AVERAGING SPECIAL VALUES OF DIRICHLET L-SERIES.

KEVIN JAMES

ABSTRACT. In this paper we derive estimates for weighted averages of the special values of Dirichlet L-series which generalize similar estimates of David and Pappalardi [1].

1. Introduction.

Fix $r, m, n \in \mathbb{Z}$ with $(m,n) = 1$. Let $d_p(f) = \frac{r^2-4p}{f^2}$ and $B(r) = \max(5, r^2/4)$. Define

$$S_f^r(m,n,X) := \left\{ \begin{array}{r} B(r) < p \leq X : \text{p is prime}; p \equiv m \pmod{n}; \\ 4p \equiv r^2 \pmod{f^2}; d_p(f) \equiv 0,1 \pmod{4} \end{array} \right\} \tag{1}$$

and

$$A(r,m,n,X) := \sum_{f \leq 2\sqrt{X}} \frac{1}{f} \sum_{p \in S_f^r(m,n,X)} L(1, \chi_{d_p(f)}) \log p \tag{2}$$

David and Pappalardi (see [1] Theorem 3.1 and Lemma 4.1) proved an estimate for $A(r,1,1,X)$ which was an integral part of their proof that the Lang-Trotter conjecture is true on average. In related work on the Lang-Trotter conjecture for elliptic curves with nontrivial rational torsion subgroups (see for example [2]) it was neccessary to prove similar estimates on $A(r, r-1, n, X)$ for various squarefree n. In this paper we give an estimate for $A(r,m,n,X)$ for $(m,n) = 1$ arbitrary. In order to state the main result, we will need a bit more notation. We will let $\Delta^{r,m} = r^2 - 4m$ and put

$$\begin{array}{l} \mathfrak{Q}^{<}_{r,m,n} = \{q > 2, \text{prime} : q | n; q \nmid r; \text{ord}_q(\Delta^{r,m}) < \text{ord}_q(n)\} \quad \text{and} \\ \mathfrak{Q}^{\geq}_{r,m,n} = \{q > 2, \text{prime} : q | n; q \nmid r; \text{ord}_q(\Delta^{r,m}) \geq \text{ord}_q(n)\} \end{array} \tag{3}$$

For $q \in \mathfrak{Q}^{<}_{r,m,n}$, we will denote by γ_q, the greatest integer which is less than $\text{ord}_q(\Delta^{r,m})/2$, that is $\gamma_q := \lfloor (\text{ord}_q(\Delta^{r,m}) - 1)/2 \rfloor$. Also, we will let

$$\Gamma_q = \begin{cases} \left(\frac{(\Delta^{r,m})/q^{\text{ord}_q(\Delta^{r,m})}}{q} \right) & \text{if } \text{ord}_q(\Delta^{r,m}) \text{ is even, positive and finite,} \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

In this paper we prove:

Date: August 23, 2005.

2000 *Mathematics Subject Classification.* Primary (11M06);Secondary (11G05).

Key words and phrases. Dirichlet L-series, Special values of L-series.

The author is partially supported by NSF grant DMS-0090117.

Theorem 1.1.

$$A(r,m,n,X) \sim C_{r,m,n}X,$$

where

$$C_{r,m,n} = \frac{1}{\phi(n)} C_{r,m,n}(2) \prod_{\substack{q,\ odd \\ q \nmid n \\ q \nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q,\ odd \\ q \nmid n \\ q \mid r}} \frac{q^2}{q^2-1} \prod_{\substack{q \mid n \\ q \mid r}} \left(\frac{q\left(q + \left(\frac{-m}{q}\right)\right)}{q^2-1} \right) \cdot$$

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

$$\prod_{q \in \mathfrak{Q}^{\geq}_{r,m,n}} \left(\frac{q^{\lfloor \frac{\mathrm{ord}_q(n)+1}{2} \rfloor} - 1}{q^{\lfloor \frac{\mathrm{ord}_q(n)-1}{2} \rfloor}(q-1)} + \frac{q^{\mathrm{ord}_q(n)+2}}{q^{3\lfloor \frac{\mathrm{ord}_q(n)+1}{2} \rfloor}(q^2-1)} \right)$$

and $C_{r,m,n}(2)$ *is defined by*

$$C_{r,m,n}(2) = \begin{cases} \frac{2}{3} & r \text{ is odd.} \\ \frac{4}{3} & \text{if } r \text{ is even; and } 4 \nmid n, \\ 2 - \frac{2}{3\cdot 2^{\lfloor \frac{\mathrm{ord}_2(n)}{2} \rfloor}} & \text{if } r \equiv 2 \pmod 4\text{; } 2 \leq \mathrm{ord}_2(n) \leq \mathrm{ord}_2(\Delta^{r,m}) - 2, \\ 2 - \frac{4}{3\cdot 2^{\frac{\mathrm{ord}_2(n)-1}{2}}} & \text{if } r \equiv 2 \pmod 4\text{; } \mathrm{ord}_2(n) = \mathrm{ord}_2(\Delta^{r,m}) - 1 \text{ and } 2 \mid \mathrm{ord}_2(\Delta^{r,m}), \\ 2 - \frac{2}{2^{\frac{\mathrm{ord}_2(n)}{2}}} & \text{if } r \equiv 2 \pmod 4\text{; } \mathrm{ord}_2(n) = \mathrm{ord}_2(\Delta^{r,m}) - 1 \text{ and } 2 \nmid \mathrm{ord}_2(\Delta^{r,m}), \\ 2 - \frac{2}{3\cdot 2^{\frac{\mathrm{ord}_2(n)}{2}}} & \text{if } r \equiv 2 \pmod 4\text{; } \mathrm{ord}_2(n) = \mathrm{ord}_2(\Delta^{r,m})\text{; } 2 \mid \mathrm{ord}_2(\Delta^{r,m})\text{;} \\ & \frac{\Delta^{r,m}}{2^{\mathrm{ord}_2(\Delta^{r,m})}} \equiv 1 \pmod 4, \\ 2 - \frac{2}{2^{\lfloor \frac{\mathrm{ord}_2(n)}{2} \rfloor}} & \text{if } r \equiv 2 \pmod 4\text{; } \mathrm{ord}_2(n) = \mathrm{ord}_2(\Delta^{r,m})\text{;} \\ & \left(2 \nmid \mathrm{ord}_2(\Delta^{r,m}) \textbf{ OR } \frac{\Delta^{r,m}}{2^{\mathrm{ord}_2(\Delta^{r,m})}} \equiv 3 \pmod 4 \right), \\ 2 & \text{if } r \equiv 2 \pmod 4\text{; } \mathrm{ord}_2(n) > \mathrm{ord}_2(\Delta^{r,m})\text{;} \\ & \mathrm{ord}_2(\Delta^{r,m}) \text{ is even and } \frac{\Delta^{r,m}}{2^{\mathrm{ord}_2(\Delta^{r,m})}} \equiv 1 \pmod 8, \\ 2 - \frac{4}{3\cdot 2^{\frac{\mathrm{ord}_2(\Delta^{r,m})}{2}}} & \text{if } r \equiv 2 \pmod 4\text{; } \mathrm{ord}_2(n) > \mathrm{ord}_2(\Delta^{r,m})\text{;} \\ & \mathrm{ord}_2(\Delta^{r,m}) \text{ is even and } \frac{\Delta^{r,m}}{2^{\mathrm{ord}_2(\Delta^{r,m})}} \equiv 5 \pmod 8, \\ 2 - \frac{2}{2^{\frac{\mathrm{ord}_2(\Delta^{r,m})}{2}}} & \text{if } r \equiv 2 \pmod 4\text{; } \mathrm{ord}_2(n) > \mathrm{ord}_2(\Delta^{r,m})\text{;} \\ & \left(2 \nmid \mathrm{ord}_2(\Delta^{r,m}) \textbf{ OR } \frac{\Delta^{r,m}}{2^{\mathrm{ord}_2(\Delta^{r,m})}} \equiv 3 \pmod 4 \right), \\ \frac{5}{3} & \text{if } r \equiv 0 \pmod 4\text{; } \mathrm{ord}_2(n) = 2\text{; } m \equiv 3 \pmod 4, \\ 2 & \text{if } r \equiv 0 \pmod 4\text{; } 8 \mid n\text{; } m \equiv 3 \pmod 4\text{; } \frac{\Delta^{r,m}}{4} \equiv 1 \pmod 8, \\ \frac{4}{3} & \text{if } r \equiv 0 \pmod 4\text{; } 8 \mid n\text{; } m \equiv 3 \pmod 4\text{; } \frac{\Delta^{r,m}}{4} \equiv 5 \pmod 8, \\ 1 & \text{if } r \equiv 0 \pmod 4\text{; } 4 \mid n\text{; } m \equiv 1 \pmod 4, \end{cases}$$

2. Proofs.

We first state the following result which is essentially due to David and Pappalardi, in the sense that one can obain a proof by following the same line of argument given in the proof of Theorem 3.1 in [1] with minor modifications such as carrying the condition $p \equiv m \pmod{n}$ throughout their argument.

Proposition 2.1. *Suppose that $r, m, n \in \mathbb{Z}$ and that $(m, n) = 1$. Then for any $c > 0$,*

$$A(r, m, n, X) = K_{r,m,n}X + \mathrm{O}\left(\frac{X}{\log^c X}\right),$$

where

$$K_{r,m,n} = \sum_{f=1}^{\infty} \frac{1}{f} \sum_{k=1}^{\infty} \frac{c_f^{r,m,n}(k)}{k\phi([n; kf^2])}.$$

and

$$c_f^{r,m,n}(k) := \sum_{\substack{a \pmod{4k} \\ a \equiv 0,1 \pmod 4 \\ (r^2 - af^2, 4kf^2) = 4 \\ 4m \equiv r^2 - af^2 \pmod{(4n, 4kf^2)}}} \left(\frac{a}{k}\right).$$

For the sake of brevity, we omit the proof of this result and refer the reader to [1].

The proof of the main result now requires only a reconciling of the constants $K_{r,m,n}$ and $C_{r,m,n}$. To that end we begin with an investigation of the $c_f^{r,m,n}(k)$. For convenience, we will split these into two sums:

$$c_{f,0}^{r,m,n}(k) := \sum_{\substack{a \pmod{4k} \\ a \equiv 0 \pmod 4 \\ (r^2 - af^2, 4kf^2) = 4 \\ 4m \equiv r^2 - af^2 \pmod{(4n, 4kf^2)}}} \left(\frac{a}{k}\right) \quad \text{and} \quad c_{f,1}^{r,m,n}(k) := \sum_{\substack{a \pmod{4k} \\ a \equiv 1 \pmod 4 \\ (r^2 - af^2, 4kf^2) = 4 \\ 4m \equiv r^2 - af^2 \pmod{(4n, 4kf^2)}}} \left(\frac{a}{k}\right). \tag{5}$$

In order to describe the behavior of the $c_{f,i}^{r,m,n}(k)$'s we have the following lemmas. The first lemma follows directly from the above definitions. We state it for the sake of convenience only.

Lemma 2.1.

(1) *For $c_{f,0}^{r,m,n}(k)$ to be nonzero, it is necessary that we have r, even; k, odd, $(r/2, f) = 1$ and $(n, f^2) | ((r/2)^2 - m)$.*
(2) *For $c_{f,1}^{r,m,n}(k)$ to be nonzero, one of the following must hold.*
   (a) *r and f are both odd, $(r, f) = 1$ and $(n, f^2) | (\Delta^{r,m})$.*
   (b) *$r \equiv 2 \pmod 4, (r/2, f) = 1, (4n, f^2) | (\Delta^{r,m})$.*
   - *If $\mathrm{ord}_2(n) \leq \mathrm{ord}_2(\Delta^{r,m}) - 2$, then we require that $\mathrm{ord}_2(f^2) \geq max(\mathrm{ord}_2(n) + 2, 4)$.*
   - *If $\mathrm{ord}_2(n) = \mathrm{ord}_2(\Delta^{r,m}) - 1$, then we require that $\mathrm{ord}_2(f^2) = \mathrm{ord}_2(n) + 1$.*
   - *If $\mathrm{ord}_2(n) \geq \mathrm{ord}_2(\Delta^{r,m})$, then we require that $\mathrm{ord}_2(f^2) = \mathrm{ord}_2(\Delta^{r,m})$ and $\frac{\Delta^{r,m}}{2^{\mathrm{ord}_2(\Delta^{r,m})}} \equiv 1 \pmod 4$.*

(c) $r \equiv 0 \pmod 4, f \equiv 2 \pmod 4, (r, f/2) = 1$ *and* $(n, (f/2)^2) | ((r/2)^2 - m)$. *If* $n \equiv 0 \pmod 4$, *then we also need* $m \equiv 3 \pmod 4$.

Lemma 2.2. *$c_{f,i}^{r,m,n}(k)$ (i=0,1) is a multiplicative function of k.*

Proof. If r is odd, $c_{f,0}^{r,m,n}(k) = 0$ and the multiplicativity of $c_{f,1}^{r,m,n}(k)$ can be shown as in [1], lemma 3.3. So, we will consider only the case when r is even.

In this case, if $(r/2, f) = 1$, $(n, f^2) | ((r/2)^2 - m)$ and k is odd, then we obtain

$$c_{f,0}^{r,m,n}(k) = \sum_{\substack{a \pmod k \\ ((r/2)^2 - af^2, k) = 1 \\ \frac{(r/2)^2 - m}{(n,f^2)} \equiv a \frac{f^2}{(n,f^2)} \pmod{(\frac{n}{(n,f^2)}, k)}}} \left(\frac{a}{k}\right), \tag{6}$$

and zero otherwise. Since, a runs through certain congruence classes modulo k in the above sum, the multiplicativity of $c_{f,0}^{r,m,n}(k)$ now follows form the Chinese remainder theorem and the multiplicative properties of the Legendre symbol.

We need only treat the cases in which $c_{f,1}^{r,m,n}(k)$ is possibly nonzero (see lemma 2.1). For case 2a, if k is odd, then we have

$$c_{f,1}^{r,m,n}(k) = \sum_{\substack{a \in \mathbb{Z}/k\mathbb{Z} \\ (r^2 - af^2, k) = 1 \\ \frac{\Delta_{r,m}}{(n,f^2)} \equiv a \frac{f^2}{(n,f^2)} \pmod{(\frac{n}{(n,f^2)}, k)}}} \left(\frac{a}{k}\right). \tag{7}$$

In cases 2b and 2c, when k is odd, we have

$$c_{f,1}^{r,m,n}(k) = \sum_{\substack{a \in \mathbb{Z}/k\mathbb{Z} \\ ((r/2)^2 - a(f/2)^2, k) = 1 \\ \frac{(r/2)^2 - m}{(n,(f/2)^2)} \equiv a \frac{(f/2)^2}{(n,(f/2)^2)} \pmod{(\frac{n}{(n,(f/2)^2)}, k)}}} \left(\frac{a}{k}\right). \tag{8}$$

In either of these cases, we see that the sums vary over congruence classes modulo k which is odd. The multiplicativity of $c_{f,1}^{r,m,n}$ now follows from the Chinese remainder theorem and the multiplicative properties of the Legendre symbol.

Lemma 2.3. *Given r, m and n, let $i = 0$ or 1 and define τ as follows.*

$$\tau = \begin{cases} 2 & \text{if } r \equiv 2 \pmod 4;\ i = 1 \text{ and } \operatorname{ord}_2(n) \leq \operatorname{ord}_2(\Delta^{r,m}) - 2 \\ & \text{and } \operatorname{ord}_2(n) \leq 2, \\ \lceil \frac{\operatorname{ord}_2(n)}{2} \rceil + 1 & \text{if } r \equiv 2 \pmod 4;\ i = 1 \text{ and } \operatorname{ord}_2(n) \leq \operatorname{ord}_2(\Delta^{r,m}) - 2 \\ & \text{and } \operatorname{ord}_2(n) > 2, \\ \frac{\operatorname{ord}_2(n)+1}{2} & \text{if } r \equiv 2 \pmod 4;\ i = 1;\ \operatorname{ord}_2(n) = \operatorname{ord}_2(\Delta^{r,m}) - 1; \\ & \text{and } \operatorname{ord}_2(n) \text{ is odd}, \\ \frac{\operatorname{ord}_2(\Delta^{r,m})}{2} & \text{if } r \equiv 2 \pmod 4;\ i = 1;\ \operatorname{ord}_2(n) \geq \operatorname{ord}_2(\Delta^{r,m}); \\ & \operatorname{ord}_2(\Delta^{r,m}) \text{ is even and } \frac{\Delta^{r,m}}{2^{\operatorname{ord}_2(\Delta^{r,m})}} \equiv 1 \pmod 4, \\ 1 & \text{if } r \equiv 0 \pmod 4 \text{ and } i = 1, \\ 0 & \text{if } r \text{ is odd or if } i = 0. \end{cases}$$

If f is chosen such that r, m, n and f satisfy one of the conditions in lemma 2.1 for $c_{f,i}^{r,m,n}$, and if q is an odd prime, then we have

$$c_{f,i}^{r,m,n}(q^\alpha) = c_{2^\tau q^{\operatorname{ord}_q(f)},i}^{r,m,n}(q^\alpha)$$

Also, if r, m, n and f satisfy one of conditions 2a, 2b or 2c of lemma 2.1, then

$$c_{f,1}^{r,m,n}(2^\alpha) = c_{2^{\operatorname{ord}_2(f)},1}^{r,m,n}(2^\alpha)$$

Proof. We will first treat the case when $i = 0$ and r, m, n and f satisfy condition (1) of lemma 2.1 Using (6), we have

$$c_{f,0}^{r,m,n}(q^\alpha) = \begin{cases} \sum_{\substack{a \pmod{q^\alpha} \\ ((r/2)^2 - af^2, q) = 1}} \left(\frac{a}{q}\right)^\alpha & \text{if } \operatorname{ord}_q(n) \leq \operatorname{ord}_q(f^2), \\ \sum_{\substack{a \pmod{q^\alpha} \\ \frac{(r/2)^2 - m}{q^{\operatorname{ord}_q(f^2)}} \equiv a \frac{f^2}{q^{\operatorname{ord}_q(f^2)}} \pmod{(\frac{n}{q^{\operatorname{ord}_q(f^2)}}, q^\alpha)}}} \left(\frac{a}{q}\right)^\alpha & \text{if } \operatorname{ord}_q(n) > \operatorname{ord}_q(f^2), \end{cases} \tag{9}$$

Note that $\frac{f^2}{q^{\operatorname{ord}_q(f^2)}}$ is a square which is coprime to q. Thus making the change of variable $a' = a\frac{f^2}{q^{\operatorname{ord}_q(f^2)}}$, the last sum becomes

$$\sum_{\substack{a' \pmod{q^\alpha} \\ \frac{(r/2)^2 - m}{q^{\operatorname{ord}_q(f^2)}} \equiv a' \pmod{(\frac{n}{q^{\operatorname{ord}_q(f^2)}}, q^\alpha)}}} \left(\frac{a'}{q}\right)^\alpha \tag{10}$$

Now combining this with (9), we have

$$c_{f,0}^{r,m,n}(q^\alpha) = \begin{cases} \sum_{\substack{a \pmod{q^\alpha} \\ ((r/2)^2 - af^2, q) = 1}} \left(\frac{a}{q}\right)^\alpha & \text{if } \operatorname{ord}_q(n) \leq \operatorname{ord}_q(f^2), \\ \sum_{\substack{a \pmod{q^\alpha} \\ \frac{(r/2)^2 - m}{q^{\operatorname{ord}_q(f^2)}} \equiv a \pmod{(\frac{n}{q^{\operatorname{ord}_q(f^2)}}, q^\alpha)}}} \left(\frac{a}{q}\right)^\alpha & \text{if } \operatorname{ord}_q(n) > \operatorname{ord}_q(f^2). \end{cases} \tag{11}$$

Using this expression one can easily see that $c_{f,0}^{r,m,n}(q^\alpha) = c_{q^{\mathrm{ord}_q(f)},0}^{r,m,n}(q^\alpha)$, and thus we have proved that the lemma holds in this case.

In all other cases when q is an odd prime, the proof is similar.

For the last assertion, we assume that r, m, n and f satisfy either of conditions 2b or 2c of lemma 2.1. From 5, we have

$$(12)\quad \begin{aligned} c_{f,1}^{r,m,n}(2^\alpha) &= \sum_{\substack{a \pmod{2^{\alpha+2}} \\ a\equiv 1 \pmod 4 \\ \frac{(r/2)^2-m}{(n,(f/2)^2)} \equiv a\frac{(f/2)^2}{(n,(f/2)^2)} \pmod{(\frac{n}{(n,(f/2)^2)},2^{\alpha+2})}}} \left(\frac{a}{2}\right)^\alpha \\ &= \begin{cases} \sum_{\substack{a \pmod{2^{\alpha+2}} \\ a\equiv 1 \pmod 4}} \left(\frac{a}{2}\right)^\alpha & \text{if } \mathrm{ord}_2(n) \le \mathrm{ord}_2(f^2), \\ \sum_{\substack{a \pmod{2^{\alpha+2}} \\ \frac{(r/2)^2-m}{2^{\mathrm{ord}_2(f^2)-2}} \equiv a\frac{f^2}{2^{\mathrm{ord}_2(f^2)}} \pmod{(\frac{n}{(n,(f/2)^2)},2^{\alpha+2})}}} \left(\frac{a}{2}\right)^\alpha & \text{if } \mathrm{ord}_2(n) \ge \mathrm{ord}_2(f^2)+1. \end{cases} \end{aligned}$$

We note that $\frac{f^2}{2^{\mathrm{ord}_2(f^2)}}$ is an odd square. Thus, letting $a' = a\frac{f^2}{2^{\mathrm{ord}_2(f^2)}}$ yeilds

$$(13)\quad c_{f,1}^{r,m,n}(2^\alpha) = \begin{cases} \sum_{\substack{a \pmod{2^{\alpha+2}} \\ a\equiv 1 \pmod 4}} \left(\frac{a}{2}\right)^\alpha & \text{if } \mathrm{ord}_2(n) \le \mathrm{ord}_2(f^2), \\ \sum_{\substack{a' \pmod{2^{\alpha+2}} \\ \frac{(r/2)^2-m}{2^{\mathrm{ord}_2(f^2)-2}} \equiv a' \pmod{(\frac{n}{(n,(f/2)^2)},2^{\alpha+2})}}} \left(\frac{a'}{2}\right)^\alpha & \text{if } \mathrm{ord}_2(n) \ge \mathrm{ord}_2(f^2)+1. \end{cases}$$

Using the last expression, one can easily check that $c_{f,1}^{r,m,n}(2^\alpha) = c_{2^{\mathrm{ord}_2(f)},1}^{r,m,n}(2^\alpha)$, as desired. In the case that r, m, n and f satisfy condition 2a of lemma 2.1, the proof is similar.

In order to evaluate the $c_{q^\beta,i}^{r,m,n}(q^\alpha)$, $(i = 0, 1)$, we have the following two lemmas.

Lemma 2.4. *Suppose that q is an odd prime and $\alpha > 0$. Letting $d = c_{q^\beta,0}^{r,m,n}(q^\alpha)$ when r is even; $(r, q) = 1$ and $(n, q^{2\beta})|((r/2)^2 - m)$, or letting $d = c_{2^\tau q^\beta,1}^{r,m,n}(q^\alpha)$ when r, m and n satisfy conditions 2a, 2b or 2c of lemma 2.1, we have*

$$(14)\quad d = \begin{cases} -\left(\frac{r^2}{q}\right) q^{\alpha-1} & \text{if } \beta = 0; \alpha, \text{ odd}; q \nmid n. \\ (q-1-\left(\frac{r^2}{q}\right))q^{\alpha-1} & \text{if } \beta = 0; \alpha, \text{ even}; q \nmid n. \\ \frac{q^\alpha}{(n,q^\alpha)}\left(\frac{\Delta^{r,m}}{q}\right)^\alpha & \text{if } \beta = 0 \text{ and } q \mid n. \\ 0 & \text{if } \beta > 0; \alpha, \text{ odd and } \mathrm{ord}_q(n) \le 2\beta. \\ q^{\alpha-1}(q-1) & \text{if } \beta > 0; \alpha, \text{ even and } \mathrm{ord}_q(n) \le 2\beta. \\ \frac{q^\alpha}{(\frac{n}{q^{2\beta}},q^\alpha)}\left(\frac{(\Delta^{r,m})/q^{2\beta}}{q}\right)^\alpha & \text{if } \beta > 0 \text{ and } \mathrm{ord}_q(n) > 2\beta. \end{cases}$$

Proof. We will prove the lemma for $c_{4q^\beta,1}^{r,m,n}(q^\alpha)$ where q is an odd prime and where r, m and n satisfy condition 2b of lemma 2.1. The proofs for the other cases are similar. From (8) above, we have

$$c_{4q^\beta,1}^{r,m,n}(q^\alpha) = \sum_{\substack{a\in\mathbb{Z}/q^\alpha Z \\ ((r/2)^2-4aq^{2\beta},q)=1 \\ \frac{(r/2)^2-m}{(n,q^{2\beta})}\equiv a\frac{4q^{2\beta}}{(n,q^{2\beta})} \pmod{(\frac{n}{(n,q^{2\beta})},q^\alpha)}}} \left(\frac{a}{q}\right)^\alpha \tag{15}$$

$$= \begin{cases} \sum\limits_{\substack{a\in\mathbb{Z}/q^\alpha Z \\ ((r/2)^2-4a,q)=1 \\ (r/2)^2-m\equiv 4a \pmod{(n,q^\alpha)}}} \left(\frac{a}{q}\right)^\alpha & \text{if } \beta=0, \\ \sum\limits_{\substack{a\in\mathbb{Z}/q^\alpha Z \\ \frac{(r/2)^2-m}{(n,q^{2\beta})}\equiv a\frac{4q^{2\beta}}{(n,q^{2\beta})} \pmod{(\frac{n}{(n,q^{2\beta})},q^\alpha)}}} \left(\frac{a}{q}\right)^\alpha & \text{if } \beta>0. \end{cases}$$

Observe, that when and $q\nmid n$, the second condition of our summation for the case $\beta=0$ is empty. We also note that when $q|n$, we have $q\nmid m$, since $(m,n)=1$. So, the second condition of the summation for the case $\beta=0$ implies the first. With these observations, one can now easily deduce the desired result.

The next lemma allows us to evaluate the $c_{f,1}^{r,m,n}$ at powers of 2. The proof is similar to that of the previous lemma and for the sake of brevity we omit it.

Lemma 2.5. (1) *If r is odd, then,*

$$c_{1,1}^{r,m,n}(2^\alpha) = \begin{cases} \frac{(-2)^\alpha}{2} & \text{if } 4\nmid n, \\ \frac{(-2)^\alpha}{(n,2^\alpha)} & \text{if } 4\mid n, \end{cases}$$

(2) *If r is even and $r, f=2^\beta, m$ and n satisfy either of conditions (2b) or (2c) of lemma 2.1, then*

$$c_{2^\beta,1}^{r,m,n}(2^\alpha) = \begin{cases} 0 & \text{if } \operatorname{ord}_2(n)\le 2\beta \text{ and } \alpha \text{ is odd,} \\ 2^\alpha & \text{if } \operatorname{ord}_2(n)\le 2\beta \text{ and } \alpha \text{ is even,} \\ \left(\frac{((r/2)^2-m)/2^{2\beta-2}}{2}\right)^\alpha \frac{2^\alpha}{\left(2^{\operatorname{ord}_2(n)-2\beta},2^\alpha\right)} & \text{if } \operatorname{ord}_2(n)\ge 2\beta+1. \end{cases}$$

Now, let $\kappa(n)$ denote the multiplicative function generated by

$$\kappa(\ell^\alpha) = \begin{cases} \ell & \text{if } \alpha \text{ is odd,} \\ 1 & \text{if } \alpha \text{ is even,} \end{cases} \tag{16}$$

for any prime ℓ and any $\alpha>0$. Then we have the following bound.

Lemma 2.6. *For all k, $c_{f,i}^{r,m,n}(k)\le k/\kappa(k)$, where $i=0,1$.*

Proof. From lemmas 2.3, 2.4 and 2.5, it follows immideately that for any prime q,

$$c_{f,i}^{r,m,n}(q^\alpha) \le \begin{cases} q^\alpha & \text{if } \alpha \text{ is even,} \\ q^{\alpha-1} & \text{if } \alpha \text{ is odd.} \end{cases} \tag{17}$$

$$= q^\alpha/\kappa(q^\alpha).$$

The lemma now follows from the multiplicativity of $c_{f,i}^{r,m,n}$ and κ.

We recall the following fact from ([1] Lemma 3.4).

Lemma 2.7. *Let* $c = \prod_{\ell, prime}\left(1 + \frac{1}{\ell(\sqrt{\ell}-1)}\right)$*. Then,* $\sum_{k\geq U} \frac{1}{\kappa(k)\phi(k)} \sim \frac{c}{\sqrt{U}}$*. In particular,* $\sum_{k=1}^{\infty} \frac{1}{\kappa(k)\phi(k)}$ *converges.*

Thus from lemmas 2.6 and 2.7, we see that $K_{r,m,n}$ is a finite constant.

We rewrite $K_{r,m,n}$ as

$$K_{r,m,n} = K_{r,m,n}^0 + K_{r,m,n}^1, \tag{18}$$

where

$$K_{r,m,n}^0 = \sum_{f=1}^{\infty} \frac{1}{f} \sum_{k=1}^{\infty} \frac{c_{f,0}^{r,m,n}(k)}{k\phi([n,kf^2])} \quad \text{and} \quad K_{r,m,n}^1 = \sum_{f=1}^{\infty} \frac{1}{f} \sum_{k=1}^{\infty} \frac{c_{f,1}^{r,m,n}(k)}{k\phi([n,kf^2])} \tag{19}$$

Now we compute the constants $K_{r,m,n}^i$ $(i = 0, 1)$. We recall the following identities

$$\phi(AB) = \phi(A)\phi(B)\frac{(A,B)}{\phi((A,B))}, \tag{20}$$

and therefore, we also have if $B|A$,

$$\phi(\frac{A}{B}) = \frac{\phi(A)\phi((\frac{A}{B},B))}{\phi(B)(\frac{A}{B},B)}. \tag{21}$$

In particular, we can write

$$\phi([n,kf^2]) = \frac{\phi(nkf^2)}{(n,kf^2)}. \tag{22}$$

Now, we recall for a fixed choice of r, m and n, that f must be chosen such that r, m, n and f satisfy the conditions of lemma 2.1 for $c_{f,i}^{r,m,n}(k)$ to be non-zero. We will denote by $S_i^{r,m,n}$ the set of f's which satisfy the conditions of lemma 2.1, and we let τ be defined as in lemma 2.3. Then, we can write

$$K_{r,m,n}^i = \frac{1}{2^\tau} \sum_{\substack{f=1 \\ 2^\tau f \in S_i^{r,m,n}}}^{\infty} \frac{1}{f\phi(2^{2\tau}nf^2)} \sum_{k=1}^{\infty} \frac{c_{2^\tau f,i}^{r,m,n}(k)(n, 2^{2\tau}kf^2)\phi((2^{2\tau}nf^2, k))}{k\phi(k)(2^{2\tau}nf^2, k)}. \tag{23}$$

Using lemma 2.2 and the multiplicativity of ϕ and letting $(a,b)_q := q^{\mathrm{ord}_q((a,b))}$, we can rewrite the inner sum above as,

$$\prod_{q,\text{ prime}} \left(\sum_{j\geq 0} \frac{c_{2^\tau f,i}^{r,m,n}(q^j)(n, 2^{2\tau}f^2q^j)_q\phi((2^{2\tau}f^2n, q^j))}{q^j\phi(q^j)(2^{2\tau}f^2n, q^j)} \right). \tag{24}$$

Using lemma 2.3, (24) can be rewritten as

$$\prod_{q\nmid f}\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau,i}(q^j)(n,2^{2\tau}q^j)_q\phi((2^{2\tau}n,q^j))}{q^j\phi(q^j)(2^{2\tau}n,q^j)}\right)\cdot\prod_{q\mid f}\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau q^{\mathrm{ord}_q(f)},i}(q^j)(n,2^{2\tau}f^2q^j)_q\phi((2^{2\tau}f^2n,q^j))}{q^j\phi(q^j)(2^{2\tau}f^2n,q^j)}\right)$$
$$=\prod_{q,\text{ prime}}\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau,i}(q^j)(n,2^{2\tau}q^j)_q\phi((2^{2\tau}n,q^j))}{q^j\phi(q^j)(2^{2\tau}n,q^j)}\right)\cdot\prod_{q\mid f}\frac{\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau q^{\mathrm{ord}_q(f)},i}(q^j)(n,2^{2\tau}f^2q^j)_q\phi((2^{2\tau}f^2n,q^j))}{q^j\phi(q^j)(2^{2\tau}f^2n,q^j)}\right)}{\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau,i}(q^j)(n,2^{2\tau}q^j)_q\phi((2^{2\tau}n,q^j))}{q^j\phi(q^j)(2^{2\tau}n,q^j)}\right)}. \tag{25}$$

Now, substituting this last expression back into (23) and using (20), we obtain the following expression for $K^i_{r,m,n}$.

$$\frac{1}{2^\tau\phi(2^{2\tau}n)}\prod_{q,\text{ prime}}\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau,i}(q^j)(n,2^{2\tau}q^j)_q\phi((2^{2\tau}n,q^j))}{q^j\phi(q^j)(2^{2\tau}n,q^j)}\right)$$
$$\cdot\sum_{\substack{f=1\\ 2^\tau f\in S^{r,m,n}_i}}^{\infty}\left(\frac{\phi((2^{2\tau}n,f^2))}{f\phi(f^2)(2^{2\tau}n,f^2)}\right)\cdot\prod_{q\mid f}\frac{\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau q^{\mathrm{ord}_q(f)},i}(q^j)(n,2^{2\tau}f^2q^j)_q\phi((2^{2\tau}f^2n,q^j))}{q^j\phi(q^j)(2^{2\tau}f^2n,q^j)}\right)}{\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau,i}(q^j)(n,2^{2\tau}q^j)_q\phi((2^{2\tau}n,q^j))}{q^j\phi(q^j)(2^{2\tau}n,q^j)}\right)}. \tag{26}$$

Now, if $S^{r,m,n}_i=\emptyset$, then the above expression is just 0. So, we will assume for now that $S^{r,m,n}_i\neq\emptyset$, and in this case we can rewrite the sum from (26) as a product

$$\prod_{q,\text{ prime}}\left(1+\sum_{\substack{\beta=1\\ 2^\tau q^\beta\in S^{r,m,n}_i}}^{\infty}\frac{\frac{\phi((2^{2\tau}n,q^{2\beta}))}{q^\beta\phi(q^{2\beta})(2^{2\tau}n,q^{2\beta})}\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau q^\beta,i}(q^j)(n,2^{2\tau}q^{2\beta+j})_q\phi((2^{2\tau}q^{2\beta}n,q^j))}{q^j\phi(q^j)(2^{2\tau}q^{2\beta}n,q^j)}\right)}{\left(\sum_{j\geq 0}\frac{c^{r,m,n}_{2^\tau,i}(q^j)(n,2^{2\tau}q^j)_q\phi((2^{2\tau}n,q^j))}{q^j\phi(q^j)(2^{2\tau}n,q^j)}\right)}\right). \tag{27}$$

This allows us to rewrite (26) as

(28)

$$\frac{1}{2^\tau\phi(2^{2\tau}n)}\prod_{\substack{q,\text{ odd}\\ q\nmid n}}\left(\sum_{j\ge 0}\frac{c^{r,m,n}_{2^\tau,i}(q^j)}{q^j\phi(q^j)} + \sum_{\substack{\beta=1\\ 2^\tau q^\beta\in S_i^{r,m,n}}}^{\infty}\frac{1}{q^\beta\phi(q^{2\beta})}\sum_{j\ge 0}\frac{c^{r,m,n}_{2^\tau q^\beta,i}(q^j)\phi((q^{2\beta},q^j))}{q^j\phi(q^j)(q^{2\beta},q^j)}\right)$$

$$\cdot\prod_{\substack{q,\text{ odd}\\ q\mid n}}\left(1+\sum_{j\ge 1}\frac{c^{r,m,n}_{2^\tau,i}(q^j)(n,q^j)(q-1)}{q^{j+1}\phi(q^j)} + \sum_{\substack{\beta=1\\ 2^\tau q^\beta\in S_i^{r,m,n}}}^{\infty}\frac{q-1}{q^{\beta+1}\phi(q^{2\beta})}\sum_{j\ge 0}\frac{c^{r,m,n}_{2^\tau q^\beta,i}(q^j)(n,q^{2\beta+j})\phi((q^{2\beta}n,q^j))}{q^j\phi(q^j)(q^{2\beta}n,q^j)}\right)$$

$$\cdot\left((n,2^{2\tau})+\sum_{j\ge 1}\frac{c^{r,m,n}_{2^\tau,i}(2^j)(n,2^{2\tau+j})\phi((2^{2\tau}n,2^j))}{2^j\phi(2^j)(2^{2\tau}n,2^j)} + \sum_{\substack{\beta=1\\ 2^{\tau+\beta}\in S_i^{r,m,n}}}^{\infty}\frac{\phi((2^\tau n,2^{2\beta}))}{2^\beta\phi(2^{2\beta})(2^\tau n,2^{2\beta})}\sum_{j\ge 0}\frac{c^{r,m,n}_{2^{\tau+\beta},i}(2^j)(n,2^{2\tau+2\beta+j})\phi((2^{2\tau+2\beta}n,2^j))}{2^j\phi(2^j)(2^{2\tau+2\beta}n,2^j)}\right).$$

Since, in the first product, $q\nmid n$, and since we are assuming that $S_i^{r,m,n}\neq\emptyset$, $2^\tau q^\beta\in S_i^{r,m,n}$ for all $\beta\ge 1$ if and only if $q\nmid r$. So using lemma 2.4, the first product in (28) becomes

$$\prod_{\substack{q,\text{ odd}\\ q\nmid n\\ q\nmid r}}\frac{q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{q,\text{ odd}\\ q\nmid n\\ q\mid r}}\frac{q^2}{q^2-1}. \tag{29}$$

Recalling (3) and (4), and using lemma 2.4 the second product of (28) becomes

$$\prod_{q\in\mathfrak{Q}^{<}_{r,m,n}}\left(1+\frac{q\left(\frac{\Delta^{r,m}}{q}\right)+\left(\frac{\Delta^{r,m}}{q}\right)^2+\frac{1}{q^{\mathrm{ord}_q(\Delta^{r,m})/2}}\left(q\Gamma_q+q^2\Gamma_q^2\right)}{q^2-1}+\frac{\Gamma_q^2(q^{\lfloor\frac{\mathrm{ord}_q(\Delta^{r,m})-1}{2}\rfloor}-1)}{q^{\lfloor\frac{\mathrm{ord}_q(\Delta^{r,m})-1}{2}\rfloor}(q-1)}\right)$$
$$\cdot\prod_{q\in\mathfrak{Q}^{\ge}_{r,m,n}}\left(\frac{q^{\lfloor\frac{\mathrm{ord}_q(n)+1}{2}\rfloor}-1}{q^{\lfloor\frac{\mathrm{ord}_q(n)-1}{2}\rfloor}(q-1)}+\frac{q^{\mathrm{ord}_q(n)+2}}{q^{3\lfloor\frac{\mathrm{ord}_q(n)+1}{2}\rfloor}(q^2-1)}\right)\cdot\prod_{\substack{q\mid n\\ q\mid r\\ q,\text{odd}}}\left(\frac{q\left(q+\left(\frac{-m}{q}\right)\right)}{q^2-1}\right) \tag{30}$$

Next, we evaluate the third factor of (28),which we will denote by $T_i^{r,m,n}$. Using lemmas 2.1 and 2.5, we find that

(31)

$$T_i^{r,m,n} = \begin{cases} \frac{\cdot 2^{\operatorname{ord}_2(n)+5}}{21} & \text{if } i=1;\ r\equiv 2 \pmod 4;\ \operatorname{ord}_2(n) \le \operatorname{ord}_2(\Delta^{r,m})-2, \\ \frac{2^{\operatorname{ord}_2(n)+2}}{3} & \text{if } i=1;\ r\equiv 2 \pmod 4;\ \operatorname{ord}_2(n) = \operatorname{ord}_2(\Delta^{r,m})-1, \\ \frac{2^{\operatorname{ord}_2(n)+2}}{3} & \text{if } i=1;\ r\equiv 2 \pmod 4;\ \operatorname{ord}_2(n) = \operatorname{ord}_2(\Delta^{r,m}); \\ & \operatorname{ord}_2(\Delta^{r,m}) \text{ is even and } \frac{\Delta^{r,m}}{2^{\Delta^{r,m}}} \equiv 1 \pmod 4, \\ 2^{\operatorname{ord}_2(\Delta^{r,m})+1} & \text{if } i=1;\ r\equiv 2 \pmod 4;\ \operatorname{ord}_2(n) > \operatorname{ord}_2(\Delta^{r,m}); \\ & \operatorname{ord}_2(\Delta^{r,m}) \text{ is even and } \frac{\Delta^{r,m}}{2^{\Delta^{r,m}}} \equiv 1 \pmod 8, \\ \frac{2^{\operatorname{ord}_2(\Delta^{r,m})+1}}{3} & \text{if } i=1;\ r\equiv 2 \pmod 4;\ \operatorname{ord}_2(n) > \operatorname{ord}_2(\Delta^{r,m}); \\ & \operatorname{ord}_2(\Delta^{r,m}) \text{ is even and } \frac{\Delta^{r,m}}{2^{\Delta^{r,m}}} \equiv 5 \pmod 8, \\ \frac{2^{\operatorname{ord}_2(n)+2}}{3} & \text{if } i=1;\ r\equiv 0 \pmod 4;\ 4\nmid n, \\ \frac{16}{3} & \text{if } i=1;\ r\equiv 0 \pmod 4;\ \operatorname{ord}_2(n)=2 \text{ and } m\equiv 3 \pmod 4, \\ 8 & \text{if } i=1;\ r\equiv 0 \pmod 4;\ 8\mid n;\ m\equiv 3 \pmod 4;\ \frac{\Delta^{r,m}}{4}\equiv 1 \pmod 8, \\ \frac{8}{3} & \text{if } i=1;\ r\equiv 0 \pmod 4;\ 8\mid n;\ m\equiv 3 \pmod 4;\ \frac{\Delta^{r,m}}{4}\equiv 5 \pmod 8, \\ \frac{2}{3} & \text{if } i=1 \text{ and } r \text{ is odd}, \\ \frac{9}{7} & \text{if } i=0;\ r\equiv 2 \pmod 4 \text{ and } n \text{ is odd}, \\ 2-\frac{6}{7\cdot 2^{\frac{\operatorname{ord}_2(n)}{2}}} & \text{if } i=0;\ r\equiv 2 \pmod 4;\ 0<\operatorname{ord}_2(n) \le \operatorname{ord}_2(\Delta^{r,m})-2;\ \operatorname{ord}_2(n) \text{ is even}, \\ 2-\frac{5}{7\cdot 2^{\frac{\operatorname{ord}_2(n)-1}{2}}} & \text{if } i=0;\ r\equiv 2 \pmod 4;\ \operatorname{ord}_2(n) \le \operatorname{ord}_2(\Delta^{r,m})-2;\ \operatorname{ord}_2(n) \text{ is odd}, \\ 2-\frac{1}{2^{\lfloor\frac{\operatorname{ord}_2(\Delta^{r,m})}{2}\rfloor-1}} & \text{if } i=0;\ r\equiv 2 \pmod 4;\ \operatorname{ord}_2(n) > \operatorname{ord}_2(\Delta^{r,m})-2, \\ 1 & \text{if } i=0 \text{ and } r\equiv 0 \pmod 4. \end{cases}$$

Thus,

(32)

$$K_{r,m,n} = \left(\frac{T_0^{r,m,n}}{\phi(n)} + \frac{T_1^{r,m,n}}{2^{\tau}\phi(2^{2\tau}n)}\right) \prod_{\substack{q,\text{ odd}\\ q\nmid n\\ q\nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q,\text{ odd}\\ q\nmid n\\ q\mid r}} \frac{q^2}{q^2-1} \prod_{\substack{q\mid n\\ q\mid r}} \left(\frac{q\left(q+\left(\frac{-m}{q}\right)\right)}{q^2-1}\right)$$

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

$$\cdot \prod_{q\in\mathfrak{Q}^{\ge}_{r,m,n}} \left(\frac{q^{\lfloor\frac{\operatorname{ord}_q(n)+1}{2}\rfloor}-1}{q^{\lfloor\frac{\operatorname{ord}_q(n)-1}{2}\rfloor}(q-1)} + \frac{q^{\operatorname{ord}_q(n)+2}}{q^{3\lfloor\frac{\operatorname{ord}_q(n)+1}{2}\rfloor}(q^2-1)}\right)$$

Now one can check that $C_{r,m,n}(2) = \phi(n) \cdot (\frac{T_0^{r,m,n}}{\phi(n)} + \frac{T_1^{r,m,n}}{2^\tau \phi(2^{2\tau} n)})$ when $S_0^{r,m,n} \cup S_1^{r,m,n} \neq \emptyset$ and 0 otherwise. Thus Theorem 1.1 now follows from Proposition 2.1 and from (32).

References

[1] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves. Internat. Math. Res. Notices (1999) 165–183.
[2] K. James, “ Average Frobenius distributions for elliptic curves with 3-torsion”, (preprint).

Department of Mathematical Sciences
Clemson University
BOX 340975
Clemson, SC 29634-0975, USA
kevja@clemson.edu

Department of Mathematical Sciences, Clemson University, BOX 340975 Clemson, SC 29634-0975, USA
E-mail address: `kevja@clemson.edu`
URL: `http://www.math.clemson.edu/ kevja/`