The Lang-Trotter Conjecture on Average for Elliptic Curves with Torsion

George J. Schaeffer, Cole T. South, Cinna J. Wu
Advisors: Bjorn Poonen, Neil J. Calkin, Kevin James, Timothy Flowers

August, 2006

Abstract

We 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 $\mathcal{E}_m(\mathbf{t})$ is the set of all such elliptic curves with parameters bounded by $\mathbf{t}$, we will show that

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

for some constant $C^{r,m}$ which we will give explicitly. The case where $m = 1$ is proven in [3], and special cases of $m \in \{3, 5, 6, 7, 9, 10\}$ are proven in [9] and [2]. This paper serves as a complete generealization of these results.

1 Introduction

One of the crowning achievements of modern number theory is Dirichlet's theorem on primes in arithmetic progressions. This result states that there are infinitely many primes in any arithmetic progression $\{ak + b\}$ so long as a and b are relatively prime, and is often stated in the stronger form

$$\pi(x; a, b) = \#\{p \le x : p \equiv b \bmod a\} \sim \frac{1}{\varphi(a)}\pi(x) \text{ as } x \to \infty,$$

where φ is the totient function and π is the usual prime counting function.

In investigating an analogous theorem for quadratic progressions, Hardy and Littlewood proposed the following [8]:

Conjecture 1.1 *Let $Q = ak^2 + bk + c$ be a quadratic progression and let $\pi(x; Q)$ be the number of primes not exceeding x which lie in the image of Q. Then $\pi(x; Q) \sim C\pi_{1/2}(x)$ as $x \to \infty$, where*

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

and C is a constant.

Such a conjecture suggests a deeper theorem concerning the size of Mordell-Weil groups of elliptic curves over the prime fields $\mathbb{F}_p$. If E is an elliptic curve defined over the rationals, let $a_p(E)$ be the trace of the Frobenius endomorphism of $E/\mathbb{F}_p$. Then $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$ and Hasse's bound $|a_p(E)| \leq 2\sqrt{p}$ applies. Now consider for example the elliptic curve $E : y^2 = x^3 - x$ with complex multiplication by $\mathbb{Z}[i]$. It is not too difficult to see that $a_p(E) = \pm 2$ iff $p = k^2 + 1$ for some integer k.

This motivates the question: Given an elliptic curve E over the rationals and $r \in \mathbb{Z}$, how often do we have $a_p(E) = r$? Define

$$\pi_E^r(x) = \{p \leq x : a_p(E) = r\}.$$

Deuring showed that about half of the primes are of supersingular reduction [4]. That is, if E has complex multiplication and $r = 0$, then $\pi_E^r(x) \sim \frac{1}{2}\pi(x)$ as $x \to \infty$. For all other cases, we have the following conjecture of Lang and Trotter:

Conjecture 1.2 *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $r \in \mathbb{Z}$. Except for the case wherein $r = 0$ and E has complex multiplication, there is a constant C_E^r such that*

$$\pi_E^r(x) \sim C_E^r \pi_{1/2}(x) \text{ as } x \to \infty.$$

Using probabilistic methods, Lang and Trotter were able to predict explicitly the constant C_E^r. More precisely, let $\rho_{E,m}$ be the Galois representation

$$\rho_{E,m} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, E(\bar{\mathbb{Q}})[m],$$

where $E(\bar{\mathbb{Q}})[m]$ is the subgroup of m-torsion points of $E(\bar{\mathbb{Q}})$. As this subgroup is isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, we may choose an appropriate basis and identify $\mathrm{Aut}\, E(\bar{\mathbb{Q}})[m]$ with $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let $G(m)$ denote the image of $\rho_{E,m}$ in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, and let $G(m)_r$ denote the set of elements in $G(m)$ having trace r (modulo m).

Provided that E does not have complex multiplication, the image of the Galois representation on the full torsion subgroup $\mathrm{tor}\, E(\bar{\mathbb{Q}})$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, where $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. It then follows that there is an integer m_E such that $\rho_{E,q}$ is surjective for all primes q which do not divide m_E; moreover, the image of this Galois representation in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is the full inverse image of $G(m_E)$ under the modular reduction $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$. Lang and Trotter thus define their constant C_E^r by

$$\begin{aligned} C_E^r &= \frac{2}{\pi}\frac{m_E|G(m_E)_r|}{|G(m_E)|}\prod_{q\nmid m_E}\frac{q|G(q)_r|}{|G(q)|}, \\ &= \frac{2}{\pi}\frac{m_E|G(m_E)_r|}{|G(m_E)|}\prod_{\substack{q\mid r\\ q\nmid m_E}}\frac{q^2}{q^2-1}\prod_{q\nmid r m_E}\frac{q(q^2-q-1)}{(q-1)^2(q+1)}. \end{aligned} \tag{1}$$

The latter equality follows from the easy estimates

$$\begin{aligned} |\,\mathrm{GL}_2(\mathbb{F}_q)| &= q(q-1)^2(q+1), \text{ and} \\ |\,\mathrm{GL}_2(\mathbb{F}_q)_r| &= \begin{cases} q^2(q-1) & \text{if } q \mid r, \\ q(q^2-q-1) & \text{otherwise.} \end{cases} \end{aligned}$$

David and Pappalardi have shown that the Lang-Trotter conjecture is true on average [3]:

Theorem 1.3 *Let $E(a,b): y^2 = x^3 + ax + b$ and $\epsilon > 0$. If $A, B > x^{1+\epsilon}$, then as $x \to \infty$,*

$$\frac{1}{4AB} \sum_{|a|\le A,\ |b|\le B} \pi^r_{E(a,b)}(x) \sim C^r \pi_{1/2}(x),$$

where

$$C^r = \frac{2}{\pi} \prod_{q \mid r} \frac{q^2}{q^2-1} \prod_{q \nmid r} \frac{q(q^2-q-1)}{(q+1)(q-1)^2}. \tag{2}$$

The constant C^r in (2) is exactly C^r_E from (1) with the substitution $m_E = 1$. Note however that we never actually have $m_E = 1$ (see [17]), and moreover, it is not known if C^r is the average of the C^r_E over all E.

In this paper, we wish to consider curves having nontrivial rational torsion subgroups. Due to Mazur's theorem, if E has nontrivial rational m-torsion, then m is in

$$\mathcal{M} = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}.$$

Kubert has systematically paramtetrized all elliptic curves having rational m-torsion ($m \in \mathcal{M}$) [12]. The details of the parametrizations are not crucially important to us; it suffices to know the number of parameters for a given m. In particular, when $m \in \{2, 3\}$, then the parametrization $\mathcal{P}_m$ has two parameters; for $m \ge 4$, $\mathcal{P}_m$ has only one parameter.

Since the set of elliptic curves with nontrivial rational torsion subgroups has density zero among all elliptic curves, the result of Theorem 1.3 ignores all such curves. However, we can see from (1) that the presence of such torsion points has a significant effect on the constant C^r_E. In particular, if E has a rational point of order m, then $m \mid m_E$ and $G(m)$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$; specifically,

$$G(m) = \rho_{E,m}\big(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\big) \le \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/m\mathbb{Z},\ d \in (\mathbb{Z}/m\mathbb{Z})^* \right\},$$

and $G(m)_r$ is all those above matrices with $1 + d \equiv r \bmod m$. This gives the motivation for the main theorem of this paper:

Theorem 1.4 *Fix $m \in \mathcal{M}$ and $r \in \mathbb{Z}$. Let $\mathcal{E}_m(\mathbf{t})$ be the parametrized family of elliptic curves having nontrivial rational m-torsion whose parameters are bounded by the vector $\mathbf{t}$ and let $\epsilon > 0$. If $T > x^{1+\epsilon}$ for every component T of $\mathbf{t}$, then as $x \to \infty$*

$$\frac{1}{\#\mathcal{E}_m(\mathbf{t})} \sum_{E \in \mathcal{E}_m(\mathbf{t})}{}' \pi^r_E(x) \sim C^{r,m} \pi_{1/2}(x), \tag{3}$$

where $\sum'$ denotes the sum over nonsingular curves, and $C^{r,m}$ is a constant dependent on r and m.

From this we can actually prove the following stronger result. The proof is identical to the proof of Theorem 1.4 in [3] so we omit the proof and focus on proving Theorem 1.4.

Theorem 1.5 *With the same notation and assumptions as in Theorem 1.4, for every $c > 0$,*

$$\frac{1}{\#\mathcal{E}_m(\mathbf{t})} \sum_{E \in \mathcal{E}_m(\mathbf{t})}{}' |\pi^r_E(x) - C^{r,m}\pi_{1/2}(x)|^2 = \mathrm{O}\left(\frac{x}{\log^c x} + \frac{x^3}{N} + \frac{x^5}{N^2} \right)$$

as $x \to \infty$ where N is the minumum of the components of $\mathbf{t}$.

This gives the easy corollary due to a standard application of the Turán normal order method.

Corollary 1.6 *Let $m \in \mathcal{M}$, $\epsilon > 0$, and fix $c > 0$. If $T > x^{2+\epsilon}$ for each component T of the vector $\mathbf{t}$ then for all $d > 2c$ and for all $E \in \mathcal{E}_m(\mathbf{t})$ we have the inequality*

$$|\pi_E^r(x) - C^{r,m}\pi_{1/2}(x)| \ll \frac{\sqrt{x}}{\log^c x},$$

with at most $\mathrm{O}(\max T^2/\log^d x)$ exceptions.

The results of Theorem 1.5 and Corollary 1.6 show that the asymptotic relation in (3) is not only true on average, it is true for "almost all" elliptic curves with rational m-torsion.

1.1 Outline of the proof of the main result

The proof of Theorem 1.4 is quite long, and requires appeals to many classical results of algebra and analytic number theory. The first step is to count elliptic curves having specified m-torsion subgroups. Due to the work of Deuring and Schoof, these counts may be expressed in terms of the class number functions H, h subject to the satisfaction of certain congruence conditions. In short, we may write the average in (3) as a sum of terms involving

$$H\left(\frac{r^2-4p}{d^2}\right) \text{ and } h(-p)$$

where d is some divisor of m. Following the procedures presented in Section 5 of [5], we show that there exists a constant $K^m > 0$ depending on m such that for all $c > 0$,

$$\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} \frac{h(-p)}{p} = K^m\pi_{1/2}(x) + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

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

Then proceeding as in [3] and [9], we write the sums involving $H(\Delta)$ in terms of Dirichlet L-series. After extensive asymptotic analysis, we show that

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

where $c > 0$, $\mathcal{S}_f(x)$ is an appropriate set of primes bounded by x, $\Delta = (r^2-4p)/f^2$, and $K^{m,d}$ is a constant determined by

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

Following standard procedure, we express $K^{m,d}$ in terms of a multiplicative number theoretic function, and then as a product over primes. Computing weighted sums of the $K^{m,d}$ and combining them with the K^m finally allows us to determine the constants $C^{r,m}$, and combining with earlier analytic calculations gives (3).

2 The average and class numbers

In this section, we will show that for a fixed value of m, the average in (3) can be written in terms of class numbers of binary quadratic forms. 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 be a nonsingular elliptic curve over F, and $m \in \mathcal{M}$. Let $E(F)$ be the set of points on E over F. Define*

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

$E(F)[m]$ 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,

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

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

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

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 $E(\mathbb{F}_p)[m] \leq E(\bar{\mathbb{F}}_p)[m]$.

Corollary 2.2 *For any $m \in \mathcal{M}$,*

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

where d is any divisor of m. In particular, if m is prime, then either

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

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 *Let $d \mid m$. The number of points $u \times v$ in $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ with order m is given by*

$$\Phi(d \times m) = \sum_{a \mid d} \varphi(a) \sum_{\substack{b \mid a \\ (b, m/a)=1}} \varphi\left(\frac{m}{b}\right) \tag{4}$$

Proof. Of course, $\operatorname{ord}(u \times v) = [\operatorname{ord} u, \operatorname{ord} v]$. To construct the above sum, consider all those points $u \times v$ such that $\operatorname{ord} u = a \mid d$, of which there are $\varphi(a)$. Now, let $b \mid a$ and write $b = a/(a, a/b)$. Multiplying both sides by $(a, a/b)$, we see that the condition $(b, m/a) = 1$ holds iff $\big(a, (a, a/b)m/a\big) = (a, a/b)$ which is equivalent to the statement

$$\left[a, \frac{m}{b}\right] = \left[a, \frac{(a, a/b)m}{a}\right] = \frac{(a, a/b)m}{\big(a, (a, a/b)m/a\big)} = m.$$

The number of $v \in \mathbb{Z}/m\mathbb{Z}$ with $\operatorname{ord} v = m/b$ is $\varphi(m/b)$, whence the formula in (4). $\square$

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

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

and also

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

Fact 2.4 *Let $p > 3$ be a prime. Then any curve E over $\mathbb{F}_p$ can be parametrized as*

$$E_{\mathcal{W}(a,b)} : y^2 = x^2 + ax + b$$

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

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

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

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

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,

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

The result follows from considering the different cases. □

Fact 2.5 *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*

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

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 [11] 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 2.6 *We have*

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \begin{cases} \#\mathcal{P}_m(E/\mathbb{F}_p)\#\mathcal{W}(\tilde{E}_{\mathcal{W}(a,b)}/\mathbb{F}_p) & \text{if } m = 2, 3, \\ \#\mathcal{P}_m(E/\mathbb{F}_p) & \text{otherwise.} \end{cases} \tag{5}$$

Proof. In [11], 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 obtain 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 2.7 *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

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

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

Fact 2.8 *The Kronecker and Dirichlet class numbers are related by the identity*

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

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

We define the following functions

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

It is important to note that the above do not count elliptic curves, but rather isomorphism classes $\tilde{E}$ of elliptic curves over a fixed field $\mathbb{F}_p$.

We will write $N''_{p,r}(m) = N_{p,r}(m \times m)$. It turns out that all values of $N_{p,r}$ which are relevant to this paper can be computed in terms of $N'_{p,r}$ and $N''_{p,r}$, which in turn can be written in terms of the class number functions H and h. This latter result is due to work by Deuring [4] and Schoof [15], whose conclusions we now summarize.

Theorem 2.9 *Fix $m \in \mathcal{M}$ and $r \in \mathbb{Z}$. Let p be a prime such that $p \nmid r$ if $r \neq 0$, and such that $p > B(r) = \max\{3, r, r^2/4\}$. We have*

$$N'_{p,r}(m) = \begin{cases} H(r^2 - 4p) & \text{if } p + 1 \equiv r \bmod m, \\ 0 & \text{otherwise,} \end{cases} \tag{6}$$

and

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

Proof. See [4] and [15]. □

If $d \mid m$ for $m \in \mathcal{M}$, then clearly

$$\left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ m \mid \#E(\mathbb{F}_p)\right\} \subseteq \left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ d \mid \#E(\mathbb{F}_p)\right\}.$$

But so long as the former set is nonempty, equality must hold, since the two sets are of equal finite cardinality by equation (6). That is, if $p + 1 \equiv r \bmod m$, then $d \mid \#E(\mathbb{F}_p)$ implies $m \mid \#E(\mathbb{F}_p)$. This fact is crucial to the inclusion-exclusion arguments we now make in order to simplify the computation of $N_{p,r}$. Since $m \in \mathcal{M}$, we need only argue the cases wherein $m = l, l^2, l^3$ for some prime l or $m = 2l, 4l$ for an odd prime l.

Lemma 2.10 *Let l be prime and $\alpha, \beta \in \mathbb{Z}$ with $0 \leq \alpha \leq \beta$ and $\beta > 0$. We have*

$$N_{p,r}(l^\alpha \times l^\beta) = \begin{cases} N'_{p,r}(l^\beta) - N''_{p,r}(l) & \text{if } \alpha = 0 \text{ and } p + 1 \equiv r \bmod l^\beta, \\ N''_{p,r}(l^\alpha) & \text{if } 0 < \alpha = \beta, \\ N''_{p,r}(l^\alpha) - N''_{p,r}(l^{\alpha+1}) & \text{if } 0 < \alpha < \beta \text{ and } p + 1 \equiv r \bmod l^{\alpha+\beta}, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

Proof. We will assume that E is an elliptic curve with p a prime of good decomposition and that E, p satisfy $a_p(E) = r$.

Suppose $E(\mathbb{F}_p)[l^\beta] \cong \mathbb{Z}/l^\beta\mathbb{Z}$. This clearly implies that $l^\beta \mid \#E(\mathbb{F}_p)$, and since $E(\mathbb{F}_p)[l] \leq E(\mathbb{F}_p)[l^\beta]$, we must have $E(\mathbb{F}_p)[l] \ncong \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z}$. Conversely, if $l^\beta \mid \#E(\mathbb{F}_p)$, then

$$E(\mathbb{F}_p)[l^\beta] \cong \frac{\mathbb{Z}}{l^{\alpha_1}\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^{\alpha_2}\mathbb{Z}}$$

where $\alpha_1 \leq \alpha_2 \leq \beta$ and $\alpha_1 + \alpha_2 \geq \beta$. If in addition, E does not have full l-torsion over $\mathbb{F}_p$, then we must have $\alpha_1 = 0$ so that $E(\mathbb{F}_p)[l^\beta] \cong \mathbb{Z}/l^\beta\mathbb{Z}$. Therefore, $E(\mathbb{F}_p)[l^\beta] = \mathbb{Z}/l^\beta\mathbb{Z}$ iff $l^\beta \mid \#E(\mathbb{F}_p)$ and E does not have full l-torsion over $\mathbb{F}_p$.

By earlier arguments, the congruence $p + 1 \equiv r \bmod l^\beta$ guarantees that $l^2 \mid \#E(\mathbb{F}_p)$ implies $l^\beta \mid \#E(\mathbb{F}_p)$. Therefore, so long as $p + 1 \equiv r \bmod l^\beta$

$$\left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ E(\mathbb{F}_p)[l] \cong \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l\mathbb{Z}}\right\}$$
$$\subseteq \left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ l^2 \mid \#E(\mathbb{F}_p)\right\} \subseteq \left\{\tilde{E}/\mathbb{F}_p : a_p(E) = r,\ l^\beta \mid \#E(\mathbb{F}_p)\right\}.$$

Combining these arguments we have proved the first case of equation (7). The second case is simply the definition of $N''_{p,r}$.

We now prove the third case. Suppose first that $E(\mathbb{F}_p)[l^\beta] = \mathbb{Z}/l^\alpha\mathbb{Z} \oplus \mathbb{Z}/l^\beta\mathbb{Z}$ with $\alpha < \beta$. By reduction modulo l^α and $l^{\alpha+1}$, E must have full l^α-torsion but cannot have full $l^{\alpha+1}$-torsion. Conversely, if $p+1 \equiv r \bmod l^{\alpha+\beta}$, then $l^{\alpha+\beta} \mid \#E(\mathbb{F}_p)$ and the conditions

$$E(\mathbb{F}_p)[l^\alpha] \cong \frac{\mathbb{Z}}{l^\alpha\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^\alpha\mathbb{Z}} \quad \text{and} \quad E(\mathbb{F}_p)[l^{\alpha+1}] \ncong \frac{\mathbb{Z}}{l^{\alpha+1}\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^{\alpha+1}\mathbb{Z}}$$

are sufficient to give $E(\mathbb{F}_p)[l^\beta] \cong \mathbb{Z}/l^\alpha\mathbb{Z} \oplus \mathbb{Z}/l^\beta\mathbb{Z}$. If E has full $l^{\alpha+1}$-torsion over $\mathbb{F}_p$, it clearly has full l^α-torsion as well, whence the third case of (7).

The fourth case is used when the relevant congruence conditions do not hold true. But upon inspection of Theorem 2.9, it is clear why the relevant values of $N_{p,r}$ are zero when these congruences fail to obtain. □

Lemma 2.11 *Let l be an odd prime and choose p, r such that $p+1 \equiv r \bmod 2l$. Then*

$$\begin{aligned} N_{p,r}(1 \times 2l) &= N'_{p,r}(2l) - N''_{p,r}(2) - N''_{p,r}(l) + N''_{p,r}(2l), \\ N_{p,r}(2 \times 2l) &= N''_{p,r}(2) - N''_{p,r}(2l), \\ N_{p,r}(l \times 2l) &= N''_{p,r}(l) - N''_{p,r}(2l), \\ N_{p,r}(2l \times 2l) &= N''_{p,r}(2l). \end{aligned} \tag{8}$$

Proof. Suppose E is an elliptic curve with $a_p(E) = r$. Then the congruence guarantees that $2l \mid \#E(\mathbb{F}_p)$. The identities then follow from simple inclusion-exclusion arguments. □

Lemma 2.12 *Let l be an odd prime. Then*

$$\begin{aligned} N_{p,r}(1 \times 4l) &= N'_{p,r}(4l) - N''_{p,r}(2) - N''_{p,r}(l) + N''_{p,r}(2l), \\ N_{p,r}(l \times 4l) &= N''_{p,r}(l) - N''_{p,r}(2l), \end{aligned} \quad \text{if } p+1 \equiv r \bmod 4l, \tag{9}$$

$$\begin{aligned} N_{p,r}(2 \times 4l) &= N''_{p,r}(2) - N''_{p,r}(4) - N''_{p,r}(2l) + N''_{p,r}(4l), \\ N_{p,r}(2l \times 4l) &= N''_{p,r}(2l) - N''_{p,r}(4l), \end{aligned} \quad \text{if } p+1 \equiv r \bmod 8l, \tag{10}$$

$$N_{p,r}(4 \times 4l) = N''_{p,r}(4) - N''_{p,r}(4l), \quad \text{if } p+1 \equiv r \bmod 16l, \tag{11}$$

$N_{p,r}(4l \times 4l) = N''_{p,r}(4l)$, and $N_{p,r}(\cdot \times 4l) = 0$ if the none of the above cases hold.

Proof. The reasoning for this lemma is a bit trickier than for the previous lemma. The first identity of (9) is easy. The second of these is pretty simple as well: $E(\mathbb{F}_p)[4l] = \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/4l\mathbb{Z}$ iff $4l \mid \#E(\mathbb{F}_p)$, E has full l-torsion over $\mathbb{F}_p$, and E does not have full $2l$-torsion.

The rest of the identities are similar, though the purpose of the congruences may not be clear. The congruences included are simply those which are not implicit in the result of Theorem 2.9; they are required to guarantee that if $a_p(E) = r$ then $\#E(\mathbb{F}_p)$ is divisible by the modulus in question. For example, given that $a_p(E) = r$, $p+1 \equiv r \bmod 8l$ implies that $8l \mid \#E(\mathbb{F}_p)$. It follows that either $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4l\mathbb{Z}$ or $\mathbb{Z}/8l\mathbb{Z}$ is a subgroup of $E(\mathbb{F}_p)[4l]$. $N''_{p,r}(2)$ counts all those in the latter case, and subtracting $N''_{p,r}(4) + N''_{p,r}(2l) - N_{p,r}(4l)$ guarantees that we do not count elliptic curves with larger $4l$-torsion subgroups. □

2.4 Simplifying the average

Definition 2.13 *To simplify the following lemmas, let*

$$A_2(p,S,T) = \left(\frac{1}{p^2} + \mathrm{O}\left(\frac{1}{Sp} + \frac{1}{Tp} + \frac{1}{ST}\right)\right), \text{ and}$$
$$A_1(p,S) = \left(\frac{1}{p} + \mathrm{O}\left(\frac{1}{S}\right)\right).$$

Lemma 2.14 *Fix $m \in \mathcal{M}$ and $r \in \mathbb{Z}$. Define $B(r) = \max\{3, r, r^2/4\}$.*
We have

$$\frac{1}{4ST}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m}(s,t)}(x) = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_2(p,S,T) \sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m}(s,t))=r}}{}' 1 + \mathrm{O}(\log\log x), \text{ or} \quad (12)$$

$$\frac{1}{2S}\sum_{|s|\le S}{}' \pi^r_{E_{\mathcal{P}_m}(s)}(x) = \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_1(p,S) \sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m}(s))=r}}{}' 1 + \mathrm{O}(\log\log x), \quad (13)$$

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

Proof. We will prove the above when $\mathcal{P}_m$ has two parameters; the proof in the one parameter case is similar. First, we replace $\pi^r_{E_{\mathcal{P}_m}(s,t)}(x)$ by a summation:

$$\frac{1}{4ST}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m}(s,t)}(x) = \frac{1}{4ST}\sum_{|s|\le S,|t|\le T}{}' \sum_{\substack{p\le x\\ a_p(E_{\mathcal{P}_m}(s,t))=r}} 1.$$

Recall that $m \mid \#E(\mathbb{F}_p)$ implying that $r \equiv p+1 \bmod m$. Moreover, by Hasse's bound, we may restrict p to those primes satisfying $B(r) < p \le x$:

$$\frac{1}{4ST}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m}(s,t)}(x) = \frac{1}{4ST}\sum_{|s|\le S,|t|\le T}{}' \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m\\ a_p(E_{\mathcal{P}_m}(s,t))=r}} 1.$$

Switching the order of summation yields

$$\frac{1}{4ST}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m}(s,t)}(x) = \frac{1}{4ST}\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} \sum_{\substack{|s|\le S,|t|\le T\\ a_p(E_{\mathcal{P}_m}(s,t))=r}}{}' 1 + \mathrm{O}(\log\log x), \quad (14)$$

where the error term represents those curves which are singular over $\mathbb{F}_p$.

The assumption $a_p(E) = r$ depends only on the congruence classes of the parameters of s, t modulo p. Thus we may estimate

$$\sum_{\substack{|s|\le S,|t|\le T\\ a_p(E_{\mathcal{P}_m}(s,t))=r}}{}' 1 = \left(\frac{4ST}{p^2} + \mathrm{O}\left(\frac{S+T+p}{p}\right)\right) \sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m}(s,t))=r}}{}' 1. \quad (15)$$

Substituting (15) into (14) and simplifying gives (12). $\square$

By Corollary 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 (12) and (13) as:

$$\sum_{\substack{0\le s,t<p \\ a_p(E_{\mathcal{P}_m(s,t)})=r}}{}' 1 = \sum_{d|m} \sum_{\substack{0\le s,t<p \\ a_p(E_{\mathcal{P}_m(s,t)})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/d\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 \tag{16}$$

and

$$\sum_{\substack{0\le s<p \\ a_p(E_{\mathcal{P}_m(s)})=r}}{}' 1 = \sum_{d|m} \sum_{\substack{0\le s<p \\ a_p(E_{\mathcal{P}_m(s)})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/d\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1. \tag{17}$$

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

$$\begin{aligned} \sum_{\substack{0\le s<p \\ a_p(E_{\mathcal{P}_m(s)})=r \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/d\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 &= \#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p)\# \left\{ \tilde{E}/\mathbb{F}_p : a_p(E) = r,\ E(\mathbb{F}_p)[m] \cong \frac{\mathbb{Z}}{d\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}} \right\} \\ &= \#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) N_{p,r}(d \times m). \end{aligned} \tag{18}$$

Due to the sheer multitude of cases involved (due especially to the choice of m, r and the congruences in Lemmas 2.10, 2.11, and 2.10), we will not simplify the above in terms of $N'_{p,r}, N''_{p,r}$ or the class number functions H, h directly for all cases of m. We give the calculations for $m = 2, 3, 5, 7, 6, 10$ to give the reader an idea of how the simplication is carried out. Though the calcluations for the remaining cases will be surpressed, the reader should keep them in mind, as they are necessary in the computation of the constants $C^{r,m}$.

Definition 2.15 *To simplify the notation in the following lemmas, define*

$$\begin{aligned} N(k) &= \sum_{\substack{B(r)<p\le x \\ p\equiv r-1 \bmod km}} A_2(p,S,T) H\left(\frac{r^2-4p}{k^2}\right) \\ N'(k) &= \sum_{\substack{B(r)<p\le x \\ p\equiv r-1 \bmod km}} A_2(p,S,T) h(-p) \\ M(k) &= \sum_{\substack{B(r)<p\le x \\ p\equiv r-1 \bmod km}} A_1(p,S) H\left(\frac{r^2-4p}{k^2}\right) \\ M'(k) &= \sum_{\substack{B(r)<p\le x \\ p\equiv r-1 \bmod km}} A_1(p,S) h(-p). \end{aligned}$$

Lemma 2.16 *Fix $m \in \{2,3\}$. Then,*

$$\frac{1}{4ST}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \frac{p}{2}N(1) + N + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_2(p,S,T)\mathrm{O}(p) + \mathrm{O}(\log\log x)$$

where

$$N = \begin{cases} \frac{mp}{2}N(m) & \text{if } r \equiv 2 \bmod m \text{ and } r \neq 0 \\ \frac{mp}{2}N'(m) & \text{if } r = 0 \text{ and } m = 2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Combining Facts 2.3 and 2.5 we obtain

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

If we substitute the above into Equation (5) (see Fact 2.6),

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

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

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \left\{ \begin{array}{ll} 1/2 & \text{if } E \text{ has cyclic 2- or 3-torsion,} \\ 3/2 & \text{if } E \text{ has full 2-torsion,} \\ 2 & \text{if } E \text{ has full 3-torsion,} \end{array} \right\}(p-1). \tag{19}$$

By Lemma 2.10, we see that

$$\begin{aligned} N_{p,r}(1\times m) &= N'_{p,r}(m) - N''_{p,r}(m), \text{ and} \\ N_{p,r}(m\times m) &= N''_{p,r}(m). \end{aligned} \tag{20}$$

Substituting the above into(18) gives us

$$\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m(s,t)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{1}{2}pN'_{p,r}(m) - \frac{1}{2}pN''_{p,r}(m) + \mathrm{O}(p), \tag{21}$$

$$\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m(s,t)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \left\{ \begin{array}{ll} 3/2 & \text{if } m=2, \\ 2 & \text{if } m=3, \end{array} \right\} pN''_{p,r}(m) + \mathrm{O}(p), \tag{22}$$

with the error term representing the contribution from the exceptional curves in (19).

Combining (21) and (22) with (16) yields

$$\sum_{\substack{0\le s,t<p\\ a_p(E_{\mathcal{P}_m(s,t)})=r}}{}' 1 = \frac{1}{2}pN'_{p,r}(m) + \frac{m}{2}pN''_{p,r}(m) + \mathrm{O}(p), \tag{23}$$

and plugging (23) into the right side of (12) gives

$$\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_2(p,S,T)\frac{1}{2}pN'_{p,r}(m) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_2(p,S,T)\frac{m}{2}pN''_{p,r}(m) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_2(p,S,T)\mathrm{O}(p) + \mathrm{O}(\log\log x).$$

Finally, we apply the results from Theorem 2.9 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 2.17 *Fix $m \in \{5,7\}$. Then,*

$$\frac{1}{2S}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \frac{m-1}{2}M(1) + M + \mathrm{O}(\log\log x)$$

where

$$M = \begin{cases} \frac{m(m-1)}{2}M(m) & \text{if } r \equiv 2 \bmod m \text{ and } r \neq 0,\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Combining the results of Facts 2.3 and 2.5 and recalling that $\varphi(m) = m-1$ for m prime,

$$\#\mathcal{P}_m(E/\mathbb{F}_p) = \begin{cases} (m-1)/2 & \text{if } E \text{ has cyclic torsion,}\\ (m+1)(m-1)/2 & \text{if } E \text{ has full torsion.}\end{cases} \tag{24}$$

Again, Lemma 2.10 gives

$$\begin{aligned} N_{p,r}(1\times m) &= N'_{p,r}(m) - N''_{p,r}(m), \text{ and}\\ N_{p,r}(m\times m) &= N''_{p,r}(m),\end{aligned} \tag{25}$$

and since $m \notin \{2,3\}$ Fact 2.6 gives

$$\#\mathcal{P}_m(\tilde{E}/\mathbb{F}_p) = \#\mathcal{P}_m(E/\mathbb{F}_p). \tag{26}$$

We combine Equations (24–26) with (18) to get

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{m-1}{2}N'_{p,r}(m) - \frac{m-1}{2}N''_{p,r}(m), \tag{27}$$

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{(m+1)(m-1)}{2}N''_{p,r}(m). \tag{28}$$

By substituting (27) and (28) into (17), we conclude

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r}}{}' 1 = \frac{m-1}{2}N_{p,r}(m) + \frac{m(m-1)}{2}N'_{p,r}(m). \tag{29}$$

Plugging (29) into the right side of (12) gives

$$\sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_1(p,S)\frac{m-1}{2}N'_{p,r}(m) + \sum_{\substack{B(r)<p\le x\\ p\equiv r-1 \bmod m}} A_1(p,S)\frac{m(m-1)}{2}N''_{p,r}(m) + \mathrm{O}(\log\log x).$$

We apply the results Theorem 2.9, and our claim follows from considering each of the cases for when $N''_{p,r}(m)$ is nonzero.$\square$

Lemma 2.18 *Fix $m \in \{6, 10\}$. Then $m = 2l$ for l an odd prime, and we have*

$$\frac{1}{2S}\sum_{|s|\le S,|t|\le T}{}' \pi^r_{E_{\mathcal{P}_m(s,t)}}(x) = \frac{\varphi(m)}{2}M(1) + M + \mathrm{O}(\log\log x)$$

where

$$M = \begin{cases} \frac{\varphi(m)}{2}\left(2M(2) + (\varphi(l)+1)M(1) + mM(m)\right) & \text{if } r \equiv 2 \bmod m \text{ and } r \neq 0 \\ \varphi(m)M(2) & \text{if } 2 \mid r, r \not\equiv 2 \bmod l, \text{and } r \neq 0 \\ \frac{\varphi(m)(\varphi(l)+1)}{2}M(l) & \text{if } r \equiv 2 \bmod l, 2 \nmid r, \text{and } r \neq 0 \\ \varphi(m)M'(2) & \text{if } r = 0 \\ 0 & \text{otherwise} \end{cases}$$

Proof. By Corollary 2.2, Facts 2.5, 2.6, and 2.3, and the assumption that $m \notin \{2, 3\}$, we have

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

By Lemma 2.11 we have,

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

Therefore, combining the above equations with Fact 2.9, we find for $r \neq 0$,

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{\varphi(m)}{2}\left(N'_{p,r}(m) - N''_{p,r}(2) - N''_{p,r}(l) + N''_{p,r}(m)\right), \tag{30}$$

as well as

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/q\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{\varphi(m)}{2}(\varphi(q)+2)\left(N''_{p,r}(q) - N''_{p,r}(m)\right), \text{ and} \tag{31}$$

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r\\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}}}{}' 1 = \frac{\varphi(m)}{2}\big(2(m+1)-\varphi(m)\big)N''_{p,r}(m). \tag{32}$$

Substituting (30–32) into (17) and collecting terms, we find

$$\sum_{\substack{0\le s<p\\ a_p(E_{\mathcal{P}_m(s)})=r}}{}' 1 = \frac{\varphi(m)}{2}N'_{p,r}(m) + \varphi(m)N''_{p,r}(2) + \frac{(\varphi(l)+1)\varphi(m)}{2}N''_{p,r}(l)$$
$$+ \frac{\varphi(m)}{2}\big(2(m-1)-\varphi(m)-\varphi(l)\big)N''_{p,r}(m). \tag{33}$$

Also note that $2(m-1)-\varphi(m)-\varphi(\ell) = m$. Plugging (33) into the right side of (12), simplifying as usual, and applying the results from Theorem 2.9 proves our claim.□

3 Averaging special values of Dirichlet L-series

We now turn our efforts towards estimating terms of the form

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

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 *Given r and m, set*

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

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*

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

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

$$H\left(\frac{r^2-4p}{d^2}\right) = \frac{1}{\pi} \sum_{\substack{d|f \\ f^2 | r^2-4p \\ \Delta \equiv 0,1 \bmod 4}} L(1,\chi_\Delta)\sqrt{-\Delta}. \tag{34}$$

In particular, we may write

$$\frac{1}{2} \sum_{\substack{B(r)<p\le x \\ p\equiv r-1 \bmod m}} \frac{1}{p} H\left(\frac{r^2-4p}{d^2}\right) = \frac{1}{\pi\sqrt{x}\log x} \sum_{\substack{f\le 2\sqrt{x} \\ d|f}} \frac{1}{f} \sum_{p\in \mathcal{S}_f(x)} L(1,\chi_\Delta)\log p$$
$$- \frac{1}{\pi}\int_2^x \sum_{\substack{f\le 2\sqrt{t} \\ d|f}} \left(\frac{1}{f}\sum_{p\in\mathcal{S}_f(t)} L(1,\chi_\Delta)\log p\right) \frac{d}{dt}\left(\frac{1}{\sqrt{t}\log t}\right)\, dt + \mathrm{O}(\log^2 x). \tag{35}$$

Proof. By Fact 2.8, we have

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

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 $d \mid f$:

$$H\left(\frac{r^2-4p}{d^2}\right) = 2 \sum_{\substack{d|f \\ f^2|r^2-4p \\ \Delta\equiv 0,1 \bmod 4}} \frac{h(\Delta)}{\omega(\Delta)}. \tag{36}$$

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

$$h(\Delta) = \frac{\omega(\Delta)\sqrt{-\Delta}}{2\pi} L(1,\chi_\Delta), \tag{37}$$

and (34) now follows from combining (37) and (36).

Substitute to obtain

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

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

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

and partial summation gives

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}\frac{L(1,\chi_\Delta)}{\sqrt{p}}=\frac{1}{\sqrt{x}\log x}\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}L(1,\chi_\Delta)\log p$$
$$-\int_2^x\sum_{\substack{f\le 2\sqrt{t}\\ d\mid f}}\left(\frac{1}{f}\sum_{p\in\mathcal{S}_f(t)}L(1,\chi_\Delta)\log p\right)\frac{d}{dt}\left(\frac{1}{\sqrt{t}\log t}\right)\,dt.$$

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*

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

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

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

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

$$\psi_1(x;n,a)=\sum_{\substack{p\le x\\ p\equiv a \bmod n}}\log p,$$
$$E_1(x;n,a)=\psi_1(x;n,a)-\frac{x}{\varphi(n)}.$$

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

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

Fact 3.6 (David and Pappalardi) *Define*

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

Then

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

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

Proof. Refer to Lemma 3.4 of [3].

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

$$\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\(a,n)=1}}\left(\frac{a}{n}\right)\sum_{\substack{p\in\mathcal{S}_f(x)\\ \Delta\equiv a \bmod 4n}}\left(\frac{\Delta}{n}\right)\log p$$
$$=\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\(a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r-1,m)=1,\ (r^2-af^2,4nf^2)=4}}\left(\frac{a}{n}\right)\psi_1(x;[nf^2,m],b)+\mathrm{O}(n), \quad (38)$$

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:

$$p\equiv r-1 \bmod m, \quad (39)$$
$$4p\equiv r^2 \bmod f^2, \quad (40)$$
$$4p\equiv r^2, r^2-f^2 \bmod 4f^2, \text{ and} \quad (41)$$
$$4p\equiv r^2-af^2 \bmod 4nf^2. \quad (42)$$

Congruence (41) implies (40), so we can ignore (40) altogether. Congruences (41) and (42) are compatible only if

$$r^2-af^2\equiv r^2, r^2-f^2 \bmod 4f^2,$$

or equivalently, only if $a\equiv 0,1 \bmod 4$. In such a case, (42) implies (41), so we are left with the congruences

$$p\equiv r-1 \bmod m, \quad (43)$$
$$4p\equiv r^2-af^2 \bmod 4nf^2, \quad (44)$$

and the preliminary assumption that $a\equiv 0,1 \bmod 4$. Congruences (43) and (44) are compatible only if

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

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

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

We may therefore write

$$\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\(a,n)=1}}\left(\frac{a}{n}\right)\sum_{\substack{p\in\mathcal{S}_f(x)\\ \Delta\equiv a \bmod 4n}}\log p=\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\(a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)}}\left(\frac{a}{n}\right)\sum_{\substack{B(r)<p\le x\\ p\equiv b \bmod [nf^2,m]}}\log p. \quad (45)$$

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

$$\sum_{\substack{B(r)<p\le x\\ p\equiv b \bmod [nf^2,m]}} \log p = \psi_1(x;[nf^2,m],b) + \mathrm{O}(1), \tag{46}$$

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 (46) into (45) establishes (38). □

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

$$\sum_{\substack{f\le 2\sqrt{x}\\ d|f}} \frac{1}{f} \sum_{p\in \mathcal{S}_f(x)} L(1,\chi_\Delta)\log p = K^{m,d}x + \mathrm{O}\left(\frac{x}{\log^c x}\right), \tag{47}$$

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

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

otherwise.

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

$$L(1,\chi_\Delta) = \sum_{n\ge 1}\left(\frac{\Delta}{n}\right)\frac{1}{n} = \sum_{n\le U}\left(\frac{\Delta}{n}\right)\frac{1}{n} + \sum_{n>U}\left(\frac{\Delta}{n}\right)\frac{1}{n}.$$

Note that

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

so that by the Polyá-Vinogradov inequality, we have

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

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

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

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

Substituting into (47), we find

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}L(1,\chi_\Delta)\log p$$

$$=\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{n\le U}\frac{1}{n}\sum_{p\in S_f(x)}\left(\frac{\Delta}{n}\right)\log p+\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in S_f(x)}\mathrm{O}\left(\frac{\sqrt{p}\log^2 p}{fU}\right)$$

Considering the sum over the error term, we have

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}\mathrm{O}\left(\frac{\sqrt{p}\log^2 p}{fU}\right)=\mathrm{O}\left(\frac{1}{U}\right)\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\mathrm{O}\left(\frac{1}{f^2}\right)\sum_{p\in\mathcal{S}_f(x)}\mathrm{O}(\sqrt{p}\log^2 p),$$

Note that

$$\sum_{p\in\mathcal{S}_f(x)}\sqrt{p}\log^2 p\le\sum_{p\le x}\sqrt{p}\log^2 p\le\sum_{n\le x}\sqrt{n}\log^2 n\le x^{3/2}\log^2 x\le x^{5/2}\log x.$$

Then

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}\mathrm{O}\left(\frac{\sqrt{p}\log^2 p}{fU}\right)=\mathrm{O}\left(\frac{x^{5/2}\log x}{U}\right)\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\mathrm{O}\left(\frac{1}{f^2}\right)$$

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

Substitution gives

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{p\in\mathcal{S}_f(x)}L(1,\chi_\Delta)\log p=\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{n\le U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{\Delta}{n}\right)\log p+\mathrm{O}\left(\frac{x^{3/2}\log x}{U}\right).\qquad(48)$$

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

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}}\frac{1}{f}\sum_{n\le U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{\Delta}{n}\right)\log p=\sum_{\substack{f\le V\\ d\mid f}}\frac{1}{f}\sum_{n\le U}\frac{1}{n}\sum_{p\in\mathcal{S}_f(x)}\left(\frac{\Delta}{n}\right)\log p$$

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

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 $p\in\mathcal{S}_f(x)$. 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

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

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

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

Combining with (48), we find

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

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

$$\sum_{\substack{f\le V\\ d\mid f}} \frac{1}{f} \sum_{n\le U} \frac{1}{n} \sum_{p\in \mathcal{S}_f} \left(\frac{\Delta}{n}\right) \log p = \sum_{\substack{n\le U, f\le V\\ d\mid f}} \frac{1}{nf} \sum_{\substack{a\in \mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1}} \left(\frac{a}{n}\right) \sum_{\substack{p\in \mathcal{S}_f(x)\\ \Delta\equiv a \bmod 4n}} \log p. \tag{49}$$

Furthermore, by Lemma 3.7, we have

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

Rewriting ψ_1 in terms of E_1, we have

$$\sum_{\substack{a\in \mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1}} \left(\frac{a}{n}\right) \sum_{\substack{p\in \mathcal{S}_f(x)\\ \Delta\equiv a \bmod 4n}} \log p = x \sum_{\substack{n\le U, f\le V\\ d\mid f,\ (r-1,m)=1}} \frac{c_f(n)}{nf\varphi[nf^2,m]} + \sum_{\substack{n\le U, f\le V\\ d\mid f,\ (r-1,m)=1}} \frac{1}{nf} \sum_{\substack{a\in \mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right) E_1(x;[nf^2,m],b) + \mathrm{O}(U\log V). \tag{50}$$

(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

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

$$\leq \sum_{f \leq V} \frac{1}{f} \left(\sum_{n \leq U} \frac{1}{n^2} \right)^{1/2} \left(\sum_{n \leq U} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ (a,n)=1,\ a \equiv 0,1 \bmod 4 \\ 4(r-1) \equiv r^2 - af^2 \bmod 4(nf^2,m) \\ (r^2-af^2, 4nf^2)=4}} E_1^2(x; [nf^2, m], b) \right)^{1/2}. \quad (51)$$

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

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

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

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

We may conclude that

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

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

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

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

whenever

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

so that

$$\sum_{\substack{n\le U, f\le V\\ d\mid f}} \frac{1}{nf} \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ (a,n)=1,\ a\equiv 0,1 \bmod 4\\ 4(r-1)\equiv r^2-af^2 \bmod 4(nf^2,m)\\ (r^2-af^2,4nf^2)=4}} \left(\frac{a}{n}\right) E_1(x;[nf^2,m],b) \le \log^{1/2} U\log V \frac{x}{\log^{c+2} x}, \quad (52)$$

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

$$\sum_{\substack{f\le 2\sqrt{x}\\ d\mid f}} \frac{1}{f} \sum_{p\in\mathcal{S}_f(x)} L(1,\chi_\Delta)\log p = x \sum_{\substack{n\le U, f\le V\\ d\mid f}} \frac{c_f(n)}{nf\varphi[nf^2,m]}$$

$$+ \mathrm{O}\left(U\log V + \frac{x\log^{1/2} U\log V}{\log^{c+2} x} + \frac{x^{3/2}\log x}{U} + \frac{x\log x\log U}{V^2}\right).$$

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 $|c_f(n)|\le 2n/\kappa(n)$ (see Lemma 4.7) and also that $\varphi[nf^2,m]\ge\varphi(n)\varphi(f^2)\ge 1$, we have

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

By Fact 3.6

$$x\sum_{\substack{n\le U, f\le V\\ d\mid f}} \frac{c_f(n)}{nf\varphi[nf^2,m]} = x\sum_{\substack{f\le V\\ d\mid f}}\sum_{n=1}^{\infty} \frac{c_f(n)}{nf\varphi[nf^2,m]} + \mathrm{O}\left(x\sum_{n>U}\frac{1}{\kappa(n)\varphi(n)}\sum_{f\le V}\frac{1}{f\varphi(f^2)}\right),$$

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

and similarly we have

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

so that

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

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

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

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

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

we find

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

as desired. □

4 The function c_f

4.1 Properties of $c_{f,i}$

Recall that $K^{m,d}=0$ if $(r,m-1)\neq 1$. Thus, for the next two sections, we may assume that $(r,m-1)=1$. 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 and r we define*

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

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

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 *The constant $c_{f,i}(n)$ is nonzero only if $(m,f) \mid (r-2)^2$. Also,*

1. *For $c_{f,0}(n)$ to be nonzero, we must have r even, n odd, and $(r/2,f)=1$;*
2. *For $c_{f,1}(n)$ 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 $(r,f/2)=1$.*

Proof. Suppose $c_{f,i}(n)$ is nonzero for a fixed set of parameters. From the definition of $c_{f,i}(n)$, there exists an $a \in \mathbb{Z}/4n\mathbb{Z}$ such that $(m,f) \mid (r-2)^2 - af^2$. Since $(m,f) \mid af^2$, we must have $(m,f) \mid (r-2)^2$.

In the case of $i=0$, there exists an $a \in \mathbb{Z}/4n\mathbb{Z}$ such that $4 \mid a$, $(r^2-af^2, 4nf^2) = 4$, and $\left(\frac{a}{n}\right) \neq 0$. Thus, $4 \mid r^2$ and r must be even. Since $\left(\frac{a}{n}\right) \neq 0$, n must be odd otherwise $(a,n) \neq 1$. Finally, the condition $(r^2-af^2, 4nf^2) = 4$ holds only if $(r/2,f)=1$.

If $i=1$, there exists an $a \in \mathbb{Z}/4n\mathbb{Z}$ such that $a \equiv 1 \bmod 4$, $(r^2-af^2, 4nf^2) = 4$, and $\left(\frac{a}{n}\right) \neq 0$. Since $a \equiv 1 \bmod 4$, a is odd and $(r^2-af^2, 4nf^2) = 4$ is satisfied only if r and f are both even or both odd. If r and f are odd, we must have $(r,f)=1$. If r and f are even, then $((r/2)^2 - a(f/2)^2, nf^2) = 1$ must hold. This is true only if $2 \nmid (r/2)^2 - a(f/2)^2$ and $(r/2, f/2) = 1$; thus, we must either have condition 2*b* or 2*c*. □

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

Proof. We first show that $c_{f,0}$ is multiplicative. In the case of r odd, we have $c_{f,0}(n) = 0$; 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

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

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

$$c_{f,0}(n) = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{af^2}{(m,f)} \bmod \left(n, \frac{m}{(m,f)}\right) \\ ((r/2)^2 - af^2, n) = 1}} \left(\frac{a}{n}\right). \tag{53}$$

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

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

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

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

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,

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

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

$$\begin{aligned}\frac{(r/2-1)^2}{(m,f)} &\equiv \frac{a_1 f^2}{(m,f)} \mod \left(n_1, \frac{m}{(m,f)}\right), \text{ and} \\ \frac{(r/2-1)^2}{(m,f)} &\equiv \frac{a_2 f^2}{(m,f)} \mod \left(n_2, \frac{m}{(m,f)}\right)\end{aligned}$$

hold iff

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

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

$$(\tfrac{1}{4}r^2 - a_j f^2)x + n_j y = 1.$$

But $a_j = a + k_j n_j$, so

$$(\tfrac{1}{4}r^2 - af^2)x' + n_j y' = 1,$$

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

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

as desired.

We now turn to the case of $i = 1$; the details of the arguments are similar here. $c_{f,1}(n)$ is nonzero only if the conditions in 2a, 2b, or 2c hold. As in [3], 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,

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

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,

$$c_{f,1}(n) = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ \frac{(r-2)^2}{(m,f)} \equiv \frac{af^2}{(m,f)} \bmod\left(n, \frac{m}{(m,f)}\right) \\ (r^2 - af^2, n) = 1}} \left(\frac{a}{n}\right). \tag{54}$$

Furthermore, in cases 2b and 2c (see [9] for details)

$$c_{f,1}(n) = \sum_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^* \\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{a(f/2)^2}{(m,f)} \bmod\left(n, \frac{m}{(m,f)}\right) \\ ((r/2)^2 - a(f/2)^2, n) = 1}} \left(\frac{a}{n}\right). \tag{55}$$

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 (54) and the Chinese remainder theorem. Cases 2b and 2c follow from equation (55) and the Chinese remainder theorem. $\square$

4.2 Computation of $c_{f,i}$

For the sake of notation, if n is a positive integer and q is a prime, set $(n)_q = q^{\mathrm{ord}_q\, n}$. 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

$$c_{f,i}(n) = \prod_{\substack{q \mid n \\ q \text{ prime}}} c_{f,i}(n)_q.$$

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

The following reduction lemma will be used to greatly simplify the computation of the $c_{f,i}$.

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

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

We have the following reduction:

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

where $\alpha \geq 0$.

Proof when $q = 2$. Reduction is immediate when $i = 0$ since Fact 4.2 implies that $c_{f,0}(2^\alpha) = 0$. In the case of $i = 1$, we show that the value of $c_{f,1}(2^\alpha)$ is independent from f when r and f satisfy one of the conditions in Fact 4.2. The reduction then follows since $(f)_2$ and r will satisfy the same condition in Fact 4.2 as f and r.

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

$$c_{f,1}(2^\alpha) = \sum_{\substack{a \in \mathbb{Z}/2^{\alpha+2}\mathbb{Z},\ a \equiv 1 \bmod 4 \\ 4(r-1) \equiv r^2 - af^2 \bmod 4(2^\alpha f^2, m) \\ (2^{\alpha+2}f^2, r^2-af^2)=4}} \left(\frac{a}{2^\alpha}\right). \tag{56}$$

Since r and f are odd, $(2^{\alpha+2}f^2, r^2-af^2) = 4$ holds iff $(f^2, r^2-af^2)=1$, $4 \mid r^2-af^2$, and $r^2-af^2 \not\equiv 0 \bmod 8$. Moreover, with the assumptions on r and f and assuming that $a \equiv 1 \bmod 4$, it is immediate that $(f^2, r^2-af^2)=1$ and $r^2-af^2 \equiv r^2-f^2 \equiv 0 \bmod 4$. Thus, $a \equiv 1 \bmod 4$ and $(2^{\alpha+2}f^2, r^2-af^2)=4$ iff $a \equiv 1 \bmod 4$ and $r^2-af^2 \not\equiv 0 \bmod 8$ iff $a \equiv 5 \bmod 8$. To see the last equivalence, write $r=2s+1$, $f=2t+1$ to get

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

We next show that the condition $4(r-1) \equiv r^2-af^2 \bmod 4(2^\alpha f^2, m)$ may be ignored. Simplication shows that $4(r-1) \equiv r^2-af^2 \bmod 4(2^\alpha f^2, m)$ holds iff $(2^\alpha f^2, m) \mid (r-2)^2+af^2$. Under the conditions on m and f, in particular $(m,f) \mid (r-2)^2$, the latter always holds unless $8 \mid m$ and $\alpha > 2$. This is because $8 \nmid (r-2)^2+af^2$; thus, reduction holds in this case since $c_{f,1}(2^\alpha)=0$ when $\alpha > 2$. In the other cases, combining the above results gives

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

Now suppose r and f satisfy 2b or 2c of Fact 4.2. We again have (56). Given the additional assumption that $a \equiv 1 \bmod 4$, 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 $(2^\alpha f^2, m) \mid (r-2)^2+af^2$. However, in these cases, $8 \mid (r-2)^2+af^2$ so $(2^\alpha f^2, m) \mid (r-2)^2+af^2$ is always true under our assumptions. Thus,

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

and reduction follows.

Proof when q is odd. We only prove the case when $i=0$ since the proofs of the other cases are essentially the same. Assume r and f satisfy condition 1 of Fact 4.2. Equation 53 gives

$$c_{f,0}(q^\alpha) = \sum_{\substack{(1)\ a \in (\mathbb{Z}/q^\alpha\mathbb{Z})^* \\ (2)\ \frac{(r/2-1)^2}{(m,f)} \equiv \frac{af^2}{(m,f)} \bmod \left(q^\alpha, \frac{m}{(m,f)}\right) \\ (3)\ ((r/2)^2-af^2, q)=1}} \left(\frac{a}{q}\right)^\alpha.$$

Reduction is clear when $\alpha=0$, so let $\alpha > 0$. If $q \nmid m$, condition (2) is always satisfied. Let $a \in (\mathbb{Z}/q^\alpha\mathbb{Z})^*$, then $q \nmid a$. By assumption, $(r/2, f)=1$. Thus, $q \mid f$ implies that (3) is always

satisfied. If $q \nmid f$, then we have a one to one correspondance between the $a \in (\mathbb{Z}/q^\alpha\mathbb{Z})^*$ such that $((r/2)^2 - af^2, q) = q$ and the $b \in (\mathbb{Z}/q^\alpha\mathbb{Z})^*$ such that $((r/2)^2 - b, q) = q$. Furthermore, for such values of a and b, $\left(\frac{a}{q}\right) = \left(\frac{b}{q}\right) = 1$, and our summation becomes

$$\sum_{\substack{a \in (\mathbb{Z}/q^\alpha\mathbb{Z})^* \\ \left((r/2)^2 - a, q\right) = 1}} \left(\frac{a}{q}\right)^\alpha.$$

Now suppose $q \mid m$ and $q \mid f$, then (3) is always satisfied since $(r/2, f) = 1$. Moreover, for the different cases of m, we either have $\left(q^\alpha, \frac{m}{(m,f)}\right) = 1$ or $\left(q^\alpha, \frac{m}{(m,f)}\right) = (m, f) = q$. It is clear that (2) always holds in the first case. In the second case, (2) becomes $\frac{(r/2-1)^2}{q} \equiv 0 \bmod q$. Since $(m, f) \mid (r-2)^2$ and q is odd, (2) is always satisfied.

In the case of $q \mid m$ and $q \nmid f$, (2) becomes $(r/2-1)^2 \equiv af^2 \bmod q, q^2$ for the different cases of m. This holds only if $(r/2)^2 - af^2 \equiv r - 1 \bmod q$. Recall that $(r-1, m) = 1$; thus $q \nmid (r/2)^2 - af^2$ and (3) is always satisfied. Since $q \nmid f$, there is a one to one correspondance between the $a \in (\mathbb{Z}/q^\alpha\mathbb{Z})^*$ such that $(r/2-1)^2 \equiv af^2 \bmod q, q^2$ and the $b \in (\mathbb{Z}/q^\alpha\mathbb{Z})^*$ such that $(r/2-1)^2 \equiv b \bmod q, q^2$. Moreover, all such a's and b's must have $\left(\frac{a}{q}\right) = \left(\frac{b}{q}\right) = 1$. Thus, our summation becomes

$$\sum_{\substack{a \in (\mathbb{Z}/q^\alpha\mathbb{Z})^* \\ (r/2-1)^2 \equiv a \bmod q}} \left(\frac{a}{q}\right)^\alpha.$$

We have now shown for all cases that our constant can be written independently of f. Thus, $c_{f,0}$ is independent of f provided r and f satisfy condition 1; since r and $(f)_q$ satisfy 1, reduction follows. □

The following two lemmas will be used to be evaluate the reduced constants $c_{\sigma_i^r(f)_q}(q^\alpha)$.

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

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

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

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

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

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

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

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

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

Proof of 1. Follows from Fact 4.2 and equation 53.

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

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

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

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

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

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

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

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

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

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

where $\left(\frac{a}{n}\right)$ is the Kronecker symbol.

Proof. The proof when $\alpha = 0$ is immediate from equations 53, 54, and 55. For the case of $\beta = 0$ and $i = 0$, we saw in the proof of 4.4 that

$$c_{1,0}(q^\alpha) = \begin{cases} \sum_{\substack{a \in \mathbb{Z}/q^\alpha\mathbb{Z} \\ \left((r/2)^2 - a, q\right) = 1}} \left(\frac{a}{q}\right)^\alpha & \text{if } q \nmid m \\ \sum_{\substack{a \in \mathbb{Z}/q^\alpha\mathbb{Z} \\ (r/2-1)^2 \equiv a \bmod q}} \left(\frac{a}{q}\right)^\alpha & \text{if } q \mid m. \end{cases}$$

There are $\frac{q-1}{2}q^{\alpha-1}$ quadratic residues and $\frac{q-1}{2}q^{\alpha-1}$ quadratic nonresidues in $\mathbb{Z}/q^\alpha\mathbb{Z}$. When $q \nmid m$, there are $q^{\alpha-1}$ a's in $\mathbb{Z}/q^{\alpha-1}\mathbb{Z}$ such that $((r/2)^2 - a, q) = q$. For each such a, $(r/2)^2 \equiv a \bmod q$ implies that

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & \text{if } \left(\frac{r^2}{q}\right) = 0 \\ 1 & \text{if } \left(\frac{r^2}{q}\right) = 1. \end{cases}$$

Thus, when $q \nmid m$,

$$c_{1,0}(q^\alpha) = \begin{cases} -\frac{q-1}{2}q^{\alpha-1} + \frac{q-1}{2}q^{\alpha-1} - \left(\frac{r^2}{q}\right)q^{\alpha-1} = -\left(\frac{r^2}{2}\right)q^{\alpha-1} & \alpha \text{ odd} \\ \frac{q-1}{2}q^{\alpha-1} + \frac{q-1}{2}q^{\alpha-1} - \left(\frac{r^2}{q}\right)q^{\alpha-1} = \left(q - 1 - \left(\frac{r^2}{q}\right)\right)q^{\alpha-1} & \alpha \text{ even.} \end{cases}$$

Similarily, when $q \mid m$ there are $q^{\alpha-1}$ a's in $\mathbb{Z}/q^{\alpha-1}\mathbb{Z}$ such that $(r/2-1)^2 \equiv a \bmod q$. Then for all such a,

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & \text{if } \left(\frac{(r-2)^2}{q}\right) = 0 \\ 1 & \text{if } \left(\frac{(r-2)^2}{q}\right) = 1. \end{cases}$$

and our claim follows. The proof when $\beta = 0$ and $i = 1$ follows from the same arguments.

Now suppose $\beta > 0$. We have

$$c_{1,0}(q^\alpha) = \sum_{a \in \mathbb{Z}/q^\alpha\mathbb{Z}} \left(\frac{a}{q}\right)^\alpha = \begin{cases} 0 & \alpha \text{ even} \\ (q-1)q^{\alpha-1} & \alpha \text{ odd. } \square \end{cases}$$

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

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

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

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

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

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

$$|c_{f,i}(n)| \leq n/\kappa(n). \ \square$$

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

Finding the constants which appear in the statement of Theorem 1.4 will require all of our computational results thus far, especially those related to the function $c_{f,i}$.

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

We first will find explicit formulae for the constants $K^{m,d}$ (when $(r-1,m)=1$) which appear in the conclusion of Theorem 3.8. In particular, we recall that

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

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

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

Replacing f by df, we have

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

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

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

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

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

Setting

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

we find

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

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

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

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

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

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

$$\begin{aligned} K_i^{m,d} &= \frac{1}{d}\prod_q \left(\sum_{\alpha\geq 0} \frac{c_{\sigma_i^r(d)_q,i}(q^\alpha)}{q^\alpha \varphi([m, q^\alpha d^2]_q)} + \sum_{\beta=1}^{\infty}\frac{1}{q^\beta}\sum_{\alpha\geq 0} \frac{c_{\sigma_i^r(d)_q q^\beta,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha+2\beta}d^2]_q)}\right), \\ &= \frac{1}{d}\prod_q \sum_{\beta=0}^{\infty}\frac{1}{q^\beta}\sum_{\alpha\geq 0} \frac{c_{\sigma_i^r(d)_q q^\beta,i}(q^\alpha)}{q^\alpha \varphi([m, q^{\alpha+2\beta}d^2]_q)}, \end{aligned}$$

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

$$K_i^{m,d} = \frac{1}{d}\prod_q K_i^{m,d}(q). \tag{57}$$

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

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

$$K_i^{m,d} = \frac{1}{d}K_i^{m,d}(2)\prod_{\substack{q\mid m\\ q\neq 2}} K_i^{m,d}(q)\prod_{\substack{q\mid r\\ q\nmid 2m}} K_i^{m,d}(q)\prod_{q\nmid 2mr} K_i^{m,d}(q). \tag{58}$$

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

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

and

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

Combining these results,

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

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 $c_{\sigma_i^r q^\beta,i}(q^\alpha)=0$ when $\beta>0$ and (since $q\mid r$ implies $(r^2/q)=0$),

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

Substitution yields

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

Therefore,

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

Combining the last two results and equation (58), we find

$$K_i^{m,d}=\frac{1}{d}K_i^{m,d}(2)\prod_{\substack{q\mid m\\ q\neq 2}}K_i^{m,d}(q)\prod_{\substack{q\mid r\\ q\nmid 2m}}\frac{q^2}{q^2-1}\prod_{q\nmid 2mr}\frac{q(q^2-q-1)}{(q-1)^2(q+1)}.\tag{59}$$

The remaining computations must be specialized for the different values of m,d, where $d\mid m$. Noting that $K_i^{m,d}(q)=K_i^{(m)_q,(d)_q}(q)$ 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 necessary values of $K_i^{m,d}(q)$ (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	$i=1$ $r\equiv 2 \bmod 4$	$i=1$ $4 \mid r$
$K_i^{1,1}(2)$	9/7	1	2/3	1/21	1/3
$K_i^{2,1}(2)$	9/7	1	1	1/21	1/3
$K_i^{4,1}(2)$	11/14	1/2	1/2	1/21	1/3
$K_i^{4,2}(2)$	4/7	0	0	2/21	2/3
$K_i^{8,1}(2)$	23/56	1/4	1/4	1/21	5/24
$K_i^{8,2}(2)$	4/7	0	0	2/21	5/12
$K_i^{16,1}(2)$	25/112	1/8	1/8	1/21	7/48
$K_i^{16,4}(2)$	1/7	0	0	4/21	0

	$i=0$ $r\equiv 2 \bmod 8$	$i=0$ $r\equiv 6 \bmod 8$	$i=0$ $4 \mid r$	$i=1$ r is odd	$i=1$ $r\equiv 2 \bmod 8$	$i=1$ $r\equiv 6 \bmod 8$	$i=1$ $4 \mid r$
$K_i^{64,8}(2)$	1/28	9/256	0	0	1/21	3/64	0

	$i=0$	$r\equiv 2 \bmod 3$ $r\not\equiv 2 \bmod 9$	$r \equiv 2 \bmod 9$	$r \not\equiv 2 \bmod 3$
$K_i^{3,1}(3)$	0	9/16	9/16	3/4
$K_i^{3,3}(3)$	0	11/48	11/48	11/36
$K_i^{9,3}(3)$	0	3/16	3/16	0
$K_i^{27,1}(3)$	0	59/729	35/432	13/108
$K_i^{81,9}(3)$	0	13/648	1/48	0

	$i=0$	$r \equiv 2 \bmod 5$	$r \not\equiv 2 \bmod 5$
$K_i^{5,1}(3)$	0	25/96	5/16
$K_i^{25,5}(3)$	0	5/96	0

	$i=0$	$r \equiv 2 \bmod 7$	$r \not\equiv 2 \bmod 7$
$K_i^{7,1}(3)$	0	49/288	7/36
$K_i^{49,7}(3)$	0	7/288	0

Given r, m and d, we now have all the necessary information to determine the value of $K^{m,d}$. First recall that $K^{m,d} = 0$ if $(r-1, m) \neq 1$. Otherwise, we determine $K_0^{m,d}$ and $K_1^{m,d}$ by plugging in the relevant values of $K_i^{m,d}(q) = K_i^{(m)_q,(d)_q}(q)$, given in the charts above, into (59). We then recall that $K^{m,d} = K_0^{m,d} + K_1^{m,d}$. The various modulo conditions in the above charts lead to an extremely large number of cases. Since the exact numeric values of $K^{m,d}$ are not important for our purposes, we leave out these final computations.

6 Additional analytic results

We now focus on proving some additional needed analytic results. Section 2 showed us how to rewrite the average in our main theorem as a summation of class numbers. The results in this section allow us to rewrite such summations in terms of our constant $K^{m,d}$ and function

$\pi_{1/2}(x)$. The following two results involve sums of the class number $H(\Delta)$. The first result is given by Lemma 1 of [2].

Lemma 6.1 *We have*

$$\sum_{\substack{B(r)<p\leq x\\ p\equiv r-1 \bmod m}} H\left(\frac{r^2-4p}{d^2}\right) = \mathrm{O}\left(x^{3/2}\right).$$

Corollary 6.2 *Fix r and m. Then for any $c>0$,*

$$\frac{1}{2}\sum_{\substack{B(r)<p\leq x\\ p\equiv r-1 \bmod m}} \frac{1}{p}H\left(\frac{r^2-4p}{d^2}\right) = \frac{2K^{m,d}}{\pi}\pi_{1/2}(x) + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c(x)}\right).$$

Proof. This follows from combining equations 35 and 47. A detailed proof is carried out in the proof of Corollary 2 of [2]. □

We now give two analogous results for sums involving the class number $h(\Delta)$.

Lemma 6.3 *We have*

$$\sum_{\substack{B(r)<p\leq x\\ p\equiv r-1 \bmod m}} h\left(-p\right) = \mathrm{O}\left(x^{3/2}\right).$$

Proof. As seen in [16], there is an upper bound on $h(-p)$; namely $h(-p)$ is $\mathrm{O}\left(p^{1/2}\log p\right)$. Applying this bound and the prime number theorem to the summation gives us our claim. □

Lemma 6.4 *Provided that $4 \mid m$, for all $c>0$,*

$$\sum_{\substack{B(r)<p\leq x\\ p\equiv -1 \bmod m}} \frac{h(-p)}{p} = K^m\pi_{1/2}(x) + \mathrm{O}\left(\frac{\sqrt{x}}{\log^c x}\right)$$

where $K^m = \frac{\pi}{3\varphi(m)}$.

Proof. The proof for the case of $m=4$ is essentially given in Section 5 of [5]. The proof for all other cases are nearly identical; thus we only give a brief sketch of the proof and refer the reader to [5] for more details.

Recall the class number formula: If $\Delta<0$,

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

where $\omega(\Delta)$ gives the number of units in the ring $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{\Delta})\right]$ and $\chi_\Delta(n)$ is the Kronecker symbol $\left(\frac{\Delta}{n}\right)$. Since $\omega(-p)=2$ for all but two cases ($p=3,4$), we may replace $\omega(-p)$ with 2. Thus,

$$\sum_{\substack{B(r)<p\leq x\\ p\equiv -1 \bmod m}} \frac{h(-p)}{p} = \frac{1}{\pi}\sum_{\substack{B(r)<p\leq x\\ p\equiv -1 \bmod m}} \frac{L(1,\chi_{-p})}{\sqrt{p}}.$$

Partial summation and the Polya-Vinogradov inequality give, for any $U > 0$,

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

For our purposes, let $U = x^{3/4}$. By our assumptions, $4 \mid m$. Thus $p \equiv -1 \bmod m$ implies that $p \equiv 3 \bmod 4$. Reciprocity then allows us to write $\chi_{-p}(n) = \left(\frac{n}{p}\right)$. We now have

$$\sum_{\substack{B(r)<p\leq x \\ p\equiv -1 \bmod m}} \frac{L(1,\chi_{-p})}{\sqrt{p}} = \sum_{\substack{B(r)<p\leq x \\ p\equiv -1 \bmod m}} \frac{1}{\sqrt{p}} \sum_{n\leq U} \frac{\left(\frac{n}{p}\right)}{n} + \sum_{\substack{B(r)<p\leq x \\ p\equiv -1 \bmod m}} \mathrm{O}\left(\frac{\log p}{U}\right).$$

Using the prime number theorem for arithmetic progressions, the second summation becomes $\mathrm{O}(x^{1/4})$. We now focus on analyzing the first summation. Switching the order of the summation gives

$$S(x) = \sum_{n\leq U} \frac{1}{n} \sum_{\substack{B(r)<p\leq x \\ p\equiv -1 \bmod m}} \frac{\left(\frac{n}{p}\right)}{\sqrt{p}}.$$

If n is a perfect square, then the inner sum becomes

$$\frac{1}{\varphi(m)} \int_2^x \frac{dt}{\sqrt{t}\log t} + \mathrm{O}\left(\sqrt{x}\exp(-\sqrt{\log x})\right),$$

giving us the following main term for $S(x)$

$$\frac{\pi^2}{6\varphi(m)} \int_2^x \frac{dt}{\sqrt{t}\log t} + \mathrm{O}\left(\sqrt{x}(U^{-1/2} + \exp(-\sqrt{\log x}))\right).$$

The remainder of the proof is identical to the proof given in [5]. We have the following estimation for the sum when n is not a perfect square (p. 13 [5]):

$$\sum_{\substack{n\leq U \\ n \text{ not a square}}} \frac{1}{n} \sum_{\substack{B(r)<p\leq x \\ p\equiv -1 \bmod m}} \frac{\left(\frac{n}{p}\right)}{\sqrt{p}} \ll \frac{\sqrt{x}}{(\log^c x)}$$

for every $c > 0$. Our claim now follows. □

7 Putting it all together

We now have all the necessary tools to prove Theorem 1.4, our main theorem. Combining the results in Section 2, 5 and 6 gives us the following lemma; we only give a sketch of the proof since it consists mainly of tedious simplication.

Lemma 7.1 *Fix $m \in \mathcal{M}$ and $r \in \mathbb{Z}$. Let $\mathcal{E}_m(\mathbf{t})$ be the parametrized family of elliptic curves having nontrivial rational m-torsion whose parameters are bounded by the vector $\mathbf{t}$. Let N equal the minimum of the components of $\mathbf{t}$. Then for all $c > 0$,*

$$\frac{1}{\#\mathcal{E}_m(\mathbf{t})} \sum_{E \in \mathcal{E}_m(\mathbf{t})}{}' \pi_E^r(x) = C^{r,m}\pi_{1/2}(x) + \mathrm{O}\left(\frac{x^{3/2}}{N} + \frac{x^{5/2}}{N^2} + \frac{\sqrt{x}}{\log^c x}\right), \tag{60}$$

where $C^{r,m}$ is a constant dependent on r and m.

Proof. The results in Section 2 have shown us how to rewrite the left side of (60) as a sum of terms involving class numbers. Many cases arise due to the different values of m and congruence conditions on r. As an example, when $m = 2$ and $r = 0$, Lemma 2.16 rewrites the average in (60) as

$$\sum_{\substack{B(r)<p\le x \\ p\equiv r-1 \bmod m}} A_2(p,S,T)\left(\frac{p}{2}H(r^2-4p)+\mathrm{O}(p)\right) + \sum_{\substack{B(r)<p\le x \\ p\equiv r-1 \bmod m^2}} \frac{mpA_2(p,S,T)}{2}h(-p)+\mathrm{O}(\log\log x).$$

Applying the results of Section 6 to the above equation gives

$$\left(\frac{\pi}{3}+\frac{2}{\pi}K^{2,1}\right)\pi_{1/2}(x) + \mathrm{O}\left(\left(\frac{1}{S}+\frac{1}{T}\right)x^{3/2} + \frac{x^{5/2}}{ST} + \frac{\sqrt{x}}{\log^c x}\right)$$

where $K^{0,2,1} = \frac{4}{3}\prod_{q\neq 2}\frac{q^2}{q^2-1}$ by the method given at the bottom of Section 5. All other cases are proven in the same way. Note that this process also allows us to determine the constant $C^{r,m}$. □

Our main theorem is then an immediate corollary of the above lemma.

Theorem 7.2 *Fix $m \in \mathcal{M}$ and $r \in \mathbb{Z}$. Let $\mathcal{E}_m(\mathbf{t})$ be the parametrized family of elliptic curves having nontrivial rational m-torsion whose parameters are bounded by the vector $\mathbf{t}$ and let $\epsilon > 0$. If $T > x^{1+\epsilon}$ for every component T of $\mathbf{t}$, then as $x \to \infty$*

$$\frac{1}{\#\mathcal{E}_m(\mathbf{t})} \sum_{E \in \mathcal{E}_m(\mathbf{t})}{}' \pi_E^r(x) \sim C^{r,m}\pi_{1/2}(x),$$

where $\sum'$ denotes the sum over nonsingular curves, and $C^{r,m}$ is a constant dependent on r and m.

Acknowledgements: This work was started at the 2005 REU for Computational Number Theory and Combinatorics at Clemson University with the help of Kevin James, Neil J. Calkin, and Timothy Flowers. The work was completed in the summer of 2006 under the supervision of Bjorn Poonen at the University of California, Berkeley. The authors would like to thank these advisors for their help and support. In addition, the authors would like to thank Kenneth A. Ribet, Francesco Pappalardi, René Schoof, and Alina Cojocaru for their helpful suggestions in Section 6.

8 Notation

- $[a, b]$ is the least common multiple of a and b
- (a, b) is the greatest common divisor of a and b
- $\left(\frac{a}{n}\right)$ is the Kronecker symbol
- $\pi_{1/2}(x) = \int_2^x \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}$
- $\pi_E^r(x) = \{p \leq x : a_p(E) = r\}$
- $\pi(x)$ counts the number of primes $\leq x$
- $\varphi(n)$ is the Euler totient function
- $\sum'$ denotes that the sum is over only those parameters resulting in nonsingular curves
- $a_p(E)$ is the trace of the Frobenius endomorphism of $E/\mathbb{F}_p$
- $B(r) = \max\{3, r, r^2/4\}$
- $E(F)$ is the set of points on an elliptic curve E over a field F
- $E(F)_{tor}$ is the torsion subgroup of $E(F)$
- $E(F)[m]$ is the m-torsion subgroup of $E(F)$
- G^* is the set of units in the group G
- $H(\Delta)$ is the Kronecker class number
- $h(\Delta)$ is the class number of $\mathbb{Q}(\sqrt{\Delta})$
- $(n)_q = q^{\mathrm{ord}_q\, n}$ where n is a postive integer and q is a prime
- $\mathcal{M} = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

[2] J. Battista, J. Bayless, D. Ivanov, and K. James, *Average Frobenius distributions for elliptic curves with nontrivial rational torsion*, Mathematics Subject Classification (2000).

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

[4] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. (1941) **14** 197–272.

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

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

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

[8] G. H. Hardy, M. R. Murty, *Some problems of partitio numenorum III*, Acta. Math. (1923) **44**, 1-70.

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

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

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

[12] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (1976) (3) **33**, 193–237.

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

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

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

[16] J. P. Serre, *Lectures on the Mordell-Weil Theorem*, Friedrick Vieweg and Son, 1997.

[17] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math., (1972) **15**, 259–331.

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

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