

Average Distributions and Product of Special Values of L-Series

Amir Akbary*, University of Lethbridge
Chantal David†, Concordia University
Robert Juricevic‡, University of 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 $E \bmod p$. 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 $|a_p(E)| \leq 2\sqrt{p}$. The case $a_p(E) = 0$ corresponds to supersingular reduction mod p .

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

$$\pi_{E_1, \dots, E_N}^r(x) = \# \{p \leq x : a_p(E_1) = \dots = a_p(E_N) = r\}.$$

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

$$\text{Prob} \{a_p(E) = r\} \sim \begin{cases} \frac{1}{4\sqrt{p}} & \text{if } |r| \leq 2\sqrt{p}; \\ 0 & \text{if } |r| > 2\sqrt{p}. \end{cases}$$

This suggests the asymptotic behavior

$$\pi_E^r(x) \sim \sum_{p \leq x} \text{Prob} \{a_p(E) = r\} \sim C_{E,r} \frac{\sqrt{x}}{\log x}$$

⁰2000 *Mathematics Subject Classification*: Primary 11G05, Secondary 11M41

*Research partially supported by University of Lethbridge Research Fund and NSERC

†Research partially supported by NSERC and FCAR

‡Research partially supported by NSERC and FCAR

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 $|r| \leq 2\sqrt{p}$

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

and more generally

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

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, \dots, E_N be elliptic curves over \mathbb{Q} , not $\overline{\mathbb{Q}}$ -isogenous and if $r = 0$ without complex multiplication. Then,*

$$\pi_{E_1, \dots, E_N}^r(x) \sim \begin{cases} C_{E_1, r} \frac{\sqrt{x}}{\log x} & \text{if } N = 1; \\ C_{E_1, E_2, r} \log \log x & \text{if } N = 2; \\ \text{is finite} & \text{if } N > 2. \end{cases}$$

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 $\pi_E^0(x) \geq \log_3 x / (\log_4 x)^{1+\delta}$ for any positive δ and x sufficiently large [FM1].

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

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

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 $x \rightarrow \infty$

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

where

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

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 in this paper for 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). Using 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 $N \geq 2$). In the case $r = 0$, one can compute those averages by splitting the L-functions

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

into 2 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 2 elliptic curves then follows from this average of products of special values of Dirichlet L-functions.

Theorem 1.2 *Let $\epsilon > 0$, and let r be an odd integer. Let A, B be positive integers with $A, B \geq x^{1+\epsilon}$. Then as $x \rightarrow \infty$,*

$$\frac{1}{16A^2B^2} \sum_{\substack{|\alpha_1|, |\alpha_2| \leq A \\ |b_1|, |b_2| \leq B}} \pi_{E_1, E_2}^r(x) \sim C_r \log \log x$$

where

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

We remark that for technical reasons, we restrict to the case 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) which is done 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 product of special values of L-series; in Section 3, we find a precise asymptotic for the average of 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 $r = 0$.

Acknowledgment: 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

$$\begin{aligned} E_1 & : y^2 = x^3 + a_1x + b_1 \\ E_2 & : y^2 = x^3 + a_2x + b_2 \end{aligned}$$

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

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

We consider

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

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

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

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,

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

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*

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

where the sum runs over all positive integers f such that $f^2 | r^2 - 4p$ and $d = (r^2 - 4p)/f^2 \equiv 0, 1 \pmod{4}$ 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].

QED.

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

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

Replacing in (4) and (3), this gives

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

We take A, B such that

$$A, B \geq x^{1+\epsilon} \quad (5)$$

for any $\epsilon > 0$. Then, we have

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

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

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

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

$$\begin{aligned} S_{f,g}(x) &= \left\{ B_r < p \leq x : f^2 | r^2 - 4p, g^2 | r^2 - 4p, \right. \\ &\quad \left. d_1 = (r^2 - 4p)/f^2 \equiv 0, 1 \pmod{4}, d_2 = (r^2 - 4p)/g^2 \equiv 0, 1 \pmod{4} \right\}. \end{aligned}$$

We rewrite the last sum as

$$\frac{1}{\pi^2} \sum_{\substack{f \leq 2\sqrt{x} \\ g \leq 2\sqrt{x}}} \frac{1}{fg} \sum_{p \in S_{f,g}(x)} \frac{L(1, \chi_{d_1}) L(1, \chi_{d_2})}{p} + O\left(\sum_{\substack{f \leq 2\sqrt{x} \\ g \leq 2\sqrt{x}}} \frac{1}{fg} \sum_{p \in S_{f,g}(x)} \frac{L(1, \chi_{d_1}) L(1, \chi_{d_2})}{p^2} \right). \quad (7)$$

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

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

Then, using Theorem 3.1 and partial summation, we find that the first sum of (7) is

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

and similarly that

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

Then,

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

and replacing in (6), we get

$$\frac{1}{16A^2 B^2} \sum_{\substack{|\alpha_1|, |\alpha_2| \leq A \\ |b_1|, |b_2| \leq B}} \pi_{E_1, E_2}^r(x) \sim \frac{K_r}{\pi^2} \log \log x$$

for $A, B \geq x^{1+\epsilon}$. Notice, assuming Theorem 3.1, this shows Theorem 1.2. The next section consists of a proof of Theorem 3.1.

3 Average values of product of Dirichlet L -functions

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

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

where

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

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

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

where

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

Let

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

where

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

We then have the trivial bound

$$a_{d_1, d_2}(\ell) \ll d(\ell) \ll \ell^\epsilon \quad (9)$$

for any $\epsilon > 0$, where $d(\ell)$ 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 $\epsilon > 0$,*

$$L(1) = \sum_{\ell=1}^{\infty} \frac{a_{d_1, d_2}(\ell)}{\ell} e^{-\ell/U} + O\left(\frac{|d_1 d_2|^{3/16+\epsilon}}{U^{1/2}}\right)$$

where the error term depends on ϵ .

Proof: We have the integral representation

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

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

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

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

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

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

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

and then

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

Replacing this in (10) completes the proof. QED.

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

$$\begin{aligned} & \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{p \in S_{f, g}(x)} L(1) \log p \\ &= \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{p \in S_{f, g}(x)} \left\{ \sum_{\ell=1}^{\infty} \frac{a_{d_1, d_2}(\ell)}{\ell} e^{-\ell/U} + O\left(\frac{|d_1 d_2|^{3/16+\epsilon}}{U^{1/2}}\right) \right\} \log p \\ &= \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{\ell=1}^{\infty} \frac{e^{-\ell/U}}{\ell} \sum_{p \in S_{f, g}(x)} a_{d_1, d_2}(\ell) \log p + O\left(\frac{1}{U^{1/2}} \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{p \in S_{f, g}(x)} |d_1 d_2|^{3/16+\epsilon} \log p\right). \end{aligned}$$

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

$$\begin{aligned} & \ll \frac{1}{U^{1/2}} \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{(fg)^{11/8+2\epsilon}} \sum_{p \in S_{f, g}(x)} p^{3/8+2\epsilon} \log p \\ & \ll \frac{x^{3/8+2\epsilon} \log x}{U^{1/2}} \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{(fg)^{11/8+2\epsilon}} \sum_{p \in S_{f, g}(x)} 1 \ll \frac{x^{11/8+2\epsilon}}{U^{1/2}}, \end{aligned}$$

and we have

$$\sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{p \in S_{f, g}(x)} L(1) \log p = \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{\ell=1}^{\infty} \frac{e^{-\ell/U}}{\ell} \sum_{p \in S_{f, g}(x)} a_{d_1, d_2}(\ell) \log p + O\left(\frac{x^{11/8+2\epsilon}}{U^{1/2}}\right) \quad (11)$$

for any $\epsilon > 0$.

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

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

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 $[f^2, g^2] \leq 4x$. We also have that $4p \equiv r^2 \pmod{f^2}$ and $4p \equiv r^2 \pmod{g^2} \iff 4p \equiv r^2 \pmod{[f^2, g^2]}$. Then,

$$\begin{aligned} & \left| \sum_{\substack{V < f, g \leq 2\sqrt{x} \\ (2r, fg)=1 \\ [f^2, g^2] \leq 4x}} \frac{1}{fg} \sum_{\ell=1}^{\infty} \frac{e^{-\ell/U}}{\ell} \sum_{p \in S_{f,g}(x)} a_{d_1, d_2}(\ell) \log p \right| \\ & \leq \log x \left| \sum_{\ell=1}^{\infty} \frac{d(\ell)}{\ell} e^{-\ell/U} \right| \sum_{\substack{V < f, g \leq 2\sqrt{x} \\ (2r, fg)=1 \\ [f^2, g^2] \leq 4x}} \frac{1}{fg} \sum_{\substack{p \leq x \\ 4p \equiv r^2 \pmod{[f^2, g^2]}}} 1 \\ & \leq x \log x \left| \sum_{\ell=1}^{\infty} \frac{d(\ell)}{\ell} e^{-\ell/U} \right| \sum_{\substack{V < f, g \leq 2\sqrt{x} \\ (2r, fg)=1 \\ [f^2, g^2] \leq 4x}} \frac{1}{fg[f^2, g^2]}. \end{aligned} \quad (12)$$

Lemma 3.3

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

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

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

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 $(-\frac{1}{2})$ and calculating the residue at $s = 0$ we get the desired bound. QED.

Using this lemma, we can bound (12) by

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

to get that

$$\begin{aligned} \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{p \in S_{f, g}(x)} L(1) \log p &= \sum_{\substack{f, g \leq V \\ (2r, fg)=1}} \frac{1}{fg} \sum_{\ell=1}^{\infty} \frac{e^{-\ell/U}}{\ell} \sum_{p \in S_{f, g}(x)} a_{d_1, d_2}(\ell) \log p \\ &+ O\left(\frac{x^{11/8+2\epsilon}}{U^{1/2}}\right) + O\left(\frac{x \log x \log^2 U}{V^2}\right). \end{aligned} \quad (13)$$

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

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

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

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

$$\begin{aligned} \sum_{\ell > U \log U} \frac{d(\ell)}{\ell} e^{-\ell/U} &\ll \sum_{\ell > U \log U} \frac{e^{-\ell/U}}{\ell^{1-\epsilon}} \ll \frac{1}{(U \log U)^{1-\epsilon}} \sum_{\ell > U \log U} e^{-\ell/U} \\ &\ll \frac{1}{(U \log U)^{1-\epsilon}} \int_{U \log U}^{\infty} e^{-t/U} dt = \frac{1}{(U \log U)^{1-\epsilon}} \end{aligned}$$

and then

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

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

$$\begin{aligned} \sum_{\substack{f, g \leq 2\sqrt{x} \\ (2r, fg)=1}} \frac{1}{fg} \sum_{p \in S_{f, g}(x)} L(1) \log p &= \sum_{\substack{f, g \leq V \\ (2r, fg)=1}} \frac{1}{fg} \sum_{\ell \leq U \log U} \frac{1}{\ell} e^{-\ell/U} \sum_{p \in S_{f, g}(x)} a_{d_1, d_2}(\ell) \log p \\ &+ O\left(\frac{x^{11/8+2\epsilon}}{U^{1/2}}\right) + O\left(\frac{x \log x \log^2 U}{V^2}\right) + O\left(\frac{x \log x \log^2 V}{(U \log U)^{1-\epsilon}}\right). \end{aligned} \quad (14)$$

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

$$\chi_{d_1}(m) = \chi_{d'_1}(m) \text{ if } d_1 \equiv d'_1 \pmod{4m}.$$

We then have

$$\begin{aligned} & \sum_{\substack{f,g \leq V \\ (2r, fg)=1}} \frac{1}{fg} \sum_{\ell \leq U \log U} \frac{e^{-\ell/U}}{\ell} \sum_{p \in S_{f,g}(x)} \log p \sum_{mn=\ell} \chi_{d_1}(m) \chi_{d_2}(n) \\ &= \sum_{\substack{f,g \leq V \\ (2r, fg)=1}} \frac{1}{fg} \sum_{\substack{\ell \leq U \log U \\ mn=\ell}} \frac{e^{-\ell/U}}{\ell} \sum_{\substack{a \pmod{4m} \\ b \pmod{4n}}} \left(\frac{a}{m}\right) \left(\frac{b}{n}\right) \sum_p^* \log p \end{aligned}$$

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

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

If $(r^2 - af^2)/4 \not\equiv (r^2 - bg^2)/4 \pmod{(mf^2, ng^2)}$, 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 $(r^2 - af^2)/4 \not\equiv (r^2 - bg^2)/4 \pmod{(mf^2, ng^2)}$, we set $\theta = 0$. Then, we can rewrite the last sum as

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

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

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

With this notation, we rewrite the last sum as

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

where $\sum_{\substack{a \pmod{4m} \\ b \pmod{4n}}}^*$ means that the sum runs over invertible residues a, b modulo m, n respectively such that $(r^2 - af^2)/4 \equiv (r^2 - bg^2)/4 \pmod{(mf^2, ng^2)}$, 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

$$c_{f,g}^r(m, n) = \sum_{\substack{a \pmod{4m} \\ (r^2 - af^2, 4m) = 4}} \sum_{\substack{b \pmod{4n} \\ (r^2 - bg^2, 4n) = 4 \\ (r^2 - af^2)/4 \equiv (r^2 - bg^2)/4 \pmod{(mf^2, ng^2)}}} \left(\frac{a}{m}\right) \left(\frac{b}{n}\right). \quad (15)$$

Using this notation, we have

$$\begin{aligned} \sum_{\substack{f,g \leq V \\ (2r,fg)=1}} \frac{1}{fg} \sum_{\ell \leq U \log U} \frac{e^{-\ell/U}}{\ell} \sum_{p \in S_{f,g}(x)} a_{d_1, d_2}(\ell) \log p = x \sum_{\substack{f,g \leq V \\ (2r,fg)=1}} \frac{1}{fg} \sum_{\substack{\ell \leq U \log U \\ mn=\ell}} \frac{e^{-\ell/U}}{\ell} \frac{c_{f,g}^r(m, n)}{\phi([mf^2, ng^2])} \\ + \sum_{\substack{f,g \leq V \\ (2r,fg)=1}} \frac{1}{fg} \sum_{\substack{\ell \leq U \log U \\ \ell=mn}} \frac{e^{-\ell/U}}{\ell} \sum_{\substack{a \bmod 4m \\ b \bmod 4n}}^* \binom{a}{m} \binom{b}{n} E(x; [mf^2, ng^2], \theta). \end{aligned} \quad (16)$$

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

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

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

$$\begin{aligned} \sum_{mn \leq U \log U} \frac{1}{mn} \sum_{\substack{a \bmod 4m \\ b \bmod 4n}}^* |E(x; [mf^2, ng^2], \theta)| &\leq \sum_{mn \leq U \log U} \frac{1}{mn} \sum_{\theta \bmod [mf^2, ng^2]} |E(x; [mf^2, ng^2], \theta)| \\ &\ll f^2 g^2 \sum_{\ell \leq U \log U f^2 g^2} \frac{1}{\ell} \sum_{\theta \bmod \ell} c(\ell) |E(x; \ell, \theta)| \end{aligned}$$

where $c(\ell)$ is the number of ways that we can write $\ell = [mf^2, ng^2]$. 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, $C(n) \leq 2^{\nu(n)} d(n)$, 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 $\alpha_i \geq 1$ 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 $0 \leq \beta_i, \gamma_i \leq \alpha_i$ 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

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

QED.

Using this result in the last bound, we get

$$\sum_{mn \leq U \log U} \frac{1}{mn} \sum_{\substack{a \bmod 4m \\ b \bmod 4n}}^* |E(x; [mf^2, ng^2], \theta)| \ll f^2 g^2 \sum_{\ell \leq U \log U f^2 g^2} \frac{d^2(\ell)}{\ell} \sum_{\theta \bmod \ell} |E(x; \ell, \theta)|$$

$$\leq f^2 g^2 \left(\sum_{\substack{\ell \leq U \log U f^2 g^2 \\ \theta \bmod \ell}} \frac{d^4(\ell)}{\ell^2} \right)^{1/2} \left(\sum_{\substack{\ell \leq U \log U f^2 g^2 \\ \theta \bmod \ell}} E^2(x; \ell, \theta) \right)^{1/2}$$

using the Cauchy-Schwartz inequality.

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

$$\sum_{\ell \leq N} d^r(\ell) \sim A_r N \log^{2^r-1}(N), \quad \text{for } r \geq 2 \text{ and } A_r \text{ an absolute constant}$$

with $r = 4$. Using partial summation, and the fact that $f, g \leq V$, this gives

$$\left(\sum_{\substack{\ell \leq U \log U f^2 g^2 \\ \theta \bmod \ell}} \frac{d^4(\ell)}{\ell^2} \right)^{1/2} \leq \left(\sum_{\ell \leq U \log U f^2 g^2} \frac{d^4(\ell)}{\ell} \right)^{1/2} \ll \log^8(V^4 U \log U).$$

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

$$\left(\sum_{\substack{\ell \leq V^4 U \log U \\ \theta \bmod \ell}} E^2(x; \ell, \theta) \right)^{1/2} \ll (V^4 U x \log U \log x)^{1/2}$$

whenever

$$\frac{x}{\log^A x} \leq V^4 U \log U \leq x, \tag{17}$$

for some $A > 0$.

Finally, summing over f, g , this gives

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

whenever (17) holds.

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

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

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

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

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 $(f', n) \neq 1$ or $(g', m) \neq 1$, 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

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

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

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

It is shown in [DP, Lemma 3.4] that

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

converges for $\text{Re}(s) > 1$. Clearly, this implies that $\sum_{\ell=1}^{\infty} \frac{d(\ell)}{\kappa(\ell)\phi(\ell)}$ 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 $\epsilon > 0$,

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

Also,

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

and then

$$x \sum_{\substack{f,g \leq V \\ (2r,fg)=1}} \frac{1}{fg} \sum_{\substack{\ell > U \log U \\ mn=\ell}} \frac{e^{-\ell/U}}{\ell} \frac{c_{f,g}^r(m, n)}{\phi([mf^2, ng^2])} = O\left(\frac{x}{(U \log U)^{1/2-\epsilon}}\right). \quad (23)$$

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

$$\begin{aligned} x \sum_{\substack{f,g > V \\ (2r,fg)=1}} \frac{1}{fg} \sum_{m,n=1}^{\infty} \frac{c_{f,g}^r(m, n)e^{-mn/U}}{mn\phi([mf^2, ng^2])} &\ll x \sum_{f,g > V} \frac{(f^2, g^2)}{fg\phi(f^2)\phi(g^2)} \\ &\leq x \left(\sum_{f > V} \frac{1}{f\phi(f)} \right)^2 \ll \frac{x}{V^{2-2\epsilon}} \end{aligned}$$

for any positive $\epsilon > 0$, as $\phi(n) \gg n^{1-\epsilon}$ for any positive $\epsilon > 0$ [HW, p. 267].

Then, replacing in (19), we get

$$\begin{aligned} &x \sum_{\substack{f,g \leq V \\ (2r,fg)=1}} \frac{1}{fg} \sum_{\ell \leq U \log U} \frac{e^{-\ell/U}}{\ell} \sum_{mn=\ell} \frac{c_{f,g}^r(m, n)}{\phi([mf^2, ng^2])} \\ &= x \sum_{\substack{f,g=1 \\ (2r,fg)=1}}^{\infty} \frac{1}{fg} \sum_{m,n=1}^{\infty} \frac{c_{f,g}^r(m, n)e^{-mn/U}}{mn\phi([mf^2, ng^2])} + O\left(\frac{x}{(U \log U)^{1/2-\epsilon}}\right) + O\left(\frac{x}{V^{2-2\epsilon}}\right). \quad (24) \end{aligned}$$

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

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

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

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

and from (21), the sum converges for $\operatorname{Re}(s) > -1/2 + \epsilon$, for any $\epsilon > 0$. Then we can move the line of integration to any $-1/2 + \epsilon < \gamma < 0$, 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

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

and replacing in (24), we have

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

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

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

for all $\epsilon > 0$, with

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

We choose $U = x/\log^\alpha x$ and $V = \log^\beta x$ for positive integers α, β such that $\alpha - 4\beta - 1 \geq 1$ insuring that the condition (17) is satisfied. Then,

$$\begin{aligned} & \sum_{\substack{f,g \leq 2\sqrt{x} \\ (2r,fg)=1}} \frac{1}{fg} \sum_{p \in S_{f,g}^r(x)} L(1, \chi_{d_1}) L(1, \chi_{d_2}) \log p = K_r x + O\left(\frac{x}{\log^\beta x} + \frac{x}{\log^{\alpha/2-6\beta-9} x}\right) \\ &= K_r x + O\left(\frac{x}{\log^c x}\right) \end{aligned}$$

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 $c_{f,g}^r(m, n)$ are multiplicative, and we then use this result to prove a bound on the size of $c_{f,g}^r(m, n)$ 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 $c_{f,g}^r(m, n)$

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

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

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

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

(3) Let

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

Of course, this definition agrees with the previous definition of $c_{f,g}^r(m, n)$ 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 $c_{f,g}^r(m, n) = 0$.

(ii) If $(n_1, n_2) = 1$, then $c_{f,g}^r(n_1 n_2; m, a) = c_{f,g}^r(n_1; m, a) c_{f,g}^r(n_2; m, a)$.

Proof: (i) As $(r^2 - bg^2)/4 \equiv (r^2 - af^2)/4 \pmod{(mf^2, ng^2)} \iff (af'^2 - bg'^2)/4 \equiv 0 \pmod{(mf'^2, ng'^2)}$, we have

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

Suppose there is a prime p dividing (n, f') . Then, $c_{f,g}^r(m, n) = 0$ because $b \equiv 0 \pmod{p}$, 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,

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

if and only if

$$(af^2 - b_1g^2)/4 \equiv 0 \pmod{(mf^2, n_1g^2)} \quad \text{and} \quad (af^2 - b_2g^2)/4 \equiv 0 \pmod{(mf^2, n_2g^2)}$$

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. QED.

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,*

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

Equivalently, the functions $c_{f,g}^r(m, n)$ are multiplicative.

Proof: Let $n = n_1n_2$ and $m = m_1m_2$. If $(m, g') \neq 1$, or $(n, f') \neq 1$, then $c_{f,g}^r(m_1m_2, n_1n_2) = 0$ 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

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

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

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

with

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

By hypothesis, $(mf'^2, n_1g'^2) = (m_1f'^2, n_1g'^2)$, and $c_{f,g}^r(n_1; m, a) = c_{f,g}^r(n_1; m_1, a_1)$ where a_1 is the reduction of a modulo $4m_1$. Similarly, we have $c_{f,g}^r(n_2; m, a) = c_{f,g}^r(n_2; m_2, a_2)$ where a_2 is the reduction of a modulo $4m_2$.

Then, applying the Generalised Chinese Remainder theorem, we have

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

which proves the lemma. QED.

4.2 Bounds for the coefficients $c_{f,g}^r(m, n)$

We prove in this section that the functions $c_{f,g}^r(m, n)$ 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) $c_{f,g}^r(1, 1) = 1$;
- (ii) If $p \nmid fg$ (i.e. $v_p(f) = v_p(g) = 0$), then $c_{f,g}^r(p^\alpha, p^\beta) = c_{1,1}^r(p^\alpha, p^\beta)$;
- (iii) If $p \mid fg$ and $v_p(f) = v_p(g)$, then $c_{f,g}^r(p^\alpha, p^\beta) = c_{p,p}^r(p^\alpha, p^\beta)$;
- (iv) Suppose $p \mid fg$ and $v_p(f) \neq v_p(g)$. If $\alpha, \beta \geq 1$, then $c_{f,g}^r(p^\alpha, p^\beta) = 0$. If $\alpha = 0$ and $\beta \geq 1$, then $c_{f,g}^r(p^\alpha, p^\beta) = 0$ when $v_p(g) < v_p(f)$ and $c_{f,g}^r(p^\alpha, p^\beta) = c_p^r(p^\beta)$ when $v_p(g) > v_p(f)$. If $\alpha \geq 1$ and $\beta = 0$, then $c_{f,g}^r(p^\alpha, p^\beta) = 0$ when $v_p(f) < v_p(g)$ and $c_{f,g}^r(p^\alpha, p^\beta) = c_p^r(p^\alpha)$ when $v_p(f) > v_p(g)$.

Proof: (i) By definition.

(ii) By definition,

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

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

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

As

$$(af^2 - bg^2)/4 \equiv 0 \pmod{(p^\alpha, p^\beta)} \iff (af^2 - bg^2)/4 \equiv 0 \pmod{(p^\alpha f^2, p^\beta g^2)}$$

and

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

we get that $c_{1,1}^r(p^\alpha, p^\beta) = c_{f,g}^r(p^\alpha, p^\beta)$.

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

$$(af^2 - bg^2)/4 \equiv 0 \pmod{(p^\alpha f^2, p^\beta g^2)} \iff af'^2 \equiv bg'^2 \pmod{(p^\alpha, p^\beta)}.$$

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,

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

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 that $c_{p,p}^r(p^\alpha, p^\beta) = c_{f,g}^r(p^\alpha, p^\beta)$.

(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, $c_{f,g}^r(p^\alpha, p^\beta) = 0$ 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 $c_{f,g}^r(p^\alpha, p^\beta) = 0$ by Lemma 4.3(i). If $\alpha = 0$, $\beta \geq 1$ and $v_p(f) < v_p(g)$, then

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

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

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

(i) *For p odd,*

$$\frac{c_1^r(p^\alpha)}{p^{\alpha-1}} = \begin{cases} -\left(\frac{r^2}{p}\right) & \text{when } \alpha \text{ is odd;} \\ p-1 - \left(\frac{r^2}{p}\right) & \text{when } \alpha \text{ is even.} \end{cases}$$

(ii) *For p odd,*

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

(iii)

$$\frac{c_1^r(2^\alpha)}{2^{\alpha-1}} = (-1)^\alpha.$$

Proof: This is [DP, Lemma 3.3].

QED.

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

(i) *For p odd,*

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

(ii) *For p odd,*

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

(iii)

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

Proof: (i) If $\alpha = 0$, then $c_{1,1}^r(1, p^\beta) = c_1^r(p^\beta)$, 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

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

This proves (i).

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

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

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

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

This proves (ii).

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

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

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

$$c_{1,1}^r(2^\alpha, 2^\beta) = 2^{\beta-\alpha} 2^{\alpha-1} \sum_{\substack{a \in (8)^* \\ a \equiv 5 \pmod{8}}} \left(\frac{a}{2}\right)^{\alpha+\beta} = 2^{\beta-1} (-1)^{\alpha+\beta}.$$

This proves (iii).

QED.

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

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

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, $c_{f,g}^r(m, n)$ is multiplicative, i.e.

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

Let p be any prime. It then follows from Lemmas 4.5, 4.6 and 4.7 that for integers $\alpha, \beta \geq 0$, we have

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

with an absolute constant. We then have

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

QED.

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)

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

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

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

Using that and the identity

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

we get that

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

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 3 parts, depending on the p -adic valuations of f and g . We first notice that for any prime p

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

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

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

where

$$\begin{aligned}
E_1(p) &= \sum_{\alpha, \beta \geq 0} \frac{c_{1,1}^r(p^\alpha, p^\beta)}{p^\alpha p^\beta \phi([p^\alpha, p^\beta])} \\
E_2(p) &= 1 + \frac{p-1}{p} \sum_{\substack{\alpha, \beta \geq 0 \\ (\alpha, \beta) \neq (0,0)}} \frac{c_{p,p}^r(p^\alpha, p^\beta)}{p^\alpha p^\beta \phi([p^\alpha, p^\beta])} \\
E_3(p) &= 1 + \frac{p-1}{p} \sum_{\beta > 0} \frac{c_p^r(p^\beta)}{p^\beta \phi(p^\beta)}.
\end{aligned}$$

Replacing the last equation in (27), we get

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

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

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

Using Lemma 4.9, this gives

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

One computes

$$\begin{aligned}
E_1(2) &= \frac{4}{9} \\
E_1(p) &= \frac{p^2(p^2+1)}{(p^2-1)^2} \quad \text{for } p \mid r \\
E_1(p) &= \frac{p^5 - p^4 - p^3 - 4p^2 + 1}{(p-1)^3(p+1)^2} \quad \text{for } p \nmid 2r \\
E_2(p) &= \frac{p^4 + p^3 + 2p^2 - p - 1}{p(p-1)(p+1)^2} \quad \text{for } p \nmid 2r \\
E_3(p) &= 1 + \frac{1}{p(p+1)} = \frac{p^2 + p + 1}{p(p+1)} \\
\sum_{\gamma \geq 1} \frac{1}{p^{2\gamma} \phi(p^{2\gamma})} &= \frac{p}{(p-1)(p^4-1)} \\
\sum_{\substack{\gamma, \delta \geq 0 \\ \gamma < \delta}} \frac{1}{p^\gamma p^\delta \phi([p^{2\gamma}, p^{2\delta}])} &= \left(\frac{p}{p-1}\right)^2 \left(\frac{1}{p^3-1} - \frac{1}{p^4-1}\right) = \frac{p^5}{(p^4-1)(p^3-1)(p-1)}.
\end{aligned}$$

Replacing in the last expression for K_r , this gives

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

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 Equation (3.1) of [FM2]

$$\begin{aligned}
T(x) &= \sum_{p \leq x} \frac{h^2(-p)}{p^2} + 2 \sum_{p \leq x} \frac{h(-p)h(-4p)}{p^2} + \sum_{p \leq x} \frac{h^2(-4p)}{p^2} \\
&= T_{1,1}(x) + 2T_{1,4}(x) + T_{4,4}(x).
\end{aligned}$$

Proceeding as in Section 2, we write

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

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

Proceeding as in Section 3, we get

$$\hat{T}_{1,1}(x) \sim \left(\sum_{m,n=1}^{\infty} \frac{c_{2,2}^0(m,n)}{mn\phi([4m, 4n])} \right) x$$

where

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

When m and n are odd, we have

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

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

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

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

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

Proceeding similarly, we get

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

where

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

When m is odd, we have

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

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

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

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

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

Proceeding in the same way, we get

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

where

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

Here m and n are odd, and we have

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

Finally, putting the last 3 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.
- [DP] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves, *Mathematics Research Notices* **no 4** (1999), 165–183.
- [DKP] C. David, H. Kisilevsky and F. Pappalardi, Galois representations with non-surjective traces, *Can. J. Math.* **51** (1999), 936–951.
- [Dav] H. Davenport, *Multiplicative number theory*, Springer-Verlag, 1980.
- [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, *Can. J. Math.* **48** (1996), 81–104.
- [FM2] E. Fouvry and M. R. Murty, Supersingular primes common to two elliptic curves, *Number Theory (Paris, 1992–1993)*, 91–102, *London Math. Soc. Lecture Note Ser.*, **215**, Cambridge Univ. Press, 1995.
- [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*, Springer-Verlag Lecture Notes in Mathematics **504**, 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, *Publ. Math. IHES*, **54** (1982), 123–201.
- [Wil] B. M. Wilson, Proofs of some formulae enunciated by Ramanujan, *Proc. London Math. Soc.* **21** (1922), 235–255.

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

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

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