SUPERSINGULAR DISTRIBUTION, CONGRUENCE CLASS BIAS, AND A REFINEMENT OF STRONG MULTIPLICITY ONE

Thesis by

Nahid Walji

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2011

(Submitted December 17, 2010)

Acknowledgements

First and foremost, it is a pleasure to thank my advisor, Dinakar Ramakrishnan, for his guidance, support, advice, and encouragement during my years in graduate school.

Thanks to Matthias Flach, Nikolai Makarov and Andrei Jorza for kindly agreeing to serve on my thesis committee. I also wish to thank Chantal David, Noam Elkies, and Etienne Fouvry for their insightful comments and encouragement. Thanks to the administrative staff of the mathematics department for ensuring everything ran smoothly.

I would also like to thank Jürg Kramer, the Berlin Mathematical School, and the Humboldt University of Berlin for accommodating me as a visitor and providing a productive work environment.

I wish to thank the graduate students, past and present, of the mathematics department, my students over the past five years, as well as friends and all others at Caltech who contributed to a positive and well-rounded graduate school experience. I would also like to thank my friends from back home who helped me maintain perspective on life.

Finally, I would like to thank my family for their love and support.

Abstract

This thesis consists of four chapters, including an introduction.

In Chapter 2, we take an averaging approach to the question of the distribution of supersingular primes of degree one, for elliptic curves over a number field. We begin by modifying the Lang-Trotter heuristic to address the case of an abelian extension, then we show that it holds on average (up to a constant) for a family of elliptic curves by using ideas of David-Pappalardi.

In Chapter 3, we prove constructively that there exists an infinite number of (arbitrarily) thin families of rational elliptic curves for which the Lang-Trotter conjecture holds on average, in part by using techniques of Fouvry-Murty.

In Chapter 4, we obtain a result related to the strong multiplicity one theorem for non-dihedral cuspidal automorphic representations for GL(2), with trivial central character and non-twist-equivalent symmetric squares. Given a real algebraic number γ, we also find a lower bound for the lower density of the set of finite places v for which $a_v \neq \gamma$.

Contents

Chapter 1

Introduction

This thesis consists of research conducted in the context of two particular notions: the Lang-Trotter predictions for supersingular primes and a refinement of the strong multiplicity one theorem for GL(2). We introduce each aspect of the thesis in turn.

The common theme to both is the occurrence of suitable L-functions.

1.1 The Lang-Trotter conjecture - congruence class bias and thin families

Given an elliptic curve E defined over some number field F and a prime $\mathfrak{p}$ of good reduction, let

$$a_{\mathfrak{p}} = N\mathfrak{p} + 1 - |E(\mathbb{F}_{\mathfrak{p}})|.$$

One says that $\mathfrak{p}$ is *supersingular* for E if $a_{\mathfrak{p}} \equiv 0 \pmod{\mathfrak{p}}$. Given Hasse's bound of $2\sqrt{\mathfrak{p}}$ on $|a_{\mathfrak{p}}|$, this occurs for $N\mathfrak{p} > 3$ iff $a_{\mathfrak{p}} = 0$.

In 1976, Lang and Trotter [LT] conjectured the distribution of supersingular primes for a non-CM elliptic curve E over $\mathbb{Q}$ to be

$$\sim c_E \frac{\sqrt{x}}{\log x}$$

for some positive constant c_E. In the CM case, one knows by Deuring [Deu] that the density of supersingular primes is $1/2$.

In 1968, Serre [Ser3] proved that the density of supersingular primes for a non-CM elliptic curve is zero, which brings up the question of whether such primes are infinite in

number for any E/F. This was answered for $F = \mathbb{Q}$ by N. Elkies in 1987 [Elk1], when he demonstrated that there is an infinite number of supersingular primes for any elliptic curve $E/\mathbb{Q}$. In 1989, Elkies [Elk2] extended his result to an elliptic curve E over any number field with a real embedding.

It is not in general known for the other fields K, even in the case of imaginary quadratic fields. Some examples are provided by Elkies and Jao, in the cases where the absolute norm of $j(E) - 1728$ has a prime factor congruent to 1 (mod 4) that has odd exponent [Elk1] and for elliptic curves parameterised by the $X_0(p)/w_p$ for certain small odd primes p [Jao], which does include some elliptic curves with imaginary quadratic j-invariant. For example, the elliptic curve with j-invariant

$$j = \frac{-489229980611 - 42355313\sqrt{-84567}}{4096}$$

has infinitely many supersingular primes. This curve was mentioned by Jao, which arises in his paper when considering $X_0(11)/w_{11}$. It does not seem that the result on $\mathbb{Q}$ can be used to deduce it for K, though this may be possible if one can show that infinitely many of the supersingular primes over $\mathbb{Q}$ have a degree one divisor over K.

This is certainly not always true, as in the case of an elliptic curve with a torsion subgroup of order four (for example $X_1(15)$, which can be represented by the affine equation $y^2 + xy + y = x^3 + x^2$) and K being the imaginary quadratic field $\mathbb{Q}(i)$:
recall the theorem on torsion injection which states that for sufficiently large p,

$$E(\mathbb{Q})_{tors} \hookrightarrow E(\mathbb{F}_p),$$

which in our case implies

$$\begin{aligned} a_p &= p + 1 - |E(\mathbb{F}_p)| \\ &\equiv p + 1 \pmod 4 \end{aligned}$$

and so p supersingular $\Rightarrow p \equiv 3 \pmod 4$ for sufficiently large p. Thus E does not have an infinite number of supersingular primes that split in $\mathbb{Q}(i)$.

Given an elliptic curve E over a number field F and a finite extension L of F, we

will construct a heuristic for the asymptotic distribution of supersingular primes of E with degree one divisors in L.

In 1996, Fouvry and Murty [FM] demonstrated that the Lang-Trotter asymptotic for supersingular primes held on average for a family of elliptic curves over $\mathbb{Q}$. David and Papparlardi [DP] later established asymptotic expressions on average for any given trace of Frobenius. We will use their techniques to establish a result for a congruence class of primes, averaging over a family of elliptic curves. Such techniques were used in a similar manner by Kevin James in [Jam], however the aim of that paper is quite different from our goal here.

The surprise of the findings is that whilst the prediction is true up to a constant, the nature of the specific constant is not what is expected.

Fix L to be an abelian extension and let $\pi_0(L, E_{a,b}, x)$ be the number of rational primes less than x that split (totally) in L and are supersingular for $E_{a,b}$, where $E_{a,b}$ is the elliptic curve represented by the equation $Y^2 = X^3 + aX + b$. We will show

Theorem A. *For $A, B > x^{1/2+\epsilon}$, $AB > x^{3/2+\epsilon}$ we have*

$$\frac{1}{4AB} \sum_{|a|\leq A} \sum_{|b|\leq B} \pi_0(L, E_{a,b}, x) \sim C_L \frac{\sqrt{x}}{\log x}$$

as $x \to \infty$, where C_L is an explicit positive constant that is addressed in section 2.3.

For example, if we set $L = \mathbb{Q}(\sqrt{-3})$, then

$$\frac{1}{4AB} \sum_{|a|\leq A} \sum_{|b|\leq B} \pi_0\left(\mathbb{Q}\left(\sqrt{-3}\right), E_{a,b}, x\right) \sim \frac{\pi}{9} \frac{\sqrt{x}}{\log x}.$$

Remark 1. Note that the constant above of $\pi/9$ is less than half of $C_{\mathbb{Q}} = \pi/3$, suggesting a slight *bias* against the occurrence of supersingular primes that split in $\mathbb{Q}(\sqrt{-3})$. In section 2.4, we will discuss the existence of this bias in the averaging result.

The double sum in the theorem above does include supersingular primes from CM elliptic curves, however this contribution does not affect the asymptotic.

We have already published this result in [Wal2]; we will give more detail of the proof in this thesis.

We plan to investigate elsewhere the reasons for this bias, which we believe holds for any non-CM elliptic curve, with the exact nature of the bias depending on the index of the Galois representation of the elliptic curve in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

In another direction, in Chapter 3 we will demonstrate that there exist infinitely many (arbitrarily) thin families over elliptic curves over $\mathbb{Q}$ for which the result of Fouvry-Murty [FM] holds.

We will construct a sequence $\{c_n\}$ such that the terms grow faster than a given function f (so $c_n > f(n)$ for all positive integers n) and use this to define a 'thin' family S of elliptic curves, where $S = \{E_{i,j} : y^2 = x^3 + c_i x^2 + c_j\}$.

We will then establish that this family satisfies the Lang-Trotter conjecture on average, using the approach of Fouvry-Murty [FM]. Denote the number of supersingular primes for $E_{a,b}$ that are less than x by $\pi_0(E_{a,b}, x)$.

Theorem B. *Given the conditions and notations above, we have*

$$\sum_{|a|\le A}\sum_{|b|\le B}\pi_0(E_{a,b},x) = \frac{2\pi}{3}AB\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left((A+B)x^{3/2} + x^{5/2} + AB\frac{\sqrt{x}}{(\log x)^c}\right).$$

Under the conditions $A, B \ge x^{1/2+\epsilon}, AB \ge x^{3/2+\epsilon}$, this gives

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\pi_0(E_{a,b},x) \sim_\epsilon \frac{\pi}{3}\frac{\sqrt{x}}{\log x}.$$

1.2 A refinement of strong multiplicity one

Let F be a number field, and let $\mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$ be the set of cuspidal automorphic representations $\pi = \otimes'_v \pi_v$ of $\mathrm{GL}_2(\mathbb{A}_F)$. Given $\pi \in \mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$, for any place v of F where π is unramified we denote the Langlands conjugacy class by $A(\pi_v) \subset \mathrm{GL}_2(\mathbb{C})$, which we will represent by the diagonal matrix $\mathrm{diag}\{\alpha_{1,v}, \alpha_{2,v}\}$. Let $a_v(\pi)$ be the trace

of this matrix.

Given $\pi, \pi' \in \mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$, one can compare local data to determine whether π, π' are globally isomorphic. In this context we ask the following question: If we have a set S such that $a_v(\pi) = a_v(\pi')$ for all $v \notin S$, what property of S is sufficient to establish that $\pi \simeq \pi'$?

One approach involves establishing a condition on the size of S. The strong multiplicity one theorem of Jacquet-Shalika [JS1] states that it is sufficient for S to be finite. In 1994, D. Ramakrishnan [Ram] proved that a set S of density less than $1/8$ is sufficient. Furthermore this result was determined to be sharp, by an example of J.-P. Serre. One can also interpret this theorem as the statement that given any two non-isomorphic cuspidal automorphic representations π, π' for $\mathrm{GL}_2(\mathbb{A}_F)$, there exists a set $S = S(\pi, \pi')$ of density greater or equal to $1/8$ such that $a_v(\pi) \neq a_v(\pi')$ for all $v \in S$.

Recall that for a set S of primes of a number field F, the *lower Dirichlet density* $\underline{\delta}(S)$ of S is

$$\underline{\delta}(S) = \lim_{s \to 1^+} \inf \frac{\sum_{\mathfrak{p} \in S} \mathrm{N}\mathfrak{p}^{-s}}{-\log(s-1)}.$$

When S admits a Dirichlet density, then it must coincide with its lower Dirichlet density.

In the context of the above we will show

Theorem C. *Let $\pi, \pi' \in \mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$ be non-dihedral representations, with trivial central character and symmetric squares that are not twist-equivalent. For finite places v where π and π' are unramified, set $a_v = \mathrm{Tr}(A(\pi_v))$, $b_v = \mathrm{Tr}(A(\pi'_v))$, and let $S = \{v \mid a_v \neq b_v\}$. Then*

$$\underline{\delta}(S) \geq \frac{2}{5},$$

where $\underline{\delta}(S)$ is the lower Dirichlet density of the set S.

Another question of interest is the following: Given $\pi \in \mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$ and a real number γ, what can we say about the set of places v for which the associated Hecke eigenvalue of π is not equal to γ? We will prove

Theorem D. *Let π be a non-dihedral cuspidal automorphic representation over a number field F, with trivial central character. We define $S_\gamma = \{v \mid a_v \neq \gamma\}$, where γ is a real scalar and let $\underline{\delta}(S_\gamma)$ represent the lower Dirichlet density of S_γ. Then*

$$\underline{\delta}(S_\gamma) \geq \frac{(\gamma^2+1)^2}{\gamma^4+6\gamma^2+2}.$$

Corollary. *In particular, the set of finite places where a_v is non-zero has lower Dirichlet density greater or equal to* $1/2$.

Remark 2. For $F = \mathbb{Q}$ and π defined by a non-CM holomorphic newform of weight $k > 1$, by J.-P. Serre we know the stronger result that S_γ has density 1 [Ser2]. This does not apply to the case $k = 1$ because the Galois representation has finite image.

In the case of Maass forms of eigenvalue λ, there is no known Galois representation (except in simple situations), none expected when $\lambda > 1/4$, and the Ramanujan conjecture has not been proved, so their lacunarity is not well understood. Thus there is no analogue of Serre's result.

Our approach involves refining the method of D. Ramakrishnan in [Ram], though it is not a straightforward extension of his proof. We also use results of Kim-Shahidi [KS1, KS2] on the existence of, and a cuspidal criterion for, the symmetric third and fourth powers of cuspidal automorphic representations of GL(2).

In order to assess the strength of theorem C in the tetrahedral case, we also construct an example of two tetrahedral cuspidal representations π,π', that have symmetric squares that are not twist-equivalent and whose set S of all places at which $a_v(\pi) \neq a_v(\pi')$ has density 15/32. This is within 11/160 of the lower bound of 2/5 given by theorem C.

Our work appears to extend to the case where the central character of the cuspidal automorphic representations are unitary, which we are addressing in a paper [Wal1] under preparation.

In the context of theorem C, we note the result of Murty-Rajan [MR], which states that for two cuspidal automorphic representations π_1, π_2 of $GL_2(\mathbb{A}_\mathbb{Q})$, if one assumes the expected, but far from known, analytic properties of the Rankin-Selberg convolution L-functions of $\mathrm{Sym}^m(\pi_1)$ and $\mathrm{Sym}^n(\pi_2)$ for all n and m, then $\#\{p \leq x \mid a_p(\pi_1) = a_p(\pi_2)\} = O\left(x^{5/6+\epsilon}\right)$.

Finally, we mention the existence of another approach to determining a sufficient condition on S: One can establish a constant C depending on the conductors and infinity types of π and π', such that if $a_v(\pi) = a_v(\pi')$ for all v satisfying $\mathrm{N}v \leq C$, then $\pi \simeq \pi'$. See the paper of J. Liu and Y. Wang [LW] and the references therein for the current status of this approach.

Chapter 2

Supersingular distribution and congruence class bias

This part of the thesis has already been published in [Wal2]. The version we present here includes more detail.

Introduction

Define $E_{a,b}$ to be the elliptic curve that can be represented by $Y^2 = X^3 + aX + b$, with a, $b \in \mathbb{Z}$, and given a set of rational primes P, let $\pi_0(P, E_{a,b}, x)$ be the number of supersingular primes for $E_{a,b}$ that are elements of P and that are less than x.

When P is determined by a congruence condition (which we will write as $p \equiv c \pmod{m}$ with $(c, m) = 1$ then we will prove

Theorem 2.1. *For $A, B > x^{1/2+\epsilon}$, $AB > x^{3/2+\epsilon}$ we have*

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \pi_0(P, E_{a,b}, x) \sim C_P \frac{\sqrt{x}}{\log x}$$

as $x \to \infty$, for an explicitly determined positive constant C_P that depends only on P.

We briefly describe the structure of this chapter. In section 2.1 we provide some background on the Sato-Tate conjecture, which is a crucial component in our heuristic. In section 2.2 we construct the heuristic, using a similar approach to that of Lang-Trotter. We then turn to averaging over a family of elliptic curves in section 2.3, expressing the average in terms of sums of Hurwitz numbers. We interpret these using L-functions and

obtain an asymptotic expression. In section 2.4 we discuss the results when applied to certain examples of number fields, and lastly in section 2.5 we explain how to refine the averaging, using an idea of Fouvry-Murty.

2.1 Background on Sato-Tate

The heuristic will rely on a variant of the Sato-Tate conjecture. Before introducing this, we cover some relevant background on equidistribution:

Definition. Let X be a compact topological space and $C(X)$ the space of continuous complex-valued functions on X with the supremum norm (i.e., $||f|| = \sup_{x\in X} |f(x)|$). For $x \in X$, we have the associated Dirac measure δ_x, where $\delta_x(f) = f(x)$ for $f \in C(X)$.

Notation 1. Given a sequence of points $\{x_i\}_{i\geq 1}$, let

$$\mu_n = \frac{1}{n}\sum_{i=0}^{n} \delta_i.$$

Definition. Let μ be a Radon measure on X. One says that the sequence is **μ-equidistributed** if $\mu_n \to \mu$ weakly as $n \to \infty$.

Remark 3. This means that μ must be positive and normalized. Furthermore, it must satisfy

$$\mu(f) = \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} f(x_i)$$

for all $f \in C(X)$.

An l-adic representation associated to an elliptic curve E and a number field K is a continuous homomorphism $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E))$. Let Σ_K be the set of places of K and let S be the set of places at which ρ is ramified, as well as those places v where $Nv = l$ ($N = N_{K/\mathbb{Q}}$). For any $v \notin S$, we have the associated Frobenius conjugacy class in $\mathrm{Aut}(T_l(E))$.

Lemma 2.2. *The eigenvalues of this Frobenius conjugacy class, when embedded into* $\mathbb{C}$*, are* π_v *and* $\overline{\pi_v}$*, where*

$$\pi_v = (Nv)^{1/2} e^{i\phi_v} \qquad \text{where} \quad \phi_v \in [0, \pi].$$

Proof. See p136 [Sil]. □

Conjecture. *(Sato-Tate for Σ) Let Σ be a subset of Σ_K. Then the angles ϕ_v, $v \in \Sigma$ of the Frobenius elements are equidistributed with respect to the measure $\frac{2}{\pi}\sin^2\phi\ d\phi$.*

Remark 4. Strictly speaking, equidistribution relates to a sequence rather than a set. It is implicit that we take Σ to be ordered by non-decreasing norm. Note that even though a finite number of elements of Σ may have the same norm (which thus allows for various orderings of Σ with non-decreasing norm), because there is a uniform bound on the number of elements sharing any given norm, the result will still stand regardless of the ordering chosen.

Proposition 2.3. *We have the hypotheses:*

1.

$$\prod_{v\in\Sigma}\frac{1}{1-(Nv)^{-s}}$$

converges for $\mathrm{Re}(s) > 1$ *and can be extended to a meromorphic function on* $\mathrm{Re}(s) \geq 1$ *with the only zero or pole in the region being a simple pole at* $s = 1$

2.

$$L(s,\rho) = \prod_{v\in\Sigma}\frac{1}{det(1-\rho(x_p)(Nv)^{-s})}$$

(where ρ is the Galois representation associated to the elliptic curve) extends to a non-zero holomorphic function on $\mathrm{Re}(s) \geq 1$.

If both 1 and 2 hold, then the Sato-Tate conjecture for Σ is true.

Proof. I 22–26 of [Ser3] . □

Given an abelian extension $L/\mathbb{Q}$ and assuming the Sato-Tate conjecture for Σ_L, it is possible to derive the Sato-Tate conjecture for the set of degree one primes of L through the use of some straightforward complex analysis.

2.2 The heuristic

In 2.2.1 we will set up the heuristic in the same manner as in Lang-Trotter, and then in 2.2.2 we will construct an approximation model. The difference between this and the standard Lang-Trotter model is that we include a term that takes into account the torsion of the elliptic curve. In subsection 2.2.3, we determine the asymptotic behaviour of the model and reduce it down to considering the behaviour of one of the terms in the model, which has already been addressed in the standard Lang-Trotter heuristic, as we will explain in 2.2.4.

We do need a condition on P_F involving the order k of the torsion subgroup of the elliptic curve, namely that $\{\mathfrak{p} \in P_F \mid N\mathfrak{p} + 1 \equiv 0 \pmod{k}\}$ must have positive density β. Note that this condition is to avoid obstruction arising from the torsion of the elliptic curve, as shown in the example in the introduction.

2.2.1 Setup

Given a non-CM elliptic curve E, we have a representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_l \mathrm{GL}_2(\mathbb{Z}_l)$$

where the product is over the good rational primes l of E.

Notation 1. Fix a positive integer M and reduce $\prod \mathrm{GL}_2(\mathbb{Z}_l)$ modulo M to obtain the representation

$$\rho_{(M)} : G \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$$

Then we can define

$$G(M) := G/\mathrm{Ker}\rho_{(M)}$$

and

$$G(M)_t := \{g \in G(M) | \mathrm{trace}(g) \equiv t \pmod{M}\}.$$

Definition. M **splits** ρ if we have

$$\rho(G) \cong \prod_{l|M} \mathrm{GL}_2(\mathbb{Z}_l) \times G_M$$

where G is the Galois group and G_M is the projection of $\rho(G)$ into $\prod_{l|M} \mathrm{GL}_2(\mathbb{Z}_l)$.

Definition. M **stabilizes** ρ if

$$G_M = r_M^{-1}(G(M))$$

where r_M is the reduction map

$$r_M : \prod_{l|M} \mathrm{GL}_2(\mathbb{Z}_l) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}).$$

Lemma 2.4. *From Serre [Ser1] we know that we can always have a representation arising from some non-CM E that has some M which 'stabilizes' and 'splits' ρ.*

This is the type of M that we fix.

We want to consider the distribution of t_p for $p \in P_F$.

Assumption 1. t_p can be considered as a random variable, independent of other $t_{p'}$, and its behaviour as a random variable is determined by the Sato-Tate conjecture and a consequence of the general form of Chebotarev's density theorem.

Definition. Let

$$F_M(t) = M\frac{|G(M)_t|}{|G(M)|}.$$

Remark 5. M is in the formula so that

$$\frac{1}{M}\sum_{t \bmod M} F_M(t) = 1,$$

i.e., the average value of F_M is 1.

From [Mar] we have that the set P_F has a density, which we will denote as α.

Lemma 2.5. *The density of primes $p \in P_F$ such that $t_p \equiv t \pmod{M}$ is*

$$\alpha\frac{|G(M)_t|}{|G(M)|}.$$

By Hasse's inequality, we know that $t_p \in (-2\sqrt{p}, 2\sqrt{p})$. Thus we define $\xi(t,p) = t/2\sqrt{p}$ so that $\xi \in [-1,1]$. Write $\xi(t,p) = \cos\theta(t,p)$, and so $\theta(t,p) \in [0,\pi]$.

Now we have, by the Sato-Tate result, that the distribution of $\theta(t,\mathfrak{p})$ is determined by the density function $\frac{2}{\pi}\sin^2\theta$ on $[0,\pi]$. Thus the relative density of primes $p \in P_F$ that lie in an interval $[\theta_1,\theta_2]$ is

$$\int_{\theta_1}^{\theta_2} \frac{2}{\pi}\sin^2\theta d\theta.$$

Now if we change variables to $\xi = \cos\theta$ so that we have a density function $g(\xi)$ on $[-1,1]$, we get that

$$g(\xi) = \frac{2}{\pi}\sqrt{1-\xi^2}.$$

2.2.2 Approximation model

Let k be the order of the torsion in the Mordell-Weil group of the elliptic curve. One knows that for sufficiently large primes p we have $|E(\mathbb{F}_p)| \equiv 0 \pmod{k}$.

Definition. Let

$$f_M(t,\mathfrak{p},k) = \mathrm{prob}_M\{a_\mathfrak{p} = t, \textit{and } a_\mathfrak{p} \equiv N\mathfrak{p}+1 \pmod{k}\}.$$

Remark 6. Note that we need $\sum_t f_M(t,\mathfrak{p},k) = 1$.

Our main assumption for this model is that

$$f_M(t,\mathfrak{p},k) = c_\mathfrak{p} \cdot g(\xi(t,\mathfrak{p})) \cdot F_M(t) \cdot h(t,k,\mathfrak{p}),$$

where $h(t,k,\mathfrak{p})$ is equal to k if $t \equiv N\mathfrak{p}+1 \pmod{k}$ and 0 otherwise.

Remark 7. The $F_M(t)$ is for consistency with the Chebotarev density theorem, $g(\xi(t,\mathfrak{p}))$ is to ensure compatibility with the Sato-Tate result (via the law of large numbers), $c_\mathfrak{p}$ is chosen so that $\sum_t f_M(t,\mathfrak{p},k) = 1$, and lastly $h(t,\mathfrak{p},k)$ accounts for the congruence obstruction from torsion injection.

We now address the asymptotic behaviour of $c_\mathfrak{p}$.

Lemma 2.6. *If* $\sum_t f_M(t,\mathfrak{p},k)=1$*, then*

$$c_{\mathfrak{p}} \sim \frac{1}{2\sqrt{N\mathfrak{p}}}$$

as $N\mathfrak{p}\to\infty$*.*

Proof. Note that

$$\int_{-1}^{1} g(\xi)d\xi = 1$$

We consider its approximating Riemann sums (where t is still an integer):

$$\frac{1}{2\sqrt{N\mathfrak{p}}}\cdot k \cdot \sum_{-2\sqrt{N\mathfrak{p}}<t<2\sqrt{N\mathfrak{p}},\ t\equiv N\mathfrak{p}+1 \pmod k} g(\xi(t,\mathfrak{p}))$$

Fix an integer t_0 and note that when taking the limit,

$$\lim_{N\mathfrak{p}\to\infty} M\frac{k}{2\sqrt{N\mathfrak{p}}} \sum_{t\equiv t_0 \pmod M,\ |t|<2\sqrt{N\mathfrak{p}},\ t\equiv N\mathfrak{p}+1 \pmod k} g(\xi(t,\mathfrak{p})) = 1$$

provided that the congruence conditions on t are compatible (see below for the incompatible case).

We multiply by $F_M(t_0)$ to get

$$\lim_{N\mathfrak{p}\to\infty} \frac{k}{2\sqrt{N\mathfrak{p}}} \sum_{t\equiv t_0 \pmod M,\ |t|<2\sqrt{N\mathfrak{p}},\ t\equiv N\mathfrak{p}+1 \pmod k} g(\xi(t,\mathfrak{p}))F_M(t_0) = \frac{F_M(t_0)}{M}$$

and so by construction of $F_M(t_0)$, when we sum over congruence classes we get

$$\lim_{N\mathfrak{p}\to\infty} \frac{k}{2\sqrt{N\mathfrak{p}}} \sum_{|t|<2\sqrt{N\mathfrak{p}},\ t\equiv N\mathfrak{p}+1 \pmod k} g(\xi(t,\mathfrak{p}))F_M(t) = 1$$

and thus

$$\lim_{N\mathfrak{p}\to\infty} \frac{1}{2\sqrt{N\mathfrak{p}}} \sum_{|t|<2\sqrt{N\mathfrak{p}}} g(\xi(t,\mathfrak{p}))F_M(t)h(t,k,\mathfrak{p}) = 1$$

as required.

In the case where incompatible congruence conditions arise (for some t_0), the last three equations above still follow as before, due to the fact that for the t_0 in question we will have $F(t_0)=0$.

□

Remark 8. Now let R be the set of degree one primes of an abelian extension L. If we have incompatibility between the congruence arising from torsion injection and the congruences satisfied by the norms of the elements of R, then the set $Q = \{\mathfrak{p} \in R \mid N\mathfrak{p} + 1 \equiv 0 \pmod{k}\}$ may only have a finite number of elements (as in the example mentioned in the introduction). Thus from here on we only consider the cases where this does not occur (i.e., when $(k, \mathrm{disc}L) = 1$). In this case the set Q' of rational primes lying under those primes in Q will have density $1/nk$, where we recall that n is the degree of the field L and k is the order of the rational torsion group of the elliptic curve.

2.2.3 Asymptotic Behaviour

The working in this subsection mainly consists of determining the behaviour of $F_M(t)$ as $M \to \infty$ (ordered by divisibility).

Note that as $N\mathfrak{p} \to \infty$,

$$c_{\mathfrak{p}} \sim \frac{1}{2\sqrt{N\mathfrak{p}}}$$

and

$$\begin{aligned} g(\xi(t_0, \mathfrak{p})) \to g(0) &= \frac{2}{\pi}\sqrt{1 - 0^2} \\ &= \frac{2}{\pi}. \end{aligned}$$

Thus

$$\mathrm{prob}_M\{t_{\mathfrak{p}} = t_0, t_{\mathfrak{p}} \equiv N\mathfrak{p} + 1 \pmod{k}\} \sim \frac{1}{2\sqrt{\mathfrak{p}}}\frac{2}{\pi}F_M(t_0).h(t_0, k, \mathfrak{p}).$$

Notation 2. Let

$$\lim_{N\mathfrak{p}\to\infty} F_M(t) = F(t).$$

Now if we take the limit as $M \to \infty$ we should get the probability that $t_{\mathfrak{p}} = t_0$:

$$\begin{aligned} &\lim_{M\to\infty} \mathrm{prob}_M\{t_{\mathfrak{p}} = t_0, t_{\mathfrak{p}} \equiv N\mathfrak{p} + 1 \pmod{k}\} \\ =&\mathrm{prob}\{t_{\mathfrak{p}} = t_0, t_{\mathfrak{p}} \equiv N\mathfrak{p} + 1 \pmod{k}\} \\ =&\frac{1}{2\sqrt{N\mathfrak{p}}}\frac{2}{\pi}F(t_0).h(t_0, k, \mathfrak{p}). \end{aligned}$$

Thus in our case, the distribution function for all the $t_{\mathfrak{p}}$ of E that satisfy $t_{\mathfrak{p}} = t_0$ and $\mathfrak{p} \in P_F$ is (as $x \to \infty$):

$$N_{t_0}(x) \sim \frac{2}{\pi} F(t_0) \sum_{\mathfrak{p} \in P_F, N\mathfrak{p} \leq x} \frac{1}{2\sqrt{N\mathfrak{p}}} . h(t_0, k, \mathfrak{p})$$

Now the series

$$\sum_{\mathfrak{p} \in P_F, N\mathfrak{p} \leq x, t_o \equiv N\mathfrak{p}+1 \pmod{k}} \frac{1}{2\sqrt{N\mathfrak{p}}} k$$

has the following asymptotic behaviour (given that we picked a suitable F with respect to the order k of the torsion subgroup):

$$\sum_{\mathfrak{p} \in P_F, N\mathfrak{p} \leq x, t_o \equiv N\mathfrak{p}+1 \pmod{k}} k \frac{1}{2\sqrt{N\mathfrak{p}}} \sim k \int_x \frac{1}{2\sqrt{N\mathfrak{p}}} d\left(\frac{1}{\beta}\pi(x)\right)$$

where $\pi(x)$ is the prime-counting function, and thus

$$\sum_{\mathfrak{p} \in P_F, N\mathfrak{p} \leq x, N\mathfrak{p}+1 \pmod{k}} k \frac{1}{2\sqrt{N\mathfrak{p}}} \sim \int_x \frac{1}{2\sqrt{N\mathfrak{p}}} \frac{k}{\beta} \frac{dx}{\log x}.$$

Now integrate by parts, setting $u = \frac{1}{\log x}$ and $v = \sqrt{x}$, to get

$$\int_x \frac{1}{2\sqrt{N\mathfrak{p}}} \frac{k}{\beta} \frac{dx}{\log x} = \frac{k}{\beta} \frac{\sqrt{x}}{\log x}.$$

What remains is to consider $F(t_0)$, in particular for $t_0 = 0$ as it is the supersingular case.

2.2.4 Investigating $F(t_0)$

Determining the existence and value of $F(t_0)$ is done in [LT] (it is the exact same $F(t_0)$ that we consider), but for completeness, we will place the details of taking the limit for $M \to \infty$ here.

We need to consider $F_M(t)$. We have the following lemmas:

Lemma 2.7. *Let $M = M_1M_2$, where $(M_1, M_2) = 1$, and $G(M) = G(M_1) \times G(M_2)$. Then $F_M(t_0) = F_{M_1}(t_0)F_{M_2}(t_0)$.*

Lemma 2.8. *Say that M_0 is stable, $M_0|M$, the same primes divide M_0 and M, and $s \equiv t \pmod{M}_0$. Then $|G(M)_s| = |G(M)_t|$ and $F_M(t) = F_{M_0}(t)$.*

Corollary 2.9. *If M is stable, then $F_{M^n}(t) = F_M(t)$.*

Remark 9. Therefore $\lim_{n\to\infty} F_{M^n}(t)$ exists, and let us define this to be $F_{M^\infty}(t)$.

We then get:

Lemma 2.10. *Assume $\rho_l(G/\mathrm{Ker}(\rho_l)) = \mathrm{GL}_2(\mathbb{Z}_l)$. Then (by counting the number of matrices) we get*

$$F_{l^\infty}(0) = F_l(0) = \frac{1}{1 - 1/l^2}$$

Theorem 2.11. *Let $N_{t_0,R}(x)$ be the number of primes $\mathfrak{p} \in R$ such that $N\mathfrak{p} \leq x$ and $t_\mathfrak{p} = t_0$. Then*

$$N_{t_0,R}(x) \sim \frac{2}{\pi} F_M(t_0) \left(\prod_{(l,M)=1} F_l(t_0) \right) k \sum_{\substack{N\mathfrak{p}\leq x \\ \mathfrak{p}\in R \\ N\mathfrak{p}+1\equiv 0(k)}} \frac{1}{2\sqrt{N\mathfrak{p}}},$$

where l is a rational prime. When $t_0 = 0$, we have (given that M splits ρ)

$$N_{0,R}(x) \sim \frac{2}{\pi} F_M(0)\zeta(2) \left(\prod_{l|M} (1 - 1/l^2) \right) k \sum_{\substack{N\mathfrak{p}\leq x \\ \mathfrak{p}\in R \\ N\mathfrak{p}+1\equiv 0(k)}} \frac{1}{2\sqrt{N\mathfrak{p}}}.$$

We consider this in the context of rational primes. Let R' be the set of rational primes that lie under the primes in R; this has density $1/n$. Thus

$$N_{0,R'}(x) \sim \frac{2}{\pi} F_M(0)\zeta(2) \left(\prod_{l|M} (1 - 1/l^2) \right) \frac{1}{n} \frac{\sqrt{x}}{\log x}.$$

Remark 10. Comparing the above with the Lang-Trotter conjecture of

$$N_0(x) \sim \frac{2}{\pi} F_M(0)\zeta(2) \left(\prod_{l|M} (1 - 1/l^2) \right) \frac{\sqrt{x}}{\log x},$$

we see that R' has an asymptotic proportion of supersingular primes of $1/n$ (when there is no congruence obstruction). However, later in this chapter we shall see that on average there is in fact a bias in the proportion of supersingular primes, reflected in the value of the constant, which is contrary to the expectations of the heuristic.

2.3 Proof of the conjecture on average

2.3.1 Setup

We recall notation from the beginning of the chapter.

Denote $E_{a,b}$ to be the elliptic curve that can be represented by $Y^2 = X^3 + aX + b$ with $a, b \in \mathbb{Z}$, let P be a set of rational primes, and set $\pi_0(P, E_{a,b}, x)$ to be the number of supersingular primes for $E_{a,b}$ that are elements of P and that are less than x.

When P is determined by a congruence condition (which we will write as $p \equiv c \pmod{m}$ with $(c, m) = 1$, in this section we will prove

Theorem A. *For $A, B > x^{1/2+\epsilon}$, $AB > x^{3/2+\epsilon}$ we have*

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \pi_0(P, E_{a,b}, x) \sim C_P \frac{\sqrt{x}}{\log x}$$

as $x \to \infty$, for an explicitly determined positive constant C_P that depends only on P.

By Deuring, the set of supersingular primes for a CM elliptic curve over $\mathbb{Q}$ has density $1/2$. Thus we must check whether the constant in the asymptotic is affected by the contribution from CM curves.

Now there are exactly thirteen isomorphism classes of CM elliptic curves over $\mathbb{Q}$. Two of these classes are of the form $E_{a,0}$ and $E_{0,b}$, where a and b can be any non-zero integers, and the other eleven classes are of the form $E_{c_i t^2, d_i t^3}$, where t is any non-zero integer and (c_i, d_i) is, depending on its index i, one of eleven distinct pairs of integers.

Thus given elliptic curves over $\mathbb{F}_p$, we note that they may be lifted to CM curves of the form $E_{a,0}$, of which there are $2A$, given the bounds of A, B on the coefficients a, b of the affine equation (respectively). Similarly, there are $2B$ CM curves of the form $E_{0,b}$, and $11 \cdot \min(A^{1/2}, B^{1/3})$ curves of the form $E_{c_i t^2, d_i t^3}$. Given that the CM curves have a

density of supersingular primes of 1/2, we have the following:

$$\begin{aligned}
&\sum_{|a|\leq A}\sum_{\substack{|b|\leq B\\ E_{a,b}\ is\ CM}} \pi_0(P, E_{a,b}, x)\\
=&O\left(\frac{1}{2}\cdot\frac{x}{\log x}2A\right)+O\left(\frac{1}{2}\cdot\frac{x}{\log x}2B\right)+O\left(11\cdot\frac{1}{2}\cdot\frac{x}{\log x}\cdot\min(A^{1/2},B^{1/3})\right)\\
=&O\left(\frac{x}{\log x}\cdot\max(A,B)\right),
\end{aligned}$$

which we note will not affect the asymptotic expression under the conditions $A, B > x^{1/2+\epsilon}, AB > x^{3/2+\epsilon}$.

We will later choose some examples of abelian extensions and use congruence conditions to determine the set of rational primes lying under the degree one primes of the extension. This will enable us to obtain explicit asymptotic expressions.

2.3.2 Lifting supersingular elliptic curves

For p a prime greater than three and for any integer $r \leq 2\sqrt{p}$, the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ with $a_p = r$ can be expressed using the Hurwitz number

$$H(r^2-4p) = 2\sum_{\substack{f^2|(r^2-4p)\\ d\equiv 0,1(4)}}\frac{h(d)}{w(d)} \tag{2.1}$$

where $h(d)$ is the class number of, and $w(d)$ the number of units in, the order $\mathbb{Z}[(d+\sqrt{d})/2]$ of discriminant d. f and r are integers and $d = (r^2-4p)/f^2$.

We define

$$\delta_f(x) = \left\{3 < p \leq x \middle| r^2-4p \equiv 0(f^2),\ \text{and}\ \frac{r^2-4p}{f^2} \equiv 0\ or\ 1\ (4)\right\}.$$

Note that the $r = 0$ case only allows for two values of f, either one or two. Thus $d = -4p$ or $-p$.

Now because the Hurwitz number only tells us about the number of isomorphism classes, we need to consider the possible sizes of an isomorphism class:

Given an affine equation $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$, its isomorphism class is $\{y^2 =$

$x^3 + at^4x + bt^6 \mid t \in \mathbb{F}_p^\times\}$. We need to determine the size of this set under various conditions. When $a, b \neq 0$, we note that $y^2 = x^3 + at^4x + bt^6$ and $y^2 = x^3 + at'^4x + bt'^6$ have the same coefficients when $t^4 = t'^4$ and $t^6 = t'^6$, which together are equivalent to having $t^2 = t'^2$, i.e., $1 = (t'/t)^2$. Since every $\mathbb{F}_p$ has a non-trivial square root of unity, we have that the affine equations are the same exactly when $t = \pm t'$, thus the size of the isomorphism class is $(p-1)/2$.

In the case of $a \neq 0, b = 0$, we have two different cases. Note that here we consider affine equations $y^2 = x^3 + at^4x + 0$ and $y^2 = x^3 + at'^4x + 0$, which are the same when $t^4 = t'^4$, i.e., $1 = (t'/t)^4$, so we need to consider whether there are fourth roots of unity in $\mathbb{F}_p$.

In the case when $p \not\equiv 1 \pmod 4$, we note that if there were (proper) fourth roots of unity, then they would generate an order 4 subgroup of $\mathbb{F}_p^\times$. But then $4 \mid |\mathbb{F}_p^\times| = p - 1$, which implies $p - 1 = 0 \pmod 4$, a contradiction of our assumption for this case. Thus there are no fourth roots of unity and so $t^4 = t'^4$ iff $t = \pm t'$, so again we have $(p-1)/2$ to be the size of our isomorphism class.

In the case when $p \equiv 1 \pmod 4$, since $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$, there is a generator g of order $p - 1$, and thus $g^{(p-1)/4}$ is an element of order 4 in $\mathbb{F}_p^\times$. Thus our isomorphism class has size $(p-1)/4$.

The case of $a = 0, b \neq 0$ is treated similarly. We have $y^2 = x^3 + 0x + bt^6$ and $y^2 = x^3 + 0x + bt'^6$, which are the same when $t^6 = t'^6$ and thus here we consider sixth roots of unity. We obtain that there are not any when $p \not\equiv 1 \pmod 6$, and thus the size of the isomorphism class is $(p-1)/2$, and that they do exist in $\mathbb{F}_p$ when $p \equiv 1 \pmod 6$, and so the size of the isomorphism class is then $(p-1)/6$. (The condition $1 \pmod 6$ can of course be replaced by $1 \pmod 3$ since we are only considering primes ≥ 5.)

Thus the number of supersingular elliptic curves over $\mathbb{F}_p$ is

$$\frac{p-1}{2}(H(-4p) + O(1)) + \frac{p-1}{4}O(1) + \frac{p-1}{6}O(1)$$

where the error terms are to account for the possibility that some of the supersingular elliptic curves may belong to an isomorphism class that has affine equations with either $a = 0$ or $b = 0$ in conjunction with the fact that p may be $1 \pmod 4$ and/or $1 \pmod 6$.

Below we will see that $H(-4p) \ll \sqrt{p}\log p$, so we can rewrite our expression above as

$$\frac{p}{2}H(-4p) + O\left(p\right).$$

We obtain

$$\frac{1}{4AB}\sum_{|a|\leq A}\sum_{|b|\leq B}\pi_0(P, E_{a,b}, x) = \frac{1}{4AB}\sum_{p\leq x, p\in P}\left(\frac{2A}{p}+O(1)\right)\cdot\left(\frac{2B}{p}+O(1)\right) \tag{2.2}$$
$$\cdot\left(\frac{p}{2}H(-4p)+O(p)\right)+O(1)$$

where the last error term is to account for possible supersingularity of 2 and 3, as well as the case when p is supersingular for an elliptic curve with a non-minimal equation that is in the kernel of the reduction map to $\mathbb{F}_p$.

This gives

$$\frac{1}{2}\sum_{3<p\leq x, p\in P}\frac{H(-4p)}{p} + O\left(\sum_{3<p\leq x, p\in P}H(-4p)\left(\frac{1}{A}+\frac{1}{B}+\frac{p}{AB}\right)\right)$$
$$+ O\left(\log\log x\right) + O\left(1\right).$$

To bound the error terms, we note that $H(-4p) = h(-p) + h(-4p)$, and using the Dirichlet class number formula

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

when $d \equiv 0$ *or* $1 \pmod 4$, and where $w(d) = 6, 4, 2$ for $d = 3, 4$, or ≥ 7 (respectively). Partial summation and the Polya-Vinogradov inequality gives

$$\begin{aligned} & L(1,\chi_d) \ll \log|d| \\ \Rightarrow\ & h(d) \ll \sqrt{|d|}\log|d| \\ \Rightarrow\ & H(-4p) \ll \sqrt{p}\log p. \end{aligned} \tag{2.3}$$

We use this to consider

$$\begin{aligned}
&O\left(\sum_{3<p\leq x, p\in P} H(-4p)\left(\frac{1}{A}+\frac{1}{B}+\frac{p}{AB}\right)\right)\\
&=O\left((1/A+1/B)\int_2^x \sqrt{t}\log t\frac{dt}{\log t}+\frac{1}{AB}\int_2^x \sqrt{t}\log t\frac{dt}{\log t}\right)\\
&=O\left((1/A+1/B)x^{3/2}+\frac{1}{AB}x^{5/2}\right),
\end{aligned}$$

which gives us

$$\begin{aligned}
\frac{1}{4AB}\sum_{\substack{|a|\leq A\\|b|\leq B}}\pi_0(P,E_{a,b},x)=&\frac{1}{2}\sum_{3<p\leq x,p\in P}\frac{H(-4p)}{p}\\
&+O\left((1/A+1/B)x^{3/2}+\frac{1}{AB}x^{5/2}+\log\log x\right).
\end{aligned}$$

Using the Dirichlet class number formula in conjunction with (2.1) gives:

$$\begin{aligned}
\frac{1}{2}H(-4p)&=\sum_{\substack{f=1,2\\d\equiv 0,1(4)}}\frac{w(d)\sqrt{|d|}L(1,\chi_d)}{w(d)2\pi}\\
&=\sum_{\substack{f=1,2\\d\equiv 0,1(4)}}\frac{\sqrt{|-4p/f^2|}L(1,\chi_d)}{2\pi}\\
&=\sum_{\substack{f=1,2\\d\equiv 0,1(4)}}\frac{\sqrt{p}L(1,\chi_d)}{f\pi}\\
&=\frac{1}{\pi}\sum_{\substack{f=1,2\\d\equiv 0,1(4)}}\frac{1}{f}\sqrt{p}L(1,\chi_d).
\end{aligned}$$

We thus substitute in for $H(-4p)$ to get

$$\frac{1}{2}\sum_{3<p\leq x,p\in P}\frac{H(-4p)}{p}=\frac{1}{\pi}\left(\sum_{f=1,2}\frac{1}{f}\sum_{p\in\delta_f(x),p\in P}\frac{L(1,\chi_d)}{\sqrt{p}}\right). \tag{2.4}$$

Partial summation for

$$\sum_{f=1,2}\frac{1}{f}\sum_{\substack{p\in\delta_f(x)\\ p\in P}}\frac{L(1,\chi_d)}{\sqrt{p}}$$

gives us

$$\frac{1}{\sqrt{x}\log x}\sum_{f=1,2}\frac{1}{f}\sum_{p\in\delta_f(x),p\in P}L(1,\chi_d)\log p$$
$$-\int_2^x\sum_{f=1,2}\left(\frac{1}{f}\sum_{p\in\delta_f(x),p\in P}L(1,\chi_d)\log p\right)\frac{d}{dt}\left(\frac{1}{\sqrt{t}\log t}\right)dt. \tag{2.5}$$

At this point we need

Theorem 2.12.

$$\sum_{f=1,2}\frac{1}{f}\sum_{\substack{p\in\delta_f(x)\\ p\in P}}L(1,\chi_d)\log p = K_P x + O\left(\frac{x}{\log^C x}\right) \tag{2.6}$$

where K_P is a constant depending only on P.

Proof. Using the series expression for the L-function and applying the Polya-Vinogradov inequality, we obtain

$$\begin{aligned}L(1,\chi_d) &= \sum_{n\geq 1}\left(\frac{d}{n}\right)\frac{1}{n}\\ &= \sum_{n\leq U}\left(\frac{d}{n}\right)\frac{1}{n}+O\left(\frac{\sqrt{|d|}\log|d|}{U}\right)\end{aligned}$$

for some positive parameter $U = U(x)$. To assess the overall contribution of the error

term above, we observe

$$\begin{aligned}
&\sum_{f=1,2}\frac{1}{f}\sum_{p\in\delta_f(x),p\in P}O\left(\frac{\sqrt{p}\log p}{U}\right)\log p\\
=&O\left(\sum_{p\leq x}\frac{\sqrt{p}\log^2 p}{U}\right)\\
=&O\left(\frac{1}{U}\int_2^x\sqrt{t}\log^2 t\frac{dt}{\log t}\right)\\
=&O\left(\frac{x^{3/2}\log x}{U}\right).
\end{aligned}$$

Thus the left-hand side of (2.6) becomes

$$\sum_{f=1,2}\frac{1}{f}\sum_{n\leq U}\frac{1}{n}\sum_{p\in\delta_f(x),p\in P}\left(\frac{d}{n}\right)\log p+O\left(\frac{x^{3/2}\log x}{U}\right). \tag{2.7}$$

We shall now consider the cases $f=1$ and $f=2$ separately.

2.3.2.1 The case $f=1$

This implies that $d=-4p$ and so we have

$$\begin{aligned}
\sum_{n\leq U}\frac{1}{n}\sum_{p\in\delta_1(x),p\in P}\left(\frac{d}{n}\right)\log p&=\sum_{n\leq U}\frac{1}{n}\sum_{p\in\delta_1(x),p\in P}\left(\frac{-4p}{n}\right)\log p\\
&=\sum_{odd\ n\leq U}\frac{1}{n}\sum_{p\in\delta_1(x),p\in P}\left(\frac{-p}{n}\right)\log p
\end{aligned} \tag{2.8}$$

where we noted that for even n the Jacobi symbol will be zero, and so the outer sum can be restricted to odd n.

At this point we introduce the notation $a(n)^*$, which when used with a sum will signify that we are summing over all the invertible elements of $\mathbb{Z}/n\mathbb{Z}$.

For the inner sum, in grouping the Jacobi symbols according to congruence conditions on p we get

$$\sum_{b(n)^*}\left(\frac{b}{n}\right)\sum_{\substack{p\in\delta_1(x)\\p\in P\\-p\equiv b(n)}}\log p,$$

which we rewrite as

$$\begin{aligned}
&\sum_{b(n)^*}\left(\frac{b}{n}\right)\sum_{\substack{3<p\leq x\\ p\in P\\ p\equiv -b(n)}}\log p\\
=&\sum_{b(n)^*}\left(\frac{b}{n}\right)\left(\sum_{\substack{p\leq x\\ p\in P\\ p\equiv -b(n)}}\log p+O\left(1\right)\right)\\
=&\sum_{b(n)^*}\left(\frac{b}{n}\right)\left(\sum_{\substack{p\leq x\\ p\in P\\ p\equiv -b(n)}}\log p\right)+O\left(\varphi(n)\right)
\end{aligned}$$

where the error term arises from including primes 2 and 3 in the sum.

We note that the overall contribution of the error term above is

$$\begin{aligned}
&O\left(\sum_{n\leq U}\frac{1}{n}\varphi(n)\right)\\
=&O\left(\sum_{n\leq U}1\right)\\
=&O\left(U\right).
\end{aligned}$$

Now we will need (see p169 of [Dav])

Theorem 2.13. *(Gallagher) Given $(a,n)=1$, let*

$$\begin{aligned}
\psi(x,n,a)&=\sum_{p\leq x,p\equiv a(n)}\log p\\
E(x,n,a)&=\psi(x,n,a)-\frac{x}{\varphi(n)}.
\end{aligned}$$

Then for any $C>0$, and Q such that $x/\log^C x\leq Q\leq x$

$$\sum_{n\leq Q}\sum_{a(n)*}E^2(x,n,a)\ll Qx\log x.$$

So we have

$$\sum_{odd\ n\leq U}\frac{1}{n}\sum_{b(n)^*}\left(\frac{b}{n}\right)\sum_{\substack{p\leq x\\ p\in P\\ p\equiv -b(n)}}\log p. \tag{2.9}$$

At this point we replace $p\in P$ by the congruence condition $p\equiv c(m)$. Define $k(n)$ to be the greatest common factor of m and n. When it is clear from context, we will suppress the variable and write k for $k(n)$. Thus (2.9) becomes

$$\sum_{odd\ n\leq U}\frac{1}{n}\sum_{\substack{b(n)^*\\ -b\equiv c(k)}}\left(\frac{b}{n}\right)\sum_{p\equiv -b'(mn/k)}\log p$$

where $-b'$ is the unique element of $\mathbb{Z}/\left(mn/k\right)\mathbb{Z}$ that satisfies $-b'\equiv -b(n)$ and $-b'\equiv c(m)$, by the Chinese remainder theorem.

Using the notation in the theorem, we rewrite the third sum

$$\begin{aligned}&\sum_{odd\ n\leq U}\frac{1}{n}\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)\left(\frac{x}{\varphi(\frac{mn}{k})}+E\left(x,\frac{mn}{k},-b'\right)\right)\\ =&x\sum_{odd\ n\leq U}\frac{1}{n}\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)\frac{1}{\varphi(\frac{mn}{k})}+\sum_{odd\ n\leq U}\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\frac{1}{n}\left(\frac{b}{n}\right)E\left(x,\frac{mn}{k},-b'\right).\end{aligned} \tag{2.10}$$

We consider the second term in (2.10) and use Cauchy-Schwarz to obtain a bound of

$$\begin{aligned}&\left(\sum_{odd\ n\leq U}\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\frac{1}{n^2}\right)^{1/2}\left(\sum_{odd\ \leq U}\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}E^2\left(x,\frac{mn}{k},-b'\right)\right)^{1/2}\\ \leq&\left(\sum_{n\leq U}\sum_{b(n)^*}\frac{1}{n^2}\right)^{1/2}\left(\sum_{n\leq U}\sum_{b'(mn/k)^*}E^2\left(x,\frac{mn}{k},-b'\right)\right)^{1/2}\end{aligned}$$

$$\leq \left(\sum_{n\leq U}\frac{\varphi(n)}{n^2}\right)^{1/2}\left(\sum_{n\leq U}\sum_{b'(mn/k)^*}E^2\left(x,\frac{mn}{k},-b'\right)\right)^{1/2}$$
$$\leq \left(\sum_{n\leq U}\frac{1}{n}\right)^{1/2}\left(\sum_{n\leq U}\sum_{b'(mn/k)^*}E^2\left(x,\frac{mn}{k},-b'\right)\right)^{1/2}$$
$$\leq (\log U+1)^{1/2}\left(\sum_{n\leq U}\sum_{b'(mn/k)^*}E^2\left(x,\frac{mn}{k},-b'\right)\right)^{1/2}.$$

This puts us in a position to use the theorem by Gallagher (setting $Q = U$), and so obtaining the asymptotic bound

$$\ll (\log U+1)^{1/2}(Ux\log x)^{1/2}$$
$$\ll (Ux\log U\log x)^{1/2},$$

and for

$$U \leq \frac{x}{\log^{2C+5}x}$$

we have

$$(Ux\log U\log x)^{1/2} \ll \frac{x}{\log^{C}x}.$$

We now consider the first expression in (2.10):

$$x\sum_{odd}\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)\frac{1}{\varphi(\frac{mn}{k})}$$

In order to interpret this, we will start with a lemma.

Lemma 2.14. *Given that* $(n,m) = k$,

$$\varphi\left(\frac{nm}{k}\right) = \frac{\varphi(n)\varphi(m)}{\varphi(k)}.$$

Proof. Write $k = p_1^{\alpha_1}\dots p_l^{\alpha_l}$. Thus $p_i^{\alpha_i}|n,m$ but either $p_i^{\alpha_i}\nmid u$ or $p_i^{\alpha_i}\nmid n$ (otherwise the

greatest common denominator of m and n would be larger than k). Thus given any p_i, either $p_i \nmid (n/p_i^{\alpha_i})$ or $p_i \nmid (m/p_i^{\alpha_i})$.

We consider this for each prime divisor of k, and obtain the result

$$p_1, \ldots, p_q \nmid \frac{n}{p_1^{\alpha_1} \ldots p_q^{\alpha_q}} =: n' \tag{2.11}$$

and

$$p_{q+1}, \ldots, p_l \nmid \frac{m}{p_{q+1}^{\alpha_{q+1}} \ldots p_l^{\alpha_l}} =: m' \tag{2.12}$$

where we have relabelled the primes appropriately.

Note that there are no common factors of n' and m' otherwise they would also divide k, which would be in contradiction to the prime decomposition of k. Thus $(n', m') = 1$, and note that $n'm' = nm/k$.

So

$$\varphi\left(\frac{nm}{k}\right) = \varphi(n'm') = \varphi(n')\varphi(m').$$

Split up k:

$$k = p_1^{\alpha_1} \ldots p_q^{\alpha_q} \cdot p_{q+1}^{\alpha_{q+1}} \ldots p_l^{\alpha_l} = a' \cdot b'.$$

Now $(a', b') = 1$, furthermore $(a', n') = 1$ and $(b', m') = 1$, using (2.11) and (2.12), so we have

$$\begin{aligned}\varphi(k)\varphi\left(\frac{nm}{k}\right) =& \varphi(a')\varphi(b')\varphi(m')\varphi(n') \\ =& \varphi(a'n')\varphi(b'm') \\ =& \varphi(n)\varphi(m),\end{aligned}$$

which proves our lemma. □

We apply this to the first expression in (2.10) to get

$$x \sum_{odd\ n \le U} \frac{1}{n} \sum_{\substack{b(n)^* \\ b \equiv -c(k)}} \left(\frac{b}{n}\right) \frac{1}{\varphi(m)\varphi(n)/\varphi(k)}$$

$$= \frac{x}{\varphi(m)} \sum_{odd\ n \le U} \left(\sum_{\substack{b(n)^* \\ b \equiv -c(k)}} \left(\frac{b}{n}\right) \frac{1}{(n\varphi(n)/\varphi(k))} \right). \tag{2.13}$$

Now we consider

$$\sum_{\substack{b(n)^* \\ b \equiv -c(k)}} \left(\frac{b}{n}\right). \tag{2.14}$$

Since $k|n$, write $n = lk$ (note that $k|l$ only if $k \nmid \frac{m}{k}$).

We have (given the conditions of the sum above)

$$\left(\frac{b}{n}\right) = \left(\frac{b}{lk}\right) = \left(\frac{b}{l}\right)\left(\frac{b}{k}\right) = \left(\frac{b}{l}\right)\left(\frac{c}{k}\right)$$

and so (2.14) becomes

$$\left(\frac{c}{k}\right) \sum_{\substack{b(n)^* \\ b \equiv -c(k)}} \left(\frac{b}{l}\right). \tag{2.15}$$

Decompose l into its prime factors as $(p_1^{\alpha_1} \dots p_l^{\alpha_l}).(p_{l+1}^{\alpha_{l+1}} \dots p_q^{\alpha_q})$, where $p_1, \dots, p_l | k$ and $p_{l+1}, \dots, p_q \nmid k$. Let $l_k = p_1^{\alpha_1} \dots p_l^{\alpha_l}$ and $l_s = p_{l+1}^{\alpha_{l+1}} \dots p_q^{\alpha_q}$.

Then

$$\left(\frac{b}{l}\right) = \left(\frac{-c}{p_1}\right)^{\alpha_l} \dots \left(\frac{-c}{p_l}\right)^{\alpha_l} \left(\frac{b}{p_{l+1}^{\alpha_{l+1}} \dots p_q^{\alpha_q}}\right)$$

and so (2.15) becomes

$$\left(\frac{-c}{k}\right)\left(\frac{-c}{p_{l+1}^{\alpha_{l+1}}\dots p_q^{\alpha_q}}\right)\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{l}\right)$$
$$=\left(\frac{-c}{l_k}\right)\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{l_s}\right).$$

Lemma 2.15. *If l_s is a square, then*

$$\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{l_s}\right)=\frac{\varphi(n)}{\varphi(k)} \tag{2.16}$$

otherwise the sum takes the value zero.

Proof. When l_s is a square, we have

$$\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{l_s}\right)=\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}1$$
$$=\frac{\varphi(n)}{\varphi(k)}.$$

If on the other hand if l_s is not a square, write $l_s = q_1\cdot\dots\cdot q_w\cdot h^2$, where the q_i are odd primes (n is odd so l_s is also odd). Then

$$\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{l_s}\right)=\sum_{\substack{b(n)^*\\ b\equiv -c(k)}}\left(\frac{b}{q_1}\right)\dots\left(\frac{b}{q_w}\right)\cdot\left(\frac{b}{h}\right)^2$$
$$=\frac{\varphi(n)}{\varphi(k)\varphi(q_1\dots q_w)}\sum_{b(q_1\dots q_w)^*}\left(\frac{b}{q_1}\right)\dots\left(\frac{b}{q_w}\right),$$

which by the Chinese remainder theorem gives us

$$\frac{\varphi(n)}{\varphi(k)\varphi(q_1\dots q_w)}\left(\sum_{b(q_1)^*}\left(\frac{b}{q_1}\right)\right)\dots\left(\sum_{b(q_w)^*}\left(\frac{b}{q_w}\right)\right)$$

and we have that

$$\sum_{b(q_1)^*} \left(\frac{b}{q_1}\right) = 0,$$

so the left-hand side of (2.16) is zero.

□

Applying all this to (2.13) we have

$$\begin{aligned}\frac{x}{\varphi(m)} \sum_{\text{odd } n\leq U} \left(\sum_{\substack{b(n)^* \\ b\equiv -c(k)}} \left(\frac{b}{n}\right) \frac{1}{n\varphi(n)/\varphi(k)} \right) =& \frac{x}{\varphi(m)} \sum_{\substack{\text{odd } n\leq U \\ l_s \text{ a square}}} \left(\left(\frac{-c}{kl_k}\right) \frac{\varphi(n)/\varphi(k)}{n\varphi(n)/\varphi(k)} \right) \\ =& \frac{x}{\varphi(m)} \sum_{\substack{\text{odd } n\leq U \\ l_s \text{ a square}}} \left(\frac{-c}{kl_k}\right) \frac{1}{n}.\end{aligned}$$

Now we want to split up this sum according to the different values of k. In order to do so, we first need to extend the range of summation:

$$\begin{aligned}\frac{x}{\varphi(m)} \sum_{\substack{\text{odd } n\leq U \\ l_s \text{ a square}}} \left(\frac{-c}{kl_k}\right) \frac{1}{n} =& \frac{x}{\varphi(m)} \sum_{\substack{\text{odd } n\geq 1 \\ l_s \text{ a square}}} \left(\frac{-c}{kl_k}\right) \frac{1}{n} \\ &+ \frac{x}{\varphi(m)} \cdot O\left(\sum_{\substack{\text{odd } n\geq U \\ l_s \text{ a square}}} \frac{1}{n} \right).\end{aligned}$$

Fix the parameter U as $\sqrt{x}\log^{C+1} x$ and note that this gives

$$\begin{aligned}\frac{x}{\varphi(m)} \cdot O\left(\sum_{\substack{\text{odd } n\geq U \\ l_s \text{ a square}}} \frac{1}{n} \right) =& O\left(x \sum_{\text{odd square } n\geq U} \frac{1}{n} \right) \\ =& O\left(\frac{x}{U}\right) \\ =& O\left(\frac{\sqrt{x}}{\log^{C+1}}\right),\end{aligned}$$

where the first equality follows because

$$\sum_{\substack{n\leq U\\ l_s \text{ a square}}} \frac{1}{n}$$

is equal to

$$\prod_{p|m}\left(1-p^{-1}\right)^{-1}\sum_{l_s\geq 1}\frac{1}{l_s^2}.$$

Now we can split the main term into a double sum

$$\frac{x}{\varphi(m)}\sum_{\substack{\text{odd } n\geq 1\\ l_s \text{ a square}}}\left(\frac{-c}{kl_k}\right)\frac{1}{n}=\frac{x}{\varphi(m)}\sum_{\text{odd } k|m}\sum_{\substack{\text{odd } m\geq 1\\ l_s \text{ a square}\\ (m,m/k)=1}}\left(\frac{-c}{kl_k}\right)\frac{1}{mk} \tag{2.17}$$

where the coprime condition on m arises from the fact that we have $k=(n,m)$, which is equivalent to $(n/k,m/k)=1$, which in turn is equivalent to $(l,m/k)=1$. Note that the first sum is over all divisors of m, including 1 and m.

In order to interpret this, we consider the possible values of the divisors l_k and l_s of l (recall that we have $l=l_kl_s$). In the first case, we note that primes p such that $p|k$ and $p\nmid m/k$ are exactly those primes that might divide l_k.

Thus we can re-express the sum of all the reciprocals of l_k:

$$\begin{aligned}\sum_{l_k}\frac{1}{l_k}&=\prod_{p|k,p\nmid m/k}\sum_{w=1}^{\infty}\frac{1}{p^w}\\ &=\prod_{p|k,p\nmid m/k}\left(1-\frac{1}{p}\right)^{-1}.\end{aligned}$$

And including the Jacobi symbol (which we need to do since it occurs in (2.17)),

$$\sum_{l_k}\frac{\left(\frac{-c}{l_k}\right)}{l_k}=\prod_{p|k,p\nmid m/k}\sum_{w=1}^{\infty}\frac{\left(\frac{-c}{p}\right)^w}{p^w}=\prod_{p|k,p\nmid m/k}\left(1-\frac{\left(\frac{-c}{p}\right)}{p}\right)^{-1}.$$

Now we address the second divisor of l. Recall that l_s is the largest divisor of l such that $(l_s, k) = 1$. We also have that $(l, m/k) = 1$ in the first sum of the right-hand side of (2.17), and so $(l_s, m/k) = 1$. Thus $(l_s, (u/k) \cdot k) = 1 \Rightarrow (l_s, m) = 1$.

So l_s is any square positive integer that satisfies $(l_s, m) = 1$ and therefore we can write

$$\sum_{\substack{\text{odd } l \geq 1 \\ (l_s, m)=1}} \frac{1}{l_s} = \zeta(2) \prod_{p|2m} \left(1 - \frac{1}{p^2}\right).$$

where p is a prime.

Putting all this together, we get that (2.8) is equal to

$$\frac{x}{\varphi(m)} \zeta(2) \prod_{p|2m} \left(1 - \frac{1}{p^2}\right) \sum_{\text{odd } k|m} \left(\frac{-c}{k}\right) \frac{1}{k} \prod_{p|k, p\nmid m/k} \left(1 - \frac{\left(\frac{-c}{p}\right)}{p}\right)^{-1} + O\left(\frac{x}{\log^C x}\right).$$

2.3.2.2 The case $f = 2$

From (2.7) for $f = 2$ we have

$$\frac{1}{2} \sum_{n \leq U} \frac{1}{n} \sum_{p \in \delta_2(x), p \in P} \left(\frac{d}{n}\right) \log p. \tag{2.18}$$

The inner sum of (2.18) can be decomposed as

$$\sum_{b(4n)} \left(\frac{b}{n}\right) \sum_{\substack{p \in \delta_f(x) \\ p \in P \\ d \equiv b(4n)}} \log p.$$

In this case we have that $d = -p \equiv 0, 1(4)$ and thus $p \equiv 3(4)$. So the expression above becomes

$$\sum_{b(4n)^*, b \equiv 1(4)} \left(\frac{b}{n}\right) \sum_{\substack{3 < p \leq x \\ p \in P \\ p \equiv -b(4n)}} \log p.$$

We put in an error term to account for summation over primes 2 and 3:

$$\sum_{n\leq U}\frac{1}{n}\sum_{b(4n)^*,b\equiv 1(4)}\left(\frac{b}{n}\right)\sum_{\substack{3<p\leq x\\ p\in P\\ p\equiv -b(4n)}}\log p \;=\sum_{n\leq U}\frac{1}{n}\sum_{b(4n)^*,b\equiv 1(4)}\left(\frac{b}{n}\right)\sum_{\substack{p\leq x\\ p\in P\\ p\equiv -b(4n)}}\log p+O\left(U\right)$$

Now at this point we will consider the odd and even cases of m separately.

I) **Odd** m

Given

$$\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv 1(4)}}\left(\frac{b}{n}\right)\sum_{\substack{p\leq x\\ p\in P\\ p\equiv -b(4n)}}\log p \tag{2.19}$$

again we write the condition $p\in P$ as the congruence condition $p\equiv c(m)$, and this time we define $k=(4n,m)$ to get

$$\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv 1(4)\\ -b\equiv c(k)}}\left(\frac{b}{n}\right)\sum_{p\equiv -b'(4mn/k)}\log p$$

where $-b'$ is the unique element in $\mathbb{Z}/(4nm/k)\mathbb{Z}$ such that $-b'\equiv -b(4n)$ and $-b'\equiv c(m)$ by the Chinese remainder theorem.

Note that we need $-b\equiv c(k)$ in the second sum so that the two initial congruence conditions are compatible.

As m is odd, k is also odd, and furthermore $k=(4n,m)=(n,m)$. Since $(k,4)=1$, we use the Chinese remainder theorem to combine the conditions of the second sum, namely $b\equiv 1(4)$ and $b\equiv -c(k)$, into $b\equiv -c'(4k)$, for some unique $c'\in\mathbb{Z}/4k\mathbb{Z}$.

We re-express the third sum in the expression above:

$$\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv -c'(4k)}}\left(\frac{b}{n}\right)\left(\frac{x}{\varphi(\frac{4nm}{k})}+E\left(x,\frac{4nm}{k},-b'\right)\right)$$

$$=\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv -c'(4k)}}\left(\frac{b}{n}\right)\left(\frac{x}{\varphi(\frac{4nm}{k})}\right)+\sum_{n\leq U}\sum_{\substack{b(4n)^*\\ b\equiv -c'(4k)}}\frac{1}{n}\left(\frac{b}{n}\right)E\left(x,\frac{4nm}{k},-b'\right) \tag{2.20}$$

We consider the second expression on the right-hand side of (2.20) and using Cauchy-Schwarz we bound it with

$$\left(\sum_{n\leq U}\sum_{\substack{b(4n)^*\\ b\equiv -c'(4k)}}\frac{1}{n^2}\right)^{1/2}\left(\sum_{n\leq U}\sum_{\substack{b(4n)^*\\ b\equiv -c'(4k)}}E^2\left(x,\frac{4mn}{k},b'\right)\right)^{1/2}$$

$$\leq\left(\sum_{n\leq U}\sum_{b(4n)^*}\frac{1}{n^2}\right)^{1/2}\left(\sum_{n\leq U}\sum_{-b'(4mn/k)^*}E^2\left(x,\frac{4mn}{k},-b'\right)\right)^{1/2}$$

$$\leq\left(\sum_{n\leq U}\frac{\varphi(4n)}{n^2}\right)^{1/2}\left(\sum_{n\leq U}\sum_{-b'(4mn/k)^*}E^2\left(x,\frac{4mn}{k},-b'\right)\right)^{1/2}$$

$$\leq\left(\sum_{n\leq U}\frac{4}{n}\right)^{1/2}\left(\sum_{n\leq U}\sum_{-b'(4mn/k)^*}E^2\left(x,\frac{4mn}{k},-b'\right)\right)^{1/2}$$

$$\leq 2\left(\log U+1\right)^{1/2}\left(\sum_{n\leq U}\sum_{-b'(4mn/k)^*}E^2\left(x,\frac{4mn}{k},-b'\right)\right)^{1/2}.$$

Applying the theorem by Gallagher, we obtain the asymptotic bound

$$\ll\left(\log U+1\right)^{1/2}\left(Ux\log x\right)^{1/2}$$

$$\ll\left(Ux\log U\log x\right)^{1/2}$$

and since $U = \sqrt{x}/\log^{C+1} x$ we have

$$(Ux \log U \log x)^{1/2} \ll \frac{x}{\log^C x}.$$

Now consider the first term in (2.20). Noting that lemma 2.14 implies

$$\varphi\left(\frac{4n.m}{k}\right) = \frac{\varphi(4n)\varphi(m)}{\varphi(k)},$$

we apply this to get

$$\frac{x}{\varphi(m)} \sum_{n \leq U} \sum_{\substack{b(4n)^* \\ b \equiv -c'(4k)}} \frac{1}{n} \left(\frac{b}{n}\right) \frac{1}{\varphi(4n)/\varphi(k)}. \tag{2.21}$$

Since $k = (n, m)$, we write $n = lk$ and observe that

$$\begin{aligned} \sum_{\substack{b(4n)^* \\ b \equiv -c'(4k)}} \left(\frac{b}{n}\right) &= \sum_{\substack{b(4n)^* \\ b \equiv -c'(4k)}} \left(\frac{b}{l}\right)\left(\frac{b}{k}\right) \\ &= \left(\frac{-c'}{k}\right) \sum_{\substack{b(4n)^* \\ b \equiv -c'(4k)}} \left(\frac{b}{l}\right). \end{aligned}$$

As before we decompose l into two factors l_k and l_s, so we get

$$\left(\frac{-c'}{k}\right)\left(\frac{-c'}{l_k}\right) \sum_{\substack{b(4n)^* \\ b \equiv -c'(4k)}} \left(\frac{b}{l_s}\right).$$

Lemma 2.16.

$$\sum_{\substack{b(4n)^* \\ b \equiv -c'(4k)}} \left(\frac{b}{l_s}\right)$$

is equal to $\varphi(4n)/\varphi(4k)$ if l_s is a square, and zero otherwise.

Proof. We split up n, l_s, and k into their odd and even parts and so write $n = 2^\alpha n'$,

$l_s = 2^\beta l'_s$, $k = 2^\gamma k'$. We have

$$\sum_{\substack{b(4n)^* \\ b\equiv -c'(4k)}} \left(\frac{b}{l_s}\right) = \sum_{\substack{b(4\cdot 2^\alpha n')^* \\ b\equiv -c'(4\cdot 2^\beta k')}} \left(\frac{b}{2^\beta}\right)\left(\frac{b}{l'_s}\right)$$

and by the Chinese remainder theorem

$$\sum_{\substack{b(4\cdot 2^\alpha)^* \\ b\equiv -c'(4\cdot 2^\beta k')}} \left(\frac{b}{2^\beta}\right) \sum_{\substack{b(n')^* \\ b\equiv -c'(k')}} \left(\frac{b}{l'_s}\right).$$

So if l'_s is a square, then the inner sum will have value $\varphi(n')/(k')$, whereas if it is not a square, then lemma 2.15 implies that the inner sum is zero.

For the l'_s square case, we now have to consider

$$\sum_{\substack{b(4\cdot 2^\alpha)^* \\ b\equiv -c'(4\cdot 2^\beta k')}} \left(\frac{b}{2^\beta}\right).$$

If β is even, then the sum has value $\varphi(4\cdot 2^\beta)/\varphi(4\cdot 2^\gamma)$ and so overall for square l_s we get

$$\frac{\varphi(4\cdot 2^\beta)}{\varphi(4\cdot 2^\gamma)} \cdot \frac{\varphi(n')}{(k')} = \frac{\varphi(4n)}{\varphi(4k)}.$$

If β is odd, then l_s must be even. Thus since k and l_s are coprime, we have that k is odd and thus $\gamma = 0$. This leaves us with having to consider

$$\sum_{\substack{b(4\cdot 2^\alpha)^* \\ b\equiv 1(4)}} \left(\frac{b}{2}\right).$$

Note that $\alpha \geq \beta$, and since $\beta \geq 1$ we have

$$\sum_{\substack{b(8\cdot 2^{\alpha-1})^* \\ b\equiv 1(4)}} \left(\frac{b}{2}\right),$$

so we are summing $2^{\alpha-1}$ pairs of elements where the first in the pair is congruent to 1 (mod 8) and the second to 5 (mod 8). Thus the Jacobi symbols of each pair will cancel out, giving us a value of zero for the sum.

We put all the above together to get that the sum in the statement of the lemma is equal to $\varphi(4n)/\varphi(4k)$ if and only if l_s is a square. □

Remark 11. This lemma also applies for even values of m, provided that we alter the value of k suitably. Therefore this result will be also used in the even case.

So (2.20) is equal to

$$\begin{aligned}&\frac{x}{\varphi(m)}\sum_{\substack{n\leq U\\ l_s \text{ a square}}}\left(\frac{-c'}{kl_k}\right)\frac{\varphi(4n)}{\varphi(4k)}\frac{1}{n\varphi(4n)/\varphi(k)}\\ =&\frac{x}{\varphi(m)}\frac{1}{2}\sum_{\substack{n=1\\ l_s \text{ a square}}}^{\infty}\left(\frac{-c'}{kl_k}\right)\frac{1}{n}+O\left(\frac{x}{\varphi(m)}\frac{1}{2}\sum_{\substack{n\geq U\\ n \text{ a square}}}\frac{1}{n}\right)\end{aligned}\tag{2.22}$$

where we have used the fact that m is odd and thus k is odd, implying that $\varphi(4k) = 2\varphi(k)$.

We consider the error term and note that

$$\begin{aligned}O\left(\frac{x}{\varphi(m)}\frac{1}{2}\sum_{\substack{n\geq U\\ n \text{ a square}}}\frac{1}{n}\right)=&O\left(x.\frac{1}{U}\right)\\ =&O\left(\frac{x}{\sqrt{x}\log^{C+1}x}\right)\\ =&O\left(\frac{\sqrt{x}}{\log^{C+1}x}\right).\end{aligned}$$

So we take the first term from (2.22) and re-express it as a double sum:

$$\frac{x}{2\varphi(m)}\sum_{k|m}\sum_{\substack{l\geq 1\\ l_s \text{ a square}\\ (l,m/k)=1}}\left(\frac{-c'}{kl_k}\right)\frac{1}{lk}.\tag{2.23}$$

As before, l_k can be any positive integer composed of exactly those primes p that satisfy

$p|k$ and $p \nmid (m/k)$. Thus we get

$$\sum_{l_k} \left(\frac{-c'}{l_k}\right) \frac{1}{l_k} = \prod_{p|k, p\nmid m/k} \sum_{w=1}^{\infty} \left(\frac{-c'}{p}\right) \frac{1}{p^w}$$
$$= \prod_{p|k, p\nmid m/k} \left(1 - \left(\frac{-c'}{p}\right) \frac{1}{p}\right)^{-1}$$

and since $c \equiv c'(k)$ and k is odd, this is equivalent to

$$\prod_{p|k, p\nmid m/k} \left(1 - \frac{\left(\frac{-c}{p}\right)}{p}\right)^{-1}.$$

Now recall that l_s is any square positive integer that satisfies $(l_s, m) = 1$, and we therefore have (for l a prime)

$$\sum_{\substack{l \geq 1 \\ (l_s, m)=1}} \frac{1}{l_s} = \zeta(2) \prod_{p|m} \left(1 - \frac{1}{p^2}\right).$$

We put all this together to get that (2.18) is equal to

$$\frac{x}{4\varphi(m)} \zeta(2) \left(\prod_{p|m} \left(1 - \frac{1}{p^2}\right)\right) \left(\sum_{k|m} \left(\frac{-c}{k}\right) \prod_{p|k, p\nmid m/k} \left(1 - \frac{\left(\frac{-c}{p}\right)}{p}\right)^{-1}\right) + O\left(\frac{x}{\log^C x}\right).$$

II) **Even** m

If m is only divisible by 2 once, i.e., if we are given a congruence condition of the form $p \equiv c(m)$ where $m = 2m'$ for m' odd, then this can be decomposed into the conditions $p \equiv c(m')$ and $p \equiv 1(2)$ (since $(c, m) = 1$ by assumption) and thus the second condition can basically be ignored — all it does is exclude the prime 2, and thus does not affect the asymptotic expression. So we can assume that $4|m$.

We start with

$$\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv 1(4)}}\left(\frac{b}{n}\right)\sum_{\substack{p\leq x\\ p\equiv -b(4n)\\ p\in P}}\log p.$$

Again we let P be defined by the congruence condition $p\equiv c(m)$, and we set $k=(4n,m)$:

$$\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv 1(4)\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)\sum_{p\equiv -b'(4mn/k)}\log p$$

with b' defined as before.

Note that m is even and furthermore is divisible by 4, so k is also divisible by 4. We consider whether the congruence conditions in the second sum are indeed compatible, i.e., whether $-c\equiv 1(4)$.

If this is not satisfied, then there is no contribution to the asymptotic from the $f=2$ case.

If this is satisfied, then we can omit the condition $b\equiv 1(4)$ as it is included in the $b\equiv -c(k)$ condition. We proceed with this case.

We rewrite the third sum in the expression above to get

$$\begin{aligned}&\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)\left(\frac{x}{\varphi(\frac{4nm}{k})}+E\left(x,\frac{4nm}{k},-b'\right)\right)\\ =&\sum_{n\leq U}\frac{1}{n}\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)\left(\frac{x}{\varphi(\frac{4nm}{k})}\right)+\sum_{n\leq U}\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\frac{1}{n}\left(\frac{b}{n}\right)E\left(x,\frac{4nm}{k},-b'\right).\end{aligned}\tag{2.24}$$

The second term above can be bounded with the use of Cauchy-Schwarz and the theorem by Gallagher, as before, to give that

$$\sum_{n\leq U}\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\frac{1}{n}\left(\frac{b}{n}\right)E\left(x,\frac{4nm}{k},-b'\right)\ll\frac{x}{\log^C x}$$

given that U is set as $\sqrt{x}\log^{C+1}x$.

We apply lemma 2.14 to the main term in (2.24) to get

$$\frac{x}{\varphi(m)}\sum_{n\leq U}\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)\frac{1}{n\varphi(4n)/\varphi(k)}. \tag{2.25}$$

Since $k=(4n,m)$, let us write $k'=k/4$, where k' will be an integer. So $k'=(n,m/4)$. Note that $m/4$ and thus k' may still be even.

So $(n,m/4)=k'$ and thus let us write $n=k'.l$. Now

$$\left(\frac{b}{n}\right)=\left(\frac{b}{k'}\right)\left(\frac{b}{l}\right)=\left(\frac{-c}{k'}\right)\left(\frac{b}{l}\right)$$

and so

$$\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\left(\frac{b}{n}\right)=\left(\frac{-c}{k'}\right)\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\left(\frac{b}{l}\right).$$

Split l into the two factors $l_{k'}$ and l'_s, where k' is as before, and $l_{s'}$ is the largest factor of l that is coprime to k'. We get

$$\left(\frac{-c}{k'}\right)\left(\frac{-c}{l_{k'}}\right)\sum_{\substack{b(4n)^*\\ b\equiv -c(k)}}\left(\frac{b}{l_{s'}}\right)$$

and applying lemma 2.16, we see that this equals

$$\left(\frac{-c}{k'l_{k'}}\right)\frac{\varphi(4n)}{\varphi(k)}$$

if $l_{s'}$ is a square, and zero otherwise.

Therefore (2.25) is equal to

$$\frac{x}{\varphi(m)} \sum_{\substack{n\leq U \\ l_s \text{ a square}}} \left(\frac{-c}{k'l_{k'}}\right) \frac{\varphi(4n)}{\varphi(k)} \frac{1}{n\varphi(4n)/\varphi(k)}$$

$$= \frac{x}{\varphi(m)} \sum_{\substack{n=1 \\ l_s \text{ a square}}}^{\infty} \left(\frac{-c}{k'l_{k'}}\right) \frac{1}{n} + O\left(\frac{x}{\varphi(m)} \frac{1}{2} \sum_{\substack{n\geq U \\ n \text{ a square}}} \frac{1}{n}\right) \tag{2.26}$$

and again the error term can be replaced by

$$O\left(\frac{\sqrt{x}}{\log^{C+1} x}\right).$$

The main term of (2.26) can now be re-expressed as

$$\frac{x}{\varphi(m)} \sum_{k'|m/4} \sum_{\substack{l\geq 1 \\ l_s \text{ a square} \\ (l,m/k)=1}} \left(\frac{-c}{k'l_{k'}}\right) \frac{1}{lk'}$$

$$= \frac{x}{\varphi(m)} \sum_{k|m} \left(\frac{-c}{k'}\right) \frac{1}{k'} \sum_{\substack{l\geq 1 \\ l_s \text{ a square} \\ (l,m/k)=1}} \left(\frac{-c}{l_{k'}}\right) \frac{1}{l}, \tag{2.27}$$

where we have noted that the condition $k'|(m/4)$ in the first sum is equivalent to the condition $k|u$.

Now l_k can be any positive integer composed of exactly those primes p that satisfy $p|k'$ and $p \nmid (m/k)$. Thus we get

$$\sum_{l_k} \left(\frac{-c}{l_k}\right) \frac{1}{l_k} = \prod_{p|k, p\nmid m/k} \sum_{w=1}^{\infty} \left(\frac{-c}{p}\right) \frac{1}{p^w}$$

$$= \prod_{p|k, p\nmid m/k} \left(1 - \left(\frac{-c}{p}\right) \frac{1}{p}\right)^{-1}.$$

Given that l_s is any square positive integer that satisfies $(l_s, m/4k') = 1$ and $(l_s, k') = 1$,

together these are equivalent to $(l_s, m/4) = 1$, so we have

$$\sum_{\substack{l\geq 1\\(l_s,m/4)=1}} \frac{1}{l_s} = \zeta(2) \prod_{p|m/4} \left(1 - \frac{1}{p^2}\right).$$

Thus for the even case we have that (2.7) is equal to

$$\frac{x}{2\varphi(m)}\zeta(2) \left(\prod_{p|m/4} \left(1 - \frac{1}{p^2}\right)\right) \left(\sum_{k'|m/4} \left(\frac{-c}{k'}\right) \frac{1}{k'} \prod_{p|k', p\nmid m/k} \left(1 - \frac{\left(\frac{-c}{p}\right)}{p}\right)^{-1}\right).$$

So we have proved that

$$\sum_{f=1,2} \frac{1}{f} \sum_{\substack{p\in\delta_f(x)\\p\in P}} L(1,\chi_d)\sqrt{p}\log p = K_P x + O\left(\frac{x}{\log^C x}\right)$$

for some constant K_P.

□

We apply the above to (2.5) to get

$$\frac{1}{\sqrt{x}\log x}\left(K_P x + O\left(\frac{x}{\log^C x}\right)\right) - \int_2^x \left(K_P t + O\left(\frac{t}{\log^C t}\right)\right)\left(\frac{1}{\sqrt{t}\log t}\right)' dt$$

and noting that

$$\left(\frac{1}{\sqrt{t}\log t}\right)' = -\frac{\frac{1}{2}\log t + 1}{t^{3/2}\log^2 t}$$

we obtain

$$\begin{aligned} &K_P \frac{\sqrt{x}}{\log x} + O\left(\frac{\sqrt{x}}{\log^{C+1} x}\right) + K_P \int_2^x \frac{1}{\sqrt{t}\log^2 t} dt \\ &+ K_P \int_2^x \frac{1}{2\sqrt{t}\log t} dt + O\left(\int_2^x \frac{1}{\sqrt{t}\log^{C+1} t}\right) \end{aligned}$$

and so we have

$$2K_P \frac{\sqrt{x}}{\log x} + o\left(\frac{\sqrt{x}}{\log x}\right).$$

We substitute back into (2.4) to get

$$\frac{1}{2}\sum_{3<p\leq x}\frac{H(-4p)}{p}=\frac{2}{\pi}K_P\frac{\sqrt{x}}{\log x}+o\left(\frac{\sqrt{x}}{\log x}\right) \tag{2.28}$$

and thus have $C_P=\frac{2}{\pi}K_P$.

2.3.3 The value of K_P

So for **odd m** we get

$$\begin{aligned}K_P=&\frac{1}{\varphi(m)}\zeta(2)\left(\prod_{p|2m}\left(1-\frac{1}{p^2}\right)\right)\sum_{k|m}\frac{1}{k}\left(\frac{-c}{k}\right)\prod_{p|k,p\nmid m/k}\left(1-\left(\frac{-c}{p}\right)\frac{1}{p}\right)^{-1}\\&+\frac{1}{4\varphi(m)}\zeta(2)\left(\prod_{p|m}\left(1-\frac{1}{p^2}\right)\right)\sum_{k|m}\frac{1}{k}\left(\frac{-c}{k}\right)\prod_{p|k,p\nmid m/k}\left(1-\left(\frac{-c}{p}\right)\frac{1}{p}\right)^{-1}\\=&\frac{1}{\varphi(m)}\zeta(2)\left(\prod_{p|m}\left(1-\frac{1}{p^2}\right)\right)\sum_{k|m}\frac{1}{k}\left(\frac{-c}{k}\right)\prod_{p|k,p\nmid m/k}\left(1-\left(\frac{-c}{p}\right)\frac{1}{p}\right)^{-1},\end{aligned}$$

and for **m divisible by 4** we get

$$\begin{aligned}K_P=&\frac{1}{\varphi(m)}\zeta(2)\left(\prod_{p|m}\left(1-\frac{1}{p^2}\right)\right)\sum_{\text{odd }k|m}\left(\frac{-c}{k}\right)\frac{1}{k}\prod_{p|k,p\nmid m/k}\left(1-\left(\frac{-c}{p}\right)\frac{1}{p}\right)^{-1}\\&+\frac{I(c)}{2\varphi(m)}\zeta(2)\left(\prod_{p|m/4}\left(1-\frac{1}{p^2}\right)\right)\sum_{k'|m/4}\left(\frac{-c}{k'}\right)\frac{1}{k'}\prod_{p|k',p\nmid m/k}\left(1-\left(\frac{-c}{p}\right)\frac{1}{p}\right)^{-1}\end{aligned}$$

where $I(c)=1$ if c is congruent to 3 (mod 4) and is zero otherwise.

2.4 Applications

2.4.1 Imaginary quadratic fields

Recall that, by way of example, we mentioned the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$ in the introduction (which is equivalent to setting $P = \{p \mid p \equiv 1 \pmod 3\}$). This gave us the asymptotic

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \pi_0(\mathbb{Q}(\sqrt{-3}), E_{a,b}, x) \sim \frac{\pi}{9} \frac{\sqrt{x}}{\log x}$$

for $A, B \geq x^{1/2+\epsilon}$ and $AB \geq x^{3/2+\epsilon}$.

Remark 12. For $P = \{p \text{ prime} \mid p \equiv 2 \pmod 3\}$ we have $C_P = 2\pi/9$, and thus it appears that the occurrence of supersingular primes $p \equiv 2 \pmod 3$ is significantly greater, whereas our heuristic does not distinguish between the constants for the $1 \pmod 3$ case and the $2 \pmod 3$ case.

In general, we have the following constants for imaginary quadratic fields $L = \mathbb{Q}(\sqrt{-q})$: if $q \equiv 3 \pmod 4$, then

$$C_L = \frac{\pi}{3} \cdot \frac{1}{2} \left(\frac{q-1}{q} \right),$$

whereas if $q \equiv 1 \pmod 4$, then

$$C_L = \frac{\pi}{3} \cdot \frac{1}{2} \left(\frac{q - \frac{1}{4}}{q} \right).$$

Remark 13. Thus for any imaginary quadratic field there is a bias against the occurrence of supersingular primes that split in that field.

2.4.2 Real quadratic fields

For $L = \mathbb{Q}(\sqrt{q})$, if $q \equiv 3 \pmod 4$,

$$C_L = \frac{\pi}{3} \cdot \frac{1}{2} \left(\frac{q + \frac{1}{4}}{q} \right),$$

whereas if $q \equiv 1 \pmod 4$, then

$$C_L = \frac{\pi}{3} \cdot \frac{1}{2} \left(\frac{q+1}{q} \right).$$

Remark 14. Here we observe a bias toward the occurrence of supersingular split primes. Note that these biases will still be present in the refined averaging of the next section.

Remark 15. We can summarise our results on quadratic fields of the form $L = \mathbb{Q}(\sqrt{\pm q})$ (where q is prime), as

$$C_L = \frac{\pi}{3} \cdot \frac{1}{2} \left(\frac{D+1}{D} \right)$$

where D is the discriminant of the quadratic field.

2.4.3 Cyclotomic fields

We could also take a cyclotomic field such as $\mathbb{Q}(\zeta_{15})$, in which case the set of split primes is $P = \{p \text{ prime} \mid p \equiv 1 \pmod{15}\}$, and so

$$\begin{aligned} K_P =& \frac{1}{8}\zeta(2) \left(1 - \frac{1}{9}\right) \left(1 - \frac{1}{25}\right) \left[1 - \frac{1}{4} + \frac{1}{4} + \frac{1}{16}\right] \\ =& \zeta(2)\frac{1}{10}, \\ \text{and so} \quad C_P =& \frac{1}{30}\pi. \end{aligned}$$

Thus

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \pi_0(P, E_{a,b}, x) \sim \frac{\pi}{3} \cdot \frac{1}{10} \left(\frac{4}{5}\right) \frac{\sqrt{x}}{\log x}$$

for $A, B \geq x^{1/2+\epsilon}$ and $AB \geq x^{3/2+\epsilon}$.

Remark 16. The sum of the C_P-coefficients for the various congruence relations modulo 15 is $\pi/3$, and thus the mean value is $\pi/24$, which is larger than the coefficient in the asymptotic above. So again it appears that we have a smaller than average occurrence of supersingular primes that split totally in the number field.

Remark 17. The bias in the distribution of supersingular primes, as seen in these examples, can be traced back to the L-functions of section 2.3. Consider the inner sum, for $f = 1$ say, of the right-hand side of equation (2.4) and express this using Euler products to get

$$\sum_{\substack{p \in \delta_1(x) \\ p \in P}} \frac{1}{\sqrt{p}} \cdot \prod_{\text{prime } q} \left(1 - \frac{\left(\frac{-p}{q}\right)}{q}\right)^{-1}.$$

Define Q to be the set of (rational) primes congruent to 2 (mod 3) and R the set of primes congruent to 1 (mod 3). If $P = Q$, the second factor in the Euler product would be $\left(1 - \frac{1}{3}\right)^{-1} = 3/2$, whereas if $P = R$, that same factor would be $\left(1 + \frac{1}{3}\right)^{-1} = 3/4$. This suggests that choosing a set of primes such as Q leads to a larger constant in the averaging expression. Furthermore, we note that the ratio of the two factors is greater (and thus the bias more pronounced) when q is a smaller prime.

2.5 A refined averaging

The averaging that we carried out included more than one elliptic curve from each isomorphism class. This can be avoided using a construct of Fouvry-Murty.

Define a 'set of minimality'

$$\mathcal{M} = \{(a, b) \in \mathbb{Z}^2 \mid p^2 | a \Rightarrow p^3 \nmid b\}.$$

A straightforward extension of a theorem from ([F-M]) gives

Theorem 2.17. *For A, B such that $A, B > x^{1+\epsilon}$ and $AB > x^{2+\epsilon} \cdot \min(A^{1/4}, B^{1/6})$, we*

have

$$\sum_{|a|\leq A}\sum_{\substack{|b|\leq B\\(a,b)\in\mathcal{M}}}\pi_0(P,E_{a,b},x)=\frac{2AB}{\zeta(10)}\sum_{\substack{p\leq x\\p\in P}}\frac{H(-4p)}{p}\left(1+O\left(p^{-1}\right)+O\left(\log^{-4}x\right)\right)$$
$$+O\left(AB\log x\right)$$

where we note that the sum is now no longer over multiple representatives of a given $\overline{\mathbb{Q}}$-isomorphism class (in the case of elliptic curves with j-invariants $\neq 0, 1728$).

We bound the error terms using (2.3), and then using (2.28) we get

Theorem 2.18. *As $x\to\infty$*

$$\sum_{|a|\leq A}\sum_{\substack{|b|\leq B\\(a,b)\in\mathcal{M}}}\pi_0(P,E_{a,b},x)\sim\frac{4AB}{\zeta(10)}C_P\frac{\sqrt{x}}{\log x}.$$

for $A,B\geq x^{1+\epsilon}$ and $AB>x^{2+\epsilon}\min(A^{1/4},B^{1/6})$, and where C_P is the same constant as mentioned earlier.

We plan to investigate elsewhere the occurrence of congruence class bias for individual elliptic curves, rather than on average for a family of elliptic curves as we have done here, in part through a careful examination of the mod p Galois representations.

Chapter 3

Supersingular distribution for thin families of elliptic curves

In this chapter we construct (arbitrarily) thin families of elliptic curves for which the Lang-Trotter conjecture holds on average, when averaging over the Weierstrass equations of the curves.

3.1 Weierstrass equations

We first note that, using averaging techniques of Fouvry-Murty, one can demonstrate that Lang-Trotter holds on average for elliptic curve families of the form $y^2 = x^3 + ax + b$ where $a, b \in \{kn + c \mid n \in \mathbb{Z}\}$, for fixed integers k and c. However, one can obtain much thinner families than this.

Construct a sequence $\{a_n\}$ of integers as follows. First we choose a function $f(n)$ and impose the condition that $a_n > f(n)$ for all n. This condition should always be assumed to stand in the description below.

Now choose a_1, a_2, a_3 such that they all have different congruence classes mod 3. Next, choose $a_4, \ldots, a_{15}$ such that $a_1, \ldots, a_{15}$ are evenly distributed across congruence classes mod 3 and mod 5. We continue by choosing $a_{16}, \ldots, a_{3\cdot5\cdot7}$ such that they are evenly distributed across congruence classes mod 3, mod 5, and mod 7. We thus construct our sequence in this manner, so that given any (large) prime p, we have $\alpha_1 < \alpha_2 < \alpha_3 < \ldots$ such that $\{a_1, \ldots, a_{\alpha_i}\}$ is evenly distributed mod p, for all i.

Note that given such a sequence $\{a_n\}$, we have sequences $\{a_n + c\}$, for a fixed integer c, which also satisfy the conditions above. Furthermore, sequences $\{ka_n + c\}$, for fixed integers k and c, satisfy the conditions above for all but finitely many primes (i.e., those coprime to k).

So let $S = \{E_{i,j} : y^2 = x^3 + a_i x^2 + a_j\}$ be our family of elliptic curves, and note that if $f(n)$ is a degree two polynomial or an exponential function, then S is a thinner family than any of those mentioned in the first paragraph of this section.

We will establish that this family satisfies the Lang-Trotter conjecture on average, using techniques of Fouvry-Murty [FM]. Denote the number of supersingular primes for $E_{a,b}$ that are less than x by $\pi_0(x; a, b)$.

Theorem 3.1. *Given the conditions and notations above, we have*

$$\sum_{|a|\leq A}\sum_{|b|\leq B}\pi_0(x;a,b) = \frac{2\pi}{3}AB\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left((A+B)x^{3/2} + x^{5/2} + AB\frac{\sqrt{x}}{(\log x)^c}\right).$$

Under the conditions $A, B \geq x^{1/2+\epsilon}, AB \geq x^{3/2+\epsilon}$, this gives

$$\frac{1}{4AB}\sum_{|a|\leq A}\sum_{|b|\leq B}\pi_0(x;a,b) \sim_\epsilon \frac{\pi}{3}\frac{\sqrt{x}}{\log x}.$$

3.2 Proof

Proof. The proof basically follows from Fouvry-Murty [FM], however we include (a more detailed version of) the argument here for the sake of completeness.

The same considerations as in (2) lead us to

$$\begin{aligned}
&\sum_{|a|\le A}\sum_{|b|\le B}\pi_0(x;a,b)\\
=&\frac{1}{2}\sum_{5\le p\le x}\left(\frac{2A}{p}+O\left(1\right)\right)\cdot\left(\frac{2B}{p}+O\left(1\right)\right)\cdot p\cdot\left(H(-4p)+O\left(1\right)\right)+O\left(AB\right)\\
=&2AB\sum_{5\le p\le x}\frac{H(-4p)}{p}+O\left((A+B)\frac{x^{3/2}}{\log x}+AB\log\log x+\frac{x^{5/2}}{\log x}\right)
\end{aligned}$$

where $O\left(AB\right)$ is to account for the possibility that 2 and 3 may be supersingular for various elliptic curves, and for the primes p that may be supersingular for curves with non-minimal equation $E_{a'p^4,b'p^6}$.

Now we note that

$$H(-4p)=h(-4p)+h(-4p)$$

where the Dirichlet class number formula tells us

$$h(-d)=\frac{w\sqrt{d}}{2\pi}L(1,\chi_{-d})$$

where $d\equiv 0$ or $3 \pmod 4$ and w is the number of units in the quadratic field to which the order is associated, thus $w=6,4,2$ when $d=3,4,\ge 7$ respectively.

This leads us to consider the expression

$$\begin{aligned}
&\frac{2AB}{\pi}\left(\sum_{\substack{5\le p\le x\\ p\equiv 3 \bmod 4}}\frac{L(1,\chi_{-p})}{\sqrt{p}}+2\sum_{5\le p\le x}\frac{L(1,\chi_{-4p})}{\sqrt{p}}\right)\\
&+O\left((A+B)x^{3/2}+AB\log x+x^{5/2}\right).
\end{aligned}\tag{3.1}$$

Note that we will repeatedly use *partial summation* in our analysis below. In order to fix notation in this context, let us recall the following statement:

Given a sum of the form

$$\sum_{n=k}^{r} a_n f(n)$$

where a_n is a sequence and $f(n)$ is a continuously differentiable function on $[k, r]$, then this is equal to

$$A(r)f(r) - \int_k^r A(t)f'(t)dt$$

where $A(y) = \sum_{n=k}^{y} a_n$.

We also recall the *Polya-Vinogradov inequality*, which states that for a non-principal character χ on $\mathbb{Z}/n\mathbb{Z}$ and for any positive integer h, we have

$$\left| \sum_{k=1}^{h} \chi(k) \right| \leq 2\sqrt{n} \log n.$$

We will handle the two sums in (3.1) separately.

3.2.1 First sum

Now we consider

$$\begin{aligned} L(1, \chi_{-p}) &= \sum_{n \geq 1} \frac{\chi_{-p}(n)}{n} \\ &= \sum_{n \leq U} \frac{\chi_{-p}(n)}{n} + \sum_{n > U} \frac{\chi_{-p}(n)}{n} \end{aligned}$$

and we apply partial summation to the second sum with $a_n = \chi_{-p}(n)$ and $f(n) = 1/n$ to obtain

$$\begin{aligned}\sum_{n>U} \frac{\chi_{-p}(n)}{n} &= \lim_{r\to\infty} \left(A(r)f(r) - \int_U^r A(t)f'(t)dt \right) \\ &= \lim_{r\to\infty} \left(\left(\sum_{U<n\le r} \chi_{-p}(n) \right) \frac{1}{r} - \int_U^r \left(\sum_{U<n\le t} \chi_{-p}(n) \right) \frac{-1}{t^2} dt \right).\end{aligned}$$

By Polya-Vinogradov we have

$$\begin{aligned}\left| \sum_{n>U} \frac{\chi_{-p}(n)}{n} \right| &\le \lim_{r\to\infty} \left(\frac{1}{r} \cdot 2\sqrt{p}\log p + 2\sqrt{p}\log p \left[\frac{1}{t} \right]_U^r \right) \\ &= \frac{1}{U} \cdot 2\sqrt{p}\log p.\end{aligned}$$

Thus as $p \to \infty$ we have

$$L(1, \chi_{-p}) = \sum_{n\le U} \frac{\chi_{-p}(n)}{n} + O\left(\frac{\sqrt{p}\log p}{U} \right).$$

We will specify U as a function of x later.

Note that for $p \equiv 3 \pmod 4$ we can express $\chi_{-p}(n)$ as the Legendre symbol $\left(\frac{n}{p}\right)$. Thus

$$\begin{aligned}\sum_{\substack{5\le p\le x \\ p\equiv 3 \bmod 4}} \frac{L(1,\chi_{-p})}{\sqrt{p}} &= \sum_{\substack{5\le p\le x \\ p\equiv 3 \bmod 4}} \left(\frac{1}{\sqrt{p}} \sum_{n\le U} \left(\frac{n}{p}\right) \frac{1}{n} + O\left(\frac{\log p}{U} \right) \right) \\ &= \sum_{n\le U} \sum_{\substack{5\le p\le x \\ p\equiv 3 \bmod 4}} \left(\frac{n}{p}\right) \frac{1}{n\sqrt{p}} + O\left(\frac{x}{U}\right).\end{aligned}$$

We estimate the contribution from the portion of the sum when n is a perfect square:

$$\sum_{n=m^2\le U} \frac{1}{m^2} \sum_{\substack{5\le p\le x \\ p\equiv 3 \bmod 4}} \frac{1}{\sqrt{p}}.$$

Fix m and consider

$$\sum_{p\nmid m, p\equiv 3 \bmod 4} \frac{1}{\sqrt{p}}.$$

We apply partial summation with $a_p = 1$ exactly when $p \equiv 3 \pmod 4$ and $p \nmid m$, and with $f(p) = 1/\sqrt{p}$ to get that the sum above is equal to

$$\frac{1}{\sqrt{x}}A(x) - \int_2^x \left(-\frac{1}{2}t^{-3/2}\right) A(t)dt \tag{3.2}$$

where $A(x) = \sum_{p\leq x} a_p$. Recall Dirichlet's theorem on arithmetic progressions in this context, which tells us that

$$\pi_{3,4}(x) = \frac{1}{2}\mathrm{li}(x) + O\left(\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right)$$

where $\pi_{3,4}(x)$ is the number of primes congruent to 3 (mod 4) that are less than x, and where a is some positive integer (for example, the equation above is known to hold for $a = 1/15$).

Thus we obtain that the contribution from the inner sum when n is a perfect square is

$$\frac{1}{2}\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left(\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right).$$

The contribution from the outer sum under this condition is

$$\sum_{m^2\leq U} \frac{1}{m^2} = \frac{\pi^2}{6} - \sum_{m^2>U} \frac{1}{m^2}.$$

Note that, as $U \to \infty$,

$$\begin{aligned}\sum_{m^2>U} \frac{1}{m^2} &\sim \int_U^\infty \frac{1}{t^2} dt \\ &= \left[\frac{-1}{t}\right]_U^\infty \\ &= \frac{1}{U};\end{aligned}$$

thus

$$\sum_{m^2 \le U} \frac{1}{m^2} = \frac{\pi^2}{6} + O\left(\frac{1}{U}\right).$$

So when n is a perfect square, the corresponding contribution is

$$\begin{aligned}&\left(\frac{\pi^2}{6} + O\left(\frac{1}{U}\right)\right) \cdot \left(\frac{1}{2}\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left(\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right)\right) \\ &= \frac{\pi^2}{12}\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left(\frac{\pi^2}{6}\cdot\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right) + O\left(\frac{1}{U}\cdot\frac{\sqrt{x}}{\log x}\right) \\ &\qquad + O\left(\frac{\sqrt{x}}{U}\exp(-a\sqrt{\log x})\right) \\ &= \frac{\pi^2}{12}\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left(\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right)\end{aligned}$$

where in the last line (and from here on) we fix U to be $x^{3/4}$.

Now we need to consider the contribution when n is not a perfect square. We first note that if $x_1 = x\cdot\exp(-c\sqrt{\log x})$ for some positive c, then

$$\begin{aligned}\sum_{n\le U}{}' \frac{1}{n}\sum_{p\le x_1}{}^{\times}\left(\frac{n}{p}\right)\frac{1}{\sqrt{p}} &\ll \sum_{n\le U}{}' \frac{1}{n}\sum_{p\le x_1}{}^{\times}\frac{1}{\sqrt{p}} \\ &\ll (\log U)\cdot\int_2^{x_1}\frac{dt}{\sqrt{t}\log t} \\ &\ll \frac{\sqrt{x_1}}{\log x_1} \\ &\ll (\log U)\cdot\sqrt{x}\cdot\exp\left(\frac{-c}{2}\sqrt{\log x}\right)\end{aligned}$$

where the prime on the sum indicates that we are summing over non-square n, and the

$\times$ indicates that we are summing over primes congruent to 3 (mod 4).

To the outer sum in the expression

$$\sum_{n\le U}{}' \frac{1}{n} \sum_{x_1<p\le x}{}^{\times} \left(\frac{n}{p}\right) \frac{1}{\sqrt{p}}$$

we now apply *dyadic decomposition* to obtain, for a suitable $V \le U$,

$$\sum_{n\le U}{}' \frac{1}{n} \sum_{x_1<p\le x}{}^{\times} \left(\frac{n}{p}\right) \frac{1}{\sqrt{p}} \ll (\log x)|T_1(V)| \tag{3.3}$$

where $T_1 = T_1(V)$ is

$$\sum_{V\le n<2V}{}' \frac{1}{n} \sum_{x_1<p\le x}{}^{\times} \left(\frac{n}{p}\right) \frac{1}{\sqrt{p}}.$$

Apply partial summation to the inner sum above with

$$a_p = \left(\frac{n}{p}\right) \log p \text{ and } f(p) = \frac{1}{\sqrt{p}\log p}$$

to obtain that

$$\begin{aligned}
\sum_{x_1<p\le x}{}^{\times} \left(\frac{n}{p}\right) \frac{1}{\sqrt{p}} =& \frac{1}{\sqrt{x}\log x} \sum_{x_1<p\le x}{}^{\times} \log p \left(\frac{n}{p}\right) \\
&- \int_{x_1}^{x} \left(\frac{1}{\sqrt{t}\log t}\right) \sum_{t_1<p\le t}{}^{\times} \log p \left(\frac{n}{p}\right) dt \\
\le& \left| \frac{1}{\sqrt{x}\log x} \sum_{x_1<p\le x}{}^{\times} \log p \left(\frac{n}{p}\right) \right| \\
&+ \left| \int_{x_1}^{x} \left(\frac{1}{\sqrt{t}\log t}\right)' \sum_{t_1<p\le t}{}^{\times} \log p \left(\frac{n}{p}\right) dt \right|,
\end{aligned}$$

and summing over n,

$$\begin{aligned}
T_1 \leq & \frac{1}{\sqrt{x}\log x} \sideset{}{'}\sum_{V\leq n<2V} \frac{1}{n} \left| \sideset{}{^\times}\sum_{x_1<p\leq x} \log p \left(\frac{n}{p}\right)\right| \\
& + \int_{x_1}^{x} \left| \left(\frac{1}{\sqrt{t}\log t}\right)' \right| \sideset{}{'}\sum_{V\leq n<2V} \frac{1}{n} \left| \sideset{}{^\times}\sum_{t_1<p\leq t} \log p \left(\frac{n}{p}\right)\right| dt \\
\leq & \frac{1}{\sqrt{x}\log x} \sideset{}{'}\sum_{V\leq n<2V} \frac{1}{V} \left| \sideset{}{^\times}\sum_{x_1<p\leq x} \log p \left(\frac{n}{p}\right)\right| \\
& + \int_{x_1}^{x} \left| \left(\frac{1}{\sqrt{t}\log t}\right)' \right| \sideset{}{'}\sum_{V\leq n<2V} \frac{1}{V} \left| \sideset{}{^\times}\sum_{t_1<p\leq t} \log p \left(\frac{n}{p}\right)\right| dt;
\end{aligned}$$

thus

$$\begin{aligned}
VT_1 \leq & \frac{1}{\sqrt{x}\log x} \sideset{}{'}\sum_{V\leq n<2V} \left| \sideset{}{^\times}\sum_{x_1<p\leq x} \log p \left(\frac{n}{p}\right)\right| \\
& + \int_{x_1}^{x} \left| \left(\frac{1}{\sqrt{t}\log t}\right)' \right| \sideset{}{'}\sum_{V\leq n<2V} \left| \sideset{}{^\times}\sum_{t_1<p\leq t} \log p \left(\frac{n}{p}\right)\right| dt. \qquad (3.4)
\end{aligned}$$

At this stage we need (see Lemma 8 of [Jut])

Lemma 3.2. *Let*

$$S(D,x) := \sideset{}{'}\sum_{|d|\leq D} \left| \sum_{3\leq n\leq x} \Lambda(n) \left(\frac{d}{n}\right)\right|$$

where $\Lambda(n)$ is the Von Mangoldt function and the prime on the summation symbol indicates that the sum is to be taken over non-square values of d.

Then for all $c > 0$, uniformly for $3 \leq D \leq x^{49/50}$,

$$S(D,x) \ll \frac{xD}{(\log x)^c}.$$

We note that this also holds if the sum over n is restricted to $n = 3 \pmod 4$ (or

$n \equiv 1 \pmod 4$). This can be achieved by detecting suitable n using $\frac{1}{2}\left(1 - \left(\frac{-1}{n}\right)\right)$ (or $\frac{1}{2}\left(1 + \left(\frac{-1}{n}\right)\right)$ for the $1 \pmod 4$ case).

We now need to determine that the same estimates apply if we restrict the inner sum to prime values of n (rather than powers of primes).

$$\begin{aligned}
&\sum_{V \le d < 2V}{}' \left| \sum_{3 \le p \le x} \log p \left(\frac{d}{p}\right) \right| \\
\le &\sum_{|d| \le 2V = D}{}' \left| \sum_{3 \le p \le x} \log p \left(\frac{d}{p}\right) \right| \\
= &S(D,x) - \sum_{|d| \le D}{}' \left| \sum_{3 \le p^\alpha \le x, \alpha \ne 1} \log p \left(\frac{d}{p^\alpha}\right) \right|
\end{aligned}$$

and note that we have set D to be $2V$.

Now

$$\begin{aligned}
&\left| \sum_{3 \le p^\alpha \le x, \alpha \ne 1} \log p \left(\frac{d}{p^\alpha}\right) \right| \\
\le &\sum_{3 \le p^\alpha \le x, \alpha \ne 1} \log p \\
\le &\log(x^{1/2}) \cdot \pi(x^{1/2}) + \log(x^{1/3}) \cdot \pi(x^{1/3}) + \cdots + \log(x^{1/w}) \pi(x^{1/w})
\end{aligned}$$

where w is the least integer greater than $\log_2 x$, and so we can bound the expression above as

$$\begin{aligned}
&\ll \sqrt{x} + x^{1/3} \log_2 x \\
&\ll \sqrt{x}.
\end{aligned}$$

Thus

$$\sum_{|d| \le D}{}' \left| \sum_{3 \le p^\alpha \le x, \alpha \ne 1} \log p \left(\frac{d}{p^\alpha}\right) \right| \ll 2\sqrt{x} \cdot 2V.$$

This is dominated by the $xV/(\log x)^c$ term and so does not affect the asymptotic.

Therefore we have that

$$\sum_{V\le d<2V}{}' \left| \sum_{3\le p\le x} \log p \left(\frac{d}{p}\right)\right| \ll \frac{xV}{(\log x)^c}.$$

So for (3.4) we have

$$\begin{aligned} VT_1 \le & \frac{1}{\sqrt{x}\log x}\cdot\frac{xV}{(\log x)^c} \\ & + \int_{x_1}^{x} \left|\left(\frac{1}{\sqrt{t}\log t}\right)'\right| \cdot \frac{tV}{(\log t)^c}dt. \end{aligned}$$

Now

$$\begin{aligned} & \int_{x_1}^{x} \left|\left(\frac{1}{\sqrt{t}\log t}\right)'\right| \frac{tV}{(\log t)^c}dt \\ =& V\int_{x_1}^{x} t^{-1/2}\cdot\frac{1}{(\log t)^{c+1}}\left(\frac{1}{2}+\frac{1}{\log t}\right) \\ \le& V\int_{x_1}^{x} t^{-1/2}\cdot\frac{1}{(\log t)^{c+1}}\left(\frac{1}{2}+\frac{c+1}{\log t}\right) \\ =& V\left[t^{1/2}\cdot\frac{1}{(\log t)^{c+1}}\right]_{x_1}^{x} \\ \ll& \frac{x^{1/2}V}{(\log x)^{c+1}}. \end{aligned}$$

Thus

$$VT_1 \ll \frac{1}{\sqrt{x}\log x}\cdot\frac{xV}{(\log x)^c} + \frac{x^{1/2}V}{(\log x)^{c+1}}$$

and so

$$T_1 \ll \frac{\sqrt{x}}{(\log x)^{c+1}}.$$

Applying this to (3.3), we have

$$\sum_{n\le U}{}' \frac{1}{n} \sum_{x_1<p\le x}{}^{\times} \left(\frac{n}{p}\right)\frac{1}{\sqrt{p}} \ll \frac{\sqrt{x}}{(\log x)^c}.$$

Combining all the results above, we obtain

$$\begin{aligned}\sum_{p\le x, p\equiv 3 \bmod 4} \frac{L(1,\chi_{-p})}{\sqrt{p}} =& \frac{\pi^2}{12}\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left(\frac{x}{U}\right) + O\left(\sqrt{x}\cdot\exp(-\sqrt{\log x})\right) \\ &+ O\left(\frac{\sqrt{x}}{U}\right) + O\left(\sqrt{x}\cdot\exp(-\frac{c}{2}\sqrt{\log x})\log U\right) \\ &+ O\left(\log x\cdot\frac{\sqrt{x}}{(\log x)^{c+1}}\right)\end{aligned}$$

and note that the right-hand side can be simplified to

$$\frac{\pi^2}{12}\int_2^x \frac{dt}{\sqrt{t}\log t} + O\left(\frac{\sqrt{x}}{(\log x)^c}\right)$$

where, as mentioned earlier, we have set $U = x^{3/4}$.

This concludes our analysis of the first sum.

3.2.2 Second sum

The analysis of the second sum follows in a similar way to that of the first. We briefly highlight the main steps.

The Polya-Vinogradov inequality and partial summation give

$$L(1,\chi_{-4p}) = \sum_{n\le U}\frac{\chi_{-4p}(n)}{n} + O\left(\frac{\sqrt{p}\log p}{U}\right)$$

and note that

$$\chi_{-4p}(n) = \left(\frac{2}{n}\right)^2 (-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right).$$

Thus the expression we consider is

$$\sum_{\text{odd } n\le U}\sum_{p\le x}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\frac{1}{\sqrt{p}}. \tag{3.5}$$

If n is an odd perfect square, then $n = m^2 \equiv 1 \pmod 4$ and so $(-1)^{\frac{p+1}{2}\frac{n-1}{2}} = +1$ and

so the inner sum is

$$\sum_{p\le x}\frac{1}{\sqrt{p}}=\int_2^x\frac{dt}{\log t}+O\left(\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right).$$

The outer sum is

$$\begin{aligned}\sum_{\text{odd } m^2\le U}\frac{1}{m^2}&=\prod_{\text{odd primes } p}\left(1-\frac{1}{p^2}\right)^{-1}-\sum_{\text{odd } m^2>U}\frac{1}{m^2}\\&=\frac{3}{4}\cdot\frac{\pi^2}{6}+O\left(\frac{1}{U}\right)\end{aligned}$$

where the estimate for the sum over odd $m^2>U$ arises from the same result in the previous subsection.

Thus the contribution for when n is square in expression (3.5) is

$$\begin{aligned}&\left(\frac{3}{4}\cdot\frac{\pi^2}{6}+O\left(\frac{1}{U}\right)\right)\cdot\left(\int_2^x\frac{dt}{\log t}+O\left(\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right)\right)\\=&\frac{\pi^2}{8}\int_2^x\frac{dt}{\sqrt{t}\log t}+O\left(\frac{\sqrt{x}}{\log x}\cdot\frac{1}{U}\right)+O\left(\sqrt{x}\cdot\exp(-a\sqrt{\log x})\right)\\&+O\left(\frac{x}{U\log x}\cdot\exp(-a\sqrt{\log x})\right).\end{aligned}$$

Now we consider the contribution from the non-square n.

We want to estimate

$$\sum_{\text{odd } n\le U}{}'\sum_{p\le x}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\frac{1}{\sqrt{p}}$$

where the prime on the outer sum indicates that we are summing over non-square n. Dyadic decomposition gives

$$\sum_{\text{odd } n\le U}{}'\sum_{p\le x}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\frac{1}{\sqrt{p}}\ll\log x\,|T_2(V)|$$

for some $3\le V\le U$, where

$$T_2(V)=\sum_{V\le\text{odd } n\le 2V}{}'\frac{1}{n}\sum_{p\le x}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\frac{1}{\sqrt{p}}.$$

Applying partial summation to the inner sum, we obtain

$$\frac{1}{\sqrt{x}\log x}\sum_{p\le x}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\log p-\int_2^x\left(\frac{1}{\sqrt{t}\log t}\right)'\sum_{p\le t}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\log p\ dt$$

and therefore

$$\begin{aligned}VT_2(V)\ll&\frac{1}{\sqrt{x}\log x}\sum_{V\le\text{odd }n\le 2V}{}'\left|\sum_{p\le x}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\log p\right|\\&+\int_2^x\left(\frac{1}{\sqrt{t}\log t}\right)'\sum_{V\le\text{odd }n\le 2V}{}'\left|\sum_{p\le t}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\log p\ dt\right|.\end{aligned}$$

Now we seek to bound

$$\begin{aligned}&\sum_{V\le\text{odd }n\le 2V}{}'\left|\sum_{p\le x}(-1)^{\frac{p+1}{2}\frac{n-1}{2}}\left(\frac{n}{p}\right)\log p\right|\\&\le\sum_{V\le\text{odd }n\le 2V}{}'\left|\sum_{\substack{p\le x\\p\equiv 3\bmod 4}}\left(\frac{n}{p}\right)\log p\right|+\sum_{V\le\text{odd }n\le 2V}{}'\left|(-1)^{\frac{n-1}{2}}\sum_{\substack{p\le x\\p\equiv 1\bmod 4}}\left(\frac{n}{p}\right)\log p\right|.\end{aligned}$$

Applying the consequences of Lemma 3.2, derived in the previous subsection, we obtain, for $D=2V$,

$$\begin{aligned}2\frac{xD}{(\log x)^C}&\gg\sum_{|d|\le D}{}'\left|\sum_{\substack{3\le p\le x\\p\equiv 3\bmod 4}}\left(\frac{n}{p}\right)\log p\right|+\sum_{|d|\le D}{}'\left|\sum_{\substack{3\le p\le x\\p\equiv 1\bmod 4}}\left(\frac{n}{p}\right)\log p\right|\\&\ge\sum_{V\le\text{odd }n\le 2V}{}'\left|\sum_{\substack{p\le x\\p\equiv 3\bmod 4}}\left(\frac{n}{p}\right)\log p\right|+\sum_{V\le\text{odd }n\le 2V}{}'\left|\sum_{\substack{p\le x\\p\equiv 1\bmod 4}}\left(\frac{n}{p}\right)\log p\right|.\end{aligned}$$

Thus we obtain

$$T_2(V)\ll\frac{\sqrt{x}}{(\log x)^c}$$

and so combining the results from this subsection, we have

$$2\sum_{p\leq x}\frac{L(1,\chi_{-4p})}{\sqrt{p}}=\frac{\pi^2}{4}\int_2^x\frac{dt}{\sqrt{t}\log t}+O\left(\frac{\sqrt{x}}{(\log x)^c}\right).$$

3.2.3 The asymptotic

Combining the results from the previous two subsections, we have

$$\begin{aligned}
&\sum_{|a|\leq A}\sum_{|b|\leq B}\pi_0(x;a,b)\\
=&2AB\sum_{5\leq p\leq x}\frac{H(-4p)}{p}+O\left((A+B)\frac{x^{3/2}}{\log x}+AB\log\log x+\frac{x^{5/2}}{\log x}\right)\\
=&\frac{2AB}{\pi}\frac{\pi^2}{3}\int_2^x\frac{dt}{\sqrt{t}\log t}+O\left((A+B)x^{3/2}+AB\log x+x^{5/2}+AB\frac{\sqrt{x}}{(\log x)^c}\right)\\
=&\frac{2\pi}{3}AB\int_2^x\frac{dt}{\sqrt{t}\log t}+O\left((A+B)x^{3/2}+x^{5/2}+AB\frac{\sqrt{x}}{(\log x)^c}\right)
\end{aligned}$$

as required. □

Chapter 4

A refinement of strong multiplicity one

Introduction

Given a number field F, let $\mathcal{A}_0(\mathrm{GL}_n(\mathbb{A}_F))$ be the set of cuspidal automorphic representations $\pi = \otimes'_v \pi_v$ of $\mathrm{GL}_n(\mathbb{A}_F)$. For $\pi \in \mathcal{A}_0(\mathrm{GL}_n(\mathbb{A}_F))$, for any place v of F where π is unramified we denote the Langlands conjugacy class by $A(\pi_v) \subset \mathrm{GL}_n(\mathbb{C})$, which we will represent by the diagonal matrix $\mathrm{diag}\{\alpha_{1,v}, \alpha_{2,v}, \ldots, \alpha_{n,v}\}$. Let $a_v(\pi)$ be the trace of this matrix.

For $n = 2$, we will prove the following two theorems.

Theorem 4.1. *Let $\pi, \pi' \in \mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$ be non-dihedral representations, with trivial central character and symmetric squares that are not twist-equivalent. For finite places v where π and π' are unramified, set $a_v = \mathrm{Tr}(A(\pi_v))$, $b_v = \mathrm{Tr}(A(\pi'_v))$, and let $S = \{v \mid a_v \neq b_v\}$. Then*

$$\underline{\delta}(S) \geq \frac{2}{5}$$

where $\underline{\delta}(S)$ is the lower Dirichlet density of the set S.

Theorem 4.2. *Let π be a non-dihedral cuspidal automorphic representation over a number field F, with trivial central character. We define $S_\gamma = \{v \mid a_v \neq \gamma\}$, where γ is*

a real scalar and let $\underline{\delta}(S_\gamma)$ represent the lower Dirichlet density of S_γ. Then

$$\underline{\delta}(S_\gamma) \geq \frac{(\gamma^2+1)^2}{\gamma^4+6\gamma^2+2}.$$

We feel that both theorems 4.1 and 4.2 could be extended, with some care, to the case of cuspidal automorphic representations for GL(2) with non-trivial unitary central character. Presenting these theorems here for the case of trivial central character allows us to simplify the notation in the proofs.

The structure of this chapter is as follows: In section 4.1, we establish some notation and recall relevant theorems on the cuspidality of known symmetric powers; in section 4.2, we prove the result relating to the strong multiplicity one theorem; in section 4.3, we address the occurrence of a fixed real algebraic number as the value taken by the trace of the Langlands conjugacy class of π at place v; lastly, in section 4.4 we consider an example relevant to theorem 4.1.

4.1 Preliminaries

We begin by introducing some notation. Let F be a number field and let S be a set of primes in F. Then the *lower Dirichlet density* of S is

$$\underline{\delta}(S) = \lim_{s\to 1^+} \inf \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}\mathfrak{p}^{-s}}{-\log(s-1)}.$$

For $\pi \in \mathcal{A}_0(\mathrm{GL}_n(\mathbb{A}_F))$ we have the associated L-function $L(s,\pi) = \prod_v L_v(s,\pi_v)$ where for π_v unramified we have

$$L_v(s,\pi_v) = \det\left(I_n - A(\pi_v)\mathrm{N}v^{-s}\right)^{-1} = \prod_{j=1}^{n}\left(1-\alpha_{j,v}\mathrm{N}v^{-s}\right)^{-1}.$$

Let T be the set of all ramified and infinite places. Define the incomplete L-function

$$L^T(s,\pi) = \prod_{v\notin T} L_v(s,\pi_v),$$

and the 'incomplete Dedekind zeta function'

$$\zeta_F^T(s) = \prod_{v \notin T} (1 - \mathrm{N}v^{-s})^{-1}.$$

Given $\pi \in \mathcal{A}_0(\mathrm{GL}_n(\mathbb{A}_F))$ and $\pi' \in \mathcal{A}_0(\mathrm{GL}_m(\mathbb{A}_F))$, we have the Rankin-Selberg L-function $L(s, \pi \times \pi') = \prod_v L_v(s, \pi_v \times \pi'_v)$, where for v such that π_v and π'_v are unramified, we have

$$L_v(s, \pi_v \times \pi'_v) = \det\left(I_{nm} - \left(A(\pi_v) \otimes A(\pi'_v)\right) \mathrm{N}v^{-s}\right)^{-1}.$$

We also note the following cuspidality results that we will use in the next few sections:

Given a cuspidal automorphic representation π for $GL_2(\mathbb{A}_F)$, by Jacquet-Shalika [JS1] and Shahidi [Sha] one knows that the symmetric second, third, and fourth power representations are isobaric sums of unitary cuspidal automorphic representations. One also knows that $\mathrm{Sym}^2\pi$ is cuspidal iff π is non-dihedral [GJ] and that $\mathrm{Sym}^3\pi$ is cuspidal iff π is not dihedral or tetrahedral [KS1]. One also knows that $L(s, \pi')$ is non-vanishing on $\mathrm{Re}(s) = 1$ for any cuspidal automorphic representation π' for $GL_n(\mathbb{A}_F)$ [JS2].

Note that for $\pi \in \mathcal{A}_0(\mathrm{GL}_n(\mathbb{A}_F))$, $\pi' \in \mathcal{A}_0(\mathrm{GL}_m(\mathbb{A}_F))$, the Rankin-Selberg L-function $L(s, \pi \times \pi')$ has a pole at $s = 1$ if $\pi' \simeq \pi^\vee$ [JS1], and otherwise is holomorphic in $\mathrm{Re}(s) \geq 1$ and non-vanishing on $\mathrm{Re}(s) = 1$ [Sha].

For π that is not dihedral or tetrahedral one knows that the completed L-functions of the symmetric square and cube are entire. Furthermore, for such π one also knows that the L-function of the symmetric fourth has no pole at $s = 1$ and in fact is non-vanishing at that point. These standard facts follow from the Clebsch-Gordon decomposition of tensor powers of representations — we include the details below for completeness.

Specifically, one can consider $L^T(s, \mathrm{Sym}^3\pi \times \pi)$ (where T is defined as above) and note that since $\mathrm{Sym}^3\pi$ is cuspidal, this incomplete Rankin-Selberg L-function does not have a pole at $s = 1$. Now we show that

$$L^T(s, \mathrm{Sym}^3\pi \times \pi) = L^T(s, \mathrm{Sym}^4\pi) L^T(s, \mathrm{Sym}^2\pi).$$

Fix $v \notin T$ and write $\alpha_{j,v}$ as α_j. Since π has trivial character, we have that $\alpha_1\alpha_2 = 1$ and so we will use the notation α, α^{-1} for α_1, α_2, respectively.

Consider $A(\mathrm{Sym}^3\pi) \otimes A(\pi)$, which can be represented by

$$\begin{pmatrix} \alpha^3 & & & \\ & \alpha & & \\ & & \alpha^{-1} & \\ & & & \alpha^{-3} \end{pmatrix} \otimes \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix}$$

$$\sim \begin{pmatrix} \alpha^4 & & & & & & & \\ & \alpha^2 & & & & & & \\ & & \alpha^2 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & \alpha^{-2} & & \\ & & & & & & \alpha^{-2} & \\ & & & & & & & \alpha^{-4} \end{pmatrix}$$

$$\sim \begin{pmatrix} \alpha^4 & & & & \\ & \alpha^2 & & & \\ & & 1 & & \\ & & & \alpha^{-2} & \\ & & & & \alpha^{-4} \end{pmatrix} \oplus \begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix}$$

and thus $A(\mathrm{Sym}^3\pi) \otimes A(\pi)$ is equivalent to $A(\mathrm{Sym}^4\pi) \oplus A(\mathrm{Sym}^2\pi)$. So we have

$$L^T(s, \mathrm{Sym}^3\pi \times \pi) = L^T(s, \mathrm{Sym}^4\pi) L^T(s, \mathrm{Sym}^2\pi).$$

Since (as mentioned) the incomplete L-function on the left-hand side has no pole at $s = 1$ and the incomplete L-function associated to the symmetric square is non-zero, we have that $L^T(s, \mathrm{Sym}^4\pi)$ has no pole at $s = 1$.

Furthermore, note that since the symmetric third and fourth powers of π are known to be isobaric sums of unitary cuspidal automorphic representations, by Jacquet-Shalika [JS1]

and Shahidi [Sha] we know that the associated L-function is non-vanishing at $s = 1$.

Similar properties of these incomplete L-functions also hold when π is tetrahedral. We have addressed this case in section 4.5.

From here on we assume that π and π' are not dihedral.

4.2 Proof of theorem 4.1 in the non-tetrahedral case

Given that π has trivial central character, we have that $a_v \in \mathbb{R}$ for all v (since in general $\overline{\pi} \simeq \pi \otimes \omega^{-1}$, where ω is the central character of π). Let $c = c_S$ be the characteristic function of the set $S = \{v \mid a_v \neq b_v\}$. We have, for real $s > 1$,

$$\begin{aligned}
&\sum_v \frac{a_v^2}{\mathrm{N}v^s} - \sum_v \frac{2a_v b_v}{\mathrm{N}v^s} + \sum_v \frac{b_v^2}{\mathrm{N}v^s} \\
=&\sum_v \frac{(a_v - b_v)^2}{\mathrm{N}v^s} \\
=&\sum_v \frac{(a_v - b_v)^2 c(v)}{\mathrm{N}v^s} \\
\leq&\left(\sum_v \frac{(a_v - b_v)^4}{\mathrm{N}v^s}\right)^{1/2} \left(\sum_v \frac{c(v)^2}{\mathrm{N}v^s}\right)^{1/2} \\
=&\left(\sum_v \frac{a_v^4}{\mathrm{N}v^s} - \sum_v \frac{4a_v^3 b_v}{\mathrm{N}v^s} + \sum_v \frac{6a_v^2 b_v^2}{\mathrm{N}v^s} - \sum_v \frac{4a_v b_v^3}{\mathrm{N}v^s} + \sum_v \frac{b_v^4}{\mathrm{N}v^s}\right)^{1/2} \\
&\cdot \left(\sum_{v \in S} \frac{1}{\mathrm{N}v^s}\right)^{1/2}
\end{aligned} \tag{4.1}$$

where the inequality above arises from applying Cauchy-Schwarz.

In order to establish the asymptotic behaviour of each side of the inequality above for real $s \to 1^+$, we make use of

Lemma 4.3. *Let T and the incomplete L-functions be defined as in the previous section. For non-dihedral cuspidal GL(2) automorphic representations π, π', with trivial central character and symmetric squares that are not twist-equivalent, we have the following*

identities:

$$\begin{aligned}
L^T(s,\pi\times\pi) =& L^T\left(s,\mathrm{Sym}^2(\pi)\right)\zeta_F^T(s)\\
L^T(s,\pi\times\pi\times\pi\times\pi) =& L^T\left(s,\mathrm{Sym}^4(\pi)\right)L^T\left(s,\mathrm{Sym}^2(\pi)\right)^3\zeta_F^T(s)^2\\
L^T(s,\pi\times\pi\times\pi\times\pi') =& L^T\left(s,\mathrm{Sym}^3(\pi)\times\pi'\right)L^T\left(s,\pi\times\pi'\right)^2\\
L^T(s,\pi\times\pi\times\pi'\times\pi') =& L^T\left(s,\mathrm{Sym}^2(\pi)\times\mathrm{Sym}^2(\pi')\right)L^T\left(s,\mathrm{Sym}^2(\pi)\right)\\
& \cdot L^T\left(s,\mathrm{Sym}^2(\pi')\right)\zeta_F^T(s).
\end{aligned}$$

Proof. This follows from the Clebsch-Gordon decomposition of tensor powers of two-dimensional representations. However, we include the details for completeness.

Fix $v\notin T$ and write $\alpha_{j,v}$ as α_j. As in the previous section, because π has trivial character, we will write α and α^{-1} for α_1 and α_2, respectively.

First equation

Consider $A(\pi_v)\otimes A(\pi_v)$, which can be represented by

$$\begin{pmatrix}\alpha & \\ & \alpha^{-1}\end{pmatrix}\otimes\begin{pmatrix}\alpha & \\ & \alpha^{-1}\end{pmatrix}$$
$$\sim\begin{pmatrix}\alpha^2 & & \\ & 1 & \\ & & \alpha^{-2}\end{pmatrix}\oplus 1.$$

Thus

$$\begin{aligned}
L_v(s,\pi_v\times\pi_v)^{-1} =& \det\left(I_4-\frac{A(\pi_v)\times A(\pi_v)}{\mathrm{N}v^s}\right)\\
=& \det\left(I_4-\begin{pmatrix}\alpha^2 & & & \\ & 1 & & \\ & & 1 & \\ & & & \alpha^{-2}\end{pmatrix}\mathrm{N}v^{-s}\right)\\
=& \det\left(I_3-\begin{pmatrix}\alpha^2 & & \\ & 1 & \\ & & \alpha^{-2}\end{pmatrix}\mathrm{N}v^{-s}\right)\cdot\det\left(1-\mathrm{N}v^{-s}\right)\\
=& L_v\left(s,\mathrm{Sym}^2\pi_v\right)\cdot\left(1-\mathrm{N}v^{-s}\right).
\end{aligned}$$

Given that this identity holds for all $v\in T$, we can take the product over all such v to obtain

$$L^T(s,\pi\times\pi)=L^T\left(s,\mathrm{Sym}^2(\pi)\right)\cdot\zeta_F^T(s).$$

Second equation

Consider $A(\pi_v)^{\otimes 4}$, which can be represented by

$$\begin{aligned}
&\begin{pmatrix}\alpha & \\ & \alpha^{-1}\end{pmatrix}^{\otimes 4}\\
\sim&\left(\begin{pmatrix}\alpha^2 & & \\ & 1 & \\ & & \alpha^{-2}\end{pmatrix}\oplus 1\right)^{\otimes 2}\\
\sim&\begin{pmatrix}\alpha^2 & & \\ & 1 & \\ & & \alpha^{-2}\end{pmatrix}^{\otimes 2}\oplus\begin{pmatrix}\alpha^2 & & \\ & 1 & \\ & & \alpha^{-2}\end{pmatrix}^{\oplus 2}\oplus 1.
\end{aligned}$$

At this point we note

$$\begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix}^{\otimes 2} \sim \begin{pmatrix} \alpha^4 & & & & \\ & \alpha^2 & & & \\ & & 1 & & \\ & & & \alpha^{-2} & \\ & & & & \alpha^{-4} \end{pmatrix} \oplus \begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix} \oplus 1.$$

Substituting into the equation above, we obtain

$$\begin{pmatrix} \alpha^4 & & & & \\ & \alpha^2 & & & \\ & & 1 & & \\ & & & \alpha^{-2} & \\ & & & & \alpha^{-4} \end{pmatrix} \oplus \begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix}^{\oplus 3} \oplus 1^{\oplus 2}.$$

As before, we use this to interpret the local factors, and thus obtain

$$L^T(s, \pi \times \pi \times \pi \times \pi) = L^T\left(s, \mathrm{Sym}^4(\pi)\right) L^T\left(s, \mathrm{Sym}^2(\pi)\right)^3 \zeta_F^T(s)^2.$$

Third equation

We keep the same notation for $A(\pi_v)$ and we represent $A(\pi'_v)$, having fixed a $v \notin T$,

by $\mathrm{diag}\{\beta, \beta^{-1}\}$. Thus we note that $A(\pi_v)^{\otimes 3} \otimes A(\pi_v')$ can be represented by

$$\begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix}^{\otimes 3} \otimes \begin{pmatrix} \beta & \\ & \beta^{-1} \end{pmatrix}$$
$$\sim \left(\begin{pmatrix} \alpha^3 & & & \\ & \alpha & & \\ & & \alpha^{-1} & \\ & & & \alpha^{-3} \end{pmatrix} \oplus \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix}^{\oplus 2} \right) \otimes \begin{pmatrix} \beta & \\ & \beta^{-1} \end{pmatrix}$$

thus

$$L^T(s, \pi \times \pi \times \pi \times \pi') = L^T\left(s, \mathrm{Sym}^3(\pi) \times \pi'\right) L^T\left(s, \pi \times \pi'\right)^2.$$

Fourth equation

We have $A(\pi_v)^{\otimes 2} \otimes A(\pi_v')^{\otimes 2}$, which can be represented by

$$\left(\begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix} \oplus 1 \right) \otimes \left(\begin{pmatrix} \beta^2 & & \\ & 1 & \\ & & \beta^{-2} \end{pmatrix} \oplus 1 \right)$$
$$\sim \left(\begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix} \otimes \begin{pmatrix} \beta^2 & & \\ & 1 & \\ & & \beta^{-2} \end{pmatrix} \right)$$
$$\oplus \begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix} \oplus \begin{pmatrix} \beta^2 & & \\ & 1 & \\ & & \beta^{-2} \end{pmatrix} \oplus 1$$

which gives us

$$\begin{aligned} L^T(s, \pi \times \pi \times \pi' \times \pi') =& L^T\left(s, \mathrm{Sym}^2(\pi) \times \mathrm{Sym}^2(\pi')\right) L^T\left(s, \mathrm{Sym}^2(\pi)\right) \\ & \cdot L^T\left(s, \mathrm{Sym}^2(\pi')\right) \zeta_F^T(s). \end{aligned}$$

□

Remark 18. The purpose of the lemma above is to be able to establish asymptotic behaviour of the completed L-functions as $s \to 1^+$. Note that it is enough to compare incomplete L-functions as the number of ramified and infinite places is finite, and thus the incomplete L-function associated to the unramified finite places has the same type of pole at $s = 1$ as the complete L-function.

We now continue with our proof of theorem 4.1 for the non-tetrahedral case.

By considering the behaviour of the incomplete L-functions, for π, π' that are not dihedral or tetrahedral, as real $s \to 1^+$, we obtain

$$\sum \frac{a_v^i b_v^j}{\mathrm{N}v^s} = k(i,j) \cdot \log\left(\frac{1}{s-1}\right) + o\left(\log\left(\frac{1}{s-1}\right)\right)$$

where

$$k(i,j) = \begin{cases} 0 & \text{for} \quad (i,j) = (1,1) \text{ or } (3,1) \\ 1 & \text{for} \quad (i,j) = (2,0) \text{ or } (2,2) \\ 2 & \text{for} \quad (i,j) = (4,0), \end{cases}$$

as real $s \to 1^+$.

Now if we divide inequality (4.1) by $\log(1/(s-1))$ and take $\lim_{s\to 1^+} \inf$ of both sides, we obtain

$$\begin{aligned} 2 &\leq 10^{1/2} \cdot \underline{\delta}(S)^{1/2} \\ \frac{2}{5} &\leq \underline{\delta}(S). \end{aligned}$$

□

4.3 Proof of theorem 4.2 in the non-tetrahedral case

Recall from the introduction that $S_\gamma = \{v \in \Sigma_F \mid a_v \neq \gamma\}$, where γ is a real scalar and let $\underline{\delta}(S_\gamma)$ represent the lower Dirichlet density of S_γ.

Let c be the characteristic function of the set S_γ, and consider

$$\begin{aligned}
&\sum_v \frac{a_v^2}{\mathrm{N}v^s} - \sum_v \frac{2a_v\gamma}{\mathrm{N}v^s} + \sum_v \frac{\gamma^2}{\mathrm{N}v^s} \\
=&\sum_{v\in S_\gamma} \frac{(a_v-\gamma)^2}{\mathrm{N}v^s} \\
=&\sum_v \frac{(a_v-\gamma)^2 c(v)}{\mathrm{N}v^s} \\
\leq&\left(\sum_v \frac{(a_v-\gamma)^4}{\mathrm{N}v^s}\right)^{1/2}\left(\sum_v \frac{c(v)^2}{\mathrm{N}v^s}\right)^{1/2} \\
=&\left(\sum_v \frac{a_v^4}{\mathrm{N}v^s} - \sum_v \frac{4a_v^3\gamma}{\mathrm{N}v^s} + \sum_v \frac{6a_v^2\gamma^2}{\mathrm{N}v^s} - \sum_v \frac{4a_v\gamma^3}{\mathrm{N}v^s} + \sum_v \frac{\gamma^4}{\mathrm{N}v^s}\right)^{1/2} \\
&\cdot\left(\sum_{v\in S_\gamma} \frac{1}{\mathrm{N}v^s}\right)^{1/2}. \qquad (4.2)
\end{aligned}$$

We have

Lemma 4.4. *For real $s \to 1^+$ we have the following identities:*

$$\sum \frac{a_v^3}{\mathrm{N}v^s} = o\left(\log\left(\frac{1}{s-1}\right)\right)$$
$$\sum \frac{a_v}{\mathrm{N}v^s} = o\left(\log\left(\frac{1}{s-1}\right)\right).$$

Proof. We can take a similar approach to that taken in the proof of lemma 4.3 from the previous section. We include the details for completeness.

First equation

We note that $A(\pi_v)^{\otimes 3}$ can be represented by

$$
\begin{aligned}
&\begin{pmatrix} \alpha & & \\ & \alpha^{-1} & \end{pmatrix}^{\otimes 3} \\
\sim &\left(\left(\begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix} \oplus 1 \right) \otimes \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix} \right) \\
\sim &\begin{pmatrix} \alpha^3 & & & & & & \\ & \alpha & & & & & \\ & & \alpha & & & & \\ & & & \alpha^{-1} & & & \\ & & & & \alpha^{-1} & & \\ & & & & & \alpha^{-3} \end{pmatrix} \oplus \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix} \\
\sim &\begin{pmatrix} \alpha^3 & & & \\ & \alpha & & \\ & & \alpha^{-1} & \\ & & & \alpha^{-3} \end{pmatrix} \oplus \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix}^{\oplus 2}
\end{aligned}
$$

and thus we have

$$L^T(s, \pi \times \pi \times \pi) = L^T\left(s, \mathrm{Sym}^3(\pi)\right) L^T(s, \pi)^2.$$

Since π is a cuspidal automorphic representation that is not dihedral or tetrahedral, we know that the first L-function on the right-hand side has no pole, and the cuspidality of π tells us that the second L-function on the right-hand side also has no pole. Thus

$$\sum \frac{a_v^3}{\mathrm{N}v^s} = o\left(\log\left(\frac{1}{s-1}\right)\right).$$

Second equation

This simply follows from the fact that π is cuspidal, thus

$$\sum \frac{a_v}{\mathrm{N}v^s} = o\left(\log\left(\frac{1}{s-1}\right)\right).$$

□

We divide inequality (4.2) by $\log(1/(s-1))$ and take $\lim_{s\to 1^+}\inf$ of both sides; we obtain

$$(1+\gamma^2) \leq (2+6\gamma^2+\gamma^4)^{1/2} \cdot (\underline{\delta}(S_\gamma))^{1/2}$$

and thus

$$\underline{\delta}(S_\gamma) \geq \frac{(\gamma^2+1)^2}{\gamma^4+6\gamma^2+2}.$$

□

4.4 An example

In this section we will consider an example due to J.-P. Serre that demonstrates that D. Ramakrishnan's strong multiplicity one theorem [Ram] is sharp, and we will verify that theorem 4.1 is compatible with this result.

Consider the quaternion group Q_8. It has a unique two-dimensional complex irreducible representation, which we will denote as τ. Now we let $G = Q_8 \times \{\pm 1\}$ and we define two representations of G, denoted by ρ and ρ', as $\tau \otimes 1$ and $\tau \otimes \mathrm{sgn}$, respectively. We note that ρ, ρ' are irreducible representations.

Now Q_8 (and thus G) is known to appear as a Galois group of a finite extension of number fields. Therefore any representation of G can be lifted to a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let S be the set $\{(\pm 1, -1)\}$. Then the traces of ρ, ρ' agree exactly outside S, and furthermore we note that $|S|/|G| = 2/2^4 = 1/8$.

Since G is nilpotent, by Arthur-Clozel [AC] the strong Artin conjecture holds for ρ and ρ'. So there exist cuspidal automorphic representations $\pi, \pi' \in GL_2(\mathbb{A}_F)$, a Galois extension K/F with group G, and a finite set T of places of F (that includes the ramified

primes for ρ, ρ', π and π') such that

$$L_v(s, \rho) = L_v(s, \pi)$$
$$L_v(s, \rho') = L_v(s, \pi')$$

for all $v \notin T$.

Thus the theorem is sharp.

In the context of theorem 4.1, we note that since the cuspidal automorphic representations ρ, ρ' are locally isomorphic for a set of places of density, and thus of lower density, greater than $3/5$, the representations must have symmetric squares that are twist-equivalent.

Indeed, we note that the representations themselves are twist-equivalent. If we tensor $\rho' = \tau \otimes \text{sgn}$ with the one-dimensional representation $1 \otimes \text{sgn}$ we obtain $(\tau \otimes \text{sgn}) \otimes (1 \otimes \text{sgn}) = \tau \otimes 1 = \rho$. Thus ρ, ρ' are twist-equivalent.

4.5 The tetrahedral case

Here we prove theorem 4.1 in the tetrahedral case.

In the case of theorem 4.2 for the tetrahedral case, we will not prove it explicitly, but we note that it simply follows from combining the approach used in section 4.3 with that of this section.

For π tetrahedral, one knows that $\text{Sym}^2\pi$ is cuspidal, but $\text{Sym}^3\pi$ and $\text{Sym}^4\pi$ are not.

We will begin by showing

Proposition 4.5. *The L-function associated to* $\text{Sym}^4\pi$ *has no pole at* $s = 1$.

Proof. This simply follows from the Clebsch-Gordon decomposition of tensor products of representations of dimension two, and is certainly well-known to the experts; we are including the details here for completeness.

We will use

Lemma 4.6. *Let T be the set of ramified and infinite places. Then for a cuspidal automorphic representation π, we have*

$$L^T(s, \mathrm{Sym}^2\pi \times \mathrm{Sym}^2\pi) = L^T(s, \mathrm{Sym}^4\pi)L^T(s, \mathrm{Sym}^2\pi)\zeta_F(s).$$

Proof. Fix $v \in T$ and write $\alpha_{j,v}$ as α_j.

Note that $A(\mathrm{Sym}^2\pi_v) \otimes A(\mathrm{Sym}^2\pi_v)$ can be represented by

$$\begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix} \otimes \begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix}$$

which can be expressed as

$$\begin{pmatrix} \alpha^4 & & & & & & & & \\ & \alpha^2 & & & & & & & \\ & & \alpha^2 & & & & & & \\ & & & 1 & & & & & \\ & & & & 1 & & & & \\ & & & & & 1 & & & \\ & & & & & & \alpha^{-2} & & \\ & & & & & & & \alpha^{-2} & \\ & & & & & & & & \alpha^{-4} \end{pmatrix}$$

$$\sim \begin{pmatrix} \alpha^4 & & & & \\ & \alpha^2 & & & \\ & & 1 & & \\ & & & \alpha^{-2} & \\ & & & & \alpha^{-4} \end{pmatrix} \oplus \begin{pmatrix} \alpha^2 & & \\ & 1 & \\ & & \alpha^{-2} \end{pmatrix} \oplus 1$$

thus $A(\mathrm{Sym}^2\pi_v) \otimes A(\mathrm{Sym}^2\pi_v)$ is equivalent to $A(\mathrm{Sym}^4\pi_v) \oplus A(\mathrm{Sym}^2\pi_v) \oplus 1$ for all unramified v, and so we obtain the identity of the lemma. □

We return to the proof of the proposition. Now given that Sym^2 is a GL(3) cusp form with trivial character, the corresponding L-function has no pole at $s = 1$ and furthermore is non-zero at that point. We also know that the Rankin-Selberg L-function on the left-hand side of the L-function identity from the lemma has a simple pole at $s = 1$. The same holds for the Dedekind zeta function $\zeta_F(s)$ at $s = 1$.

Thus examining the identity from the lemma, we obtain that the symmetric fourth power L-function has no pole at $s = 1$ and is non-zero at that point.

Thus the proposition holds.

□

We also note, by Jacquet-Shalika [JS1] and Shahidi [Sha], that the L-function associated to the symmetric fourth power is non-vanishing at $s = 1$ since the symmetric fourth power automorphic representation is an isobaric sum of unitary cuspidal automorphic representations.

We now prove

Theorem 4.7. *Let $\pi, \pi' \in \mathcal{A}_0(\mathrm{GL}_2(\mathbb{A}_F))$ be tetrahedral representations with trivial central character and symmetric squares that are not twist-equivalent. For finite places v where π and π' are unramified, set $a_v = \mathrm{Tr}(A(\pi_v))$, $b_v = \mathrm{Tr}(A(\pi'_v))$, and let $S = \{v \mid a_v \neq b_v\}$. Then*

$$\underline{\delta}(S) \geq \frac{2}{5}$$

where $\underline{\delta}(S)$ is the lower Dirichlet density of the set S.

Proof. From inequality (4.1)

$$\begin{aligned}
&\sum_v \frac{a_v^2}{\mathrm{N}v^s} - \sum_v \frac{2a_v b_v}{\mathrm{N}v^s} + \sum_v \frac{b_v^2}{\mathrm{N}v^s} \\
&\leq \left(\sum_v \frac{a_v^4}{\mathrm{N}v^s} - \sum_v \frac{4a_v^3 b_v}{\mathrm{N}v^s} + \sum_v \frac{6a_v^2 b_v^2}{\mathrm{N}v^s} - \sum_v \frac{4a_v b_v^3}{\mathrm{N}v^s} + \sum_v \frac{b_v^4}{\mathrm{N}v^s} \right)^{1/2} \\
&\quad \cdot \left(\sum_{v \in S} \frac{1}{\mathrm{N}v^s} \right)^{1/2} \\
&\leq \left(\sum_v \frac{a_v^4}{\mathrm{N}v^s} + \sum_v \frac{6a_v^2 b_v^2}{\mathrm{N}v^s} + \sum_v \frac{b_v^4}{\mathrm{N}v^s} \right)^{1/2} \cdot \left(\sum_{v \in S} \frac{1}{\mathrm{N}v^s} \right)^{1/2}.
\end{aligned}$$

Using the proposition above and results from earlier in this chapter, we have the following:

$$\begin{aligned}
\sum \frac{a_v^4}{\mathrm{N}v^s} &= 2 \log \left(\frac{1}{s-1} \right) + o\left(\log \left(\frac{1}{s-1} \right) \right) \\
\sum \frac{a_v^2 b_v^2}{\mathrm{N}v^s} &= \log \left(\frac{1}{s-1} \right) + o\left(\log \left(\frac{1}{s-1} \right) \right).
\end{aligned}$$

Applying this and earlier results to the inequality above, we obtain

$$\begin{aligned}
2 &\leq 10^{1/2} \cdot \underline{\delta}(S)^{1/2} \\
\frac{2}{5} &\leq \underline{\delta}(S).
\end{aligned}$$

□

4.6 The tetrahedral case: an example

We will construct two tetrahedral cuspidal automorphic representations whose symmetric squares are not twist-equivalent and whose Hecke eigenvalues agree on a set on density 17/32.

We achieve this by constructing two representations of dimension two of the binary tetrahedral group $\widetilde{A_4}$ with suitable properties. Since $\widetilde{A_4}$ is well-known to appear as a Galois group over $\mathbb{Q}$, we can lift such representations to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then we apply

Arthur-Clozel [AC] to obtain the existence of automorphic representations as described in the paragraph above.

4.6.1 The binary tetrahedral group

We will present the binary tetrahedral group $G := \widetilde{A_4}$ as follows. Let i, j, k be the quaternions and let $\omega = -\frac{1}{2}(1 + i + j + k)$. Note that ω has order 3. G is generated by i, j, ω, with the following relations:

$$\begin{aligned}\omega i\omega^{-1} &= j\\ \omega j\omega^{-1} &= k\\ \omega k\omega^{-1} &= i.\end{aligned}$$

Thus we can express G as the semi-direct product $Q \rtimes_\phi C$ where C is the order 3 subgroup generated by ω, $\phi : C \to \mathrm{Aut}Q$ with $\phi(\omega) = \phi_\omega : q \mapsto \omega q\omega^{-1}$, where the conjugate satisfies the relations mentioned above. Thus G has 24 elements; the only (non-trivial) normal subgroup, other than Q, is $\{\pm 1\}$.

Note that the conjugacy classes of this group are

$$\{1\}, \{-1\}, \{\pm i, \pm j, \pm k\}, \{\omega, -i\omega, -j\omega, -k\omega\}, \{-\omega, i\omega, j\omega, k\omega\},$$
$$\{\omega^2, -i\omega^2, -j\omega^2, -k\omega^2\}, \{-\omega^2, i\omega^2, j\omega^2, k\omega^2\}.$$

Thus the 24 elements are distributed over 7 conjugacy classes.

4.6.2 Irreducible representations

We have three one-dimensional irreducible representations coming from the irreducible representations on C, so that leaves us with four irreducible representations whose degrees n_i give $\sum n_i^2 = 24 - 3 = 21$. We need at least one three-dimensional representation to help achieve this number, and two of them would lead to the remaining ones satisfying $n^2 + n'^2 = 3$ which is not possible. Thus we have exactly one three-dimensional representation. This leaves $n^2 + n'^2 + n''^2 = 12$ thus the remaining three irreducible representations must all be two-dimensional.

Starting with the one-dimensional representations, we note that this is based on C, where we map the generator of this subgroup to 1, ζ or ζ^2, where ζ is the primitive root of unity $e^{2\pi i/3}$.

The three-dimensional representation can be found using SO(3). We do not need the details of this particular representation for the purposes of this section, but, for completeness, we will still include its character table below.

This leaves the three two-dimensional representations. First, we have the representation ρ, under which

$$i \mapsto \begin{pmatrix} i & \\ & -i \end{pmatrix}$$
$$\omega \mapsto -\frac{1}{2}\begin{pmatrix} 1+i & -1+i \\ 1+i & 1-i \end{pmatrix}.$$

The other two can be obtained by twisting ρ by the two non-trivial one-dimensional characters.

Thus the character table is:

	$\{1\}$	$\{-1\}$	$[i]$	$[\omega]$	$[-\omega]$	$[\omega^2]$	$[-\omega^2]$
χ_0	1	1	1	1	1	1	1
χ_1	1	1	1	ζ	ζ	ζ^2	ζ^2
χ_2	1	1	1	ζ^2	ζ^2	ζ	ζ
ρ	2	-2	0	-1	1	-1	1
$\rho \otimes \chi_1$	2	-2	0	$-\zeta$	ζ	$-\zeta^2$	ζ^2
$\rho \otimes \chi_2$	2	-2	0	$-\zeta^2$	ζ^2	$-\zeta$	ζ
ψ	3	3	-1	0	0	0	0

4.6.3 Galois structure

We are interested in the image in $\mathrm{GL}_2(\mathbb{C})$ of a tetrahedral representation, which is isomorphic to the binary tetrahedral group $\widetilde{A_4}$. This allows us to establish the nature

of the (smallest) Galois group that the representation factors through. Let us denote this Galois group as $\mathrm{Gal}(K/\mathbb{Q})$. We have the following structure of Galois fields:

$$\begin{array}{c} K \\ | \\ 2 \\ | \\ F \\ | \\ 4 \\ | \\ k \\ | \\ 3 \\ | \\ \mathbb{Q} \end{array}$$

Note that $F/\mathbb{Q}$ is Galois since $\{\pm 1\} \lhd \widetilde{A_4}$ and furthermore its Galois group is isomorphic to A_4. Similarly, we have that $k/\mathbb{Q}$ is also Galois with group isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

4.6.4 Combined Galois structures for two different tetrahedral Artin representations

We would like to determine how similar (in terms of agreement on traces of Frobenius) two Artin representations ρ_1, ρ_2 can be without having symmetric squares that are twist-equivalent.

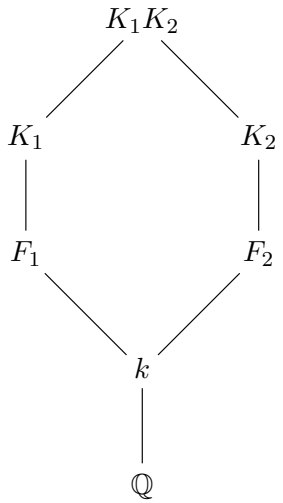
For each representation ρ_i we have a structure

$$\begin{array}{c} K_i \\ | \\ 2 \\ | \\ F_i \\ | \\ 4 \\ | \\ k_i \\ | \\ 3 \\ | \\ \mathbb{Q} \end{array}$$

and we will add the condition that $k_1 = k_2 = k$ with the intention of increasing the

amount of agreement on the traces of Frobenius. Note that we could also require $F_1 = F_2$, which gives us representations with 5/8 of Frobenius traces in common (assuming that $K_1 \neq K_2$), but they will have twist-equivalent symmetric squares, which is not what we want. Therefore we will specify that $F_1 \neq F_2$ and $K_1 \neq K_2$.

In order to establish the density of primes such that Frobenius traces are equal for both representations, we need to consider:



Thus we not only need to establish the degree of the compositum extension, but its Galois group.

4.6.5 The compositum

We recall the following theorem:
Given two Galois extensions E,F of K, we have that $E \cap F$ and EF are Galois over K. Furthermore, we have a map

$$\mathrm{Gal}(EF/K) \hookrightarrow \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$$
$$\sigma \mapsto (\sigma|_E, \sigma|_F)$$

(note that the kernel would be any element of $\mathrm{Gal}(EF/K)$ that fixes both E and F, but then this would mean that EF is fixed; thus the map is injective).
The image of this map is $H = \{(\phi, \psi) \mid \phi|_{E\cap F}, \psi|_{E\cap F}\}$.

Thus we need to use this theorem to determine (using the notation from the previous section) $\mathrm{Gal}(K_1K_2/\mathbb{Q})$. This gives us an explicit form for the group, which is made up of the following elements:

- pairs of the form (a, b) where $a, b \in \{\pm 1, \pm i, \pm j, \pm k\}$,
- pairs of the form (a, b) where $a, b \in \{\pm\omega, \pm i\omega, \pm j\omega, \pm k\omega\}$,
- pairs of the form (a, b) where $a, b \in \{\pm\omega^2, \pm i\omega^2, \pm j\omega^2, \pm k\omega^2\}$.

We note that this Galois group thus has size $3 \cdot 8^2 = 192$.
We can consider the representation $\rho_1 \times \rho_2 : \mathrm{Gal}(K_1K_2/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$. Given a conjugacy class of this Galois group, if we take the trace of the individual components and observe them to be equal, then that will correspond to a set of rational primes P of given positive density d where $\mathrm{tr}\rho_1(\mathrm{Frob}_p) = \mathrm{tr}\rho_2(\mathrm{Frob}_p)$.

4.6.6 Counting

We will count these occurrences, which can be achieved by listing those elements of $\mathrm{Gal}(K_1K_2/\mathbb{Q})$ that satisfy this condition on the traces:

- pairs $(1, 1)$ and $(-1, -1)$
- pairs (a, b) where $a, b \in \{\pm i, \pm j, \pm k\}$
- pairs (a, b) where $a, b \in \{\omega, -i\omega, -j\omega, -k\omega\}$
- pairs (a, b) where $a, b \in \{-\omega, i\omega, j\omega, k\omega\}$
- pairs (a, b) where $a, b \in \{\omega^2, i\omega^2, j\omega^2, k\omega^2\}$
- pairs (a, b) where $a, b \in \{-\omega^2, -i\omega^2, -j\omega^2, -k\omega^2\}$

These pairs have traces in common of 2, -2, 0, -1, 1, -1 and 1, respectively.
Counting the number of these pairs $(1 + 1 + 36 + 16 + 16 + 16 + 16)$ we obtain a density

of 17/32 (using the Chebotarev density theorem) for those primes that have traces of Frobenius that agree under the two different representations.

Since we can lift such representations to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, by Arthur-Clozel [AC] we obtain the existence of tetrahedral cuspidal automorphic representations π, π' such that the set $\{v \mid a(\pi_v) = a(\pi'_v)\}$ has a density of 17/32.

4.6.7 Symmetric squares

We now need to establish that the two representations do not have twist-equivalent symmetric squares.

First we determine the character table of the symmetric square representations. Using the formula $\chi_{\mathrm{Sym}^2}(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$,we obtain the following table:

	$\{1\}$	$\{-1\}$	$[i]$	$[\omega]$	$[-\omega]$	$[\omega^2]$	$[-\omega^2]$
χ_{Sym^2}	3	3	-1	0	0	0	0

Using the same idea as that in the previous subsection, we now examine pairs (as elements of $\mathrm{Gal}(K_1K_2/\mathbb{Q})$) to determine those that have different traces. The issue is to examine whether there exists a character ψ such that $\rho_1 \otimes \psi \simeq \rho_2$.
We note the element $(1, i)$, where the individual components have traces 3 and -1, respectively. However, since ψ must only take complex values of norm 1, there is no such character that will enable the above isomorphism to exist. Thus the symmetric squares are not twist-equivalent.

Bibliography

[AC] James Arthur and Laurent Clozel. *Simple algebras, base change, and the advanced theory of the trace formula*, volume 120 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1989.

[Dav] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[Deu] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DP] Chantal David and Francesco Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, (4):165–183, 1999.

[Elk1] Noam D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[Elk2] Noam D. Elkies. Supersingular primes for elliptic curves over real number fields. *Compositio Math.*, 72(2):165–172, 1989.

[FM] Etienne Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[GJ] Stephen Gelbart and Hervé Jacquet. A relation between automorphic representations of GL(2) and GL(3). *Ann. Sci. École Norm. Sup. (4)*, 11(4):471–542, 1978.

[Jam] Kevin James. Averaging special values of Dirichlet L-series. *Ramanujan J.*, 10(1):75–87, 2005.

[Jao] David Jao. Supersingular primes for points on $X_0(p)/w_p$. *J. Number Theory*, 113(2):208–225, 2005.

[JS1] H. Jacquet and J. A. Shalika. On Euler products and the classification of automorphic forms. II. *Amer. J. Math.*, 103(4):777–815, 1981.

[JS2] Hervé Jacquet and Joseph A. Shalika. A non-vanishing theorem for zeta functions of GL_n. *Invent. Math.*, 38(1):1–16, 1976/77.

[Jut] M. Jutila. On the mean value of $L(\frac{1}{2}, \chi)$ for real characters. *Analysis*, 1(2):149–161, 1981.

[KS1] Henry H. Kim and Freydoon Shahidi. Functorial products for $\mathrm{GL}_2 \times \mathrm{GL}_3$ and functorial symmetric cube for GL_2. *C. R. Acad. Sci. Paris Sér. I Math.*, 331(8):599–604, 2000.

[KS2] Henry H. Kim and Freydoon Shahidi. Cuspidality of symmetric powers with applications. *Duke Math. J.*, 112(1):177–197, 2002.

[LT] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in $\mathrm{G}L_2$-extensions of the rational numbers.

[LW] Jianya Liu and Yonghui Wang. A theorem on analytic strong multiplicity one. *J. Number Theory*, 129(8):1874–1882, 2009.

[Mar] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[MR] M. Ram Murty and C. S. Rajan. Stronger multiplicity one theorems for forms of general type on GL_2. In *Analytic number theory, Vol. 2 (Allerton Park, IL, 1995)*, volume 139 of *Progr. Math.*, pages 669–683. Birkhäuser Boston, Boston, MA, 1996.

[Ram] Dinakar Ramakrishnan. A refinement of the strong multiplicity one theorem for GL(2). Appendix to: "l-adic representations associated to modular forms over imaginary quadratic fields. II" [Invent. Math. **116** (1994), no. 1-3, 619–643; MR1253207 (95h:11050a)] by R. Taylor. *Invent. Math.*, 116(1-3):645–649, 1994.

[Ser1] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser2] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Ser3] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sha] Freydoon Shahidi. On certain L-functions. *Amer. J. Math.*, 103(2):297–355, 1981.

[Sil] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Wal1] Nahid Walji. A refinement of strong multiplicity one for GL(2). *preprint*.

[Wal2] Nahid Walji. Supersingular distribution on average for congruence classes of primes. *Acta Arith.*, 142(4):387–400, 2010.