\frac{\Delta}{n}\right)\frac{1}{n}=\sum_{n\leq U}\left(\frac{\Delta}{n}\right)\frac{1}{n}+\mathrm{O}\left(\frac{\sqrt{-\Delta}\log(-\Delta)}{U}\right). \tag{110}$$

Because $\Delta=\mathrm{O}(p/f^2)$, we have

$$L(1,\chi_\Delta)=\sum_{n\geq 1}\left(\frac{\Delta}{n}\right)\frac{1}{n}=\sum_{n\leq U}\left(\frac{\Delta}{n}\right)\frac{1}{n}+\mathrm{O}\left(\frac{\sqrt{p}\log p}{fU}\right). \tag{111}$$

Substituting into (105), we find

$$\begin{aligned}\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}&L(1,\chi_\Delta)\log p\\ &=\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in S_f^{r,m}(x)}\left(\frac{\Delta}{n}\right)\log p+\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in S_f^{r,m}(x)}\mathrm{O}\left(\frac{\sqrt{p}\log^2 p}{fU}\right)\end{aligned} \tag{112}$$

Considering the sum over the error term, we have

$$\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}\mathrm{O}\left(\frac{\sqrt{p}\log^2 p}{fU}\right)=\mathrm{O}\left(\frac{1}{U}\right)\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\mathrm{O}\left(\frac{1}{f^2}\right)\sum_{p\in\mathcal{S}_f^{r,m}(x)}\mathrm{O}(\sqrt{p}\log^2 p), \tag{113}$$

Note that

$$\sum_{p\in\mathcal{S}_f^{r,m}(x)}\sqrt{p}\log^2 p\leq\sum_{p\leq x}\sqrt{p}\log^2 p\leq\sum_{n\leq x}\sqrt{n}\log^2 n\leq x^{3/2}\log^2 x\leq x^{5/2}\log x. \tag{114}$$

Then

$$\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}\mathrm{O}\left(\frac{\sqrt{p}\log^2 p}{fU}\right)=\mathrm{O}\left(\frac{x^{5/2}\log x}{U}\right)\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\mathrm{O}\left(\frac{1}{f^2}\right) \tag{115}$$

$$=\mathrm{O}\left(\frac{x^{3/2}\log x}{U}\right). \tag{116}$$

Substitution gives

$$\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}L(1,\chi_\Delta)\log p=\sum_{\substack{f\leq 2\sqrt{x}\\ d|f}}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in\mathcal{S}_f^{r,m}(x)}\left(\frac{\Delta}{n}\right)\log p+\mathrm{O}\left(\frac{x^{3/2}\log x}{U}\right). \tag{117}$$

Fix a second parameter V with $1 \le V \le 2\sqrt{x}$ and write

$$\sum_{\substack{f \le 2\sqrt{x} \\ d \mid f}} \frac{1}{f} \sum_{n \le U} \frac{1}{n} \sum_{p \in \mathcal{S}_f^{r,m}(x)} \left(\frac{\Delta}{n}\right) \log p = \sum_{\substack{f \le V \\ d \mid f}} \frac{1}{f} \sum_{n \le U} \frac{1}{n} \sum_{p \in \mathcal{S}_f^{r,m}(x)} \left(\frac{\Delta}{n}\right) \log p + \sum_{\substack{V < f \le 2\sqrt{x} \\ d \mid f}} \frac{1}{f} \sum_{n \le U} \frac{1}{n} \sum_{p \in \mathcal{S}_f^{r,m}(x)} \left(\frac{\Delta}{n}\right) \log p. \quad (118)$$

The sum over the larger values of f can be bounded. First we note that the middle sum is bounded by $\log U$, and the innermost sum is bounded by $\log x \sum_p (\Delta/n)$ for $p \in \mathcal{S}_f^{r,m}(x)$. Note also that $\sum_p (\Delta/n)$ is bounded by the function which counts those $n \le x$ with $4n \equiv r^2 \bmod f^2$. By relaxing the second and third conditions on our outermost sum, we conclude that

$$\left| \sum_{\substack{V < f \le 2\sqrt{x} \\ d \mid f}} \frac{1}{f} \sum_{n \le U} \frac{1}{n} \sum_{p \in \mathcal{S}_f^{r,m}(x)} \left(\frac{\Delta}{n}\right) \log p \right| \le \log x \log U \sum_{V < f \le 2\sqrt{x}} \frac{1}{f} \sum_{\substack{n \le x \\ 4n \equiv r^2 \bmod f^2}} 1. \quad (119)$$

In the above, the inner sum is clearly bounded by x/f^2, so

$$\left| \sum_{\substack{V < f \le 2\sqrt{x} \\ d \mid f}} \frac{1}{f} \sum_{n \le U} \frac{1}{n} \sum_{p \in \mathcal{S}_f^{r,m}(x)} \left(\frac{\Delta}{n}\right) \log p \right| \le x \ll x \log x \log U \sum_{V < f \le 2\sqrt{x}} \frac{1}{f^3} \ll \frac{x \log x \log U}{V^2}. \quad (120)$$

Combining with (117), we find

$$\sum_{\substack{f \le 2\sqrt{x} \\ d \mid f}} \frac{1}{f} \sum_{p \in \mathcal{S}_f^{r,m}} L(1, \chi_\Delta) \log p = \sum_{\substack{f \le V \\ d \mid f}} \frac{1}{f} \sum_{n \le U} \frac{1}{n} \sum_{p \in \mathcal{S}_f^{r,m}} \left(\frac{\Delta}{n}\right) \log p + \mathrm{O}\left(\frac{x^{3/2} \log x}{U} + \frac{x \log x \log U}{V^2}\right). \quad (121)$$

The main term is obtained from the sum over the smaller values of f. In particular, we will evaluate our sum by splitting the inner sum by the residue of Δ modulo $4n$. By general properties of the Kronecker symbol, $(\Delta/n) = 0$ when $(\Delta, n) > 1$. Thus, we may write

$$\sum_{\substack{f \le V \\ d \mid f}} \frac{1}{f} \sum_{n \le U} \frac{1}{n} \sum_{p \in \mathcal{S}_f^{r,m}} \left(\frac{\Delta}{n}\right) \log p = \sum_{\substack{n \le U, f \le V \\ d \mid f}} \frac{1}{nf} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ (a,n)=1}} \left(\frac{a}{n}\right) \sum_{\substack{p \in \mathcal{S}_f^{r,m}(x) \\ \Delta \equiv a \bmod 4n}} \log p. \quad (122)$$

Furthermore, by Lemma 3.7, we have

$$\sum_{\substack{f\le V\\ d\mid f}}\frac{1}{f}\sum_{n\le U}\frac{1}{n}\sum_{p\in\mathcal{S}_f^{r,m}}\left(\frac{\Delta}{n}\right)\log p$$
$$=\sum_{\substack{n\le U, f\le V\\ d\mid f,\ (r-1,m)=1}}\frac{1}{nf}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}}\left(\frac{a}{n}\right)\psi_1(x;[nf^2,m],b)+\mathrm{O}(U\log V). \quad (123)$$

Rewriting ψ_1 in terms of E_1, we have

$$\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1}}\left(\frac{a}{n}\right)\sum_{\substack{p\in\mathcal{S}_f^{r,m}(x)\\ \Delta\equiv a \bmod 4n}}\log p = x\sum_{\substack{n\le U, f\le V\\ d\mid f,\ (r-1,m)=1}}\frac{c_f^{r,m}(n)}{nf\varphi[nf^2,m]}$$
$$+\sum_{\substack{n\le U, f\le V\\ d\mid f,\ (r-1,m)=1}}\frac{1}{nf}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}}\left(\frac{a}{n}\right)E_1(x;[nf^2,m],b)+\mathrm{O}(U\log V). \quad (124)$$

(When $(r-1,m)\neq 1$, all but the error terms vanish in agreement with the proposition of the theorem. For the remainder of the proof we will consider the trivial case dealt with and assume only the nontrivial case wherein $(r-1,m)=1$.)

We will now show that the second summation is dominated by the error term. In particular, we apply the Cauchy-Schwarz inequality to obtain

$$\left|\sum_{\substack{n\le U, f\le V\\ d\mid f}}\frac{1}{nf}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4n\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}}\left(\frac{a}{n}\right)E_1(x;[nf^2,m],b)\right|$$
$$\le\sum_{f\le V}\frac{1}{f}\left(\sum_{n\le U}\frac{1}{n^2}\right)^{1/2}\left(\sum_{n\le U}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}}E_1^2(x;[nf^2,m],b)\right)^{1/2}. \quad (125)$$

Because $\sum_n n^{-2} \le \sum_n n^{-1} = \mathrm{O}(\log U)$, we may write

$$\sum_{\substack{n\le U, f\le V\\ d\mid f}} \frac{1}{nf} \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right) E_1(x;[nf^2,m],b)$$

$$\le \log^{1/2} U \sum_{f\le V} \frac{1}{f} \left(\sum_{n\le U} \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}} E_1^2(x;[nf^2,m],b) \right)^{1/2} \tag{126}$$

$$\le \log^{1/2} U \sum_{f\le V} \frac{1}{f} \left(\sum_{n\le U} \sum_{b\in(\mathbb{Z}/[nf^2,m]\mathbb{Z})^*} E_1^2(x;[nf^2,m],b) \right)^{1/2}.$$

We may conclude that

$$\sum_{\substack{n\le U, f\le V\\ d\mid f}} \frac{1}{nf} \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right) E_1(x;[nf^2,m],b)$$

$$\le \log^{1/2} U \log V \left(\sum_{N\le UV^2} \sum_{A\in(\mathbb{Z}/N\mathbb{Z})^*} E_1^2(x;N,A) \right)^{1/2}. \tag{127}$$

Setting $c>0$ and applying Fact 3.5, we find

$$\sum_{N\le UV^2} \sum_{A\in(\mathbb{Z}/N\mathbb{Z})^*} E_1^2(x;N,A) \le UV^2 x \log x \tag{128}$$

whenever

$$UV^2 \le \frac{x}{\log^{2c+6} x}. \tag{129}$$

so that

$$\sum_{\substack{n\le U, f\le V\\ d\mid f}} \frac{1}{nf} \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right) E_1(x;[nf^2,m],b) \le \log^{1/2} U \log V \frac{x}{\log^{c+2} x}, \tag{130}$$

showing that the left hand side is dominated by $\mathrm{O}(U \log V)$ when x is fixed. When $(r-1, m) = 1$, combining equations (list of equations combined) establishes the estimate

$$\sum_{\substack{f \le 2\sqrt{x} \\ d|f}} \frac{1}{f} \sum_{p \in \mathcal{S}_f^{r,m}(x)} L(1, \chi_\Delta) \log p = x \sum_{\substack{n \le U, f \le V \\ d|f}} \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} + \mathrm{O}\left(U \log V + \frac{x \log^{1/2} U \log V}{\log^{c+2} x} + \frac{x^{3/2} \log x}{U} + \frac{x \log x \log U}{V^2} \right). \quad (131)$$

It remains only to be shown that the coefficient summation of x tends to a constant as $U, V \to \infty$ and to define the parameters U and V explicitly in terms of x. First, we note that $|c_f^{r,m}(n)| \le 2n/\kappa(n)$ (see Lemma 4.7) and also that $\varphi[nf^2, m] \ge \varphi(n)\varphi(f^2) \ge 1$, we have

$$\left| \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} \right| \le \frac{2}{f\kappa(n)\varphi[nf^2, m]} \le \frac{1}{f\varphi(f^2)} \frac{2}{\kappa(n)\varphi(n)}. \quad (132)$$

By Fact 3.6

$$\begin{aligned} x \sum_{\substack{n \le U, f \le V \\ d|f}} \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} &= x \sum_{\substack{f \le V \\ d|f}} \sum_{n=1}^{\infty} \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} + \mathrm{O}\left(x \sum_{n > U} \frac{1}{\kappa(n)\varphi(n)} \sum_{f \le V} \frac{1}{f\varphi(f^2)} \right), \\ &= x \sum_{\substack{f \le V \\ d|f}} \sum_{n=1}^{\infty} \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} + \mathrm{O}\left(\frac{x}{\sqrt{U}} \right), \end{aligned} \quad (133)$$

and similarly we have

$$x \sum_{n=1}^{\infty} \frac{2}{\kappa(n)\varphi(n)} \sum_{f > V} \frac{1}{f\varphi(f^2)} = \mathrm{O}\left(\frac{x}{V^2} \right), \quad (134)$$

so that

$$x \sum_{\substack{n \le U, f \le V \\ d|f}} \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} = x \sum_{\substack{f=1 \\ d|f}}^{\infty} \sum_{n=1}^{\infty} \frac{c_f^{r,m}(n)}{nf\varphi[nf^2, m]} + \mathrm{O}\left(\frac{x}{\sqrt{U}} + \frac{x}{V^2} \right). \quad (135)$$

The above guarantees that the double infinite series over n, f converges to some constant $K^{r,m,d}$. We therefore shall write

$$\sum_{\substack{f \le 2\sqrt{x} \\ d|f}} \frac{1}{f} \sum_{p \in \mathcal{S}_f^{r,m}(x)} L(1, \chi_\Delta) \log p = K^{r,m,d} x + \mathrm{O}\left(U \log V + \frac{x \log^{1/2} U \log V}{\log^{c+2} x} + \frac{x^{3/2} \log x}{U} + \frac{x \log x \log U}{V^2} + \frac{x}{\sqrt{U}} + \frac{x}{V^2} \right). \quad (136)$$

where U, V satisfy (some equation). If we choose

$$U = \sqrt{x} \log^{c+1} x, \quad \text{and} \quad V^2 = \log^{c+2} x, \quad (137)$$

we find

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f^{r,m}(x)}L(1,\chi_\Delta)\log p = K^{r,m,d}x + \mathrm{O}\left(\frac{x}{\log^c x}\right), \tag{138}$$

as desired. □

4 The function $c_f^{r,m}$

4.1 Properties of $c_{f,i}^{r,m}$

We now wish to describe the behavior of the following function, which arises naturally in the computation of our average:

Definition 4.1 *For fixed values of m, r, f and $i = 0, 1$ we define*

$$c_{f,i}^{r,m}(n) = \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv i \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}}\left(\frac{a}{n}\right), \tag{139}$$

and set $c_f^{r,m}(n) = c_{f,0}^{r,m}(n) + c_{f,1}^{r,m}(n)$.

Fact 4.2 and Lemma 4.3 will be invaluable in the next part of this section and later in the paper, as they aid greatly in subsequent calculations.

Fact 4.2 *Suppose that $8\nmid m$. Then $c_{f,i}^{r,m}(n)$ is nonzero only if $(m,f)\mid(r-2)^2$. Also,*

1. *For $c_{f,0}^{r,m}(n)$ to be nonzero, we must have r even, n odd, and $(r/2,f)=1$;*
2. *For $c_{f,1}^{r,m}(n)$ to be nonzero, we must have*
   a. *r and f both odd and $(r,f)=1$,*
   b. *$r\equiv 2 \bmod 4$, $4\mid f$, and $(r/2,f)=1$,*
   c. *$4\mid r$, $f\equiv 2 \bmod 4$, and $(r,f/2)=1$.*

(While the above follows quickly from the given definition of $c_{f,i}^{r,m}$, we can refer the reader to [5] for more detail.)

Lemma 4.3 *$c_{f,i}^{r,m}(n)$ is a multiplicative arithmetic function of n.*

Proof. We first show that $c_{f,0}^{r,m}$ is multiplicative. In the case of r odd, we have $c_{f,0}^{r,m}(n)=0$; suppose then that r is even. There is a bijective correspondence between the set of residue classes a modulo $4n$ which are divisible by 4 and relatively prime to n and the set of invertible residue classes modulo n; furthermore, when n is odd, $(4/n)=1$. In particular, this allows us to write

$$c_{f,0}^{r,m}(n) = \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (4nf^2,r^2-af^2)=4}}\left(\frac{a}{n}\right) = \sum_{\substack{a\in(\mathbb{Z}/n\mathbb{Z})^*\\ (r/2-1)^2\equiv af^2 \bmod (nf^2,m)\\ (nf^2,(r/2)^2-af^2)=1}}\left(\frac{a}{n}\right). \tag{140}$$

For $c_{f,0}^{r,m}(n)$ to be nonzero, we also require that $(r/2, f) = 1$ and that $(m, f) \mid (r-2)^2$. We may therefore rewrite

$$c_{f,0}^{r,m}(n) = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{af^2}{(m,f)} \bmod\left(n, \frac{m}{(m,f)}\right) \\ ((r/2)^2 - af^2, n) = 1}} \left(\frac{a}{n}\right). \tag{141}$$

Now suppose we have $n = n_1 n_2$ with n_1 and n_2 relatively prime. We have

$$c_{f,0}^{r,m}(n_1) c_{f,0}^{r,m}(n_2) = \sum_{\substack{a_1 \in (\mathbb{Z}/n_1\mathbb{Z})^* \\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{a_1 f^2}{(m,f)} \bmod\left(n_1, \frac{m}{(m,f)}\right) \\ ((r/2)^2 - a_1 f^2, n_1) = 1}} \sum_{\substack{a_2 \in (\mathbb{Z}/n_2\mathbb{Z})^* \\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{a_2 f^2}{(m,f)} \bmod\left(n_2, \frac{m}{(m,f)}\right) \\ ((r/2)^2 - a_2 f^2, n_2) = 1}} \left(\frac{a_1}{n_1}\right)\left(\frac{a_2}{n_2}\right). \tag{142}$$

We can combine the summations as required using basic results of number theory; if $(n_1, n_2) = 1$ there is a natural bijection

$$\left(\frac{\mathbb{Z}}{n_1\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{n_2\mathbb{Z}}\right)^* \longrightarrow \left(\frac{\mathbb{Z}}{n_1 n_2 \mathbb{Z}}\right)^*. \tag{143}$$

More explicitly, let $a_1 \in (\mathbb{Z}/n_1\mathbb{Z})^*$ and $a_2 \in (\mathbb{Z}/n_2\mathbb{Z})^*$. Since $(n_1, n_2) = 1$, there is a unique $a \in \mathbb{Z}/n_1 n_2 \mathbb{Z}$ such that $a \equiv a_j \mod n_j$. Moreover, $(a, n_j) = 1$, so $a \in (\mathbb{Z}/n_1 n_2 \mathbb{Z})^*$. Because (a/n) is periodic with period n and the Kronecker symbol is bimultiplicative,

$$\left(\frac{a_1}{n_1}\right)\left(\frac{a_2}{n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right) = \left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n}\right). \tag{144}$$

Note that by the same application of the Chinese remainder theorem the congruences

$$\frac{(r/2-1)^2}{(m,f)} \equiv \frac{a_1 f^2}{(m,f)} \bmod \left(n_1, \frac{m}{(m,f)}\right), \text{ and} \tag{145}$$

$$\frac{(r/2-1)^2}{(m,f)} \equiv \frac{a_2 f^2}{(m,f)} \bmod \left(n_2, \frac{m}{(m,f)}\right) \tag{146}$$

hold iff

$$\frac{(r/2-1)^2}{(m,f)} \equiv \frac{af}{(m,f)} \bmod \left(n, \frac{m}{(m,f)}\right). \tag{147}$$

Now, $(\frac{1}{4}r^2 - a_j f^2, n_j) = 1$ iff there exist integers X, Y such that

$$(\tfrac{1}{4}r^2 - a_j f^2)X + n_j Y = 1. \tag{148}$$

But $a_j = a + k_j n_j$, so

$$(\tfrac{1}{4}r^2 - af^2)X' + n_j Y' = 1, \tag{149}$$

where $X' = X$ and $Y' = (k_j f^2 X + 1)Y$. Thus, $(\frac{1}{4}r^2 - af^2, n_j) = 1$ for $j = 1, 2$ which is true iff $(\frac{1}{4}r^2 - af^2, n) = 1$.
The converse follows from the same sort of argument, so

$$c_{f,0}^{r,m}(n_1) c_{f,0}^{r,m}(n_2) = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{af}{(m,f)} \bmod\left(n, \frac{m}{(m,f)}\right) \\ ((r/2)^2 - af^2, n) = 1}} \left(\frac{a}{n}\right) = c_{f,0}^{r,m}(n), \tag{150}$$

as desired.

We now turn to the case of $i = 1$; the details of the arguments are similar here. $c_{f,1}^{r,m}(n)$ is nonzero only if the conditions in 2a, 2b, or 2c hold. As in [1], we see that when n is odd, $(r^2 - af^2, 4nf^2) = 4$ if and only if $(r^2 - af^2, nf^2) = 1$. Thus,

$$c_{f,1}^{r,m}(n) = \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^*,\ a \equiv 1 \bmod 4 \\ r-1 \equiv r^2 - af^2 \bmod (nf^2, m) \\ (r^2 - af^2, nf^2) = 1}} \left(\frac{a}{n}\right). \tag{151}$$

As n is odd, there is a bijection between the invertible residues modulo $4n$ which are congruent to 1 modulo 4 and the invertible residues modulo n. Using arguments previously seen,

$$c_{f,1}^{r,m}(n) = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ \frac{(r-2)^2}{(m,f)} \equiv \frac{af^2}{(m,f)} \bmod \left(n, \frac{m}{(m,f)}\right) \\ (r^2 - af^2, n) = 1}} \left(\frac{a}{n}\right). \tag{152}$$

Furthermore, in cases 2b and 2c (see **??** for details)

$$c_{f,1}^{r,m}(n) = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{a(f/2)^2}{(m,f)} \bmod \left(n, \frac{m}{(m,f)}\right) \\ ((r/2)^2 - a(f/2)^2, n) = 1}} \left(\frac{a}{n}\right). \tag{153}$$

Now, let $n = n_1 n_2$ where $(n_1, n_2) = 1$. Multiplicativity in 2a follows from assuming without loss of generality that n_1 is odd and applying (152) and the Chinese remainder theorem. Cases 2b and 2c follow from equation (153) and the Chinese remainder theorem. □

4.2 Computation of $c_{f,i}^{r,m}$

For the sake of notation, if n is a positive integer and q is a prime, set $(n)_q = q^{\operatorname{ord}_q n}$. By Lemma 4.3, for all fixed values of i, r, m, f, n satisfying the conditions given in Fact 4.2, we may write

$$c_{f,i}^{r,m}(n) = \prod_{q \mid n} c_{f,i}^{r,m}(n)_q. \tag{154}$$

Accordingly, we will now attempt to give computations for $c_{f,i}^{r,m}(q^\alpha)$, where q is a prime and $\alpha \geq 0$.

Lemma 4.4 *Let $i = 0, 1$ and q be prime. If i, r, m, f, n satisfy the conditions given in Fact 4.2 and q is odd, define*

$$\sigma_i^r(f)_q = \begin{cases} 4(f)_q & \text{if } i = 1,\ r \equiv 2 \bmod 4, \text{ and } q \text{ is odd,} \\ 2(f)_q & \text{if } i = 1,\ 4 \mid r, \text{ and } q \text{ is odd,} \\ (f)_q & \text{otherwise,} \end{cases} \tag{155}$$

By definition, if $\beta \geq 0$, $\sigma_i^r(q^\beta)_q = \sigma_i^r(1)_q q^\beta$. We also have the following reduction:

$$c_{f,i}^{r,m}(q^\alpha) = c_{\sigma_i^r(f)_q, i}^{r,m}(q^\alpha), \tag{156}$$

where $\alpha \geq 0$.

Proof when $q = 2$. The idea of the proof is to show that when r and f satisfy one of the conditions under 2 in Fact 4.2, then $c_{f,1}^{r,m}(2^\alpha)$ can be written independently of f for each case. Since $(f)_2$ and r satisfy one of the conditions under 2 in Fact 4.2 as f and r, we have our desired equality.

First assume r and f satisfy condition 2a of Fact 4.2. This means r and f are odd, $(r, f) = 1$, and $(m, f) \mid (r-2)^2$. By definition,

$$c_{f,1}^{r,m}(2^\alpha) = \sum_{\substack{a \in \mathbb{Z}/2^{\alpha+2}\mathbb{Z} \\ (a,2^\alpha)=1,\ a \equiv 1 \bmod 4 \\ 4(r-1) \equiv r^2 - af^2 \bmod 4(2^\alpha f^2, m) \\ (2^{\alpha+2} f^2, r^2 - af^2) = 4}} \left(\frac{a}{2^\alpha}\right) \tag{157}$$

We simplify the conditions of the summation by noting the following:

a. We have $a \in \mathbb{Z}/2^{\alpha+2}\mathbb{Z}$ and $(a, 2^\alpha) = 1$ iff $a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^*$.

b. Since r and f are odd, the condition $(2^{\alpha+2} f^2, r^2 - af^2) = 4$ holds iff $(f^2, r^2 - af^2) = 1$, $r^2 - af^2 \equiv 0 \bmod 4$, $r^2 - af^2 \not\equiv 0 \bmod 8$. Since $(r, f) = 1$ we have $(f^2, r^2 - af^2) = 1$, and when given $a \equiv 1 \bmod 4$ and r, f odd, $r^2 - af^2 \equiv r^2 - f^2 \equiv 0 \bmod 4$. Finally, note that $r^2 - af^2 \not\equiv 0 \bmod 8$ and $a \equiv 1 \bmod 4$ iff $a \equiv 5 \bmod 8$. To see this, write $r = 2s + 1$, $f = 2t + 1$ to get

$$\begin{aligned} r^2 - af^2 &= 4t^2 - 4t + 1 - 4as^2 - 4as - a, \\ &= 4t(t-1) - 4as(s-1) + 1 - a, \\ &\equiv 1 - a \bmod 8. \end{aligned} \tag{158}$$

Now $a \equiv 1 \bmod 4$ iff $a \equiv 1 \bmod 8$ or $a \equiv 5 \bmod 8$. If $a \equiv 1 \bmod 8$ then $r^2 - af^2 \equiv 0 \bmod 8$ while $a \equiv 5 \bmod 8$ gives $r^2 - af^2 \not\equiv 0 \bmod 8$. We may now conclude that with our assumptions on r and f, $a \equiv 1 \bmod 4$ and $(a^{\alpha+2} f^2, r^2 - af^2) = 4$ iff $a \equiv 5 \bmod 8$.

c. We now want to show that the assumption $(m, f) \mid (r-2)^2$ allows us to get rid of $4(r-1) \equiv r^2 - af^2 \bmod 4(2^\alpha f^2, m)$. By simplification, we have $4(r-1) \equiv r^2 - af^2 \bmod 4(2^\alpha f^2, m)$ iff $(2^\alpha f^2, m) \mid (r-2)^2 + af^2$ which holds iff (m, f) and $(2^\alpha, m)$ both divide $\left((r-2)^2 + af^2\right)$.

First suppose $4 \mid m$ and $\alpha > 1$. Then we have $4 \mid (2^\alpha, m)$ but $4 \nmid (r-2)^2 + af^2$ so we must have $c_f^{r,m}(2^\alpha, 1) = 0$. Now consider all other cases. Since $(r-2)^2$ and af^2 are both odd, $(2^\alpha, m) = 2, 1$ divides $(r-2)^2 + af^2$. Since $(m, f) \mid af^2$, we have $(m, f) \mid (r-2)^2 + af^2$ iff $(m, f) \mid (r-2)^2$, and our claim follows.

Combining the above results gives

$$c_{f,1}^{r,m}(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ a \equiv 5 \bmod 8}} \left(\frac{a}{2^\alpha}\right). \tag{159}$$

for any r,f satisfying condition 2a of Fact 4.2. Since f is odd, $(f)_2 = 1$, and $f = 1 = r$ satisfy 2a,

$$c_{f,1}^{r,m}(2^\alpha) = c_{2^{ord_2(f)},1}^{r,m}(2^\alpha). \tag{160}$$

Now suppose r and f satisfy 2b or 2c of Fact 4.2. We again have (157). Given $a \equiv 1 \bmod 4$ and r, f satisfying 2b or 2c we have $(f^2, r^2 - af^2) = 4$ and $r^2 - af^2 \not\equiv 0 \bmod 8$. The condition $(2^{\alpha+2}f^2, r^2 - af^2) = 4$ is satisfied so it may deleted from our summation.

As we have already seen, $4(r-1) \equiv r^2 - af^2 \bmod 4(2^\alpha f^2, m)$ iff (m, f) and $(2^\alpha, m)$ both divide $(r-2)^2 + af^2$. Since r and f satisfy 2b and 2c, we have the following: It is always the case that $(2^\alpha, m) \mid (r-2)^2 + af^2$ since $(2^\alpha, m) = 1, 2, 4, 8$, and $8 \mid (r-2)^2 + af^2$. We also have the assumption that $(m, f) \mid (r-2)^2$ which implies $(m, f) \mid (r-2)^2 + af^2$. These results show that the condition $4(r-1) \equiv r^2 - af^2 \bmod 4(2^\alpha f^2, m)$ may be deleted since it is automatically satisfied.

The results in the two paragraphs above and item a in the previous case give

$$c_{f,1}^{r,m}(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ a \equiv 1 \bmod 8}} \left(\frac{a}{2^\alpha}\right). \tag{161}$$

By the same reasoning in the case where r and f satisfy 2a, we have our desired equality. □

Lemma 4.5 *Let $\alpha, \beta \geq 0$. By definition, $\sigma_i^r(f)_2 = (f)_2$, so $c_{\sigma_i^r(2^\beta)_2,i}^{r,m}(2^\alpha) = c_{2^\beta,i}^{r,m}(2^\alpha)$.*

1. *If $(r/2, 2^\beta) = 1$, then*

$$c_{2^\beta,0}^{r,m}(2^\alpha) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \text{if } \alpha > 0. \end{cases} \tag{162}$$

2. a. *If r is odd, then $c_{2^\beta,1}^{r,m}(q^\alpha)$ is nonzero only if $\beta = 0$, and*

$$c_{1,1}^{r,m}(2^\alpha) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \text{if } m \text{ is even and } \alpha > 0, \\ (-2)^\alpha/2 & \text{if } m \text{ is odd and } \alpha > 0. \end{cases} \tag{163}$$

   b. *If $r \equiv 2 \bmod 4$, then $c_{2^\beta,1}^{r,m}(q^\alpha)$ is nonzero only if $\beta \geq 2$, and*

$$c_{2^\beta,1}^{r,m}(2^\alpha) = \begin{cases} 0 & \text{if } \alpha \text{ is odd} \\ 2^\alpha & \text{if } \alpha \text{ is even.} \end{cases} \tag{164}$$

   c. *If $4 \mid r$, then $c_{2^\beta,1}^{r,m}(q^\alpha)$ is nonzero only if $\beta = 1$, and*

$$c_{2,1}^{r,m}(2^\alpha) = \begin{cases} 0 & \text{if } \alpha \text{ is odd} \\ 2^\alpha & \text{if } \alpha \text{ is even.} \end{cases} \tag{165}$$

Proof of 1. Follows from Fact 4.2.

Proof of 2a. In the proof of Lemma 4.4, we saw that for such values of r and f,

$$c_{1,1}^{r,m}(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ a \equiv 5 \bmod 8}} \left(\frac{a}{2^\alpha}\right). \tag{166}$$

The number of $a \in (Z/2^{\alpha+2}Z)^*$ such that $a \equiv 5 \bmod 8$ is $2^{\alpha+2}/8 = 2^\alpha/2$, and $a \equiv 5 \bmod 8$ implies $(a/2) = -1$. This means

$$c_{1,1}^{r,m}(2^\alpha) = \sum_{j=1}^{2^\alpha/2} (-1)^\alpha = (-2)^\alpha/2. \tag{167}$$

Proof of 2b and 2c. In the proof of Lemma 4.4, we saw that for such values of r and f,

$$c_{2^\beta,1}^{r,m}(2^\alpha) = \sum_{\substack{a\in(\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ a\equiv 1 \bmod 8}} \left(\frac{a}{2^\alpha}\right) \tag{168}$$

The number of $a \in (Z/2^{\alpha+2}Z)^*$ such that $a \equiv 1 \bmod 8$ is $2^{\alpha+2}/4 = 2^\alpha$. Also note that $a \equiv 1 \bmod 4$ alternates between $a \equiv 1 \bmod 8$ and $a \equiv 5 \bmod 8$ so the terms in our summation alternate between $(1)^\alpha$ and $(-1)^\alpha$. Our summation has an even number of terms so we have an equal number of $a \equiv 1 \bmod 8$ and $a \equiv 5 \bmod 8$. This means

$$c_{2^\beta,1}^{r,m}(2^\alpha) = \sum_{j=1}^{2^\alpha/2}(1)^\alpha + \sum_{j=1}^{2^\alpha/2}(-1)^\alpha = \begin{cases} 0 & \text{if } \alpha \text{ is odd,} \\ 2^\alpha & \text{if } \alpha \text{ is even.} \end{cases} \quad \square \tag{169}$$

Lemma 4.6 *Let $\alpha, \beta \geq 0$ and let q be an odd prime. If $i, r, m, f = q^\beta, n = q^\alpha$ satisfy the conditions set forth in 4.2, then $c_{\sigma_i^r(1)_q q^\beta,i}^{r,m}(q^\alpha)$ is nonzero, and we have*

$$c_{\sigma_i^r(1)_q q^\beta,i}^{r,m}(q^\alpha) = \begin{cases} 1 & \text{if } \alpha = 0, \\ -(r^2/q)q^{\alpha-1} & \text{if } \beta = 0,\ \alpha \text{ odd},\ q \nmid m, \\ \big(q-1-(r^2/q)\big)q^{\alpha-1} & \text{if } \beta = 0,\ \alpha \text{ even},\ q \nmid m, \\ q^{\alpha-1}\big((r-2)^2/q\big) & \text{if } \beta = 0 \text{ and } q \mid m, \\ 0 & \text{if } \beta > 0 \text{ and } \alpha \text{ odd}, \\ q^{\alpha-1}(q-1) & \text{if } \beta > 0 \text{ and } \alpha \text{ even}, \end{cases} \tag{170}$$

where (a/n) is the Kronecker symbol.

Lemma 4.7 *For any prime q and $\alpha \geq 0$ define*

$$\kappa(q^\alpha) = \begin{cases} q & \text{if } \alpha \text{ is odd}, \\ 1 & \text{if } \alpha \text{ is even}, \end{cases} \tag{171}$$

and extend to all positive integers by multiplicativity. For all fixed values of i, r, m, f, $|c_{f,i}^{r,m}(n)| \leq n/\kappa(n)$.

Proof. By Lemmas 4.5 and 4.6, for any prime q, we have

$$|c_{f,i}^{r,m}(q^\alpha)| \leq \left\{ \begin{array}{ll} q^{\alpha-1} & \text{if } \alpha \text{ is odd}, \\ q^\alpha & \text{if } \alpha \text{ is even.} \end{array} \right\} = q^\alpha/\kappa(q^\alpha). \tag{172}$$

Since $c_{f,i}^{r,m}$ and κ are multiplicative functions, we have

$$|c_{f,i}^{r,m}(n)| \leq n/\kappa(n). \tag{173}$$

5 The constant $C^{r,m}$

Finding the constants which appear in the statement of Theorem **??** will require all of our computational results thus far, especially those related to the function $c_{f,i}^{r,m}$.

5.1 Expressing $K_i^{r,m,d}$ as a product over primes

We first will find explicit formulae for the constants $K^{r,m,d}$ which appear in the conclusion of Theorem 3.8. In particular, we recall that

$$K^{r,m,d} = \sum_{\substack{f=1 \\ d|f}}^{\infty} \frac{1}{f} \sum_{n=1}^{\infty} \frac{c_f^{r,m}(n)}{n\varphi[m, nf^2]}, \tag{174}$$

where $d \mid m$. Clearly, $K^{r,m,d} = K_0^{r,m,d} + K_1^{r,m,d}$, where

$$K_i^{r,m,d} = \sum_{\substack{f=1 \\ d|f}}^{\infty} \frac{1}{f} \sum_{n=1}^{\infty} \frac{c_{f,i}^{r,m}(n)}{n\varphi[m, nf^2]}. \tag{175}$$

Replacing f by df, we have

$$K_i^{r,m,d} = \frac{1}{d} \sum_{f=1}^{\infty} \frac{1}{f} \sum_{n=1}^{\infty} \frac{c_{df,i}^{r,m}(n)}{n\varphi[m, nd^2f^2]}. \tag{176}$$

As the summand is multiplicative (see Lemma 4.3) we can rewrite this as

$$K_i^{r,m,d} = \frac{1}{d} \sum_{f=1}^{\infty} \frac{1}{f} \prod_q \sum_{\alpha=0}^{\infty} \frac{c_{df,i}^{r,m}(q^\alpha)}{q^\alpha \varphi([m, q^\alpha d^2 f^2]_q)}, \tag{177}$$

where the product is taken over all primes q. By Lemma 4.4 we have $c^{r,m}_{\sigma_i^r(df)_q,i}(q^\alpha) = c^{r,m}_{\sigma_i^r(df)_q,i}(q^\alpha)$, so we can express the product as

$$\prod_q \sum_{\alpha=0}^{\infty} \frac{c^{r,m}_{\sigma_i^r(df)_q,i}(q^\alpha)}{q^\alpha \varphi([m, q^\alpha d^2 f^2]_q)} = \prod_q \sum_{\alpha=0}^{\infty} \frac{c^{r,m}_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m, q^\alpha d^2]_q)} \prod_{q|f} \frac{\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(df)_q,i}(q^\alpha)}{q^\alpha \varphi([m,q^\alpha d^2 f^2]_q)}}{\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m,q^\alpha d^2]_q)}}. \tag{178}$$

Setting

$$M(f) = \prod_{q|f} \frac{\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(df)_q,i}(q^\alpha)}{q^\alpha \varphi([m,q^\alpha d^2 f^2]_q)}}{\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m,q^\alpha d^2]_q)}}, \tag{179}$$

we find

$$K_i^{r,m,d} = \frac{1}{d} \left(\prod_q \sum_{\alpha=0}^{\infty} \frac{c^{r,m}_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m, q^\alpha d^2]_q)} \right) \left(\sum_{f=1}^{\infty} \frac{M(f)}{f} \right) \tag{180}$$

Noting that $M(f)$ is a multiplicative function (as it is a product over primes dividing f), we can rewrite the summation by

$$\sum_f = \frac{M(f)}{f} = \prod_q \left(1 + \sum_{\beta=1}^{\infty} \frac{M(q^\beta)}{q^\beta} \right). \tag{181}$$

Calculating $M(q^\beta)$, we have

$$M(q^\beta) = \left(\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q q^\beta,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha+2\beta}d^2]_q)}\right)\left(\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha}d^2]_q)}\right)^{-1} \tag{182}$$

Combining equations, we obtain the following expression for $K_i^{r,m,d}$:

$$K_i^{r,m,d} = \frac{1}{d}\prod_q \left(\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha}d^2]_q)} + \sum_{\beta=1}^{\infty}\frac{1}{q^\beta}\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q q^\beta,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha+2\beta}d^2]_q)}\right), \tag{183}$$

$$= \frac{1}{d}\prod_q \sum_{\beta=0}^{\infty}\frac{1}{q^\beta}\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q q^\beta,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha+2\beta}d^2]_q)}, \tag{184}$$

for the sake of convenience, we will denote the summation over β in the above product by $K_i^{r,m,d}(q)$; we can then rewrite

$$K_i^{r,m,d} = \frac{1}{d}\prod_q K_i^{r,m,d}(q). \tag{185}$$

5.2 Computation of $K_i^{r,m,d}$

We now compute $K_i^{r,m,d}$ by computing the contributions $K_i^{r,m,d}(q)$ from each prime q. Special cases in the computation of $c^{r,m}_{\sigma(d)_q q^\beta,i}(q^\alpha)$ occur when $q \mid 2mr$ (since $d \mid m$, $q \mid d$ implies $q \mid m$). Accordingly, we write

$$K_i^{r,m,d} = \frac{1}{d}K_i^{r,m,d}(2)\prod_{\substack{q\mid m\\ q\neq 2}} K_i^{r,m,d}(q)\prod_{\substack{q\mid r\\ q\nmid 2m}} K_i^{r,m,d}(q)\prod_{q\nmid 2mr} K_i^{r,m,d}(q). \tag{186}$$

We shall begin by simplifying the product over $q \nmid 2mr$.

Note that because ($q \nmid m$ and therefore $q \nmid d$), $[m, q^\gamma d^2]_q = q^\gamma$; we also recall that $\varphi(q^\gamma) = q^{\gamma-1}(q-1)$. Since $q \neq 2$, we will now apply Lemma 4.6; in order to do this, we will first verify that the conditions of Fact 4.2 hold. When r is even and $q \nmid r$, only condition 1 holds; when r is odd, only condition 2a holds. We therefore have

$$\begin{aligned}\sum_{\alpha\geq 0} \frac{c^{r,m}_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha}d^2]_q)} &= 1 - \frac{1}{q-1}\sum_{\substack{\alpha>0\\ \alpha \text{ odd}}}\frac{1}{q^\alpha} + \frac{q-2}{q-1}\sum_{\substack{\alpha>0\\ \alpha \text{ even}}}\frac{1}{q^\alpha},\\ &= 1 - \frac{1}{q-1}\frac{q}{q^2-1} + \frac{q-2}{q-1}\frac{1}{q^2-1},\\ &= \frac{q(q^2-q-1)-1}{(q-1)^2(q+1)},\end{aligned} \tag{187}$$

and

$$\begin{aligned}\sum_{\beta=1}^{\infty}\frac{1}{q^{\beta}}\sum_{\alpha\geq 0}\frac{c^{r,m}_{\sigma_i^r(d)_q q^{\beta},i}(q^{\alpha})}{q^{\alpha}\varphi([m,q^{\alpha+2\beta}d^2]_q)} &= \sum_{\beta=1}^{\infty}\frac{1}{q^{3\beta}}\left(\frac{q}{q-1}+\sum_{\substack{\alpha>0\\ \alpha \text{ even}}}\frac{1}{q^{\alpha}}\right),\\ &= \frac{1}{q^3-1}\left(\frac{q}{q-1}+\frac{1}{q^2-1}\right),\\ &= \frac{1}{(q-1)^2(q+1)}.\end{aligned} \tag{188}$$

Combining these results,

$$K_i^{r,m,d}(q) = \frac{q(q^2-q-1)}{(q-1)^2(q+1)} \quad \text{when } q\nmid 2mr, \text{ and so,} \tag{189}$$

$$\prod_{q\nmid 2mr} K_i^{r,m,d}(q) = \prod_{q\nmid 2mr}\frac{q(q^2-q-1)}{(q-1)^2(q+1)}. \tag{190}$$

We will now deal with the product over primes q for which $q \mid r$ but $q\nmid 2m$.

From Fact 4.2 and Lemma 4.6, we find that $c^{r,m}_{\sigma_i^r(1)_q q^{\beta},i}(q^{\alpha}) = 0$ when $\beta > 0$ and (since $q \mid r$ implies $(r^2/q) = 0$),

$$c^{r,m}_{\sigma_i^r(1)_q,i}(q^{\alpha}) = \begin{cases} 1 & \text{if } \alpha = 0\\ 0 & \text{if } \alpha > 0 \text{ and } \alpha \text{ is odd,}\\ q^{\alpha-1}(q-1) & \text{if } \alpha > 0 \text{ and } \alpha \text{ is even.}\end{cases} \tag{191}$$

Substitution yields

$$K_i^{r,m,d}(q) = \sum_{\alpha\geq 0}\frac{c^{r,m}_{\sigma_i^r,i}(q^{\alpha})}{q^{\alpha}\varphi(q^{\alpha})} = 1+\sum_{\substack{\alpha>0\\ \alpha \text{ even}}}\frac{1}{q^{\alpha}} = \frac{q^2}{q^2-1} \quad \text{when } q\mid r \text{ and } q\nmid 2m. \tag{192}$$

Therefore,

$$\prod_{\substack{q\mid r\\ q\nmid 2m}} K_i^{r,m,d}(q) = \prod_{\substack{q\mid r\\ q\nmid 2m}}\frac{q^2}{q^2-1}. \tag{193}$$

Combining the last two results and equation (186), we find

$$K_i^{r,m,d} = \frac{1}{d}K_i^{r,m,d}(2)\prod_{\substack{q\mid m\\ q\neq 2}} K_i^{r,m,d}(q)\prod_{\substack{q\mid r\\ q\nmid 2m}}\frac{q^2}{q^2-1}\prod_{q\nmid 2mr}\frac{q(q^2-q-1)}{(q-1)^2(q+1)}. \tag{194}$$

The remaining computations must be specialized for the different values of m, d, where $d \mid m$. Noting that $K_i^{r,m,d}(q) = K_i^{r,(m)_q,(d)_q}(q)$ greatly decreases the number of calculations one has to perform. However, there are still a good many cases to deal with, and thus, we will omit the details of our computations. The distinct values of $K_i^{r,m,d}(q)$ (which were computed first by hand and then checked against machine computations) are given in the below tables:

	$i=0$ $r\equiv 2 \bmod 4$	$i=0$ $4\mid r$	$i=1$ r is odd	$i=1$ $r\equiv 2 \bmod 4$	$i=1$ $4\mid r$
$K_i^{r,1,1}(2)$	9/7	1	2/3	1/21	1/3
$K_i^{r,2,1}(2)$	9/7	1	1	1/21	1/3
$K_i^{r,2,2}(2)$	4/7	0	0	2/21	2/3
$K_i^{r,4,1}(2)$	11/14	1/2	1/2	1/21	1/3
$K_i^{r,4,2}(2)$	4/7	0	0	2/21	2/3
$K_i^{r,4,4}(2)$	1/7	0	0	4/21	0

(Tables for values of $K_i^{r,m,d}(3)$, $K_i^{r,m,d}(5)$, and $K_i^{r,m,d}(7)$.)

References

[1] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, International Mathematical Research Notices (1999) 165–183.

[2] E. Fouvry, M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. (1996) **48**, 31–104.

[3] S. Frechette, K. Ono, M. Papanikolas, *Gaussian hypergeometric functions and traces of Hecke operators*, International Mathematical Research Notices (2004) **60**, 3233–3262.

[4] H. Halberstam and H. E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[5] K. James, *Average Frobenius distributions for elliptic curves with* 3*-torsion*, J. Number Theory **109** No. 2, 278–298.

[6] K. James, *Averaging special values of Dirichlet L-series*, to appear in the Ramanujan Journal.

[7] A. W. Knapp, *Elliptic curves*, Mathematical Notes, **40**. Princeton University Press, Princeton, NJ, 1992.

[8] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Math **504**, Springer-Verlag, Berlin, 1976.

[9] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld), Invent. Math. (1978) **44**, no. 2, 129–162.

[10] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combinatorial Theory, (1987) **A46** No. 2, 183–208.

[11] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[12] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.