Average Lang–Trotter Conjecture

for 2 Elliptic Curves

Robert Juričević

A Thesis

in

The Department

of

Mathematics

Presented in Partial Fulfilment of the Requirements
for the degree of Masters of Science at
Concordia University
Montréal, Québec, Canada

August 2000

0-612-54295-5

ABSTRACT

Average Lang–Trotter Conjecture for 2 Elliptic Curves

Robert Juričević

Let E_1 and E_2 be two elliptic curves without complex multiplication over the rationals. For primes p of good reduction, let $a_p(E_1)$ and $a_p(E_2)$ be the traces of the Frobenius morphism of E_1 and E_2 respectively. By Hasse's theorem, we know that $a_p(E_i), i = 1, 2$, are integers and satisfy the inequality $|a_p(E_i)| \leqslant 2\sqrt{p}$. For fixed integers r_1 and r_2, we define

$$\pi_{E_1,E_2}^{r_1,r_2}(x) = \#(\{p \leqslant x \,:\, a_p(E_1) = r_1\} \cap \{p \leqslant x \,:\, a_p(E_2) = r_2\}).$$

The Lang–Trotter conjecture for 2 elliptic curves asserts that there exists a constant C_1 (depending on the elliptic curves E_1, E_2, and the fixed integers r_1, r_2) such that $\pi_{E_1,E_2}^{r_1,r_2}(x)$ is asymptotic to $C_1 \log\log x$. The average Lang–Trotter conjecture for 2 elliptic curves asserts that there exists a constant C_2 (depending only on the fixed integers r_1, r_2) such that $\frac{1}{A_1A_2B_1B_2}\sum_{|a_1|\leqslant A_1}\sum_{|a_2|\leqslant A_2}\sum_{|b_1|\leqslant B_1}\sum_{|b_2|\leqslant B_2}\pi_{E_1,E_2}^{r_1,r_2}(x)$ is asymptotic to $C_2 \log\log x$. Unfortunately, this does not imply the Lang–Trotter conjecture for any 2 elliptic curves E_1, E_2, but gives further evidence for it. This thesis presents an asymptotic result related to the average Lang–Trotter conjecture for 2 elliptic curves.

Acknowledgements

First, I want to thank my thesis advisor Chantal David. What better way than with a poem[1].

This Is Just To Say

so much depends

upon

my thesis advisor

chantal david

glazed with ideas

like pearls

beside the round, bright and beautiful nature of her

personality.

Second, I would like to thank Ram Murty for it was Ram and Peter Taylor (Math and Poetry) who inspired me at Queen's University, Kingston, to play with numbers. It was through Ram that I came to Le Centre Interuniversitaire Calcul Mathematique Algebraic (CICMA) and mathematics at Concordia. His energy has no bounds

[1] This is a spin on two of my favorite poems by William Carlos Williams (1883-1963), namely *The Red Wheelbarrow* and *This Is Just To Say*, extracted from *The Broadview Anthology of Poetry, pg. 432, 433*, and a remark by Paulo Ribenboim on the proof of the infinitude of primes by Kummer.

(as is evident in the energy he passes on to his students, notably Chantal) and his kindness is second to none. During *Theme Year in Number Theory* festivities last year in Montreal, he gave me the opportunity to get my fingers dirty in hard core number theory by allowing me to take formal notes for his mini course on Sieve methods. This opportunity taught me the meaning of the following remark by Ram taken from a recent book he wrote on analytic number theory: *Unless the student is able to sift out from the mass of theory the underlying techniques, his/her understanding will only be academic and not that of a participant in research.*

Third, I would like to thank Amir Akbary. Ram inspired me to consider analytic number theory, Amir taught me analytic number theory. It was through Amir's winter of 99 course in analytic number theory that I finally started to understand the formal notes I had taken for Ram that past November. Furthermore, Amir played a crucial role in changing our direction in this present thesis by re-focusing our attention on the power of contour integration. Amir's gentle, kind and approachable manner and genuine interest in his students is second to none.

Fourth, I would like to thank Hershy Kisilevsky and his doctoral student Jack Fearnley. Their interest and energy towards number theory is unmatched.

Fifth, I would like to thank Francisco Thaine. My first course at Concordia was with Dr. Thaine in Algebraic number theory. A few weeks into the course I came across *Thaine's Theorem* for the first time in Washington's book. It humbled me beyond belief and taught me about my own academic mortality.

Sixth, I would like to thank the trio of David Ford, his post-doctoral researcher

Xavier Roblot, and his doctoral student Sebastian Pauli. During the sieve note project, it was Sebastian who introduced me to Latex and taught me the tricks. Through him I met David and Xavier over lunch and *Law and Order* on wednesday nights. We shared a beer and tomato juice on occasion as well.

Stopping here would be *perfect.*

However, I would like to thank Nevia, Diana, Nina and Ivan for keeping me real.

R.J.

Contents

Chapter 1

Introduction

Any natural number greater than 1 which has exactly 2 divisors is called a prime number, and is denoted by the lower case letter p. For example, $2, 17, 1093, 3511$, are prime numbers, whereas $4 = 2^2$, $105 = 3 \times 5 \times 7$, $187 = 11 \times 17$, $1729 = 7 \times 13 \times 19$, are not. In book 9 of Elements, Euclid (355-265) proves the existence of infinitely many primes. Analogously, we can ask similar questions regarding the distribution of primes in other sequences. Dirichlet (1805-1859) was the first to show there exist infinitely many primes in the arithmetic progression a, $a+k$, $a+2k$, ..., whenever the greatest common divisor of a and k is equal to 1. For example, $a = 3, k = 25$. Are there infinitely many primes p of the form $1 + n^2$ for some natural number n? In other words, are there infinitely many primes like $2 = 1+1^2$, $5 = 1+2^2$, $17 = 1+4^2$, $37 = 1 + 6^2$, $101 = 1 + 10^2$? This is an ancient problem in mathematics and its solution is unknown at present. The surprising thing is that this problem has a connection with the theory of elliptic curves. An *elliptic curve* E is a cubic equation in two variables of the form $y^2 = x^3 + ax + b$, where a and b are rational numbers. The equation defining E can be reduced modulo all but finitely many prime numbers

p. If the resulting equation is nonsingular over the finite field with p elements $\mathbb{Z}/p\mathbb{Z}$, then E is said to have *good reduction* at p. All but finitely many primes are primes of good reduction for a given E. Let N_p be the number of solutions (over the field $\mathbb{Z}/p\mathbb{Z}$) of the reduced equation, and set $a_p(E) = p+1-N_p$. The sequence $\{a_p(E)\}_p$ (indexed by the primes p of good reduction) encodes basic arithmetic information on E. By a theorem of Hasse we know that $a_p(E)$ is an integer which lies in the interval $-2\sqrt{p} \leqslant a_p(E) \leqslant 2\sqrt{p}$. The study of the distribution of $a_p(E)$'s is closely related to the study of the distribution of primes in certain sequences. For example, let E be the curve $y^2 = x^3 - x$. Then $a_p(E) = \pm 2$ if and only if $p = 1 + n^2$ for some natural number n. On the distribution of $a_p(E)$'s, an unsolved conjecture of Lang and Trotter asserts that for a fixed integer r, the number of primes $p \leqslant x$ such that $a_p(E) = r$, denoted $\pi_E^r(x)$, is roughly $\sqrt{x}/\log x$, as x approaches infinity, where $\log x$ is the natural logarithm of x. This conjecture seems extremely hard to prove. Elkies [Elk87] proved that for each elliptic curve E over the rationals, there are infinitely many primes such that $a_p(E) = 0$ (supersingular primes). But it is not known if there are infinitely many primes p such that $a_p(E) = r \neq 0$, for any E over the rationals. It is also known that the number of primes p such that $a_p(E) = r$ has density 0 in the set of all primes [Ser81].

In order to get further evidence for the Lang–Trotter conjecture, Murty and Fouvry showed in [FM96] that the Lang–Trotter conjecture is true on *average* in the supersingular case $r = 0$. David and Pappalardi generalized their work in [DP99] and showed that the Lang–Trotter conjecture is true on average for any $r \in \mathbb{Z}$. More precisely, they show that for any $r \in \mathbb{Z}$,

$$\frac{1}{4AB} \sum_{|a| \leqslant A} \sum_{|b| \leqslant B} \pi_E^r(x) \sim K_r \frac{\sqrt{x}}{\log x},$$

where K_r is a non–zero constant depending only on r. This thesis studies the distribution of $a_p(E)$'s associated to 2 elliptic curves E_1 and E_2. The Lang–Trotter conjecture for 2 elliptic curves asserts that for fixed integers r_1 and r_2, the number of primes $p \leqslant x$ such that $a_p(E_1) = r_1$ and $a_p(E_2) = r_2$, denoted $\pi_{E_1,E_2}^{r_1,r_2}(x)$, is asymptotic to $C_1 \log\log x$, as x approaches infinity, where C_1 is a constant depending on the fixed integers r_1, r_2, and E_1, E_2. This conjecture also seems extremely hard to prove; furthermore, as the set of primes in question is very sparse, no convincing numerical evidence can be obtained to verify the conjecture. In order to get evidence for the Lang–Trotter conjecture for 2 elliptic curves, Murty and Fouvry showed in [FM95] that the Lang–Trotter conjecture for 2 elliptic curves is true on average in the supersingular case $r_1 = r_2 = 0$. More precisely,

$$\frac{1}{16A_1A_2B_1B_2} \sum_{|a_1| \leqslant A_1} \sum_{|a_2| \leqslant A_2} \sum_{|b_1| \leqslant B_1} \sum_{|b_2| \leqslant B_2} \pi_{E_1,E_2}^{0,0}(x) \sim \frac{35}{96} \log\log x.$$

We study the general case $r_1, r_2 \in \mathbb{Z}$. In our proof of Theorem 1, we display the techniques we developed for a proof of the general case $r_1, r_2 \in \mathbb{Z}$; the average Lang–Trotter conjecture for 2 elliptic curves. We believe that these techniques, modulo a few unresolved technical problems, will enable us to prove the average Lang–Trotter conjecture for 2 elliptic curves. This work is in progress [ADJ00]. On the techniques, a result of Deuring coupled with partial summation links the average Lang–Trotter conjecture for 2 elliptic curves to an average of a product of special values of 2

L–series. We extend the techniques of [DP99] which involve an average of special values of 1 L–series. In particular, we give a new representation for a product of Dirichlet L–Functions $L(s, \chi_{d_1})L(s, \chi_{d_2})$, valid for non–trivial Dirichlet characters $\chi_{d_i}, i = 1, 2$, and $s = 1$, in lemma 4.1.

This thesis consists of 3 parts.

Part 1 (chapter 2) is concerned with the mathematical backround needed to state and prove Theorem 1 and lemma 4.1. The symbols and notation are standard for the most part but should be glanced over. The tools include partial summation, Dirichlet's Theorem on $\sum_{\substack{p \leqslant x \\ p \equiv a \bmod k}} \log p$, and Montgomery's result [Mon71] on the Barban–Davenport–Halberstam Theorem. The elementary lemmas are on properties of the arithmetic functions $d(n)$ and $\phi(n)$ used later in our work on $K(r)$. The analytic lemmas are backround for lemma 4.1, and Proposition 4.1.

Part 2 (chapter 3) is concerned with the Lang–Trotter conjecture, the average Lang–Trotter conjectures, and Deuring's link between the average Lang–Trotter conjectures and averages of special values of L–series. We state Theorem 1 and explain how it relates to the average Lang–Trotter conjecture for 2 elliptic curves.

Part 3 (chapter 4) is concerned with proving Theorem 1.

Chapter 2

Background

This chapter contains the mathematical backround needed to state and prove the results of the thesis.

2.1 Notation

2.1.1 List of Symbols

The following notation is standard for the most part:

$\mathbb{N} = \{\,1, 2, 3, \ldots\}$, the natural numbers.

The lower case letter p denotes a prime number. That is, $p \in \{\,2, 3, 5, 7, 11, 13, \ldots\}$.

$\mathbb{Z} = \{\,0, \pm 1, \pm 2, \ldots\}$, the integers.

$\mathbb{Z}^+ = \mathbb{N} \cup \{0\}$, the non-negative integers.

$\mathbb{Q} = \{\,\frac{a}{b} \,:\, a \in \mathbb{Z}, b \in \mathbb{N}\}$, the rational numbers.

$\mathbb{Q}^c$, the irrational numbers. For example, $\sqrt{2}, \pi, e \in \mathbb{Q}^c$.

$\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c$, the real numbers.

$\mathbb{C} = \{\,a + bi \,:\, a, b \in \mathbb{R}, i = \sqrt{-1}\,\}$, the complex numbers.

$\mathbb{C}^*$, the multiplicative group of complex numbers.

$\mathbb{F}_p = \{0, 1, 2, \ldots, p-2, p-1\}$, the finite field of prime p elements. Note that sometimes we write $\mathbb{Z}/p\mathbb{Z}$ instead of $\mathbb{F}_p$.

$\mathbb{F}_p^* = \{1, 2, \ldots, p-2, p-1\} = (\mathbb{Z}/p\mathbb{Z})^*$.

$[x]$, the integer part of the real number x, that is, the integer uniquely determined by the inequality $[x] \leqslant x < [x] + 1$.

$\{x\}$, the fractional part of the real number x, that is, $\{x\} = x - [x] \in [0, 1)$.

$(n_1, n_2), n_i \in \mathbb{N}, i = 1, 2$ denotes an ordered pair.

$a|b$, a divides b ($b = ak$ for some $k \in \mathbb{Z}$).

$a \nmid b$, a does not divide b.

$b \equiv a \bmod m$, means $m|b - a$.

$(a_1, \ldots, a_n)$, the greatest common divisor of the integers $a_1, \ldots, a_n$.

$[a_1, \ldots, a_n]$, the least common multiple of the integers $a_1, \ldots, a_n$.

$\#X$, the cardinality of the set X.

$|x|$, absolute value of x. That is, $|x| = \sqrt{x^2}$.

$\overset{\text{con}}{=}$, equality holds by convention.

$\overset{\text{def}}{=}$, equality holds by definition.

$\approx$, approximately equal.

$\neq$, equality does not hold.

$\leftrightarrow$, two sets are in one-to-one correspondence.

$\Leftrightarrow$, if and only if.

$\mapsto$, maps to.

We write $\log x$ to mean $\log_e x$; $e^{\log_e x} = x$.

MT denotes main term, while **ET** denotes error term.

ET0i denotes error term number i, where $i = 1, 2, 3, 4, 5, 6, 7, 8$.

Respecting Euclid, we write **Q.E.D.** (Quad Erat Demonstradum) to denote the end of a proof.

Greek alphabet

α, *alpha.*

β, *beta.*

Γ, γ, *gamma.*

Δ, δ, *delta.*

ϵ, *epsilon.*

η, *eta.*

ζ, *zeta.*

Θ, θ, *theta.*

ι, *iota.*

κ, *kappa.*

Λ, λ, *lambda.*

μ, *mu.*

ν, *nu.*

Ξ, ξ, *xi.*

o, *omicron.*

Π, π, *pi*, where $\prod_{p|r}$ is read the product over all prime p dividing r.

ρ, *rho.*

Σ, σ, *sigma*, where $\sum_{p \leqslant x}$ is read the sum over all prime p up to x.

τ, *tau*.

Υ, υ, *upsilon*.

Φ, ϕ, *phi*.

χ, *chi*.

Ψ, ψ, *psi*.

Ω, ω, *omega*.

2.1.2 The Big O and Little o Notation.

Let f be any real or complex-valued function, and let g be a positive function. The functions f and g can be functions of a real variable x or arithmetic functions defined only on the positive integers. Respecting Landau's notation, we write

$$f = O(g),$$

or respecting Vinogradov's notation,

$$f \ll g,$$

or

$$g \gg f,$$

if there exists a constant $c > 0$ such that

$$|f(x)| \leqslant cg(x),$$

for all x in the domain of f. The constant c is called the *implied constant.*

We write

$$f \ll_{\mathcal{A},\mathcal{B},\ldots} g,$$

if there exists a constant $c > 0$ that depends on $\mathcal{A}, \mathcal{B}, \ldots$ such that

$$|f(x)| \leqslant cg(x),$$

for all x in the domain of f.

We write

$$f = o(g),$$

if

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.$$

The function f is *asymptotic* to g, denoted

$$f \sim g,$$

if

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$

We make use of the following properties of the O notation.

1. If $f \ll g$ and $g \ll h$, then $f \ll h$.
2. If $f_1 = O(g_1)$ and $f_2 = O(g_2)$, then $f_1 f_2 = O(g_1 g_2)$ and $f_1 + f_2 = O(g_1 + g_2) = O(max(g_1, g_2))$.
3. If $f \ll g$ on $[a, b]$, then $\int_a^b f \ll \int_a^b g$ for $x \in [a, b]$.

Note that the second properties follow from the properties of the absolute value metric. Namely, $|f_1 f_2| = |f_1||f_2|$ and $|f_1 + f_2| \leqslant |f_1| + |f_2| \leqslant 2\max(|f_1|, |f_2|)$. To see the third property recall that if $cg \geqslant |f|$, then $cg - |f| \geqslant 0$, so that $\int_a^b (cg - |f|) \geqslant 0$, which is equivalent to $c\int_a^b g - \int_a^b |f| \geqslant 0$, which is equivalent to

$$c\int_a^b g \geqslant \int_a^b |f| \geqslant \left|\int_a^b f\right|.$$

2.1.3 Conventions

We adhere to the usual convention that the *empty sum* (the sum containing no terms) is equal to zero and the *empty product* is equal to one. We remark on some conventions in analysis.

We write $\int_{(c)}$ to mean we are integrating over the line $c \pm i\infty$. That is, from $c - i\infty$, to $c + i\infty$. Furthermore, we define what we mean when we say that a function is *holomorphic*, *analytic*, *regular*, or *meromorphic*. The point is that *holomorphic*, *analytic*, and *regular* are synonyms so that authors use these words interchangeably.

Definition A *holomorphic* function is a single-valued, continuous, and differentiable function of a complex variable.

The synonyms of holomorphic are *analytic* and *regular*.

Definition A *meromorphic* function is *analytic* except at a finite number of poles.

2.2 Tools

Our tool belt consists of partial summation, a lemma comparing a sum and an integral which will be needed in our work on the error terms in the following chapters, for $\alpha > 0, \beta > 0$, a lemma comparing $(\log x)^{\beta}$ and x^{α} as $x \to \infty$ which will also be needed in our work on the error terms in the following chapters, a big theorem by Dirichlet, and a result by Montgomery on the Barban–Davenport–Halberstam theorem.

Tool 1: Partial Summation. Let $x \in \mathbb{N}$, and $A_n \overset{\text{def}}{=} \sum_{1 \leqslant m \leqslant n} a_m$, where $\{a_i\}_{i=1}^{\infty}$ is a sequence of complex numbers. Then

$$\begin{aligned}\sum_{1\leqslant n\leqslant x} a_n b_n &= \sum_{1\leqslant n\leqslant x} (A_n - A_{n-1}) b_n \\ &= \sum_{1\leqslant n\leqslant x} A_n b_n - \sum_{1\leqslant n\leqslant x-1} A_n b_{n+1} \\ &= \sum_{1\leqslant n\leqslant x-1} A_n (b_n - b_{n+1}) + A_x b_x.\end{aligned}$$

This is called Abel's partial summation formula. If $f(t)$ is a continuous function on $[1, x]$, we get the following Stieltjes[1] integral analog.

Lemma 2.1 (Partial summation formula) *For any arithmetical function* $a(n) : \mathbb{N} \to \mathbb{C}$, *let* $A(x) \overset{\text{def}}{=} \sum_{n\leqslant x} a(n)$, *where* $A(x) = 0$ *if* $x < 1$. *Assume* f *has a continuous derivative on the interval* $[1, x]$. *Then*

$$\sum_{n\leqslant x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t) dt.$$

Proof Let $x \in \mathbb{N}$. Since $A(n)$ is a step function we have

$$\begin{aligned}\sum_{n\leqslant x} a(n) f(n) &= \sum_{n\leqslant x} [A(n) - A(n-1)] f(n) \\ &= \sum_{n\leqslant x} A(n) f(n) - \sum_{n\leqslant x-1} A(n) f(n+1) \\ &= A(x) f(x) - \sum_{n\leqslant x-1} A(n) \int_n^{n+1} f'(t) dt\end{aligned}$$

[1] The Dutch mathematician Thomas Stieltjes (1856-1894) was responsible for the notion of integrating one function with respect to another function. Notice $\int_1^x A(t) df(t) = \int_1^x A(t) f'(t) dt$.

$$\begin{aligned} &= A(x)f(x) - \sum_{n \leqslant x-1} \int_n^{n+1} A(t)f'(t)dt \\ &= A(x)f(x) - \int_1^x A(t)f'(t)dt. \end{aligned}$$

For $x \in \mathbb{R}$,

$$\sum_{n \leqslant [x]} a(n)f(n) = A([x])f([x]) - \int_1^{[x]} A(t)f'(t)dt.$$

Noting $A(x) = A([x])$,

$$\sum_{n \leqslant [x]} (\cdots) = \sum_{n \leqslant x} (\cdots),$$

and $\int_{[x]}^x A(t)f'(t)dt = A(x)\left(f(x) - f([x])\right)$ gives the general result.

Q.E.D.

Tool 2: Comparing a Sum and an Integral.

Lemma 2.2 *Let $a, b \in \mathbb{Z}, a < b$ and $f(t)$ a monotonic function on $[a, b]$. Then*

$$\min(f(a), f(b)) \leqslant \sum_{k=a}^{b} f(k) - \int_a^b f(t)dt \leqslant \max(f(a), f(b)).$$

Proof If $f(t)$ is increasing on $[a, b]$, then $f(k) \leqslant \int_k^{k+1} f(t)dt$ for $k = a, a+1, ..., b-1$, and $f(k) \geqslant \int_{k-1}^{k} f(t)dt$ for $k = a+1, ..., b$. It follows that

$$\sum_{k=a}^{b} f(k) = \sum_{k=a}^{b-1} f(k) + f(b) \leqslant \int_a^b f(t)dt + f(b),$$

and $\sum_{k=a}^{b} f(k) = \sum_{k=a+1}^{b} f(k) + f(a) \geqslant \int_a^b f(t)dt + f(a)$. Thus

$$f(a) \leqslant \sum_{k=a}^{b} f(k) - \int_a^b f(t)dt \leqslant f(b).$$

Similarly, if $f(t)$ is decreasing, then $f(b) \leqslant \sum_{k=a}^{b} f(k) - \int_a^b f(t)dt \leqslant f(a)$.

Q.E.D.

Tool 3: Comparing $(\log x)^\alpha$ and x^β for Every $\alpha > 0, \beta > 0$.

Lemma 2.3 *For every $\alpha > 0, \beta > 0$, $(\log x)^\alpha = o\left(x^\beta\right)$.*

Proof By ℓ'Hopital's rule we see

$$\begin{aligned}
\lim_{x\to\infty} \frac{(\log x)^\alpha}{x^\beta} &= \lim_{x\to\infty} \frac{\alpha(\log x)^{\alpha-1}}{\beta x^\beta} \\
&= \lim_{x\to\infty} \frac{\alpha(\alpha-1)(\log x)^{\alpha-2}}{\beta^2 x^\beta} \\
&= \lim_{x\to\infty} \frac{\alpha(\alpha-1)(\alpha-2)(\log x)^{\alpha-3}}{\beta^3 x^\beta} \\
&= \cdots \\
&= 0.
\end{aligned}$$

Q.E.D.

Tool 4: Dirichlet's Theorem.

Lemma 2.4 (Dirichlet) *Let*

$$\psi(x; n, a) \overset{\text{def}}{=} \sum_{\substack{p \leqslant x \\ p \equiv a \bmod n}} \log p.$$

Then for $(a, n) = 1$,

$$\psi(x; n, a) = \frac{x}{\phi(n)} + E(x; n, a),$$

where $E(x; n, a) = o(x)$.

Tool 5: Barban–Davenport–Halberstam Theorem.

Lemma 2.5 (Montgomery,[Mon71]) *Let*

$$E_1(x; k, a) \overset{\text{def}}{=} \sum_{\substack{p \leqslant x \\ p \equiv a \bmod k}} \log p - \frac{x}{\phi(k)}.$$

For $1 \leqslant Q \leqslant x$, and any $A > 0$,

$$\sum_{k \leqslant Q} \sum_{\substack{0 < a \leqslant k \\ (a,k)=1}} E_1^2(x; k, a) = Qx \log Q + O\left(Qx + \frac{x^2}{(\log x)^A}\right).$$

More precisely, for $\frac{x}{(\log x)^A} \leqslant Q \leqslant x$,

$$\sum_{k \leqslant Q} \sum_{\substack{1 \leqslant a \leqslant k \\ (a,k)=1}} E_1^2(x; k, a) \ll Qx \log x.$$

2.3 Elementary Lemmas

Here we define the divisor function $d(n)$, Euler's ϕ function and prove related properties. Note that *elementary* means elementary in a technical sense; the proofs avoid the use of complex analysis.

Definition For $n \in \mathbb{N}$, we let $d(n)$ denote the number of divisors of n,

$$d(n) \stackrel{\text{def}}{=} \sum_{\delta | n} 1.$$

Definition An arithmetic function $f : \mathbb{N} \to \mathbb{C}$ is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. Further, $f(n)$ is completely multiplicative if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

Lemma 2.6 *The following properties hold for* $d(n)$.

1. $d(n)$ *is multiplicative.*

2. *For every* $\epsilon > 0$, $d(n) \ll_\epsilon n^\epsilon$.

3. $\sum_{n \leqslant x} d(n) = x \log x + O(x)$.

Proof 1. Let $p_1, ..., p_k$ be prime numbers that divide $m, n \in \mathbb{N}$. For $\alpha_i, \beta_i \in \mathbb{Z}^+$ we have $m = \prod_{i=1}^k p_i^{\alpha_i}, n = \prod_{i=1}^k p_i^{\beta_i}$. Then $d(mn) = \prod_{i=1}^k (\alpha_i + \beta_i + 1)$. If $(m, n) = 1$, then $\alpha_i = 0$ or $\beta_i = 0$ for each $i = 1, ..., k$. Hence $(\alpha_i + \beta_i + 1) = (\alpha_i + 1)(\beta_i + 1)$

and $d(mn) = \prod_{i=1}^{k}(\alpha_i + \beta_i + 1) = \prod_{i=1}^{k}(\alpha_i + 1)\prod_{i=1}^{k}(\beta_i + 1) = d(m)d(n)$. That is, $d(n)$ is multiplicative.

2. Let $f(n) = \frac{d(n)}{n^\epsilon}$. We show $f(n) = o(1)$. Since $d(n)$ and n^ϵ are multiplicative, $f(n)$ is multiplicative and it is enough[2] to show that $\lim_{p^k \to \infty} f(p^k) = 0$.

By ℓ'Hopital's rule, $\frac{k+1}{2^{k\epsilon/2}}$ is bounded for $k \geqslant 1$ (see proof of Lemma 2.3). It follows that

$$\begin{aligned} f(p^k) &= \frac{d(p^k)}{p^{k\epsilon}} \\ &= \frac{k+1}{p^{k\epsilon}} \\ &= \left(\frac{k+1}{p^{k\epsilon/2}}\right)\left(\frac{1}{p^{k\epsilon/2}}\right) \\ &\leqslant \left(\frac{k+1}{2^{k\epsilon/2}}\right)\left(\frac{1}{p^{k\epsilon/2}}\right) \\ &\ll \left(\frac{1}{p^k}\right)^{\epsilon/2}. \end{aligned}$$

Letting $p^k \to \infty$, $\left(\frac{1}{p^k}\right)^{\epsilon/2} \to 0$, and we see that $\lim_{p^k \to \infty} f(p^k) = 0$ as desired.

3. Since $[\frac{x}{\delta}] = \frac{x}{\delta} + O(1)$,

$$\begin{aligned} \sum_{n \leqslant x} d(n) &= \sum_{n \leqslant x}\sum_{\delta | n} 1 \\ &= \sum_{\delta \leqslant x}\left[\frac{x}{\delta}\right] \\ &= \sum_{\delta \leqslant x}\left\{\frac{x}{\delta} + O(1)\right\} \\ &= x\sum_{\delta \leqslant x}\frac{1}{\delta} + O(x). \end{aligned}$$

By Lemma 2.1,

$$\sum_{\delta \leqslant x}\frac{1}{\delta} = \log x + O(1).$$

Q.E.D.

[2] See [HW64], pg. 260.

Definition For $n \in \mathbb{N}$,

$$\phi(n) \overset{\text{def}}{=} \#\{1 \leqslant j \leqslant n \,:\, (j,n) = 1\}.$$

ϕ is called Euler's ϕ function.

Lemma 2.7 *The following properties hold for ϕ.*

1. *ϕ is multiplicative.*

2. *$\phi(ab) \geqslant \phi(a)\phi(b)$.*

3. *If $b|a$, $\phi(ab) = b\phi(a)$.*

4. *$\phi(ab) = (a,b)\phi([a,b])$.*

5. *$\phi((a,b))\phi([a,b]) = \phi(a)\phi(b)$.*

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

Proof 1. See [HW64], pg. 53.

2. Let $p_1, \ldots, p_k$ be prime numbers that divide $a, b \in \mathbb{N}$. Then for $\alpha_i, \beta_i \in \mathbb{Z}^+$, $a = \prod_{i=1}^k p_i^{\alpha_i}$, $b = \prod_{i=1}^k p_i^{\beta_i}$, and $ab = \prod_{i=1}^k p_i^{\alpha_i+\beta_i}$. Since ϕ is multiplicative,

$$\begin{aligned}\phi(a) &= \prod_{p|a} \phi(p^\alpha) = \prod_{p|a} p^\alpha(1-p^{-1}) = a\prod_{p|a}(1-p^{-1}),\\ \phi(b) &= b\prod_{p|b}(1-p^{-1}),\end{aligned}$$

and

$$\phi(ab) = ab\prod_{p|ab}(1-p^{-1}).$$

Recall if $p|ab$, then $p|a$ or $p|b$. Since $\frac{1}{2} \leqslant (1-p^{-1}) < 1$, it follows that

$$\prod_{p|ab}(1-p^{-1}) \geqslant \prod_{p|a}(1-p^{-1})\prod_{p|b}(1-p^{-1}),$$

from which we deduce the result.

3. If $b|a$, then $\alpha_i - \beta_i \geqslant 0$ for all i. Since ϕ is multiplicative, and $\phi(p^\alpha) = p^{\alpha-1}(p-1)$, we have

$$\begin{aligned}
\phi(ab) &= \prod_{i=1}^{k} \phi(p_i^{\alpha_i+\beta_i}) \\
&= \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i-1}(p_i - 1) \\
&= \prod_{i=1}^{k} p_i^{\beta_i}\phi(p_i^{\alpha_i}) \\
&= b\phi(\prod_{i=1}^{k} p_i^{\alpha_i}) \\
&= b\phi(a).
\end{aligned}$$

4. Since $ab = [a,b](a,b)$, and (a,b) divides $[a,b]$, by part 3

$$\phi(ab) = \phi([a,b](a,b)) = (a,b)\phi([a,b]).$$

5. Let a, b be defined as above. We have $\{\max(\alpha_i,\beta_i), \min(\alpha_i,\beta_i)\} = \{\alpha_i, \beta_i\}$. Since ϕ is multiplicative, it follows that

$$\begin{aligned}
\phi([a,b])\phi((a,b)) &= \prod_{i=1}^{k} \phi(p_i^{\max(\alpha_i,\beta_i)}) \prod_{i=1}^{k} \phi(p_i^{\min(\alpha_i,\beta_i)}) \\
&= \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) \prod_{i=1}^{k} \phi(p_i^{\beta_i}) \\
&= \phi(a)\phi(b).
\end{aligned}$$

6. By part 4 $\phi(ab) = (a,b)\phi([a,b])$. Since $\phi([a,b]) = \frac{\phi(a)\phi(b)}{\phi((a,b))}$ by part 5, we deduce the result.

Q.E.D.

2.4 Analytic Lemmas

The fundamental difference between the methods found in David's and Pappalardi's paper [DP99] and our methods is an expression for the product $L(1,\chi_{d_1})L(1,\chi_{d_2})$ using contour integration. Here we recall definitions and prove lemmas which we use in our proof of lemma 4.1 that given $\epsilon > 0, U > 1$,

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

where $\chi_{d_i} = \left(\frac{d_i}{n}\right), i = 1,2$ are non-trivial Dirichlet[3] characters. In addition, we prove lemmas called in our work on error terms **ET02, ET03** and **ET08**.

Let $s = \sigma + it \in \mathbb{C}$. The next lemma allows us to interchange an infinite sum and integral.

Lemma 2.8 *Let $f(s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s}$ be a Dirichlet series absolutely convergent in $\sigma > c-\epsilon$, and let $g(s)$ be a meromorphic function with no poles on the line $\sigma = c$. Then*

$$\int_{(c)} f(s)g(s)ds = \sum_{n=1}^{\infty} a_n \int_{(c)} \frac{g(s)}{n^s}ds,$$

provided that

$$\int_{-\infty}^{\infty}|g(c+it)|dt$$

is convergent.

[3] Consider the group $(\mathbb{Z}/q\mathbb{Z})^*$. A homomorphism $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ is called a *Dirichlet character* modulo q. Since $(\mathbb{Z}/q\mathbb{Z})^*$ has order $\phi(q)$, and by Euler's theorem, $a^{\phi(q)} \equiv 1 \bmod q$, then we must have $(\chi(a))^{\phi(q)} = 1$ for all $a \in (\mathbb{Z}/q\mathbb{Z})^*$. Thus $\chi(a)$ must be a $\phi(q)^{th}$ root of unity. We extend the definition of χ to all integers by setting $\chi(n) = \chi(n \bmod q)$, if $(n,q) = 1$, and 0 otherwise. The character $\chi_0 : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ satisfying $\chi_0(a) = 1$ for all $(a,q) = 1$ is called the trivial character (or principal) character.

Proof The proof of lemma 2.8 is based on the following fact. If $u_n(x) \geqslant 0$ for all values of n and x, and

$$\int_a^b \left\{ \sum_{n\geqslant 1} u_n(x) \right\} = \sum_{n\geqslant 1} \int_a^b u_n(x)dx,$$

for all finite values of b, then

$$\int_a^\infty \left\{ \sum_{n\geqslant 1} u_n(x) \right\} dx = \sum_{n\geqslant 1} \int_a^\infty u_n(x)dx,$$

provided that either side is convergent. It can be shown that this fact remains true for functions $u_n(x)$ which are real or complex provided that either of

$$\int_a^\infty \left\{ \sum_{n\geqslant 1} |u_n(x)| \right\} dx,$$

or

$$\sum_{n\geqslant 1} \int_a^\infty |u_n(x)|dx,$$

is convergent. To complete the proof of lemma 2.8, note that $f(s)$ is uniformly convergent on the compact subsets of the line $\sigma = c$, and therefore we can interchange the sum and the integral over the finite intervals.

Q.E.D.

We define the Γ–function by Euler's formula. That is,

$$\Gamma(s) \overset{\text{def}}{=} \int_0^\infty e^{-t} t^{s-1} dt, \quad \sigma > 0.$$

Note that the inversion formula for $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$ is given by[4]

$$e^{-t} = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \Gamma(s) t^{-s} ds, \quad c > 0.$$

[4] For a proof see [KM84], pg. 82, 83.

To apply lemma 2.8 in our work on $L(1,\chi_{d_1})L(1,\chi_{d_2})$, we need to know the following facts about the Γ function.

Lemma 2.9 (Stirling's formula)

$$|\Gamma(\sigma+it)| = \sqrt{2\pi}e^{-\frac{1}{2}\pi|t|}|t|^{\sigma-\frac{1}{2}}\left\{1+r(\sigma,t)\right\},$$

where $r(\sigma,t)\to 0$, while $|t|\to\infty$, and $|\sigma|\leqslant\alpha$. Here α is a fixed constant.

Proof See [Tit78], pg. 58.

Lemma 2.10

$$\int_{-\infty}^{\infty}|\Gamma(1+it)|dt<\infty.$$

Proof By lemma 2.9,

$$|\Gamma(1+it)| = \sqrt{2\pi}e^{-\frac{1}{2}\pi|t|}|t|^{\frac{1}{2}}\{1+r(1,t)\}.$$

We write

$$\int_{-\infty}^{\infty}|\Gamma(1+it)|dt=\left\{\int_{-\infty}^{-1}+\int_{-1}^{1}+\int_{1}^{\infty}\right\}|\Gamma(1+it)|dt.$$

Consider the middle integral.

$$\begin{aligned}\int_{-1}^{1}|\Gamma(1+it)|dt \ll \int_{-1}^{1}e^{-\frac{1}{2}\pi|t|}|t|^{\frac{1}{2}}dt &\ll \int_{-\pi/2}^{\pi/2}e^{-|t'|}\left|\frac{2t'}{\pi}\right|^{\frac{1}{2}}dt'\\ &\ll \int_{-\pi/2}^{\pi/2}e^{-|t'|}dt'\\ &\ll 1.\end{aligned}$$

For the others, since $r(1,t)\to 0$ as $|t|\to\infty$, there exists a $k\in\mathbb{N}$ such that $\sqrt{2\pi}(1+r(1,t))\leqslant k$, so

$$\int_{-\infty}^{-1}\sqrt{2\pi}e^{-\frac{1}{2}\pi|t|}|t|^{1/2}(1+r(1,t))dt\leqslant k\int_{-\infty}^{-1}e^{-\frac{1}{2}\pi|t|}|t|^{\frac{1}{2}}dt,$$

and

$$\int_1^\infty \sqrt{2\pi} e^{-\frac{1}{2}\pi|t|}|t|^{1/2}(1+r(1,t))dt \leqslant k\int_1^\infty e^{-\frac{1}{2}\pi|t|}|t|^{\frac{1}{2}}dt.$$

The integrals on the right hand side of the last two inequalities are the same because t is in absolute value. Putting $u = \frac{1}{2}\pi t, du = \frac{1}{2}\pi dt$ in the second gives

$$\frac{2k}{\pi}\int_{\pi/2}^\infty e^{-u}\left|\frac{2u}{\pi}\right|^{\frac{1}{2}} du = \frac{2k}{\pi}\left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_{\frac{\pi}{2}}^\infty e^{-u}u^{\frac{1}{2}}du,$$

which is absolutely convergent as $\Gamma(s)$ is absolutely convergent for $\sigma > 0$.

Q.E.D.

We use lemma 2.11 in our proof of lemma 2.12. First we define the Riemann $\zeta-$ function. By definition, for $s = \sigma + it \in \mathbb{C}$,

$$\zeta(s) \stackrel{\text{def}}{=} \sum_{n\geqslant 1}\frac{1}{n^s}.$$

Lemma 2.11 *Let* $0 < \delta < 1, c \geqslant \delta$. *For* $\sigma \in [\delta, c], t \geqslant 1$,

$$\zeta(\sigma + it) = O_\delta\left(t^{1-\delta}\right).$$

Proof It follows by lemma 2.1, where $\{t\} = t - [t]$ is the fractional part of t, that

$$\begin{aligned}
\zeta(s) &= \frac{s}{s-1} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt \\
&= \frac{s}{s-1} - s\left\{\int_1^x \frac{\{t\}}{t^{s+1}}dt + \int_x^\infty \frac{\{t\}}{t^{s+1}}dt\right\} \\
&= \sum_{n\leqslant x}\frac{1}{n^s} + \frac{1}{(s-1)x^{s-1}} + \frac{\{x\}}{x^s} - s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt.
\end{aligned}$$

For $x \geqslant 1, \sigma \geqslant \delta, 0 < \delta < 1$,

$$\begin{aligned}
|\zeta(s)| &\leqslant \sum_{n\leqslant x}\frac{1}{n^\sigma} + \frac{1}{|s-1|x^{\sigma-1}} + \frac{1}{x^\sigma} + |s|\int_x^\infty \frac{dt}{t^{\sigma+1}} \\
&\leqslant \sum_{n\leqslant x}\frac{1}{n^\sigma} + \frac{1}{tx^{\sigma-1}} + \frac{1}{x^\sigma} + \left(1 + \frac{t}{\sigma}\right)\frac{1}{x^\sigma}
\end{aligned}$$

$$\begin{aligned} &\leqslant \sum_{n\leqslant x}\frac{1}{n^{\sigma}}+\frac{1}{tx^{\delta-1}}+\left(2+\frac{t}{\delta}\right)\frac{1}{x^{\delta}} \\ &\leqslant \int_0^x \frac{dt}{t^{\sigma}}+\frac{1}{tx^{\delta-1}}+\left(2+\frac{t}{\delta}\right)\frac{1}{x^{\delta}} \\ &= \frac{1}{1-\sigma}x^{1-\sigma}+\frac{1}{tx^{\delta-1}}+\left(2+\frac{t}{\delta}\right)\frac{1}{x^{\delta}}. \end{aligned}$$

Choosing $x = t$, $(x \geqslant 1, t \geqslant 1)$ gives

$$|\zeta(s)| \leqslant \frac{t^{1-\delta}}{1-c}+t^{-\delta}+2t^{-\delta}+\frac{t^{1-\delta}}{\delta}.$$

For $t \geqslant 1, t^{1-\delta}$ dominates $t^{-\delta}$, so that

$$|\zeta(s)| = O\left(\frac{t^{1-\delta}}{1-c}+\frac{t^{1-\delta}}{\delta}\right) = O_{\delta}\left(t^{1-\delta}\right).$$

Q.E.D.

We recall lemma 2.12 in our work on **ET02**. Furthermore, we recall the method of proving lemma 2.12 at the end of our work on **ET08**.

Lemma 2.12 *For any $U > 1$,*

$$\sum_{n=1}^{\infty}\frac{d(n)}{n}e^{-\frac{n}{U}} = \frac{1}{2}(\log U)^2+2\gamma\log U+B+O\left(\frac{1}{\sqrt{U}}\right),$$

where B is a constant independent of U.

Proof By lemma 2.8, for $c > 0$,

$$\begin{aligned} \sum_{n=1}^{\infty}\frac{d(n)}{n}e^{-\frac{n}{U}} &= \sum_{n=1}^{\infty}\frac{d(n)}{n}\frac{1}{2\pi i}\int_{(c)}\Gamma(s)\left(\frac{U}{n}\right)^{s}ds \\ &= \frac{1}{2\pi i}\int_{(c)}\left(\sum_{n=1}^{\infty}\frac{d(n)}{n^{s+1}}\right)\frac{\Gamma(s+1)U^{s}}{s}ds \\ &= \frac{1}{2\pi i}\int_{(c)}\zeta^{2}(s+1)\frac{\Gamma(s+1)U^{s}}{s}ds. \end{aligned}$$

Recall that the Laurent expansion of $\zeta(s)$ at $s = 1$ looks like

$$\zeta(s) = \frac{1}{s-1}+\gamma+a_1(s-1)+a_2(s-1)^2+\cdots,$$

so that the Laurent expansion of $\zeta(s+1)$ at $s=0$ looks like

$$\zeta(s+1)=\frac{1}{s}+\gamma+a_1s+a_2s^2+\cdots,$$

which implies

$$\zeta^2(s+1)=\frac{1}{s^2}+\frac{2\gamma}{s}+(2+\gamma)a_1+(2a_2+a_1\gamma)s+\cdots.$$

Further,

$$U^s=e^{s\log U}=1+\frac{\log U}{1!}s+\frac{(\log U)^2}{2!}s^2+\frac{(\log U)^3}{3!}s^3+\cdots.$$

Since $\Gamma(1)=1$, therefore

$$\begin{aligned}
&Res_{s=0}\frac{\zeta^2(s+1)\Gamma(s+1)U^s}{s}\\
&= Res_{s=0}\left(\frac{1}{s^2}+\frac{2\gamma}{s}+(2+\gamma)a_1+(2a_2+a_1\gamma)s+\cdots\right)\times\\
&\times \left(\frac{1}{s}+\frac{\log U}{1!}+\frac{(\log U)^2}{2!}s+\frac{(\log U)^3}{3!}s^2+\cdots\right)\\
&= \frac{1}{2}(\log U)^2+2\gamma\log U+(2+\gamma)a_1.
\end{aligned}$$

Let $R_{c,-\frac{1}{2},\pm iT}$, $|T|>1$ denote the boundary of the rectangle with vertices $c\pm iT$, $-\frac{1}{2}\pm iT$. Then by Cauchy's residue theorem[5],

$$\frac{1}{2\pi i}\int_{R_{c,-\frac{1}{2},\pm iT}}\zeta^2(s+1)\frac{\Gamma(s+1)}{s}U^s ds=\frac{1}{2}(\log U)^2+2\gamma\log U+(2+\gamma)a_1.$$

That is,

$$\begin{aligned}
&\frac{1}{2\pi i}\left\{\int_{c-iT}^{c+iT}+\int_{c+iT}^{-\frac{1}{2}+iT}+\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT}+\int_{-\frac{1}{2}-iT}^{c-iT}\right\}\zeta^2(s+1)\frac{\Gamma(s+1)}{s}U^s ds\\
&= \frac{1}{2}(\log U)^2+2\gamma\log U+(2+\gamma)a_1.
\end{aligned}$$

[5] See [Tit78], pg. 102.

Since $\zeta(\sigma+1+iT) \ll T^{\frac{1}{2}}$ for $\sigma \in [-\frac{1}{2}, c], T > 1$, by lemma 2.11, for $U > 1$,

$$\begin{aligned}
&\left|\frac{1}{2\pi i}\int_{c+iT}^{-\frac{1}{2}+iT} \zeta^2(s+1)\frac{\Gamma(s+1)}{s}U^s ds\right| \\
&= \frac{1}{2\pi}\left|\int_{c}^{-\frac{1}{2}} \zeta^2(\sigma+1+iT)\Gamma(\sigma+1+iT)\frac{U^{\sigma+iT}}{\sigma+iT}d\sigma\right| \\
&\leqslant \frac{1}{2\pi}\int_{-\frac{1}{2}}^{c} |\zeta^2(\sigma+1+iT)||\Gamma(\sigma+1+iT)|\frac{U^{\sigma}}{\sqrt{\sigma^2+T^2}}d\sigma \\
&\ll \frac{U^c}{T}\int_{-\frac{1}{2}}^{c} |\zeta^2(\sigma+1+iT)||\Gamma(\sigma+1+iT)|d\sigma \\
&\ll U^c e^{-\frac{1}{2}\pi T}\int_{-\frac{1}{2}}^{c} T^{\sigma+\frac{1}{2}}d\sigma \\
&\ll U^c e^{-\frac{1}{2}\pi T}T^{c+\frac{1}{2}}\left(c+\frac{1}{2}\right),
\end{aligned}$$

which goes to 0 as $T \to \infty$. The same argument shows that

$$\frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{c-i\infty} \zeta^2(s+1)\frac{\Gamma(s+1)}{s}U^s ds = 0.$$

Since $\zeta\left(\frac{1}{2}+it\right) \ll t^{1/2}$ for $t > 1$ by lemma 2.11, and $(\frac{1}{4}+t^2)^{-1/2} \leqslant t^{-1}$, it follows by lemma 2.9 that

$$\int_0^1 \frac{|\zeta^2(1/2+it)||\Gamma(1/2+it)|}{\sqrt{1/4+t^2}}dt \ll \int_0^1 e^{-1/2\pi t}dt \ll 1,$$

and

$$\int_1^T \frac{|\zeta^2(1/2+it)||\Gamma(1/2+it)|}{\sqrt{1/4+t^2}}dt \ll \int_1^T e^{-1/2\pi t}dt,$$

which implies

$$\begin{aligned}
&\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT} \zeta^2(s+1)\frac{\Gamma(s+1)}{s}U^s ds\right| \\
&= \frac{1}{2\pi}\left|\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT} \zeta^2(s+1)\frac{\Gamma(s+1)}{s}U^s ds\right| \\
&\leqslant \frac{1}{2\pi}\int_{-T}^{T} |\zeta^2(1/2+it)|\frac{|\Gamma(1/2+it)|}{\sqrt{1/4+t^2}}U^{-1/2}dt
\end{aligned}$$

$$\begin{aligned}
&\ll U^{-\frac{1}{2}}\int_1^T \frac{|\zeta^2(1/2+it)||\Gamma(1/2+it)|}{\sqrt{1/4+t^2}}dt + U^{-\frac{1}{2}}\int_0^1 \frac{|\zeta^2(1/2+it)||\Gamma(1/2+it)|}{\sqrt{1/4+t^2}}dt \\
&\ll U^{-\frac{1}{2}}\int_1^T e^{-\frac{1}{2}\pi t}dt + U^{-\frac{1}{2}} \\
&\ll U^{-\frac{1}{2}}Te^{-\frac{1}{2}\pi T} + U^{-\frac{1}{2}},
\end{aligned}$$

which goes to $U^{-\frac{1}{2}}$ as $T \to \infty$.

Q.E.D.

We recall lemma 2.13 in our work on **ET03**. Note that it is because of this lemma 2.13 that we break the n sum at $U \log U^2$ and not U, as done in [DP99].

Lemma 2.13 *For any* $0 < \delta \leqslant 1, U > 1$,

$$\sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \ll_\delta \frac{1}{U}.$$

Proof Since $0 < \delta \leqslant 1$ implies $1 \leqslant t^\delta \leqslant t$, by lemma 2.6, part 2,

$$\begin{aligned}
\sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} &\ll_\delta \sum_{n > U \log U^2} \frac{n^\delta}{n} e^{-\frac{n}{U}} \\
&\ll_\delta \lim_{T\to\infty} \int_{U \log U^2}^T \frac{t^\delta}{t} e^{-\frac{t}{U}} dt \\
&\ll_\delta \lim_{T\to\infty} \int_{U \log U^2}^T e^{-\frac{t}{U}} dt \\
&= \frac{1}{U}.
\end{aligned}$$

Q.E.D.

2.5 An Upper Bound for $L(1, \chi_d)$ and $L(s, \chi_{d_1})L(s, \chi_{d_2})$

The purpose of this section is to deduce an upper bound for $L(s, \chi_{d_1})L(s, \chi_{d_2})$ which we need in our proof of lemma 4.1. For $s = \sigma + it \in \mathbb{C}$,

$$L(s) \overset{\text{def}}{=} L(s, \chi_{d_1})L(s, \chi_{d_2}) = \sum_{n=1}^{\infty} a_{d_1,d_2}(n)\frac{1}{n^s},$$

where

$$a_{d_1,d_2}(n) \overset{\text{def}}{=} \sum_{n=\delta e} \left(\frac{d_1}{\delta}\right)\left(\frac{d_2}{e}\right).$$

We do this in lemma 2.18. First we recall the Pólya–Vinogradov inequality. We will use lemma 2.14 in our proof of lemma 2.15 and lemma 2.18.

Lemma 2.14 (The Pólya-Vinogradov inequality) *Let $S(\chi, x) = \sum_{y<n\leqslant x} \chi(n)$, where χ is a non-trivial character modulo q. Then $S(\chi, x) \ll \sqrt{q}\log q$, uniformly in χ and x.*

Proof See [Pól18] or [Vin19] for historical interest, and [MM97], pg. 91 for a proof of the case where χ is *primitive.*[6]

We include lemma 2.15 for completion as it is precisely the result used by David and Pappalardi in [DP99]. First recall that for a complex number s and a Dirichlet character χ_d,

$$L(s, \chi_d) = \sum_{n\geqslant 1} \left(\frac{d}{n}\right)\frac{1}{n^s}.$$

Lemma 2.15 *Let $\chi_d = \left(\frac{d}{n}\right)$ be a non-trivial Dirichlet character. For any $U > 0$,*

$$L(1, \chi_d) = \sum_{n\leqslant U} \left(\frac{d}{n}\right)\frac{1}{n} + O\left(\frac{\sqrt{|d|}\log|d|}{U}\right).$$

[6] An important notion is the *propriety* of characters. Let q be a multiple of d, and let $\chi(n)$ be a Dirichlet character (mod d). The group of reduced residue classes (mod q) maps homomorphically onto the corresponding group (mod d), and we define a character $\chi^{\checkmark}$ (mod q) by the equation

$$\chi^{\checkmark} \overset{\text{def}}{=} \chi^{\checkmark}(n) \overset{\text{def}}{=} \begin{cases} \chi(n) & \text{if } (n,q) = 1; \\ 0 & \text{if } (n,q) > 1. \end{cases}$$

We note that χ and $\chi^{\checkmark}$ are different arithmetic functions. For example, if $d = 3$ and $q = 6$, and χ takes the values $1, -1, 0, 1, -1, 0$ for $n = 1, 2, 3, 4, 5, 6$, then $\chi^{\checkmark}$ takes the values $1, 0, 0, 0, -1, 0$, since $\chi^{\checkmark}$ is zero when n is a multiple of 2, as well as when n is a multiple of 3. When $\chi^{\checkmark}$ is constructed as above, we say that χ (mod d) *induces* $\chi^{\checkmark}$ (mod q), and if $q \neq d$, that $\chi^{\checkmark}$ (mod q) is *imprimitive*. A *primitive* character is one that is not induced by a character (mod d) for any divisor d of q other than q itself. The smallest f for which a character χ (mod f) induces $\chi^{\checkmark}$ (mod q) is called the *conductor* of χ.

Proof By Lemma 2.14, $A(x) = \sum_{U<n\leqslant x} \left(\frac{d}{n}\right) \ll \sqrt{|d|}\log|d|$, so by Lemma 2.1 we have

$$\begin{aligned}
\sum_{n>U} \left(\frac{d}{n}\right)\frac{1}{n} &= \int_U^\infty \frac{A(t)}{t^2}dt \\
&= \int_U^\infty \frac{O(\sqrt{|d|}\log|d|)}{t^2}dt \\
&= O\left(\sqrt{|d|}\log|d| \lim_{T\to\infty} t^{-1}|_U^T\right) \\
&= O\left(\frac{\sqrt{|d|}\log|d|}{U}\right).
\end{aligned}$$

Q.E.D.

Furthermore, we include lemma 2.16 as it is precisely the bound used by David and Pappalardi in [DP99].

Lemma 2.16 $L(1,\chi_d) = O(\log|d|)$.

Proof Choose $U = \sqrt{|d|}$ in lemma 2.15,

$$\left|\sum_{n\leqslant\sqrt{|d|}} \left(\frac{d}{n}\right)\frac{1}{n}\right| \leqslant \sum_{n\leqslant\sqrt{|d|}} \frac{1}{n} \ll \int_1^{|d|} \frac{1}{t}dt = \log|d|.$$

Q.E.D.

In order to prove lemma 2.18, we need to further recall Dirichlet's hyperbola method. Let $f(n) = \sum_{\delta|n} g(\delta)h\left(\frac{n}{\delta}\right)$. We define $G(x) \overset{\text{def}}{=} \sum_{n\leqslant x} g(n)$, and $H(x) \overset{\text{def}}{=} \sum_{n\leqslant x} h(n)$.

Lemma 2.17 *For any* $y > 0$,

$$\sum_{n\leqslant x} f(n) = \sum_{\delta\leqslant y} g(\delta)H\left(\frac{x}{\delta}\right) + \sum_{\delta<\frac{x}{y}} h(\delta)G\left(\frac{x}{\delta}\right) - G(y)H\left(\frac{x}{y}\right).$$

Proof

$$\sum_{n\leqslant x} f(n)$$

$$
\begin{aligned}
&= \sum_{\delta e \leqslant x} g(\delta)h(e) \\
&= \sum_{\substack{\delta e \leqslant x \\ \delta \leqslant y}} g(\delta)h(e) + \sum_{\substack{\delta e \leqslant x \\ \delta > y}} g(\delta)h(e) \\
&= \sum_{\delta \leqslant y} g(\delta) \sum_{e \leqslant \frac{x}{\delta}} h(e) + \sum_{ye < \delta e \leqslant x} g(\delta)h(e) \\
&= \sum_{\delta \leqslant y} g(\delta) H\left(\frac{x}{\delta}\right) + \sum_{\substack{\delta e \leqslant x \\ ye < x}} g(\delta)h(e) - \sum_{\substack{ye < x \\ \delta \leqslant y}} g(\delta)h(e) \\
&= \sum_{\delta \leqslant y} g(\delta) H\left(\frac{x}{\delta}\right) + \sum_{e < \frac{x}{y}} h(e) G\left(\frac{x}{e}\right) - H\left(\frac{x}{y}\right) G(y).
\end{aligned}
$$

Q.E.D.

We now apply the Pólya–Vinogradov inequality and Dirichlet's hyperbola method in order to deduce an upper bound on $L(s)$.

Lemma 2.18 *For any $\sigma > 0$, and $T > 1$,*

$$L(\sigma + iT) \ll \sqrt{|d_1 d_2|} \log |d_1| \log |d_2| \frac{\sqrt{\sigma^2 + T^2}}{\sigma}.$$

Proof If $\sigma > 0$, and $A(t) = \sum_{m \leqslant t} a_{d_1,d_2}(m)$, then by lemma 2.1,

$$L(s) = s \int_1^\infty \frac{A(t)}{t^{s+1}} dt.$$

But by lemma 2.14 together with lemma 2.17,

$$A(t) \ll \sqrt{|d_1 d_2|} \log |d_1| \log |d_2|.$$

Thus for $\sigma > 0$,

$$
\begin{aligned}
L(s) &\ll \sqrt{|d_1 d_2|} \log |d_1| \log |d_2| |s| \int_1^\infty t^{-(\sigma+1)} dt \\
&= \sqrt{|d_1 d_2|} \log |d_1| \log |d_2| \frac{\sqrt{\sigma^2 + t^2}}{\sigma}.
\end{aligned}
$$

Q.E.D.

Chapter 3

Lang–Trotter Conjecture

This chapter explains all of the mathematical background needed to state and justify the Lang–Trotter conjectures and to explain the link between the Lang–Trotter conjectures and L–series, which is the theme of the thesis. It also reviews the existing results contained in the literature, explaining their relevance to the present work. Moreover, it presents Theorem 1 proven in the next chapter, and it's relation with the average Lang–Trotter conjecture for 2 elliptic curves.

3.1 Motivation

Any natural number greater than 1 which has exactly 2 divisors is called a prime number. Let

$$\pi(x) \overset{\text{def}}{=} \#\{ p \leqslant x \ : p \text{ is a prime } \}.$$

In book 9 of Elements, Euclid (355-265) proves the existence of infinitely many primes. That is, as $x \to \infty$,

$$\pi(x) \to \infty.$$

In 1896, Hadamard (1865-1963) and de la Vallée Poussin (1866-1962) proved (independently) the prime number theorem. That is,

$$\pi(x) \sim \frac{x}{\log x},$$

which means

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

Similarly, for fixed $a, k \in \mathbb{N}, (a,k) = 1$, we define

$$\pi(x;k,a) \overset{\text{def}}{=} \#\{\, p \leqslant x \ : \ p \equiv a \pmod{k} \,\}.$$

Dirichlet (1805-1859) was the first to show as $x \to \infty$,

$$\pi(x;k,a) \to \infty.$$

That is, there exist infinitely many primes in the arithmetic progression

$$a, a+k, a+2k, \ldots$$

whenever $(a,k) = 1$. The prime number theorem for arithmetic progressions[1] is the fact that for fixed a, $k \in \mathbb{N}, (a,k) = 1$,

$$\pi(x;k,a) \sim \frac{\pi(x)}{\phi(k)}.$$

Analogously, we can ask similar questions regarding the distribution of primes in other sequences. In 1923, Hardy and Littlewood [HL23] conjectured the following statement about the distribution of primes in a quadratic progression. For fixed

[1] For an elementary proof see [Sel50].

$a \neq 0, b, c, \in \mathbb{Z}^+$, and some $n \in \mathbb{N}$, we let

$$q(n) = an^2 + bn + c$$

be a quadratic progression, and we define

$$Q(x) \overset{\text{def}}{=} \#\{ p \leqslant x \, : \, p = q(n) \text{ for some } n \}.$$

Conjecture (Hardy–Littlewood, 1923) For some constant $C > 0$,

$$Q(x) \sim C \frac{\sqrt{x}}{\log x}.$$

This conjecture is related to a more general conjecture of Lang and Trotter [LT76]. Both conjectures are unproven to this day, and so motivate our study. In the next section we recall the facts from the theory of elliptic curves that are needed for understanding the Lang–Trotter conjecture.

3.2 Elliptic Curves

An *elliptic curve* E defined over a field K is a curve that is given by an equation of the *generalized Weierstrass form*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \; a_i \in K, i = 1, \ldots, 6.$$

We let $E(K)$ denote the set of points $(x, y) \in K \times K$ that satisfy this equation along with a point at infinity denoted P_∞. If F is any extension of K, then $E(F)$ denotes the set of $(x, y) \in F \times F$ that satisfy the above equation, along with P_∞. In order for E to be an *elliptic curve* it must be smooth. This means that there is no point of $E(\bar{K})$ ($\bar{K}$ denotes the algebraic closure of K) where both partial derivatives vanish.

If the characteristic of K is neither 2 nor 3, without loss of generality we may suppose that our elliptic curve is given by an equation of the form

$$E : y^2 = x^3 + ax + b, \ \ a, b \in K.$$

In this case the condition that the curve be smooth is equivalent to requiring that the cubic on the right have no multiple roots. This holds if and only if the *discriminant* of $x^3 + ax + b$ is non-zero. The discriminant of this cubic is $-4a^3 - 27b^2$.

Definition The discriminant of the elliptic curve E is defined as follows:

$$\Delta_E \overset{\text{def}}{=} -16(4a^3 + 27b^2).$$

Definition The *j-invariant* of the elliptic curve E is defined as follows:

$$j(E) \overset{\text{def}}{=} -1728\frac{4a^3}{\Delta_E}.$$

From now on, we assume that $K = \mathbb{Q}$, which has characteristic 0, so that E has coefficients $a, b \in \mathbb{Q}$. We first note that there is a cubic equation for E with coefficients $a, b \in \mathbb{Z}$.

The point is that we want to consider curves originally defined over $\mathbb{Z}$ as if defined over finite fields $\mathbb{F}_p$. That is, we will consider reductions of the curve modulo p. Now for every $p \nmid \Delta_E$, we can associate a new elliptic curve E_p with coefficients in $\mathbb{F}_p$. Namely,

$$E_p : y^2 = x^3 + \bar{a}x + \bar{b}.$$

Here $\bar{a}$ and $\bar{b}$ are modulo p reductions of a and b. Let

$$\#E_p(\mathbb{F}_p) = \#(\{\,(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \ : \ y^2 = x^3 + \bar{a}x + \bar{b}, \ \ \bar{a}, \bar{b} \in \mathbb{F}_p\} \cup \{P_\infty\}).$$

It is not hard to see that

$$\#E_p(\mathbb{F}_p) \leqslant 2p+1,$$

as $x \in \mathbb{F}_p$ can be any of the p elements $0, 1, ..., p-1$, so there are at most $2p$ solutions to $y^2 = x^3 + \bar{a}x + \bar{b}$. Not forgetting to count the point P_∞ at infinity which is already in $E_p(\mathbb{F}_p)$, we deduce the result. The following heuristic suggests the right order of magnitude to be p, and not $2p+1$. It is known that among the non-zero elements $1, 2, \ldots, p-1$ of the field $\mathbb{F}_p$, half of them are squares[2]. Hence, a "randomly chosen" quadratic equation has a 50 percent chance of being solvable in $\mathbb{F}_p$. It follows that $\#E_p(\mathbb{F}_p) \approx p$.

The following theorem (conjectured by E. Artin in his thesis) and proved by Hasse, shows that this heuristic is correct.

Theorem (Hasse, 1938) *Let E_p be the modulo p reduction of E, and $\#E_p(\mathbb{F}_p)$ the number of $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ which satisfy E_p along with the point at infinity P_∞. Then*

$$\#E_p(\mathbb{F}_p) = p + 1 - a_p(E),$$

where $a_p(E)$ is an integer, $|a_p(E)| \leqslant 2\sqrt{p}$.

In order to study more properties of $a_p(E)$, we need to study the ring $\mathrm{End}(E)$.

The points on an elliptic curve form a group. The group law can be characterized in a number of equivalent ways. Recall that we have assumed E to be an elliptic curve

[2] Note (see [Sie64], pg. 17) that for p prime, $n \in \mathbb{N}, g = (n, p-1)$, the number of different n^{th} power residues modulo p (excluding 0) is $(p-1)/g$. Consequently, if $p \equiv 1 \bmod n$, then $(n, p-1) = n$, and the number of different n^{th} power residues modulo p (excluding 0) is $(p-1)/n$. Equivalently, if $p \equiv 1 \bmod n$, $\frac{1}{n}$th of the elements in $\mathbb{F}_p^*$ are n^{th} powers. In particular, if $p \equiv 1 \bmod 2$, one half of the $t \in \mathbb{F}_p^*$ are squares.

over $\mathbb{Q}$ so that it has the special form with coefficients $a, b \in \mathbb{Q}$. Geometrically, three points sum to zero if and only if they are collinear. Using this geometric characterization, we can write down explicit formulas. For example, if $P = (x, y)$ and $Q = (x', y')$ are on E, then

$$\begin{aligned} P + Q &= \left(\frac{y' - y}{x' - x}\right)^2 - x - x', \\ 2P &= \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}. \end{aligned}$$

Similarly, the additive inverse of $P = (x, y)$ is $-P = (x, -y)$; the reflection of P in the x–axis. Notice repeated addition gives multiplication maps $[n] : E \to E, n \in \mathbb{Z}$,

$$[n]P = \begin{cases} P + P + P + \cdots + P & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ -(P + P + P + \cdots + P) & \text{if } n < 0. \end{cases}$$

Definition An *isogeny* is a homomorphism $\phi : E(\mathbb{Q}) \to E(\mathbb{Q})$ which is defined by rational functions. That is, an isogeny is a homomorphism $\phi : E(\mathbb{Q}) \to E(\mathbb{Q})$ that has the form

$$\phi(x, y) = \left(\frac{\text{polynomial in } x \text{ and } y}{\text{polynomial in } x \text{ and } y}, \frac{\text{polynomial in } x \text{ and } y}{\text{polynomial in } x \text{ and } y}\right).$$

We define isogenies in this way because we are interested in isogenies from an elliptic curve to itself; such isogenies are called *endomorphisms.* Notice that every elliptic curve has the multiplication–by–n endomorphisms, one for each integer n. For most elliptic curves, there will be no other endomorphisms. The *degree* of an isogeny ϕ is its degree as a finite map of curves. It is denoted by $\deg(\phi)$. Associated to an isogeny ϕ of degree n is a *dual isogeny* $\hat{\phi} : E \to E$, characterized by the property that $\hat{\phi} \circ \phi = [n]_E$, and $\phi \circ \hat{\phi} = [n]_E$. The dual isogeny has the following additional properties; $\hat{\hat{\phi}} = \phi$, $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$, $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$, $[\hat{n}] = [n]$.

Definition The *endomorphism ring* of E, denoted $\mathrm{End}(E)$, is defined as follows:

$$\mathrm{End}(E) \overset{\text{def}}{=} \{\, \text{isogenies}\, \phi \,:\, E \to E \,\},$$

together with the zero map. We make $\mathrm{End}(E)$ into a ring via the rules $(\phi+\psi)(P) = \phi(P) + \psi(P)$ and $(\phi\psi)(P) = \phi(\psi(P))$. The unit group of $\mathrm{End}(E)$ consists of the isomorphisms from E to itself. It is called the *automorphism group* of E. With regards to the next theorem, note that we define what we mean by an *order in a quadratic field* in a later section.

Definition A *quaternion algebra* is an algebra of the form

$$\mathcal{H} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta,$$

with the multiplication rules α^2, $\beta^2 \in \mathbb{Q}$, $\alpha^2 < 0$, $\beta^2 < 0$, $\beta\alpha = -\alpha\beta$.

Theorem *Let E be an elliptic curve defined over a field K. The endomorphism ring of E is one of the following 3 sorts of rings:*

$$\mathrm{End}(E) = \begin{cases} \mathbb{Z}, \\ \textit{an order in a quadratic field (ordinary)}, \\ \textit{a maximal order in a quaternion algebra (supersingular)}. \end{cases}$$

The third possibility can occur if and only if the characteristic of K is strictly larger than 0.

Proof See [Sil99], Corollary 9.4, pg. 102.

Definition An elliptic curve E has complex multiplication (CM in short) provided $\mathbb{Z} \neq \mathrm{End}(E)$.

Definition For an element $\phi \in \mathrm{End}(E)$, the *trace* is $T(\phi) = \phi + \hat{\phi}$, and the *characteristic polynomial* is

$$c_\phi(t) = t^2 - T(\phi)t + \deg(\phi).$$

The point of discussing all of these notions is that we want to define the integer $a_p(E)$ from Hasse's theorem in a precise way, and show by an example that the study of the distribution of $a_p(E)$'s is closely related to the problem of the distribution of primes in certain sequences. Before discussing the example, we observe for $\bar{a} \in \mathbb{F}_p$,

$$\bar{a}^p \equiv \bar{a} \bmod p$$

by *Fermat's little theorem.* It follows by taking p^{th} powers on both sides of the equation for E_p, the modulo p reduction of E, that $y^{2p} = x^{3p} + \bar{a}^p x^p + \bar{b}^p$ if and only if $(y^p)^2 = (x^p)^3 + \bar{a}x^p + \bar{b}$. That is, the *Frobenius map*

$$\phi_p : E_p \to E_p, (x, y) \mapsto (x^p, y^p),$$

is an endomorphism of E_p. Hasse's theorem says that the *trace of Frobenius*,

$$T(\phi_p) = \phi_p + \hat{\phi}_p \overset{\text{def}}{=} a_p(E),$$

is an integer in the endomorphism ring of E_p of magnitude at most $2\sqrt{p}$. Since the degree of ϕ_p is p, note that the characteristic polynomial of ϕ_p is given by

$$c_{\phi_p}(t) \overset{\text{def}}{=} t^2 - a_p(E)t + p.$$

Example Let E over $\mathbb{Q}$ be the curve $y^2 = x^3 - x$, and let E_p be the reduction of E modulo p. E has CM by $\mathbb{Z}[i]$. For some $n \in \mathbb{N}$, we show

$$a_p(E) = \pm 2 \Rightarrow p = 1 + n^2.$$

In fact, $a_p(E) = \pm 2 \Leftrightarrow p = 1 + n^2$.

Proof Let $\phi : (x, y) \mapsto (-x, iy)$. Note that $\phi \circ \phi : (x, y) \mapsto (x, -y)$. That is, $\phi \circ \phi = [-1]$; ϕ is a root of $x^2 + 1 = 0$. It follows that $\mathrm{End}(E) = \mathbb{Z}[i]$. Let $\mathrm{End}(E_p)$ be the endomorphism ring of the reduced curve. Since $\mathrm{End}(E) \subseteq \mathrm{End}(E_p)$, therefore $\mathbb{Z}[i] \subseteq \mathrm{End}(E_p)$. It follows from a previous theorem that $\mathrm{End}(E_p)$ is either an order in a quadratic field (ordinary), or a maximal order in a quaternion algebra (supersingular). But[3] E_p is supersingular if and only if $a_p(E) = 0$. Since $a_p(E) = \pm 2$, then $\mathrm{End}(E_p) = \mathbb{Z}[i]$. But we know one element of the ring $\mathrm{End}(E_p)$, namely the Frobenius endomorphism ϕ_p. It is a root of $t^2 - a_p(E)t + p$. That is,

$$\phi_p = \frac{a_p(E) \pm \sqrt{(a_p(E))^2 - 4p}}{2} \in \mathbb{Z}[i].$$

As $a_p(E) = \pm 2$, this gives $\phi_p = \pm 1 \pm \sqrt{1-p} \in \mathbb{Z}[i]$, which for some $n \in \mathbb{N}$ is equivalent to $1 - p = -n^2$, which is equivalent to $p = 1 + n^2$. We have shown that $a_p(E) = \pm 2 \Rightarrow p = 1 + n^2$, for some $n \in \mathbb{N}$, from which we deduce the result.

Q.E.D.

For $r \in \mathbb{Z}$, let $\pi_E^r(x) = \#\{\, p \leqslant x \, : \, a_p(E) = r \,\}$. In light of the example,

$$\pi_E^{\pm 2}(x) = \#\{\, p \leqslant x \, : \, a_p(E) = \pm 2 \,\},$$

and

$$\#\{\, p \leqslant x \, : \, p = 1 + n^2 \text{ for some } n \,\},$$

are equal. Notice for some constant $C > 0$, Hardy-Littlewood's conjecture gives

$$\pi_E^{\pm 2}(x) \sim C \frac{\sqrt{x}}{\log x}.$$

[3] See [Sil99], chapter 3, Corollary 5.5 together with chapter 5, Theorem 3.1 a(ii).

In fact, the Lang and Trotter conjecture predicts that for some constant C_E,

$$\pi_E^{\pm 2}(x) \sim C_E \frac{\sqrt{x}}{\log x}.$$

In the case that E has CM as in the above example, we can relate the conjecture made by Lang and Trotter to the distribution of primes in quadratic progressions and is consistent with the conjecture made by Hardy and Littlewood. But if E has no CM, then the conjecture by Lang and Trotter is new and nothing was known about it untill recently. In the next section we state the Lang-Trotter conjecture, describe a heuristic indicating the plausibility of the conjecture, and discuss the recent progress made towards proving it.

3.3 The Lang–Trotter Conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$, and for a fixed integer r, let

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

The conjecture of Lang and Trotter predicts the asymptotic behaviour of $\pi_E^r(x)$.

Conjecture (Lang–Trotter, [LT76]) *Except for the case where $r = 0$ and E has CM, there is a constant $C_{E,r}$ such that*

$$\pi_E^r(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x}.$$

Notice that the constant $C_{E,r}$ can be zero, and then the asymptotic relation is interpreted to mean that there is only a finite number of primes such that $a_p(E) = r$.

The exceptional case, *supersingular primes*[4] *of a CM curve* was treated by Deuring in the following theorem, and was based on a criterion of Deuring [Deu41], which states that if E over $\mathbb{Q}$ has CM, then a prime p is supersingular for E if and only if it is ramified or inert in the field of complex multiplication, with finitely many exceptions.

Theorem (Deuring, [Deu41]) *If E over $\mathbb{Q}$ has CM, then*

$$\pi_E^0(x) \sim \frac{1}{2}\pi(x) \sim \frac{x}{2\log x}.$$

That is, the set of supersingular primes has density 1/2 in the set of primes.

Let E be an elliptic curve over $\mathbb{Q}$ without CM. A naive heuristic suggests that as $a_p(E) = r$ if and only if it has $p+1-r$ points over $\mathbb{F}_p$, and $\#E_p(\mathbb{F}_p)$ can take only one of $4\sqrt{p}$ values by Hasse's inequality, each p is supersingular with "probability" proportional to $1/\sqrt{p}$. That is,

$$\text{Prob}\{\, a_p(E) = 0 \,\} \approx \frac{1}{\sqrt{p}}.$$

Generally, fix $r \in \mathbb{Z}$. It follows by the same heuristic that

$$\text{Prob}\{\, a_p(E) = r \,\} \approx \frac{1}{\sqrt{p}}.$$

Let

$$\pi_E^r(x) = \sum_{p \leqslant x} \lambda_p,$$

where

$$\lambda_p = \begin{cases} 1 & \text{if } a_p(E) = r, \\ 0 & \text{otherwise.} \end{cases}$$

[4] Recall that a prime p is called *supersingular* (or of supersingular reduction) if and only if $p \nmid \Delta_E$ and $a_p(E) = 0$.

Then $\lambda_p = 1$ with probability proportional to $1/\sqrt{p}$. It follows that

$$\pi_E^r(x) \approx \sum_{p \leqslant x} \frac{1}{\sqrt{p}}.$$

By partial summation lemma 2.1, we write

$$\begin{aligned}
\sum_{p \leqslant x} \frac{1}{\sqrt{p}} &= \pi(x)\frac{1}{\sqrt{x}} + \frac{1}{2}\int_1^x \frac{\pi(t)}{t^{3/2}}dt \\
&= \pi(x)\frac{1}{\sqrt{x}} + \frac{1}{2}\int_1^x \left\{\frac{1}{\sqrt{t}\log t} + o\left(\frac{1}{\sqrt{t}\log t}\right)\right\} dt \\
&= \frac{\pi(x)}{\sqrt{x}} + \frac{1}{2}\left[\frac{2\sqrt{x}}{\log x} + o\left(\frac{\sqrt{x}}{\log x}\right)\right] \\
&= \frac{2\pi(x)}{x} + o\left(\frac{\sqrt{x}}{\log x}\right).
\end{aligned}$$

By the prime number theorem, we see that

$$\pi_E^r(x) \approx \sum_{p \leqslant x} \frac{1}{\sqrt{p}} \sim \frac{2\sqrt{x}}{\log x},$$

which is consistent with the Lang–Trotter conjecture.

The Lang–Trotter conjecture is based on a sophisticated probabalistic model which generalizes the naive heuristic presented above. Their model also predicts the value of the constant $C_{E,r}$.

The conjecture we are considering in this thesis is not the Lang–Trotter conjecture, but rather the following conjecture which we call *the Lang–Trotter conjecture for 2 elliptic curves.*

Let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$. Fix r_1 and r_2 in $\mathbb{Z}$, and let

$$\pi_{E_1,E_2}^{r_1,,r_2}(x) = \sum_{p \leqslant x} \lambda_p,$$

where

$$\lambda_p = \begin{cases} 1 & \text{if } a_p(E_1) = r_1 \text{ and } a_p(E_2) = r_2, \\ 0 & \text{otherwise.} \end{cases}$$

Conjecture (Lang–Trotter for 2 elliptic curves) *There exists a constant* $C_{E_1,E_2,r_1,r_2} \geqslant 0$ *such that*

$$\pi^{r_1,r_2}_{E_1,E_2}(x) \sim C_{E_1,E_2,r_1,r_2} \log\log x.$$

This conjecture seems extremely hard to prove. Also, the set in question is very sparse so that gathering numerical evidence is futile.

We can motivate this conjecture with the naive heuristic used above. We have

$$\text{Prob}\{\, a_p(E_1) = r_1 \,\} \approx \frac{1}{\sqrt{p}},$$

and

$$\text{Prob}\{\, a_p(E_2) = r_2 \,\} \approx \frac{1}{\sqrt{p}}.$$

Then $\lambda_p = 1$ with probability proportional to

$$\frac{1}{\sqrt{p}} \times \frac{1}{\sqrt{p}} = \frac{1}{p}.$$

Such a probalistic assumption of independence appears in [LT76], page 37. Consequently,

$$\pi^{r_1,r_2}_{E_1,E_2}(x) = \sum_{p\leqslant x} \lambda_p \approx \sum_{p\leqslant x} \frac{1}{p}.$$

Since

$$\sum_{p\leqslant x} \frac{1}{p} = \log\log x + O(1),$$

a classical result by Čhebyšev[5], for some constant $C > 0$, our heuristic leads to

$$\pi^{r_1,r_2}_{E_1,E_2}(x) \approx \sum_{p\leqslant x} \frac{1}{p} \sim C \log\log x.$$

[5] See [Čhe51] for historical interest, or recall Mertens' theorem, $\sum_{p\leqslant x} \frac{\log p}{p} = \log x + O(1)$, and apply partial summation lemma 2.1 to $\sum_{p\leqslant x} \frac{1}{p} = \sum_{p\leqslant x} \frac{\log p}{p} \frac{1}{\log p}$.

We further remark that if we were to consider for fixed $r_1, r_2, r_3 \in \mathbb{Z}$, the set

$$\pi^{r_1,r_2,r_2}_{E_1,E_2,E_3}(x) = \sum_{p \leqslant x} \lambda_p,$$

where now $\lambda_p = 1$ if $a_p(E_i) = r_i$ for $i = 1, 2$, and 3, then by the same heuristic we obtain

$$\pi^{r_1,r_2,r_2}_{E_1,E_2,E_3}(x) \approx \sum_{p \leqslant x} \frac{1}{p^{3/2}}.$$

Since

$$\sum_{p \leqslant x} \frac{1}{p^{3/2}} \leqslant \sum_{\substack{n \in \mathbb{N} \\ n \leqslant x}} \frac{1}{n^{3/2}} \ll \int_1^x t^{-3/2} dt \ll 2,$$

it follows that

$$\pi^{r_1,r_2,r_2}_{E_1,E_2,E_3}(x) = O(1).$$

That is, the set $\pi^{r_1,r_2,r_2}_{E_1,E_2,E_3}(x)$ is finite.

We now give a survey of what results are known regarding the *Lang–Trotter conjecture* and the *Lang–Trotter conjecture for 2 elliptic curves.*

Let E be an elliptic curve over $\mathbb{Q}$ without CM. It is not immediately obvious that either

$$\pi^0_E(x) = o(\pi(x)).$$

That is, that the supersingular primes have density zero, or that

$$\pi^0_E(x) \neq O(1).$$

That is, that there are infinitely many such primes.

Serre [Ser68] proved $\pi^0_E(x) = o(\pi(x))$ by applying the Čebotarev Density Theorem to the number fields generated by the coordinates of the torsion points of E. Later in [Ser81], he combined this idea with sieve techniques in order to show

$$\pi_E^r(x) \ll_r \begin{cases} \frac{x}{(\log x)^{3/2-\epsilon}} & \text{if } r = 0, \\ \frac{x}{(\log x)^{5/4-\epsilon}} & \text{for any } r \in \mathbb{Z} \text{ (including 0)}. \end{cases}$$

Furthermore, assuming the *Generalized Riemann Hypothesis* (GRH)[6] for these number fields, he showed that

$$\pi_E^r(x) \ll_r \begin{cases} x^{3/4} & \text{if } r = 0, \\ x^{7/8}(\log x)^{-1/2} & \text{for any } r \in \mathbb{Z} \text{ (including 0)}. \end{cases}$$

Elkies [Elk87] made a big breakthrough and showed $\pi_E^0(x) \neq O(1)$, and that there are infinitely many supersingular primes. This result was improved by Fouvry and Murty ([FM96], Théorème 1). Note that Elkies and Murty [Elk91] obtained unconditionally the upper bound $x^{3/4}$ for $\pi_E^0(x)$ obtained by Serre under GRH.

Murty and Fouvry also showed in [FM96] that the Lang-Trotter conjecture, is true on *average* in the supersingular case. More precisely,

Theorem B ([FM96], Théorème 6) *Given $\epsilon > 0$, if $A(x) \geqslant x^{1/2+\epsilon}$ and $B(x) \geqslant x^{1/2+\epsilon}$, then*

$$\sum_{|a|\leqslant A(x)} \sum_{|b|\leqslant B(x)} \pi_E^0(x) \sim \frac{\pi}{3} \frac{\sqrt{x}}{\log x}(4A(x)B(x)).$$

In 1997, David and Pappalardi generalized the work of Murty and Fouvry showing that the Lang-Trotter conjecture is true on average for any $r \in \mathbb{Z}$.

[6] Let K be an algebraic number field, $\mathcal{O}_K$ its ring of integers, a an ideal of $\mathcal{O}_K$, and $\zeta_K(s) = \sum \frac{1}{(\mathrm{N}a)^s}$, where the sum is over all ideals a of $\mathcal{O}_K$, and $\mathrm{N}a$ is the norm of a; defined to be the index of a in $\mathcal{O}_K$.

Conjecture (Generalized Riemann Hypothesis–GRH) *All non-trivial zeros of $\zeta_K(s)$ lie on the line $\sigma = \frac{1}{2}$.*

Theorem ([DP99], Corollary 1.3) *For any $r \in \mathbb{Z}$, given $\epsilon > 0$, if $A(x) > x^{1+\epsilon}, B(x) > x^{1+\epsilon}$, then*

$$\sum_{|a| \leqslant A(x)} \sum_{|b| \leqslant B(x)} \pi_E^r(x) \sim \frac{2}{\pi} \prod_{p|r} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p \nmid r} \frac{p(p^2-p-1)}{(p-1)(p^2-1)} \frac{\sqrt{x}}{\log x}(4A(x)B(x)).$$

We observe that for $r = 0$,

$$\prod_{p \nmid 0} \frac{p(p^2-p-1)}{(p-1)(p^2-1)} \overset{\text{con}}{=} 1.$$

On the other hand,

$$\prod_{p|0} \left(1 - \frac{1}{p^2}\right)^{-1} = \prod_{p} \left(1 - \frac{1}{p^2}\right)^{-1} = \zeta(2) = \frac{\pi^2}{6},$$

so that David's and Pappalardi's constant reduces to

$$\frac{2}{\pi}\frac{\pi^2}{6} = \frac{\pi}{3},$$

the constant obtained by Fouvry and Murty.

In a subsequent paper, Fouvry and Murty also proved the Lang–Trotter conjecture for 2 supersingular elliptic curves E_1 and E_2 over $\mathbb{Q}$. Recall for fixed $r_1, r_2 \in \mathbb{Z}$,

$$\pi_{E_1,E_2}^{r_1,r_2}(x) \overset{\text{def}}{=} \#(\{p \leqslant x \,:\, a_p(E_1) = r_1\} \cap \{p \leqslant x \,:\, a_p(E_2) = r_2\}),$$

and in particular for $r_1 = r_2 = 0$,

$$\pi_{E_1,E_2}^{0,0}(x) \overset{\text{def}}{=} \#(\{p \leqslant x \,:\, a_p(E_1) = 0\} \cap \{p \leqslant x \,:\, a_p(E_2) = 0\}).$$

Theorem ([FM95], Theorem 1) *For every positive ϵ, we have for $x \to \infty$, the asymptotic relation*

$$\sum_{|a_1| \leqslant A_1(x)} \sum_{|a_2| \leqslant A_2(x)} \sum_{|b_1| \leqslant B_1(x)} \sum_{|b_2| \leqslant B_2(x)} \pi_{E_1,E_2}^{0,0}(x) \sim \frac{35}{96} \log\log x(16A_1(x)A_2(x)B_1(x)B_2(x)),$$

holds uniformly for $A_i(x) \geqslant x^{1/2+\epsilon}, B_i(x) \geqslant x^{1/2+\epsilon}, A_i(x)B_i(x) \geqslant x^{3/2+\epsilon}, i = 1, 2.$

In the spirit of [DP99], we attempt to prove a similar result for all $r_1, r_2 \in \mathbb{Z}$. That is, we would like to prove the following average Lang–Trotter conjecture for 2 elliptic curves.

Conjecture (Average Lang–Trotter for 2 elliptic curves) *For fixed* $r_1, r_2 \in \mathbb{Z}$,

$$\sum_{|a_1|\leqslant A_1(x)} \sum_{|a_2|\leqslant A_2(x)} \sum_{|b_1|\leqslant B_1(x)} \sum_{|b_2|\leqslant B_2(x)} \pi_{E_1,E_2}^{r_1,r_2}(x) \sim C(r_1, r_2) \log\log x(16A_1(x)A_2(x)B_1(x)B_2(x)),$$

where $C(r_1, r_2)$ *is a constant depending only on fixed* $r_1, r_2 \in \mathbb{Z}$. This is the subject of ongoing research [ADJ00].

We have discussed the notions underlying the Lang-Trotter conjectures. In addition, we have discussed what work has been done in the direction of proving them.

Our direction now changes toward understanding the notions of our present work in this thesis on the *average Lang–Trotter conjecture for 2 elliptic curves*. We begin in the next section with an overview of some of the theory of *quadratic fields* and *orders* in quadratic fields.

3.4 Quadratic Fields and Orders

We start by recalling some facts regarding *quadratic fields*.

Definition Any extension of degree 2 over the field $\mathbb{Q}$ is called a *quadratic field*.

Let $d \neq 1$ be a square-free[7] rational integer[8] (positive or negative). Since the

[7] If $d = a^2$, for some $a \in \mathbb{Z}$, then we say that d is a square. If $d \neq a^2$, for any $a \in \mathbb{Z}$, then we say that d is non square, or not a square. If $p|d \Rightarrow p^2 \nmid d$, then we say that d is square-free. If $p|d \Rightarrow p^2|d$, then we say that d is square-full.

[8] By a rational integer we mean $d \in \mathbb{Z}$. This is used to distinguish integer between rational integer and algebraic integer.

polynomial $p(x) = x^2 - d$ is irreducible over $\mathbb{Q}$, the field $\mathbb{Q}(\alpha)$, obtained from $\mathbb{Q}$ by adjoining a root α of $p(x)$, is of degree 2 over $\mathbb{Q}$; $\mathbb{Q}(\alpha)$ is a quadratic field. We denote it by $\mathbb{Q}(\sqrt{d})$. It can be seen that any quadratic field is of this type. Furthermore, it can be shown that for distinct d (not equal to 1 and square-free), the fields $\mathbb{Q}(\sqrt{d})$ are distinct[9]. It follows that there is a one-to-one correspondence between quadratic fields and square-free rational integers $d \neq 1$.

In fact, $\mathbb{Q}(\sqrt{d})$ has exactly two distinct $\mathbb{Q}$-monomorphisms[10] to $\mathbb{C}$, namely

$$\begin{aligned} \sigma_1, \sigma_2 : \mathbb{Q}(\sqrt{d}) &\to \mathbb{C} \\ \sigma_1(r + s\sqrt{d}) &= r + s\sqrt{d} \\ \sigma_2(r + s\sqrt{d}) &= r - s\sqrt{d}. \end{aligned}$$

Definition Let $\{\omega_1, \omega_2\}$ be a basis[11] of $\mathbb{Q}(\sqrt{d})$. The *discriminant* $D(\omega_1, \omega_2)$ of this basis is defined as

$$D(\omega_1, \omega_2) \overset{\text{def}}{=} \left\{ \det \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) \end{bmatrix} \right\}^2 .$$

Definition Let $d \neq 1$ be a square–free rational integer. An element θ of $\mathbb{Q}(\sqrt{d})$ is called an *algebraic integer* if there is a monic[12] quadratic polynomial $p(t)$ with integer coefficients such that $p(\theta) = 0$.

It is known that the set of all algebraic integers in $K \overset{\text{def}}{=} \mathbb{Q}(\sqrt{d})$ forms a ring which is called the *ring of integers* of K.

Definition We let $\mathcal{O}_K$ denote the *ring of integers* of K.

[9] See [BŠ66], pg. 130

[10] A monomorphism is an injective homomorphism.

[11] $\{\omega_1, \omega_2\}$ span a $\mathbb{Z}$-submodule of rank 2 of $\mathbb{Q}(\sqrt{d})$.

[12] A quadratic polynomial over $\mathbb{Z}$ has the shape $ax^2 + bx + c$, with $a, b, c \in \mathbb{Z}$. It is monic when $a = 1$.

In fact, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank 2. A $\mathbb{Z}$-basis for $(\mathcal{O}_K, +)$ is called an integral basis for K (or for $\mathcal{O}_K$). Thus $\{1, \omega\}$ is an integral basis if and only if all $z \in \mathcal{O}_K$ are uniquely expressible in the form $a_1 1 + a_2\omega$, $a_i \in \mathbb{Z}$. The discriminants of the bases of the $\mathbb{Z}$-module $\mathcal{O}_K$ differ by a square unit in $\mathbb{Z}$. This can only be 1. That is, the discriminant of the $\mathbb{Z}$-module $\mathcal{O}_K$ is a well-defined element of $\mathbb{Z}$. It is called the *absolute discriminant* or *the discriminant* of K.

Our next lemma gives a complete description of the ring of integers and the discriminant of quadratic fields.

Lemma 3.1 *Let K be a quadratic field, $1, \omega$ be an integral basis and D_K the discriminant of K. Then,*

1. *If $d \equiv 1 \bmod 4$, we can take $\omega = \frac{1+\sqrt{d}}{2}$, and we have $D_K = d$.*

2. *If $d \equiv 2$ or $3 \bmod 4$, we can take $\omega = \sqrt{d}$, and we have $D_K = 4d$.*

Proof See [ST87], pg. 68, Theorem 3.3.

We now discuss *orders* in quadratic fields.

Definition An *order R* in K is a subring of K which as a $\mathbb{Z}$-submodule is finitely generated and has rank 2.

Example If $d \equiv 1 \bmod 4$, then $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ are two different orders in $\mathbb{Q}(\sqrt{d})$.

In a similar way we define the discriminant of an order.

Definition An integer D is called a *fundamental discriminant* if D is the discriminant of a quadratic field K. In other words, $D \neq 1$ and either $D \equiv 1 \bmod 4$ and square-free, or $D \equiv 0 \bmod 4$, $\frac{D}{4}$ is square-free and $\frac{D}{4} \equiv 2$ or $3 \bmod 4$.

The next lemma suggests that it is natural to consider quadratic fields together with their orders, since their discriminants form a sequence which is almost a union of two arithmetic progressions.

Lemma 3.2 *If K is a quadratic field of discriminant D, then every order R of K has discriminant Df^2 where f is a positive integer called the conductor of the order. Conversely, if A is any non-square integer such that $A \equiv 0$ or $1 \bmod 4$, then A is uniquely of the form $A = Df^2$ where D is a fundamental discriminant, and there exists a unique order R of discriminant A, and R is an order of the quadratic field $\mathbb{Q}(\sqrt{D})$.*

Proof See [Coh93], pg. 219, Proposition 5.1.3.

For an order R in a quadratic field K, we define the *class group* $c\ell(R)$ as the quotient of the group of non–zero fractional ideals[13] in R, $\Im_R$, by the group of non-zero principal fractional ideals[14] in R, $\mathcal{P}_R$.

Definition

$$c\ell(R) \stackrel{\text{def}}{=} \Im_R/\mathcal{P}_R.$$

It can be proved that[15] $\#c\ell(R) < \infty$.

Definition The number of ideal classes in $c\ell(R)$ is called the *class number* of R and is denoted by $h(D_R)$ or $h(R)$.

[13] Fractional ideals of R are subsets of K of the form $c^{-1}\mathbf{b}$ where $\mathbf{b}$ is an ideal of R and c is a non-zero element of R. For example, the fractional ideals of $\mathbb{Z}$ are of the form $q\mathbb{Z}$ where $q \in \mathbb{Q}$.

[14] A fractional ideal of R is principal if it is of the form $c^{-1}\mathbf{a}$, where $\mathbf{a}$ is a principal ideal in R.

[15] See [BŠ66], pg. 221, Theorem 2.

From Lemma 3.2 it is clear that if a is any non-square integer such that $a \equiv 0$ or $1 \bmod 4$, then $h(a)$ is well defined. We need one more concept from the theory of quadratic fields.

Definition (Hurwitz–Kronecker class number) Let $n \in \mathbb{Z}, n < 0$ and $\omega(a)$ be the number of roots of unity[16] in the quadratic order of discriminant a. Then the *Hurwitz-Kronecker* class number $H(n)$ is defined as

$$H(n) \stackrel{\text{def}}{=} 2 \sum_{\substack{e \in \mathbb{N}, e^2 \mid n \\ a = \frac{n}{e^2} \\ a \equiv 0,1 \bmod 4}} \frac{h(a)}{\omega(a)}.$$

Notice that $H(n)$ involves all of the orders containing the order of discriminant a. Now we have the definitions and notions in place to discuss the work of Deuring.

3.5 A Result of Deuring

Let E and E' be two elliptic curves over $\mathbb{Q}$, and for primes p of good reduction, let $\bar{E}$ and $\bar{E}'$ be their modulo p reductions respectively[17]. Recall that the elliptic curves $\bar{E}'$ over $\mathbb{F}_p$, which are $\mathbb{F}_p$–isomorphic to E, are given by all the choices

$$\bar{a}' = u^4 \bar{a} \text{ and } \bar{b}' = u^6 \bar{b}, \text{ with } u \in \mathbb{F}_p^*.$$

The number of such $\bar{E}'$ is[18]

$\frac{p-1}{6}$ when $\bar{a} = 0$ and $p \equiv 1 \bmod 3$,

$\frac{p-1}{4}$ when $\bar{b} = 0$ and $p \equiv 1 \bmod 4$,

[16] $\omega(-3) = 6, \omega(-4) = 4, \omega(a) = 2$ for $a < -4$, see [Coh93], pg. 226, Proposition 5.3.1.

[17] We change notation because we will be considering two elliptic curves E_1, and E_2, and their reductions $\bar{E}_1$ and $\bar{E}_2$ respectively in this section.

[18] This is true because if $p \equiv 1 \bmod n$, the number of different nth power residues modulo p (excluding 0) is $(p-1)/n$. See [Sie64], page 17.

$\frac{p-1}{2}$ when $\bar{a} = \bar{b} = 0$ and $p \equiv 1 \bmod 2$.

Theorem (Deuring) Let $p \geqslant 5$ be a prime, and let $r \in \mathbb{Z}, |r| \leqslant 2\sqrt{p}$. Then the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ with $p + 1 - r$ points is equal to $H(r^2 - 4p)$.

Proof See [Cox89], pg. 319, Theorem 14.18.

Deurings result provides a link between the average Lang-Trotter conjectures and class numbers.

Let $\xi_p^i, i = 1, 2$, be complete sets of residues $(\bmod\ p) \times (\bmod\ p)$. For fixed $r_1, r_2 \in \mathbb{Z}$, recall $\lambda_p = 1$ if $a_p(E_i) = r_i, i = 1, 2$, and 0 otherwise. For clarity in the exposition we denote

$$\sum_{\substack{|a_i| \leqslant A_i(x) \\ |b_i| \leqslant B_i(x)}},$$

to mean

$$\sum_{|a_1| \leqslant A_1(x)} \sum_{|b_1| \leqslant B_1(x)} \sum_{|a_2| \leqslant A_2(x)} \sum_{|b_2| \leqslant B_2(x)},$$

and generally a sum over i will mean a double sum. Further, let $A = A_1(x)A_2(x), B = B_1(x)B_2(x), C = A_1(x) + A_2(x), D = B_1(x) + B_2(x)$. Then

$$\begin{aligned}
\frac{1}{16AB} \sum_{\substack{|a_i| \leqslant A_i(x) \\ |b_i| \leqslant B_i(x)}} \pi_{E_1,E_2}^{r_1,r_2}(x) &= \frac{1}{16AB} \sum_{\substack{|a_i| \leqslant A_i(x) \\ |b_i| \leqslant B_i(x)}} \sum_{B_{r_i} \leqslant p \leqslant x} \lambda_p \\
&= \frac{1}{16AB} \sum_{B_{r_i} \leqslant p \leqslant x} \sum_{\substack{|a_i| \leqslant A_i(x) \\ |b_i| \leqslant B_i(x)}} \lambda_p \\
&\overset{\text{con}}{=} \frac{1}{16AB} \sum_{B_{r_i} \leqslant p \leqslant x} \sum_{(\bar{a}_i, \bar{b}_i) \in \xi_p^i} \sum_{\substack{a_i \equiv \bar{a}_i \pmod p \\ |a_i| \leqslant A_i(x)}} \sum_{\substack{b_i \equiv \bar{b}_i \pmod p \\ |b_i| \leqslant B_i(x)}} \lambda_p,
\end{aligned}$$

with the convention that the last sum expression is zero when it is empty, and where

$$B_{r_i} \overset{\text{def}}{=} \max_{i=1,2}\{5, |r_i| + 1, \frac{r_i^2}{4}\}.$$

Notice for each $i = 1, 2$,

$$\begin{aligned}\sum_{\substack{a_i \equiv \bar{a}_i \pmod p \\ |a_i| \leqslant A_i(x)}} 1 &= \frac{2A_i(x)}{p} + O(1), \\ \sum_{\substack{b_i \equiv \bar{b}_i \pmod p \\ |b_i| \leqslant B_i(x)}} 1 &= \frac{2B_i(x)}{p} + O(1).\end{aligned}$$

Hence,

$$\begin{aligned}&\frac{1}{16AB} \sum_{\substack{|a_i| \leqslant A_i(x) \\ |b_i| \leqslant B_i(x)}} \pi^{r_1,r_2}_{E_1,E_2}(x) \\ &\quad = \frac{1}{16AB} \sum_{B_{r_i} \leqslant p \leqslant x} \prod_{i=1,2} \left\{ \frac{2A_i(x)}{p} + O(1) \right\} \prod_{i=1,2} \left\{ \frac{2B_i(x)}{p} + O(1) \right\} \sum_{(\bar{a}_i, \bar{b}_i) \in \xi^i_p} \lambda_p.\end{aligned}$$

Consider the inner sum.

$$\begin{aligned}&\sum_{(\bar{a}_i, \bar{b}_i) \in \xi^i_p} \lambda_p \\ &\overset{\text{def}}{=} \#\{ \bar{E}_1/\mathbb{F}_p \ : \ a_p(E_1) = r_1 \} \times \#\{ \bar{E}_2/\mathbb{F}_p \ : \ a_p(E_2) = r_2 \} \\ &= \# \left\{ \frac{\bar{E}_1/\mathbb{F}_p}{\mathbb{F}_p\text{–isomorphism class}} \right\} \times \# \left\{ \frac{\bar{E}_2/\mathbb{F}_p}{\mathbb{F}_p\text{–isomorphism class}} \right\} \times \\ &\times \ \# \left\{ \begin{matrix} \mathbb{F}_p\text{–isomorphism classes} \\ \text{of elliptic curves with} \\ {\scriptstyle p+1-r_1} \text{ points} \end{matrix} \right\} \times \# \left\{ \begin{matrix} \mathbb{F}_p\text{–isomorphism classes} \\ \text{of elliptic curves with} \\ {\scriptstyle p+1-r_2} \text{ points} \end{matrix} \right\}.\end{aligned}$$

We observed at the beginning of this section that for each $i = 1, 2$,

$$\# \left\{ \frac{\bar{E}_i/\mathbb{F}_p}{\mathbb{F}_p\text{–isomorphism class}} \right\} = \frac{p}{2} + O(1).$$

Deuring's theorem implies for each $i = 1, 2$,

$$\# \left\{ \begin{matrix} \mathbb{F}_p\text{–isomorphism classes} \\ \text{of elliptic curves with} \\ {\scriptstyle p+1-r_i} \text{ points} \end{matrix} \right\} = H(r_i^2 - 4p).$$

It follows that,

$$\begin{aligned}\sum_{(\bar{a}_i, \bar{b}_i) \in \xi^i_p} \lambda_p &= \left\{ \frac{p}{2} + O(1) \right\}^2 H(r_1^2 - 4p) H(r_2^2 - 4p) \\ &= \frac{p^2}{4} H(r_1^2 - 4p) H(r_2^2 - 4p) + O(pH(r_1^2 - 4p) H(r_2^2 - 4p)).\end{aligned}$$

Moreover,

$$\prod_{i=1,2}\left\{\frac{2A_i(x)}{p}+O(1)\right\}\prod_{i=1,2}\left\{\frac{2B_i(x)}{p}+O(1)\right\}$$
$$=\frac{16AB}{p^4}+O\left(\frac{AD+BC}{p^3}+\frac{A+B+CD}{p^2}+\frac{C+D}{p}+1\right).$$

Then,

$$\frac{1}{16AB}\sum_{\substack{|a_i|\leqslant A_i(x)\\|b_i|\leqslant B_i(x)}}\sum_{B_{r_i}\leqslant p\leqslant x}\pi^{r_1,r_2}_{E_1,E_2}(x) = \frac{1}{4}\sum_{B_{r_i}\leqslant p\leqslant x}\frac{H(r_1^2-4p)H(r_2^2-4p)}{p^2}+\mathbf{ET},$$

where **ET** is equal to

$$O\left(\left\{\frac{D}{B}+\frac{C}{A}\right\}x+\left\{\frac{1}{A}+\frac{1}{B}+\frac{CD}{AB}\right\}x^2+\frac{C+D}{AB}x^3+\frac{1}{AB}x^4\right)(\log x)^3+$$
$$+O\left(\sum_{p\leqslant x}\frac{H(r_1^2-4p)H(r_2^2-4p)}{p^3}\right).$$

The point is that Deuring's theorem has transformed the study of the average Lang–Trotter conjecture for 2 elliptic curves to the study of the asymptotic behaviour of

$$\mathbf{MT}=\frac{1}{4}\sum_{B_{r_i}\leqslant p\leqslant x}\frac{H(r_1^2-4p)H(r_2^2-4p)}{p^2}.$$

In order to study **MT**, and justify **ET**, we recall Dirichlet's class number formula in the next section.

3.6 Dirichlet's Class Number Formula

Before we can apply Dirichlet's class number formula to study the main term **MT** and the error term **ET** from the last section, we need to be able to associate a Dirichlet character to a number, $A<0$, $A\equiv 0,1 \bmod 4$. We do this in subsection 3.6.2. In the next subsection we define the Legendre–Jacobi–Kronecker symbol.

3.6.1 The Legendre–Jacobi–Kronecker (LJK) symbol

Here we define Legendre's symbol, Jacobi's symbol, and the Legendre-Jacobi-Kronecker symbol. Let $a \in \mathbb{Z}$.

Definiton (Legendre's symbol) If $p > 2$, then we define the *Legendre symbol* $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) \overset{\text{def}}{=} \begin{cases} 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \bmod p \text{ has a solution;} \\ 0 & \text{if } p \mid a; \\ -1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \bmod p \text{ has no solution.} \end{cases}$$

Note that Legendre's symbol is to the prime modulus p. Jacobi's symbol is a natural generalization to the modulus Q, where Q is any positive, odd integer.

Definition (Jacobi's symbol) Let Q be positive and odd. We write $Q = p_1 p_2 \cdots p_k$, where the p_i are odd primes, not necessarily distinct. Then we define the *Jacobi symbol* as follows:

$$\left(\frac{a}{Q}\right) \overset{\text{def}}{=} \prod_{j=1}^{k} \left(\frac{a}{p_i}\right).$$

We are now ready to define[19] the LJK symbol to the modulus m, where m is any positive integer.

Definition (LJK symbol) Let $m > 0, m = 2^c p_1 p_2 \cdots p_k$ where the p_i are odd primes, $c \geqslant 0$, $A \in \mathbb{Z}$, $A \equiv 0$ or $1 \bmod 4$, and A not a perfect square. The LJK symbol $\left(\frac{A}{m}\right)$ is defined by

$$\left(\frac{A}{m}\right) \overset{\text{def}}{=} \left(\frac{A}{2}\right)^c \prod_{i=1}^{k} \left(\frac{A}{p_i}\right),$$

[19] See [Hua82], pg. 304.

where

$$\left(\frac{A}{2}\right) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } A \equiv 0 \bmod 4, \\ 1 & \text{if } A \equiv 1 \bmod 8, \\ \text{-1} & \text{if } A \equiv 5 \bmod 8; \end{cases}$$

$$\left(\frac{A}{p}\right) \stackrel{\text{def}}{=} \text{Legendre's symbol } (p > 2).$$

3.6.2 Properties of the LJK Symbol

We list the properties of the Legendre symbol, Jacobi symbol and the LJK symbol. Furthermore, we use the properties of the LJK symbol in order to associate a Dirichlet character to a number, $A < 0, A \equiv 0, 1 \bmod 4$. Let $a, a', b \in \mathbb{Z}$.

Properties of the Legendre symbol

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. See [EM99], pg. 162, exercise 7.1.4.

2. If $a \equiv b \bmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. This is clear from the definition of the Legendre symbol. That is, if a is a quadratic residue modulo p, then so is b. The same holds if a is a quadratic non residue.

3. If p, q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

or equivalently, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \pmod 4$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Note that this is *Gauss's law of quadratic reciprocity.* An equivalent formulation[20] of Gauss's law of quadratic reciprocity is as follows. For p, q as above, and $\delta \geqslant 1$, if $p \equiv \pm q \pmod{4\delta}$, then $\left(\frac{\delta}{p}\right) = \left(\frac{\delta}{q}\right)$.

[20] See [Ros94], pg. 67.

Properties of the Jacobi symbol

1. If Q and Q' are odd and positive, then[21]

   (a) $\left(\frac{a}{Q}\right)\left(\frac{a}{Q'}\right) = \left(\frac{a}{QQ'}\right)$.

   (b) $\left(\frac{a}{Q}\right)\left(\frac{a'}{Q}\right) = \left(\frac{aa'}{Q}\right)$.

   (c) $\left(\frac{a}{Q}\right) = \left(\frac{a'}{Q}\right)$ if $a \equiv a' \bmod Q$.

2. If P and Q are odd, positive and coprime, then

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

   This is the reciprocity law for the Jacobi symbol[22].

Properties of the LJK symbol

1. The following are true:

   (a) If $(A, m) > 1$, then $\left(\frac{A}{m}\right) = 0$;

   (b) If $(A, m) = 1$, then $\left(\frac{A}{m}\right) = \pm 1$;

   (c) If $m_1 > 0, m_2 > 0$, then $\left(\frac{A}{m_1 m_2}\right) = \left(\frac{A}{m_1}\right)\left(\frac{A}{m_2}\right)$.

2. If $m > 0, (m, A) = 1$, then the LJK symbol is given by

$$\left(\frac{A}{m}\right) = \begin{cases} \left(\frac{m}{|A|}\right), & \text{when } A \text{ is odd;} \\ \left(\frac{2}{m}\right)^c (-1)^{\frac{u-1}{2}\frac{m-1}{2}} \left(\frac{m}{|u|}\right), & \text{when } A = 2^c u, 2 \nmid u. \end{cases}$$

   Here $\left(\frac{m}{|A|}\right), \left(\frac{2}{m}\right), \left(\frac{m}{|u|}\right)$ are all Jacobi symbols[23].

[21] See [EM99], pg. 183, exercise 7.6.12.

[22] See [EM99], pg. 184, exercise 7.6.15.

[23] See [Hua82], pg.305, Theorem 3.1.

3. Suppose that $m > 0, n > 0$, and $m \equiv -n \bmod |A|$. Then[24]

$$\left(\frac{A}{m}\right) = \begin{cases} \left(\frac{A}{m}\right), & \text{if } A > 0; \\ -\left(\frac{A}{n}\right), & \text{if } A < 0. \end{cases}$$

4. The LJK symbol $\left(\frac{A}{m}\right) = \left(\frac{A}{|A|+m}\right)$ is a real[25] Dirichlet character modulo $|A|$.

Now if $A < 0$, $A \equiv 0, 1 \bmod 4$, then by lemma 3.2 there exists a fundamental discriminant D such that $A = Df^2$. By the properties of the LJK symbol we can associate a Dirichlet character to a number, $A < 0$, $A \equiv 0, 1 \bmod 4$, namely

$$\chi_A(m) = \left(\frac{A}{m}\right).$$

We have the notions in place to discuss Dirichlet's class number formula.

3.6.3 Dirichlet's Class Number Formula

Let $s = \sigma + it \in \mathbb{C}$, then for $\sigma > 0$, $A \in \mathbb{Z}$, $A < 0$, $A \equiv 0, 1 \bmod 4$, we consider the Dirichlet L-series

$$L(s, \chi_A) \overset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{\chi_A(n)}{n^s},$$

where $\chi_A(n) = \left(\frac{A}{n}\right)$ is LJK symbol. $L(s, \chi_A)$ satisfies a functional equation[26] and is an analytic function of s for all $s \in \mathbb{C}$ whenever χ_A is non-trivial[27].

Dirichlet showed at $s = 1$, $L(1, \chi_A) \neq 0$, and deduced *Dirichlet's class number formula*[28]:

$$h(A) = \frac{\omega(A)\sqrt{|A|}L(1, \chi_A)}{2\pi},$$

[24] See [Hua82], pg. 305, Theorem 3.3.

[25] See [Hua82], pg. 305, Theorem 3.2.

[26] See [Dav80], pg. 11.

[27] The character $\chi_0 : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ satisfying $\chi_0(a) = 1$ for all $(a, q) = 1$ is called the trivial character (or principal) character.

[28] See [EM99], exercise 10.5.12, for a sketch of a proof in the case that A is a fundamental discriminant. See also [BŠ66], chapter 5.

where $\omega(A)$ is the number of units in R_A (order associated to A).

We may now justify the error term **ET** from the last section. For $i = 1, 2$, $|r_i| \leqslant 2\sqrt{p}$ implies

$$\sqrt{4p - r_i^2} = 2\sqrt{p} + O(1).$$

The definition of the Hurwitz–Kronecker class number and the fact that $w(d_i) \geqslant 2$ together imply

$$H(r_i^2 - 4p) = 2 \sum_{\substack{f_i^2 | r_i^2 - 4p \\ f_i^2 d_i = r_i^2 - 4p \\ d_i \equiv 0,1 \bmod 4}} \frac{h(d_i)}{w(d_i)} \leqslant \sum_{\substack{f_i^2 | r_i^2 - 4p \\ f_i^2 d_i = r_i^2 - 4p \\ d_i \equiv 0,1 \bmod 4}} h(d_i).$$

Dirichlets class number formula, and an upper bound for $L(1, \chi_{d_i})$ obtained in lemma 2.16 together imply

$$h(d_i) = \frac{w(d_i)}{2\pi} \sqrt{|d_i|} L(1, \chi_{d_i}) \ll \sqrt{|d_i|} \log |d_i| \ll \frac{\sqrt{p} \log p}{f_i}.$$

It follows that

$$H(r_i^2 - 4p) \quad \ll \quad \sqrt{p} \log p \sum_{\substack{f_i^2 | r_i^2 - 4p \\ f_i^2 d_i = r_i^2 - 4p}} \frac{1}{f_i}.$$

But

$$\sum_{f_i^2 | r_i^2 - 4p} \frac{1}{f_i} \ll \sum_{f_i \leqslant 2\sqrt{p}} \frac{1}{f_i} \ll \int_1^{2\sqrt{p}} \frac{1}{s} ds \ll \log p,$$

so that

$$H(r_i^2 - 4p) \ll \sqrt{p} (\log p)^2.$$

It follows that $H(r_1^2 - 4p) H(r_2^2 - 4p) \ll p (\log p)^4$, and

$$\sum_{p \leqslant x} \frac{H(r_1^2 - 4p) H(r_2^2 - 4p)}{p} \ll \sum_{p \leqslant x} (\log p)^4 \leqslant (\log x)^4 \sum_{p \leqslant x} 1 \ll x (\log x)^3,$$

$$\sum_{p\leqslant x} H(r_1^2-4p)H(r_2^2-4p) \ll \sum_{p\leqslant x} p(\log p)^4 \leqslant x(\log x)^4 \sum_{p\leqslant x} 1 \ll x^2(\log x)^3,$$

$$\sum_{p\leqslant x} pH(r_1^2-4p)H(r_2^2-4p) \ll x^3(\log x)^3,$$

and

$$\sum_{p\leqslant x} p^2 H(r_1^2-4p)H(r_2^2-4p) \ll x^4(\log x)^3.$$

Hence, the error term **ET** is equal to

$$\begin{aligned}
&\frac{1}{16AB}\sum_{B_{r_i}\leqslant p\leqslant x}\frac{p^2}{4}H(r_1^2-4p)H(r_2^2-4p)O\left(\frac{AD+BC}{p^3}+\frac{A+B+CD}{p^2}+\frac{C+D}{p}+1\right)\\
+&\ \frac{1}{16AB}\sum_{B_{r_i}\leqslant p\leqslant x} O(pH(r_1^2-4p)H(r_2^2-4p))\times\\
\times&\ O\left(\frac{AD+BC}{p^3}+\frac{A+B+CD}{p^2}+\frac{C+D}{p}+1\right)\\
+&\ \frac{1}{16AB}\sum_{B_{r_i}\leqslant p\leqslant x} O(pH(r_1^2-4p)H(r_2^2-4p))\frac{16AB}{p^4},
\end{aligned}$$

which is equal to

$$\begin{aligned}
&O\left(\frac{1}{AB}\sum_{p\leqslant x}\left\{\frac{AD+BC}{p}+(A+B+CD)+(C+D)p+p^2\right\}H(r_1^2-4p)H(r_2^2-4p)\right)\\
+&\ O\left(\sum_{p\leqslant x}\left\{\frac{AD+BC}{p^2}+(A+B+CD)\frac{1}{p}+(C+D)+p\right\}H(r_1^2-4p)H(r_2^2-4p)\right)\\
+&\ O\left(\sum_{p\leqslant x}\frac{H(r_1^2-4p)H(r_2^2-4p)}{p^3}\right),
\end{aligned}$$

which is equal to

$$\begin{aligned}
&O\left(\left\{\frac{D}{B}+\frac{C}{A}\right\}x+\left\{\frac{1}{A}+\frac{1}{B}+\frac{CD}{AB}\right\}x^2+\frac{(C+D)}{AB}x^3+\frac{1}{AB}x^4\right)(\log x)^3\\
+&\ O\left(\sum_{p\leqslant x}\frac{H(r_1^2-4p)H(r_2^2-4p)}{p^3}\right).
\end{aligned}$$

We have completed our survey of the notions underlying our thesis. In the next section we present Theorem 1 proven in the next chapter and discuss it's relationship with the Lang–Trotter conjecture for 2 elliptic curves.

3.7 On a Theorem of Fouvry and Murty

We prove the following theorem in the next chapter.

Theorem 1 *For $r \in \mathbb{Z}$, r of odd parity,*

$$\sum_{p \leqslant x} \frac{1}{p^2} H_{dg}^2(r^2 - 4p) \sim \frac{K(r)}{\pi^2} \log \log x,$$

where

$$\begin{aligned} H_{dg}^2(r^2-4p) &\stackrel{\text{def}}{=} \sum_{\substack{f \in \mathbb{N}, f^2 | r^2-4p \\ df = r^2-4p \\ d \equiv 0,1 \bmod 4}} \frac{h^2(d)}{w^2(d)}, \\ K(r) &= \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)}{nf^2\phi(nf^2)} \sum_{\substack{a \bmod 4n \\ (r^2-af^2,4n)=4}} \left(\frac{a}{n}\right) \\ &= \frac{4}{9} \prod_{p|r} \frac{p^2(p^2+1)}{(p^2-1)^2} \prod_{p \nmid 2r} \frac{2p^8 - p^7 - 4p^6 - 4p^5 - 3p^4 - 2p^3 + p^2 - p - 1}{(p^4-1)(p^2-1)^2}, \end{aligned}$$

is a non-zero constant depending only on r, $d(n)$ is the number of divisors of n, ϕ is Euler's ϕ function, $\sum_{a \bmod 4n}$ is a sum over a complete set of invertible residues modulo $4n$, and $(\frac{a}{n})$ is the Legendre-Jacobi-Kronecker (LJK) symbol.

We explain the relationship between Theorem 1 and the average Lang–Trotter conjecture for 2 elliptic curves.

Using Deuring's theorem, the number of $\mathbb{F}_p$–isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ is $H(-4p)$, Murty and Fouvry [FM95] reduce the

$$\sum_{|a_1| \leqslant A_1(x)} \sum_{|a_2| \leqslant A_2(x)} \sum_{|b_1| \leqslant B_1(x)} \sum_{|b_2| \leqslant B_2(x)} \pi_{E_1,E_2}^{r_1,r_2}(x),$$

in the case $r_1 = r_2 = 0$ (as we did in section 3.5 in the general case $r_1, r_2 \in \mathbb{Z}$), to

$$\frac{1}{4} \sum_{p \leqslant x} \frac{H^2(-4p)}{p^2} + \mathbf{ET},$$

and then prove

$$\sum_{p\leqslant x}\frac{H^2(-4p)}{p^2}\sim\frac{35}{24}\log\log x.$$

More precisely, by the definition of the Hurwitz–Kronecker class number $H(-4p)$,

$$\sum_{p\leqslant x}\frac{H^2(-4p)}{p^2}=\sum_{p\leqslant x}\frac{1}{p^2}\left\{2\sum_{\substack{f^2|-4p\\ d=\frac{-4p}{f^2}\\ d\equiv 0,1 \bmod 4}}\frac{h(d)}{w(d)}\right\}^2,$$

and

$$2\sum_{\substack{f^2|-4p\\ d=\frac{-4p}{f^2}\\ d\equiv 0,1 \bmod 4}}\frac{h(d)}{w(d)}=2\sum_{\substack{f=1,2\\ d=\frac{-4p}{f^2}\\ d\equiv 0,1 \bmod 4}}\frac{h(d)}{w(d)}=2\begin{cases}\frac{h(-4p)}{w(-4p)}+\frac{h(-p)}{w(-p)} & \text{if } p\equiv 3 \bmod 4,\\ \frac{h(-4p)}{w(-4p)} & \text{if } p\equiv 1 \bmod 4.\end{cases}$$

Recall that $w(-4)=4, w(-3)=6$, and $w(d)=2$ for all other $d<-4$. Notice for all primes p, $-4p<-4$, so that $w(-4p)=2$ for all p. By excluding the primes 2 and 3, $-p<-4$, so that $w(-p)=2$ for all $p\neq 2,3$. It follows that

$$\begin{aligned}
&\sum_{5\leqslant p\leqslant x}\frac{1}{p^2}H^2(-4p)\\
&=\sum_{\substack{5\leqslant x\\ p\equiv 3 \bmod 4}}\frac{1}{p^2}\{h(-p)+h(-4p)\}^2+\sum_{\substack{5\leqslant p\leqslant x\\ p\equiv 1 \bmod 4}}\frac{1}{p^2}h^2(-4p)\\
&=\sum_{\substack{5\leqslant p\leqslant x\\ p\equiv 3 \bmod 4}}\frac{h^2(-p)}{p^2}+2\sum_{\substack{5\leqslant p\leqslant x\\ p\equiv 3 \bmod 4}}\frac{h(-p)h(-4p)}{p^2}+\left\{\sum_{\substack{5\leqslant p\leqslant x\\ p\equiv 3 \bmod 4}}+\sum_{\substack{5\leqslant p\leqslant x\\ p\equiv 1 \bmod 4}}\right\}\frac{1}{p^2}h^2(-4p)\\
&=\sum_{\substack{5\leqslant p\leqslant x\\ p\equiv 3 \bmod 4}}\frac{h^2(-p)}{p^2}+2\sum_{\substack{5\leqslant p\leqslant x\\ p\equiv 3 \bmod 4}}\frac{h(-p)h(-4p)}{p^2}+\sum_{5\leqslant p\leqslant x}\frac{h^2(-4p)}{p^2}\\
&\overset{\text{def}}{=} T_{1,1}(x)+2T_{1,4}(x)+T_{4,4}(x).
\end{aligned}$$

Murty and Fouvry show that

$$T_{1,1}(x)\sim\frac{5}{24}\log\log x,$$

$$T_{1,4}(x) \sim \frac{1}{4} \log\log x,$$

and

$$T_{4,4}(x) \sim \frac{3}{4} \log\log x,$$

from which they deduce

$$\sum_{5 \leqslant p \leqslant x} \frac{1}{p^2} H^2(-4p) \sim \left(\frac{5}{24} + \frac{1}{2} + \frac{3}{4} \right) \log\log x = \frac{35}{24} \log\log x.$$

Generally, for $r \in \mathbb{Z}, |r| \leqslant 2\sqrt{p}$, by the definition of the Hurwitz–Kronecker class number $H(r^2 - 4p)$,

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

Observe that

$$\sum_{p \leqslant x} \frac{1}{p^2} H^2(r^2 - 4p),$$

may be written as a sum over a diagonal (dg) part and a non-diagonal (ndg) part. That is,

$$\begin{aligned} &\sum_{p \leqslant x} \frac{1}{p^2} H^2(r^2 - 4p) \\ &= \sum_{p \leqslant x} \frac{1}{p^2} \left(2 \sum_{\substack{f^2 | r^2 - 4p \\ d = \frac{r^2 - 4p}{f^2} \\ d \equiv 0,1 \bmod 4}} \frac{h(d)}{w(d)} \right)^2 \\ &= 4 \sum_{p \leqslant x} \frac{1}{p^2} \sum_{\substack{f_1^2 | r^2 - 4p \\ d_1 \equiv 0,1 \bmod 4 \\ f_2^2 | r^2 - 4p \\ d_2 \equiv 0,1 \bmod 4}} \frac{h(d_1)}{w(d_1)} \frac{h(d_2)}{w(d_2)} \end{aligned}$$

$$= 4\sum_{p\leqslant x}\frac{1}{p^2}\left\{\sum_{\substack{f_1^2|r^2-4p\\ d_1\equiv 0,1 \bmod 4\\ f_2^2|r^2-4p\\ d_2\equiv 0,1 \bmod 4\\ f_1=f_2}}\frac{h^2(d_1)}{w^2(d_1)}+\sum_{\substack{f_1^2|r^2-4p\\ d_1\equiv 0,1 \bmod 4\\ f_2^2|r^2-4p\\ d_2\equiv 0,1 \bmod 4\\ f_1\neq f_2}}\frac{h(d_1)}{w(d_1)}\frac{h(d_2)}{w(d_2)}\right\}$$

$$= 4\sum_{p\leqslant x}\frac{1}{p^2}\left\{\sum_{\substack{f^2|r^2-4p\\ d\equiv 0,1 \bmod 4}}\frac{h^2(d)}{w^2(d)}+2\sum_{\substack{f_1^2|r^2-4p\\ d_1\equiv 0,1 \bmod 4\\ f_2^2|r^2-4p\\ d_2\equiv 0,1 \bmod 4\\ f_1< f_2}}\frac{h(d_1)}{w(d_1)}\frac{h(d_2)}{w(d_2)}\right\}$$

$$\overset{\text{def}}{=} 4\sum_{p\leqslant x}\frac{1}{p^2}H^2_{\text{dg}}(r^2-4p)+8\sum_{p\leqslant x}\frac{1}{p^2}H^2_{\text{ndg}}(r^2-4p).$$

We modify the methods found in David's and Pappalardi's paper [DP99] to obtain a result (Theorem 1) on the diagonal part,

$$\sum_{p\leqslant x}\frac{1}{p^2}H^2_{\text{dg}}(r^2-4p)\sim\frac{K(r)}{\pi^2}\log\log x,$$

for $r\in\mathbb{Z}$, r of odd parity, which is analogous to the result obtained by Fouvry and Murty in [FM95] after summing their diagonal parts,

$$T_{1,1}(x)+T_{4,4}(x)\sim\left(\frac{5}{24}+\frac{3}{4}\right)\log\log x=\frac{23}{24}\log\log x.$$

More precisely, instead of using the result of lemma 2.15; for $U>0$,

$$L(1,\chi_d)=\sum_{n\leqslant U}\left(\frac{d}{n}\right)\frac{1}{n}+O\left(\frac{\sqrt{|d|}\log|d|}{U}\right),$$

whose proof depends on the Pólya–Vinogradov inequality lemma 2.14, as used in [DP99], we use the result of lemma 4.1 on $L(1,\chi_{d_1})L(1,\chi_{d_2})$.

Chapter 4

Proof of Theorem 1

This chapter is solely concerned with the proof of Theorem 1. It displays the technique we developed in order to prove the average Lang–Trotter conjecture for 2 elliptic curves. This work is in progress [ADJ00]. The main difference between our technique and the technique from [DP99] is lemma 4.1. We give a new representation for a product of Dirichlet L–Functions $L(s, \chi_{d_1})L(s, \chi_{d_2})$, valid for non–trivial Dirichlet characters $\chi_{d_i}, i = 1, 2$, and $s = 1$, using the technique of contour integration.

Theorem 1 *For $r \in \mathbb{Z}$, r of odd parity,*

$$\sum_{p \leqslant x} \frac{1}{p^2} H^2_{d_g}(r^2 - 4p) \sim \frac{K(r)}{\pi^2} \log\log x,$$

where

$$\begin{aligned} H^2_{d_g}(r^2 - 4p) &\overset{\text{def}}{=} \sum_{\substack{f \in \mathbb{N}, f^2 \mid r^2 - 4p \\ df = r^2 - 4p \\ d \equiv 0,1 \bmod 4}} \frac{h^2(d)}{w^2(d)}, \\ K(r) &= \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)}{nf^2 \phi(nf^2)} \sum_{\substack{a \bmod 4n \\ (r^2 - af^2, 4n) = 4}} \left(\frac{a}{n}\right) \\ &= \frac{4}{9} \prod_{p \mid r} \frac{p^2(p^2+1)}{(p^2-1)^2} \prod_{p \nmid 2r} \frac{2p^8 - p^7 - 4p^6 - 4p^5 - 3p^4 - 2p^3 + p^2 - p - 1}{(p^4-1)(p^2-1)^2}, \end{aligned}$$

is a non-zero constant depending only on r, $d(n)$ is the number of divisors of n, ϕ is Euler's ϕ function, $\sum_{a \bmod 4n}$ is a sum over a complete set of invertible residues modulo $4n$, and $(\frac{a}{n})$ is the Legendre-Jacobi-Kronecker (LJK) symbol.

Proof of Theorem 1 By Dirichlet's class number formula,

$$h^2(d) = \frac{w^2(d)}{4\pi^2}|d|L^2(1,\chi_d),$$

we have[1]

$$\begin{aligned}
\sum_{B_r \leqslant p \leqslant x} \frac{1}{p^2} H^2_{\mathrm{dg}}(r^2-4p) &= \sum_{B_r \leqslant p \leqslant x} \frac{1}{p^2} \sum_{\substack{f^2|r^2-4p \\ f^2d=r^2-4p \\ d\equiv 1 \bmod 4}} \frac{h^2(d)}{w^2(d)} \\
&= \frac{1}{4\pi^2} \sum_{B_r \leqslant p \leqslant x} \frac{1}{p^2} \sum_{\substack{f^2|r^2-4p \\ f^2d=r^2-4p \\ d\equiv 1 \bmod 4}} |d|L^2(1,\chi_d) \\
&= \frac{1}{4\pi^2} \sum_{B_r \leqslant p \leqslant x} \frac{1}{p^2} \sum_{\substack{f^2|r^2-4p \\ f^2d=r^2-4p \\ d\equiv 1 \bmod 4}} \frac{4p-r^2}{f^2} L^2(1,\chi_d).
\end{aligned}$$

For clarity we define,

$$S_f^r(B_r, x) \overset{\text{def}}{=} \{\, B_r \leqslant p \leqslant x \,:\, r^2-4p \equiv 0 \bmod f^2, f \in \mathbb{N}, d = \frac{r^2-4p}{f^2} \equiv 1 \bmod 4 \,\}.$$

Our next move is to interchange the sums. We observe since f^2 divides r^2-4p, $|f| \leqslant 2\sqrt{p}$. Further, as $p \leqslant x$, we have that $|f| \leqslant 2\sqrt{x}$. We range the f's over all numbers less than $2\sqrt{x}$, and then pick primes p satisfying the conditions of $S_f^r(B_r, x)$.

[1] Note that we define $B_r \overset{\text{def}}{=} \max\{5, |r|+1, \frac{r^2}{4}\}$ and set $p \geqslant B_r$ to ensure $p \geqslant \frac{r^2}{4}, p \geqslant 5$, and $p \geqslant |r|+1$. We take a moment to explain why we set $p \geqslant B_r$. Since r is odd, if $f^2|r^2-4p$, then f is odd, and $d = \frac{r^2-4p}{f^2} \equiv 1 \bmod 4$. Since $(r,f)|p$, therefore $(r,f)=p$ or $(r,f)=1$. We set $p \geqslant |r|+1$ to ensure $(r,f)=1$, a necessary condition for p to be in the arithmetic progression $4p \equiv r^2 \bmod f^2$. Furthermore, we have $p \geqslant \frac{r^2}{4}$, as $|r| \leqslant 2\sqrt{p}$, and $p \geqslant 5$, as we excluded the primes 2 and 3. We encode these inequalities on p by setting $p \geqslant B_r$.

It follows that by interchanging the sums,

$$
\begin{aligned}
&\frac{1}{4\pi^2}\sum_{B_r\leqslant p\leqslant x}\frac{1}{p^2}\sum_{\substack{f^2|r^2-4p\\ f^2d=r^2-4p\\ d\equiv 1 \bmod 4}}\frac{4p-r^2}{f^2}L^2(1,\chi_d)\\
&\overset{\text{con}}{=}\frac{1}{4\pi^2}\sum_{f\leqslant 2\sqrt{x}}\frac{1}{f^2}\sum_{p\in S_f^r(B_r,x)}\frac{4p-r^2}{p^2}L^2(1,\chi_d)\\
&=\frac{1}{\pi^2}\sum_{f\leqslant 2\sqrt{x}}\frac{1}{f^2}\sum_{p\in S_f^r(B_r,x)}\frac{L^2(1,\chi_d)}{p}-\frac{r^2}{4\pi^2}\sum_{f\leqslant 2\sqrt{x}}\frac{1}{f^2}\sum_{p\in S_f^r(B_r,x)}\frac{L^2(1,\chi_d)}{p^2},
\end{aligned}
$$

with the convention that the sum expression is zero when it is empty. By partial summation lemma 2.1,

$$
\begin{aligned}
&\sum_{p\in S_f^r(B_r,x)}\frac{L^2(1,\chi_d)}{p}\frac{\log p}{\log p}\\
&=\frac{1}{x\log x}\left\{\sum_{p\in S_f^r(1,x)}L^2(1,\chi_d)\log p\right\}-\frac{1}{B_r\log B_r}\left\{\sum_{p\in S_f^r(1,B_r)}L^2(1,\chi_d)\log p\right\}\\
&-\int_{B_r}^{x}\left\{\sum_{p\in S_f^r(1,t)}L^2(1,\chi_d)\log p\right\}\left\{\frac{d}{dt}\frac{1}{t\log t}\right\}dt\\
&=\frac{1}{x\log x}\left\{\sum_{p\in S_f^r(B_r,x)}L^2(1,\chi_d)\log p\right\}-\int_{B_r}^{x}\left\{\sum_{p\in S_f^r(B_r,t)}L^2(1,\chi_d)\log p\right\}\left\{\frac{d}{dt}\frac{1}{t\log t}\right\}dt\\
&+\left(\frac{1}{x\log x}-\frac{1}{B_r\log B_r}\right)\sum_{p\in S_f^r(1,B_r)}L^2(1,\chi_d)\log p\\
&-\int_{B_r}^{x}\left\{\sum_{p\in S_f^r(1,B_r)}L^2(1,\chi_d)\log p\right\}\left\{\frac{d}{dt}\frac{1}{t\log t}\right\}dt.
\end{aligned}
$$

We claim[2] for any $0<\epsilon<\frac{1}{12}, c>6-3\epsilon$,

$$
\sum_{f\leqslant 2\sqrt{x}}\frac{1}{f^2}\sum_{p\in S_f^r(B_r,x)}L^2(1,\chi_d)\log p=K(r)x+O_{c,\epsilon,r}\left(\frac{x}{(\log x)^c}\right).
$$

Assuming the claim for the moment, we complete the proof. Observe,

$$
\frac{1}{x\log x}\left\{\sum_{f\leqslant 2\sqrt{x}}\frac{1}{f^2}\sum_{p\in S_f^r(B_r,x)}L^2(1,\chi_d)\log p\right\}
$$

[2] Note that we call this claim Proposition 4.1, and prove it in section 4.2.

$$\begin{aligned}
& - \int_{B_r}^{x} \left\{ \sum_{f\leqslant 2\sqrt{t}} \frac{1}{f^2} \sum_{p\in S_f^r(B_r,t)} L^2(1,\chi_d)\log p \right\} \left\{ \frac{d}{dt}\frac{1}{t\log t} \right\} dt \\
&= \frac{1}{x\log x}\left\{ K(r)x + O_{r,c,\epsilon}\left(\frac{x}{(\log x)^c}\right)\right\} \\
&+ \int_{B_r}^{x} \left\{ K(r)t + O_{r,c,\epsilon}\left(\frac{t}{(\log t)^c}\right)\right\}\left\{\frac{1+\log t}{t^2(\log t)^2}\right\} dt \\
&= K(r)\left\{\frac{1}{\log x} + \int_{B_r}^{x}\frac{dt}{t(\log t)^2} + \int_{B_r}^{x}\frac{dt}{t\log t}\right\} \\
&+ O_{r,c,\epsilon}\left(\max\left\{\frac{1}{(\log x)^{c+1}}, \int_{B_r}^{x}\frac{dt}{t(\log t)^{c+2}}, \int_{B_r}^{x}\frac{dt}{t(\log t)^{c+1}}\right\}\right) \\
&= K(r)\left\{\log\log x + \frac{1}{\log B_r} - \log\log B_r\right\} \\
&+ O_{r,c,\epsilon}\left(\max\left\{\frac{1}{(\log x)^{c+1}}, \frac{1}{c(\log B_r)^c} - \frac{1}{c(\log x)^c}\right\}\right).
\end{aligned}$$

Moreover,

$$\Omega(r) \overset{\text{def}}{=} \sum_{f\leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p\in S_f^r(1,B_r)} L^2(1,\chi_d)\log p,$$

is a constant depending on r. This is true because $\log|d| \overset{\text{def}}{=} \log\frac{4p-r^2}{f^2} \ll \log p$, together with lemma 2.16, implies $L^2(1,\chi_d) \ll (\log|d|)^2 \ll (\log p)^2$, so that,

$$\begin{aligned}
\Omega(r) &\ll \sum_{f\leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p\in S_f^r(1,B_r)} (\log|d|)^2\log p \\
&\ll \sum_{f\leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p\leqslant B_r} (\log p)^3 \\
&\ll_r [B_r](\log B_r)^2.
\end{aligned}$$

Hence,

$$\begin{aligned}
& \left(\frac{1}{x\log x} - \frac{1}{B_r\log B_r}\right)\Omega(r) - \Omega(r)\int_{B_r}^{x}\left\{\frac{d}{dt}\frac{1}{t\log t}\right\} dt \\
&= \left(\frac{1}{x\log x} - \frac{1}{B_r\log B_r}\right)\Omega(r) - \Omega(r)\left(\frac{1}{x\log x} - \frac{1}{B_r\log B_r}\right) \\
&= 0.
\end{aligned}$$

Letting $x \to \infty$, we deduce,

$$\sum_{f\leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p\in S_f^r(B_r,x)} \frac{L^2(1,\chi_d)}{p} \sim K(r)\log\log x.$$

Since

$$\int_{B_r}^{x} \frac{\log\log t}{t^2} dt = \frac{\log\log B_r}{B_r} - \frac{\log\log x}{x} + \int_{B_r}^{x} \frac{dt}{t^2\log t},$$

and

$$\int_{B_r}^{x} \frac{dt}{t^2\log t} \ll \frac{1}{B_r\log B_r},$$

therefore by partial summation lemma 2.1,

$$\begin{aligned} & \sum_{f\leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p\in S_f^r(B_r,x)} \frac{L^2(1,\chi_d)}{p^2} \\ = \; & \frac{1}{x} \sum_{f\leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p\in S_f^r(B_r,x)} \frac{L^2(1,\chi_d)}{p} + \int_{B_r}^{x} \left\{ \sum_{f\leqslant 2\sqrt{t}} \frac{1}{f^2} \sum_{p\in S_f^r(B_r,t)} \frac{L^2(1,\chi_d)}{p} \right\} \frac{1}{t^2} dt \\ = \; & o(\log\log x). \end{aligned}$$

We have shown

$$\sum_{B_r\leqslant p\leqslant x} \frac{1}{p^2} H_{\mathrm{dg}}^2(r^2-4p) \sim \frac{K(r)}{\pi^2}\log\log x.$$

Lastly, note that $\sum_{p\leqslant B_r} \frac{1}{p^2} H_{\mathrm{dg}}^2(r^2-4p)$ is a constant depending on r. It follows that

$$\begin{aligned} & \lim_{x\to\infty} \frac{\sum_{p\leqslant x} \frac{1}{p^2} H_{\mathrm{dg}}^2(r^2-4p)}{\frac{K(r)}{\pi^2}\log\log x} \\ = \; & \lim_{x\to\infty} \frac{\sum_{p\leqslant B_r} \frac{1}{p^2} H_{\mathrm{dg}}^2(r^2-4p)}{\frac{K(r)}{\pi^2}\log\log x} + \lim_{x\to\infty} \frac{\sum_{B_r\leqslant p\leqslant x} \frac{1}{p^2} H_{\mathrm{dg}}^2(r^2-4p)}{\frac{K(r)}{\pi^2}\log\log x} \\ = \; & 0+1 \\ = \; & 1. \end{aligned}$$

Q.E.D. Theorem 1

4.1 An Expression for $L(1, \chi_{d_1})L(1, \chi_{d_2})$

In order to prove Proposition 4.1 we need an expression for $L^2(1, \chi_d)$. We obtain an expression for $L^2(1, \chi_d)$ using contour integration. Notice that the fundamental difference between the methods found in David's and Pappalardi's paper [DP99] and our methods is an estimate for the product $L^2(1, \chi_d)$ using contour integration. This estimate seems necessary as using the Pólya–Vinogradov inequality (lemma 2.14) as in [DP99] does not suffice. In fact, in lemma 4.1, we obtain a more general expression for $L(1, \chi_{d_1})L(1, \chi_{d_2})$, where $\chi_{d_i}, i = 1, 2$ are non–trivial Dirichlet characters, because in our proof in progress of the average Lang–Trotter conjecture for 2 elliptic curves the more general expression is used.

Lemma 4.1 *Given $\epsilon > 0$, $\chi_{d_i} = \left(\frac{d_i}{n}\right), i = 1, 2$ non-trivial*[3] *Dirichlet characters, $a_{d_1,d_2}(n) = \sum_{\delta e = n} \left(\frac{d_1}{\delta}\right)\left(\frac{d_2}{e}\right)$, for $U > 1$,*

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

In particular, given $\epsilon_1 > 0$, for $d_1 = d_2 = d$, and $U > 1$,

$$L^2(1, \chi_d) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{d(n)}{n} e^{-\frac{n}{U}} + O_{\epsilon_1}\left(\frac{|d|^{3/8+\epsilon_1}}{U^{1/2}}\right).$$

Proof of Lemma 4.1 Let $s = \sigma + it \in \mathbb{C}$. By definition,

$$L(s) \overset{\text{def}}{=} L(s, \chi_{d_1})L(s, \chi_{d_2}) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{\delta e = n} \left(\frac{d_1}{\delta}\right)\left(\frac{d_2}{e}\right) \overset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{a_{d_1,d_2}(n)}{n^s}.$$

[3] The term $L(s, \chi_0)$, where χ_0 corresponds to the trivial character, differs only slightly from the Riemann ζ-function, $\zeta(s)$. Since $\chi_0(p) = 1$ for $(p, d) = 1$ and $\chi_0(p) = 0$ for $(p, d) > 1$, then $L(s, \chi_0) = \left(\prod_{p|d} \frac{1}{1-p^{-s}}\right)^{-1} \zeta(s)$. However, $\zeta(s)$ has a simple pole at $s = 1$. See [BŠ66], pg. 330.

Following Barban[4] for $U > 1$, we consider

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

By lemma 2.10, $\int_{-\infty}^{\infty}\Gamma(1+it)|dt < \infty$, so we can apply lemma 2.8 in order to interchange the sum and the integral. It follows that

$$\begin{aligned}&\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\sum_{n=1}^{\infty}\frac{a_{d_1,d_2}(n)}{n}\Gamma(s-1)\left(\frac{U}{n}\right)^{s-1}ds\\ &= \sum_{n=1}^{\infty}\frac{a_{d_1,d_2}(n)}{n}\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\Gamma(s-1)\left(\frac{U}{n}\right)^{s-1}ds.\end{aligned}$$

Recall that $\Gamma(s')$ is regular in the entire complex plane except for simple poles at $s' = 0, -1, -2, \ldots$, and for[5] $c > 0, x > 0$,

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\Gamma(s')x^{s'}ds' = e^{-\frac{1}{x}}.$$

Let $s = s' + 1, ds = ds'$. Then,

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\Gamma(s-1)\left(\frac{U}{n}\right)^{s-1}ds = \frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\Gamma(s')\left(\frac{U}{n}\right)^{s'}ds' = e^{-\frac{n}{U}}.$$

Hence,

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

For any $T > 1$, let $R_{1/2,2,\pm iT}$ denote the boundary of the rectangle with vertices $1/2 \pm iT, 2 \pm iT$ in the complex plane. Since $(s-1)\Gamma(s-1) = \Gamma(s)$, and $L(s,\chi_d)$ is an analytic function[6] of s for all $s \in \mathbb{C}$ whenever χ_d is non-trivial, the only pole of

$$L(s)\Gamma(s-1)U^{s-1} = L(s)\frac{\Gamma(s)}{s-1}U^{s-1},$$

[4] See [Bar66], section 5. Note that $L(s)$ is absolutely convergent for $\sigma > 1$ and so uniformly convergent for $\sigma > 1$ by comparison with $|L(s)| \leqslant \sum_{n=1}^{\infty}\frac{d(n)}{n^{\sigma}} = \zeta^2(\sigma)$. Furthermore, $\Gamma(s) \overset{\text{def}}{=} \int_0^{\infty} e^{-t}t^{s-1}dt$ is absolutely convergent for $\sigma > 0$, so that $\Gamma(s-1)$ is absolutely convergent for $\sigma > 1$.

[5] See [KM84], pg. 82 and 83.

[6] See [Dav80], pg. 11.

inside $R_{1/2,2,\pm iT}$ is a simple pole at $s = 1$. Thus, by Cauchy's residue theorem[7],

$$Res_{s=1}L(s)\Gamma(s-1)U^{s-1} = \frac{1}{2\pi i}\int_{R_{1/2,2,\pm iT}} L(s)\Gamma(s-1)U^{s-1}ds.$$

Observe at $s = 1$, $L(s) = L(1)$,

$$Res_{s=1}\Gamma(s-1) = \lim_{s\to 1}(s+1)\frac{\Gamma(s)}{s+1} = \Gamma(1) = 1,$$

and $Res_{s=1}U^{s-1} = 1$, so that we may write

$$L(1) = \frac{1}{2\pi i}\left\{\int_{2-iT}^{2+iT} + \int_{2+iT}^{1/2+iT} + \int_{1/2+iT}^{1/2-iT} + \int_{1/2-iT}^{2-iT}\right\} L(s)\Gamma(s-1)U^{s-1}ds.$$

Notice

$$\begin{aligned}
&\left|\frac{1}{2\pi i}\int_{1/2-iT}^{2-iT} L(s)\Gamma(s-1)U^{s-1}ds\right| \\
&= \frac{1}{2\pi}\left|\int_{1/2}^{2} L(\sigma+iT)\Gamma(\sigma-1+iT)U^{\sigma-1+iT}d\sigma\right| \\
&\leqslant \frac{1}{2\pi}\int_{1/2}^{2} |L(\sigma+iT)|\,|\Gamma(\sigma-1+iT)|U^{\sigma-1}d\sigma,
\end{aligned}$$

and by lemma 2.18, for any $\sigma > 0$,

$$L(\sigma+iT) \ll \sqrt{|d_1d_2|}\log|d_1|\log|d_2|\frac{\sqrt{\sigma^2+T^2}}{\sigma}.$$

Also, by Stirling's lemma 2.9 we have

$$|\Gamma(\sigma-1+iT)| = \sqrt{2\pi}e^{-1/2\pi T}T^{\sigma-3/2}\{1+r(\sigma-1,T)\}.$$

Note if $T > 1, U > 1$, and $1/2 \leqslant \sigma \leqslant 2$, then $U^{\sigma-1} \leqslant U$, $T^{\sigma-3/2} \leqslant T^{1/2}$, and $\frac{\sqrt{\sigma^2+T^2}}{\sigma} \leqslant \sqrt{1+4T^2}$. It follows that

$$\frac{1}{2\pi i}\int_{1/2-iT}^{2-iT} L(s)\Gamma(s-1)U^{s-1}ds$$

[7] See [Tit78], pg 102.

$$\ll \sqrt{|d_1d_2|}\log|d_1|\log|d_2|\int_{1/2}^{2}\frac{\sqrt{\sigma^2+T^2}}{\sigma}e^{-1/2\pi T}T^{\sigma-3/2}\{1+r(\sigma-1,T)\}U^{\sigma-1}d\sigma$$
$$\ll \sqrt{|d_1d_2|}\log|d_1|\log|d_2|e^{-1/2\pi T}U\sqrt{T+4T^3}\left(1+\int_{1/2}^{2}r(\sigma-1,T)d\sigma\right).$$

Furthermore, note that the same bound is realized by the integral from $2+iT$ to $1/2+iT$. Letting $T\to\infty$, we deduce

$$\frac{1}{2\pi i}\int_{1/2-i\infty}^{2-i\infty}L(s)\Gamma(s-1)U^{s-1}ds=0,$$

and

$$\frac{1}{2\pi i}\int_{2+i\infty}^{1/2+i\infty}L(s)\Gamma(s-1)U^{s-1}ds=0.$$

Now we consider,

$$\left|\frac{1}{2\pi i}\int_{1/2+iT}^{1/2-iT}L(s)\Gamma(s-1)U^{s-1}ds\right|$$
$$=\frac{1}{2\pi}\left|\int_{1/2-iT}^{1/2+iT}L(s)\Gamma(s-1)U^{s-1}ds\right|$$
$$\leqslant U^{-1/2}\frac{1}{2\pi}\int_{-T}^{T}|L(1/2+it)||\Gamma(-1/2+it)|dt.$$

Again, by Stirling's lemma 2.9, we know that

$$|\Gamma(-1/2+it)|=\sqrt{2\pi}e^{-1/2\pi|t|}|t|^{-1}\{1+r(-1/2,t)\}.$$

Since $r(-1/2,t)\to 0$ as $|t|\to\infty$, there exists a $k\in\mathbb{N}$ such that

$$\sqrt{2\pi}(1+r(-1/2,t))\leqslant k.$$

Moreover, by Burgess's result[8] on character sums and Dirichlet series, we have for any $\epsilon>0$,

$$L(1/2+it,\chi_d)\ll_{\epsilon/2}|t||d|^{3/16+\epsilon/2},$$

[8] See [Bur63].

so that

$$L(1/2+it) = L(1/2+it,\chi_{d_1})L(1/2+it,\chi_{d_2}) \ll_\epsilon |t|^2|d_1d_2|^{3/16+\epsilon}.$$

We write $\int_{-T}^{T}$ as $\left\{\int_{-T}^{-1}+\int_{-1}^{0}+\int_{0}^{1}+\int_{1}^{T}\right\}$ since $T>1$ and by Stirling's lemma 2.9, $|\Gamma(-1/2+it)|$ has a discontinuity at $T=0$. It follows that

$$\begin{aligned} &U^{-\frac{1}{2}}\frac{1}{2\pi}\int_{-T}^{T}|L(1/2+it)||\Gamma(-1/2+it)|dt \\ &\ll_\epsilon \frac{|d_1d_2|^{3/16+\epsilon}}{U^{1/2}}\left\{\int_{-T}^{-1}+\int_{-1}^{0}+\int_{0}^{1}+\int_{1}^{T}\right\}|t|e^{-1/2\pi|t|}dt. \end{aligned}$$

Let $g(t) \overset{\text{def}}{=} |t|e^{-1/2\pi|t|}$. Integrating by parts we see

$$\int_1^T g(t)dt \ll \frac{T}{e^{1/2\pi T}}.$$

Since $g(t)=g(-t)$, the same bound is realized by $\int_{-T}^{-1} g(t)dt$. Moreover, by changing variables we see

$$\int_0^1 g(t)dt \ll \int_0^{\pi/2} e^{-t'}t'dt' \ll \int_0^\infty e^{-t'}t'dt' = \Gamma(2) = O(1).$$

Since $g(t)=g(-t)$, the same bound is realized by $\int_{-1}^{0} g(t)dt$. It follows that

$$\begin{aligned} &\frac{|d_1d_2|^{3/16+\epsilon}}{U^{1/2}}\left\{\int_{-T}^{-1}+\int_{-1}^{0}+\int_{0}^{1}+\int_{1}^{T}\right\}g(t)dt \\ &\ll \frac{|d_1d_2|^{3/16+\epsilon}}{U^{1/2}} + \frac{|d_1d_2|^{3/16+\epsilon}}{U^{1/2}}\frac{T}{e^{1/2\pi T}}. \end{aligned}$$

Letting $T\to\infty$, $\frac{T}{e^{1/2\pi T}}\to 0$, and we obtain for any $\epsilon>0$

$$\frac{1}{2\pi i}\int_{1/2+i\infty}^{1/2-i\infty} L(s)\Gamma(s-1)U^{s-1}ds = O_\epsilon\left(\frac{|d_1d_2|^{3/16+\epsilon}}{U^{1/2}}\right).$$

Q.E.D. Lemma 4.1

4.2 Proposition 1

This section should be read in conjunction with section 4.3. In addition, note that the notation **ET0i**, where i=1,2,3,4,5,6,7,8, means *error term* 1,2,3,4,5,6,7,8. These error terms are evaluated in subsections 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.3.7, and 4.3.8 respectively.

Proposition 4.1 *Fix an $r \in \mathbb{Z}$ of odd parity. Let $B_r \overset{\text{def}}{=} \max\{5, |r|+1, \frac{r^2}{4}\}$, χ_d LJK symbol, and*

$$S_f^r(B_r, x) \overset{\text{def}}{=} \{\, B_r \leqslant p \leqslant x \,:\, r^2 - 4p \equiv 0 \bmod f^2, f \in \mathbb{N}, d = \frac{r^2-4p}{f^2} \equiv 1 \bmod 4\,\}.$$

For any $0 < \epsilon < \frac{1}{12}, c > 6 - 3\epsilon,$

$$\sum_{f \leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p \in S_f^r(B_r,x)} L^2(1, \chi_d) \log p = K(r)x + O_{c,\epsilon,r}\left(\frac{x}{(\log x)^c}\right).$$

Proof of Proposition 4.1 By lemma 4.1, given an $\epsilon_1 > 0$, for $U > 1$,

$$L^2(1, \chi_d) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{d(n)}{n} e^{-\frac{n}{U}} + O_{\epsilon_1}\left(\frac{|d|^{3/8+\epsilon_1}}{U^{1/2}}\right).$$

This means we can write,

$$\sum_{f \leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p \in S_f^r(B_r,x)} L^2(1, \chi_d) \log p,$$

as

$$\sum_{\substack{f \leqslant 2\sqrt{x} \\ (2r,f)=1}} \frac{1}{f^2} \sum_{p \in S_f^r(B_r,x)} \left\{ \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{d(n)}{n} e^{-\frac{n}{U}} + O_{\epsilon_1}\left(\frac{|d|^{3/8+\epsilon_1}}{U^{1/2}}\right) \right\} \log p.$$

Let

$$\mathbf{ET01} \overset{\text{def}}{=} \frac{1}{U^{1/2}} \sum_{\substack{f \leqslant 2\sqrt{x} \\ (2r,f)=1}} \frac{1}{f^2} \sum_{p \in S_f^r(B_r,x)} |d|^{3/8+\epsilon_1} \log p.$$

We evaluate **ET01** in subsection 4.3.1, showing that $\mathbf{ET01} = O_{r,\epsilon_1}\left(\frac{x^{11/8+\epsilon_1}}{U^{1/2}}\right)$. It follows that

$$\sum_{f \leqslant 2\sqrt{x}} \frac{1}{f^2} \sum_{p \in S_f^r(B_r,x)} L^2(1,\chi_d) \log p$$

$$= \sum_{\substack{f \leqslant 2\sqrt{x} \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n=1}^{\infty} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{p \in S_f^r(B_r,x)} \left(\frac{d}{n}\right) \log p + \mathbf{ET01}.$$

Let $1 < V \leqslant 2\sqrt{x}$ be a parameter to be chosen later,

$$\mathbf{ET02} \stackrel{\text{def}}{=} \sum_{\substack{V < f \leqslant 2\sqrt{x} \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n=1}^{\infty} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{p \in S_f^r(B_r,x)} \left(\frac{d}{n}\right) \log p,$$

$$\mathbf{ET03} \stackrel{\text{def}}{=} \sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{p \in S_f^r(B_r,x)} \left(\frac{d}{n}\right) \log p.$$

We cut off the f sum at V, and the n sum at $U \log U^2$ because of lemma 2.13, which we use to evaluate **ET03**. We evaluate the error terms **ET02** and **ET03** in subsections 4.3.2 and 4.3.3, where we show that $\mathbf{ET02} = O\left(\frac{x \log x (\log U)^2}{V^3}\right)$, and $\mathbf{ET03} = O_{\delta_1}\left(\frac{x}{U}\right)$. Then, for any $0 < \delta_1 \leqslant 1$,

$$\sum_{\substack{f \leqslant 2\sqrt{x} \\ (2r,f)=1}} \frac{1}{f^2} \sum_{p \in S_f^r(B_r,x)} L^2(1,\chi_d) \log p$$

$$= \sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n \leqslant U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{p \in S_f^r(B_r,x)} \left(\frac{d}{n}\right) \log p + \mathbf{ET01} + \mathbf{ET02} + \mathbf{ET03}.$$

Now we evaluate the sum over "small" values of f and n by splitting the sum according to the residue of d mod $4n$. By the equivalent formulation of *Gauss's law of quadratic reciprocity*[9],

$$d \equiv a \bmod 4n \Rightarrow \left(\frac{d}{n}\right) = \left(\frac{a}{n}\right) \quad \text{for } n \in \mathbb{N}.$$

[9] See introductory subsection 3.6.2.

Since $\left(\frac{a}{n}\right) = 0$ when[10] $(a, n) > 1$, and the conditions

$$p \in S_f^r(B_r, x) \text{ and } d = \frac{r^2 - 4p}{f^2} \equiv a \bmod 4n,$$

are equivalent to the conditions

$$B_r \leqslant p \leqslant x, \text{ and } p \equiv \frac{r^2 - af^2}{4} \bmod nf^2,$$

it follows that

$$\begin{aligned} &\sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n \leqslant U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{p \in S_f^r(B_r, x)} \left(\frac{d}{n}\right) \log p \\ \overset{\text{con}}{=} &\sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n \leqslant U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \sum_{\substack{p \in S_f^r(B_r, x) \\ d \equiv a \bmod 4n}} \log p \\ = &\sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n \leqslant U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \sum_{\substack{B_r \leqslant p \leqslant x \\ p \equiv \frac{r^2 - af^2}{4} \bmod nf^2}} \log p. \end{aligned}$$

Since we are summing over a complete set of invertable residues mod $4n$, we note that the convention is the sum expression is zero when it is empty. A necessary[11] condition for p to be in the arithmetic progression $\frac{r^2 - af^2}{4} \bmod nf^2$, is that

$$\begin{aligned} &\left(\frac{r^2 - af^2}{4}, nf^2\right) = 1 \\ \Leftrightarrow \quad &\text{there exists } z_1, z_2 \in \mathbb{Z} \text{ such that } \left(\frac{r^2 - af^2}{4}\right) z_1 + nf^2 z_2 = 1 \\ \Leftrightarrow \quad &(r^2 - af^2) z_1 + 4nf^2 z_2 = 4 \\ \Leftrightarrow \quad &\text{For some } k \in \mathbb{Z}, (r^2 - af^2, 4n) = (4(p + nf^2 k), 4n) = 4. \end{aligned}$$

By Dirichlet's Theorem (lemma 2.4), we have

$$\sum_{\substack{p \leqslant x \\ p \equiv \frac{r^2 - af^2}{4} \bmod nf^2}} \log p = \frac{x}{\phi(nf^2)} + E_1(x; nf^2, \frac{r^2 - af^2}{4}),$$

[10] See introductory subsection 3.6.1.

[11] Consider the arithmetic progression $a + kq, k \in \mathbb{N}$. If $(a, q) = d > 1$, then there is no prime in this progression. That is, $a + kq = d\left(\frac{a}{d} + k\frac{q}{d}\right)$ is a composite number.

where $E_1(x; nf^2, \frac{r^2-af^2}{4}) = o(x)$. Respecting David's and Pappalardi's notation we define

$$c_f^r(n) \overset{\text{def}}{=} \sum_{\substack{a \bmod 4n \\ (r^2-af^2,4n)=4}} \left(\frac{a}{n}\right).$$

Let

$$\mathbf{ET04} \overset{\text{def}}{=} \sum_{f\leqslant V} \frac{1}{f^2} \sum_{n \leqslant U\log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \sum_{\substack{p<B_r \\ p\equiv \frac{r^2-af^2}{4} \bmod nf^2}} \log p,$$

$$\mathbf{ET05} \overset{\text{def}}{=} \sum_{\substack{f\leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n \leqslant U\log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{\substack{a \bmod 4n \\ (r^2-af^2,4n)=4}} \left(\frac{a}{n}\right) E_1(x; nf^2, \frac{r^2-af^2}{4}).$$

In subsection 4.3.4 we show that

$$\mathbf{ET04} = O_r\left(U(\log U)^2\right),$$

while in subsection 4.3.5, using Mongomery's [Mon71] result on the Barban–Davenport–Halberstam Theorem (lemma 2.5), we show that the *main error term*

$$\mathbf{ET05} = O\left((\log U)^{\frac{5}{2}}(UV^2(\log U^2)x\log x)^{\frac{1}{2}}\right),$$

whenever $\frac{x}{(\log x)^A} \leqslant UV^2 \log U^2 \leqslant x$, for any $A>0$. It follows that[12]

$$\begin{aligned}
&\sum_{\substack{f\leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n \leqslant U\log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \sum_{\substack{B_r\leqslant p\leqslant x \\ p\equiv \frac{r^2-af^2}{4} \bmod nf^2}} \log p \\
&= \sum_{\substack{f\leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n \leqslant U\log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \\
&\times \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \left\{ \sum_{\substack{p\leqslant x \\ p\equiv \frac{r^2-af^2}{4} \bmod nf^2}} \log p - \sum_{\substack{p<B_r \\ p\equiv \frac{r^2-af^2}{4} \bmod nf^2}} \log p \right\}
\end{aligned}$$

[12] Notice if we defined

$$\psi(x; n, a) \overset{\text{def}}{=} \sum_{\substack{B_r\leqslant p\leqslant x \\ p\equiv a \bmod n}} \log p,$$

then the same result would hold as this differs from the previous definition (see lemma 2.4) by only a constant. This way we would not have to carry the B_r everywhere.

$$\begin{aligned}
&= \sum_{\substack{f\leqslant V\\(2r,f)=1}} \frac{1}{f^2} \sum_{n\leqslant U\log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \sum_{\substack{p\leqslant x\\ p\equiv\frac{r^2-af^2}{4} \bmod nf^2}} \log p + \ \mathbf{ET04}\\
&= \sum_{\substack{f\leqslant V\\(2r,f)=1}} \frac{1}{f^2} \sum_{n\leqslant U\log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}}\\
&\times \sum_{\substack{a \bmod 4n\\(r^2-af^2,4n)=4}} \left(\frac{a}{n}\right) \left\{ \frac{x}{\phi(nf^2)} + E_1(x; nf^2, \frac{r^2-af^2}{4}) \right\} + \mathbf{ET04}\\
&= x \sum_{\substack{f\leqslant V\\(2r,f)=1}} \frac{1}{f^2} \sum_{n\leqslant U\log U^2} \frac{d(n)}{n\phi(nf^2)} e^{-\frac{n}{U}} \sum_{\substack{a \bmod 4n\\(r^2-af^2,4n)=4}} \left(\frac{a}{n}\right) + \mathbf{ET04}\\
&+ \sum_{\substack{f\leqslant V\\(2r,f)=1}} \frac{1}{f^2} \sum_{n\leqslant U\log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{\substack{a \bmod 4n\\(r^2-af^2,4n)=4}} \left(\frac{a}{n}\right) E_1(x; nf^2, \frac{r^2-af^2}{4})\\
&= x \sum_{\substack{f\leqslant V\\(2r,f)=1}} \sum_{n\leqslant U\log U^2} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}} + \mathbf{ET04} + \mathbf{ET05}.
\end{aligned}$$

Let

$$\begin{aligned}
\mathbf{ET06} &\overset{\text{def}}{=} -x \sum_{\substack{f\leqslant V\\(2r,f)=1}} \sum_{n>U\log U^2} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}},\\
\mathbf{ET07} &\overset{\text{def}}{=} -x \sum_{\substack{f> V\\(2r,f)=1}} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}},\\
\mathbf{ET08} &\overset{\text{def}}{=} x \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}}.
\end{aligned}$$

In subsections 4.3.6, 4.3.7, and 4.3.8, we show that for any $0 < \delta_2 < \frac{1}{2}$, $0 < \delta_3 + \epsilon_2 < \frac{1}{2}$, $\mathbf{ET06} = O_{\delta_2}\left(\frac{x}{(U\log U^2)^{1/2-\delta_2}}\right)$, $\mathbf{ET07} = O\left(\frac{x}{V^2}\right)$, and $\mathbf{ET08} = O_{\delta_3,\epsilon_2}\left(\frac{x}{U^{\epsilon_2}}\right)$.

Continuing , we re-write the finite sums over n and f as infinite sums and remove the exponential $e^{-\frac{n}{U}}$ as it depends on the parameter U. If follows that for any $0 < \delta_2 < \frac{1}{2}$, $0 < \delta_3 + \epsilon_2 < \frac{1}{2}$,

$$x \sum_{\substack{f\leqslant V\\(2r,f)=1}} \sum_{n\leqslant U\log U^2} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}} = x \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} + \mathbf{ET06} + \mathbf{ET07} + \mathbf{ET08}.$$

To this point we have shown

$$\begin{aligned}
&\sum_{\substack{f\leqslant 2\sqrt{x}\\(2r,f)=1}} \frac{1}{f^2} \sum_{p\in S_f^r(x)} L^2(1,\chi_d)\log p \\
&= x \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} + \sum_{i\leqslant 8} \mathbf{ET0i}.
\end{aligned}$$

By subsection 4.3.9, for any $0<\epsilon<\frac{1}{12}, c>6-3\epsilon$, we have that

$$\begin{aligned}
\mathbf{ET} &= \sum_{i\leqslant 8} \mathbf{ET0i} \\
&= O_{c,\epsilon,r}\left(\frac{x}{(\log x)^c}\right).
\end{aligned}$$

Q.E.D. Proposition 4.1

4.3 The Error Term ET

4.3.1 On ET01

Notice

$$|d| = \frac{4p-r^2}{f^2},$$

$$\sum_{\substack{f\leqslant 2\sqrt{x}\\(2r,f)=1}} \frac{1}{f^{2+3/4+2\epsilon_1}\phi(f^2)} \ll \sum_{f\leqslant 2\sqrt{x}} \frac{1}{f^2} \ll \int_1^{2\sqrt{x}} t^{-2}dt \ll 1,$$

and by the prime number theorem for arithmetic progressions,

$$\sum_{\substack{p\leqslant x\\ 4p\equiv r^2 \bmod f^2}} \log p \sim \frac{x}{\phi(f^2)}.$$

Hence,

$$\begin{aligned}
&\frac{1}{U^{1/2}} \sum_{\substack{f\leqslant 2\sqrt{x}\\(2r,f)=1}} \frac{1}{f^2} \sum_{p\in S_f^r(B_r,x)} |d|^{3/8+\epsilon_1}\log p \\
\ll_r\ & \frac{1}{U^{1/2}} \sum_{\substack{f\leqslant 2\sqrt{x}\\(2r,f)=1}} \frac{1}{f^{2+3/4+2\epsilon_1}} \sum_{\substack{p\leqslant x\\ 4p\equiv r^2 \bmod f^2}} p^{3/8+\epsilon_1}\log p
\end{aligned}$$

$$\begin{aligned} &\ll \frac{x^{3/8+\epsilon_1}}{U^{1/2}} \sum_{\substack{f\leqslant 2\sqrt{x}\\(2r,f)=1}} \frac{1}{f^{2+3/4+2\epsilon_1}} \sum_{\substack{p\leqslant x\\4p\equiv r^2 \bmod f^2}} \log p \\ &\ll \frac{x^{11/8+\epsilon_1}}{U^{1/2}}. \end{aligned}$$

That is,

$$\mathbf{ET01} = O_{r,\epsilon_1}\left(\frac{x^{11/8+\epsilon_1}}{U^{1/2}}\right).$$

4.3.2 On ET02

Since

$$\sum_{\substack{n\in\mathrm{N}, n\leqslant x\\4n\equiv r^2 \bmod f^2}} 1 = \sum_{\substack{k\in\mathrm{N}\\k\leqslant \frac{4x-r^2}{f^2}}} 1 \ll \frac{x}{f^2},$$

$$\sum_{V<f\leqslant 2\sqrt{x}} \frac{1}{f^4} \ll \int_V^{2\sqrt{x}} t^{-4}dt \ll \frac{1}{V^3},$$

and by lemma 2.12,

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

therefore

$$\begin{aligned} &\sum_{\substack{V<f\leqslant 2\sqrt{x}\\(2r,f)=1}} \frac{1}{f^2} \sum_{n=1}^{\infty} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{p\in S_f^r(B_r,x)} \left(\frac{d}{n}\right) \log p \\ \ll &\sum_{\substack{V<f\leqslant 2\sqrt{x}\\(2r,f)=1}} \frac{1}{f^2} \left| \sum_{n=1}^{\infty} \frac{d(n)}{n} e^{-\frac{n}{U}} \right| \sum_{\substack{p\leqslant x\\4p\equiv r^2 \bmod f^2}} \log p \\ \ll &\log x \sum_{V<f\leqslant 2\sqrt{x}} \frac{1}{f^2} \left| \sum_{n=1}^{\infty} \frac{d(n)}{n} e^{-\frac{n}{U}} \right| \sum_{\substack{n\in\mathrm{N}, n\leqslant x\\4n\equiv r^2 \bmod f^2}} 1 \\ \ll &\frac{x\log x(\log U)^2}{V^3}. \end{aligned}$$

That is,

$$\mathbf{ET02} = O\left(\frac{x\log x(\log U)^2}{V^3}\right).$$

4.3.3 On ET03

$$\begin{aligned}
&\sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{p \in S_f^r(B_r, x)} \left(\frac{d}{n}\right) \log p \\
\ll \;& \sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \left| \sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \right| \sum_{\substack{p \leqslant x \\ 4p \equiv r^2 \bmod f^2}} \log p \\
\ll \;& x \left| \sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \right| \sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2 \phi(f^2)} \\
\ll \;& x \left| \sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \right|,
\end{aligned}$$

and by lemma 2.13, for any $0 < \delta_1 \leqslant 1$,

$$\sum_{n > U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \ll_{\delta_1} \frac{1}{U}.$$

That is,

$$\mathbf{ET03} = O_{\delta_1}\left(\frac{x}{U}\right).$$

4.3.4 On ET04

Notice

$$\sum_{\substack{p < B_r \\ p \equiv \frac{r^2 - af^2}{4} \bmod nf^2}} \log p,$$

is a constant depending only on r. For $n \geqslant 1$, $U > 1$,

$$\begin{aligned}
|e^{-\frac{n}{U}}| &\leqslant |e^{-\frac{1}{U}}| \\
&= \left|1 - \frac{1}{U} + \frac{1}{U^2 2!} - \frac{1}{U^3 3!} + \ldots\right| \\
&\leqslant 1 + \frac{1}{U} + \frac{1}{U^2 2!} + \frac{1}{U^3 3!} + \ldots \\
&< 1 + (1 + \frac{1}{2!} + \frac{1}{3!} + \ldots).
\end{aligned}$$

Since $n! \geqslant 2^{n-1}$, therefore $\sum_{n=1}^{\infty} \frac{1}{n!} \leqslant \sum_{n=1}^{\infty} \frac{1}{2^{n-1}} = 2$, so that $|e^{-\frac{n}{U}}| < 3$. Moreover,

$$\left| \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \right| \leqslant \phi(4n) \ll n,$$

and by lemma 2.6, part 3,

$$\sum_{n \leqslant x} d(n) = x \log x + O(x),$$

so that we have

$$\begin{aligned}
& \sum_{f \leqslant V} \frac{1}{f^2} \sum_{n \leqslant U \log U^2} \frac{d(n)}{n} e^{-\frac{n}{U}} \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \sum_{\substack{p < B_r \\ p \equiv \frac{r^2 - af^2}{4} \bmod nf^2}} \log p \\
\ll_r \; & \sum_{f \leqslant V} \frac{1}{f^2} \sum_{n \leqslant U \log U^2} \frac{d(n)}{n} |e^{-\frac{n}{U}}| \left| \sum_{a \bmod 4n} \left(\frac{a}{n}\right) \right| \\
\ll \; & \sum_{n \leqslant U \log U^2} d(n) \\
\ll \; & U (\log U)^2.
\end{aligned}$$

That is,

$$\mathbf{ET04} = O_r\left(U (\log U)^2\right).$$

4.3.5 On ET05

We begin by introducing new notation.

Definition We write $a \pmod{c}^*$ to mean $a \bmod c$, $(a, c) = 1$.

Definition We write $a \equiv b \pmod{c}^*$ to mean $a = b + cz, z \in \mathbb{Z}, (a, c) = (b, c) = 1$.

By the Cauchy-Schwarz inequality, recall for $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{R}$,

$$\sum_{i \leqslant n} x_i y_i \leqslant \left(\sum_{i \leqslant n} {x_i}^2\right)^{\frac{1}{2}} \left(\sum_{i \leqslant n} {y_i}^2\right)^{\frac{1}{2}},$$

we have that

$$\left|\sum_{\substack{f\leqslant V\\(2r,f)=1}}\frac{1}{f^2}\sum_{n\leqslant U\log U^2}\frac{d(n)}{n}e^{-\frac{n}{U}}\sum_{\substack{a \bmod 4n\\(r^2-af^2,4n)=4}}\left(\frac{a}{n}\right)E_1(x;nf^2,\frac{r^2-af^2}{4})\right|$$

$$\leqslant 3\sum_{\substack{f\leqslant V\\(2r,f)=1}}\frac{1}{f^2}\sum_{\substack{n\leqslant U\log U^2\\a\pmod{4n}^*\\(r^2-af^2,4n)=4}}\frac{d(n)}{n}|E_1(x;nf^2,\frac{r^2-af^2}{4})|$$

$$\leqslant 3\sum_{\substack{f\leqslant V\\(2r,f)=1}}\frac{1}{f^2}\left(\sum_{\substack{n\leqslant U\log U^2\\a\pmod{4n}^*\\(r^2-af^2,4n)=4}}\frac{d^2(n)}{n^2}\right)^{\frac{1}{2}}\left(\sum_{\substack{n\leqslant U\log U^2\\a\pmod{4n}^*\\(r^2-af^2,4n)=4}}E_1^2(x;nf^2,\frac{r^2-af^2}{4})\right)^{\frac{1}{2}}.$$

Since[13]

$$\sum_{n\leqslant x}d^2(n)=O(x(\log x)^3),$$

by partial summation lemma 2.1 we obtain[14]

$$\sum_{n\leqslant U\log U^2}\frac{d^2(n)}{n}\ll(\log U)^5.$$

It follows that

$$\left(\sum_{\substack{n\leqslant U\log U^2\\a\pmod{4n}^*\\(r^2-af^2,4n)=4}}\frac{d^2(n)}{n^2}\right)^{\frac{1}{2}}\ll\left(\sum_{n\leqslant U\log U^2}\frac{d^2(n)}{n}\right)^{\frac{1}{2}}\ll(\log U)^{\frac{5}{2}}.$$

We now consider,

$$\sum_{\substack{f\leqslant V\\(2r,f)=1}}\frac{1}{f^2}\left(\sum_{\substack{n\leqslant U\log U^2\\a\pmod{4n}^*\\(r^2-af^2,4n)=4}}E_1^2(x;nf^2,\frac{r^2-af^2}{4})\right)^{\frac{1}{2}}.$$

[13] $\sum_{n\leqslant x}d^r(n)=x(A_1(\log x)^{2^r-1}+A_2(\log x)^{2^r-2}+\ldots+A_{2^r})+O\left(x^{(2^r-1)/(2^r+2)+\epsilon}\right)$ for $r\geqslant 2$, and $A_1,\ldots,A_{2^r}$ constants. See [Wil22] for a proof.

[14] We note that Ramanujan proved $\sum_{n=1}^{\infty}\frac{d^2(n)}{n^s}=\frac{\zeta^4(s)}{\zeta(2s)}$ (see [HW64], pg. 256), and since $\sum_{n=1}^{\infty}\frac{d^2(n)}{n}e^{-\frac{n}{U}}=\frac{1}{2\pi i}\int_{(c)}\frac{\zeta^4(s)}{\zeta(2s)}\Gamma(s)\frac{U^{s-1}}{s-1}ds$, and $\zeta^4(s)$ has a quadruple pole at $s=1$, we may use Cauchy's residue theorem to deduce an asymptotic formula for $\sum_{n=1}^{\infty}\frac{d^2(n)}{n}e^{-\frac{n}{U}}$, which gives a precise upper bound on $\sum_{n\leqslant U\log U^2}\frac{d^2(n)}{n}$.

Let $b = \frac{r^2-af^2}{4}$ and $b' = \frac{r^2-a'f^2}{4}$. Notice

$$b \equiv b' \pmod{nf^2}^* \Rightarrow a \equiv a' \pmod{4n}^*.$$

It follows that,

$$\sum_{\substack{n \leqslant U \log U^2 \\ a \pmod{4n)^*} \\ (r^2-af^2,4n)=4}} E_1^2(x; nf^2, \frac{r^2-af^2}{4}) \leqslant \sum_{\substack{n \leqslant U \log U^2 \\ b \pmod{nf^2)^*}}} E_1^2(x, nf^2, b).$$

Notice

$$\sum_{\substack{n \leqslant U \log U^2 \\ b \pmod{nf^2)^*}}} E_1^2(x, nf^2, b) \leqslant \sum_{\substack{m \leqslant Uf^2 \log U^2 \\ b \pmod{m)^*}}} E_1^2(x; m, b),$$

which implies

$$\sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \left(\sum_{\substack{n \leqslant U \log U^2 \\ a \pmod{4n)^*} \\ (r^2-af^2,4n)=4}} E_1^2(x; nf^2, \frac{r^2-af^2}{4}) \right)^{\frac{1}{2}}$$

$$\leqslant \sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^2} \left(\sum_{\substack{m \leqslant Uf^2 \log U^2 \\ b \pmod{m)^*}}} E_1^2(x; m, b) \right)^{\frac{1}{2}}$$

$$\ll \left(\sum_{\substack{m \leqslant UV^2 \log U^2 \\ b \pmod{m)^*}}} E_1^2(x; m, b) \right)^{\frac{1}{2}}.$$

Recall the result of Montgomery on the *Barban–Davenport–Halberstam theorem* (lemma 2.5); for $\frac{x}{(\log x)^A} \leqslant Q \leqslant x, A > 0$,

$$\sum_{k \leqslant Q} \sum_{\substack{1 \leqslant a \leqslant k \\ (a,k)=1}} E_1^2(x; k, a) \ll Qx \log x.$$

Consequently,

$$\left(\sum_{\substack{m \leqslant UV^2 \log U^2 \\ b \pmod{m)^*}}} E_1^2(x; m, b) \right)^{\frac{1}{2}} \ll (UV^2(\log U^2)x \log x)^{\frac{1}{2}},$$

whenever $\frac{x}{(\log x)^A} \leqslant UV^2 \log U^2 \leqslant x$, for any $A > 0$. That is,

$$\mathbf{ET05} = O\left((\log U)^{\frac{5}{2}}(UV^2(\log U^2)x\log x)^{\frac{1}{2}}\right),$$

whenever $\frac{x}{(\log x)^A} \leqslant UV^2 \log U^2 \leqslant x$, for any $A > 0$.

4.3.6 On ET06

In order to evaluate error term six, we need to recall some lemmas from David's and Pappalardi's work. For fixed $r \in \mathbb{Z}, f, n \in \mathbb{N}$, we define

$$c_f^r(n) \overset{\text{def}}{=} \sum_{\substack{a \pmod{4n}^* \\ (r^2 - af^2, 4n) = 4}} \left(\frac{a}{n}\right),$$

where $a \pmod{4n}^*$ means a mod $4n$, $(a, 4n) = 1$, and for $n \in \mathbb{N}$, we define $\kappa(n)$ to be the smallest positive integer dividing n such that $\frac{n}{\kappa(n)}$ is a square.

Lemma 4.2 *The following hold,*

1. *If n is odd, $c_f^r(n) = \sum_{\substack{a \pmod{n}^* \\ (r^2 - af^2, n) = 1}} \left(\frac{a}{n}\right)$.*

2. *$c_f^r(n)$ is a multiplicative function of n.*

3. *For any prime p, $c_f^r(p^\alpha) = c_{(f,p)}^r(p^\alpha)$.*

4. *If $\alpha \geqslant 1$, $c_1^r(2^\alpha) = (-2)^\alpha/2$.*

5. *If p is an odd prime, then $c_1^r(p^\alpha)/p^{\alpha-1} = p - 1 - \left(\frac{r^2}{p}\right)$ if α is even, and $-\left(\frac{r^2}{p}\right)$ if α is odd.*

6. *If p is an odd prime $(p \nmid r)$, then $\frac{c_p^r(p^\alpha)}{p^{\alpha-1}}$ is equal to 0 if α is odd, and is equal to $p - 1$ if α is even.*

7. *For all* $n \in \mathbb{N}$, $|c_f^r(n)| \leqslant \frac{n}{\kappa(n)}$.

Proof See [DP99], lemma 3.3.

Lemma 4.3 *Let* $c = \prod_p \left(1 + \frac{1}{p(\sqrt{p}-1)}\right)$. *Then*

$$\sum_{n>U} \frac{1}{\kappa(n)\phi(n)} \sim \frac{c}{\sqrt{U}}.$$

In particular, $\sum_{n=1}^{\infty} \frac{1}{\kappa(n)\phi(n)}$ *converges.*

Proof See [DP99], lemma 3.4.

We are now ready to evaluate **ET06**. Notice by lemma 2.7, part 2,

$$\phi(nf^2) \geqslant \phi(n)\phi(f^2) = \phi(n)f\phi(f),$$

by lemma 4.2, part 7,

$$|c_f^r(n)| \leqslant \frac{n}{\kappa(n)},$$

and by lemma 2.6, part 2, for any $\delta_2 > 0$,

$$d(n) \ll_{\delta_2} n^{\delta_2}.$$

It follows that

$$\begin{aligned} -x \sum_{\substack{f \leqslant V \\ (2r,f)=1}} \sum_{n>U\log U^2} & \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}} \\ \ll \quad x & \sum_{\substack{f \leqslant V \\ (2r,f)=1}} \frac{1}{f^3\phi(f)} \sum_{n>U\log U^2} \frac{d(n)}{\kappa(n)\phi(n)} \\ \ll_{\delta_2} \quad x & \sum_{n>U\log U^2} \frac{n^{\delta_2}}{\kappa(n)\phi(n)}. \end{aligned}$$

We are now interested in obtaining an upper bound for $\sum_{n>U\log U^2}\frac{n^{\delta_2}}{\kappa(n)\phi(n)}$. Let $F(t)=\sum_{n\leqslant t}\frac{n^{3/2}}{\kappa(n)\phi(n)}$. We know[15]

$$F(t)\sim\frac{c}{2}t.$$

If follows by lemma 2.1,

$$\begin{aligned}&\sum_{U\log U^2<n\leqslant N}\frac{n^{\delta_2}}{\kappa(n)\phi(n)}\\ &=\sum_{n\leqslant N}\frac{n^{3/2}}{\kappa(n)\phi(n)}\frac{1}{n^{3/2-\delta_2}}-\sum_{n\leqslant U\log U^2}\frac{n^{3/2}}{\kappa(n)\phi(n)}\frac{1}{n^{3/2-\delta_2}}\\ &=\frac{F(N)}{N^{3/2-\delta_2}}-\frac{F(U)}{(U\log U^2)^{3/2-\delta_2}}+\left(\frac{3}{2}-\delta_2\right)\int_{U\log U^2}^{N}\frac{F(t)}{t^{5/2-\delta_2}}dt.\end{aligned}$$

Letting $N\to\infty$, we obtain for any $0<\delta_2<\frac{1}{2}$,

$$\sum_{n>U\log U^2}\frac{n^{\delta_2}}{\kappa(n)\phi(n)}\ll_{\delta_2}\frac{c}{(U\log U^2)^{1/2-\delta_2}}.$$

It now follows that for any $0<\delta_2<\frac{1}{2}$,

$$\mathbf{ET06}=O_{\delta_2}\left(\frac{x}{(U\log U^2)^{1/2-\delta_2}}\right).$$

4.3.7 On ET07

Observe

$$\sum_{n=1}^{\infty}\frac{d(n)}{\kappa(n)\phi(n)}=\left\{\sum_{n\leqslant 2e}+\sum_{n>2e}\right\}\frac{d(n)}{\kappa(n)\phi(n)}.$$

In subsection 4.3.6 we showed for any $U\geqslant 1$, $0<\delta_2<\frac{1}{2}$,

$$\sum_{n>U\log U^2}\frac{d(n)}{\kappa(n)\phi(n)}\ll_{\delta_2}\frac{c}{(U\log U^2)^{1/2-\delta_2}}.$$

[15] See proof of lemma 4.3.

In particular, for $U = e, U \log U^2 = 2e$, we have for any $0 < \delta_2 < \frac{1}{2}$,

$$\sum_{n>2e} \frac{d(n)}{\kappa(n)\phi(n)} \ll_{\delta_2} c.$$

Morever, since $\sum_{n=1}^{2e} \frac{d(n)}{\kappa(n)\phi(n)}$ is finite, therefore $\sum_{n=1}^{\infty} \frac{d(n)}{\kappa(n)\phi(n)}$ converges. It follows that

$$\begin{aligned} -x \sum_{\substack{f>V \\ (2r,f)=1}} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}} &\ll x \sum_{\substack{f>V \\ (2r,f)=1}} \frac{1}{f^3\phi(f)} \sum_{n=1}^{\infty} \frac{d(n)}{\kappa(n)\phi(n)} \\ &\ll x \sum_{\substack{f>V \\ (2r,f)=1}} \frac{1}{f^3} \\ &\ll x \lim_{T\to\infty} \int_V^T t^{-3} dt \\ &\ll \frac{x}{V^2}. \end{aligned}$$

That is,

$$\mathbf{ET07} = O\left(\frac{x}{V^2}\right).$$

4.3.8 On ET08

Here we remove the exponential $e^{-\frac{n}{U}}$ from the main term as it depends on U. Recall[16] for any $c_1 > 0$,

$$e^{-\frac{n}{U}} = \frac{1}{2\pi i} \int_{(c_1)} \Gamma(s) \left(\frac{U}{n}\right)^s ds.$$

It follows that

$$x \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}} = x \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} \frac{1}{2\pi i} \int_{(c_1)} \Gamma(s) \left(\frac{U}{n}\right)^s ds.$$

By lemma 4.2, part 7, and by lemma 2.6, part 2, for any $\delta_3 > 0$, $\delta_3 - \frac{1}{2} < \sigma < \delta_3$,

$$\left| \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{n^{s+1}f^2\phi(nf^2)} \right| \leqslant \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{|d(n)||c_f^r(n)|}{n^{\sigma+1}f^2\phi(nf^2)}$$

[16] For a proof see [KM84], pg. 82, 83.

$$\begin{aligned} &\ll_{\delta_3} \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \frac{1}{f^3\phi(f)} \sum_{n=1}^{\infty} \frac{n^{\delta_3}}{n^{\sigma}\kappa(n)\phi(n)} \\ &\ll_{\delta_3} 1. \end{aligned}$$

That is, $\sum_{\substack{f\geqslant 1\\(2r,f)=1}} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{n^{s+1}f^2\phi(nf^2)}$ converges absolutcly. Hence, by lemma 2.8, we may interchange the sum and the integral to obtain

$$x \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}} = x\frac{1}{2\pi i} \int_{(c_1)} \left(\sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{n^{s+1}f^2\phi(nf^2)} \right) \Gamma(s)U^s ds.$$

Note that in the proof of lemma 4.3, it is shown that

$$\sum_{n=1}^{\infty} \frac{n^{3/2-s}}{\kappa(n)\phi(n)} = \prod_p \left(1 + \frac{p(p^{s-3/2}+1)}{(p-1)(p^{2s-1}-1)}\right),$$

converges for $\sigma > 1$. More precisely, given an $\epsilon > 0$, $\sum_{n\geqslant 1} \frac{n^{3/2-s}}{\kappa(n)\phi(n)}$ converges for any $\sigma \geqslant 1+\epsilon$, or equivalently $\sum_{n\geqslant 1} \frac{n^{1/2-\epsilon}}{\kappa(n)\phi(n)}$ converges for any $\epsilon > 0$.

Thus, for given $\epsilon_2 > 0, s = -\epsilon_2$,

$$\left| \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{n^{s+1}f^2\phi(nf^2)} \right| \ll_{\delta_3,\epsilon_2} \sum_{n=1}^{\infty} \frac{n^{\delta_3+\epsilon_2}}{\kappa(n)\phi(n)},$$

converges whenever $\delta_3 + \epsilon_2 < \frac{1}{2}$, which means we may move the line of integration from (c_1), to $(-\epsilon_2)$. As $\Gamma(s)$ has a simple pole at $s = 0$, by using Cauchy's residue theorem, in an analogous way to our proof of lemma 2.12, we deduce

$$x \sum_{\substack{f=1\\(2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n)c_f^r(n)}{nf^2\phi(nf^2)} e^{-\frac{n}{U}} = xK(r) + O_{\delta_3,\epsilon_2}\left(\frac{x}{U^{\epsilon_2}}\right).$$

That is,

$$\mathbf{ET08} = O_{\delta_3,\epsilon_2}\left(\frac{x}{U^{\epsilon_2}}\right).$$

4.3.9 On ET=$\sum_{i\leqslant 8}$ET0i

Since $\frac{x}{(\log x)^A} \leqslant UV^2 \log U^2 \leqslant x$ for any $A > 0$, let

$$U = \frac{x}{(\log x)^\alpha},$$

and

$$V^2 = ((\log x)^{\beta/2})^2 = (\log x)^\beta,$$

for some α, β to be determined later. It follows that

$$UV^2 \log U^2 = \frac{x}{(\log x)^\alpha}(\log x)^\beta\{2(\log x - \alpha \log\log x)\} \ll \frac{x}{(\log x)^{\alpha-\beta-1}}.$$

Notice

$$\frac{x}{(\log x)^{\alpha-\beta-1}} \leqslant x,$$

implies our first conditions

$$\alpha > \beta \geqslant 0, \alpha - \beta \geqslant 1.$$

Let $c > 0$. Observe

- **ET01** $\ll_{r,\epsilon_1} \frac{x^{11/8+\epsilon_1}}{U^{1/2}} = x^{7/8+\epsilon_1}(\log x)^{\frac{\alpha}{2}}$. By lemma 2.3, for any $\epsilon' > 0$,

  $$(\log x)^{\frac{\alpha}{2}+c} \ll x^{\epsilon'}.$$

  It follows that

  $$x^{7/8+\epsilon_1}(\log x)^{\frac{\alpha}{2}+c} \ll x^{7/8+\epsilon_1+\epsilon'} < x,$$

  for any $0 < \epsilon_1 + \epsilon' < \frac{1}{8}$.

- **ET02** $\ll \frac{x\log x(\log U)^2}{V^3} = \frac{x\log x(\log x-\alpha\log\log x)^2}{(\log x)^{3/2\beta}}$. Notice

$$\begin{aligned}\frac{x\log x(\log x-\alpha\log\log x)^2}{(\log x)^{3/2\beta}} &< \frac{x\log x(\log x)^2+x\log x(\alpha\log\log x)^2}{(\log x)^{3/2\beta}}\\ &\ll \frac{x}{(\log x)^{3/2\beta-3}},\end{aligned}$$

which implies the condition $c \leqslant \frac{3}{2}\beta-3$.

- **ET03** $\ll_{\delta_1} \frac{x}{U} = (\log x)^{\alpha}$. By lemma 2.3,

$$(\log x)^{\alpha+c} \ll x.$$

It follows that **ET03** $\ll \frac{x}{(\log x)^c}$, for any $0<\delta_1\leqslant 1$.

- **ET04** $\ll_r U(\log U)^2 = \frac{x}{(\log x)^{\alpha}}(\log x-\alpha\log\log x)^2$. Notice

$$\begin{aligned}\frac{x}{(\log x)^{\alpha}}(\log x-\alpha\log\log x)^2 &< \frac{x}{(\log x)^{\alpha}}\left\{(\log x)^2+\alpha^2(\log\log x)^2\right\}\\ &\ll \frac{x}{(\log x)^{\alpha-2}},\end{aligned}$$

which implies the condition $c\leqslant\alpha-2$.

- **ET05** $\ll (\log U)^{5/2}(UV^2(\log U^2)x\log x)^{1/2}$. Notice

$$\begin{aligned}&(\log U)^{5/2}(UV^2(\log U^2)x\log x)^{1/2}\\ &= (\log x-\alpha\log\log x)^{5/2}\left(\frac{x}{(\log x)^{\alpha}}(\log x)^{\beta}2(\log x-\alpha\log\log x)x\log x\right)^{1/2}\\ &= \sqrt{2}\frac{x}{(\log x)^{\frac{\alpha-\beta-1}{2}}}(\log x-\alpha\log\log x)^3\\ &\ll \frac{x}{(\log x)^{\frac{\alpha-\beta-1}{2}}}\{(\log x)^3+3\log x(\alpha\log\log x)^2\}\\ &\ll \frac{x}{(\log x)^{\frac{\alpha-\beta-1}{2}-\frac{6}{2}}},\end{aligned}$$

which implies the condition $2c\leqslant\alpha-\beta-7$.

- **ET06** $\ll_{\delta_2} \frac{x}{(U \log U^2)^{1/2+\delta_2}}$ for any $0 < \delta_2 < \frac{1}{2}$. By lemma 2.3, for any $\epsilon' > 0$,

$$\left[\frac{(\log x)^{\frac{\alpha}{2}+\alpha\delta_2+c}}{(2\log x - 2\alpha \log\log x)^{\frac{1}{2}+\delta_2}} \right] \ll x^{\epsilon'}.$$

  It follows that

$$\begin{aligned} \frac{x(\log x)^c}{(U\log U^2)^{1/2+\delta_2}} &= x^{\frac{1}{2}-\delta_2} \left[\frac{(\log x)^{\frac{\alpha}{2}+\alpha\delta_2+c}}{(2\log x - 2\alpha \log\log x)^{\frac{1}{2}+\delta_2}} \right] \\ &\ll x^{\frac{1}{2}-\delta_2+\epsilon'} \\ &< x, \end{aligned}$$

  whenever $0 < \epsilon' - \delta_2 < \frac{1}{2}$.

- **ET07** $\ll \frac{x}{V^2} = \frac{x}{(\log x)^{\beta}}$, which implies the condition $\beta \geqslant c$.

- **ET08** $\ll_{\delta_3,\epsilon_2} \frac{x}{U^{\epsilon_2}} = x^{1-\epsilon_2}(\log x)^{\alpha\epsilon_2}$. By lemma 2.3, for any $\epsilon' > 0$,

$$(\log x)^{\alpha\epsilon_2+c} \ll x^{\epsilon'}.$$

  It follows that

$$x^{1-\epsilon_2}(\log x)^{\alpha\epsilon_2+c} \ll x^{1-\epsilon_2+\epsilon'} < x,$$

  whenever $0 < \epsilon' < \epsilon_2$, $0 < \delta_3 + \epsilon_2 < \frac{1}{2}$.

Consider the following conditions:

$$\alpha - \beta - 7 \geqslant 2c, \tag{4.1}$$

$$\beta \geqslant c, \tag{4.2}$$

$$\alpha > \beta \geqslant 0, \tag{4.3}$$

$$\alpha - \beta \geqslant 1, \tag{4.4}$$

$$\frac{3}{2}\beta - 3 \geqslant c, \tag{4.5}$$

$$\alpha - 2 \geqslant c. \tag{4.6}$$

Let $\alpha - \beta - 7 = 2c$ and $\beta = c + \delta', \delta' > 0$, so that the first two conditions (4.1) and (4.2) are satisfied. Notice

$$3c + 7 + \delta' > c + \delta' > 0,$$

$$2c + 7 > 1,$$

$$c + \left(\frac{1}{2}c + \frac{3}{2}\delta' - 3\right) > c,$$

whenever $\frac{1}{2}c + \frac{3}{2}\delta' > 3$, and

$$3c + 5 + \delta' > c,$$

satistying conditions (4.3), (4.4), (4.5), and (4.6) respectively. To double sum up, given any $c > 0, \delta' > 0, \delta_1 > 0, \delta_2 > 0, \delta_3 > 0, \epsilon' > 0, \epsilon_1 > 0, \epsilon_2 > 0$, such that $c + 3\delta' > 6, 0 < \delta_1 \leqslant 1, 0 < \delta_2 < \frac{1}{2}, 0 < \epsilon' + \epsilon_1 < \frac{1}{8}, 0 < \epsilon' - \delta_2 < \frac{1}{2}, 0 < \epsilon' < \epsilon_2$, and $0 < \epsilon_2 + \delta_3 < \frac{1}{2}$, choosing

$$\begin{aligned} U &= \frac{x}{(\log x)^{\alpha}}, \text{ where } \alpha = 3c + 7 + \delta', \\ V &= (\log x)^{\frac{\beta}{2}}, \text{ where } \beta = c + \delta', \end{aligned}$$

we have that

$$\begin{aligned} \mathbf{ET} &= \sum_{i \leqslant 8} \mathbf{ET0i} \\ &= O_{c,\delta',\delta_1,\delta_2,\delta_3,\epsilon',\epsilon_1,\epsilon_2,r}\left(\frac{x}{(\log x)^c}\right). \end{aligned}$$

Lastly, let $\epsilon > 0$,

$$\delta' = \delta_1 = \epsilon_1 = \epsilon_2 = \epsilon,$$

$$\delta_2 = \frac{\epsilon}{4},$$

and

$$\delta_3 = \epsilon' = \frac{\epsilon}{2}.$$

It follows that

$$\begin{aligned}
c + 3\delta' > 6 \quad &\Leftrightarrow \quad c > 6 - 3\epsilon, \\
0 < \delta_1 \leqslant 1 \quad &\Leftrightarrow \quad 0 < \epsilon \leqslant 1, \\
0 < \delta_2 < \frac{1}{2} \quad &\Leftrightarrow \quad 0 < \epsilon < 2, \\
0 < \epsilon' + \epsilon_1 < \frac{1}{8} \quad &\Leftrightarrow \quad 0 < \epsilon < \frac{1}{12}, \\
0 < \epsilon' - \delta_2 < \frac{1}{2} \quad &\Leftrightarrow \quad 0 < \epsilon < 2, \\
0 < \epsilon' < \epsilon_2 \quad &\Leftrightarrow \quad 0 < \frac{\epsilon}{2} < \epsilon, \\
0 < \delta_3 + \epsilon_2 < \frac{1}{2} \quad &\Leftrightarrow \quad 0 < \epsilon < \frac{1}{3}.
\end{aligned}$$

Hence for $0 < \epsilon < \frac{1}{12}, c > 6 - 3\epsilon$,

$$O_{c,\delta',\delta_1,\delta_2,\delta_3,\epsilon',\epsilon_1,\epsilon_2,r}\left(\frac{x}{(\log x)^c}\right) = O_{c,\epsilon,r}\left(\frac{x}{(\log x)^c}\right).$$

4.4 The Constant Term $K(r)$

For $r \in \mathbb{Z}$ of odd parity, recall that

$$c_f^r(n) \stackrel{\text{def}}{=} \sum_{\substack{a \bmod 4n \\ (r^2 - af^2, 4n) = 4}} \left(\frac{a}{n}\right).$$

The purpose of this section is to write

$$K(r) = \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n) c_f^r(n)}{nf^2 \phi(nf^2)},$$

as a product, thereby showing that $K(r)$ is non-zero. We digress for the moment in order to prove some lemmas.

Lemma 4.4 *For* $p \nmid 2r$,

$$\sum_{\alpha \geqslant 1} \frac{c_p^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) = \frac{1}{(p^2-1)} \left\{ \frac{2p^2}{(p^2-1)} + 1 \right\}.$$

Proof For $p \nmid 2r$, by lemma 4.2, part 6, we have that

$$\begin{aligned}
\sum_{\alpha \geqslant 1} \frac{c_p^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) &= \sum_{\alpha \geqslant 1} \frac{c_p^r(p^\alpha)}{p^\alpha p^{\alpha-1}(p-1)}(\alpha+1) \\
&= \sum_{\substack{\alpha \geqslant 2 \\ \alpha \text{ even}}} \frac{\alpha+1}{p^\alpha} \\
&= 2\sum_{\alpha' \geqslant 1} \frac{\alpha'}{p^{2\alpha'}} + \sum_{\alpha' \geqslant 1} \frac{1}{p^{2\alpha'}}.
\end{aligned}$$

Let $x = \frac{1}{p^2}$. Then

$$\begin{aligned}
\sum_{\alpha' \geqslant 1} \frac{1}{p^{2\alpha'}} &= x + x^2 + x^3 + \ldots \\
&= x\left(\frac{1}{1-x}\right) \\
&= \frac{1}{p^2-1},
\end{aligned}$$

and

$$\begin{aligned}
2\sum_{\alpha' \geqslant 1} \frac{\alpha'}{p^{2\alpha'}} &= 2x(1 + 2x + 3x^2 + 4x^3 + \ldots) \\
&= 2x\frac{d}{dx}(x + x^2 + x^3 + x^4 + \ldots) \\
&= \frac{2x}{(1-x)^2} \\
&= \frac{2p^2}{(p^2-1)^2}.
\end{aligned}$$

Q.E.D.

Lemma 4.5 *For $p = 2$,*

$$\sum_{\alpha \geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) = \frac{4}{9}.$$

Proof Let $x = -\frac{1}{2}$. Then by lemma 4.2, part 4,

$$\begin{aligned}
\sum_{\alpha \geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) &= 1 + \sum_{\alpha \geqslant 1} \frac{c_1^r(2^\alpha)}{2^\alpha \phi(2^\alpha)} d(2^\alpha) \\
&= 1 + \sum_{\alpha \geqslant 1} \frac{(-1)^\alpha}{2^\alpha}(\alpha + 1) \\
&= 1 + 2x + 3x^2 + 4x^3 + \ldots \\
&= \frac{d}{dx}(x + x^2 + x^3 + \ldots) \\
&= \frac{d}{dx}\left(\frac{x}{1-x}\right) \\
&= \frac{1}{(1-x)^2} \\
&= \frac{1}{(3/2)^2}.
\end{aligned}$$

Q.E.D.

Lemma 4.6 *Let $p > 2$. For $p|r$,*

$$\sum_{\alpha \geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) = \frac{p^2(p^2+1)}{(p^2-1)^2}.$$

Proof Let $x = \frac{1}{p^2}$. For $p|r$, $\left(\frac{r^2}{p}\right) = 0$. Thus by lemma 4.2, part 5, we have

$$\begin{aligned}
\sum_{\alpha \geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) &= \sum_{\alpha' \geqslant 0} \frac{2\alpha' + 1}{p^{2\alpha'}} \\
&= 1 + 3x + 5x^2 + 7x^3 + \ldots \\
&= (1 + 2x + 3x^2 + 4x^3 + \ldots)(1 + x) \\
&= \frac{p^2(p^2+1)}{(p^2-1)^2}.
\end{aligned}$$

Q.E.D.

Lemma 4.7 *Let $p > 2$. For $p \nmid r$,*

$$\sum_{\alpha \geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) = \frac{p^2(p^3 - 2p^2 - p - 2)}{(p-1)(p^2-1)^2}.$$

Proof, Since $p \nmid r$, $\left(\frac{r^2}{p}\right) = 1$. It follows by lemma 4.2, part 5, that

$$\begin{aligned}
&\sum_{\alpha \geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) \\
&= \sum_{\alpha \geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha p^{\alpha-1}(p-1)} (\alpha + 1) \\
&= \frac{p-2}{p-1} \sum_{\substack{\alpha \geqslant 0 \\ \alpha \, even}} \frac{(\alpha+1)}{p^\alpha} - \frac{1}{p-1} \sum_{\substack{\alpha \geqslant 1 \\ \alpha \, odd}} \frac{(\alpha+1)}{p^\alpha} \\
&= \frac{p-2}{p-1} \left\{ \frac{p^2(p^2+1)}{(p^2-1)^2} \right\} - \frac{1}{p-1} \left\{ \frac{2p^3}{(p^2-1)^2} \right\} \\
&= \frac{p^3(p^2+1)}{(p-1)(p^2-1)^2} - \frac{2p^2(p^2+1)}{(p-1)(p^2-1)^2} - \frac{2p^3}{(p-1)(p^2-1)^2} \\
&= \frac{p^5 - 2p^4 - p^3 - 2p^2}{(p-1)(p^2-1)^2} \\
&= \frac{p^2(p^3 - 2p^2 - p - 2)}{(p-1)(p^2-1)^2}.
\end{aligned}$$

Q.E.D.

We now have the lemmas in place and may proceed to show $K(r)$ has a product expansion. Note by lemma 2.6, part 6,

$$\phi(nf^2) = \frac{(n, f^2)\phi(n)\phi(f^2)}{\phi((n, f^2))},$$

so that

$$K(r) = \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \sum_{n=1}^{\infty} \frac{d(n) c_f^r(n) \phi((n, f^2))}{nf^2 (n, f^2) \phi(n) \phi(f^2)}.$$

Let $f(n) = \frac{d(n) c_f^r(n) \phi((n,f^2))}{n(n,f^2)\phi(n)}$. Note that by lemma 4.2, part 2, $c_f^r(n)$ is multiplicative, $d(n)$ is multiplicative, and ϕ is multiplicative, so that $f(n)$ is a multiplicative function. Furthermore,

$$|f(n)| \leqslant \frac{d(n)}{\phi(n)\kappa(n)},$$

and we know from our work in subsection 4.3.7 on **ET07** that $\sum_{n\geqslant 1} \frac{d(n)}{\phi(n)\kappa(n)}$ converges, so that $\sum_{n\geqslant 1} |f(n)|$ converges by comparison. It follows by the *analytic fundamental theorem of arithemetic*[17] that

$$K(r) = \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \frac{1}{f^2\phi(f^2)} \prod_p \left(\sum_{\alpha\geqslant 0} \frac{c_f^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} \frac{\phi((p^\alpha, f^2))}{(p^\alpha, f^2)} d(p^\alpha) \right).$$

We consider the inner product. Note by lemma 4.2, part 3, $c_f^r(p^\alpha) = c_{(f,p)}^r(p^\alpha)$, so that

$$\begin{aligned}
&\prod_p \left(\sum_{\alpha\geqslant 0} \frac{c_f^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} \frac{\phi((p^\alpha, f^2))}{(p^\alpha, f^2)} d(p^\alpha) \right) \\
&\quad = \prod_{p\nmid f} \left(\sum_{\alpha\geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) \right) \prod_{p\mid f} \left(\sum_{\alpha\geqslant 0} \frac{c_p^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} \frac{\phi((p^\alpha, f^2))}{(p^\alpha, f^2)} d(p^\alpha) \right),
\end{aligned}$$

which is equal to

$$\prod_p \left(\sum_{\alpha\geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) \right) \prod_{p\mid f} \left(\frac{\sum_{\alpha\geqslant 0} \frac{c_p^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} \frac{\phi((p^\alpha, f^2))}{(p^\alpha, f^2)} d(p^\alpha)}{\sum_{\alpha\geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha)} \right).$$

Substituting back into the equation for $K(r)$ we obtain

$$\begin{aligned}
K(r) &= \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \frac{1}{f^2\phi(f^2)} \prod_p \left(\sum_{\alpha\geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) \right) \prod_{p\mid f} \left(\frac{\sum_{\alpha\geqslant 0} \frac{c_p^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} \frac{\phi((p^\alpha, f^2))}{(p^\alpha, f^2)} d(p^\alpha)}{\sum_{\alpha\geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha)} \right) \\
&= \prod_p \left(\sum_{\alpha\geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha) \right) \sum_{\substack{f=1 \\ (2r,f)=1}}^{\infty} \frac{1}{f^2\phi(f^2)} \prod_{p\mid f} \left(\frac{\sum_{\alpha\geqslant 0} \frac{c_p^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} \frac{\phi((p^\alpha, f^2))}{(p^\alpha, f^2)} d(p^\alpha)}{\sum_{\alpha\geqslant 0} \frac{c_1^r(p^\alpha)}{p^\alpha \phi(p^\alpha)} d(p^\alpha)} \right).
\end{aligned}$$

[17] Let f be a multiplicative function such that the $\sum f(n)$ is absolutely convergent. Then the series can be expressed as an absolutely convergent infinite product. That is,

$$\sum_{n\geqslant 1} f(n) = \prod_p (1 + f(p) + f(p^2) + \ldots).$$

Applying the *analytic fundamental theorem of arithmetic* to the inner sum over f we obtain

$$\prod_{p}\left(\sum_{\alpha\geqslant 0}\frac{c_1^r(p^\alpha)}{p^\alpha\phi(p^\alpha)}d(p^\alpha)\right)\prod_{p\nmid 2r}\left\{1+\sum_{\beta\geqslant 1}\frac{1}{p^{2\beta}\phi(p^{2\beta})}\left(\frac{\sum_{\alpha\geqslant 0}\frac{c_p^r(p^\alpha)\phi((p^\alpha,p^{2\beta}))}{p^\alpha\phi(p^\alpha)(p^\alpha,p^{2\beta})}d(p^\alpha)}{\sum_{\alpha\geqslant 0}\frac{c_1^r(p^\alpha)}{p^\alpha\phi(p^\alpha)}d(p^\alpha)}\right)\right\},$$

which is equal to

$$\prod_{p|2r}\left(\sum_{\alpha\geqslant 0}\frac{c_1^r(p^\alpha)}{p^\alpha\phi(p^\alpha)}d(p^\alpha)\right)\prod_{p\nmid 2r}\left\{\sum_{\alpha\geqslant 0}\frac{c_1^r(p^\alpha)}{p^\alpha\phi(p^\alpha)}d(p^\alpha)+\sum_{\beta\geqslant 1}\frac{1}{p^{2\beta}\phi(p^{2\beta})}\sum_{\alpha\geqslant 0}\frac{c_p^r(p^\alpha)\phi((p^\alpha,p^{2\beta}))}{p^\alpha\phi(p^\alpha)(p^\alpha,p^{2\beta})}d(p^\alpha)\right\}.$$

Notice

$$\begin{aligned}&\sum_{\beta\geqslant 1}\frac{1}{p^{2\beta}\phi(p^{2\beta})}\sum_{\alpha\geqslant 0}\frac{c_p^r(p^\alpha)\phi((p^\alpha,p^{2\beta}))}{p^\alpha\phi(p^\alpha)(p^\alpha,p^{2\beta})}d(p^\alpha)\\ &\quad=\ \sum_{\beta\geqslant 1}\frac{1}{p^{2\beta}\phi(p^{2\beta})}+\sum_{\alpha\geqslant 1}\frac{c_p^r(p^\alpha)d(p^\alpha)}{p^\alpha\phi(p^\alpha)}\sum_{\beta\geqslant 1}\frac{1}{p^{2\beta}\phi(p^{2\beta})}\frac{\phi((p^\alpha,p^{2\beta}))}{(p^\alpha,p^{2\beta})},\end{aligned}$$

and by lemma 2.7, part 6,

$$\begin{aligned}\frac{\phi((p^\alpha,p^{2\beta}))}{(p^\alpha,p^{2\beta})} &= \frac{\phi(p^\alpha)\phi(p^{2\beta})}{\phi(p^{2\beta+\alpha})}\\ &= \frac{p^{\alpha-1}(p-1)p^{2\beta-1}(p-1)}{p^{2\beta+\alpha-1}(p-1)}\\ &= \frac{p-1}{p}.\end{aligned}$$

Furthermore,

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

so that

$$\sum_{\beta\geqslant 1}\frac{1}{p^{2\beta}\phi(p^{2\beta})}=\frac{p}{p-1}\left(\frac{1}{p^4-1}\right),$$

and

$$\sum_{\beta\geqslant 1}\frac{1}{p^{2\beta}\phi(p^{2\beta})}\frac{\phi((p^\alpha,p^{2\beta}))}{(p^\alpha,p^{2\beta})}=\frac{1}{p^4-1}.$$

Hence, $K(r)$ is equal to

$$\prod_{p|2r}\left(\sum_{\alpha\geqslant 0}\frac{c_1^r(p^\alpha)}{p^\alpha\phi(p^\alpha)}d(p^\alpha)\right)\prod_{p\nmid 2r}\left\{\sum_{\alpha\geqslant 0}\frac{c_1^r(p^\alpha)}{p^\alpha\phi(p^\alpha)}d(p^\alpha)+\frac{1}{p^4-1}\left(\frac{p}{p-1}+\sum_{\alpha\geqslant 1}\frac{c_p^r(p^\alpha)d(p^\alpha)}{p^\alpha\phi(p^\alpha)}\right)\right\},$$

which by lemmas 4.4, 4.5, 4.6 and 4.7, is equal to

$$\frac{4}{9}\prod_{p|r}\frac{p^2(p^2+1)}{(p^2-1)^2}\prod_{p\nmid 2r}\left(\frac{p^2(p^3-2p^2-p-2)}{(p-1)(p^2-1)^2}+\frac{1}{p^4-1}\left(\frac{p}{p-1}+\frac{1}{(p^2-1)}\left\{\frac{2p^2}{(p^2-1)}+1\right\}\right)\right),$$

which is equal to

$$\frac{4}{9}\prod_{p|r}\frac{p^2(p^2+1)}{(p^2-1)^2}\prod_{p\nmid 2r}\frac{2p^9-3p^8-3p^7+p^5+p^4+3p^3-2p^2+1}{(p-1)(p^4-1)(p^2-1)^2},$$

which is equal to

$$\frac{4}{9}\prod_{p|r}\frac{p^2(p^2+1)}{(p^2-1)^2}\prod_{p\nmid 2r}\frac{(p-1)(2p^8-p^7-4p^6-4p^5-3p^4-2p^3+p^2-p-1)}{(p-1)(p^4-1)(p^2-1)^2},$$

which is equal to

$$\frac{4}{9}\prod_{p|r}\frac{p^2(p^2+1)}{(p^2-1)^2}\prod_{p\nmid 2r}\frac{2p^8-p^7-4p^6-4p^5-3p^4-2p^3+p^2-p-1}{(p^4-1)(p^2-1)^2}.$$

Bibliography

[ADJ00] A. Akbary, C. David, and R. Juričević, *Average Lang–Trotter Conjecture for 2 Elliptic Curves*, In Progress (2000).

[Bar66] M. B. Barban, *The large sieve method and its application to number theory*, Russian Math. Surveys **no. 1** (1966), 49–103.

[BŠ66] Z. I. Borevič and I. R. Šafarevič, *Number theory*, Academic Press Inc, New York, 1966.

[Bur63] D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. **13** (1963), 524–536.

[Čhe51] P. L. Čhebyšev, *Sur la fonction qui détermine la totalite des nombres premiers inférieurs à une limite donnée*, Mém. présenté à l'Acad. Imp. Sci. St.Pétersbourg par divers savants **6** (1851), 141–157.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, New York, 1993.

[Cox89] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, John Wiley and Sons Inc, New York, 1989.

[Dav80] H. Davenport, *Multiplicative Number Theory–Second Edition*, Springer–Verlag, New York, 1980.

[Deu41] M. Deuring, *Die typen der multiplikatorenringe elliptischer funktionenköper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[DP99] C. David and F. Pappalardi, *Average Frobenius Distributions of Elliptic curves*, Mathematics Research Notices **no 4** (1999), 165–183.

[Elk87] N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over the rationals*, Invent. Math. **89** (1987), 561–567.

[Elk91] N. Elkies, *Distribution of supersingular primes*, Astérisque-Journées Arithmétiques de Luminy **198/199/200** (1991), 127–132.

[EM99] J. Esmonde and M. R. Murty, *Problems in Algebraic Number Theory*, Springer-Verlag, New York, 1999.

[FM95] E. Fouvry and M. R. Murty, *Supersingular primes common to two elliptic curves*, Number theory: Seminaire de theorie des nombres de Paris, 1992-3, London Math Soc. Lecture Note Series, Cambridge Univ. Press, Cambridge **215** (1995), 91–101.

[FM96] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Can. J. Math. **48** (1996), 81–104.

[HL23] G. H. Hardy and J. E. Littlewood, *Some problems of partitio numenorum III*, Acta. Math. **44** (1923), 1–70.

[Hua82] L. K. Hua, *Introduction to Number Theory*, Springer–Verlag, New York, 1982.

[HW64] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1964.

[KM84] J. Kečkić and D. Mitrinović, *The Cauchy Method of residues: theory and applications-volume 2*, Kluwer Academic publishers, Boston, 1984.

[LT76] S. Lang and H. Trotter, *Frobenius distributions in GL2-extensions*, Springer-Verlag lecture notes in mathematics 504, New York, 1976.

[MM97] M. R. Murty and V. K. Murty, *Non Vanishing of L-functions and Applications*, progress in mathematics 157, Birkhäuser-Verlag,Basel, 1997.

[Mon71] H. L. Montgomery, *Topics in multiplicative number theory*, Springer-Verlag lecture notes in mathematics number 227, New York, 1971.

[Pól18] G. Pólya, *über die verteilung der quadratischen Reste und Nichtreste*, Nachr. Königl. Ges. Wiss. Göttingen (1918), 21–29.

[Ros94] H. E. Rose, *A Course in Number Theory*, Clarendon Press, Oxford, 1994.

[Sel50] A. Selberg, *An elementary proof of the prime number theorem for arithmetic progressions*, Can. J. Math. **2** (1950), 66–78.

[Ser68] J. P. Serre, *Abelian ℓ–adic representations and elliptic curves*, Benjamin, New York, 1968.

[Ser81] J. P. Serre, *Quelques applications du théorème de densité de Chebotarev*, IHES Publ. Math. **54** (1981), 123–201.

[Sie64] W. Sierpiński, *Elementary Theory of Numbers*, Kluwer, Warszawa, 1964.

[Sil99] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, New York, 1999.

[ST87] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, Chapman and Hall, Cambridge, 1987.

[Tit78] E. C. Titchmarsh, *The Theory of Functions*, Oxford University Press, London, 1978.

[Vin19] I. M. Vinogradov, *über die verteilung der quadratischen Reste und Nichtreste*, J. Soc. Phys. Math. Univ. Permi. **2** (1919), 1–14.

[Wil22] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. **21** (1922), 235–255.