AVERAGE FROBENIUS DISTRIBUTIONS FOR ELLIPTIC CURVES WITH 3-TORSION.

KEVIN JAMES

This paper is dedicated to the memory of George J. Fix

ABSTRACT. In this paper, we examine the Lang-Trotter conjecture for elliptic curves which possess rational 3-torsion points. We prove that if one averages over all such elliptic curves then one obtains an asymptotic similar to the one predicted by Lang and Trotter.

1. INTRODUCTION

Let $E/\mathbb{Q}$ denote an elliptic curve and let Δ_E denote its discriminant. As usual, let $a_p(E) = p+1-\#E(\mathbb{F}_p)$. It has been conjectured by Lang and Trotter [8] that for any elliptic curve E and any $r \in \mathbb{Z}$ ($r \neq 0$ if E has complex multiplication),

$$\pi_E^r(X) := \#\{p \leq X : a_p(E) = r\} \sim C_{E,r}\frac{\sqrt{X}}{\log X}, \tag{1}$$

where $C_{E,r}$ is an explicit constant depending only on E and r. More precisely, let $\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ denote the Galois representation on the full torsion subgroup of $E(\overline{\mathbb{Q}})$ where $\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$. Let $\tilde{\rho}_{E,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ denote its reduction modulo m which yields the usual Galois representation on the m-torsion points of $E(\overline{\mathbb{Q}})$ Then there is an integer m_E guaranteed by [12] such that for all $p \not| m_E$, $\tilde{\rho}_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and such that $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the full inverse image through the reduction modulo m_E map of $\tilde{\rho}_{E,m_E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. (see section 2 of [2], for a more detailed explanation). Lang and Trotter define

$$C_{E,r} := \frac{2}{\pi}\cdot\frac{m_E\cdot\#\left(\tilde{\rho}_{E,m_E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))_r\right)}{\#\left(\tilde{\rho}_{E,m_E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))\right)}\prod_{\substack{q\not| m_E\\ q\not| r}}\frac{q(q^2-q-1)}{(q+1)(q-1)^2}\prod_{\substack{q\not| m_E\\ q| r}}\frac{q^2}{q^2-1}, \tag{2}$$

where for G any subgroup of $\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$, G_r denotes the subset of elements of trace r. Note that the ratios of polynomials in q in the previous expression are

$$\frac{q|(\mathrm{GL}_2(\mathbb{F}_q))_r|}{|\mathrm{GL}_2(\mathbb{F}_q)|}. \tag{3}$$

Date: June 12, 2005.

2000 *Mathematics Subject Classification.* Primary (11G05);Secondary (11F30, 11F80).

Key words and phrases. elliptic curves, Lang-Trotter conjecture, average Frobenius distributions.

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

In [4] and [2], this conjecture is proved to hold in an average sense, if one averages over all elliptic curves. As in [8], let

$$\pi_{1/2} = \int_2^X \frac{\mathrm{d}t}{2\sqrt{t}\log t} \sim \frac{\sqrt{X}}{\log X}.$$

Then from [2], we have the following result

Theorem 1.1. *Let $E(a,b) : y^2 = x^3 + ax + b$ and let $\epsilon > 0$. If $A, B > X^{1+\epsilon}$, then we have as $X \to \infty$,*

$$\frac{1}{4AB} \sum_{\substack{|a|\leq A \\ |b|\leq B}} \pi^r_{E(a,b)}(X) \sim D_r \pi_{1/2}(X),$$

where

$$D_r := \frac{2}{\pi} \prod_{q \not| r} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{q|r} \frac{q^2}{q^2-1},$$

In fact, David and Pappalardi [2] prove the following stronger result.

Theorem 1.2. *Let $\epsilon > 0$ and fix $c > 0$. If $A, B > X^{2+\epsilon}$, then for all $d > 2c$ and for all elliptic curves $E(a,b)$ with $|a| \leq A$ and $|b| \leq B$, with at most $\mathrm{O}(AB/\log^d X)$ exceptions, we have the inequality*

$$|\pi^r_{E(a,b)} - D_r \pi_{1/2}(X)| \ll \frac{\sqrt{X}}{\log^c X}.$$

One immediately notices the similarities between $C_{E,r}$ and D_r. From Theorem 1.1 we see when one averages over all elliptic curves that the the constant obtained is similar to the conjectured constant $C_{E,r}$. In fact if we set $m_E = 1$ in (2) then we obtain D_r. One should note, however, that m_E is never 1 (see [12]). However, Duke [3] has shown that for almost all elliptic curves $\tilde{\rho}_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for all primes p. It is still not known if the constants obtained in [2, 4] are consistent with the ones conjectured by Lang and Trotter, that is we don't know if the average of the $C_{E,r}$'s above is D_r.

Since the set of elliptic curves having nontrivial rational torsion subgroups has density zero in the set of all elliptic curves, the results mentioned above ignore curves with nontrivial rational torsion subgroups. From (2), we see that the presence of nontrivial rational torsion points has a substantial effect on the constant $C_{E,r}$ conjectured by Lang and Trotter. In particular, if E has a rational point of order m, then $m|m_E$ and $\tilde{\rho}_{E,m}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus, it seems quite natural to investigate the behavior of $\pi^r_E(X)$ for elliptic curves with nontrivial rational torsion points.

The families of elliptic curves defined over $\mathbb{Q}$ with prescribed torsion subgroups have been parameterized by Kubert [7]. The family of elliptic curves containing a rational point of order 3 is given by

$$E_{(a_1,a_3)} : y^2 + a_1xy + a_3y = x^3, \tag{4}$$

which has discriminant

$$\Delta(E_{(a_1,a_3)}) = a_3^3(a_1^3 - 27a_3). \tag{5}$$

Also, for any prime p one can follow the argument given in [[6], pp. 145–146] to see that any elliptic curve over $\mathbb{F}_p$ with an $\mathbb{F}_p$-point of order 3 can be written in the form (4). Thus, the reductions of the curves in (4) modulo a prime p cover all 3-torsion elliptic curves over $\mathbb{F}_p$. We shall make use of this fact in section 2.

For the family of curves (4), we see that $3|m_{E_{(a_1,a_3)}}$ for all a_1 and a_3 and in fact for the obvious choice of generators for $E[3]$, we have that

$$G := \rho_{E_{a_1,a_3},3}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \subseteq \left\{ \begin{array}{cc} 1 & b \\ 0 & d \end{array} : b \in \mathbb{F}_3; d \in \mathbb{F}_3^* \right\}.$$

Thus one expects that when one averages over curves with rational 3-torsion, the contribution to the constant from the prime 3 is

$$C_r(3) = \frac{3|G_r|}{|G|} = \begin{cases} 0 & \text{when } r \equiv 1 \pmod 3, \\ 3/2 & \text{otherwise.} \end{cases}$$

That is to say, one might expect that C_r should be $\frac{2}{\pi} \cdot 3/2 \cdot \prod_{\substack{q \neq 3 \\ q \nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q \neq 3 \\ q | r}} \frac{q^2}{q^2-1}$.

In this paper we prove the following.

Theorem 1.3. *Let $E_{(a_1,a_3)}$ be the parameterization of elliptic curves which have a rational point of order 3 and let $r \equiv 0, 1 \pmod 3$. Then for every $c > 0$,*

$$\frac{1}{\mu(N)} \sum_{|a_1|,|a_3| \leq N}{}' \pi^r_{E_{a_1,a_3}}(X) = C_r \pi_{1/2}(X) + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{X^{5/2}}{N^2} + \frac{\sqrt{X}}{\log^c X} \right).$$

with

$$C_r = \frac{2}{\pi} \cdot C_r(3) \cdot \prod_{\substack{q \neq 3 \\ q \nmid r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q \neq 3 \\ q | r}} \frac{q^2}{q^2-1}, \tag{6}$$

where

$$C_r(3) := \begin{cases} 3/2 & \text{if } r \equiv 0 \pmod 3, \\ 0 & \text{it } r \equiv 1 \pmod 3. \end{cases}$$

and $\mu(N)$ denotes the number of $(|a_1|, |a_3|) \leq N$ such that $E_{(a_1,a_3)}$ is nonsingular and $\sum'$ denotes the sum over such curves.

An immediate corollary of this result is

Corollary 1.1. *Let $\epsilon > 0$. If $N > X^{1+\epsilon}$, then for $r \equiv 0, 1 \pmod 3$ we have*

$$\frac{1}{\mu(N)} \sum_{|a_1|,|a_3| \leq N}{}' \pi^r_{E_{a_1,a_3}}(X) \sim C_r \frac{\sqrt{X}}{\log X}$$

Actually we are able to obtain the following stronger result. Since the proof is identical to the proof of Theorem 1.4 in [2], we omit the proof and refer the reader to [2] for details.

Theorem 1.4. *Let $\epsilon > 0$. If $N > X^{1+\epsilon}$ and $r \equiv 0, 1 \pmod 3$, then for every $c > 0$,*

$$\frac{1}{\mu(N)} \sum_{|a_1|,|a_3| \leq N} |\pi^r_{E_{(a_1,a_3)}}(X) - C_r \pi_{1/2}(X)|^2 = \mathrm{O}\left(\frac{X}{\log^c(X)} + \frac{X^3}{N} + \frac{X^5}{N^2} \right).$$

This yields the following immediate corollary.

Corollary 1.2. *Let $\epsilon > 0$ and fix $c > 0$. If $N > X^{2+\epsilon}$ and $r \equiv 0, 1 \pmod 3$, then for all $d > 2c$ and for all elliptic curves $E_{(a_1,a_3)}$ with $|a_1|, |a_3| \leq N$ with at most $\mathrm{O}(N^2/\log^d X)$ exceptions, we have the inequality*

$$|\pi^r_{E_{(a_1,a_3)}} - C_r \pi_{1/2}(X)| \ll \frac{\sqrt{X}}{\log^c X}.$$

We should also note that the contribution of complex multiplication curves to

$$\frac{1}{\mu(N)} \sum_{|a_1|,|a_3| \leq N}{}' \pi^r_{E_{a_1,a_3}}(X) \tag{7}$$

is dominated by the error term. To see this, we note that the j-invariant of $E_{(a_1,a_3)}$ is given by

$$j(E_{(a_1,a_3)}) = \frac{(a_1^3 - 24a_3)^3}{a_3^3 - 27a_1} \tag{8}$$

and recall that there are only 13 j-invariants of curves which have complex multiplication. For any $J \in \mathbb{C}$, we have the estimate

$$\frac{1}{\mu(N)} \sum_{\substack{|a_1|,|a_3| \leq N \\ j(E_{(a_1,a_3)})=J}}{}' \pi^r_{E_{a_1,a_3}}(X) < \frac{X}{\mu(N) \log X} \sum_{a_1=-N}^{N} \sum_{\substack{|a_3| \leq N \\ j(E_{(a_1,a_3)})=J}} 1 < \frac{6NX}{\mu(N) \log X}. \tag{9}$$

Thus

$$\frac{1}{\mu(N)} \sum_{\substack{|a_1|,|a_3| \leq N \\ E_{(a_1,a_3)} \text{ has CM}}}{}' \pi^r_{E_{a_1,a_3}}(X) = \mathrm{O}\left(\frac{X}{N \log X} \right) \tag{10}$$

2. Averaging the special values of L-series.

As a first step toward proving Theorem 1.3, we let

$$B(r) := \max(r^2/4, 5) \quad \text{and} \quad d_p := \frac{r^2 - 4p}{f^2} \tag{11}$$

and let

$$\begin{aligned} S^r_f(X) &:= \left\{ B(r) < p \leq X : p \equiv r - 1 \pmod 3; 4p \equiv r^2 \pmod{f^2}; d_p \equiv 0, 1 \pmod 4 \right\} \\ &= \left\{ B(r) < p \leq X : p \equiv r - 1 \pmod 3; 4p \equiv r^2, r^2 - f^2 \pmod{4f^2} \right\} \end{aligned} \tag{12}$$

and prove:

Proposition 2.1. *For $r \equiv 0, 1 \pmod 3$,*

$$\begin{aligned}
&\frac{1}{\mu(N)} {\sum_{|a_1|,|a_3|\le N}}' \pi^r_{E_{a_1,a_3}}(X) \\
&= \frac{8N^2}{\pi\mu(N)} \Bigg[\frac{1}{\sqrt{X}\log X} \sum_{f\le 2\sqrt{X}} \frac{1}{f} \sum_{p\in S_f^r(r-1,3,X)} L(1,\chi_{d_p(f)})\log p \\
&\qquad - \int_2^X \left(\sum_{f\le 2\sqrt{t}} \frac{1}{f} \sum_{p\in S_f^r(r-1,3,t)} L(1,\chi_{d_p(f)})\log p \right) \frac{d}{dt}\left[\frac{1}{\sqrt{t}\log t}\right] dt \Bigg] \\
&\qquad + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{X^{5/2}}{N^2} + \log\log X \right).
\end{aligned} \tag{13}$$

Proof. Let $r \in \mathbb{Z}$ with $r \equiv 0, 1 \pmod 3$. Let $E_{(a_1,a_3)}$ be the parameterization of elliptic curves having a rational point of order 3. Provided that $p \nmid \Delta_{E_{(a_1,a_3)}}$, we know that $E_{(a_1,a_3)}(\mathbb{Q})_{\mathrm{tor}}$ injects into $E_{(a_1,a_3)}(\mathbb{F}_p)$ via the reduction modulo p map. Thus, if $a_p(E_{(a_1,a_3)}) = r$ then we must have $p \equiv r-1 \pmod 3$. So, we can write

$$\frac{1}{\mu(N)} {\sum_{|a_1|,|a_3|\le N}}' \pi^r_{E_{(a_1,a_3)}}(X) \quad = \quad \frac{1}{\mu(N)} \sum_{\substack{B(r)\le p\le X \\ p\equiv r-1 \pmod 3}} \left({\sum_{\substack{|a_1|,|a_3|\le N \\ a_p(E_{(a_1,a_3)})=r}}}' 1 \right) + \mathrm{O}(\log\log X), \tag{14}$$

where the inner sum on the righthand side is over (a_1, a_3) which yield nonsingular curves over $\mathbb{F}_p$. The O-term comes from number of curves from the lefthand side which reduce to singular curves modulo p.

We recall (see[1] or [9]) that if $r \le 2\sqrt{p}$, which is true when $p \ge B(r)$ then we have

$$\sum_{\substack{\tilde{E}/\mathbb{F}_p \\ a_p(\tilde{E})=r}} \frac{1}{\#\mathrm{Aut}(\tilde{E})} = \frac{1}{2} H(r^2-4p), \tag{15}$$

where $H(r^2-4p)$ denotes the Kronecker class number and is given by

$$H(r^2-4p) = 2 \sum_{\substack{f^2 | (r^2-4p) \\ \frac{r^2-4p}{f^2} \equiv 0,1 \pmod 4}} \frac{h((r^2-4p)/f^2)}{\omega((r^2-4p)/f^2)}. \tag{16}$$

Since $\mathrm{Aut}(\tilde{E}) = 2$ for all but at most 10 isomorphism classes of elliptic curves over $\mathbb{F}_p$, the number of isomorphism classes of elliptic curves $\tilde{E}/\mathbb{F}_p$ with $a_p(\tilde{E}) = r$ is $H(r^2-4p) + \mathrm{O}(1)$ Also, we note that if $p \equiv r-1 \pmod 3$ and if $p+1-\#\tilde{E}(\mathbb{F}_p) = r$, then $3 | \#\tilde{E}(\mathbb{F}_p)$. This implies that $\tilde{E}(\mathbb{F}_p)$ has a point of order 3 and therefore has a model of the form (4) (this follows from the argument given in [[6], pp. 145–146]). Thus, one of the curves $E_{(a_1,a_3)}$ will reduce to $\tilde{E}$. So, each of the $H(r^2-4p) + \mathrm{O}(1)$ isomorphism classes of curves over $\tilde{E}/\mathbb{F}_p$ with $a_p(\tilde{E}) = r$ is in the image of our

family $\{E_{(a_1,a_3)}\}$ under the reduction modulo p map. Thus, if we consider the reductions modulo p of all $E_{(a_1,a_3)}$ with $0 \leq a_1, a_3 \leq p-1$, then we will encounter each isomorphism class $\tilde{E}$ of elliptic curves over $\mathbb{F}_p$ with $a_p(\tilde{E}) = r$ at least once. Now, we must estimate the number of times each isomorphism class is encountered. It is easy to see ([2] p. 177) that the number of $(A, B) \in \mathbb{F}_p^2$ for which $E : y^2 = x^3 + Ax + B$ is isomorphic to a given elliptic curve is given by

$$\begin{cases} \frac{p-1}{6} & \text{if } A = 0 \text{ and } p \equiv 1 \pmod 3, \\ \frac{p-1}{4} & \text{if } B = 0 \text{ and } p \equiv 1 \pmod 4, \\ \frac{p-1}{2} & \text{otherwise.} \end{cases}$$

Thus we only need to know how many of the $E_{(a_1,a_3)}$ have the same c_4 and c_6 coefficients (see [11] pp. 46-48). Following the argument given in [[6], pp. 145–146]) we see given $E : y^2 = x^3 + Ax + B$ with 3-torsion over $\mathbb{F}_p$ that each choice of an order three point to be moved to the origin yields a different E_{a_1,a_3}. Thus the number of $E_{(a_1,a_3)}$ which have the same c_4 and c_6 coefficient is equal to the number of order 3 $\mathbb{F}_p$-points possessed by these curves. This is either 2 or 8 depending on whether the curves in question have cyclic or full 3-torsion over $\mathbb{F}_p$. So, we see that the number of $(a_1, a_3) \in \mathbb{F}_p$ for which $E_{(a_1,a_3)}$ is isomorphic to a given curve is given by

$$\begin{cases} \frac{p-1}{3} & \text{if } c_4 = 0, \text{ 3-torsion is cyclic and } p \equiv 1 \pmod 3, \\ \frac{p-1}{2} & \text{if } c_6 = 0, \text{ 3-tor is cyclic and } p \equiv 1 \pmod 4, \\ (p-1) & \text{otherwise when 3-torsion is cyclic,} \\ \frac{4(p-1)}{3} & \text{if } c_4 = 0, \text{ full 3-torsion and } p \equiv 1 \pmod 3, \\ 2(p-1) & \text{if } c_6 = 0, \text{ full 3-torsion and } p \equiv 1 \pmod 4, \\ 4(p-1) & \text{otherwise with full 3-torsion.} \end{cases}$$

We note that if $E_{(a_1,a_3)}(\mathbb{F}_p)$ possesses full 3-torsion then the action of Frobenius on $E_{(a_1,a_3)}[3]$ is trivial and thus the trace r of Frobenius must be 2 modulo 3. Since we are only considering the case $r \equiv 0, 1 \pmod 3$ which implies that $p \not\equiv 1 \pmod 3$, we may assume that $E_{(a_1,a_3)}(\mathbb{F}_p)$ has only cyclic 3-torsion. Thus the number of times each isomorphism class is encountered when considering $E_{(a_1,a_3)}$ where $0 \leq a_1, a_3 \leq p-1$ is given by

$$\begin{cases} \frac{p-1}{2} & \text{if } c_6 = 0 \text{ and } p \equiv 1 \pmod 4, \\ (p-1) & \text{otherwise.} \end{cases}$$

Therefore, we have

$$\sum_{\substack{0 \leq a_1, a_3 < p \\ a_p(E_{(a_1,a_3)}) = r}}{}' 1 = pH(r^2 - 4p) + \mathrm{O}(p), \tag{17}$$

Thus,

$$\sum_{\substack{|a_1|, |a_3| \leq N \\ a_p(E_{(a_1,a_3)}) = r}}{}' 1 = (pH(r^2 - 4p) + \mathrm{O}(p)) \left(\frac{2N}{p} + \mathrm{O}(1) \right)^2 \tag{18}$$

Substituting this into (14),we have

$$\begin{aligned}\frac{1}{\mu(N)}\sum_{|a_1|,|a_3|\le N}{}' \pi^r_{E_{a_1,a_3}}(X) \quad &= \\ \frac{4}{\mu(N)}\sum_{\substack{B(r)\le p\le X\\ p\equiv r-1 \pmod 3}}&\left(\frac{N^2H(r^2-4p)}{p}+\mathrm{O}\left(H(r^2-4p)(N+p)+\frac{N^2}{p}\right)\right)+\mathrm{O}\left(\log\log X\right),\end{aligned} \tag{19}$$

We recall that $H(r^2-4p)=2\sum_{\substack{f^2\mid(r^2-4p)\\ d_p(f)\equiv 0,1 \pmod 4}}\frac{h(d_p(f))}{w(d_p(f))}$, where $d_p(f)$ is as in (11). Thus, the right-hand side of (19) becomes

$$\frac{8}{\mu(N)}\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(r-1,3,X)}\left(\frac{h(d_p(f))}{w(d_p(f))}\left(\frac{N^2}{p}+\mathrm{O}(N+p)\right)\right)+\mathrm{O}\left(\log\log X\right). \tag{20}$$

By the class number formula, we have,

$$h(d)=\frac{w(d)|d|^{1/2}}{2\pi}L(1,\chi_d). \tag{21}$$

Combining this with the main result of [10], we see that $\frac{h(d_p(f))}{w(d_p(f))}=\mathrm{O}(\frac{\sqrt{p}\log p}{f})$. Thus (20) becomes

$$\begin{aligned}\frac{4}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(r-1,3,X)}&\left(\frac{N^2\sqrt{4p-r^2}}{pf}L(1,\chi_{d_p(f)})\right)\\ &+\mathrm{O}\left(\frac{1}{N^2}\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(r-1,3,X)}\frac{(N+p)\sqrt{p}\log p}{f}\right)+\mathrm{O}\left(\log\log X\right).\end{aligned} \tag{22}$$

Now using $\sqrt{4p-r^2}=2\sqrt{p}+\mathrm{O}(\frac{1}{\sqrt{p}})$ and the Brun-Titchmarsh inequality (see [5]), (22) becomes

$$\begin{aligned}\frac{8N^2}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(r-1,3,X)}&\left(\frac{L(1,\chi_{d_p(f)})}{\sqrt{p}f}\right)+\mathrm{O}\left(\sum_{f\le 2\sqrt{X}}\sum_{p\in S_f^r(r-1,3,X)}\frac{\log p}{p^{3/2}f}\right)\\ &+\mathrm{O}\left(\frac{1}{N^2}(N+X)\sqrt{X}\log X\cdot\sum_{f\le 2\sqrt{X}}\frac{1}{f}\frac{3X}{\phi(f^2)\log X}\right)+\mathrm{O}\left(\log\log X\right),\end{aligned} \tag{23}$$

which is the same as

$$\frac{8N^2}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(X)}\left(\frac{L(1,\chi_{d_p(f)})}{\sqrt{p}}\right)+\mathrm{O}\left(\frac{X^{3/2}}{N}+\frac{X^{5/2}}{N^2}+\log\log X\right). \tag{24}$$

Next, we use partial summation to rewrite the main term as

$$\begin{aligned}\frac{8N^2}{\pi\mu(N)}\cdot\frac{1}{\sqrt{X}\log X}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(r-1,3,X)}L(1,\chi_{d_p(f)})\log p\\ -\frac{8N^2}{\pi\mu(N)}\int_2^X\left(\sum_{f\le 2\sqrt{t}}\frac{1}{f}\sum_{p\in S_f^r(r-1,3,t)}L(1,\chi_{d_p(f)})\log p\right)\frac{d}{dt}\left[\frac{1}{\sqrt{t}\log t}\right]dt\end{aligned}\tag{25}$$

which completes the proof of Proposition 2.1

We also have the following proposition which is due to David and Pappalardi in the sense that one can obtain a proof of this proposition by carrying the condition that $p\equiv r-1 \pmod 3$ throughout the proof of Theorem 3.1 in [2] and slightly modifying their proof so as to allow for the possibility of r being even. For the sake of brevity, we omit the proof and refer the reader to [2] for details.

Proposition 2.2. *Let r be any integer. Then for any $c>0$,*

$$\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(X)}L(1,\chi_{d_p(f)})\log p = K_rX+\mathrm{O}\left(\frac{X}{\log^c X}\right),$$

where

$$K_r=\sum_{f=1}^{\infty}\frac{1}{f}\sum_{k=1}^{\infty}\frac{c_f^r(k)}{k\phi([3;kf^2])}\quad\text{and}\quad c_f^r(k):=\sum_{\substack{a \pmod{4k}\\ a\equiv 0,1 \pmod 4\\ (r^2-af^2,4kf^2)=4\\ 4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}}}\left(\frac{a}{k}\right),$$

Remark 2.1. *Comparing the above result with Theorem 3.1 in* [2] *one notices an extra condition in the definition of the $c_f^r(k)$, namely $4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}$. We give a brief explanation of this difference. In the proof of Theorem 3.1 in* [2] *one is lead (see equation (12) and following remark in* [2]*) to consider the sum*

$$\sum_{p\in S_f(X)}\left(\frac{d_p}{k}\right)\log p=\sum_{\substack{a \pmod{4k}\\ a\equiv 0,1 \pmod 4\\ (r^2-af^2,4kf^2)=4}}\left(\frac{a}{k}\right)\sum_{4p\equiv r^2-af^2 \pmod{4kf^2}}\log p$$

where $S_f(X):=\{B(r)<p\le X : 4p\equiv r^2, r^2-f^2 \pmod{4f^2}\}$ (see [2] *p. 169).*

To prove Proposition 2.2, we follow the proof of Theorem 3.1 in [2] *and are lead to consider the sum*

$$\sum_{p\in S_f^r(X)}\left(\frac{d_p}{k}\right)\log p=\sum_{\substack{a \pmod{4k}\\ a\equiv 0,1 \pmod 4\\ (r^2-af^2,4kf^2)=4}}\left(\frac{a}{k}\right)\sum_{\substack{4p\equiv r^2-af^2 \pmod{4kf^2}\\ p\equiv r-1 \pmod 3}}\log p$$

where as in (12), $S_f^r(X)=\{B(r)<p\le X : p\equiv r-1 \pmod 3;\ 4p\equiv r^2, r^2-f^2 \pmod{4f^2}\}$.

The two congruences $4p\equiv r^2-af^2 \pmod{4kf^2}$ and $p\equiv r-1 \pmod 3$ underneath the inner sum are compatible if and only if $4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}$. Thus, we can rewrite the righthand side of the last expression as

$$\sum_{\substack{a \pmod{4k} \\ a\equiv 0,1 \pmod 4 \\ (r^2-af^2,4kf^2)=4 \\ 4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}}} \left(\frac{a}{k}\right) \sum_{\substack{4p\equiv r^2-af^2 \pmod{4kf^2} \\ p\equiv r-1 \pmod 3}} \log p$$

We then estimate the inner sum just as in [2] *to obtain Proposition 2.2 with the extra congruence* $4(r-1) \equiv r^2 - af^2 \pmod{(12, 4kf^2)}$ *in the* $c_f^r(k)$*'s.*

Combining Propositions 2.1 and 2.2 we obtain the estimate:

$$\begin{aligned}
&\frac{1}{\mu(N)} {\sum_{|a_1|,|a_3|\le N}}' \pi^r_{E_(a_1,a_3)}(X) \\
&\quad = \frac{8N^2}{\pi\mu(N)} \left(\frac{1}{\sqrt{X}\log X} \left(K_r X + \mathrm{O}\left(\frac{X}{\log^c X}\right)\right) \right. \\
&\qquad \left. - \int_2^X \left(K_r t + \mathrm{O}\left(\frac{t}{\log^c t}\right)\right) \frac{d}{dt}\left[\frac{1}{\sqrt{t}\log t}\right] dt \right) \\
&\qquad + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{X^{5/2}}{N^2} + \log\log X\right).
\end{aligned} \tag{26}$$

The righthand side can be rewritten as,

$$\begin{aligned}
&\frac{8N^2}{\pi\mu(N)} K_r \left(\frac{\sqrt{X}}{\log X} + \int_2^X \frac{\mathrm{dt}}{\sqrt{t}\log^2 t} + \int_2^X \frac{\mathrm{dt}}{2\sqrt{t}\log t} \right) \\
&\qquad + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{X^{5/2}}{N^2} + \frac{\sqrt{X}}{\log^c X}\right).
\end{aligned} \tag{27}$$

Thus, noting that $\mu(N) = 4N^2 + \mathrm{O}(N)$, we have proved the following.

Proposition 2.3.

$$\frac{1}{\mu(N)} {\sum_{|a_1|,|a_3|\le N}}' \pi^r_{E_{(a_1,a_3)}}(X) = \frac{4}{\pi} K_r \cdot \pi_{1/2}(X) + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{X^{5/2}}{N^2} + \frac{\sqrt{X}}{\log^c X}\right) \tag{28}$$

Thus to prove Theorem 1.3 it remains only to show that $\frac{4}{\pi}K_r$ has the Euler-product expansion given for C_r in (6). We will do this in the next section.

3. The constant.

In this section we will derive an Euler product representation of the constant K_r which was defined in Proposition 2.2. The arguments and results in this section hold for any $r \in \mathbb{Z}$ although we will only use these results for the case that $r \equiv 0, 1 \pmod 3$. Recall from Proposition 2.2 that we have

$$K_r := \sum_{f=1}^{\infty} \frac{1}{f} \sum_{k=1}^{\infty} \frac{c_f^r(k)}{k\phi([3, kf^2])} \tag{29}$$

where

$$c_f^r(k) := \sum_{\substack{a \pmod{4k} \\ a\equiv 0,1 \pmod 4 \\ (r^2-af^2,4kf^2)=4 \\ 4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}}} \left(\frac{a}{k}\right), \tag{30}$$

We will split the previous sum into the two sums:

$$c_{f,0}^r(k) := \sum_{\substack{a \pmod{4k} \\ a\equiv 0 \pmod 4 \\ (r^2-af^2,4kf^2)=4 \\ 4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}}} \left(\frac{a}{k}\right) \quad \text{and} \quad c_{f,1}^r(k) := \sum_{\substack{a \pmod{4k} \\ a\equiv 1 \pmod 4 \\ (r^2-af^2,4kf^2)=4 \\ 4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}}} \left(\frac{a}{k}\right). \tag{31}$$

In order to further describe the behavior of the $c_{f,i}^r(k)$'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 3.1.

1. *For $c_{f,0}^r(k)$ to be nonzero, it is necessary that we have r, even; k, odd, $(r/2, f) = 1$ and $(3, f)|(r-2)$.*
2. *For $c_{f,1}^r(k)$ to be nonzero it is necessary that one of the following conditions hold.*
   (a) *r and f are both odd, $(r, f) = 1$ and $(3, f)|(r-2)$.*
   (b) *$r \equiv 2 \pmod 4, 4|f, (r/2, f) = 1$ and $(3, f)|(r-2)$.*
   (c) *$r \equiv 0 \pmod 4, f \equiv 2 \pmod 4, (r, f/2) = 1$ and $(3, f)|(r-2)$.*

Lemma 3.2. *$c_{f,i}^r(k)$ (i=1,2) is a multiplicative function of k.*

Proof. If r is odd, $c_{f,0}^r(k) = 0$ and the multiplicativity of $c_{f,1}^r(k)$ can be shown as in [2], lemma 3.3. So, we will consider only the case when r is even which can be handled by a very similar argument. In this case, we have

$$c_{f,0}^r(k) = \sum_{\substack{a \pmod{k} \\ ((r/2)^2-af^2,kf^2)=1 \\ (r/2-1)^2\equiv af^2 \pmod{(3,kf^2)}}} \left(\frac{a}{k}\right) \tag{32}$$

So, if $(r/2, f) = 1$, $(3, f)|(r-2)$ and k is odd, then we obtain

$$c_{f,0}^r(k) = \sum_{\substack{a \pmod{k} \\ ((r/2)^2-af^2,k)=1 \\ \frac{(r/2-1)^2}{(3,f)}\equiv a\frac{f^2}{(3,f)} \pmod{(\frac{3}{(3,f)},k)}}} \left(\frac{a}{k}\right), \tag{33}$$

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

We need only treat the cases in which $c^r_{f,1}(k)$ is possibly nonzero (see lemma 3.1). For case 2a, if k is odd, then we have

$$c^r_{f,1}(k) = \sum_{\substack{a\in\mathbb{Z}/k\mathbb{Z}\\(r^2-af^2,k)=1\\ \frac{(r-2)^2}{(3,f)}\equiv a\frac{f^2}{(3,f)} \pmod{(\frac{3}{(3,f)},k)}}} \left(\frac{a}{k}\right). \tag{34}$$

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

$$c^r_{f,1}(k) = \sum_{\substack{a\in\mathbb{Z}/k\mathbb{Z}\\((r/2)^2-a(f/2)^2,k)=1\\ \frac{(r/2-1)^2}{(3,f)}\equiv a\frac{(f/2)^2}{(3,f)} \pmod{(\frac{3}{(3,f)},k)}}} \left(\frac{a}{k}\right). \tag{35}$$

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

Lemma 3.3. *Given r, let $i = 0$ or 1 and define τ^r_i as follows.*

$$\tau^r_i = \begin{cases} 2 & \text{if } r \equiv 2 \pmod 4 \text{ and } i = 1,\\ 1 & \text{if } r \equiv 0 \pmod 4 \text{ and } i = 1,\\ 0 & \text{if } r \text{ is odd or if } i = 0. \end{cases}$$

If f is chosen such that r and f satisfy one of the conditions in lemma 3.1 for $c^r_{f,i}$, and if l is an odd prime, then we have

$$c^r_{f,i}(l^\alpha) = c^r_{2^{\tau^r_i} l^{\mathrm{ord}_l(f)},i}(l^\alpha)$$

If r and f satisfy one of conditions 2a, 2b or 2c of lemma 3.1, then

$$c^r_{f,1}(2^\alpha) = c^r_{2^{\mathrm{ord}_2(f)},1}(2^\alpha)$$

Proof. We will first treat the case when $i = 0$ and r and f satisfy condition (1) of lemma 3.1 Using (33), we have

$$\begin{aligned} c^r_{f,0}(l^\alpha) &= \sum_{\substack{a \pmod{l^\alpha}\\((r/2)^2-af^2,l)=1\\ \frac{(r/2-1)^2}{(3,f)}\equiv a\frac{f^2}{(3,f)} \pmod{(\frac{3}{(3,f)},l^\alpha)}}} \left(\frac{a}{l}\right)^\alpha \\ &= \begin{cases} \sum_{\substack{a \pmod{l^\alpha}\\((r/2)^2-af^2,l)=1}} \left(\frac{a}{l}\right)^\alpha & \text{if } l \neq 3,\\ \sum_{a \pmod{3^\alpha}} \left(\frac{a}{3}\right)^\alpha & \text{if } l = 3 \text{ and } 3|f,\\ \sum_{\substack{a \pmod{3^\alpha}\\(r/2-1)^2\equiv a \pmod 3}} \left(\frac{a}{3}\right)^\alpha & \text{if } l = 3 \text{ and } 3\not|f. \end{cases} \end{aligned} \tag{36}$$

Using this last expression one can easily see that $c^r_{f,0}(l^\alpha) = c^r_{l^{\mathrm{ord}_l(f)},0}(l^\alpha)$, and thus we have proved that the lemma holds in this case.

In all other cases when l is an odd prime, the proof is the essentially the same.

For the last assertion, we first assume that r and f satisfy condition 2a of lemma 3.1. From (31), one obtains

$$c^r_{f,1}(2^\alpha) = \sum_{\substack{a \pmod{2^{\alpha+2}} \\ a \equiv 5 \pmod 8}} \left(\frac{a}{2}\right)^\alpha \tag{37}$$

Using this expression, it is obvious that $c^r_{f,1}(2^\alpha) = c^r_{1,1}(2^\alpha)$ as desired.

Now assuming that r and f satisfy either of conditions 2b or 2c of lemma 3.1 we deduce from 31 that

$$c^r_{f,1}(2^\alpha) = \sum_{\substack{a \pmod{2^{\alpha+2}} \\ a \equiv 1 \pmod 4}} \left(\frac{a}{2}\right)^\alpha \tag{38}$$

and, again it is obvious that $c^r_{f,1}(2^\alpha) = c^r_{2^{\mathrm{ord}_2(f)},1}(2^\alpha)$.

In order to evaluate the $c^r_{l^{\beta|},i}(l^\alpha)$, $(i = 0, 1)$, we have the following two lemmas.

Lemma 3.4. *Suppose that l is an odd prime and $\alpha > 0$. Letting $d = c^r_{l^\beta,0}(l^\alpha)$ when r is even; $(r, l^\beta) = 1$ and $(3, l^{2\beta})|((r/2-1)^2)$, or letting $d = c^r_{2^{\tau_1 r} l^\beta,1}(l^\alpha)$ when r and $f = l^\beta$ satisfy conditions 2a, 2b or 2c of lemma 3.1, we have*

$$d = \begin{cases} -\left(\frac{r^2}{l}\right) l^{\alpha-1} & \text{if } \beta = 0; \alpha, \text{ odd; } l \neq 3. \\ (l - 1 - \left(\frac{r^2}{l}\right))l^{\alpha-1} & \text{if } \beta = 0; \alpha, \text{ even; } l \neq 3. \\ 3^{\alpha-1}\left(\frac{(r-2)^2}{3}\right)^\alpha & \text{if } \beta = 0 \text{ and } l = 3. \\ 0 & \text{if } \beta > 0 \text{ and } \alpha \text{ is odd,} \\ l^{\alpha-1}(l-1) & \text{if } \beta > 0 \text{ and } \alpha \text{ is even.} \end{cases} \tag{39}$$

Proof. We will prove the lemma for $c^r_{4l^\beta,1}(l^\alpha)$ where l is an odd prime and where r and $f = l^\beta$ satisfy condition 2b of lemma 3.1. The proofs for all other cases are similar. From (35) above, we deduce

$$c^r_{4l^\beta,1}(l^\alpha) = \begin{cases} \sum_{\substack{a \in \mathbb{Z}/l^\alpha Z \\ ((r/2)^2 - 4a, l) = 1 \\ (r/2-1)^2 \equiv 4a \pmod{(3, l^\alpha)}}} \left(\frac{a}{l}\right)^\alpha & \text{if } \beta = 0, \\ \sum_{a \in \mathbb{Z}/l^\alpha Z} \left(\frac{a}{l}\right)^\alpha & \text{if } \beta > 0. \end{cases} \tag{40}$$

The desired result now follows.

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

Lemma 3.5. (1) *If r is odd, then $c^r_{1,1}(2^\alpha) = \frac{(-2)^\alpha}{2}$.*

(2) *If r is even and r and $f = 2^\beta$ satisfy either of conditions (2b) or (2c) of lemma 3.1, then*

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

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

$$\kappa(\ell^\alpha) = \begin{cases} \ell & \text{if } \alpha \text{ is odd,} \\ 1 & \text{if } \alpha \text{ is even,} \end{cases} \tag{41}$$

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

Lemma 3.6. *For all k, $c^r_{f,i}(k) \leq k/\kappa(k)$, where $i = 0, 1$.*

Proof. From lemmas 3.3, 3.4 and 3.5, it follows immediately that for any prime l,

$$\begin{aligned} c^r_{f,i}(l^\alpha) &\leq \begin{cases} l^\alpha & \text{if } \alpha \text{ is even,} \\ l^{\alpha-1} & \text{if } \alpha \text{ is odd.} \end{cases} \\ &= l^\alpha/\kappa(l^\alpha). \end{aligned} \tag{42}$$

The lemma now follows from the multiplicativity of $c^r_{f,i}$ and κ.

We recall the following fact from ([2] Lemma 3.4).

Lemma 3.7. [David-Pappalardi] *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 K_r (see (29)) is a finite constant. We rewrite K_r as

$$K_r = K_r^0 + K_r^1, \tag{43}$$

where

$$K_r^0 = \sum_{f=1}^{\infty} \frac{1}{f} \sum_{k=1}^{\infty} \frac{c^r_{f,0}(k)}{k\phi([3, kf^2])} \quad \text{and} \quad K_r^1 = \sum_{f=1}^{\infty} \frac{1}{f} \sum_{k=1}^{\infty} \frac{c^r_{f,1}(k)}{k\phi([3, kf^2])} \tag{44}$$

Now we compute the constants K_r^i $(i = 0, 1)$. We recall the following identities

$$\phi(AB) = \phi(A)\phi(B)\frac{(A, B)}{\phi((A, B))}, \tag{45}$$

and therefore, if $B|A$,

$$\phi(\frac{A}{B}) = \frac{\phi(A)\phi((\frac{A}{B}, B))}{\phi(B)(\frac{A}{B}, B)}. \tag{46}$$

In particular, we can write

$$\phi([3, k \cdot 2^{2\tau_i^r} f^2]) = \frac{\phi(3 \cdot 2^{2\tau_i^r} f^2)\phi(k)(3 \cdot 2^{2\tau_i^r} f^2, k)}{(3, kf^2)\phi((3 \cdot 2^{2\tau_i^r} f^2, k))}. \tag{47}$$

Now, we recall for a fixed r, that f must be chosen such that r and f satisfy the conditions of lemma 3.1 for $c^r_{f,i}(k)$ to be non-zero. We will denote by S^r_i the set of f's which satisfy the conditions of lemma 3.1, and we let τ^r_i be defined as in lemma 3.3. Then, we can write

$$\begin{aligned} K^i_r &= \sum_{\substack{f,k=1 \\ 2^{\tau^r_i} f \in S^r_i}}^{\infty} \frac{c^r_{2^{\tau^r_i} f,i}(k)}{2^{\tau^r_i} fk\phi([3, k2^{2\tau^r_i} f^2])} \\ &= \frac{1}{2^{\tau^r_i}} \sum_{\substack{f=1 \\ 2^{\tau^r_i} f \in S^r_i}}^{\infty} \frac{1}{f\phi(3 \cdot 2^{2\tau^r_i} f^2)} \sum_{k=1}^{\infty} \frac{c^r_{2^{\tau^r_i} f,i}(k)(3, kf^2)\phi((3 \cdot 2^{2\tau^r_i} f^2, k))}{k\phi(k)(3 \cdot 2^{2\tau^r_i} f^2, k)}. \end{aligned} \tag{48}$$

Using lemma 3.2 and the multiplicativity of ϕ and letting $(a, b)_q := q^{\mathrm{ord}_q((a,b))}$, we can rewrite the inner sum above as,

$$\prod_{q,\text{ prime}} \left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i} f,i}(q^j)(3, f^2 q^j)_q \phi((3 \cdot 2^{2\tau^r_i} f^2, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i} f^2, q^j)} \right). \tag{49}$$

Using lemma 3.3, (49) can be rewritten as

$$\begin{aligned} &\prod_{q \nmid f} \left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i},i}(q^j)(3, q^j)_q \phi((3 \cdot 2^{2\tau^r_i}, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i}, q^j)} \right) \cdot \prod_{q|f} \left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i} q^{\mathrm{ord}_q(f)},i}(q^j)(3, f^2 q^j)_q \phi((3 \cdot 2^{2\tau^r_i} f^2, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i} f^2, q^j)} \right) \\ &= \prod_{q,\text{ prime}} \left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i},i}(q^j)(3, q^j)_q \phi((3 \cdot 2^{2\tau^r_i}, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i}, q^j)} \right) \cdot \prod_{q|f} \frac{\left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i} q^{\mathrm{ord}_q(f)},i}(q^j)(3, f^2 q^j)_q \phi((3 \cdot 2^{2\tau^r_i} f^2, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i} f^2, q^j)} \right)}{\left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i},i}(q^j)(3, q^j)_q \phi((3 \cdot 2^{2\tau^r_i}, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i}, q^j)} \right)}. \end{aligned} \tag{50}$$

Now, substituting this last expression back into (48) and using (45), we obtain the following expression for K^i_r.

$$\begin{aligned} &\frac{1}{2^{\tau^r_i} \phi(3)\phi(2^{2\tau^r_i})} \prod_{q,\text{ prime}} \left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i},i}(q^j)(3, q^j)_q \phi((3 \cdot 2^{2\tau^r_i}, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i}, q^j)} \right) \\ &\cdot \sum_{\substack{f=1 \\ 2^{\tau^r_i} f \in S^r_i}}^{\infty} \left(\frac{\phi((3 \cdot 2^{2\tau^r_i}, f^2))}{f\phi(f^2)(3 \cdot 2^{2\tau^r_i}, f^2)} \right) \cdot \prod_{q|f} \frac{\left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i} q^{\mathrm{ord}_q(f)},i}(q^j)(3, f^2 q^j)_q \phi((3 \cdot 2^{2\tau^r_i} f^2, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i} f^2, q^j)} \right)}{\left(\sum_{j \geq 0} \frac{c^r_{2^{\tau^r_i},i}(q^j)(3, q^j)_q \phi((3 \cdot 2^{2\tau^r_i}, q^j))}{q^j \phi(q^j)(3 \cdot 2^{2\tau^r_i}, q^j)} \right)}. \end{aligned} \tag{51}$$

Now, if $S_i^r = \emptyset$, then the above expression is just 0. So, we will assume for now that $S_i^r \neq \emptyset$, and in this case we can rewrite the sum from (51) as a product

$$\prod_{q,\text{ prime}} \left(1 + \sum_{\substack{\beta=1 \\ 2^{\tau_i^r} q^\beta \in S_i^r}}^{\infty} \frac{\frac{\phi((3\cdot 2^{2\tau_i^r}, q^{2\beta}))}{q^\beta \phi(q^{2\beta})(3\cdot 2^{2\tau_i^r}, q^{2\beta})} \left(\sum_{j\geq 0} \frac{c^r_{2^{\tau_i^r} q^\beta, i}(q^j)(3, q^{2\beta+j})_q \phi((3\cdot 2^{2\tau_i^r} q^{2\beta}, q^j))}{q^j \phi(q^j)(3\cdot 2^{2\tau_i^r} q^{2\beta}, q^j)} \right)}{\left(\sum_{j\geq 0} \frac{c^r_{2^{\tau_i^r}, i}(q^j)(3, q^j)_q \phi((3\cdot 2^{2\tau_i^r}, q^j))}{q^j \phi(q^j)(3\cdot 2^{2\tau_i^r}, q^j)} \right)} \right). \tag{52}$$

This allows us to rewrite (51) as

$$\frac{1}{2^{\tau_i^r}\phi(3)\phi(2^{2\tau_i^r})} \prod_{q,\text{ prime}} \left(\begin{array}{l} \displaystyle\sum_{j\geq 0} \frac{c^r_{2^{\tau_i^r}, i}(q^j)(3, q^j)_q \phi((3\cdot 2^{2\tau_i^r}, q^j))}{q^j \phi(q^j)(3\cdot 2^{2\tau_i^r}, q^j)} \\ \quad + \displaystyle\sum_{\substack{\beta=1 \\ 2^{\tau_i^r} q^\beta \in S_i^r}}^{\infty} \frac{\phi((3\cdot 2^{2\tau_i^r}, q^{2\beta}))}{q^\beta \phi(q^{2\beta})(3\cdot 2^{2\tau_i^r}, q^{2\beta})} \displaystyle\sum_{j\geq 0} \frac{c^r_{2^{\tau_i^r} q^\beta, i}(q^j)(3, q^{2\beta+j})_q \phi((3\cdot 2^{2\tau_i^r} q^{2\beta}, q^j))}{q^j \phi(q^j)(3\cdot 2^{2\tau_i^r} q^{2\beta}, q^j)} \end{array} \right). \tag{53}$$

We rearrange (53) to obtain the following expression for K_r^i.

$$\begin{aligned} &\frac{1}{2^{\tau_i^r}\phi(3)\phi(2^{2\tau_i^r})} \prod_{q\not| 6} \left(\sum_{j\geq 0} \frac{c^r_{2^{\tau_i^r}, i}(q^j)}{q^j \phi(q^j)} + \sum_{\substack{\beta=1 \\ 2^{\tau_i^r} q^\beta \in S_i^r}}^{\infty} \frac{1}{q^\beta \phi(q^{2\beta})} \sum_{j\geq 0} \frac{c^r_{2^{\tau_i^r} q^\beta, i}(q^j)\phi((q^{2\beta}, q^j))}{q^j \phi(q^j)(q^{2\beta}, q^j)} \right) \\ &\cdot \left(1 + \sum_{j\geq 1} \frac{c^r_{2^{\tau_i^r}, i}(3^j)}{3^{2j-1}} + \sum_{\substack{\beta=1 \\ 2^{\tau_i^r} 3^\beta \in S_i^r}}^{\infty} \frac{1}{3^{3\beta}} \left(3 + \sum_{j\geq 1} \frac{c^r_{2^{\tau_i^r} 3^\beta, i}(3^j)}{3^{2j-1}} \right) \right) \\ &\cdot \left(\begin{array}{l} 1 + \displaystyle\sum_{j\geq 1} \frac{c^r_{2^{\tau_i^r}, i}(2^j)\phi((2^{2\tau_i^r}, 2^j))}{2^j \phi(2^j)(2^{2\tau_i^r}, 2^j)} \\ \quad + \displaystyle\sum_{\substack{\beta=1 \\ 2^{\tau_i^r+\beta} \in S_i^r}}^{\infty} \frac{\phi((2^{\tau_i^r}, 2^{2\beta}))}{2^\beta \phi(2^{2\beta})(2^{\tau_i^r}, 2^{2\beta})} \displaystyle\sum_{j\geq 0} \frac{c^r_{2^{\tau_i^r+\beta}, i}\phi((2^{2\tau_i^r+2\beta}, 2^j))}{2^j \phi(2^j)(2^{2\tau_i^r+2\beta}, 2^j)} \end{array} \right). \end{aligned} \tag{54}$$

We will deal with the product and the contribution from the primes 2 and 3 separately. For convenience let $K_r^i(l)$ denote the contribution of the prime l to the above product. In particular, the second and third factors above will be denoted $K_r^i(2)$ and $K_r^i(3)$ respectively.

In the first factor of (54), since $q\not|6$, and since we are assuming that $S_i^r \neq \emptyset$, $2^{\tau_i^r} q^\beta \in S_i^r$ for all $\beta \geq 1$ if and only if $q\not|r$. So using lemma 3.4, the first product in (54) becomes

$$\prod_{\substack{q\not|6\\ q\not|r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q\not|6\\ q|r}} \frac{q^2}{q^2-1}. \tag{55}$$

We can now use lemmas 3.4 and 3.5 to simplify $K_r^i(3)$ and $K_r^i(2)$. We obtain,

$$K_r(3) := K_r^i(3) = \begin{cases} \frac{9}{8} & \text{if } r \equiv 2 \pmod 3, \\ \frac{3}{2} & \text{if } r \equiv 0 \pmod 3. \end{cases} \tag{56}$$

$$K_r^i(2) = \begin{cases} \frac{32}{21} & \text{if } i = 1;\ r \equiv 2 \pmod 4, \\ \frac{4}{3} & \text{if } i = 1;\ r \equiv 0 \pmod 4, \\ \frac{2}{3} & \text{if } i = 1 \text{ and } r \text{ is odd}, \\ \frac{9}{7} & \text{if } i = 0;\ r \equiv 2 \pmod 4, \\ 1 & \text{if } i = 0 \text{ and } r \equiv 0 \pmod 4. \end{cases} \tag{57}$$

Thus,

$$K_r = \frac{1}{\phi(3)} \left(K_r^0(2) + \frac{K_r^1(2)}{2^{\tau_1^r}\phi(2^{2\tau_1^r})} \right) K_r(3) \prod_{\substack{q\not|6\\ q\not|r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q\not|6\\ q|r}} \frac{q^2}{q^2-1}. \tag{58}$$

We note that

$$\left(K_r^0(2) + \frac{K_r^1(2)}{2^{\tau_1^r}\phi(2^{w\tau_1^r})} \right) = \begin{cases} \frac{4}{3} & \text{if } r \text{ is even}, \\ \frac{2}{3} & \text{if } r \text{ is odd}. \end{cases} \tag{59}$$

Thus we have

$$K_r = \frac{1}{2} K_r(3) \prod_{\substack{q\neq 3\\ q\not|r}} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{\substack{q\neq 3\\ q|r}} \frac{q^2}{q^2-1}. \tag{60}$$

Theorem 1.3 now follows from Proposition 2.3 and (60).

References

[1] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57-60.

[2] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves. Internat. Math. Res. Notices (1999) 165–183.

[3] W. Duke,*Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), No. 8, 813-818.

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

[5] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Math. Soc. Mongr. **4**, Academic Press, London, 1974.

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

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

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

[9] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673.
[10] S. Louboutin, *Majorations explicites de* $|L(1,\chi)|$, C. R. Acad. Paris Ser. I Math. **323** (1996) no. 5, 443-446.
[11] J. Silverman, The arithmetic of elliptic curves.
[12] J. P. Serre, *Properties galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

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/