ACTA ARITHMETICA
111.3 (2004)

Average distributions and products of special values of L-series

by

Amir Akbary (Lethbridge), Chantal David (Montréal)
and Robert Juricevic (Waterloo)

1. Introduction. Let E be an elliptic curve defined over the rationals. For any prime p of good reduction, let E_p be the elliptic curve over $\mathbb{F}_p$ obtained by reducing E modulo p. Let $a_p(E)$ be the trace of the Frobenius morphism of E_p. Then Hasse proved that $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$ with $|a_p(E)| \le 2\sqrt{p}$. The case $a_p(E) = 0$ corresponds to supersingular reduction modulo p.

Let N be a positive integer. For a fixed $r \in \mathbb{Z}$ and fixed curves $E_1, \dots, E_N$, we define

$$\pi^r_{E_1,\dots,E_N}(x) = \#\{p \le x : a_p(E_1) = \dots = a_p(E_N) = r\}.$$

There is a simple heuristic that can be used to predict the asymptotic behavior of $\pi^r_{E_1,\dots,E_N}(x)$. From Hasse's bound, the probability that $a_p(E) = r$ is

$$\mathrm{Prob}\{a_p(E) = r\} \sim \begin{cases} \dfrac{1}{4\sqrt{p}} & \text{if } |r| \le 2\sqrt{p}, \\ 0 & \text{if } |r| > 2\sqrt{p}. \end{cases}$$

This suggests the asymptotic behavior

$$\pi^r_E(x) \sim \sum_{p \le x} \mathrm{Prob}\{a_p(E) = r\} \sim C_{E,r}\,\frac{\sqrt{x}}{\log x}$$

where $C_{E,r}$ is a constant depending on E and r. Similarly, assuming that $a_p(E_1) = r$ and $a_p(E_2) = r$ are independent events for non-isogenous curves E_1 and E_2, we have for $|r| \le 2\sqrt{p}$,

2000 *Mathematics Subject Classification*: Primary 11G05; Secondary 11M41.

Research of A. Akbary partially supported by University of Lethbridge Research Fund and NSERC.

Research of C. David partially supported by NSERC and FCAR.

Research of R. Juricevic partially supported by NSERC and FCAR.

$$\mathrm{Prob}\{a_p(E_1) = a_p(E_2) = r\} \sim \frac{1}{16p}$$

and more generally

$$\mathrm{Prob}\{a_p(E_1) = \ldots = a_p(E_N) = r\} \sim \frac{1}{4^N p^{N/2}}.$$

Summing the probabilities as above leads to the following conjecture.

CONJECTURE 1.1 (Lang–Trotter conjecture). *Let N be a positive integer, let $r \in \mathbb{Z}$, and let $E_1, \ldots, E_N$ be elliptic curves over $\mathbb{Q}$, not $\overline{\mathbb{Q}}$-isogenous and if $r = 0$ without complex multiplication. Then*

$$\pi^r_{E_1,\ldots,E_N}(x) \sim \begin{cases} C_{E_1,r}\,\dfrac{\sqrt{x}}{\log x} & \text{if } N = 1, \\ C_{E_1,E_2,r}\log\log x & \text{if } N = 2, \\ \text{is finite} & \text{if } N > 2. \end{cases}$$

For $N = 1$, there is a more precise conjecture by Lang and Trotter [LT]. Their conjecture is based on a probabilistic model more refined than the simple heuristic above, and they then get a conjectural value for the constant $C_{E,r}$. In particular, the constant can be 0, and the asymptotic relation is then interpreted to mean that there are only finitely many primes p such that $a_p(E) = r$. This can happen, for example, if E has rational torsion over $\mathbb{Q}$. Some other such cases were classified in [DKP].

To this date, very little is known about the Lang–Trotter conjecture. It was shown by Elkies [Elk] that for any elliptic curve E over $\mathbb{Q}$, there are infinitely many primes such that $a_p(E) = 0$, but this result is not known for any curve E if $r \neq 0$. The best (unconditional) lower bound for this case is $\pi^0_E(x) \geq \log_3 x/(\log_4 x)^{1+\delta}$ for any positive δ and x sufficiently large [FM1].

For any $r \in \mathbb{Z}$, it was shown by Serre [S] that $\pi^r_E(x)$ has density 0 in the set of primes, and the best result for this case is $\pi^r_E(x) \ll x^{4/5}(\log x)^{-1/5}$ ([MMS]) under the Generalised Riemann Hypothesis. For $r = 0$, the unconditional bound $\pi^0_E(x) \ll x^{3/4}$ was obtained by Elkies and Ram Murty.

A classical way to get evidence for hard distribution questions like the Lang–Trotter conjecture is to look at average estimates. For any $a, b \in \mathbb{Z}$ such that $4a^3 + 27b^2 \neq 0$, let $E(a, b)$ be the elliptic curve

$$y^2 = x^3 + ax + b.$$

It was shown by Murty and Fouvry [FM1] that for $r = 0$, the Lang–Trotter conjecture holds on average, i.e. as $x \to \infty$,

$$\frac{1}{4AB}\sum_{\substack{|a|\leq A\\ |b|\leq B}} \pi^0_{E(a,b)}(x) \sim C_0\,\frac{\sqrt{x}}{\log x}$$

where C_0 is an explicit non-zero constant. This result was extended to all $r \in \mathbb{Z}$ by David and Pappalardi [DP] who showed that as $x \to \infty$,

$$\frac{1}{4AB}\sum_{\substack{|a|\le A\\ |b|\le B}}\pi^r_{E(a,b)}(x)\sim C_r\,\frac{\sqrt{x}}{\log x}$$

where

$$C_r=\frac{2}{\pi}\prod_{p\mid r}\frac{p^2}{p^2-1}\prod_{p\nmid r}\frac{p(p^2-p-1)}{(p-1)(p^2-1)}. \tag{1}$$

We prove in this paper that the Lang–Trotter conjecture holds on average when $N=2$. If $r=0$, this was done by Fouvry and Murty [FM2]. We extend it to all $r\in\mathbb{Z}$. As for all those average results, the key step is a theorem of Deuring which relates the number of elliptic curves over the finite fields $\mathbb{F}_p$ with $a_p(E)=r$ to the class number of the quadratic imaginary order of discriminant r^2-4p (see Section 2). By Dirichlet's class number formula, the averages to consider are then averages of special values of Dirichlet L-functions (for $N=1$), or averages of products of special values of Dirichlet L-functions (for $N\ge 2$). In the case $r=0$, one can compute those averages by splitting the L-functions

$$L(1,\chi)=\sum_{n\ge 1}\frac{\chi(n)}{n}$$

into two sums, depending if n is a square or not, as only the terms with n a square will contribute to the main term. This is not the case when $r\neq 0$, because there is a *shifting* in the characters χ. Then all the terms of the Dirichlet L-functions will contribute to the main term, and the computations are more delicate. The average Lang–Trotter conjecture for two elliptic curves then follows from this average of products of special values of Dirichlet L-functions.

THEOREM 1.2. *Let $\varepsilon>0$, and let r be an odd integer. Let A,B be positive integers with $A,B\ge x^{1+\varepsilon}$. Then as $x\to\infty$,*

$$\frac{1}{16A^2B^2}\sum_{\substack{|a_1|,|a_2|\le A\\ |b_1|,|b_2|\le B}}\pi^r_{E_1,E_2}(x)\sim C_r\log\log x$$

where

$$C_r=\frac{3}{\pi^2}\prod_{p\mid r}\frac{p^2(p^2+1)}{(p^2-1)^2}\prod_{p\nmid r}\frac{p^2(p^4-2p^2-3p-1)}{(p+1)^3(p-1)^3}. \tag{2}$$

We remark that for technical reasons, we restrict to the case of r odd in the statement of Theorem 1.2. A similar result (with a different constant) would hold for r even, but is not included here, except for the case $r=0$ (done previously by Fouvry and Murty) in Section 5.

The structure of this paper is as follows: in Section 2, we reduce the statement of Theorem 1.2 to an average of a product of special values of L-series; in Section 3, we find a precise asymptotic for the average of the product of special values of L-series that is necessary for our application; in Section 4, we find the expression for the constant C_r as an Euler product; in Section 5, we show that our method implies the Fouvry–Murty result in the case $r = 0$.

Acknowledgments. We would like to thank Ram Murty for reading the manuscript and for commenting on an earlier version of this work.

2. From elliptic curves to L-series. In all the following, we fix an integer r. For any integers a_1, a_2, b_1, b_2 such that $4a_1^3 + 27b_1^2 \neq 0$ and $4a_2^3 + 27b_2^2 \neq 0$, let

$$E_1 : y^2 = x^3 + a_1x + b_1, \qquad E_2 : y^2 = x^3 + a_2x + b_2$$

be two elliptic curves over $\mathbb{Z}$. Then, for such a_1, b_1, a_2, b_2, we define

$$\pi^r_{E_1,E_2}(x) = \#\{p \leq x : a_p(E_1) = a_p(E_2) = r\}.$$

We consider

$$\sum_{\substack{|a_1|,|a_2|\leq A\\ |b_1|,|b_2|\leq B}} \pi^r_{E_1,E_2}(x)$$

where a_1, a_2, b_1, b_2 are such that $(4a_1^3+27b_1^2)(4a_2^3+27b_2^2) \neq 0$. Reversing the summations, this is

$$\sum_{B_r<p\leq x} \#\{|a_1|, |a_2| \leq A,\ |b_1|, |b_2| \leq B : a_p(E_1) = a_p(E_2) = r\} + O(A^2B^2) \tag{3}$$

where $B_r = \max(3, r^2/4)$, and the $O(A^2B^2)$ comes from the fact that we removed the primes 2 and 3 from the sum.

Let $E(a, b)$ be the elliptic curve $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. The reduced curve $E(a, b)_p/\mathbb{F}_p$ is the reduction modulo p of a minimal model at p for $E(a, b)$. Write $a = p^{4k}a'$ and $b = p^{6k}b'$ with $k \geq 0$ and integers a', b' such that $v_p(a') < 4$ or $v_p(b') < 6$ ($v_p(n)$ is the power of p appearing in n). Then, for $p > 3$, $E(a', b') : y^2 = x^3 + a'x + b'$ is a minimal model for $E(a, b)$ at p. Hence, each elliptic curve E_p over the finite field $\mathbb{F}_p$ is the reduction of

$$\left(\frac{2A}{p} + O(1)\right)\left(\frac{2B}{p} + O(1)\right) + O\left(\frac{AB}{p^{10}}\right)$$

curves $E(a, b)$ with $a, b \in \mathbb{Z}$ and $|a| \leq A$, $|b| \leq B$, where the second term accounts for non-minimal models. It follows that

$$\#\{|a_1|,|a_2|\le A,\ |b_1|,|b_2|\le B : a_p(E_1)=a_p(E_2)=r\} = \left(\frac{4AB}{p^2}+O\left(\frac{A}{p}+\frac{B}{p}+\frac{AB}{p^{10}}+1\right)\right)^2 N(p,r)^2 \tag{4}$$

where $N(p,r)$ is the number of curves E over the finite field $\mathbb{F}_p$ such that $a_p(E)=r$, or equivalently with $p+1-r$ points over that field.

LEMMA 2.1 (Deuring's Theorem). *Let p be a prime, and r an integer such that $r^2-4p<0$. Let $H(r^2-4p)$ be the Kronecker class number*

$$H(r^2-4p)=2\sum_{f^2\mid r^2-4p}\frac{h(d)}{w(d)}$$

where the sum runs over all positive integers f such that $f^2\mid r^2-4p$ and $d=(r^2-4p)/f^2\equiv 0,1 \bmod 4$ and is not a square, and $h(d)$ and $w(d)$ are the class number and the number of units in the order of discriminant d respectively. Then

$$N(p,r)=\frac{p-1}{2}H(r^2-4p).$$

Proof. See [Deu] or [Cox, Theorem 14.18]. ∎

Using the last lemma and the standard bound $H(r^2-4p)\ll\sqrt{p}\log^2 p$, we get

$$N(p,r)^2=\frac{p^2H^2(r-4p)}{4}+O(p^2\log^4 p)\ll p^3\log^4 p.$$

Inserting this in (4) and (3) gives

$$\begin{aligned}\sum_{\substack{|a_1|,|a_2|\le A\\ |b_1|,|b_2|\le B}}\pi^r_{E_1,E_2}(x) &= 4A^2B^2\sum_{B_r\le p\le x}\frac{H^2(r^2-4p)}{p^2}\\ &\quad+O(A^2B^2+(A^2B+AB^2)x\log^4 x\\ &\quad+(A^2+AB+B^2)x^2\log^4 x+\dots\\ &\quad\dots+(A+B)x^3\log^4 x+x^4\log^4 x).\end{aligned}$$

We take A,B such that

$$A,B\ge x^{1+\varepsilon} \tag{5}$$

for any $\varepsilon>0$. Then we have

$$\sum_{\substack{|a_1|,|a_2|\le A\\ |b_1|,|b_2|\le B}}\pi^r_{E_1,E_2}(x)=4A^2B^2\sum_{B_r<p\le x}\frac{H^2(r^2-4p)}{p^2}+O(A^2B^2). \tag{6}$$

We now analyse the main term. By definition of the Kronecker class number, and using the class number formula, we get

$$\begin{aligned}\frac{1}{4}\sum_{B_r\le p\le x}\frac{H^2(r^2-4p)}{p^2} &= \sum_{B_r<p\le x}\frac{1}{p^2}\sum_{\substack{f^2\mid r^2-4p\\ f^2d_1=r^2-4p}}\frac{h(d_1)}{w(d_1)}\sum_{\substack{g^2\mid r^2-4p\\ g^2d_2=r^2-4p}}\frac{h(d_2)}{w(d_2)}\\ &= \frac{1}{4\pi^2}\sum_{B_r<p\le x}\frac{1}{p^2}\sum_{\substack{f^2\mid r^2-4p\\ f^2d_1=r^2-4p}}\frac{\sqrt{4p-r^2}}{f}L(1,\chi_{d_1})\\ &\quad\times\sum_{\substack{g^2\mid r^2-4p\\ g^2d_2=r^2-4p}}\frac{\sqrt{4p-r^2}}{g}L(1,\chi_{d_2})\\ &= \frac{1}{4\pi^2}\sum_{\substack{f\le 2\sqrt{x}\\ g\le 2\sqrt{x}}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}\frac{4p-r^2}{p^2}L(1,\chi_{d_1})L(1,\chi_{d_2}),\end{aligned}$$

where $S_{f,g}(x)$ is the set of primes

$$\begin{aligned}S_{f,g}(x)=\{&B_r<p\le x : f^2\mid r^2-4p,\ g^2\mid r^2-4p,\\ &d_1=(r^2-4p)/f^2\equiv 0,1 \bmod 4,\ d_2=(r^2-4p)/g^2\equiv 0,1 \bmod 4\}.\end{aligned}$$

We rewrite the last sum as

$$\begin{aligned}(7)\qquad &\frac{1}{\pi^2}\sum_{\substack{f\le 2\sqrt{x}\\ g\le 2\sqrt{x}}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}\frac{L(1,\chi_{d_1})L(1,\chi_{d_2})}{p}\\ &\qquad+O\Bigg(\sum_{\substack{f\le 2\sqrt{x}\\ g\le 2\sqrt{x}}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}\frac{L(1,\chi_{d_1})L(1,\chi_{d_2})}{p^2}\Bigg).\end{aligned}$$

We will prove in the next section (Theorem 3.1) that for any $c>0$,

$$\sum_{\substack{f\le 2\sqrt{x}\\ g\le 2\sqrt{x}}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}L(1,\chi_{d_1})L(1,\chi_{d_2})\log p = K_r x+O\Bigg(\frac{x}{\log^c x}\Bigg).$$

Then, by Theorem 3.1 and partial summation, the first sum of (7) is

$$\begin{aligned}&\frac{1}{\pi^2 x\log x}\Bigg(K_r x+O\Bigg(\frac{x}{\log^c x}\Bigg)\Bigg)+\frac{1}{\pi^2}\int_2^x\Bigg(K_r t+O\Bigg(\frac{t}{\log^c t}\Bigg)\Bigg)\Bigg(\frac{1+\log t}{t^2\log^2 t}\Bigg)\,dt\\ &\qquad\sim\frac{K_r}{\pi^2}\log\log x\end{aligned}$$

and similarly

$$\sum_{\substack{f\le 2\sqrt{x}\\ g\le 2\sqrt{x}}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}\frac{L(1,\chi_{d_1})L(1,\chi_{d_2})}{p^2}=O(1).$$

Then

$$\frac{1}{4}\sum_{B_r\le p\le x}\frac{H^2(r^2-4p)}{p^2}\sim\frac{K_r}{\pi^2}\log\log x$$

and inserting this in (6) we get

$$\frac{1}{16A^2B^2}\sum_{\substack{|a_1|,|a_2|\le A\\ |b_1|,|b_2|\le B}}\pi^r_{E_1,E_2}(x)\sim\frac{K_r}{\pi^2}\log\log x$$

for $A,B\ge x^{1+\varepsilon}$. Notice that, assuming Theorem 3.1, this shows Theorem 1.2.

3. Average values of product of Dirichlet L-functions

THEOREM 3.1. *Let r be an odd integer. Then, for any $c>0$,*

$$\sum_{f\le 2\sqrt{x}}\sum_{g\le 2\sqrt{x}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}L(1,\chi_{d_1})L(1,\chi_{d_2})\log p=K_rx+O\Big(\frac{x}{\log^c x}\Big),$$

where

$$K_r=3\prod_{p\mid r}\frac{p^2(p^2+1)}{(p^2-1)^2}\prod_{p\nmid r}\frac{p^2(p^4-2p^2-3p-1)}{(p+1)^3(p-1)^3}.$$

This section consists of a proof of Theorem 3.1. As r is odd, it follows from the definition of $S_{f,g}(x)$ that f,g are also odd, and that d_1,d_2 are congruent to 1 modulo 4. Also, any common factor between r and f would divide the primes $p\in S_{f,g}(x)$, which is impossible because $p>B_r=\max(3,r^2/4)$. Then the sum is empty unless $(2r,fg)=1$, and we can rewrite the sum of Theorem 3.1 as

$$\sum_{\substack{f,g\le 2\sqrt{x}\\ (2r,fg)=1}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}L(1,\chi_{d_1})L(1,\chi_{d_2})\log p$$

where

$$S_{f,g}(x)=\{B_r<p\le x: f^2\mid r^2-4p,\ g^2\mid r^2-4p\}.$$

Let

$$L(s)=L(s,\chi_{d_1})L(s,\chi_{d_2})=\sum_{m,n=1}^{\infty}\frac{\chi_{d_1}(m)\chi_{d_2}(n)}{(mn)^s}=\sum_{l=1}^{\infty}\frac{a_{d_1,d_2}(l)}{l^s},$$

where

$$a_{d_1,d_2}(l) = \sum_{mn=l} \chi_{d_1}(m)\chi_{d_2}(n). \tag{8}$$

We then have the trivial bound

$$a_{d_1,d_2}(l) \ll d(l) \ll l^{\varepsilon} \tag{9}$$

for any $\varepsilon > 0$, where $d(l)$ is the number of divisors of l. We need an expression for the truncated L-series of $L(1)$.

LEMMA 3.2. *Let $U > 0$. Then, for any $\varepsilon > 0$,*

$$L(1) = \sum_{l=1}^{\infty} \frac{a_{d_1,d_2}(l)}{l}\, e^{-l/U} + O\bigg(\frac{|d_1 d_2|^{3/16+\varepsilon}}{U^{1/2}}\bigg)$$

where the error term depends on ε.

Proof. We have the integral representation

$$e^{-1/U} = \frac{1}{2\pi i} \int\limits_{(1)} \Gamma(s+1)U^s\, \frac{ds}{s}$$

(see [M, p. 353] for a proof). Using this we have

$$\sum_{l=1}^{\infty} \frac{a_{d_1,d_2}(l)}{l}\, e^{-l/U} = \frac{1}{2\pi i} \int\limits_{(1)} L(s+1)\Gamma(s+1)U^s\, \frac{ds}{s}.$$

Now moving the line of integration from (1) to $(-1/2)$ and calculating the residue at $s = 0$ yields

$$\sum_{l=1}^{\infty} \frac{a_{d_1,d_2}(l)}{l}\, e^{-l/U} = L(1) + \frac{1}{2\pi i} \int\limits_{(-1/2)} L(s+1)\Gamma(s+1)U^s\, \frac{ds}{s}. \tag{10}$$

Recalling Burgess's result (see [Bur]), we have, for any $\varepsilon > 0$,

$$L(1/2+it) = L(1/2+it, \chi_{d_1})L(1/2+it, \chi_{d_2}) \ll_{\varepsilon} |d_1 d_2|^{3/16+\varepsilon},$$

and then

$$\frac{1}{2\pi i} \int\limits_{(-1/2)} L(s+1)\Gamma(s+1)U^s\, \frac{ds}{s} \ll_{\varepsilon} \frac{|d_1 d_2|^{3/16+\varepsilon}}{U^{1/2}}.$$

Inserting this in (10) completes the proof. ∎

Using Lemma 3.2, we write, for any $\varepsilon > 0$,

$$\sum_{\substack{f,g \le 2\sqrt{x} \\ (2r,fg)=1}} \frac{1}{fg} \sum_{p \in S_{f,g}(x)} L(1)\log p$$

$$= \sum_{\substack{f,g \le 2\sqrt{x} \\ (2r,fg)=1}} \frac{1}{fg} \sum_{p \in S_{f,g}(x)} \bigg\{ \sum_{l=1}^{\infty} \frac{a_{d_1,d_2}(l)}{l}\, e^{-l/U} + O\bigg(\frac{|d_1 d_2|^{3/16+\varepsilon}}{U^{1/2}}\bigg) \bigg\} \log p$$

$$= \sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}} \frac{1}{fg}\sum_{l=1}^{\infty}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)} a_{d_1,d_2}(l)\log p$$

$$+ O\Bigg(\frac{1}{U^{1/2}}\sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}|d_1d_2|^{3/16+\varepsilon}\log p\Bigg).$$

Replacing d_1 and d_2 by their definition, we can bound the sum in the error term by

$$\ll \frac{1}{U^{1/2}}\sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{(fg)^{11/8+2\varepsilon}}\sum_{p\in S_{f,g}(x)} p^{3/8+2\varepsilon}\log p$$

$$\ll \frac{x^{3/8+2\varepsilon}\log x}{U^{1/2}}\sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{(fg)^{11/8+2\varepsilon}}\sum_{p\in S_{f,g}(x)} 1 \ll \frac{x^{11/8+2\varepsilon}}{U^{1/2}},$$

and we have

$$\sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)} L(1)\log p$$

$$= \sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{fg}\sum_{l=1}^{\infty}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)} a_{d_1,d_2}(l)\log p + O\Bigg(\frac{x^{11/8+2\varepsilon}}{U^{1/2}}\Bigg) \tag{11}$$

for any $\varepsilon > 0$.

Let $1 < V \le 2\sqrt{x}$ be a parameter to be chosen later. We write the sum in (11) as

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}}\sum_{l=1}^{\infty}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)} a_{d_1,d_2}(l)\log p$$

$$+ \sum_{\substack{V<f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{fg}\sum_{l=1}^{\infty}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)} a_{d_1,d_2}(l)\log p.$$

For the sum over large values of f and g, we first notice that for such f and g, we have $[f^2,g^2]\,|\,r^2-4p$, which implies that $[f^2,g^2]\le 4x$. We also have $4p\equiv r^2 \bmod f^2$ and $4p\equiv r^2 \bmod g^2 \;\Leftrightarrow\; 4p\equiv r^2 \bmod [f^2,g^2]$. Then

$$(12)\qquad \Big|\sum_{\substack{V<f,g\le 2\sqrt{x}\\(2r,fg)=1\\[f^2,g^2]\le 4x}} \frac{1}{fg}\sum_{l=1}^{\infty}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)} a_{d_1,d_2}(l)\log p\Big|$$

$$\le \log x\Big|\sum_{l=1}^{\infty}\frac{d(l)}{l}\,e^{-l/U}\Big|\sum_{\substack{V<f,g\le 2\sqrt{x}\\(2r,fg)=1\\[f^2,g^2]\le 4x}}\frac{1}{fg}\sum_{\substack{p\le x\\4p\equiv r^2 \bmod [f^2,g^2]}} 1$$

$$\le x\log x\Big|\sum_{l=1}^{\infty}\frac{d(l)}{l}\,e^{-l/U}\Big|\sum_{\substack{V<f,g\le 2\sqrt{x}\\(2r,fg)=1\\[f^2,g^2]\le 4x}}\frac{1}{fg[f^2,g^2]}.$$

Lemma 3.3.

$$\sum_{l=1}^{\infty}\frac{d(l)}{l}\,e^{-l/U}\ll \log^2 U.$$

Proof. As in Lemma 3.2, we have the integral representation

$$\sum_{l=1}^{\infty}\frac{d(l)}{l}\,e^{-l/U}=\frac{1}{2\pi i}\int\limits_{(1)}\zeta^2(s+1)\Gamma(s+1)U^s\,\frac{ds}{s}$$

for the infinite sum that we want to bound, where $\zeta(s)$ is the Riemann zeta function. Note that since

$$\zeta(s)=\frac{1}{s-1}+\gamma+c_1(s-1)+\dots$$

(see [M, p. 63]), the residue of the integrand at $s=0$ is

$$\frac{1}{2}\log^2 U+2\gamma\log U+c_0,$$

where γ is the Euler constant and c_0 a constant. Now by moving the line of integration from (1) to $(-1/2)$ and calculating the residue at $s=0$ we get the desired bound. ∎

Using this lemma, we can bound (12) by

$$x\log x\log^2 U\sum_{\substack{V<f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{(f^2,g^2)}{f^3g^3}\le x\log x\log^2 U\sum_{\substack{V<f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{f^2g^2}$$

$$\ll \frac{x\log x\log^2 U}{V^2}$$

to get

$$\sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}L(1)\log p \tag{13}$$
$$=\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{l=1}^{\infty}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)}a_{d_1,d_2}(l)\log p$$
$$+O\Big(\frac{x^{11/8+2\varepsilon}}{U^{1/2}}\Big)+O\Big(\frac{x\log x\log^2 U}{V^2}\Big).$$

We now write the sum on the right hand side of (13) as

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{l\le U\log U}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)}a_{d_1,d_2}(l)\log p$$
$$+\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{l>U\log U}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)}a_{d_1,d_2}(l)\log p$$

for some parameter $U=U(x)$ to be chosen later.

We first estimate the sum for large values of l. For any $\varepsilon>0$, we have

$$\sum_{l>U\log U}\frac{d(l)}{l}\,e^{-l/U}\ll\sum_{l>U\log U}\frac{e^{-l/U}}{l^{1-\varepsilon}}\ll\frac{1}{(U\log U)^{1-\varepsilon}}\sum_{l>U\log U}e^{-l/U}$$
$$\ll\frac{1}{(U\log U)^{1-\varepsilon}}\int_{U\log U}^{\infty}e^{-t/U}\,dt=\frac{1}{(U\log U)^{1-\varepsilon}}$$

and then

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{l>U\log U}\frac{1}{l}\,e^{-l/U}\sum_{p\in S_{f,g}(x)}a_{d_1,d_2}(l)\log p$$
$$\ll x\log x\sum_{l>U\log U}\frac{d(l)}{l}\,e^{-l/U}\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg[f^2,g^2]}\ll\frac{x\log x\log^2 V}{(U\log U)^{1-\varepsilon}}.$$

Using this last result and (13), we find that for any $\varepsilon>0$,

$$\sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}}\frac{1}{fg}\sum_{p\in S_{f,g}(x)}L(1)\log p \tag{14}$$
$$=\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{l\le U\log U}\frac{1}{l}\,e^{-l/U}\sum_{p\in S_{f,g}(x)}a_{d_1,d_2}(l)\log p$$
$$+O\Big(\frac{x^{11/8+2\varepsilon}}{U^{1/2}}\Big)+O\Big(\frac{x\log x\log^2 U}{V^2}\Big)+O\Big(\frac{x\log x\log^2 V}{(U\log U)^{1-\varepsilon}}\Big).$$

We now estimate the sum of the right hand side of (14). By quadratic reciprocity,

$$\chi_{d_1}(m) = \chi_{d_1'}(m) \quad \text{if } d_1 \equiv d_1' \bmod (4m).$$

We then have

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{1}{fg} \sum_{l\le U\log U} \frac{e^{-l/U}}{l} \sum_{p\in S_{f,g}(x)} \log p \sum_{mn=l} \chi_{d_1}(m)\chi_{d_2}(n)$$

$$= \sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{1}{fg} \sum_{\substack{l\le U\log U\\ mn=l}} \frac{e^{-l/U}}{l} \sum_{\substack{a \bmod 4m\\ b \bmod 4n}} \left(\frac{a}{m}\right)\left(\frac{b}{n}\right) \sum_p{}^{*} \log p$$

where $\sum_p^*$ runs over primes p such that $p \in S_{f,g}(x)$ and $d_1 \equiv a \bmod (4m)$, $d_2 \equiv b \bmod (4n)$, i.e. the primes p such that $B_r < p \le x$ and

$$p \equiv (r^2 - af^2)/4 \bmod mf^2 \quad \text{and} \quad p \equiv (r^2 - bg^2)/4 \bmod ng^2.$$

If $(r^2 - af^2)/4 \not\equiv (r^2 - bg^2)/4 \bmod (mf^2, ng^2)$, there are no such primes. If the above congruence is satisfied, let $\theta = \theta(a, b, m, n, f, g)$ be the unique residue modulo $[mf^2, ng^2]$ which is congruent to $(r^2 - af^2)/4$ modulo mf^2, and congruent to $(r^2 - bg^2)/4$ modulo ng^2. If $(r^2 - af^2)/4 \not\equiv (r^2 - bg^2)/4 \bmod (mf^2, ng^2)$, we set $\theta = 0$. Then we can rewrite the last sum as

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{1}{fg} \sum_{\substack{l\le U\log U\\ mn=l}} \frac{1}{l}\, e^{-l/U} \sum_{\substack{a \bmod 4m\\ b \bmod 4n}} \left(\frac{a}{m}\right)\left(\frac{b}{n}\right) \sum_{\substack{B_r<p\le x\\ p\equiv\theta \bmod [mf^2,ng^2]}} \log p.$$

Let a, n be positive integers with $(a, n) = 1$. Following the standard notation, we write

$$\psi(x; n, a) = \sum_{\substack{p\le x\\ p\equiv a \bmod n}} \log p = \frac{x}{\phi(n)} + E(x; n, a).$$

With this notation, we rewrite the last sum as

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{1}{fg} \sum_{\substack{l\le U\log U\\ mn=l}} \frac{1}{l}\, e^{-l/U} \sum_{\substack{a \bmod 4m\\ b \bmod 4n}}{}^{*} \left(\frac{a}{m}\right)\left(\frac{b}{n}\right)$$

$$\times \left(\frac{x}{\phi([mf^2, ng^2])} + E(x; [mf^2, ng^2], \theta)\right)$$

where $\sum^*_{\substack{a \bmod 4m\\ b \bmod 4n}}$ means that the sum runs over invertible residues a, b modulo m, n respectively such that $(r^2 - af^2)/4 \equiv (r^2 - bg^2)/4 \bmod (mf^2, ng^2)$, and θ is invertible modulo $[mf^2, ng^2]$, or equivalently $(r^2 - af^2, 4m) = 4$ and $(r^2 - bg^2, 4n) = 4$. We then define

$$(15)\qquad c^r_{f,g}(m,n)=\sum_{\substack{a\,(4m)^*\\(r^2-af^2,4m)=4}}\ \sum_{\substack{b\,(4n)^*\\(r^2-bg^2,4n)=4\\(r^2-af^2)/4\equiv(r^2-bg^2)/4\bmod(mf^2,ng^2)}}\left(\frac{a}{m}\right)\left(\frac{b}{n}\right),$$

where $\sum_{a\,(4m)^*}$ denotes the sum over a complete set of invertible residues modulo $4m$. Using this notation, we have

$$(16)\qquad \sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{l\le U\log U}\frac{e^{-l/U}}{l}\sum_{p\in S_{f,g}(x)}a_{d_1,d_2}(l)\log p$$

$$=x\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{\substack{l\le U\log U\\mn=l}}\frac{e^{-l/U}}{l}\frac{c^r_{f,g}(m,n)}{\phi([mf^2,ng^2])}$$

$$+\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{\substack{l\le U\log U\\l=mn}}\frac{e^{-l/U}}{l}\sum^*_{\substack{a\bmod 4m\\b\bmod 4n}}\left(\frac{a}{m}\right)\left(\frac{b}{n}\right)E(x;[mf^2,ng^2],\theta).$$

We first deal with the second sum of (16), which is bounded by

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{mn\le U\log U}\frac{1}{mn}\sum^*_{\substack{a\bmod 4m\\b\bmod 4n}}|E(x;[mf^2,ng^2],\theta)|.$$

In the sum $\sum^*_{\substack{a\bmod 4m\\b\bmod 4n}}$, each pair of residues a,b modulo $4m$ and $4n$ respectively yields a different residue θ modulo $[mf^2,ng^2]$. We then have

$$\sum_{mn\le U\log U}\frac{1}{mn}\sum^*_{\substack{a\bmod 4m\\b\bmod 4n}}|E(x;[mf^2,ng^2],\theta)|$$

$$\le\sum_{mn\le U\log U}\frac{1}{mn}\sum_{\theta\bmod[mf^2,ng^2]}|E(x;[mf^2,ng^2],\theta)|$$

$$\ll f^2g^2\sum_{l\le U\log Uf^2g^2}\frac{1}{l}\sum_{\theta\bmod l}c(l)|E(x;l,\theta)|$$

where $c(l)$ is the number of ways that we can write $l=[mf^2,ng^2]$. More generally, we have

LEMMA 3.4. *Let n be a positive integer, and let $C(n)$ be the number of ways to write $n=[n_1,n_2]$ for any positive integers n_1 and n_2. Then $C(n)\le 2^{\nu(n)}d(n)$, where $\nu(n)$ is the number of distinct prime factors of n and $d(n)$ is the number of divisors of n.*

Proof. Let $n=\prod_{i=1}^r p_i^{\alpha_i}$ with $\alpha_i\ge 1$ for $i=1,\dots,r$. Then $n=[n_1,n_2]$ implies that $n_1=\prod_{i=1}^r p_i^{\beta_i}$ and $n_2=\prod_{i=1}^r p_i^{\gamma_i}$ with $0\le\beta_i,\gamma_i\le\alpha_i$ and

$\max(\beta_i, \gamma_i) = \alpha_i$ for $i = 1, \dots, r$. As there are $2\alpha_i + 1$ such pairs (β_i, γ_i) for each i, we have

$$C(n) = \prod_{i=1}^{r}(2\alpha_i + 1) \le \prod_{i=1}^{r} 2(\alpha_i + 1) = 2^{\nu(n)} d(n). \ \blacksquare$$

Using this result in the last bound, we get

$$\begin{aligned}
&\sum_{mn \le U \log U} \frac{1}{mn} \sideset{}{^*}\sum_{\substack{a \bmod 4m \\ b \bmod 4n}} |E(x; [mf^2, ng^2], \theta)| \\
&\qquad \ll f^2 g^2 \sum_{l \le U \log U f^2 g^2} \frac{d^2(l)}{l} \sum_{\theta \bmod l} |E(x; l, \theta)| \\
&\qquad \le f^2 g^2 \Big(\sum_{\substack{l \le U \log U f^2 g^2 \\ \theta \bmod l}} \frac{d^4(l)}{l^2} \Big)^{1/2} \Big(\sum_{\substack{l \le U \log U f^2 g^2 \\ \theta \bmod l}} E^2(x; l, \theta) \Big)^{1/2}
\end{aligned}$$

using the Cauchy–Schwarz inequality.

For the first parenthesis, we use the result of Ramanujan [Wil]

$$\sum_{l \le N} d^r(l) \sim A_r N \log^{2^r - 1}(N)$$

for $r \ge 2$ and A_r an absolute constant with $r = 4$. If we use partial summation, and the fact that $f, g \le V$, this gives

$$\Big(\sum_{\substack{l \le U \log U f^2 g^2 \\ \theta \bmod l}} \frac{d^4(l)}{l^2} \Big)^{1/2} \le \Big(\sum_{l \le U \log U f^2 g^2} \frac{d^4(l)}{l} \Big)^{1/2} \ll \log^8(V^4 U \log U).$$

For the second parenthesis, we apply the theorem of Barban–Davenport–Halberstam [Dav, p. 169]. This gives

$$\Big(\sum_{\substack{l \le V^4 U \log U \\ \theta \bmod l}} E^2(x; l, \theta) \Big)^{1/2} \ll (V^4 U x \log U \log x)^{1/2}$$

whenever

$$\frac{x}{\log^A x} \le V^4 U \log U \le x \quad \text{for some } A > 0. \tag{17}$$

Finally, summing over f, g gives

$$\begin{aligned}
&\sum_{\substack{f,g \le V \\ (2r, fg) = 1}} \frac{1}{fg} \sum_{\substack{l \le U \log U \\ l = mn}} \frac{e^{-l/U}}{l} \sideset{}{^*}\sum_{\substack{a \bmod 4m \\ b \bmod 4n}} \Big(\frac{a}{m}\Big)\Big(\frac{b}{n}\Big) E(x; [mf^2, ng^2], \theta) \qquad (18) \\
&\qquad \ll (V^4 U x \log U \log x)^{1/2} \log^8(V^4 U \log U) \sum_{\substack{f,g \le V \\ (2r, fg) = 1}} fg \\
&\qquad \ll V^6 (U x \log U \log x)^{1/2} \log^8 x
\end{aligned}$$

whenever (17) holds.

We now have to evaluate the first sum of (16). We first rewrite the sum as

$$\begin{aligned}(19)\qquad x \sum_{\substack{f,g=1\\(2r,fg)=1}}^{\infty} \frac{1}{fg} \sum_{m,n=1}^{\infty} \frac{c_{f,g}^r(m,n)e^{-mn/U}}{mn\phi([mf^2,ng^2])} \\ - x \sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{1}{fg} \sum_{\substack{l>U\log U\\mn=l}} \frac{e^{-l/U}}{l} \frac{c_{f,g}^r(m,n)}{\phi([mf^2,ng^2])} \\ - x \sum_{\substack{f,g>V\\(2r,fg)=1}} \frac{1}{fg} \sum_{m,n=1}^{\infty} \frac{c_{f,g}^r(m,n)e^{-mn/U}}{mn\phi([mf^2,ng^2])}.\end{aligned}$$

We first deal with the two error terms of (19). This is done using the bound

$$(20)\qquad c_{f,g}^r(m,n) \ll \frac{mn}{\kappa(mn)(m,n)},$$

which is shown in Lemma 4.8. Using the notation of Section 4, we write $k=(f,g)$ and $f=kf'$ and $g=kg'$. If $(f',n)\ne 1$ or $(g',m)\ne 1$, we have $c_{f,g}^r(m,n)=0$ by Lemma 4.3(i). If $(f',n)=(g',m)=1$, then $(mf^2,ng^2)=(m,n)(f^2,g^2)$. This gives

$$\begin{aligned}\frac{c_{f,g}^r(m,n)}{\phi([mf^2,ng^2])} &= \frac{(mf^2,ng^2)c_{f,g}^r(m,n)}{\phi(mnf^2g^2)} = \frac{(m,n)(f^2,g^2)c_{f,g}^r(m,n)}{\phi(mnf^2g^2)} \\ &\le \frac{(m,n)(f^2,g^2)c_{f,g}^r(m,n)}{\phi(mn)\phi(f^2)\phi(g^2)} \ll \frac{mn(f^2,g^2)}{\kappa(mn)\phi(mn)\phi(f^2)\phi(g^2)}\end{aligned}$$

by the bound (20) for $c_{f,g}^r(m,n)$. Inserting this in the first error term of (19), we get

$$\begin{aligned}x \sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{1}{fg} \sum_{\substack{l>U\log U\\mn=l}} \frac{e^{-l/U}}{l} \frac{c_{f,g}^r(m,n)}{\phi([mf^2,ng^2])} \\ \ll x \sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{(f^2,g^2)}{fg\phi(f^2)\phi(g^2)} \sum_{l>U\log U} \frac{d(l)}{\kappa(l)\phi(l)}.\end{aligned}$$

It is shown in [DP, Lemma 3.4] that

$$(21)\qquad \sum_{l=1}^{\infty} \frac{l^{3/2}}{\kappa(l)\phi(l)}\, l^{-s}$$

converges for $\mathrm{Re}(s)>1$. Clearly, this implies that $\sum_{l=1}^{\infty}\frac{d(l)}{\kappa(l)\phi(l)}$ converges. Furthermore, using the Wiener–Ikehara Tauberian Theorem and partial summation as in the proof of [DP, Lemma 3.4], we can show that for any $\varepsilon>0$,

$$\sum_{l>U\log U}\frac{d(l)}{\kappa(l)\phi(l)}\ll (U\log U)^{-1/2+\varepsilon}. \tag{22}$$

Also,

$$\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{(f^2,g^2)}{fg\phi(f^2)\phi(g^2)}\le 2\sum_{\substack{f,g\le V\\f\le g}}\frac{1}{g^2\phi(f)\phi(g)}\le 2\bigg(\sum_{f\le V}\frac{1}{f\phi(f)}\bigg)^2=O(1)$$

and then

$$x\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{\substack{l>U\log U\\mn=l}}\frac{e^{-l/U}}{l}\frac{c^r_{f,g}(m,n)}{\phi([mf^2,ng^2])}=O\bigg(\frac{x}{(U\log U)^{1/2-\varepsilon}}\bigg). \tag{23}$$

We now look at the second error term of (19). As above, we have

$$\begin{aligned}x\sum_{\substack{f,g>V\\(2r,fg)=1}}\frac{1}{fg}\sum_{m,n=1}^{\infty}\frac{c^r_{f,g}(m,n)e^{-mn/U}}{mn\phi([mf^2,ng^2])}&\ll x\sum_{f,g>V}\frac{(f^2,g^2)}{fg\phi(f^2)\phi(g^2)}\\&\le x\bigg(\sum_{f>V}\frac{1}{f\phi(f)}\bigg)^2\ll\frac{x}{V^{2-2\varepsilon}}\end{aligned}$$

for any positive $\varepsilon>0$, as $\phi(n)\gg n^{1-\varepsilon}$ for any positive $\varepsilon>0$ [HW, p. 267]. Then, by (19), we get

$$\begin{aligned}&x\sum_{\substack{f,g\le V\\(2r,fg)=1}}\frac{1}{fg}\sum_{l\le U\log U}\frac{e^{-l/U}}{l}\sum_{mn=l}\frac{c^r_{f,g}(m,n)}{\phi([mf^2,ng^2])}\qquad(24)\\&=x\sum_{\substack{f,g=1\\(2r,fg)=1}}^{\infty}\frac{1}{fg}\sum_{m,n=1}^{\infty}\frac{c^r_{f,g}(m,n)e^{-mn/U}}{mn\phi([mf^2,ng^2])}+O\bigg(\frac{x}{(U\log U)^{1/2-\varepsilon}}\bigg)+O\bigg(\frac{x}{V^{2-2\varepsilon}}\bigg).\end{aligned}$$

Finally, we remove the exponential $e^{-l/U}$ from the main term. We have, for any $c_1>0$,

$$\begin{aligned}&x\sum_{\substack{f,g,m,n=1\\(2r,fg)=1}}^{\infty}\frac{c^r_{f,g}(m,n)e^{-mn/U}}{mnfg\phi([mf^2,ng^2])}\\&\qquad=\frac{x}{2\pi i}\sum_{\substack{f,g,m,n=1\\(2r,fg)=1}}^{\infty}\frac{c^r_{f,g}(m,n)}{fgmn\phi([mf^2,ng^2])}\int\limits_{(c_1)}\Gamma(s)\bigg(\frac{U}{mn}\bigg)^s ds\\&\qquad=\frac{x}{2\pi i}\int\limits_{(c_1)}\bigg(\sum_{\substack{f,g,m,n=1\\(2r,fg)=1}}^{\infty}\frac{c^r_{f,g}(m,n)}{fg(mn)^{s+1}\phi([mf^2,ng^2])}\bigg)\Gamma(s)U^s\,ds.\end{aligned}$$

Using the bound (20) and working as above, we get

$$\sum_{\substack{f,g,m,n=1\\(2r,fg)=1}}^{\infty} \frac{c_{f,g}^r(m,n)}{(mn)^{s+1}fg\phi([mf^2,ng^2])} \ll \sum_{l=1}^{\infty} \frac{d(l)}{\kappa(l)\phi(l)l^s}$$

and from (21), the sum converges for $\mathrm{Re}(s) > -1/2+\varepsilon$, for any $\varepsilon > 0$. Then we can move the line of integration to any $-1/2+\varepsilon < \gamma < 0$, say $\gamma = -1/4$. As $\Gamma(s)$ has a simple pole at $s = 0$, by using Cauchy's residue theorem and working as in the proof of Lemma 3.2, we get

$$x \sum_{\substack{f,g,m,n=1\\(2r,fg)=1}}^{\infty} \frac{c_{f,g}^r(m,n)}{fgmn\phi([mf^2,ng^2])}\, e^{-mn/U} = x \sum_{\substack{f,g,m,n=1\\(2r,fg)=1}}^{\infty} \frac{c_{f,g}^r(m,n)}{fgmn\phi([mf^2,ng^2])} + O\bigg(\frac{x}{U^{1/4}}\bigg)$$

and by (24), we have

$$\begin{aligned}(25)\quad & x \sum_{\substack{f,g\le V\\(2r,fg)=1}} \frac{1}{fg} \sum_{l\le U\log U} \frac{e^{-l/U}}{l} \sum_{mn=l} \frac{c_{f,g}^r(m,n)}{\phi([mf^2,ng^2])}\\ &= x \sum_{\substack{f,g,m,n=1\\(2r,fg)=1}}^{\infty} \frac{c_{f,g}^r(m,n)}{fgmn\phi([mf^2,ng^2])} + O\bigg(\frac{x}{(U\log U)^{1/2-\varepsilon}} + \frac{x}{V^{2-2\varepsilon}} + \frac{x}{U^{1/4}}\bigg).\end{aligned}$$

This finishes the proof of Theorem 3.1. Indeed, inserting (25) and (18) in (16) and (14), we get

$$\begin{aligned}\sum_{\substack{f,g\le 2\sqrt{x}\\(2r,fg)=1}} \frac{1}{fg} \sum_{p\in S_{f,g}^r(x)} & L(1,\chi_{d_1})L(1,\chi_{d_2})\log p\\ &= K_r x + O\bigg(\frac{x}{(U\log U)^{1/2-\varepsilon}} + \frac{x}{V^{2-2\varepsilon}} + \dots\\ &\quad \dots + \frac{x}{U^{1/4}} + V^6(Ux\log U\log x)^{1/2}\log^8 x\\ &\quad + \frac{x^{11/8+2\varepsilon}}{U^{1/2}} + \frac{x\log x\log^2 U}{V^2} + \frac{x\log x\log^2 V}{(U\log U)^{1-\varepsilon}}\bigg)\end{aligned}$$

for all $\varepsilon > 0$, with

$$(26)\qquad K_r = \sum_{\substack{f,g=1\\(2r,fg)=1}}^{\infty} \frac{1}{fg} \sum_{mn=1}^{\infty} \frac{c_{f,g}^r(m,n)}{mn\phi([mf^2,ng^2])}.$$

We choose $U = x/\log^{\alpha} x$ and $V = \log^{\beta} x$ for positive integers α, β such that

$\alpha - 4\beta - 1 \geq 1$ ensuring that the condition (17) is satisfied. Then

$$\sum_{\substack{f,g\leq 2\sqrt{x}\\(2r,fg)=1}} \frac{1}{fg} \sum_{p\in S^r_{f,g}(x)} L(1,\chi_{d_1})L(1,\chi_{d_2})\log p$$
$$= K_r x + O\bigg(\frac{x}{\log^{\beta} x} + \frac{x}{\log^{\alpha/2-6\beta-9} x}\bigg) = K_r x + O\bigg(\frac{x}{\log^{c} x}\bigg)$$

for any $c > 0$ for an appropriate choice of α and β. This proves Theorem 3.1, provided that we get the Euler product expansion for the constant K_r of (26). This is done in the next section.

4. The constant. In this section, we express the constant K_r as an Euler product of local factors. We first prove that the coefficients $c^r_{f,g}(m,n)$ are multiplicative, and we then use this result to prove a bound on the size of $c^r_{f,g}(m,n)$ needed to complete the proof of Theorem 3.1 (see Lemma 4.8). Moreover, we also use the multiplicativity of these coefficients to derive the Euler product for the constant K_r in Theorem 3.1.

4.1. *Multiplicativity of the coefficients $c^r_{f,g}(m,n)$.* For all this section, let r be an odd integer, and let f and g be positive odd integers. Let $k = (f,g)$, and let f', g' be such that $f = f'k$ and $g = g'k$. Let m and n be positive integers. For a prime p and an integer n, the valuation $v_p(n)$ is the power of p appearing in the integer n.

Definition 4.1. (1) Let

$$c^r_f(m) = \sum_{\substack{a\,(4m)^*\\(r^2-af^2,4m)=4}} \left(\frac{a}{m}\right).$$

(2) For any invertible residue a modulo $4m$, let

$$c^r_{f,g}(n;m,a) = \sum_{\substack{b\,(4n)^*\\(r^2-bg^2,4n)=4\\(r^2-bg^2)/4\equiv(r^2-af^2)/4 \bmod (mf^2,ng^2)}} \left(\frac{b}{n}\right).$$

(3) Let

$$c^r_{f,g}(m,n) = \sum_{\substack{a\,(4m)^*\\(r^2-af^2,4m)=4}} \left(\frac{a}{m}\right) c^r_{f,g}(n;m,a).$$

Of course, this definition agrees with the previous definition of $c^r_{f,g}(m,n)$ in (15).

DEFINITION 4.2. A function $F(m,n)$ defined on the set of positive integers m, n is *multiplicative* if it satisfies

$$F(m,n) = \prod_{p|mn} F(p^{v_p(m)}, p^{v_p(n)}).$$

LEMMA 4.3. (i) *If* $(m,g') \neq 1$ *or* $(n,f') \neq 1$, *then* $c^r_{f,g}(m,n) = 0$.
(ii) *If* $(n_1,n_2) = 1$, *then* $c^r_{f,g}(n_1n_2;m,a) = c^r_{f,g}(n_1;m,a)c^r_{f,g}(n_2;m,a)$.

Proof. (i) As

$$(r^2 - bg^2)/4 \equiv (r^2 - af^2)/4 \bmod (mf^2, ng^2)$$
$$\Leftrightarrow\ (af'^2 - bg'^2)/4 \equiv 0 \bmod (mf'^2, ng'^2),$$

we have

$$c^r_{f,g}(m,n) = \sum_{\substack{a\,(4m)^*\\(r^2-af^2,4m)=4}} \left(\frac{a}{m}\right) \sum_{\substack{b\,(4n)^*\\(r^2-bg^2,4n)=4\\(af'^2-bg'^2)/4\equiv 0 \bmod (mf'^2,ng'^2)}} \left(\frac{b}{n}\right).$$

Suppose there is a prime p dividing (n,f'). Then $c^r_{f,g}(m,n) = 0$ because $b \equiv 0 \bmod p$, as p divides (mf'^2, ng'^2) and $(g',p) = 1$. The case $(m,g') \neq 1$ is similar.

(ii) From the Generalised Chinese Remainder Theorem, there is a bijection between the set of invertible residues b modulo $4n_1n_2$ such that $(r^2-bg^2, 4n_1n_2) = 4$ and the set of pairs (b_1,b_2) of invertible residues modulo $4n_1$ and $4n_2$ respectively such that $(r^2 - b_1g^2, 4n_1) = 4$ and $(r^2 - b_2g^2, 4n_2) = 4$. Furthermore,

$$(af^2 - bg^2)/4 \equiv 0 \bmod (mf^2, n_1n_2g^2)$$

if and only if

$$(af^2 - b_1g^2)/4 \equiv 0 \bmod (mf^2, n_1g^2), \quad (af^2 - b_2g^2)/4 \equiv 0 \bmod (mf^2, n_2g^2)$$

as the least common multiple of (mf^2, n_1g^2) and (mf^2, n_2g^2) is $(mf^2, n_1n_2g^2)$. This proves the result. ∎

LEMMA 4.4. *Let* m_1, m_2, n_1, n_2 *be positive integers such that* $(m_1,m_2) = (n_1,n_2) = (m_1,n_2) = (m_2,n_1) = 1$. *Then*

$$c^r_{f,g}(m_1m_2, n_1n_2) = c^r_{f,g}(m_1,n_1)c^r_{f,g}(m_2,n_2).$$

Equivalently, the functions $c^r_{f,g}(m,n)$ *are multiplicative.*

Proof. Let $n = n_1n_2$ and $m = m_1m_2$. If $(m,g') \neq 1$, or $(n,f') \neq 1$, then $c^r_{f,g}(m_1m_2, n_1n_2) = 0$ by Lemma 4.3(i). But then one of $(m_1,g'), (m_2,g')$, $(n_1,f'), (n_2,f')$ is not 1, and either

$$c^r_{f,g}(m_1,n_1) = 0 \quad \text{or} \quad c^r_{f,g}(m_2,n_2) = 0$$

by Lemma 4.3(i). This proves the lemma in this case, and we now suppose that $(m,g') = (n,f') = 1$. Using Lemma 4.3(ii), we have

$$c^r_{f,g}(m, n_1n_2) = \sum_{\substack{a\ (4m)^*\\(r^2-af^2,4m)=4}} \left(\frac{a}{m}\right) c^r_{f,g}(n_1; m, a)c^r_{f,g}(n_2; m, a)$$

with

$$c^r_{f,g}(n_1; m, a) = \sum_{\substack{b_1\ (4n_1)^*\\(r^2-b_1g^2,4n_1)=4\\(af'^2-b_1g'^2)/4\equiv 0 \bmod (mf'^2,n_1g'^2)}} \left(\frac{b_1}{n_1}\right).$$

By hypothesis, $(mf'^2, n_1g'^2) = (m_1f'^2, n_1g'^2)$, and

$$c^r_{f,g}(n_1; m, a) = c^r_{f,g}(n_1; m_1, a_1)$$

where a_1 is the reduction of a modulo $4m_1$. Similarly, we have

$$c^r_{f,g}(n_2; m, a) = c^r_{f,g}(n_2; m_2, a_2)$$

where a_2 is the reduction of a modulo $4m_2$.

Then, applying the Generalised Chinese Remainder Theorem, we have

$$\begin{aligned} c^r_{f,g}(m, n) &= \sum_{\substack{a\ (4m_1m_2)^*\\(r^2-af^2,4m_1m_2)=4}} \left(\frac{a}{m_1m_2}\right) c^r_{f,g}(n_1; m_1, a_1)c^r_{f,g}(n_2; m_2, a_2)\\ &= \sum_{\substack{a_1\ (4m_1)^*\\(r^2-a_1f^2,4m_1)=4}} \left(\frac{a_1}{m_1}\right) c^r_{f,g}(n_1; m_1, a_1)\\ &\quad\times \sum_{\substack{a_2\ (4m_2)^*\\(r^2-a_2f^2,4m_2)=4}} \left(\frac{a_2}{m_2}\right) c^r_{f,g}(n_2; m_2, a_2) \end{aligned}$$

which proves the lemma. ∎

4.2. *Bounds for the coefficients $c^r_{f,g}(m, n)$.* We prove in this section that the functions $c^r_{f,g}(m, n)$ satisfy the bound (20). This is the result needed to complete the proof of Theorem 3.1.

LEMMA 4.5. *Let p be a prime, and let $\alpha, \beta \geq 0$ be integers. Then*

(i) $c^r_{f,g}(1, 1) = 1$;

(ii) *If $p \nmid fg$ (i.e. $v_p(f) = v_p(g) = 0$), then $c^r_{f,g}(p^\alpha, p^\beta) = c^r_{1,1}(p^\alpha, p^\beta)$;*

(iii) *If $p \mid fg$ and $v_p(f) = v_p(g)$, then $c^r_{f,g}(p^\alpha, p^\beta) = c^r_{p,p}(p^\alpha, p^\beta)$;*

(iv) *Suppose $p \mid fg$ and $v_p(f) \neq v_p(g)$. If $\alpha, \beta \geq 1$, then $c^r_{f,g}(p^\alpha, p^\beta) = 0$. If $\alpha = 0$ and $\beta \geq 1$, then $c^r_{f,g}(p^\alpha, p^\beta) = 0$ whenever $v_p(g) < v_p(f)$ and $c^r_{f,g}(p^\alpha, p^\beta) = c^r_p(p^\beta)$ whenever $v_p(g) > v_p(f)$. If $\alpha \geq 1$ and $\beta = 0$, then $c^r_{f,g}(p^\alpha, p^\beta) = 0$ whenever $v_p(f) < v_p(g)$ and $c^r_{f,g}(p^\alpha, p^\beta) = c^r_p(p^\alpha)$ whenever $v_p(f) > v_p(g)$.*

Proof. (i) By definition.

(ii) By definition,

$$c^r_{1,1}(p^\alpha,p^\beta)=\sum_{\substack{a\,(4p^\alpha)^*\\(r^2-a,4p^\alpha)=4}}\left(\frac{a}{p^\alpha}\right)\sum_{\substack{b\,(4p^\beta)^*\\(r^2-b,4p^\beta)=4\\(a-b)/4\equiv 0 \bmod (p^\alpha,p^\beta)}}\left(\frac{b}{p^\beta}\right).$$

As $(f,2p)=(g,2p)=1$, there is a bijection between the invertible residues modulo $4p^\alpha$ (respectively $4p^\beta$) and the set of af^2 (respectively bg^2), where a (respectively b) runs over the set of invertible residues modulo $4p^\alpha$ (respectively $4p^\beta$). This gives

$$c^r_{1,1}(p^\alpha,p^\beta)=\sum_{\substack{a\,(4p^\alpha)^*\\(r^2-af^2,4p^\alpha)=4}}\left(\frac{af^2}{p^\alpha}\right)\sum_{\substack{b\,(4p^\beta)^*\\(r^2-bg^2,4p^\beta)=4\\(af^2-bg^2)/4\equiv 0 \bmod (p^\alpha,p^\beta)}}\left(\frac{bg^2}{p^\beta}\right).$$

As

$$(af^2-bg^2)/4\equiv 0 \bmod (p^\alpha,p^\beta)\ \Leftrightarrow\ (af^2-bg^2)/4\equiv 0 \bmod (p^\alpha f^2,p^\beta g^2)$$

and

$$\left(\frac{af^2}{p^\alpha}\right)=\left(\frac{a}{p^\alpha}\right),\qquad \left(\frac{bg^2}{p^\beta}\right)=\left(\frac{b}{p^\beta}\right)$$

we get $c^r_{1,1}(p^\alpha,p^\beta)=c^r_{f,g}(p^\alpha,p^\beta)$.

(iii) As $p\,|\,fg$, and $v_p(f)=v_p(g)$, p is odd, and we have

$$(af^2-bg^2)/4\equiv 0 \bmod (p^\alpha f^2,p^\beta g^2)\ \Leftrightarrow\ af'^2\equiv bg'^2 \bmod (p^\alpha,p^\beta).$$

Let $h=f'^{-2}g'^2$ modulo $4p^\beta$. Then there is a bijection between the set of invertible residues b modulo $4p^\beta$ and the set of hb, where b runs over the invertible residues b modulo $4p^\beta$. Then

$$\begin{aligned}c^r_{p,p}(p^\alpha,p^\beta)&=\sum_{\substack{a\,(4p^\alpha)^*\\(r^2-ap^2,4p^\alpha)=4}}\left(\frac{a}{p^\alpha}\right)\sum_{\substack{b\,(4p^\beta)^*\\(r^2-bp^2,4p^\beta)=4\\a\equiv b \bmod (p^\alpha,p^\beta)}}\left(\frac{b}{p^\beta}\right)\\&=\sum_{\substack{a\,(4p^\alpha)^*\\(r^2-ap^2,4p^\alpha)=4}}\left(\frac{a}{p^\alpha}\right)\sum_{\substack{b\,(4p^\beta)^*\\(r^2-hbp^2,4p^\beta)=4\\a\equiv hb \bmod (p^\alpha,p^\beta)}}\left(\frac{bh}{p^\beta}\right).\end{aligned}$$

As $(r^2-ap^2,4p^\alpha)=4$ if and only if $(r^2-af^2,4p^\alpha)=4$, $(r^2-hbp^2,4p^\beta)=4$ if and only if $(r^2-bg^2,4p^\beta)=4$, and

$$\left(\frac{bh}{p^\beta}\right)=\left(\frac{b}{p^\beta}\right)$$

we get $c^r_{p,p}(p^\alpha,p^\beta)=c^r_{f,g}(p^\alpha,p^\beta)$.

(iv) Suppose that $p \mid fg$, and $v_p(f) \neq v_p(g)$. If $\alpha, \beta \geq 1$, then one of (p^α, g') or (p^β, f') is divisible by p. Then $c^r_{f,g}(p^\alpha, p^\beta) = 0$ by Lemma 4.3(i).

If $\alpha = 0$, $\beta \geq 1$ and $v_p(f) > v_p(g)$, then (p^β, f') is divisible by p and $c^r_{f,g}(p^\alpha, p^\beta) = 0$ by Lemma 4.3(i). If $\alpha = 0$, $\beta \geq 1$ and $v_p(f) < v_p(g)$, then

$$c^r_{f,g}(1, p^\beta) = \sum_{\substack{b \,(4p^\beta)^* \\ (r^2 - bg^2, 4p^\beta) = 4 \\ (af'^2 - bg'^2)/4 \equiv 0 \bmod (f'^2, p^\beta g'^2)}} \left(\frac{b}{p^\beta}\right)$$

is equal to $c_g(p^\beta)$ as $(f'^2, p^\beta g'^2) = 1$. Finally, from [DP, Lemma 3.3(3)], $c^r_g(p^\beta) = c^r_p(p^\beta)$. The proof is similar for $\alpha \geq 1$, $\beta = 0$ and $v_p(f) \neq v_p(g)$. ∎

LEMMA 4.6. *Let* $\alpha \geq 0$.

(i) *For* p *odd*,

$$\frac{c^r_1(p^\alpha)}{p^{\alpha-1}} = \begin{cases} -\left(\dfrac{r^2}{p}\right) & \text{when } \alpha \text{ is odd}, \\ p - 1 - \left(\dfrac{r^2}{p}\right) & \text{when } \alpha \text{ is even}. \end{cases}$$

(ii) *For* p *odd*,

$$\frac{c^r_p(p^\alpha)}{p^{\alpha-1}} = \begin{cases} 0 & \text{when } p \mid r, \\ p - 1 & \text{when } \alpha \text{ is even and } p \nmid r, \\ 0 & \text{when } \alpha \text{ is odd and } p \nmid r. \end{cases}$$

(iii)

$$\frac{c^r_1(2^\alpha)}{2^{\alpha-1}} = (-1)^\alpha.$$

Proof. This is [DP, Lemma 3.3]. ∎

LEMMA 4.7. *Let* $\alpha, \beta \geq 0$, *not both* 0.

(i) *For* p *odd*,

$$\frac{c^r_{1,1}(p^\alpha, p^\beta)}{p^{\max(\alpha,\beta)-1}} = \begin{cases} -\left(\dfrac{r^2}{p}\right) & \text{when } \alpha + \beta \text{ is odd}, \\ p - 1 - \left(\dfrac{r^2}{p}\right) & \text{when } \alpha + \beta \text{ is even}. \end{cases}$$

(ii) *For* p *odd*,

$$\frac{c^r_{p,p}(p^\alpha, p^\beta)}{p^{\max(\alpha,\beta)-1}} = \begin{cases} 0 & \text{when } p \mid r, \\ p - 1 & \text{when } \alpha + \beta \text{ is even and } p \nmid r, \\ 0 & \text{when } \alpha + \beta \text{ is odd and } p \nmid r. \end{cases}$$

(iii)

$$\frac{c^r_{1,1}(2^\alpha, 2^\beta)}{2^{\max(\alpha,\beta)-1}} = (-1)^{\alpha+\beta}.$$

Proof. (i) If $\alpha = 0$, then $c^r_{1,1}(1, p^\beta) = c^r_1(p^\beta)$, and the result follows from Lemma 4.6(i). Similarly for $\beta = 0$. We then suppose that $\alpha, \beta \geq 1$, and without loss of generality that $\alpha \leq \beta$. As p is odd, we have

$$\begin{aligned} c^r_{1,1}(p^\alpha, p^\beta) &= \sum_{\substack{a\,(p^\alpha)^* \\ (r^2-a,p)=1}} \left(\frac{a}{p}\right)^\alpha \sum_{\substack{b\,(p^\beta)^* \\ (r^2-b,p)=1 \\ b\equiv a \bmod p^\alpha}} \left(\frac{b}{p}\right)^\beta \\ &= p^{\beta-\alpha} \sum_{\substack{a\,(p^\alpha)^* \\ (r^2-a,p)=1}} \left(\frac{a}{p}\right)^{\alpha+\beta} = p^{\beta-1} \sum_{\substack{a\,(p)^* \\ a\not\equiv r^2 \bmod p}} \left(\frac{a}{p}\right)^{\alpha+\beta}. \end{aligned}$$

This proves (i).

(ii) As in (i), we can suppose that $1 \leq \alpha \leq \beta$. As p is odd, we have

$$c^r_{p,p}(p^\alpha, p^\beta) = \sum_{\substack{a\,(p^\alpha)^* \\ (r^2-ap^2,p)=1}} \left(\frac{a}{p}\right)^\alpha \sum_{\substack{b\,(p^\beta)^* \\ (r^2-bp^2,p)=1 \\ bp^2\equiv ap^2 \bmod p^{\alpha+2}}} \left(\frac{b}{p}\right)^\beta.$$

If $p \,|\, r$, then $p \,|\, (r^2-ap^2, p)$, and $c^r_{p,p}(p^\alpha, p^\beta) = 0$. If $p \nmid r$, then $(r^2-ap^2, p) = 1$, and

$$\begin{aligned} c^r_{p,p}(p^\alpha, p^\beta) &= \sum_{a\,(p^\alpha)^*} \left(\frac{a}{p}\right)^\alpha \sum_{\substack{b\,(p^\beta)^* \\ b\equiv a \bmod p^\alpha}} \left(\frac{b}{p}\right)^\beta \\ &= p^{\beta-\alpha} \sum_{a\,(p^\alpha)^*} \left(\frac{a}{p}\right)^{\alpha+\beta} = p^{\beta-1} \sum_{a\,(p)^*} \left(\frac{a}{p}\right)^{\alpha+\beta}. \end{aligned}$$

This proves (ii).

(iii) As above, we can suppose that $1 \leq \alpha \leq \beta$. We have

$$\begin{aligned} c^r_{1,1}(2^\alpha, 2^\beta) &= \sum_{\substack{a\,(2^{\alpha+2})^* \\ (r^2-a,2^{\alpha+2})=4}} \left(\frac{a}{2}\right)^\alpha \sum_{\substack{b\,(2^{\beta+2})^* \\ (r^2-b,2^{\beta+2})=4 \\ a\equiv b \bmod 2^{\alpha+2}}} \left(\frac{b}{2}\right)^\beta \\ &= 2^{\beta-\alpha} \sum_{\substack{a\,(2^{\alpha+2})^* \\ (r^2-a,2^{\alpha+2})=4}} \left(\frac{a}{2}\right)^{\alpha+\beta}. \end{aligned}$$

As the value of the character depends only on the value of a modulo 8, and as $r^2 \equiv 1 \bmod 8$, we have

$$c^r_{1,1}(2^\alpha, 2^\beta) = 2^{\beta-\alpha}2^{\alpha-1} \sum_{\substack{a\,(8)^* \\ a\equiv 5 \bmod 8}} \left(\frac{a}{2}\right)^{\alpha+\beta} = 2^{\beta-1}(-1)^{\alpha+\beta}.$$

This proves (iii). ∎

LEMMA 4.8. *For any integers $m, n \geq 1$, we have*

$$c^r_{f,g}(m,n) = O\left(\frac{mn}{\kappa(mn)(m,n)}\right).$$

Here $\kappa(n)$ is the multiplicative arithmetic function generated by the identity

$$\kappa(p^\alpha) = \begin{cases} p, & \alpha \text{ odd}, \\ 1, & \alpha \text{ even} \end{cases}$$

for any prime p and any positive integer α.

Proof. From Lemma 4.4, $c^r_{f,g}(m,n)$ is multiplicative, i.e.

$$c^r_{f,g}(m,n) = \prod_{p|mn} c^r_{f,g}(p^{\alpha(p)}, p^{\beta(p)}).$$

Let p be any prime. It then follows from Lemmas 4.5–4.7 that for integers $\alpha, \beta \geq 0$, we have

$$c^r_{f,g}(p^\alpha, p^\beta) \ll \left(\frac{p^{\alpha+\beta}}{\kappa(p^{\alpha+\beta})(p^\alpha, p^\beta)}\right)$$

with an absolute constant. We then have

$$c^r_{f,g}(m,n) \ll \prod_{p|mn} \frac{p^{\alpha(p)+\beta(p)}}{\kappa(p^{\alpha(p)+\beta(p)})(p^{\alpha(p)}, p^{\beta(p)})} = \frac{mn}{\kappa(mn)(m,n)}. \ ∎$$

4.3. *Euler product.* We compute in this section the Euler product for the constant C_r. We recall from Section 2 that

$$C_r = \frac{K_r}{\pi^2}$$

and from (26),

$$K_r = \sum_{\substack{f,g=1 \\ (2r,fg)=1}}^{\infty} \frac{1}{fg} \sum_{m,n=1}^{\infty} \frac{c^r_{f,g}(m,n)}{mn\phi([mf^2, ng^2])}.$$

From Lemma 4.3(i), $c^r_{f,g}(m,n) = 0$ when $(f', n) \neq 1$ or $(g', m) \neq 1$. Now, if $(f', n) = (g', m) = 1$,

$$[mf^2, ng^2] = k^2[mf'^2, ng'^2] = k^2[m,n]f'^2g'^2 = [m,n][f^2, g^2].$$

Using that and the identity

$$\phi(ab) = \frac{\phi(a)\phi(b)(a,b)}{\phi(a,b)}$$

we get

$$K_r = \sum_{\substack{f,g\geq 1\\(2r,fg)=1}} \frac{1}{fg\phi([f^2,g^2])} \sum_{m,n=1}^{\infty} \frac{c_{f,g}^r(m,n)\phi([f^2,g^2],[m,n])}{mn\phi([m,n])([f^2,g^2],[m,n])}. \tag{27}$$

One can check that the function in the inside sum is a multiplicative function of m and n. For such functions, we have the following.

LEMMA 4.9 (Euler product). *Let $F(m,n)$ be a multiplicative function. Then*

$$\sum_{m,n\geq 1} F(m,n) = \prod_p \sum_{\alpha,\beta\geq 0} F(p^\alpha, p^\beta).$$

We then write the inside sum of (27) as

$$\sum_{m,n=1}^{\infty} \frac{c_{f,g}^r(m,n)\phi([f^2,g^2],[m,n])}{mn\phi([m,n])([f^2,g^2],[m,n])} = \prod_p \sum_{\alpha,\beta\geq 0} \frac{c_{f,g}^r(p^\alpha,p^\beta)\phi([f^2,g^2],[p^\alpha,p^\beta])}{p^\alpha p^\beta \phi([p^\alpha,p^\beta])([f^2,g^2],[p^\alpha,p^\beta])}.$$

We now break the product in three parts, depending on the p-adic valuations of f and g. We first notice that for any prime p,

$$\frac{\phi([f^2,g^2],[p^\alpha,p^\beta])}{([f^2,g^2],[p^\alpha,p^\beta])} = \begin{cases} 1 & \text{if } \alpha=\beta=0,\\ 1 & \text{if } p\nmid fg,\\ \dfrac{p-1}{p} & \text{if } p\mid fg,\ \alpha,\beta \text{ not both 0.}\end{cases}$$

Then, using Lemma 4.5, we can rewrite the last product as

$$\prod_{p\nmid fg} \sum_{\alpha,\beta\geq 0} \frac{c_{1,1}^r(p^\alpha,p^\beta)}{p^\alpha p^\beta \phi([p^\alpha,p^\beta])} \prod_{\substack{p\mid fg\\ v_p(f)=v_p(g)}} \left(1+\frac{p-1}{p} \sum_{\substack{\alpha,\beta\geq 0\\(\alpha,\beta)\neq(0,0)}} \frac{c_{p,p}^r(p^\alpha,p^\beta)}{p^\alpha p^\beta \phi([p^\alpha,p^\beta])}\right)$$
$$\times \prod_{\substack{p\mid fg\\ v_p(f)<v_p(g)}} \left(1+\frac{p-1}{p}\sum_{\beta>0}\frac{c_p^r(p^\beta)}{p^\beta\phi(p^\beta)}\right) \prod_{\substack{p\mid fg\\ v_p(f)>v_p(g)}} \left(1+\frac{p-1}{p}\sum_{\alpha>0}\frac{c_p^r(p^\alpha)}{p^\alpha\phi(p^\alpha)}\right)$$
$$= \prod_p E_1(p) \prod_{\substack{p\mid fg\\ v_p(f)=v_p(g)}} \frac{E_2(p)}{E_1(p)} \prod_{\substack{p\mid fg\\ v_p(f)<v_p(g)}} \frac{E_3(p)}{E_1(p)} \prod_{\substack{p\mid fg\\ v_p(f)>v_p(g)}} \frac{E_3(p)}{E_1(p)}$$

where

$$E_1(p) = \sum_{\alpha,\beta\geq 0} \frac{c_{1,1}^r(p^\alpha, p^\beta)}{p^\alpha p^\beta \phi([p^\alpha, p^\beta])},$$

$$E_2(p) = 1 + \frac{p-1}{p} \sum_{\substack{\alpha,\beta\geq 0 \\ (\alpha,\beta)\neq(0,0)}} \frac{c_{p,p}^r(p^\alpha, p^\beta)}{p^\alpha p^\beta \phi([p^\alpha, p^\beta])},$$

$$E_3(p) = 1 + \frac{p-1}{p} \sum_{\beta>0} \frac{c_p^r(p^\beta)}{p^\beta \phi(p^\beta)}.$$

Inserting the last equation in (27), we get

$$K_r = \prod_p E_1(p) \sum_{\substack{f,g\geq 1 \\ (2r,fg)=1}} \frac{1}{fg\phi([f^2,g^2])} \prod_{\substack{p|fg \\ v_p(f)=v_p(g)}} \frac{E_2(p)}{E_1(p)} \times \prod_{\substack{p|fg \\ v_p(f)<v_p(g)}} \frac{E_3(p)}{E_1(p)} \prod_{\substack{p|fg \\ v_p(f)>v_p(g)}} \frac{E_3(p)}{E_1(p)}.$$

One can check that the function

$$F(f,g) = \frac{1}{fg\phi([f^2,g^2])} \prod_{\substack{p|fg \\ v_p(f)=v_p(g)}} \frac{E_2(p)}{E_1(p)} \prod_{\substack{p|fg \\ v_p(f)<v_p(g)}} \frac{E_3(p)}{E_1(p)} \prod_{\substack{p|fg \\ v_p(f)>v_p(g)}} \frac{E_3(p)}{E_1(p)}$$

is a multiplicative function of f and g. We compute $F(1,1) = 1$, and for $\gamma, \delta \geq 0$ not both 0,

$$F(p^\gamma, p^\delta) = \begin{cases} \dfrac{1}{p^\gamma p^\delta \phi([p^{2\gamma}, p^{2\delta}])} \dfrac{E_2(p)}{E_1(p)} & \text{if } \gamma = \delta, \\ \dfrac{1}{p^\gamma p^\delta \phi([p^{2\gamma}, p^{2\delta}])} \dfrac{E_3(p)}{E_1(p)} & \text{if } \gamma < \delta, \\ \dfrac{1}{p^\gamma p^\delta \phi([p^{2\gamma}, p^{2\delta}])} \dfrac{E_3(p)}{E_1(p)} & \text{if } \gamma > \delta. \end{cases}$$

By Lemma 4.9, this gives

$$\begin{aligned} K_r &= \prod_p E_1(p) \prod_{p\nmid 2r} \sum_{\gamma,\delta\geq 0} F(p^\gamma, p^\delta) \\ &= \prod_{p|2r} E_1(p) \\ &\quad \times \prod_{p\nmid 2r} \left(E_1(p) + E_2(p) \sum_{\gamma\geq 1} \frac{1}{p^{2\gamma}\phi(p^{2\gamma})} + 2E_3(p) \sum_{\substack{\gamma,\delta\geq 0 \\ \gamma<\delta}} \frac{1}{p^\gamma p^\delta \phi([p^{2\gamma}, p^{2\delta}])} \right). \end{aligned}$$

One computes

$$E_1(2) = \frac{4}{9},$$

$$E_1(p) = \frac{p^2(p^2+1)}{(p^2-1)^2} \quad \text{for } p \mid r,$$

$$E_1(p) = \frac{p^5 - p^4 - p^3 - 4p^2 + 1}{(p-1)^3(p+1)^2} \quad \text{for } p \nmid 2r,$$

$$E_2(p) = \frac{p^4 + p^3 + 2p^2 - p - 1}{p(p-1)(p+1)^2} \quad \text{for } p \nmid 2r,$$

$$E_3(p) = 1 + \frac{1}{p(p+1)} = \frac{p^2+p+1}{p(p+1)},$$

$$\sum_{\gamma \geq 1} \frac{1}{p^{2\gamma}\phi(p^{2\gamma})} = \frac{p}{(p-1)(p^4-1)},$$

$$\sum_{\substack{\gamma,\delta \geq 0 \\ \gamma < \delta}} \frac{1}{p^\gamma p^\delta \phi([p^{2\gamma}, p^{2\delta}])}$$

$$= \left(\frac{p}{p-1}\right)^2 \left(\frac{1}{p^3-1} - \frac{1}{p^4-1}\right) = \frac{p^5}{(p^4-1)(p^3-1)(p-1)}.$$

Inserting this in the last expression for K_r gives

$$K_r = \frac{4}{9} \prod_{p \mid r} \frac{p^2(p^2+1)}{(p^2-1)^2} \prod_{p \nmid 2r} \frac{p^2(p^4-2p^2-3p-1)}{(p+1)^3(p-1)^3}$$

$$= 3 \prod_{p \mid r} \frac{p^2(p^2+1)}{(p^2-1)^2} \prod_{p \nmid r} \frac{p^2(p^4-2p^2-3p-1)}{(p+1)^3(p-1)^3}$$

and finally

$$C_r = \frac{3}{\pi^2} \prod_{p \mid r} \frac{p^2(p^2+1)}{(p^2-1)^2} \prod_{p \nmid r} \frac{p^2(p^4-2p^2-3p-1)}{(p+1)^3(p-1)^3}.$$

5. The supersingular case. The case $r = 0$ was considered by Fouvry and Murty in [FM2], and we verify here that our method gives the same asymptotic. We start by considering (3.1) of [FM2]:

$$T(x) = \sum_{p \leq x} \frac{h^2(-p)}{p^2} + 2 \sum_{p \leq x} \frac{h(-p)h(-4p)}{p^2} + \sum_{p \leq x} \frac{h^2(-4p)}{p^2}$$

$$= T_{1,1}(x) + 2T_{1,4}(x) + T_{4,4}(x).$$

Proceeding as in Section 2, we write

$$T_{1,1}(x) = \sum_{p \in S_{2,2}(x)} \frac{L(1,\chi_{-p})L(1,\chi_{-p})}{p},$$
$$T_{1,4}(x) = 2 \sum_{p \in S_{2,1}(x)} \frac{L(1,\chi_{-p})L(1,\chi_{-4p})}{p},$$
$$T_{4,4}(x) = 4 \sum_{p \in S_{1,1}(x)} \frac{L(1,\chi_{-4p})L(1,\chi_{-4p})}{p}.$$

We replace $1/p$ by $\log p$ in the above sums, and we call the corresponding new sums $\widehat{T}_{i,j}(x)$. One can easily get the asymptotic for T from $\widehat{T}$ by partial summation as in Section 2. We now calculate each of the sums $\widehat{T}_{i,j}(x)$.

Proceeding as in Section 3, we get

$$\widehat{T}_{1,1}(x) \sim \Big(\sum_{m,n=1}^{\infty} \frac{c^0_{2,2}(m,n)}{mn\phi([4m,4n])} \Big) x$$

where

$$c^0_{2,2}(m,n) = \sum_{\substack{a \,(4m)^* \\ a \equiv 1 \bmod 4}} \left(\frac{a}{m}\right) \sum_{\substack{b \,(4n)^* \\ b \equiv 1 \bmod 4 \\ (a-b)/4 \equiv 0 \bmod (m,n)}} \left(\frac{b}{n}\right).$$

When m and n are odd, we have

$$c^0_{2,2}(m,n) = \sum_{a \,(m)^*} \left(\frac{a}{m}\right) \sum_{\substack{b \,(n)^* \\ a \equiv b \bmod (m,n)}} \left(\frac{b}{n}\right)$$

and for $1 \le \alpha \le \beta$, we have

$$c^0_{2,2}(2^\alpha, 2^\beta) = 2^{\beta-1}(1 + (-1)^{\alpha+\beta}).$$

Using these and following the arguments of Section 4, we get the Euler product

$$\sum_{m,n=1}^{\infty} \frac{c^0_{2,2}(m,n)}{mn\phi([4m,4n])} = \frac{1}{2} \prod_p \frac{1 + 1/p^2}{(1 - 1/p^2)^2} = \frac{5\pi^2}{24}.$$

Proceeding similarly, we get

$$\widehat{T}_{1,4}(x) \sim \Big(2 \sum_{\substack{m,n=1 \\ n \text{ odd}}}^{\infty} \frac{c^0_{2,1}(m,n)}{mn\phi([4m,n])} \Big) x$$

where

$$c^0_{2,1}(m,n) = \sum_{\substack{a\,(4m)^*\\ a\equiv 1 \bmod 4}} \left(\frac{a}{m}\right) \sum_{\substack{b\,(n)^*\\ a\equiv b \bmod (4m,n)}} \left(\frac{b}{n}\right).$$

When m is odd, we have

$$c^0_{2,1}(m,n) = \sum_{a\,(m)^*} \left(\frac{a}{m}\right) \sum_{\substack{b\,(n)^*\\ a\equiv b \bmod (m,n)}} \left(\frac{b}{n}\right)$$

and for $\alpha \geq 1$, we have

$$c^0_{2,1}(2^\alpha, 1) = 2^{\alpha-1}(-1)^\alpha.$$

Using these and following the arguments of Section 4, we get the Euler product

$$2 \sum_{\substack{m,n=1\\ n \text{ odd}}}^{\infty} \frac{c^0_{2,1}(m,n)}{mn\phi([4m,n])} = 2\left(\frac{1}{2}\right)\left(\frac{1}{1-1/2^2}\right) \prod_{p\geq 3} \frac{1+1/p^2}{(1-1/p^2)^2} = \frac{\pi^2}{4}.$$

Proceeding in the same way, we get

$$\widehat{T}_{4,4}(x) \sim \left(4 \sum_{\substack{m,n=1\\ m,n \text{ odd}}}^{\infty} \frac{c^0_{1,1}(m,n)}{mn\phi([m,n])}\right) x$$

where

$$c^0_{1,1}(m,n) = \sum_{a\,(m)^*} \left(\frac{a}{m}\right) \sum_{\substack{b\,(n)^*\\ a\equiv b \bmod (m,n)}} \left(\frac{b}{n}\right).$$

Here m and n are odd, and we have

$$4 \sum_{\substack{m,n=1\\ m,n \text{ odd}}}^{\infty} \frac{c^0_{1,1}(m,n)}{mn\phi([m,n])} = 4 \prod_{p\geq 3} \frac{1+1/p^2}{(1-1/p^2)^2} = \frac{3\pi^2}{4}.$$

Finally, putting the last three estimates together, we get

$$T(x) \sim \left(\frac{5}{24} + \frac{1}{2} + \frac{3}{4}\right) \frac{x}{\log x} = \frac{35}{24} \frac{x}{\log x}$$

and then Theorem 1.2 also holds for $r = 0$ with $C_0 = 35/96$. This is the result obtained by Fouvry and Murty in [FM2].

References

[Bur] D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. 13 (1963), 524–536.

[Cox] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, 1989.
[Dav] H. Davenport, *Multiplicative Number Theory*, Springer, 1980.
[DKP] C. David, H. Kisilevsky and F. Pappalardi, *Galois representations with non-surjective traces*, Canad. J. Math. 51 (1999), 936–951.
[DP] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices, 1999, no. 4, 165–183.
[Deu] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197–272.
[Elk] N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. 89 (1987), 561–567.
[FM1] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. 48 (1996), 81–104.
[FM2] —, —, *Supersingular primes common to two elliptic curves*, in: Number Theory (Paris, 1992–1993), London Math. Soc. Lecture Note Ser. 215, Cambridge Univ. Press, 1995, 91–102.
[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford, 1979.
[LT] S. Lang and H. Trotter, *Frobenius Distributions in GL_2-Extensions*, Lecture Notes in Math. 504, Springer, 1976.
[M] M. R. Murty, *Problems in Analytic Number Theory*, Springer, 2001.
[MMS] M. R. Murty, V. K. Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. 110 (1998), 253–281.
[S] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.
[Wil] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. 21 (1922), 235–255.

Department of Mathematics
and Computer Science
University of Lethbridge
4401 University Drive West
Lethbridge, Alberta, T1K 3M4, Canada
E-mail: akbary@cs.uleth.ca

Department of Mathematics and Statistics
Concordia University
1455 de Maisonneuve Blvd. West, Montréal
Quebec, H3G 1M8, Canada
E-mail: cdavid@mathstat.concordia.ca

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: rjuricevic@math.uwaterloo.ca

Received on 18.6.2002
and in revised form on 25.2.2003 (4312)