The Parity of Analytic Ranks among Quadratic Twists of Elliptic Curves over Number Fields

Nava Balsam

Submitted in partial fulfillment of the
requirements for the degree
of Doctor of Philosophy
in the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2015

ABSTRACT

The Parity of Analytic Ranks among Quadratic Twists of Elliptic Curves over Number Fields

Nava Balsam

The parity of the analytic rank of an elliptic curve is given by the root number in the functional equation L(E,s). Fixing an elliptic curve over any number field and considering the family of its quadratic twists, it is natural to ask what the average analytic rank in this family is. A lower bound on this number is given by the average root number. In this paper, we investigate the root number in such families and derive an asymptotic formula for the proportion of curves in the family that have even rank. Our results are then used to support a conjecture about the average analytic rank in this family of elliptic curves.

Contents

0.1 Introduction 1

0.2 Elliptic Curves, Modular Forms, Modularity 4

0.2.1 Elliptic curves 4

0.2.2 Invariants of Elliptic Curves 7

0.2.3 A Theorem About $\mathrm{Pic}^0(E)$ 8

0.2.4 Isogenies 10

0.2.5 The Tate Module 11

0.2.6 The Weil Pairing 12

0.2.7 The Endomorphism Ring 14

0.2.8 The Weil Conjectures 15

0.2.9 The Weak Mordell-Weil Theorem 18

0.2.10 The Method of Descent 22

0.2.11 Modular forms 23

0.2.12 L-function of an elliptic curve and the Modularity Theorem 28

0.3 Automorphic Representation Theory 30

0.3.1 Introduction 30

0.3.2 Adeles and Automorphic Forms for GL(1) 31

0.3.3 Tate's Thesis 34

0.3.4 The work of Jacquet-Langlands on $GL(2)$. 37

0.3.5 Tabulation of Epsilon Factors 50

0.4 Root Numbers of Quadratic Twists of Elliptic Curves 52

0.4.1 Modularity, Revisited 52
0.4.2 Some Notation 53
0.4.3 Change in Global Root Number 54
0.4.4 The Density of Even Analytic Ranks 58
0.4.5 The Main Computations 62
0.4.6 Local Epsilon Factor Changes 62
0.4.7 A word about function fields 68
0.5 Comparison with Algebraic Results 68
0.5.1 Selmer Groups 68
0.5.2 Selmer Groups in Quadratic Families 70
0.5.3 Parity Conjectures 71

Bibliography **72**

Acknowledgements

I would like to thank Dorian Goldfeld for advising me on this thesis and for suggesting the problem. Dorian's earlier work on this problem has paved the way for many explorations of the subject and I'm grateful for the chance to be advised by him. Our weekly chats initially helped me grasp the subject more fully, and later, to understand and interpret the results of this thesis.

I would also like to thank my friends and colleagues for useful discussions: Rahul Krishna, Karl Koziol, Raju Krishnamoorthy, Phil Engel, Ashwin Deoparkur, Mike Woodbury, Ali Altug and professor Wei Zhang.

My parents and siblings: Ari, Rachel, Sara, Levi, Sima, Dani and Eli I would like to thank for their confidence and support.

I would like to thank Dave Bayer for inspiring to become a mathematician by being an awesome one. I would also like to thank Robert Lipshitz for his early encouragement and advice, without which I would have floundered before I had even begun.

Finally and most of all, I thank my dear husband Ben Balsam, for his patience, love, and for being a terrific listener.

To Ben and Bertram.

0.1 Introduction

Associated to an elliptic curve E over a field K is a family of curves, its quadratic twists. Within this family, it is natural to consider the the distribution of the most intriguing invariant of an elliptic curve, its Mordell-Weil rank, which, via the Birch and Swinnerton-Dyer conjecture is equal to its analytic rank. This investigation began when Goldfeld [8] conjectured that the average analytic rank in such a family associated to an elliptic curve over $\mathbb{Q}$, is $\frac{1}{2}$. The motivation for this conjecture comes from considering the root number in the $L-$function of a twisted elliptic curve and the folklore conjecture that elliptic curves of rank ≥ 2 are rare. The result of this paper is a generalization of the conjecture to elliptic curves over arbitrary number fields. In many cases we find that the twists of E/K do not have even and odd analytic rank in equal proportion and therefore the conjectured average value of the analytic rank is not $\frac{1}{2}$.

Recently, such an analysis was undertaken by Klagsbrun, Mazur and Rubin [11], wherein they find the density of curves of even Selmer rank among a family of quadratic twists. Using their results, they formulate a generalization of Goldfeld's conjecture for elliptic curves over number fields. Some of their techniques lend themselves to the analytic aspect as well and have been a major inspiration for this paper. We are able to verify their results in many cases, equating the average algebraic rank (mod 2) with the average analytic rank (mod 2). Thus, the result of this paper can be viewed as a parity conjecture *on average* in this family of elliptic curves. In other words, the proportion of elliptic curves with even algebraic rank is equal to the proportion of curves that have even analytic rank, in a family of quadratic twists.

Because of the convenience of dealing with automorphic representations of $GL(2)$, in this paper we only consider elliptic curves which are modular, a property which is defined as follows. Let E be an elliptic curve with conductor $\mathfrak{N}$ over a number field K. Then E is modular if the Hasse-Weil $L-$function of E/K is equal to the $L-$function of a cuspidal Hilbert modular form of parallel weight 2, and level $\mathfrak{N}$ (See[7]). In particular, the Hasse-Weil $L-$function of E, denoted $L(E/K, s)$ or simply $L(E, s)$ is equal to the $L-$function of

a cuspidal automorphic representation $\pi_E = \otimes \pi_{E,v}$ of $GL(2, \mathbb{A}_K)$ associated to a Hilbert modular form, and therefore $L(E, s)$ satisfies a functional equation. It is known that all elliptic curves over $K = \mathbb{Q}$ are modular [1] and recently it has been shown that most elliptic curves over totally real fields and real quadratic extensions of totally real fields, are modular [12; 6].

Let $\Lambda_E(s)$ denote the "completed" L-function of π_E , that is, including the factors at the archimedian places. Then the functional equation takes the form $\Lambda_E(s) = w\Lambda(1-s)$ where $w \in \{\pm 1\}$, called the root number will play a pivotal role in this paper. The **analytic rank** of E, denoted $rk(E)$ is defined as

$$rk(E) = \text{order of vanishing of } \Lambda_E(s) \text{ at } s = \frac{1}{2}.$$

For an elliptic curve E/K, we study the **quadratic twists** of E: these are elliptic curves E' which are isomorphic to E over some quadratic extension K'/K. In order to make assertions about density in a family of curves, it is necessary to order them in some way. Suppose that E' is isomorphic to E over some quadratic field K'. Then via standard class field theory, there is a unique quadratic Hecke character χ, associated to the extension K'/K. Let E^χ be the curve which is isomorphic to E over the quadratic field K' with associated Hecke character χ and let $C(K)$ be the set of all quadratic Hecke characters of $\mathbb{A}_K^\times$. For $\chi \in C(K)$, let $q_1, q_2, ..., q_n$ be the places where χ is ramified. Then we define the norm, $N\chi = \max_i \{Nq_i\}$ which gives an ordering of twists of an elliptic curve. Our main result is the following,

Theorem. *Let E be a modular elliptic curve over a number field K such that no local supercuspidal representations occur in the factorization of π_E, then*

$$\lim_{X \to \infty} \frac{\#\{\chi \in C(K) \mid N\chi \leq X \text{ and } rk(E^\chi) \text{ is even}\}}{\#\{\chi \in C(K) \mid N\chi \leq X\}} = \frac{1 + (-1)^{rk(E)}\kappa}{2}$$

where $\kappa = \prod \kappa_v$ is a product over the places of K given by

$$\kappa_v = \begin{cases} 0 & \text{if } K_v \backsimeq \mathbb{R} \\ 1 & \text{if } K_v \backsimeq \mathbb{C} \\ 2/|c_v| - 1 & E \text{ has split mutiplicative reduction at } v \\ 1 - 2/|c_v| & E \text{ has nonsplit multiplicative reduction at } v \\ 1 - 2/|c_v| & E \text{ has multiplicative reduction in a quadratic extension at } v \\ 1 & E \text{ has potentially multiplicative reduction (non-quadratic)} \\ 1 & \text{otherwise} \end{cases}$$

and $|c_v|$ *is the number of degree 2 extensions of* K_v *(if* $v \mid 2$ *then* $|c_v| = 4 \cdot 2^{[K_v:\mathbb{Q}_v]}$*) otherwise* $|c_v| = 4$*)* .

Note that if the field K has a real embedding then the density of even analytic ranks is exactly $\frac{1}{2}$.

The organization of this thesis is as follows. Section 0.2 provides a brief background and summary of elliptic curves and modular forms focussing on the results that are needed for the main results. The next section, Section 0.3, is a brief overview of the theory of automorphic representations for $GL(1)$ (Tate's thesis) and $GL(2)$ (via Jacquet-Langlands) concluding with the tabulation of the local epsilon factors in each case. In Section 0.4 we present the main result of the paper along with the computation of the changes in the local epsilon factors. Finally, in sections 5 and 6 we present the algebraic side of our main result together with the work of Klagsbrun, Mazur and Rubin [11] and the work of Dokchitser and Dokchitser which relate the algebraic and analytic sides[5].

0.2 Elliptic Curves, Modular Forms, Modularity

0.2.1 Elliptic curves

In number theory, the study of elliptic curves is related to some very well-known problems including Fermat's Last Theorem, the Birch and Swinnerton-Dyer theorem, and the ABC-conjecture to name a few. The intrigueing arithmetic properties of elliptic curves are thought to contain deep secrets of number theory and they have been a subject of active research for quite some time. I will begin with some basic definitions and facts about elliptic curves, mainly to introduce the notation and background material for this thesis.

Definition 1. An elliptic curve is a smooth projective curve of genus 1 with a marked point.

The marked point will ensure that we have a group structure, indeed it is usually taken to be the identity element. Next, we show that every elliptic curve can be embedded in $\mathbb{P}^2$ by using the Riemann Roch Theorem. Suppose that C is a curve with field of definition K.

Let D be a divisor on C. We define the vector space:

$$\mathcal{L}(D) = \left\{ f \in \bar{K}(C) \middle| div(f) \geq -D \right\} \cup \{0\}$$

Where $D_1 > D_2$ if the coefficient at every point is larger in D_1.

We also define $\ell(D) = \dim\mathcal{L}(D)$. Two divisors are said to be equivalent if their formal difference is the divisor of a function on C. That is

$$D_1 \sim D_2 \text{ if } div(f) = D_1 - D_2 \text{ for some } f \in \bar{K}(C).$$

Claim 2. If $deg(D) < 0$ then $\mathcal{L}(D) = 0$

Claim 3. If $D \sim D'$ then $\mathcal{L}(D) \cong \mathcal{L}(D')$

If K_C is the divisor of a differential (called a canonical divisor) then $\mathcal{L}(K_C)$ space of holomorphic differentials.

These claims are proved easily from the definitions.

Theorem 4. *(Riemann-Roch)*

$$\ell(D) - \ell(K_C - D) = deg(D) - g + 1$$

Corollary 5. $\ell(K_C) = g$ *(proved using D=0)*

$degK_C$ =2(g-1) *(proved using* $D = K_C$*)*

If $degD > 2g - 2$ *then* $\ell(D) = degD - g + 1$ *(follows from* $deg(K_C - D) < 0$*)*

Note: Riemann Roch can also be used to define the genus as the invariant g .

Fact 6. *Riemann Roch is true also if we only consider functions in* $K(C)$ *and not in the algebraic closure which can be proved via a galois-descent argument. We will need this version below, since elliptic curves over non-algebraically closed fields will be of interest.*

Theorem 7. *Any genus 1 curve with a basepoint is isomorphic to a curve of the form*

$$x^3 + Bx^2y + Dxy + Ex^2 + y^2 + Gx + Hy + I = 0$$

with basepoint (in projective space [x:y:z]) equal to [0:1:0].

Proof. Let the basepoint of the curve be denoted $\mathcal{O}$. We consider the divisor $2\mathcal{O}$. Since $2 = deg(2\mathcal{O}) = 2g - 2 = 0$ by corollary5, $\ell(2\mathcal{O}) = 2$. We can take $\{1, X\}$ as a basis for $\mathcal{L}(2\mathcal{O})$ where X is some function with a pole of order 2 at $\mathcal{O}$. Similarly $\ell(3\mathcal{O}) = 3$ and since $\mathcal{L}(2\mathcal{O}) \subset \mathcal{L}(3\mathcal{O})$ we can complete to a basis $\{1, X, Y\}$ where Y has a pole of order 3 at $\mathcal{O}$. By the same arguments, $\ell(6\mathcal{O}) = 6$ and $\mathcal{L}(6\mathcal{O})$ contains the seven elements $\{X^3, Y^2, X^2, Y, X, XY, 1\}$ therefore there must be a linear relationship

$$AX^3 + BX^2Y + DXY + EX^2 + FY^2 + GX + HY + I = 0 \tag{0.2.1}$$

Furthermore, $AF \neq 0$ otherwise every term would have a pole of a different order at $\mathcal{O}$ which could never add up to zero. We then scale X and Y to make the coefficients A and F equal to 1.

Now consider the map $\phi : E \to \mathbb{P}^2$ given by

$$\phi(p) = [X(p), Y(p), 1]$$

Which surjects onto the locus of the curve (0.2.1). Furthermore this map has degree one since if we look at the function field extensions

$$[K(E) : K(X)] = 2$$

and

$$[K(E) : K(Y)] = 3$$

and since $[K(E) : K(X, Y)]$ divides both 2 and 3 it must be 1 and so the map ϕ is degree 1; the map is an isomorphism. □

Claim 8. The Weierstrass equation for $E \to C \subset \mathbb{P}^2$ is smooth. If it were singular then there would exist a map $\psi : C \to \mathbb{P}^1$ of degree 1 and we'd have that

$$\psi \circ \phi : E \to \mathbb{P}^1$$

is a map of smooth curves of degree 1. Therefore it must be an isomorphism. But E has genus 1 so such an isomorphism is impossible and the map $E \to C \subset \mathbb{P}^2$ is smooth.

Theorem 9. (Isomorphic change of variables). Two curves in Weierstrass form are isomorphic if and only if

$$x = u^2x' + r, y = u^3y' + su^2 + t$$

Proof. The only choice we made was in picking a basis of $\mathcal{L}(2\mathcal{O})$ and $\mathcal{L}(3\mathcal{O})$. If instead we chose a new basis

$$x = u_1x' + r$$
$$y = u_2y' + s_2x' + t$$

Since the Weierstrass equation is monic in X^3 and Y^2 we have that $u_1^2 = u_2^3$. Then if $u = u_2/u_1$ and $s = s_2/u^2$ we get the result. □

Theorem 10. *A smooth Weierstrass equation*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with basepoint $[0:1:0]$ *has genus 1.*

Proof. We consider the differential

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

has trivial divisor (it is nowhere vanishing and holomorphic). Therefore by Rieman Roch, $K_C = div(\omega) = 0 = 2g - 2$. So $g = 1$. □

The above discussion shows that in studying elliptic curves we are justified in studying their embeddings in $\mathbb{P}^2$ via the Weirstrass equation.

0.2.2 Invariants of Elliptic Curves

Let E/K be an elliptic curve. If $char(K) \neq 2, 3$ we can always choose an isomorphism of the curve to give the Weierstrass form

$$E : y^2 = x^3 + Ax + B$$

It is very easy to state the Δ and j-invariants in this form (otherwise it quite a messy formula involving the full set of coefficients)

$$\Delta(E) = -16(4A^3 + 27B^2)$$
$$j(E) = -1728\left(\tfrac{4A}{\Delta}\right)^3$$

Again if $char(K) \neq 2, 3$ then we can put it in the form (if we work over the algebraic closure of K)

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

in this form we have the invariant $\lambda \in \bar{K}$. And

$$j(E_\lambda) = \frac{2^8(\lambda^2-\lambda-1)^3}{\lambda^2(\lambda-1)^2}$$

$$j(E_\lambda)$$

There's a surjective map

$$\bar{K}\backslash 0,1, \to \bar{K} \text{ by } \lambda \mapsto j(E_\lambda)$$

that is $6:1$ at most places.

The Δ-invariant is called the **discriminant** of the Weirstrass equation of elliptic curve. It is a useful invariant but unfortunately, it depends on the Weirstrass form and a change of variables in x, y will change the discriminant. One way around this fact is the following: if K is a local field, with a valuation v then consider the set S of *all* the discriminants of E/K and choose one with the smallest valuation (of course this is unique only up to a unit). The Weirstrass form with the smallest valuation is called the **minimal model** for E/K and it has **minimal discriminant** Δ. When no model for E/K is indicated, the symbol Δ refers to it's minimal discriminant.

0.2.3 A Theorem About $\mathbf{Pic}^0(E)$

Theorem 11. *$Pic^0(E) \cong E$*

Proof. First we must say what the map is. In one direction the maps is

$$\kappa : E \to Pic^0(E),\ P \mapsto (P) - (O).$$

We'll show what the map in the other direction is. Consider a degree-zero divisor D. By Riemann Roch,

$$\ell(D + (\mathcal{O})) = deg(D + (\mathcal{O})) - g + 1 = 1.$$

So let the function $f \in \mathcal{L}((D + (\mathcal{O})) = \left\{ g \in K(E) \middle| div(g) \geq -D - (\mathcal{O}) \right\}$. But since $f \in K(E)$, $deg(div(f)) = 0$. On the other hand $div(f) \geq -D - (\mathcal{O})$ so f has *exactly* one more zero. Therefore $div(f) = -D - (\mathcal{O}) + (P)$. So $D \sim (P) - (\mathcal{O})$. We take the map

$$\sigma : Div^0 \to E, \qquad \sigma(D) = P$$

Alternatively, we can take σ to be the map which "adds up" the divisor as if it were a group element:

$$\sigma\left(\sum_i e_i(P_i)\right) = \sum_i [e_i]P_i$$

That σ is well defined and injective will follow from the following lemma. □

Lemma 12. *Suppose that* $(P) - (O) \sim (Q) - (O)$ *then* $P = Q$

Proof. Suppose there were a function f such that $div(f) = (P) - (Q)$. Then f is in $\mathcal{L}((Q))$. But $\ell((Q)) = deg(Q) - g + 1 = 1$. The constant functions are certainly in $\mathcal{L}((Q))$, therefore f must be a constant function with empty divisor and therefore $P = Q$. □

Proposition 13. $\sigma : Pic^0(E) \to E$ *is an isomorphism.*

Proof. We already showed injectivity. σ is certainly surjective since $\sigma\left((P) - (\mathcal{O})\right) = P$. So we have a bijection of sets.

Let κ be the inverse of σ. In other words $\kappa(P) = (P) - (\mathcal{O})$. Suppose that $P + Q + R = 0$. Let $f_1(X, Y, Z)$ be a line in $\mathbb{P}^2$ that intersects E at P, Q and R. Let $f_2(X, Y, Z)$ be a line that intersects E at R and $\mathcal{O}$ (and at $-R$). Then $0 \sim div(f_1/f_2) = (P) + (Q) - (\mathcal{O}) - (P + Q)$. So .

$$\kappa(P) + \kappa(Q) - \kappa(P + Q) = (P) + (Q) - (\mathcal{O}) - (P + Q) \sim 0$$

□

0.2.4 Isogenies

Definition 14. An isogeny is a morphism $E_1 \to E_2$ such that $\mathcal{O}_1 \mapsto \mathcal{O}_2$.

Example 15. The map $[m] : E \to E$ by $x \mapsto \underbrace{x + x + ... + x}_{m}$ where addition denotes the group law on the elliptic curve.

Lemma 16. *Multiplication by m is non-constant*

Proof. $[2] \neq 0$. This is clear because there are only finitely many points of order 2.

$[m] \neq 0$ When m is odd. Choose P, a non-trivial point of order 2 (in the algebraic closure). Then $[m]P \neq 0$ since m is odd. □

Proposition 17. *$Hom(E_1, E_2)$ is an integral domain (and a torsion free $\mathbb{Z} - module$.)*

Proof. Suppose that $\phi \circ \psi = [0]$, then the degree of $\phi \circ \psi$ is 0. So one of ψ or ϕ must have degree 0. □

Proposition 18. *Any isogeny is a homomorphism.*

Proof. Suppose $\phi : E_1 \to E_2$ and $\phi(\mathcal{O}_1) = \mathcal{O}_2$. Then $\phi_* : Pic^0(E_1) \to Pic^0(E_2)$, $\phi_*((\mathcal{O}_1)) = ((\mathcal{O}_2))$ and $\phi_*((P)) = (\phi(P))$ and we extend linearly to the whole group so that it is a homomorphism. Then by Proposition 13, ϕ is a homomorphism. □

Definition 19. (The dual Isogeny) Let $\phi : E_1 \to E_2$ be an isogeny we have the following sequence of functions

$$\begin{array}{lllll} E_2 \to & Div^0(E_2) & \overset{\phi^*}{\to} Div^0(E_1) & & \to E_1 \\ Q \mapsto & (Q) - (\mathcal{O}) & \to \sum\limits_{\phi(P)=Q} e_p P & & \to \sum [e_p]P \end{array}$$

We define the dual isogeny $\hat{\phi} : E_2 \to E_1$ as the composition of these. More explicitly

$$\hat{\phi}(Q) = \sum_{\substack{\phi(P)=Q \\ \text{with degree} e_p}} [e_p]P$$

Where the sum is over the elements in the inverse image with multiplicity. The following facts follow from the definitions above:

- $\phi \circ \hat{\phi} = [deg\phi]$
- $\widehat{\phi_1 + \phi_2} = \hat{\phi}_1 + \hat{\phi}_2$
- $\widehat{\phi_1 \circ \phi_2} = \hat{\phi}_1 \circ \hat{\phi}_2$
- $\hat{\hat{\phi}} = \phi$
- $[m] = [\hat{m}]$
- $deg[m] = m^2$
- The $\hat{}$-operator is an involution on the ring $End(E_1, E_2)$

0.2.5 The Tate Module

The ℓ-adic Tate module is an object attached to an elliptic curve. It is used to define the Galois Representation associated to the elliptic curve and the eigenvalues of the Galois group acting on it are used in the definition of the $L-$function.

The following is a useful lemma about the p-torsion of an elliptic curve.

Lemma 20. *Let $E[m]$ denote the elements P of E such that $mP = \mathcal{O}$. Suppose that $m \neq 0$ and that $p = char(K)$ does not divide m. Then*

$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m$$

otherwise, if p divides m then

$$E[p^e] = \begin{cases} \{0\} \\ \mathbb{Z}/p^e\mathbb{Z} \end{cases}$$

Definition 21. The $\ell - adic$ Tate module is defined as

$$T_\ell = \underleftarrow{lim}_n E[\ell^n]$$

If m doesn't divide the characteristic of K then

$$T_\ell \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

There is a representation $G_{\bar{K}/K} \to Aut(T_\ell)$ induced from the action of $G_{\bar{K}/K}$ on $E[m]$ for each m. The group $Aut(T_\ell)$ is just $GL(2, \mathbb{Z}_\ell)$.

Lemma 22. *The abelian group $Hom(E_1, E_2)$ has rank at most 4.*

Proof. There's an injection

$$Hom(E_1, E_2) \bigotimes \mathbb{Z}_\ell \hookrightarrow Hom(T_\ell(E_1), T_\ell(E_2))$$

(this requires a bit of algebra). Now, since $Hom(T_\ell(E_1), T_\ell(E_2))$ has rank at most 4 the lemma follows. □

0.2.6 The Weil Pairing

Definition 23. The Weil Pairing is a map

$$e_m(S, T) : E[m] \times E[m] \to \mathbb{C}$$

defined as follows. Fix $T \in E[m]$ then there exists a function f_T with divisor $(T) - (O)$. Let T' bec such that $[m]T' = T$ (rememeber we're in the algebraic closure) then there exists g_T such that $div(g_T) = [m]^*T - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R)$

then, scaling if necessary, $f_T \circ [m] = g_T^m$. (since they have the same divisor)

We can now define

$$e_m(S, T) = \frac{g_T(S + X)}{g_T(X)} \text{ for any } X \in E$$

Definition 24. (Alternate Definition of the Weil Pairing) Let $S, T \in E[m]$ then choose f and g such that

$$div(f) = m(S) - m(O)$$
$$div(g) = m(T) - m(O)$$

Then

$$e_m(S,T) = \frac{f(T)}{f(O)} \cdot \frac{g(O)}{g(S)}$$

By Weil Reciprocity this is a mth root of unity, giving us a pairing.[1]

Claim 25. The Weil Pairing is alternating, bilinear, Galois invariant and surjective

Claim 26. An isogeny and its dual are adjoint with respect to the Weil Pairing

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$$

We easily extend the Weil pairing to the $\ell-$ adic Tate modules

$$e(S, \hat{\phi}_\ell(T)) = e(\phi_\ell(S), T)$$

The next lemma will be the main tool in proving the Weil Conjectures. It is quite remarkable.

Lemma 27. *Let ϕ be an isogeny and let ϕ_ℓ be the induced homomorphism on the Tate-modules. Then ϕ_ℓ is a linear map in $GL(2, \mathbb{Z}_\ell)$ and*

$$det(\phi_\ell) = deg(\phi)$$

Proof. The result follows from the above claims. Let u, v be a basis for T_ℓ and suppose that $\phi_\ell = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then we compute:

[1] $f(div(g)) = g(div(f))$ in this case: $f(T)^m \Big/ f(O)^m = g(T)^m \Big/ g(O)^m$

$$\begin{aligned} e(u,v)^{deg\phi} &= e([deg\phi]u, v) \\ &= e(\phi_\ell \circ \hat{\phi}_\ell u, v) \\ &= e(\phi(u), \phi(b)) \\ &= e(au + bv, cu + dv) \\ &= e(u,v)^{ad-bc} \end{aligned}$$

□

Lemma 28. $tr(\phi_\ell) = 1 + det(\phi_\ell) - det(1 - \phi_\ell) = 1 + deg(\phi) - deg(1 - \phi)$

Proof. It is true that for any 2x2 matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ that $det(1 - A) = (1 - a)(1 - d) - bc = 1 - a - d + ad - bc = 1 - tr(A) + det(A)$ □

0.2.7 The Endomorphism Ring

Theorem 29. *Let $End(E)$ be the ensome complicated stuff that boils downdomorphism ring of an elliptic curve. Then*

$$End(E) = \begin{cases} \mathbb{Z} & or \\ \text{an order in an imaginary quadratic extension of } \mathbb{Q} & or \\ \text{an order in a quaternion algebra} & or \end{cases}$$

Proof. We already showed that $End(E)$ has rank at most 4. Then using the involution $\hat{}$, we invoke the fact that any rank 4 $\mathbb{Z} - module$ with an involution that satisfies $\alpha\hat{\alpha} = 0 \iff \alpha = 0$ must be one of the above rings. We define norm and trace: $N(\alpha) = \alpha\hat{\alpha}$ and $Tr(\alpha) = \alpha + \hat{\alpha}$. Suppose there were an element such that $\alpha \notin \mathbb{Q}$, by a bit of subtracting, we can make it so that $Tr(\alpha) = 0$ and that $\alpha^2 = -N(\alpha)$ so $\alpha^2 < 0$ and $\alpha^2 \in \mathbb{Q}$. One keeps going, by finding such elements until you can't find anymore linearly independent ones. □

In characteristic 0, the endomorphism ring must be commutative so only the first two can happen. This is due to the fact that all field extensions are separable in characteristic 0.

In contrast to the Endomorphism ring, the Automorphism group is always finite and much simpler to compute. One already knows that the isomorphisms of an elliptic curve embedded in $\mathbb{P}^2$ are of the form

$$x = u^2x' + r$$
$$y = u^3y' + u^2x' + s$$

Now in characteristic $\neq 2, 3$ one can put the curve in the form

$$y^2 = x^3 + Ax + B$$

and the only isomorphisms preserving this form are

$$x = u^2x'$$
$$y = u^3y'$$

Substituting this into the curve we have that

$$u^6y^2 = u^6x^3 + Au^2x + B$$

So we need that $u^{-4}A = A$ and $u^{-6}B = B$. So unless $AB = 0$ u can only be ± 1.

The other cases (characteristic $2, 3$ and $AB = 0$) follow similarly and we find that the Automorphism group of an elliptic curves is always of degree dividing 24.

0.2.8 The Weil Conjectures

Definition 30. The Zeta-function of a projective variety V of dimension N over $\mathbb{F}_q$ is defined as follows

$$Z(V/\mathbb{F}_q; T) = exp\left(\sum_1^\infty \#V(\mathbb{F}_{q^n})\frac{T^n}{n}\right)$$

where $\#V(\mathbb{F}_{q^n})$ is the number of $\mathbb{F}_{q^n}$-points of V.

Conjecture 31. *(The Weil Conjectures)*

1. $Z(V/\mathbb{F}_q; T) \in \mathbb{Q}(T)$
2. $Z(V/\mathbb{F}_q; \frac{1}{q^N T}) = \pm q^{N\epsilon/2} T^{\epsilon} \cdot Z(V/\mathbb{F}_q; T)$ for some $\epsilon \in \mathbb{Z}$
3. $Z(V/\mathbb{F}_q; T)$ has a pole at 1 and at $\frac{1}{q^N}$ and all the other poles and zeros have magnitude $q^{1/2}$.

We will prove the Weil conjectures for elliptic curves. The results will follow from direct computation of the Zeta-function.

Lemma 32. *$\#E(\mathbb{F}_{q^n}) = 1 - \alpha^n - \beta^n + q^n$ for complex numbers α, β such that $\alpha\beta = q$*

Proof. Consider the Frobenius map from the curve to itself

$$\phi(x, y) = (x^q, y^q)$$

Since the frobenius fixes only the base field $\mathbb{F}_q$, in counting $\#E(\mathbb{F}_{q^n})$ we seek solutions to $\phi - I = 0$ and

$$\#E(\mathbb{F}_q) = deg(1 - \phi)$$

Recall that $det(\phi_\ell) = deg(\phi) = q$. We also showed that $Tr(\phi_\ell) = 1 + deg(\phi) - deg(1 - \phi) = 1 + q - \#E(\mathbb{F}_q) = a$

Now, consider the characteristic function of ϕ_ℓ,

$$det(T \cdot I - \phi_\ell) = T^2 - Tr(\phi_\ell)T + det(\phi_\ell) = T^2 - aT + q$$

We can factor this polynomial over $\mathbb{C}$:

$$det(T \cdot I - \phi_\ell) = (T - \alpha)(T - \beta)$$

Furthermore, we can show that this polynomial is always positive since for any rational number $\frac{m}{n}$

$$det(\frac{m}{n} - \phi_\ell) = \frac{det(m - n\phi_\ell)}{n^2} = \frac{deg(m - n\phi)}{n^2} \geq 0$$

So the polynomials roots α and β must be complex conjugates and $\alpha\beta = |\alpha|^2 = |\beta|^2 = q$.

Also_note that_α and β are the eigenvalues of the action of ϕ_ℓ. Indeed, we could put ϕ_ℓ in Jordan normal form:

$$\phi_\ell = \begin{pmatrix} \alpha & \\ & \beta \end{pmatrix}$$

We get that $Tr(\phi_\ell) = 1 + q - \#E(\mathbb{F}_q) = \alpha + \beta$. So we get the result for $n = 1$. For higher n we consider $deg(\phi^n - 1) = det(\phi_\ell^n - 1) = (1 - \alpha^n - \beta^n + 1) = 1 - \alpha^n - \beta^n + q^n$ which is obtained by raising the matrix to the nth power. □

Proof. (Weil Conjectures for Elliptic curves)

Taking the logarithm of the zeta-function,

$$\begin{aligned} \log(Z(E,T)) &= \sum \#\mathbb{F}_{q^n} \frac{T^n}{n} \\ &= \sum (1 - \alpha^n - \beta^n + q^n) \frac{T^n}{n} \\ &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT) \end{aligned}$$

yields that

$$Z(E,T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

and $|\alpha| = |\beta| = q^{\frac{1}{2}}$. The functional equation just follows by straightforward calculation.

□

0.2.9 The Weak Mordell-Weil Theorem

We will prove the so called- weak Mordell-Weil Theorem for number fields. Combined with the method of descent this will prove that for a number field K, the group of K-points on an elliptic curve is a finitely generated group.

Theorem 33. *Let K be a number field. Then $E(K)/mE(K)$ is a finite set for each $m \in \mathbb{N}$.*

Proof. We will complete the following steps □

1. Define a perfect pairing

$$G_{L/K} \times E(K)/mE(K) \to E[m]$$

reducing the problem to showing that L/K is finite, L to be defined.

   (a) Show that L is unramified outside a finite set and has exponent m and is abelian

   (b) Show that the maximal abelian extension of exponent m which is unramified outside a finite set is a finite extension.

Proof. Step 1. We need to assume that $E[m] \subset E(K)$. This so that the Kummer pairing (see below) is well defined. We can assume that $E[m] \subset E(K)$ because suppose instead we had to extend the field to some finite L/K so that $E[m] \subset E(L)$. Then the inclusion $E(K) \hookrightarrow E(L)$ induces the exact sequence

$$0 \to \ker(\phi) \longrightarrow E(K)/mE(K) \longrightarrow E(L)/mE(L) \longrightarrow 0$$

Now, $\ker \phi = \frac{E(K) \cap mE(L)}{mE(K)}$, and there is an injective map $\ker \phi \to \mathrm{Hom}(G_{L/K}, E[m])$ given as follows:

$$P \mapsto (\sigma \to Q^\sigma - Q) \text{ where } mQ = P \tag{0.2.2}$$

and $Q \in E(L), P \in E(K)$. Now we will show that $\ker \phi$ is finite.

First note that $Q^\sigma - Q$ is actually in $E[m]$ since $m(Q^\sigma - Q) = P^\sigma - P = P - P = O$.

Second, the map 0.2.2 is not a homomorphism, it is just a map of sets, indeed it's not even well defined since it depends on our choice of Q.

Next, note that the the map 0.2.2 is injective. Indeed, suppose that $P_1 = mQ_1$ and $P_2 = mQ_2$ as above, and $(Q_1^\sigma - Q_1) - (Q_2^\sigma - Q_2) = 0$ then $(Q_1 - Q_2)^\sigma - (Q_1 - Q_2) = 0$ so that $(Q_1 - Q_2) \in K(E)$ (because it is fixed by all Galois automorphisms). But then $P_1 - P_2 \in mK(E)$ which is in the denominator of $\ker \phi$.

Therefore the kernel of ϕ is always finite since it injects into the homomorphism ring $Hom(G_{L/K}, E[m])$, of two finite groups. Now by glancing at the exact sequence, you see that if $E(L)/mE(L) < \infty$, since $E(K)/mE(K)$, being sandwiched between two finite groups will also be finite. So we can always prove the weak Mordell-Weil theorem for finite extensions and it will hold for the ground field. Therefore we henceforth assume that $E[m] \subset E(K)$.

Now we define the Kummer pairing on $\kappa : G_{\bar{K}/K} \times E(K) \to E[m]$ as follows

$$(\sigma, P) \mapsto Q^\sigma - Q$$

where Q is some element such that $mQ = P$.

This pairing is is well defined. Indeed, suppose that $P = mQ = mQ'$. Then $m(Q - Q') = O$ so $Q' = Q + T$ for some $T \in E[m]$. Therefore

$$(Q' - Q)^\sigma - (Q' - Q) = T^\sigma - T = 0$$

since we assumed that $E[m] \subset E(K)$.

Now we mod out by the kernel of each side of the pairing. From the above discussion, it's clear that the kernel on the right is just $mE(K)$. On the left, the kernel is obviously $G_{\bar{K}/L}$ where L is some field such that $E(L)$ contains all of the elements Q such that $mQ = P$ for some point $P \in E(K)$. More formally,

$$L = \bigcup_{P \in E(K)} K([m]^{-1}P)$$

So after we mod out by the kernels on both sides we get a "perfect pairing"

$$\kappa : G_{L/K} \times E(K)/mE(K) \to E[m]$$

that is, there's no element σ such that $\kappa(\sigma, X) = 0 \,\forall\, X$ and also no element Y such that $\kappa(\tau, Y) = 0 \,\forall\, \tau$. Since $E[m]$ is finite, we have that

$$|G_{L/K}| < \infty \iff |E(K)/mE(K)| < \infty$$

This brings us to step 2 of the proof of the weak-Mordell Weil Theorem.

Step 2. We show that L is unramified outside of a finite set.

We now introduce the concept of reduction of an elliptic curve. Suppose one had a Weierstrass equation for a curve over K. Now over K_v we can look at various isomorphisms of the curve that give rise to different Weierstrass equations. We can choose one that minimizes (the absolute value of) Δ. We call this a "minimal Weierstrass equation". Now that we have it in this form we can reduce mod a prime to get a curve $\tilde{E}(k)$ where k is the residue field.. We say that there's bad reduction if this curve is singular (i.e. $\bar{\Delta} = 0$ or any geometric thing).

The places where this is singular are just the places where $p \big| \Delta_{min}$. Therefore there are only finitely many places where there is bad reduction.

There's one more fact which will be useful in this discussion: □

Fact 34. *If* $\tilde{E}(k)$ is non-singular, and $v(m) \neq 0$, then $E(K)[m] \to \tilde{E}(k)$ is injective. To justify this a little bit, notice that in a formal group over a complete local ring, an element of finite order has order that is a power of p where $p =$the characteristic of the residue field.

Proof. The fact that L is an abelian extension follows from the existance of the perfect pairing which gives us

$$G_{K/L} \hookrightarrow Hom(E(K)/mE(K), E[m])$$

Let

$$S = \{\text{places } v \text{ with bad reduction}\} \cup \left\{v \middle| v(m) \neq 0\right\} \cup \{\infty\text{'s}\}$$

We'll show that L is unramified outside of such places.

Since L is a compositum of $K^{'} = K(Q)$ where $[m]Q \in E(K)$, we consider these one at a time. We'll show that all of these are unramified outside of S. Since we're outside of S we know that there's a reduction

$$E(K^{'}) \to E(k_v^{'})$$

Let $\sigma \in I_{v'/v} \subset G_{K'/K}$. Recall that we have the exact sequence

$$0 \to I_{v'/v} \to D_{v'/v} \to G_{k_{v'}/k_v} \to 0$$

and that being unramified means that $I_{v'/v} = 0$. Then we have that $\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = O$ since by definition $I_{v'/v}$ are the elements which act trivially on the residue field. On the other hand,

$$[m](Q^\sigma - Q) = ([m]Q)^{\,\sigma} - [m]Q = P^\sigma - P = 0$$

so $Q^\sigma - Q$ is an element of $E[m] \subset E(K)$, which, under these conditions, injects into $E(k_v^{'})$. So σ must have been trivial, and since σ was arbitrary, $I_{v'/v}$ is trivial.

Finally, each element in the compositum $K([m^{-1}]P)$ can have degree at most $m^2!$ since there are at most m^2 elements being adjoined and we can have no larger a Galois group than the Galois group act on them by the symmetric group.

If we consider all field extensions of a number field of degree less than or equal to $m^2!$ and unramified outside of a certain set then by Minkowski's theorem there are only finitely many such fields. Therefore L is a finite extension of K and we have complete the proof that $E(K)/mE(K)$ is finite. $\square$

0.2.10 The Method of Descent

The method descent is a broad technique which is used in many settings. In its most basic incarnation, it seeks to establish a contradiction by constructing a seemingly infinite sequence of decreasing natural numbers.

Theorem 35. *Let A be an abelian group with a height function $h : A \to \mathbb{R}$ satisfying*

1. $\forall Q \in A$ there exists C_1such that $h(P+Q) \leq 2h(P) + C_1$

   (a) $\exists m \in \mathbb{Z}$ such that $h(mP) \geq m^2 h(P) - C_2$

   (b) $\forall C_3 \in \mathbb{R}$, $\#\left\{P \in A \middle| h(P) \leq C_3\right\} < \infty$

   (c) for the m above, A/mA is a finite group.

Theorem 36. *Then A is finitely generated.*

Proof. Let $Q_1, ...Q_r$ be coset representatives for A/mA. Let $P \in A$. Then write

$$\begin{array}{ccc} P & = & P_1 m + Q_{i,1} \\ P_1 & = & P_2 m + Q_{i,2} \\ \vdots & \vdots & \vdots \\ P_{n-1} & = & P_n m + Q_{i,n} \end{array}$$

Working upward, we have the expansion $P = m^n P_n + \sum_{j=1}^{n} m Q_{i,j}$.

Let C_k be the constant of property (1) for $-Q_k$ and let $C = \max_k C_k$. Now we compute:

$$
\begin{aligned}
h(P_n) &= h(P_{n-1}m - Q_{i,n}) \\
&\leq 2h(mP_{n-1}) + C \\
&\leq 2(\frac{1}{m^2}h(P_{n-1}) - C_2) + C \\
&\leq 2(\frac{1}{m^2}\left(2(\frac{1}{m^2}h(P_{n-2}) - C_2) + C\right) - C_2) + C \\
&\cdots \\
&\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{2}{m^2} + \frac{2^2}{(m^2)^2} + \cdots \frac{2^{n-1}}{(m^2)^n}\right) C \\
&\leq 1 + C_3 \text{ for a high enough } n
\end{aligned}
$$

Now there are only finitely many such elements with $h(P_n) \leq 1 + C_3$. Let's call them $R_1, ..., R_m$. Now $\{Q_1, ..., Q_r, R_1, ..., R_m\}$ generate A because of the following argument: Let P be any point on the curve. Using the above process we may write it in the form

$$P = m^n P_n + \sum_{j=1}^{n} mQ_{i,j}$$

We take n large enough so that $h(P_n) = R_i$ which as we showed above, it must. Then P is in the ($\mathbb{Z}$) span of $\{Q_1, ..., Q_r, R_1, ..., R_m\}$. □

0.2.11 Modular forms

This section is a sparse overview of modular forms with the sole interest of defining the L-function of a modular form. It is not necessary to build up too much of this theory in order to reach the main points of this thesis, but since this is a work about automorphic representations which have grown out of the theory of modular forms, we feel we would be remiss in not devoting a little bit of discussion to them. In addition, this discussion lends a slightly more concrete meaning to the word *modularity* which will be used throughout.

Modular forms have played a central role in classical analytic number theory because the generating function for many interesting sequences turn out to be modular forms. For instance, the sequence

$$\{a_n\}_{n\in\mathbb{N}} = \{\text{number of quadruples of integers solutions to } x_1^2 + x_2^2 + x_3^2 + x_4^2 = n\}$$

describes a modular form as well as the sequence

$$\{p_n\}_{n\in\mathbb{N}} = \{\text{ the number of ways to write n as a sum of positive integers}\}$$

Thus, some basic motivation being established, we will build up some of the definitions and known facts about modular forms. Beginning with the classical work on modular forms, that is, modular forms for the classical upper half plane, we then use the remainder of this section to briefly mention the generalization to so-called "Hilbert Modular Forms" but not dwell too deeply on their properties since these modular forms are best understood as automorphic representations, which will come up in section 0.3.

Let $\mathcal{H}$ be the Poincaré upper half-plane consisting of elements of the form $x+iy$, where $x, y \in \mathbb{R}$ and $y > 0$. Then the group $G = SL(2,\mathbb{R})$ acts on $\mathcal{H}$ via

$$g(z) = \frac{az+b}{cz+d}, \quad g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$$

The subgroup $SL(2,\mathbb{Z})$ inherits this action and is called the **modular group.** The modular group itself has many interesting subgroups:

Definition 37. Let N be a positive integer. The subgroup

$$\Gamma(N) = \{\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL(2,\mathbb{Z}) : \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \equiv \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \pmod{N}\}$$

is called the **principal congruence subgroup of level** N**.** Any subgroup of $SL(2,\mathbb{Z})$ containing a principal congruence subgroup of some level is called a **congruence subgroup.**

Example 38. Let N be a positive integer. The subgroup

$$\Gamma_0(N) = \{\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL(2,\mathbb{Z}) : \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \equiv \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \pmod{N}\}$$

is a congruence subgroup.

Definition 39. Let Γ be a congruence subgroup and let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a **modular form of weight k with respect to** Γ if

1. f is holomorphic
2. $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ for all $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma$ and τ in $\mathcal{H}$.
3. f is holomorphic at all points that can be mapped, under Γ, to ∞. (Holomorphic at the cusps)

if, in addition, $f = 0$ at all the cusps, then f is also said to be a **cusp form. [4]**

Now, let h be the smallest h for which $\left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$. Such a matrix is called a translation matrix because it executes the action $z \mapsto z + h$. Every congruence subgroup contains one of these translations because the element $\left[\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right]$ is in the principal congruence subgroup $\Gamma(N)$. Now, condition (2.) above, implies that f has a Fourier expansion of the form:

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n, \quad q_h = e^{2\pi i \tau / h}$$

Definition 40. (The L-function of a modular form) Let f be a modular form of weight k. The the L-function of f is the Mellin-transform of f given by

$$L(f, s) = \sum_{n=0}^{\infty} a_n(f) n^{-s}$$

where $a_n(f)$ are the Fourier coefficients of f.

We conclude with similar definition of a Hilbert modular form and it's L-function. We will treat the case of a totally real field, for simplicity.

Let K be a totally real field of degree n with ring of integers $\mathfrak{o}$. We can regard K as a subring of $\mathbb{R}^n$ by use of its n embeddings into $\mathbb{R}$:

$$\alpha \mapsto (a^{(1)}, ..., a^{(n)}). \tag{0.2.3}$$

We define the analog of the upper half plane and the modular group. Let $\mathcal{H}^n = (z_1, z_2, z_3...)$, $z_i \in \mathcal{H}$; this will be the geometric space we are interested in. Upon this space there is the action of $SL(2, \mathbb{R}^n)$ which is component-wise.

Definition 41. If we regard $SL(2, K)$ as a subgroup of $SL(2, \mathbb{R})^n$ via the embedding 0.2.3 then the image of the group $SL(2, \mathfrak{o})$ is called the **Hilbert modular group.**

We now expand the notion of a principal congruence subgroup and level.

Definition 42. Let $\mathfrak{n}$ be a non-zero ideal of $\mathfrak{o}$. Define the **principal congruence subgroup** of level $\mathfrak{n}$ as

$$\Gamma(\mathfrak{n}) = \left\{\gamma \in GL^+(2, \mathfrak{o}) : \gamma \equiv I \mod \mathfrak{n}\right\}.$$

A subgroup Γ of $GL(2, F)$ is called a **congruence subgroup** if $Z(GL^+(2, \mathfrak{o}))\Gamma$ contains some $\Gamma(\mathfrak{n})$ with finite index.

Definition 43. Let k be a vector of positive integers $k = (k_1, ..., k_n)$. A **Hilbert modular form** of weight k is a holomorphic function on $\mathcal{H}^n$ such that

$$f(\gamma(z)) = N(cz + d)^k f(z)$$

where

$$N(cz + d)^k = \prod_{i=1}^{n} (c^{(i)} z_i + d^{(i)})^{k_i}.$$

Note: for $n > 1$, the condition of holomorphicity at the cusps is automatically satisfied.

Proposition 44. *(Fourier expansion) Let Γ be a congruence subgroup and let $\Lambda = \{u \in F : \left[\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma\}$. Then any Hilbert modular form f has a Fourier expansion:*

$$f(z) = \sum_{\xi \in \Lambda^*} c_\xi exp(2\pi i Tr(\xi z))$$

where Tr is the linear extension of the Galois trace $F \to \mathbb{Q}$ and $\Lambda^\star$ is the dual $\mathbb{Z}$ module to Λ.

0.2.11.1 The functional equation for L-functions of modular forms

The main result of this section is the discussion of the L-function attached to a modular form. The definitions are essentially the same as for modular forms for $\mathbb{Q}$.

Definition 45. Let f be a Hilbert modular form with the Fourier expansion:

$$f(z) = \sum_{\xi} c_\xi exp(2\pi i \mathrm{Tr}(\xi z)),$$

and let

$$U = \left\{ a \in (\mathbb{R}^+)^m : a \in \mathfrak{o}^\times, a \equiv 1 \pmod{\mathfrak{n}} \right\}.$$

Then the $L - function$ attached to f is given by

$$L(s, f) = \sum_{\xi \in U} c_\xi \xi^{-(s+k/2-1/2)}$$

where we use a multi-index notation.

As in the classical case, the L-function shows up in an integral involving f , which is then manipulated to obtain the functional equation. Namely let

$$\tilde{L}(s, f) = \int_{(\mathbb{R}^+)^m/U} y^{s+k/2-1/2} f(iy) d^\times y$$

then for $Re(s) > 3/2$,

$$\tilde{L}(s, f) = \left\{ \prod_j (2\pi)^{-(s+1/2k_j-1/2+\pi i\alpha_j)} \Gamma(s + \frac{1}{2}k_j - \frac{1}{2} + \pi i\alpha_j) \right\} L(s, f)$$

by essentially the same manipulations as when $n = 1$. Finally, we record the theorem governing the functional equation of this L-series.

Theorem 46. *The function $\tilde{L}(s, f)$ has analytic continuation to the entire complex plane. Furthermore,*

$$\tilde{L}(s, f) = \lambda \tilde{L}(1 - s, f)$$

$\lambda \in \{\pm 1\}$.

We have recorded the basic definitions and results of Hilbert modular forms and their L-functions. These concern one side of the modularity theorem which is required for our results. On the other side are elliptic curves which are geometric objects and whose L-functions are defined by counting points on curves. The marvel of the modularity theorem is that these two L-functions, defined by such disparate methods, should be connected.

0.2.12 L-function of an elliptic curve and the Modularity Theorem

A fundamental object in analytic number theory, the L-function is a complex function that can be constructed from various algebraic and geometric objects. Notationally, the L-function attached to an object X is written $L(s, X)$ or $L(X, s)$ depending on whether the object, or the complex function is emphasized.

The first L-function to be studied was Riemann's Zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

which converges absolutely in the half plane $Re(s) > 1$ and was discovered to have a so-called Euler product:

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1}$$

over the rational primes. It was also known that the zeta function satisfied a functional equation of the form

$$\Gamma(s/2)\pi^{-s/2}\zeta(s) = \Gamma(1 - s/2)\pi^{(s-1)/2}\zeta(1 - s)$$

which also provides a meromorphic continuation to the entire complex plane. These properties have been found to hold for a wide variety of functions of the form

$$L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

which are called the Dirichlet series attached to the sequence $\{a_1, a_2...\}$. We can attach such a sequence to many different sorts of objects including characters, geometrical objects and

representations. For an object f we create the function $L(s,f) = \sum_{n=1}^{\infty} a_{f,n} n^{-s}$ and call it the "L-function attached to f" and it has been speculated that this L-function encodes a tremendous amount of the arithmetic data of the object f. Indeed much of analytic number theory is concerned with the study of these $L-$functions.

By far the hardest property of an L-function to prove is the functional equation and for some objects this property is shown by highly indirect methods. For others, the functional equation comes from basic (but very clever) algebraic manipulation of the function and have been known for over 100 years.

We move on to the definition of the L-function attached to an elliptic curve.

Definition 47. Let E/K be an elliptic curve over a number field. Then the L-function attached to E is defined as

$$L(E/K,s) = \prod_{p \in S} (1 - a_p Np^{-s})^{-1} \prod_{p \notin S} (1 - a_p Np^{-s} - Np^{1-2s})^{-1}$$

where S is a set of primes where E has bad reduction, Np is the ideal norm of the prime p. The numbers a_p are either -1,0,1 when E has bad reduction at p and $a_p = Np + 1 - \#(E \text{ reduced at } p)$. Alternatively, we can define the a_p using the action of the Tate-module, see section (0.2.5) . [14]

Now, the above L-function converges in the half-plane $Re(s) > 3/2$ because of Hasse's bound: $|a_v| \leq 2Np^{\frac{1}{2}}$ and the function is already given as an Euler product. The only thing remaining is to show that $L(E/K,s)$ satisfies a functional equation. This fact was first proved for Elliptic curves with complex multiplication because it was shown that the L-functions attached to these elliptic curves were Hecke L-functions whose functional equations were known. The concept of relating the L-functions of one object to another has become an object of intense study and has led to the functional equations of the L-functions in special cases but remains as a conjecture of the following form:

Conjecture 48. *(Taniyama, Shimura, Weil) Let E/K be an elliptic curve over a number field K. Then E is modular.*

where, modular is defined as:

Definition 49. Let E/K be an elliptic curve over a number field with L-function $L(E, s)$. Then E is said to be modular if $L(E, s) = L(f, s)$ for some weight-2 Hilbert modular form.

Note: the property of modularity is more naturally defined in the context of the representation theory which will be introduced in the next section. We will redefine and make use of this more natural definition in section 0.4.

Thus, the only known way of proving the functional equation for elliptic curves is by showing that their L-functions are that of modular forms, for which the functional equation has already been established. Thus recent work surround elliptic curves have focused on the modularity of elliptic curves and thus far has produced the following results: First, as the last step in the program that solved Fermat's Last Theorem:

Theorem 50. *All elliptic curves defined over $\mathbb{Q}$ are modular. [1]*

And more recently, expanded to include many more fields:

Theorem 51. *Let K be a totally real field or a real quadratic extension of a totally real field. Let E be an elliptic curve over K, then E is modular.[12; 6; 7]*

0.3 Automorphic Representation Theory

0.3.1 Introduction

The doctoral thesis of John Tate and the work of Jacquet & Langlands in their book [10] lay the foundations for understanding the functional equations attached to so-called automorphic representations. In it, they rely heavily on the factorization of the L-function and show how the epsilon factors are in fact a product of local factors arising at places of "bad reduction." We begin with the theory of automorphic forms for $\mathbb{A}^\times$ which is often called "Tate's Thesis" after the occasion of its first appearance. In it, Tate developed a framework for proving

the functional equations of Hecke L-functions by treating Hecke characters as automorphic representations of $GL(1, \mathbb{A})$. In a similar fashion, the work of Jacquet and Langlands proves the functional equation of a modular form by treating them as automorphic representations on $GL(2, \mathbb{A})$.

0.3.2 Adeles and Automorphic Forms for GL(1)

The first step in understanding automorphic forms is the construction of the so-called Adele group associated to a global field. Let K be a global field (that is, a finite extension of $\mathbb{Q}$, or the function field of an algebraic curve over a finite field, for example $\mathbb{F}_q(T)$).

Definition 52. Let $|\cdot|_v : K \to \mathbb{R}$ be a function such that

1. $|ab|_v = |a|_v |b|_v$
2. $|a + b|_v \leq |a|_v + |b|_v$
3. $|x|_v = 0$ if and only if $x = 0$

then $|\cdot|_v$ is called an **absolute value** on K.

Two absolute values, $|\cdot|_{v_1}, |\cdot|_{v_2}$are said to be equivalent if $|\cdot|_{v_1} = |\cdot|_{v_2}^{\alpha}$ for some $\alpha \in \mathbb{R}_{>0}$. Furthermore, if an absolute value has the property that

$$|a_v + b_v| \leq max\{|a|_v, |b_v|\}$$

then it is called **non-archimedian**. Otherwise, the absolute value is called **archimedian.**

Let $|\cdot|_v$ be an absolute value on K. Then we construct the **completion of** K **by** v denoted K_v as follows. Recall that given an absolute value $|\cdot|_v$, a Cauchy-sequence in K with respect to $|\cdot|_v$ is a sequence $A = \{a_1, a_2, ...\}$ of elements of K such that for any $\epsilon > 0$, there exists an $N \in \mathbb{N}$ whereby $|a_n - a_m|_v < \epsilon$ whenever n and m are greater than N.

Note: When $|\cdot|_v$ is non-archimedian, a Cauchy sequence has the peculiar property that $\{a_1, a_2...\}$ converges *if and only if* the terms $a_n \to 0$.

Now we define K_v as:

$$K_v = \frac{\{ \text{ cauchy-sequences with respect to } |\cdot|_v\}}{\{\text{cauchy sequences with respect to } |\cdot|_v \text{ that converge to } 0\}}$$

The equivalence classes are closed under addition, multiplication, contain inverses with respect to these operations (except the equivalence class of $\{0, 0, ...\}$ with respect to multiplication) and thus, K_v is a field. If $|\cdot|_v$ is archimedian we say that the field K_v is archimedian and if $|\cdot|_v$ is non-archimedian then we say K_v is non-archimedian.

It shall be convenient to deal with a slightly different, but equivalent form of K_v when $|\cdot|_v$ is non-archimedian.

Proposition 53. *If K_v is non-archimedian, $\mathfrak{o} = \{a \in K_v \mid |a|_v \leq 1\}$ is a local ring.*

Definition 54. Let π be an element of a non-archimedian field K_v such that $|\pi| < 1$ and π is maximal with respect to this property. Then π is called a **uniformizer** for K_v. The uniformizer is not unique. Indeed, for any unit $u \in \mathfrak{o}^\times = \{a \in K_v \mid |a|_v \leq 1\}$, $u\pi$ is also a uniformizer. The ideal generated by π is the maximal ideal of $\mathfrak{o}$.

Example 55. Let $K = \mathbb{Q}$ and $|\cdot|_v = |\cdot|$ be the ordinary absolute value on $|\mathbb{Q}|$. Then $K_v \simeq \mathbb{R}$.

Example 56. Let $K = \mathbb{Q}$ and let $|\cdot|_v = |\cdot|_p$ for a rational prime p be defined as follows: for any element $r \in \mathbb{Q}$, write $r = p^n \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and p divides neither a nor b. Then $|r|_p := p^{-n}$. Then the completion of $\mathbb{Q}$ by $|\cdot|_p$ is denoted $\mathbb{Q}_p$ and has a uniformizer p.

We will now concern ourselves by considering all the completions of a given field as a set.

Proposition 57. *Suppose $|\cdot|_{v_1}$ and $|\cdot|_{v_2}$ are two absolute values on K. Then $|\cdot|_{v_1} \sim |\cdot|_{v_2}$ if and only if $K_{v_1} \simeq K_{v_2}$ as fields and as topological spaces.*

Thus we are justified in considering just a single absolute value in each equivalence class of absolute values of K. In each equivalence class we choose a particular element v and call the absolute value given by v, a **place** of K. Sometimes v itself is called a place, the meaning is usually clear: we use v to enumerate the absolute values of K, up to equivalence.

Theorem 58. *(Ostrowski) Up to equivalence, the absolute values on $\mathbb{Q}$ are the standard one $|\cdot| = |\cdot|_\infty$ and the ones given by the primes $|\cdot|_p$.*

Thus for the field $\mathbb{Q}$, its completions are enumerated by the primes and $\mathbb{R}$. For a more general number field we have a similar theorem in which the completions are given by several copies of $\mathbb{C}$, $\mathbb{R}$ and K_v attached to a prime ideal of K. Note that the topology of two different completions may have the same underlying sets but we consider them different completions if the metric is different.

Proposition 59. *Let K_v be a non-archimedian field and ω a uniformizer for K_v. Any element of K_v can be written uniquely in the form*

$$\sum_{n=-N}^{\infty} a_n \pi^n$$

where a_n are chosen from a set of coset representatives of $K_v^\times/\mathfrak{o}^\times$.

Definition 60. (Adele, Ideles) Let K be a global field. The set

$$\mathbb{A}_K = \prod_v{}' K_v$$

of elements $\alpha = (\alpha_v)$ where v runs through the places of K, such that $\alpha_v \in \mathfrak{o}_\mathfrak{v}$ for all but finitely many v is called the **adele ring** of K. Addition and multiplication are defined component-wise and the topology is given by the product topology. That is, the open sets are generated by the sets $\prod U_v$ where U_v is an open set in K_v and $U_v = K_v$ for all but finitely many v.

The **Idele group of K** is the multiplicative group of the adele ring

$$\mathbb{I}_K = \mathbb{A}_K^\times$$

or, more precisely, it is the family of elements $\beta = (\beta_v)$, such that $\beta_v \in K_v^\times$ and $\alpha_v \in \mathfrak{o}_\mathfrak{v}^\times$ for all but finitely many places v.

The inclusion $K \subset K_v$ allows us to define the diagonal embeddings:

$$K \hookrightarrow \mathbb{A}_K$$

and

$$K^\times \hookrightarrow \mathbb{I}_K$$

given by $\alpha \mapsto (\alpha,\alpha,...)$ in each case.

There is an absolute value on $\mathbb{A}_K$:

$$|(a_{v_1}, a_{v_2}, ...)| := \prod_v |a_v|_v$$

which is well defined since all but finitely many of the coordinates have $|a_v|_v \leq 1$. It is also true that if $a \in K$, $|a| = 1$, by standard arguments.

0.3.3 Tate's Thesis

In this setting, we are in a position to classify automorphic forms for $GL(1) = \mathbb{I}_K$. In fact they are in bijection with a set of familiar algebraic objects!

Of much interest in this section will be the study of additive characters on $\mathbb{A}_K$ which take trivial values on K and multiplicative characters on $\mathbb{A}_K^\times$ which are trivial on $K^\times$. It is required that these characters be continuous but because of the topology on these groups it is only necessary to check continuity at the identity element: $(0, 0, 0, ...)$ and $(1, 1, 1, ...)$ respectively. If a character $\chi : G \to \mathbb{C}^\times$ has image in the complex numbers $\{z \in \mathbb{C}^\times : |z| = 1\}$ then the character is labeled **unitary**. If there exists a positive integer m such that $\chi(g)^m = 1$ for all $g \in G$ then χ is said to be of **finite order**.

Proposition 61. *Suppose χ is a character of $\mathbb{A}_K^\times/K^\times$. Then $\chi = \chi_1|\cdot|^\lambda$ for some unique character χ_1 of finite order and $\lambda \in \mathbb{C}$, λ purely imaginary. There is a bijection between characters of finite order on $\mathbb{A}_K^\times/K^\times$ and classical primitive Hecke characters of $K^\times$.*

We now define the Fourier transform of functions in the Schwartz space $S(\mathbb{A}_K)$:

Definition 62. Let $\psi = \prod_v \psi_v$ be a fixed additive character on $\mathbb{A}_K/K$. And let Φ be an element of $S(\mathbb{A}_K)$. The the Fourier transform is defined as

$$\hat{\Phi}(x) = \int_{\mathbb{A}_K} \Phi(y)\psi(xy)dy$$

where the measure $\int_{\mathbb{A}_K} dy$ is chose to be the Haar measure such that $\hat{\hat{\Psi}}(x) = \Psi(-x)$ (self-dual).

Definition 63. An automorphic form for $GL(1, \mathbb{A}_K)$ is a homomorphism $\phi : \mathbb{A}_K^\times \to \mathbb{C}^\times$ such that

1. $\phi(k\alpha) = \phi(\alpha)$ for all $k \in K^\times, \alpha \in \mathbb{A}_K^\times$
2. ϕ is continuous at $(1, 1, 1, ...)$
3. ϕ has moderate growth

From the discussion above and from Proposition 61 it is clear that automorphic forms for $GL(1)$ are no more than the classical Hecke characters which we have now "adelicized." This allows us to study them in their natural factorization as characters over each place, as we shall see. This last condition is a technical one that will allow us to integrate automorphic forms. To that end, we introduce a measure $d^\times x$ on $\mathbb{A}_K^\times$ multiplicatively as follows:

$$d^\times x_v = \begin{cases} \frac{dx_v}{|x_v|_v} & \text{if } v\text{is archimedian} \\ \frac{1}{\left(1-\frac{1}{q_v}\right)} \frac{dx_v}{|x_v|_v} & \text{if } v\text{is non-archimedian} \end{cases}$$

where dx_v is the standard, self-dual haar measure on K_v and q_v is the cardinality of $\mathfrak{o}_\mathfrak{v}/\pi_\mathfrak{v}$.

We now introduce an integral, the **zeta integral**, which will be the basis for much of the rest of this exposition in this section:

$$\zeta(s, \chi, \Phi) = \int_{\mathbb{A}^\times} \Phi(x)\chi(x)|x|^s d^\times x$$

where χ is a character of $\mathbb{A}_K^\times/K^\times$ and we shall be concerned with functions of the form $\Phi(x) = \prod_v \Phi_v(x_v)$. Because $\Phi \in S(\mathbb{A}_K)$ it follows that $\Phi_v(x)$ is the characteristic function of $\mathfrak{o}_v$ for all but finitely many v. In that case we have that (formally at least):

$$\zeta(s,\chi,\Phi) = \prod_v \zeta_v(s,\chi_v,\Phi_v) = \prod_v \int_{K^\times} \Phi_v(x_v)\chi_v(x_v)|x_v|_v^s d^\times x_v \tag{0.3.1}$$

Proposition 64. *The local integrals in (0.3.1) are absolutely convergent for $Re(s) > 0$.*

0.3.3.1 The functional equation for automorphic functions on $GL(1)$

Definition 65. (Local L-factors). We define local L factors associated to an automorphic form as follows:

$$L_v(s,\chi_v) = (1 - \chi(\pi_v)q_v^{-s})^{-1}$$

for non-ramified, non-archimedian places v. For ramified non-archimedian places, $L_v = 1$. If K_v is real then χ_v has form form $\chi_v(x) = \left(\frac{x}{|x|_v}\right)^\epsilon$ and we define

$$L_v(s,\chi_v) = \pi^{-(s+\epsilon)/2}\Gamma(\frac{s+\epsilon}{2}) \text{ (real places)}$$

On the other hand, if v is a complex place then $\chi_v(x) = |x|_v^\nu \left(\frac{x}{\sqrt{|x|_v}}\right)^k$ and we define

$$L_v(s,\chi_v) = 2(2\pi)^{-s+\nu+|k|/2}\Gamma\left(s+\nu+\frac{|k|}{2}\right) \text{ (complex places)}$$

Theorem 66. *(Tate) The local integrals in 0.3.1 satisfy*

$$\zeta_v(s,\chi_v,\Phi_v) = \gamma(s,\chi_v)\zeta_v(1-s,\chi_v^{-1},\hat{\Phi}_v)$$

where γ is a meromorphic function independent of Φ (but it <u>is</u> dependent on the additive character ψ_v used to define the Fourier transform)

Next we define

$$\epsilon(s, \chi_v) = \frac{\gamma_v(s, \chi_v) L_v(s, \chi_v)}{L_v(1-s, \chi_v^{-1})}$$

Since the functions $\epsilon(s, \chi_v)$ are independent of the 'test function', Φ, for a suitable choice of Φ which was worked out by Tate and are tabulated in section 0.3.5.1.

Theorem 67. *(Tate) The function* $\zeta(s, \chi, \Phi)$ has meromorphic continuation to all of $\mathbb{C}$. We have the functional equation:

$$\zeta(s, \chi, \Phi) = \zeta(1-s, \chi^{-1}, \hat{\Phi})$$

We omit the proof of this theorem but note that the main tools in the proof are the Poisson summation theorem and the splitting of the integral into two pieces where $|x| < 1$ and $|x| > 1$.

The two theorems 66 and 67 now give us the functional equation for the Hecke L-functions as follows. Define

$$L(s, \chi) = \prod_v L_v(s, \chi_v)$$

by their definitions given in 65. Then, the local and global functional equations give us that

$$L(s, \chi) = \prod_v \epsilon(s, \chi_v) L(1-s, \chi^{-1})$$

and the function $\prod_v \epsilon(s, \chi_v)$ is well-defined since all but finitely many of the multiplicands are 1. The product $\prod_v \epsilon(s, \chi_v)$ is the classical epsilon factor in the functional equation of the $L-$function which is quite mystifying without the modern adelic approach of Tate and the theory of automorphic forms.

0.3.4 The work of Jacquet-Langlands on $GL(2)$.

In their book "Automorphic Forms on GL(2)", Herve Jacquet and Robert Langlands showed how to extend the concepts of Tate's thesis to automorphic representations of $GL(2, \mathbb{A}_K)$. Let F be a number field and let $\mathbb{A}$ be its adele ring. Let $\mathbb{A}_f$ be the ring of finite adeles.

We shall be interested in the vector space of automorphic forms defined as follows: Let K be a maximal compact subgroup of $GL(2, \mathbb{A}_F)$ and for an archimedian place v, let $Z_v(U(\mathfrak{g}))$ denote the center of the universal enveloping algebra of $\mathfrak{gl}(2, F_v)$. Let $\mathfrak{g}_\infty = \prod \mathfrak{gl}(2, F_v)$ and let $K_\infty = \prod K_v$ where the product is taken over the archimedian places and K_v is taken to be $O(2)$ at the real places and $U(2)$ at the complex places and $GL(2, \mathfrak{o}_\mathfrak{v})$ at the archimedian places.

Definition 68. Let ω be a unitary character on $F^\times \backslash \mathbb{A}_F^\times$. An automorphic form for $GL(2, \mathbb{A}_F)$ is a smooth function $\phi : GL(2, F) \backslash GL(2, \mathbb{A}_F) \to \mathbb{C}$ such that

1. $\phi(zg) = \omega(z)\phi(g)$ for all $g \in GL(2, \mathbb{A}_F)$, and scalar matrices $z = \left[\begin{smallmatrix} a & \\ & a \end{smallmatrix}\right]$ $a \in \mathbb{A}_F^\times$
2. The set $\{\phi(gk) | k \in K\}$ is a finite dimensional vector space (Right K-finite)
3. The set $\{D\phi(g) | D \in Z_v(U(\mathfrak{g}))\}$ is a finite dimensional vector space for all archimedian places v. ($Z_v(U(\mathfrak{g}))$-finite)
4. ϕ is of moderate growth

I won't define moderate growth here but the meaning can be found in [9] and [2] where the above definition is taken from.

Definition 69. (Automorphic representation) Let $\mathcal{A}(GL(2, F) \backslash GL(2, \mathbb{A}_F), \omega)$ be the set of automorphic forms with central quasicharacter ω. An automorphic "representation" π of $GL(2, \mathbb{A}_F)$ is a representation of $GL(2, \mathbb{A}_f)$ and a commuting action of $(\mathfrak{g}_\infty, K_\infty)$ at the infinite places, that can be realized as a subquotient of $\mathcal{A}(GL(2, F) \backslash GL(2, \mathbb{A}_F), \omega)$. The character ω is called the central character of π.[2]

The study of automorphic representations only involves representations with certain convenient properties, which, possessing of these, the representation is called **admissible**. They are, that if (π, V) is an automorphic representation, then for any irreducible finite dimension representation ρ of K, the ρ-isotypic parts $V(\rho)$ is a finite dimensional vector space. If (π, V)

satisfies this requirement it is deemed **admissible**. There is a exactly analogous meaning for a local representation (π_v, V_v) of $GL(2, F_v)$ to be admissible.

The approach to classifying and understanding automorphic representations is at the local level. For this we need the tensor product theorem which says that:

Theorem 70. *(Tensor Product theorem). Let (V, π) be an irreducible admissible representation of $GL(2, \mathbb{A})$. Then for each archimedian place v of F there exists an irreducible $(\mathfrak{g}_\infty, K_\infty)$ module and for each non-archimedian place, a representation (π_v, V_v) of $GL(2, F_v)$ such that these "local representations" are all admissible and for almost all v,V_v contains a non-zero K_v fixed vector w_v such that π is the restricted tensor product of the representations π_v.*

Recall that the restricted direct product has the following definition

Definition 71. (Restricted Tensor Product) Let $\{V_v\}_{v \leq \infty}$be a family of representations and let $\xi_v^\circ \in V_v$ be a vector specified for all v except for possibly some finite set S. We define the restricted tensor product of the representations V_v with respect to ξ_v° to be the set of vectors

$$\xi = \bigotimes_{v \leq \infty} \xi_v \text{ such that } \xi_v = \xi_v^\circ \text{ at all but finitely many places}$$

The tensor product theorem leads us to the the study of local representations. Let π_v be a local representation of $GL(2, F_v)$. We shall first deal with the non-archimedian fields K_v.

Definition 72. Let χ_1 and χ_2 be characters of $F^\times$. Let

$$\mathcal{B}(\chi_1, \chi_2) = \left\{ f : G \to \mathbb{C} | f\left(\left(\begin{smallmatrix} a & b \\ & c \end{smallmatrix}\right) g\right) = \chi_1(a)\chi_2(c) \left|\frac{a}{c}\right|^{\frac{1}{2}} f(g) \text{ and } f \text{is locally constant} \right\}$$

and let the action of G on this vector space be given by $g.f(x) = f(xg)$, also called a **right action**. If $\pi(\left(\begin{smallmatrix} a & b \\ & c \end{smallmatrix}\right)) = \chi_1(a)\chi_2(b) \left|\frac{a}{c}\right|^{\frac{1}{2}}$ is a representation of P then $\mathcal{B}(\chi_1, \chi_2)$ is the (compactly) induced representation.. This action is denoted the **principal series representation**. Suppose that χ_1 and χ_2 are unramified and $\mathcal{B}(\chi_1, \chi_2)$ is irreducible. Then $\chi_1(\varpi_v)$ and $\chi_2(\varpi_v)$, where ϖ_v is a uniformizer at v, are called the **Satake parameters** of $\mathcal{B}(\chi_1, \chi_2)$ and they will come up again when we introduce local $L-$factors.

Proposition 73. *$\mathcal{B}(\chi_1, \chi_2)$ is a smooth and admissible representation.*

Proof. Let $f(g) \in \mathcal{B}(\chi_1, \chi_2)$. From the definition and the decomposition $G = PK$, where P is the subgroup of upper-triangular matrices and K is a maximal compact subgroup, $f(g)$ is determined by what it does on K and also f is locally constant. For every $k \in K$ let U_k be a compact neighborhood of 1 such that $f(k \cdot U_k) = f(k)$. Then by compactness, finitely many $U_1, U_2, ..., U_N$ suffice to cover K. So if we let $U = \bigcap_N U_i$ then $f(k \cdot U) = f(k)$. And so the representation is smooth.

For admissibility, let K' be a compact open subgroup in K. Let $f \in \mathcal{B}(\chi_1, \chi_2)^{K'}$ so that $f(kk') = f(k)$. Now since $K' \subset K$ has finite index, the values of $f(k)$ depends only on what coset of K' it is in, hence $f(k)$ is determined by what it does on many things. Therefore $\mathcal{B}(\chi_1, \chi_2)^{K'}$ is a finite dimensional vector space. □

For any representation, we will define a certain module called the Jacquet Module and a functor, the Jacquet Functor which takes a representation to its Jacquet module. The Jacquet module will provide us with many things, but mainly it will allow us to determine if a representation is isomorphic to a principal series. Namely, if the Jacquet module is trivial then it will not be a sub-representation of a Principal-Series representation.

Definition 74. The **Jacquet module** of a representation (π, V) is defined as

$$J(V) = V / span\left\{\pi\left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right).v - v\right\}$$

and the **Jacquet functor**

$$V \mapsto J(V)$$

There is a nice criterion to determine if a representation is has trivial Jacquet module give by the following.

Lemma 75. *Let π be a smooth representation Then, $w \in span\left\{\pi\left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right).v - v\right\} \iff \int_U \pi(u).w\,du = 0$ for some compact open subgroup $U \subset F$.*

Proof. Suppose $w \in span\{\pi\left(\begin{smallmatrix}1 & x\\ & 1\end{smallmatrix}\right).v - v\}$, so that $w = \sum_1^N \pi\left(\begin{smallmatrix}1 & x_i\\ & 1\end{smallmatrix}\right).v_i - v_i$. Pick some neighborhood U containing all of the$\left(\begin{smallmatrix}1 & x_i\\ & 1\end{smallmatrix}\right)$. Then,

$$\begin{aligned}
\int_U \pi(u).w\mathrm{d}u &= \int_U \pi(u).\left(\sum_1^N \pi\left(\begin{smallmatrix}1 & x_i\\ & 1\end{smallmatrix}\right).v_i - v_i\right)\mathrm{d}u \\
&= \sum_1^N \int_U \pi(u)\pi\left(\begin{smallmatrix}1 & x_i\\ & 1\end{smallmatrix}\right)\mathrm{d}u - \int_U \pi(u)\mathrm{d}u \\
&= \sum_1^N \int_U \pi(u')\mathrm{d}u' - \int_U \pi(u)\mathrm{d}u \text{ (take } u' = u\left(\begin{smallmatrix}1 & x_i\\ & 1\end{smallmatrix}\right)) \\
&= 0
\end{aligned}$$

Conversely, suppose $\int_U \pi(u).w\mathrm{d}u = 0$. Let U' be such that $U'.w = w$ (smoothness). Then, intersecting if necessary ensure that $U' \subset U$ so that $U = \bigcup_{i=1}^N u_i U'$ and $u_1 = 1$. Then

$$\begin{aligned}
0 = \int_U \pi(u).w\mathrm{d}u &= \sum_i \int_{u_i U} \pi(u).w\mathrm{d}u \\
&= \sum_i \mu(u_i U)\cdot \pi(u_i).w \\
&= \sum_i a_i \cdot \pi(u_i).w \\
&\text{by adding } w\text{to both sides,} \\
w &= \sum_i a_i \cdot \pi(u_i)w - (-\frac{1}{N})w \\
&= \sum_i a_i' \cdot \pi(u_i)w' - w'
\end{aligned}$$

□

Proposition 76. The Jacquet functor $V \mapsto J(V)$ is exact.

Proof. Suppose

$$0 \to V' \xrightarrow{\alpha} V \xrightarrow{\beta} V'' \to 0$$

was an exact sequence of representations. Then, we need to show that

$$0 \to J(V') \xrightarrow{[\alpha]} J(V) \xrightarrow{[\beta]} J(V'') \to 0$$

is exact. Now, taking quotients is right exact so we only need to check that $[\alpha]$ is still injective. For this we will use the lemma. Let $v' \in V'$ such that $\alpha(v') \in span\{\pi\left(\begin{smallmatrix}1 & x\\ & 1\end{smallmatrix}\right).v - v\}$ i.e. v' is in the kernel of $[\alpha]$. Then there's some neighborhood $U \subset G$ with

$$\begin{aligned} 0 &= \int_U \pi(u).\alpha v' \mathrm{d}u \\ &= \alpha \int_U \pi(u).v' \mathrm{d}u && \alpha \text{ is an intertwiner } + \text{linearity} \\ 0 &= \int_U \pi(u).v' \mathrm{d}u && \text{since } \alpha \text{is injective} \end{aligned}$$

So that $v' = 0$ in $J(V')$. □

Definition 77. An admissible representation is called **supercuspidal** if $J(V) = 0$.

We may classify representations based on the dimension of their Jacquet modules. We first need a small lemma:

Lemma 78. *Let (π, V) be a finitely generated representation of a group G in the sense that there exists $v_1, v_2, , ..., v_N \in V$ such that for any element $v \in V$, $v = \sum_{i=1}^{N} \pi(g_i)v_i$. Then (π, V) has an irreducible quotient.*

Proof. If we take a chain of quotients $V/V_0 \supset V/V_1 \supset V/V_2 \supset ... \supset V/V_k = \{0\}$. then this corresponds to a chain of subspaces $V_0 \subset V_1 \subset V_2 \subset ... \subset V_k = V$. By finite generation the first chain has an upper bound always, and so the first chain has a lower bound - that, is, we can't keep taking smaller and smaller quotients-eventually one will be irreducible. □

Proposition 79. *Let (π, V) be an irreducible admissible representation. Then (π, V) is not supercuspidal $\iff$ it is a sub-representation of a principal series $\mathcal{B}(\chi_1, \chi_2)$.*

Proof. Suppose that $J(V) = V_N \neq 0$. Let $A = \{\left(\begin{smallmatrix} a & \\ & a \end{smallmatrix}\right)\}$, then we can show that V_N is a finitely generated A-module, and so, by the lemma, it has an irreducible quotient. Since A is abelian, we conclude that this quotient is isomorphic to $\mathbb{C}$. Let θ denote the map

$$\theta : V \twoheadrightarrow V_N \twoheadrightarrow \mathbb{C}$$

Since P must act on $\mathbb{C}$ by some character, say $\chi_1(a_1)\chi_2(a_2)\left|\frac{a_1}{a_2}\right|^{\frac{1}{2}}$, for some χ_1, χ_2, we can define the intertwiner $L : V \to \mathcal{B}(\chi_1, \chi_2)$ by

$$L(v) = \theta(\pi(g).v)$$

Conversely, define the following functional on $\mathcal{B}(\chi_1, \chi_2)$

$$L : \mathcal{B}(\chi_1, \chi_2) \to \mathbb{C}, \quad f \mapsto f(1)$$

Since

$$L(\pi\left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right).f(y) - f(y)) = L(\chi_1(1)\chi_2(1)\left|\frac{1}{1}\right|^{\frac{1}{2}} f(y) - f(y)) = L(0) = 0$$

we can say that L descends to a linear functional on $\mathcal{B}(\chi_1, \chi_2)_N$. On the other hand, L is not identically zero on any subspace of $\mathcal{B}(\chi_1, \chi_2)$: we can always find a function f and an element $g \in G$ such that $f(g) \neq 0$ (otherwise its the zero-subspace) then $L(\pi(g)f) = f(g) \neq 0$. So there's a non-zero linear functional on $\mathcal{B}(\chi_1, \chi_2)_N$ so that no subspace of $\mathcal{B}(\chi_1, \chi_2)$ has trivial Jacquet module. □

Theorem 80. *$dim B(\chi_1, \chi_2)_N = 2$*

Proof. The dual of $B(\chi_1, \chi_2)_N$ are linear functionals satisfying $L(\pi(n)f) = L(f)$ where $n \in N = \{\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)\}$. Therefore it is enough to show that the space of such linear functionals is two dimensional. We recall the Bruhat decomposition

$$G = \left\{ P \bigsqcup P\omega N \right\}$$

Let's first consider functions in $B(\chi_1, \chi_2)_N$ that vanish at 1. These are the functions with support on $P\omega N$ - the "big" cell. Then we map the set of Bruhat -Schwartz functions [2] $\mathcal{S}(\mathbb{Q}_p)$ into $B(\chi_1, \chi_2)$ by

$$h(x) \mapsto f_h(g) = \begin{cases} \chi_1(a_1)\chi_2(a_2) \left|\frac{a_1}{a_2}\right|^{\frac{1}{2}} h(x) & g = \left(\begin{smallmatrix} a_1 & * \\ & a_2 \end{smallmatrix}\right) \omega \left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right) \\ 0 & g \text{ in the little cell} \end{cases}$$

This defines an isomorphism with the set of functions such that $f(1) = 0$. Now, if L is a linear functional on $\mathcal{S}(\mathbb{Q}_p)$ which is translation invariant (i.e. $L(\pi(n)f) = L(f)$) then we are in a position to invoke the Reese-Representation Theorem which tells us that

$$L(f) - c \int_{\mathbb{Q}_p} f\left(\omega \left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right)\right) dx = L - c_1 L_1 = 0$$

on functions that vanish at 1. Then, since $L(f) - c_1 L_1$ is a linear functional that takes on the value zero on functions such that $f(1) = 0$. Let W be the set of functions vanishing at 1. This condition makes W a co-dimension 1 set. If we have a linear functional that vanishes on W then it must be a constant, i.e. it must be a linear multiple of the functional $L_2(f) = f(1)$. Therefore $L(f) - c_1 L_1 = c_2 L_2$. So L must be an element in the vector space spanned by $L_1$and L_2. □

Corollary 81. *A composition series i.e. a chain*

$$V_0 \subsetneq V_1 \subsetneq ... \subsetneq V = \mathcal{B}(\chi_1, \chi_2)$$

such that V_i/V_{i-1} is irreducible has length at most two for $\mathcal{B}(\chi_1, \chi_2)$.

Proof. We can take the Jacquet module of this chain and it will still be injective and V_N has dimension two. So the chain can have had length at most 2. □

[2] functions that are compactly supported and locally constant

Corollary 82. $\widehat{\mathcal{B}(\chi_1,\chi_2)} \cong \mathcal{B}(\chi_1^{-1},\chi_2^{-1}) \cong (\chi_1,\chi_2)^{-1} \bigotimes \mathcal{B}(\chi_1,\chi_2)$

Proof. We define an inner product on $\widehat{\mathcal{B}(\chi_1,\chi_2)} \times B(\chi_1^{-1},\chi_2^{-1})$ by

$$< v_1, v_2 >= \int_K v_1(k)v_2(k)dk$$

this gives an injection $\widehat{\mathcal{B}(\chi_1,\chi_2)} \hookrightarrow \mathcal{B}(\chi_1^{-1},\chi_2^{-1})$. We repeat the process in the other direction and by symmetry $\mathcal{B}(\chi_1^{-1},\chi_2^{-1}) \hookrightarrow \widehat{\mathcal{B}(\chi_1,\chi_2)}$. □

0.3.4.1 Classification of Principal Series Representations

We use the results above to classify the principal series representations. We want to know which of these are isomorphic to each other, and which are irreducible.

Theorem 83. $\mathcal{B}(\chi_1,\chi_2)$ is irreducible unless

1. $\chi_1\chi_2^{-1}(a) = |a|^{-\frac{1}{2}}$
2. $\chi_1\chi_2^{-1}(a) = |a|^{\frac{1}{2}}$.

Proof. In the first case, let $\chi(a) = \chi_1(a)|a|^{\frac{1}{2}} = \chi_2(a)|a|^{-\frac{1}{2}}$. Then $\chi(det(g))$ is an invariant subspace

$$\chi(det(\left(\begin{smallmatrix} a & x \\ & b \end{smallmatrix}\right) g) = \chi(ab)\chi(det(g)) = \chi_1(a)\chi_2(b)\left|\frac{a}{b}\right|^{\frac{1}{2}} det(g)$$

If we quotient out by this we get an irreducible representation called the Steinberg representation.

In the second case we have the opposite, $\chi(a) = \chi_1^{-1}(a)|a|^{\frac{1}{2}} = \chi_2^{-1}(a)|a|^{-\frac{1}{2}}$. But here

$$\chi(det(\left(\begin{smallmatrix} a & x \\ & b \end{smallmatrix}\right) g) = \chi(ab)\chi(det(g)) = \chi_1^{-1}(a)\chi_2^{-1}(b)\left|\frac{a}{b}\right|^{\frac{1}{2}} det(g)$$

which is an element of $\mathcal{B}(\chi_1^{-1},\chi_2^{-1})$, the contragredient representation. Therefore, if we look at the space of functions in $\mathcal{B}(\chi_1,\chi_2)$ that are fixed by this linear functional we get a G fixed sub-representation. □

The irreducible (quotient or sub-) representations in cases 1 and 2 in proposition 83 will be called **special representations.**

Theorem 84. *Suppose* $\chi_1 \neq \chi_2$

$$Hom(\mathcal{B}(\chi_1,\chi_2),\mathcal{B}(\eta_1,\eta_2)) = \begin{cases} \mathbb{C} & \text{if } (\chi_1,\chi_2) = (\eta_1,\eta_2) \text{ or } (\eta_2,\eta_1) \\ 0 & \text{otherwise} \end{cases}$$

Proof. Let $V \subset \mathcal{B}(\chi_1,\chi_2)$ be the set of functions which are supported only on the big cell, that is, $V = \left\{ f \in \mathcal{B}(\chi_1,\chi_2) \middle| f(1) = 0 \right\}$. Consider the exact sequence

$$0 \to V \to \mathcal{B}(\chi_1,\chi_2) \overset{ev(1)}{\to} \mathbb{C} \to 0.$$

Taking the Jacquet functor, we find that

$$0 \to V_N \to \mathcal{B}(\chi_1,\chi_2)_N \overset{ev(1)}{\to} \mathbb{C} \to 0$$

is an exact sequence.

Recall that $V = C_c^\infty(F)$, so the action of the diagonal matrices A on V_N is given by $\chi_2(a_1)\chi_1(a_2)\left|\frac{a_1}{a_2}\right|^{\frac{1}{2}}$ since the linear functional (integration) on V acts this way. We get that the action of A is given by $\chi_1(a_1)\chi_2(a_2)\left|\frac{a_1}{a_2}\right|^{\frac{1}{2}}$ on the right. Suppose there were an intertwiner $\mathcal{B}(\chi_1,\chi_2) \to \mathcal{B}(\eta_1,\eta_2)$, we would also have a map on the Jacquet modules

$$\begin{array}{ccccccc} 0 \to & & V_N \to & & \mathcal{B}(\chi_1,\chi_2)_N \overset{ev(1)}{\to} & \mathbb{C} \to & 0 \\ & & \downarrow & & \downarrow & \downarrow & \\ 0 \to & & V_N \to & & \mathcal{B}(\eta_1,\eta_2)_N \overset{ev(1)}{\to} & \mathbb{C} \to & 0 \end{array}$$

The Jacquet modules are $A-$modules (Where $A = \{(\begin{smallmatrix} a_1 & \\ & a_2 \end{smallmatrix})\}$) and they decompose as $\mathbb{C} \bigoplus \mathbb{C}$ as in the above exact sequence. [3] Now any intertwiner gives a map $\mathcal{B}(\chi_1, \chi_2)_N \to \mathcal{B}(\eta_1, \eta_2)_N$ each of which is isomorphic to $\mathbb{C} \bigoplus \mathbb{C}$ so the intertwiner can either swap the two components, or preserve them. In the first case, by comparing the action of A it must be that $\chi_i = \eta_i$ and in the second case that $\chi_1 = \eta_2$ and $\chi_2 = \eta_1$. In either case, there's at most 1-dimension of homomorphisms between the Jacquet modules. This assumes that $\chi_1 \neq \chi_2$ (otherwise both cases can happen) so we deal with that case below. $\square$

We will show that $\dim End(\mathcal{B}(\chi_1, \chi_2)) \leq 1$ when $\chi_1 \neq \chi_2$. We use the same process as above. Suppose we had an intertwiner in $End(\mathcal{B}(\chi_1, \chi_2))$, then it would descend to a map $\mathcal{B}(\chi_1, \chi_2)_N \to \mathcal{B}(\chi_1, \chi_2)_N$. Now there's a bijection between intertwiners M and linear functionals

$$\left\{ L : \mathcal{B}(\chi_1, \chi_2) \to \mathbb{C} \middle| L(\pi(\begin{smallmatrix} a_1 & x \\ & a_2 \end{smallmatrix}) f = \chi_1(a_1)\chi_2(a_2) \left|\frac{a_1}{a_2}\right|^{\frac{1}{2}} L(f) \right\}.$$

Now it's clear that if we had such a linear functional and it was the zero functional on the Jacquet module, then it had to have been trivial to begin with. Therefore there's an injection from intertwiners to maps between the Jacquet modules. Therefore there's at most one dimension of intertwiners of $\mathcal{B}(\chi_1, \chi_2)$.

0.3.4.2 Local Zeta Integral and Functional Equation

Of interest will be the $L-$factors of a local representation. They are defined to be

---

[3] *Proof.* The reason that $\mathcal{B}(\chi_1, \chi_2)_N$ decomposes so nicely is because if f_1 and f_2 were basis vectors then $\pi(\begin{smallmatrix} a_1 & \\ & a_2 \end{smallmatrix})(f_1 + V(N)) = \chi_1(a_1)\chi_2(a_2)\left|\frac{a_1}{a_2}\right|^{\frac{1}{2}} f_1 + V(N)$ because A fixes $V(N)$. So f_1 and f_2 are mapped to their own subspaces under the action of A. We can always take the first function f_1 to vanish at 1. $\square$

1. Unramified principal series. $\mathcal{B}(\chi_1, \chi_2)$ where both characters have no ramification we get the L-function

$$L_v(s, \pi) = (1 - \chi_1(\varpi_v)q^{-s})(1 - \chi_2(\varpi_v)q^{-s})$$

2. Ramified principal series

$$L_v(s, \pi) = L_v(s, \chi_1)L_v(s, \chi_2) \text{ as in } GL(1)$$

3. Special Representation (unitary)

$$L_v(s, \pi) = (1 - \chi(\varpi)|\varpi|^s)^{-1}$$

4. Supercuspidal representation

$$L_v(s, \pi) = 1$$

There are several ways to define the Zeta-integral for $GL(2)$ but one that is convenient and also generalizes well uses a so-called "matrix coefficient" of a representation.

Definition 85. A matrix coefficient of a representation (π, V) is a function from G to $\mathbb{C}$ of the following form. Let $v \in V$ and $\tilde{v} \in V^*$, then we construct the function

$$f_{v,\tilde{v}}(g) =< \pi(g).v, \tilde{v} > .$$

Such a function is called a **matrix coefficient for** π.

Theorem 86. *Let (π, V) be supercuspidal. Then matrix coefficients are compactly supported modulo the center. If (π, V) is a special representation then the matrix coefficients are in $\mathcal{L}^2(Z\backslash G)$.*

Definition 87. Let $s \in \mathbb{C}$, ϕ be a locally constant, compactly supported (Bruhat-Schwartz) function on $GL(2, F_v)$ and $\beta(g)$ a matrix coefficient for some representation (π, V) We define the local-zeta integral

$$Z_v(s,\phi,\beta) := \int\limits_{GL(2,F_v)} \phi(g)\beta(g)|\det(g)|^{s+\frac{1}{2}}d^\times g$$

Theorem 88. *(local functional equation).*

1. The local zeta integral Z_v converges in some half-plan.
2. Z_v is a rational function of q^{-s} and as we range over all ϕ, β they have a common divisor given by $L_v(s,\pi)$. Furthermore, there exist ϕ and β such that $Z_v(s,\phi,\beta) = L_v(s,\pi)$
3. $Z_v(s,\phi,\beta) = \gamma(s,\pi)Z_v(1-s,\hat{\phi},\check{\beta})$ where $\check{\beta}(g) = \beta(g^{-1})$
4. $\frac{Z_v(s,\phi,\beta)}{L(s,\pi)} = \epsilon(s,\pi)\frac{Z_v(1-s,\hat{\phi},\check{\beta})}{L(1-s,\tilde{\pi})}$ for some function $\epsilon(s,\pi)$ not depending on β or ϕ. The epsilon factors are tabulated in section 0.3.5

0.3.4.3 The Global Zeta Integral

Let (π, V) be a cuspidal automorphic representation. A matrix coefficient is of the form $< \pi(g).v, \tilde{v} >$ but if we're if the representation is unitary then using the inner product we get an association $V \to \tilde{V}$ and so we can write any matrix coefficient as

$$\beta(g) = \int\limits_{GL_2(F)\cdot Z\backslash GL(2,\mathbb{A}_F)} f_1(hg)\overline{f_2(h)}d^\times h$$

Definition 89. Let $\Re(s) \gg 0$ and Φ be a Bruhat-Schwartz function. We define the global-zeta integral to be

$$Z(s,\Phi,\beta) := \int\limits_{GL(2,\mathbb{A}_F)} \Phi(g)\beta(g)|det(g)|^{s+\frac{1}{2}}d^\times g$$

Theorem 90. *With the zeta integral defined as above,*

$$Z(s,\Phi,\beta) = Z(1-s,\hat{\Phi},\check{\beta})$$

Proposition 91. *Let β be a matrix coefficient. Thenβ factors into $\prod \beta_v$. If Φ is factorizable then*

$$Z(s, \Phi, \beta) = \prod_{v \leq \infty} Z_v(s, \Phi_v, \beta_v)$$

(This leads to the classical functional equation of modular forms).

0.3.5 Tabulation of Epsilon Factors

In this section we record the $\epsilon-$factors for $GL(2)$ as in Jacquet-Langlands. For this we will need the results of Tate's thesis as well which we record here.

0.3.5.1 Epsilon Factors for $GL(1)$ (Tate's Thesis)

1. At a finite prime. Let μ be a character of conductor $\mathfrak{f}$ of the non-archimedian field F_v

$$\epsilon(s, \mu)^{-1} = \begin{cases} 1 & \mu \text{ is unramified} \\ \frac{N(\mathfrak{d}\mathfrak{f})^{s-\frac{1}{2}} N(\mathfrak{f})^{-\frac{1}{2}}}{\mu(\mathfrak{d}\mathfrak{f})} \tau(\mu) & \mu \text{ ramified} \end{cases}$$

[4]where

- ϖ is the local uniformizer
- $\tau(\mu) = \sum_{a \in \mathfrak{o}^\times/\mathfrak{f}} \mu(a) e^{2\pi i \Lambda(a/\varpi^{ord(\mathfrak{d}\mathfrak{f})})}$
- $\Lambda(x) = Tr(\sum_{-N}^{-1} a_i \varpi^i)$ where Tr is the field trace $K_v \to \mathbb{Q}_v$ and $x = \sum_{-N}^{\infty} a_i \varpi^i$
- The local ring of integers has different ideal $\mathfrak{d} = \varpi^{ord(\mathfrak{d})}$
- $\psi(x) = e^{2\pi i \Lambda(x/\varpi^{ord(\mathfrak{d}\mathfrak{f})})}$ is an additive character of F_v

---

[4]

- This expression differs a bit from the one in Tate's thesis because we do not assume $\mu(\pi) = 1$

2. At a real place. There are two possible characters

$$\epsilon(s,\mu)^{-1} = \begin{cases} 1 & \mu = \mathbf{1} \\ i & \mu = \text{sign} \end{cases}$$

3. At a complex place. If $\mu|\cdot|^s = e^{in\theta}r^s$, take $L_{\mathbb{C}}(s,\mu) = 2\pi^{-s}\Gamma(s+\frac{|n|}{2})$

$$\epsilon(s,\mu)^{-1} = (-i)^{|n|}$$

0.3.5.2 Epsilon Factors for $GL(2)$ (as in Jacquet-Langlands)

1. At a finite prime,

$$\epsilon(s,\pi,\psi) = \begin{cases} \epsilon(\mu_1,s)\epsilon(\mu_1,s) & \pi = \pi(\mu_1,\mu_2) \text{ a principal series representation} \\ \epsilon(\mu_1,s)\epsilon(\mu_2,s) & \pi = \sigma(\mu_1,\mu_2) \text{ a special representation where } \mu \text{ is ramified} \\ -\mu_1(\varpi)|\varpi|^{s-1}. & \\ \epsilon(\mu_1,s)\epsilon(\mu_2,s) & \pi = \sigma(\mu_1,\mu_2) \text{ a special representation where } \mu \text{ is unramified} \end{cases}$$

2. At a real place

$$\epsilon(s,\pi) = \begin{cases} \epsilon(s,\mu_1)\epsilon(s,\mu_2) & \pi \text{ is a principal series,} \\ \epsilon(s,\omega)\lambda(\mathbb{C}/\mathbb{R},\psi_{\mathbb{R}}) & \text{otherwise. Where } \omega \text{ is the central character} \\ & \text{and } \lambda\text{depends on the additive character only.} \end{cases}$$

3. At a complex place (this case will not come up in my computations because there are no non-trivial quadratic characters of $\mathbb{C}$)

$$\epsilon(s,\pi) = \epsilon(s,\mu_1)\epsilon(s,\mu_2)$$

0.4 Root Numbers of Quadratic Twists of Elliptic Curves

0.4.1 Modularity, Revisited

Because automorphic representations of $GL(2)$ are such a powerful tool, in this thesis we only consider elliptic curves which are modular, a property which is defined as follows. Let E be an elliptic curve with conductor $\mathfrak{N}$ over a number field K. Then E is modular if the Hasse-Weil $L-$function of E/K is equal to the $L-$function of a cuspidal Hilbert modular form of parallel weight 2, and level $\mathfrak{N}$ (See[7]). In particular, the Hasse-Weil $L-$function of E, denoted $L(E/K, s)$ or simply $L(E, s)$ is equal to the $L-$function of a cuspidal automorphic representation $\pi_E = \otimes \pi_{E,v}$ of $GL(2, \mathbb{A}_K)$ associated to a Hilbert modular form, and therefore $L(E, s)$ satisfies a functional equation. It is known that all elliptic curves over $K = \mathbb{Q}$ are modular [1] and recently it has been shown that most elliptic curves over totally real fields and real quadratic extensions of totally real fields, are modular [12; 6].

Let $\Lambda_E(s)$ denote the "completed" L-function of π_E , that is, including the factors at the archimedian places. Then the functional equation takes the form $\Lambda_E(s) = w\Lambda(1-s)$ where $w \in \{\pm 1\}$, called the root number will play a pivotal role in this paper. The **analytic rank** of E, denoted $rk(E)$ is defined as

$$rk(E) = \text{order of vanishing of } \Lambda_E(s) \text{ at } s = \frac{1}{2}.$$

For an elliptic curve E/K, we study the **quadratic twists** of E: these are elliptic curves E' which are isomorphic to E over some quadratic extension K'/K. In order to make assertions about density in a family of curves, it is necessary to order them in some way. Suppose that E' is isomorphic to E over some quadratic field K'. Then via standard class field theory, there is a unique quadratic Hecke character χ, associated to the extension K'/K. Let E^χ be the curve which is isomorphic to E over the quadratic field K' with associated Hecke character χ and let $C(K)$ be the set of all quadratic Hecke characters of $\mathbb{A}_K^\times$. For $\chi \in C(K)$, let $q_1, q_2, ..., q_n$ be the places where χ is ramified. Then we define the norm, $N\chi = \max_i\{Nq_i\}$ which gives an ordering of twists of an elliptic curve. Our main result is the following:

Theorem 92. *Let E be a modular elliptic curve over a number field K such that no local supercuspidal representations occur in the factorization of π_E, then*

$$\lim_{X\to\infty} \frac{\#\{\chi \in C(K) \mid N\chi \leq X \text{ and } rk(E^\chi) \text{ is even}\}}{\#\{\chi \in C(K) \mid N\chi \leq X\}} = \frac{1+(-1)^{rk(E)}\kappa}{2}$$

where $\kappa = \prod \kappa_v$ is a product over the places of K given by

Theorem.

$$\kappa_v = \begin{cases} 0 & \text{if } K_v \backsimeq \mathbb{R} \\ 1 & \text{if } K_v \backsimeq \mathbb{C} \\ 2/|c_v| - 1 & E \text{ has split mutiplicative reduction at } v \\ 1 - 2/|c_v| & E \text{ has nonsplit multiplicative reduction at } v \\ 1 - 2/|c_v| & E \text{ has multiplicative reduction in a quadratic extension at } v \\ 1 & E \text{ has potentially multiplicative reduction (non-quadratic)} \\ 1 & \text{otherwise} \end{cases}$$

and $|c_v|$ is the number of degree 2 extensions of K_v (if $v \mid 2$ then $|c_v| = 4 \cdot 2^{[K_v:\mathbb{Q}_v]}$) otherwise $|c_v| = 4$) .

In particular the theorem holds unconditionally for semi-stable curves over a real quadratic field[12]. Note that if the field K has a real embedding then the density of even analytic ranks is exactly $\frac{1}{2}$.

0.4.2 Some Notation

Let K be a number field and let E be an elliptic curve over K with conductor $\mathfrak{N}$. Let $\Lambda_E(s)$ be the completed L-function of E, which, under the assumption of modularity, is also the $L-$function of a cuspidal automorphic representation of $GL(2, \mathbb{A}_K)$. Let $\chi : K^\times \backslash \mathbb{A}_K^\times \to \pm 1$ be a quadratic Hecke character with conductor $\mathfrak{f}$ and let $\Lambda_E(s, \chi) = \Lambda_{E^\chi}(s)$ denote the L-function of the quadratic twist E^χ. Let $w \in \{\pm 1\}$ be the "root number" in the functional

equation, i.e. such that $\Lambda_E(s) = w\Lambda_E(1-s)$ and let $n(\chi)$ be the "change" in the epsilon factor, i.e such that $\Lambda_E(s,\chi) = n(\chi)\cdot\omega\Lambda_E(1-s,\chi)$ holds. Recall that $rk(E)$ denotes the analytic rank of E, as defined in the previous section.

Let $C(K)$ be the group of global quadratic Hecke characters and $C(K_v)$ be the group of local quadratic characters at a place v of K. We define the norm of a Hecke character as $N\chi := \max_{\substack{\chi \text{ ramifies} \\ \text{at } q}} \{Nq\}$.

Let $C(K,X)$ be the group of global Hecke characters such that $N\chi \leq X$ and $\Gamma = \prod_{v\in\Sigma} C(K_v)$ where Σ is a finite set of places including ∞, and all $v \mid \mathfrak{N}$.

Let E/K be a modular elliptic curve, then the L-function $\Lambda_E(s)$ is equal to the $L-$function $\Lambda(\pi_E, s)$ attached to a global automorphic representation π_E of $GL(2,\mathbb{A}_Q)$ arising from a Hilbert modular form. In particular, this implies that $\Lambda(\pi_{E^\chi}, s) = \Lambda(\chi\otimes\pi_E, s)$.

Let K_v be a local field. If K_v is non-archimedian, let ϖ be a uniformizing element and let$\mathfrak{o}_v$ be the ring of integers of K_v.

At a non-archimedian place v, the admissible representations of $GL(2,K_v)$ are classified into 3 basic types of representation [10]. The class of supercuspidal representations is excluded from this paper because their local epsilon factors present difficulties with respect to computation. The other two types, the principal series representations, denoted $\pi(\mu_1,\mu_2)$ and the special representation denoted $\sigma(\mu_1,\mu_2)$ are discussed in detail in [10] which is also a major reference for the computational aspects in this paper. Because elliptic curves are self-dual we have that $\mu_1 = \mu_2^{-1}$ in both the supercuspidal and the special representations occurring in the factorization of π_E.

0.4.3 Change in Global Root Number

The functional equation of an elliptic curve takes the form $\Lambda_E(s) = w\Lambda_E(1-s)$ where w is either +1 or -1. Thus, the order of vanishing at $s=\frac{1}{2}$ is even if and only if $w=1$. Consider a quadratic twist of this $L-$function $\Lambda_E(s,\chi)$, we expect the root number to change by a

prescribed amount

$$\Lambda_E(s,\chi) = n(\chi) w \Lambda_E(1-s,\chi)$$

so that,

$$rk(E^\chi) \equiv rk(E) \mod 2 \iff n(\chi) = 1 \tag{0.4.1}$$

Next we compute $n(\chi)$ explicitly.

Proposition 93. *Let $\chi = \prod_v \chi_v$ and let ϖ denote a local uniformizer at v. Then*

$$n(\chi) = \prod_v n_v(\chi_v)$$

where the n_v are given explicitly by the following table:

i	Type of Representation		$n_v(\chi)$
1	$\pi_v = \pi_v(\mu_v, \mu_v^{-1})$	χ_v is unramified.	1
2	, μ_v is	χ_v is ramified.	$\chi(-1)$
3	unramified, $\pi_v = \pi_v(\mu_v, \mu_v^{-1})$	χ_v is unramified.	1
4	, μ_v is ramified	χ_v is ramified, $\mu_v\chi_v$ is unramified.	$\chi_v(-1)$
5		χ_v is ramified, $\mu_v\chi_v$ is ramified.	$\chi_v(-1)$
6	$\pi_v = \sigma_v(\mu_v, \mu_v^{-1})$	χ_v is unramified.	$\chi_v(\varpi)$
7	, μ_v is	χ_v is ramified.	$-\chi_v(-1)\mu_v(\varpi)^{-1}$
8	unramified, $\pi_v = \sigma_v(\mu_v, \mu_v^{-1})$	χ_v is ramified, $\mu_v\chi_v$ is ramified.	$\chi_v(-1)$
9	, μ_v is ramified,	χ_v is ramified, $\mu_v\chi_v$ is unramified.	$-\chi_v(-\varpi)\mu_v(\varpi)$
10		χ_v is unramified.	1

Proof. Let $\mathfrak{N} = \prod \eta_v$ be the conductor of the elliptic curve E, and $\mathfrak{f} = \prod \mathfrak{f}_\mathfrak{v}$, the conductor of χ as in section 2, and let ϖ_v be a local uniformizer at v. It follows from the tensor-product theorem ([9] Chapter 10, [10]), that $n = \prod_v n(\chi_v)$, where the local root number $n(\chi_v) \in \{\pm 1\}$

is such that

$$L_v(s, \chi \otimes \pi) = n(\chi_v) \cdot w_v L_v(1-s, \chi \otimes \pi)$$

holds, where w_v is the local root number of the (untwisted) local L-function. In order to find $n(\chi_v)$ we first compute

$$a_v(s) = \frac{\epsilon(s, \pi_v)}{\epsilon(s, \pi_v \otimes \chi_v)}$$

and then for any $s \in \mathbb{R}_{>0}$ we have that

$$n(\chi_v) = \frac{a_v(s)}{|a_v(s)|}$$

The essence of this manipulation is that the root number is the "sign" of the epsilon factor. The proposition then follows from local epsilon factor computations in each case as given in Jacquet-Langlands [10]. As an illustration we include the proof in one of the above cases.

The case presented here is when π_v is an unramified representation but $\chi_v \otimes \pi_v$ is not (line 2 in the chart). This is equivalent to the statement that $v \nmid \mathfrak{N}$, $v \mid \mathfrak{f}$ i.e. that the representation π_v is an unramified principal series $\pi(\mu_1, \mu_2)$ and that χ_v is ramified with conductor $\mathfrak{f}_v$. Choose an additive character of K_v, say $\psi(x) = e^{2\pi i \Lambda(a/\mathfrak{d}\mathfrak{f}_\mathfrak{v})}$, as defined in Tate's thesis [13]. With the formulas as in [10], we compute:

$$\begin{aligned}
\epsilon(s, \pi_v \otimes \chi_v, \psi)^{-1} &= \epsilon(s, \chi_v \mu_1)^{-1} \epsilon(s, \chi_v \mu_2)^{-1} \\
&= \prod_{i=1,2} \frac{1}{\mu_i \chi_v(\mathfrak{d}\mathfrak{f})} N(\mathfrak{d}\mathfrak{f})^{s-\frac{1}{2}} N\mathfrak{f}^{-\frac{1}{2}} \sum \mu_i \chi_v(a) \psi(a) \\
&= \frac{1}{\mu_1 \mu_2 (\mathfrak{d}\mathfrak{f}_\mathfrak{v})} \epsilon(s, \chi_v, \psi)^{-2} \\
&= \epsilon(s, \chi_v, \psi)^{-2}
\end{aligned}$$

the last formula following from the fact that $\mu_1 \mu_2 = 1$ for all elliptic curves. We also have that

$$\epsilon(s, \pi_v) = N(\mathfrak{d})^{2s-1}$$

whenever π_v is unramified. So that

$$\begin{aligned} a_v &= \tfrac{\epsilon(s,\chi_v,\psi)^{-2}}{N(\mathfrak{d})^{2s-1}} \\ &= \tfrac{N\mathfrak{f}_\mathfrak{v}{}^{2s-2}}{\chi_v(\mathfrak{d}\mathfrak{f}_v)^2}\left(\sum_{a \bmod \mathfrak{f}_v}\chi(a)\psi(a)\right)^2 \\ &= N\mathfrak{f}_v^{2s-2}\tau(\chi_v)^2 \\ &= N\mathfrak{f}_v^{2s-1}\chi_v(-1) \end{aligned}$$

Where $\tau(\chi_v)$ is the gauss sum of χ_v with respect to the additive character ψ. The fact that $\tau(\chi_v)^2 = N\mathfrak{f}_v\chi(-1)$ can be shown using the epsilon factors for GL(1) (e.g. see [3], section 23.) We have that $n_v(\chi_v) = \chi(-1)$.

Let S_i be the set of places that have the properties of the ith row in the Table. For example, S_1 is the set of places where π_v is unramified and χ_v is unramified. □

Proposition 94. *We have*

$$rk(E^\chi) \equiv rk(E) \mod 2 \iff \prod_{\substack{v|\infty \\ v \text{ real}}}\chi_v(-1)\prod_{S_6}\chi_v(\varpi_v)\prod_{S_7}\frac{-1}{\mu_v(\varpi)}\prod_{S_9} -\chi_v\mu_v(\varpi) = 1$$

where S is the set of places where π_v is a special representation.

Proof. By equation 0.4.1 and Proposition 93 we have that

$$rk(E^\chi) \equiv rk(E) \mod 2$$

$$\iff$$

$$\prod_{S_1,S_3,S_{10}} 1 \prod_{S_2,S_4,S_5,S_8}\chi_v(-1)\prod_{S_6}\chi_v(\varpi)\prod_{S_7}\tfrac{-\chi_v(-1)}{\mu_v(\varpi)}\prod_{S_9} -\chi_v(-\varpi)\mu_v(\varpi) = 1$$

Now, since χ is a Hecke character, $\chi(-1,-1,...-1...) = \prod\chi_v(-1) = 1$. Therefore, we may multiply the right hand side by $\prod\chi_v(-1)$. Now since χ_v is unramified in the sets S_1, S_3, S_{10} and S_6, the result follows. □

It will be useful to simplify the expression in Proposition 94. Let us denote $\Sigma_1 = S_6 \cup S_7$ and $\Sigma_2 = S_8 \cup S_9 \cup S_{10}$. Let $m_v(\chi) = \chi_v(-1)a_v(\chi)$ for finite places v and $m_v(\chi) = \chi_v(-1)$

for real places. More explicitly,

$$m_v(\chi) = \begin{cases} \chi_v(\varpi) & \text{if } \chi_v\text{is unramified} \\ -\mu_v(\varpi)^{-1} & \text{if } \chi_v \text{ is ramified} \end{cases} \quad \text{for } v \in \Sigma_1$$

$$m_v(\chi) = \begin{cases} 1 & \text{if } \chi_v\text{is unramified} \\ 1 & \text{if } \chi_v \text{ and } \chi_v\mu_v\text{are ramified} \\ -\chi_v\mu_v(\varpi) & \text{if } \chi_v \text{ is ramified and } \chi_v\mu_v \text{ is unramified} \end{cases} \quad \text{for } v \in \Sigma_2$$

and

$$m_v(\chi) = \chi_v(-1) \qquad \text{for } v\text{real}$$

in

We will rewrite Proposition 94 as

$$rk(E^\chi) \equiv rk(E) \mod 2 \iff \prod_{\Sigma_1 \cup \Sigma_2 \cup \Sigma_\mathbb{R}} m_v(\chi). \tag{0.4.2}$$

Note that $\Sigma_\mathbb{R}$ are the real places, Σ_1 are places where π_v is a special representation with unramified character and Σ_2 are places where π_v is a special representation with a ramified character. Thus, only the places where special representations occur (or real places) change the root number of a twisted curve.

0.4.4 The Density of Even Analytic Ranks

According to equation 0.4.2, the parity of the analytic rank doesn't change upon twisting by χ if and only a certain product of $-1's$ and $+1's$ occurring on the right-hand side of 0.4.2 is equal to 1. The next step involves computation the proportion of cases where the product is $+1$. This amounts to an exercise in counting quadratic characters.

Let c_v be the set of local quadratic characters (if $v \nmid 2$ then $|c_v| = 4$, and if $v \mid 2$ then $|c_v| = 4 \cdot 2^{[K_v:\mathbb{Q}_v]}$), and let $\Sigma = \Sigma_1 \cup \Sigma_2 \cup \Sigma_\mathbb{R}$, where $\Sigma_\mathbb{R}$ is the set of real places of K. For

each element of Σ, define

$$\kappa_v = \frac{1}{|c_v|} \sum_{\chi_v \in c_v} m_v(\chi_v), \qquad \text{for } v\text{in } \Sigma$$

Lemma 95. *Let* $\Gamma = \prod_{v \in \Sigma} C(K_v)$ *. Then,*

$$\frac{|\{\chi \in \Gamma \mid n(\chi) = 1\}|}{|\Gamma|} = \frac{1 + \prod_{v \in \Sigma} \kappa_v}{2}$$

Proof. (This is lemma 7.5 in [11]) Let $N = |\{\chi \in \Gamma \mid n(\chi) = 1\}|$. Then$\Gamma$ can be written as $\prod_{v \in \Sigma} c_v$, and we have that

$$N - (|\Gamma| - N) = \sum_{\gamma \in \Gamma} \prod_{v \in \Sigma} m_v(\gamma_v) = \prod_{v \in \Sigma} \sum_{\gamma_v \in c_v} m_v(\gamma_v).$$

Now when we divide both sides by $\Gamma = \prod_{v \in \Sigma} c_v$ we get that $2N/|\Gamma| - 1 = \prod_{v \in \Sigma} \kappa_v$ and the lemma follows. □

Next, we compute the values of κ_v.

Lemma 96. *The local factors* κ *have the following values*

- $\kappa_v = 0$ when $K_v \backsimeq \mathbb{R}$
- $\kappa_v = \begin{cases} 2/|c_v| - 1 & E \text{ has split mutiplicative reduction at } v \\ 1 - 2/|c_v| & E \text{ has nonsplit multiplicative reduction at } v \end{cases}$ for $v \in \Sigma_1$
- $\kappa_v = \begin{cases} 1 - 2/|c_v| & E \text{ has mult. red. in a quad. extension at } v \\ 1 & \text{otherwise} \end{cases}$ for $v \in \Sigma_2$
- $\kappa_v =$1 if E has good reduction, potentially good reduction, or $K_v \backsimeq \mathbb{C}$

Note that Σ_1 are the places where E has multiplicative reduction and Σ_2 are the places where E has potentially multiplicative reduction. Thus, $\Sigma_1 \cup \Sigma_2 \cup \{\text{real places}\}$ are the only places that affect the value of κ.

Proof. For a real place, there are exactly two characters: χ_{triv} and χ_{sign} and $\kappa_\infty = \frac{1}{2}(\chi_{triv}(-1)+\chi_{sign}(-1)) = 0$.

For a non-archimedian place in Σ_1, there is one trivial character χ_{triv} and an unramified character $\chi_{u.r.}$. For the first two, $m_v(\chi_v) = \chi_v(\varpi)$, so that $m_v(\chi_{triv}) = 1$ and $m_v(\chi_{u.r.}) = -1$. For the ramified characters χ_{ram}, $m_v(\chi_{ram}) = -\mu_v(\varpi_v)$. In total we have

$$\kappa_v = \frac{1}{|c_v|}\left(1 - 1 + (|c_v| - 2)\,\mu_v(\varpi)\right)$$

It follows from a comparison of the $L-$function at multiplicative reduction and at a special representation with unramified character that $\mu_v(\varpi) = 1$ at split multiplicative reduction and $\mu_v(\varpi) = -1$ at non-split multiplicative reduction, which gives the result for $v \in \Sigma_1$.

For $v \in \Sigma_2$, we are in the situation where the local representation is of the form $\sigma_v(\mu_v, \mu_v^{-1})$ where μ_v is ramified. If χ_v is unramified, then $m_v(\chi_v) = 1$. If χ_v is ramified and $\chi_v\mu_v$ is also ramified, then $m_v(\chi_v) = 1$. If $\chi_v\mu_v$ is unramified, then $\mu_v\mid_{\mathfrak{o}_k^\times}$ must be a quadratic character and then there are exactly two characters $\chi_{v,1}$ and $\chi_{v,2}$ such that $\chi_v\mu_v$ is unramified and furthermore, $\chi_{v,1}(\varpi) = 1$, and $\chi_{v,2}(\varpi) = -1$ so that $m_v(\chi_{v,1}) = -\mu_v(\varpi)$ and $m_v(\chi_{v,2}) = \mu_v(\varpi)$. In total, if $\mu_v\mid_{\mathfrak{o}_k^\times}$ is not quadratic, then $m_v(\chi_v) = 1$ for all local characters χ_v and if $\mu_v\mid_{\mathfrak{o}_k^\times}$ is quadratic then

$$\kappa_v = \frac{1}{|c_v|}\left(1 \cdot (2 - |c_v|) + \mu_v(\varpi) - \mu_v(\varpi)\right) = 1 - 2/|c_v|$$

Now, if $\mu_v\mid_{\mathfrak{o}_k^\times}$ is quadratic, then the elliptic curve has potential multiplicative reduction at v (in particular, multiplicative reduction in a quadratic extension of K_v). □

The following lemma deals with the problem that not all collections of local characters give rise to global characters.

Lemma 97. *Recall that $C(K)$ is the group of global quadratic characters, and $\Gamma = \prod_{v\in\Sigma} C(K_v)$. The natural homomorphism $\alpha : C(K) \to \Gamma$ is surjective.*

Proof. Let $\gamma = \prod \gamma_v \in \prod_{v \in \Sigma} C(K_v)$ and let s be a place of K, not in Σ. Then if we set $\gamma_s(q) = \gamma^{-1}(q)$, for all $q \in K^\times \subset K_v^\times$, this defines a character on a dense subset of K_v, hence on all of K_v by continuity. Then $\gamma' = (\prod \gamma_v) \cdot \gamma_s$ is trivial on $K^\times$ and $\alpha(\gamma') = \gamma$. □

The lemma allows us to convert statements about the density of even analytic ranks among arbitrary products of local characters to statements about the density of even analytic ranks among Hecke characters.

To conclude, I will restate and prove the main theorem

Theorem. *For all X large enough,*

$$\frac{\#\{\chi \in C(K,X) \text{ such that } rk(E^\chi) \text{ is even}\}}{|C(K,X)|} = \frac{1 + (-1)^{rk(E)}\kappa}{2}$$

where $\kappa = \prod_v \kappa_v$ are defined and computed above.

Proof. For X large enough, the set of characters with norm less than X surjects onto Γ by lemma 97. Now by Proposition 94 the analytic rank only depends on a local product, and since the map $C(K) \to \Gamma$ is a homomorphism, all its fibers have the same size. Therefore,

$$\frac{\#\{\chi \in C(K,X) \text{ such that } \mathrm{rk}(E^\chi) = \mathrm{rk}(E)\ \}}{|C(K,X)|} = \frac{\#\{\chi \in \Gamma \text{ such that } n(\chi) = 1\ \}}{|\Gamma|}$$

And now the theorem follows from lemma 95. □

Our theorem is about the expected parity of twists of E. The heuristic that elliptic curves have rank as low as possible implies that given the parity constraints, the curves in this family will have analytic rank 0 or 1 with far greater frequency than the higher order ranks. Thus together with the Birch and Swinnerton-Dyer conjecture, our results support the conjecture in [11]

Conjecture. *(Klagsbrun-Mazur-Rubin)*

$$\lim_{X \to \infty} \frac{\sum_{\chi \in C(K,X)} rk(E^\chi)}{|C(K,X)|} = \frac{1 + (-1)^{rk(E)}\kappa}{2}$$

Where the conjecture is adapted to *analytic* ranks and the local factors of κ are explicitly computed in the cases of lemma 96.

0.4.5 The Main Computations

0.4.6 Local Epsilon Factor Changes

We assume that we have a representation $\pi = \bigotimes \pi_v$ and that it has associated epsilon factors $\epsilon = \bigotimes \epsilon_v$. We'd like to know what the epsilon factor is for $\chi \otimes \pi$, I'm going to record the factor it changes by in each case, keeping in mind that this is a quadratic twist of an elliptic curve which implies that the representations are unitary, self-dual and that the central character is trivial. I am also going to assume that E has no local supercuspidal representations attached to it (because it's very difficult to deal with the epsilon factors in this case)

- Let, $N = \prod \eta_v = \prod \varpi^{n_v}$ be the conductor of E (the places where it has bad reduction).
- Let $\mathfrak{f} = \prod \mathfrak{f}_p$ be the conductor of χ(the places where χ is ramified). That is, χ_v is trivial on $1 + \varpi_v^{ord(\mathfrak{f}_v)} \mathfrak{o}_{\mathfrak{v}}^{\times}$
- Let $a_v(\chi) = sign(\frac{\epsilon(\pi_v \otimes \chi)}{\epsilon(\pi_v)})$

1. Nothing is ramified. $a_v(\chi) = 1$

2. $\pi_v = \pi(\mu_v, \mu_v^{-1})$ is unramified and χ_v is ramified. Then,

$$\begin{aligned} \epsilon(\pi_v, s) &= \epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= 1 \\ &= 1 \end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi, s) &= \epsilon(\chi\mu_v, s)\epsilon(\chi\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}_\mathfrak{v}\mathfrak{f}_v)^{2s-1}N(\mathfrak{f}_\mathfrak{v})^{-1}}{\mu_v\mu_v^{-1}\chi_v^2(\mathfrak{d}\mathfrak{f})}\tau(\chi\mu)\tau(\chi\mu^{-1}) \\ &= N(\mathfrak{d}_\mathfrak{v}\mathfrak{f}_v)^{2s-1}N(\mathfrak{f}_\mathfrak{v})^{-1}N(f_v)\chi(-1) \\ &= N(\mathfrak{d}_\mathfrak{v}\mathfrak{f}_v)^{2s-1}\chi(-1)\end{aligned}$$

so $a_v(\chi) = sign\left(\frac{N(\mathfrak{d}_\mathfrak{v}\mathfrak{f}_v)^{2s-1}\chi(-1)}{N\mathfrak{d}^{2s-1}}\right) = sign\left(N(\mathfrak{f}_v)^{2s-1}\chi(-1)\right) = \chi(-1)$

3. χ_v is unramified, $\pi_v = \pi(\mu_v, \mu_v^{-1})$ and μ_v is ramified.

$$\begin{aligned}\epsilon(\pi_v, s) &= \epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}_v\eta_v)^{2s-1}N(\eta_v)^{-1}}{\mu_v\mu_v^{-1}(\mathfrak{d}\eta_v)}\tau(\mu_v)\tau(\mu_v^{-1}) \\ &= N(\mathfrak{d}_v\eta_v)^{2s-1}\mu_v(-1)\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi, s) &= \epsilon(\chi\mu_v, s)\epsilon(\chi\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}_\mathfrak{v}\eta_v)^{2s-1}N(\eta_v)^{-1}}{\mu_v\mu_v^{-1}\chi_v^2(\mathfrak{d}\mathfrak{f})}\tau(\chi\mu_v)\tau(\chi\mu_v^{-1}) \\ &= N(\mathfrak{d}_\mathfrak{v}\eta_v)^{2s-1}N(\eta_v)^{-1}N(\eta_v)\chi\mu(-1) \\ &= N(\mathfrak{d}_\mathfrak{v}\eta_v)^{2s-1}\mu(-1)\end{aligned}$$

so $a_v(\chi) = sign\left(\frac{N(\mathfrak{d}_\mathfrak{v}\eta_v)^{2s-1}\mu(-1)}{N(\mathfrak{d}_v\eta_v)^{2s-1}\mu_v(-1)}\right) = 1$

4. χ_v is unramified, $\pi_v = \sigma(\mu_v, \mu_v^{-1})$ and μ_v is ramified. Then,

$$\begin{aligned}\epsilon(\pi_v, s) &= \epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= N(\mathfrak{d}_v\eta_v)^{2s-1}\mu_v(-1) \text{ (as above)}\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi, s) &= \epsilon(\chi\mu_v, s)\epsilon(\chi\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}_\mathfrak{v}\eta_v)^{2s-1}N(\eta_v)^{-1}}{\mu_v\mu_v^{-1}\chi_v^2(\mathfrak{df})}\tau(\chi\mu_v)\tau(\chi\mu_v^{-1}) \\ &= N(\mathfrak{d}_\mathfrak{v}\eta_v)^{2s-1}N(\eta_v)^{-1}N(\eta_v)\chi\mu(-1) \\ &= N(\mathfrak{d}_\mathfrak{v}\eta_v)^{2s-1}\mu_v(-1)\end{aligned}$$

so $a_v(\chi) = 1$

5. χ_v is unramified, $\pi_v = \sigma(\mu_v, \mu_v^{-1})$ and μ_v is unramified.

$$\begin{aligned}\epsilon(\pi_v, s) &= -\mu_v(\varpi)|\varpi|^{s-1}\epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= -\mu_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{2s-1}\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi, s) &= -\mu_v\chi_v(\varpi)|\varpi|^{s-1}\epsilon(\mu_v\chi_v, s)\epsilon(\mu_v^{-1}\chi_v, s) \\ &= -\mu_v\chi_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{2s-1}\end{aligned}$$

so $a_v(\chi) = sign\left(\frac{-\mu_v\chi_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{2s-1}}{-\mu_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{2s-1}}\right) = \chi_v(\varpi)$

6. χ_v is ramified, $\pi_v = \pi(\mu_v, \mu_v^{-1})$ and μ_v is ramified, and $\chi_v\mu_v$ is ramified. We don't necessarily know what the conductor of $\chi_v\mu_v$ is, let's call it c_v.

$$\begin{aligned}\epsilon(\pi_v, s) &= \epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}\eta_v)^{2s-1}N(\eta_v)^{-1}}{\mu_v\mu_v^{-1}(\mathfrak{d}\eta_v)}\tau(\mu_v)\tau(\mu_v^{-1}) \\ &= N(\mathfrak{d}\eta_v)^{2s-1}\mu_v(-1)\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi_v, s) &= \epsilon(\chi_v\mu_v, s)\epsilon(\chi_v\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}c_v)^{2s-1}N(c_v)^{-1}}{\chi_v^2\mu_v\mu_v^{-1}(\mathfrak{d}c_v)}\tau(\chi_v\mu_v)\tau(\chi_v^{-1}\mu_v^{-1}) \\ &= N(\mathfrak{d}c_v)^{2s-1}\mu_v(-1)\chi_v(-1)\end{aligned}$$

so $a_v = sign\left(\frac{N(\mathfrak{d}c_v)^{2s-1}\mu_v(-1)\chi_v(-1)}{N(\mathfrak{d}\eta_v)^{2s-1}\mu_v(-1)}\right) = \chi_v(-1)$

7. χ_v is ramified, $\pi_v = \pi(\mu_v, \mu_v^{-1})$ and μ_v is ramified, and $\chi_v\mu_v$ is unramified.

$$\begin{aligned}\epsilon(\pi_v, s) &= \epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}\eta_v)^{2s-1}N(\eta_v)^{-1}}{\mu_v\mu_v^{-1}(\mathfrak{d}\eta_v)}\tau(\mu_v)\tau(\mu_v^{-1}) \\ &= N(\mathfrak{d}\eta_v)^{2s-1}\mu_v(-1)\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi_v, s) &= \epsilon(\chi_v\mu_v, s)\epsilon(\chi_v\mu_v^{-1}, s) \\ &= N\mathfrak{d}^{2s-1} \\ &=\end{aligned}$$

so $a_v(\chi) = sign\left(\frac{N\mathfrak{d}^{s-\frac{1}{2}}}{N(\mathfrak{d}\eta_v)^{2s-1}\mu_v(-1)}\right) = \mu_v(-1)$. Now, $\chi_v\mu_v(-1) = 1$, since $\chi_v\mu_v$ is unramified. Therefore, $\mu_v(-1) = \chi_v^{-1}(-1) = \chi_v(-1)$ and $a_v(\chi) = \chi_v(-1)$.

8. χ_v is ramified, $\pi_v = \sigma(\mu_v, \mu_v^{-1})$ and μ_v is unramified.

$$\begin{aligned}\epsilon(\pi_v, s) &= -\mu_v(\varpi)|\varpi|^{s-1}\epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= -\mu_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{2s-1}\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi_v, s) &= \epsilon(\chi_v\mu_v, s)\epsilon(\chi_v\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}\mathfrak{f}_v)^{2s-1}N(\mathfrak{f}_v)^{-1}}{\chi_v^2\mu_v\mu_v^{-1}(\mathfrak{d}\mathfrak{f}_v)}\tau(\chi_v\mu_v)\tau(\chi_v^{-1}\mu_v^{-1}) \\ &= N(\mathfrak{d}\mathfrak{f}_v)^{2s-1}\chi_v(-1)\mu_v(-1)\end{aligned}$$

so $a_v(\chi) = sign\left(\frac{N(\mathfrak{d}\mathfrak{f}_v)^{2s-1}\chi_v(-1)}{-\mu_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{2s-1}}\right) = \frac{\chi_v(-1)}{-\mu_v(\varpi)}$

9. χ_v is ramified, $\pi_v = \sigma(\mu_v, \mu_v^{-1})$ and μ_v is ramified, and $\chi_v\mu_v$ is ramified with conductor c_v.

$$\begin{aligned}\epsilon(\pi_v, s) &= \epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= N(\mathfrak{d}_v\eta_v)^{2s-1}\mu_v(-1) \text{ (as above)}\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi_v, s) &= \epsilon(\chi_v\mu_v, s)\epsilon(\chi_v\mu_v^{-1}, s) \\ &= \frac{N(\mathfrak{d}c_v)^{2s-1}N(c_v)^{-1}}{\chi_v^2\mu_v\mu_v^{-1}(\mathfrak{d}c_v)}\tau(\chi_v\mu_v)\tau(\chi_v^{-1}\mu_v^{-1}) \\ &= N(\mathfrak{d}\mathfrak{c}_v)^{2s-1}\chi_v(-1)\mu_v(-1)\end{aligned}$$

so $a_v(\chi) = sign\left(\frac{N(\mathfrak{d}\mathfrak{c}_v)^{2s-1}\chi_v(-1)\mu_v(-1)}{N(\mathfrak{d}_v\eta_v)^{2s-1}\mu_v(-1)}\right) = \chi_v(-1)$

10. χ_v is ramified, $\pi_v = \sigma(\mu_v, \mu_v^{-1})$ and μ_v is ramified, and $\chi_v\mu_v$ is unramified.

$$\begin{aligned}\epsilon(\pi_v, s) &= \epsilon(\mu_v, s)\epsilon(\mu_v^{-1}, s) \\ &= N(\mathfrak{d}_v\eta_v)^{2s-1}\mu_v(-1) \text{ (as above)}\end{aligned}$$

and

$$\begin{aligned}\epsilon(\pi_v \otimes \chi_v, s) &= \epsilon(\chi_v\mu_v, s)\epsilon(\chi_v\mu_v^{-1}, s) \\ &= -\chi_v\mu_v(\varpi)|\varpi|^{s-1}\epsilon(\chi_v\mu_v, s)\epsilon(\chi_v\mu_v^{-1}, s) \\ &= -\chi_v\mu_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{s-\frac{1}{2}}\end{aligned}$$

so $a_v = sign\left(\frac{-\chi_v\mu_v(\varpi)|\varpi|^{s-1}N\mathfrak{d}^{s-\frac{1}{2}}}{N(\mathfrak{d}_v\eta_v)^{2s-1}\mu_v(-1)}\right) = -\chi_v(\varpi)\mu_v(-\varpi)$. Now, since, $\chi_v\mu_v(-1) = 1$, $a_v(\chi) = -\chi_v(-\varpi)\mu_v(\varpi)$ as well.

	Type of Representation	$a_v(\chi)$	Type of Reduction
1	$\pi_v = \pi_v(\mu_v, \mu_v^{-1})$ μ_v is unramified, χ_v is unramified.	1	Smooth
2	$\pi_v = \pi_v(\mu_v, \mu_v^{-1})$ μ_v is unramified, χ_v is ramified.	$\chi(-1)$	Additive
3	$\pi_v = \pi_v(\mu_v, \mu_v^{-1})$ μ_v is ramified, χ_v is unramified.	1	Additive
4	$\pi_v = \sigma_v(\mu_v, \mu_v^{-1})$ μ_v is ramified, χ_v is unramified.	1	Additive
5	$\pi_v = \sigma_v(\mu_v, \mu_v^{-1})$. μ_v is unramified, χ_v is unramified.	$\chi_v(\varpi)$	Multiplicative
6	$\pi_v = \pi_v(\mu_v, \mu_v^{-1})$ μ_v is ramified, χ_v is ramified, $\mu_v\chi_v$ is ramified.	$\chi_v(-1)$	Additive
7	$\pi_v = \pi_v(\mu_v, \mu_v^{-1})$ μ_v is ramified, χ_v is ramified, $\mu_v\chi_v$ is unramified.	$\chi_v(-1)$	Additive
8	$\pi_v = \sigma_v(\mu_v, \mu_v^{-1})$ μ_v is unramified, χ_v is ramified.	$-\chi_v(-1)\mu_v(\varpi)^{-1}$	Multiplicative
9	$\pi_v = \sigma_v(\mu_v, \mu_v^{-1})$ μ_v is ramified, χ_v is ramified, $\mu_v\chi_v$ is ramified.	$\chi_v(-1)$	Additive
10	$\pi_v = \sigma_v(\mu_v, \mu_v^{-1})$ μ_v is ramified, χ_v is ramified, $\mu_v\chi_v$ is unramified.	$-\chi_v(-\varpi)\mu_v(\varpi)$	Additive

0.4.7 A word about function fields

All of the above work is valid, nearly trivially for the function field case. Of course, when we're working over a global function field, there are no archimedian places so the theorem and furthermore, the functional equation for elliptic curves follows from the Weil Conjectures. We have the following analog of Theorem 92.

Theorem 98. *Let E be an elliptic curve over a function field K such that no local supercuspidal representations occur in the factorization of π_E, then*

$$\lim_{X\to\infty} \frac{\#\{\chi \in C(K) \mid N\chi \leq X \text{ and } rk(E^\chi) \text{ is even}\}}{\#\{\chi \in C(K) \mid N\chi \leq X\}} = \frac{1+(-1)^{rk(E)}\kappa}{2}$$

where $\kappa = \prod \kappa_v$ is a product over the places of K given by

$$\kappa_v = \begin{cases} 2/|c_v| - 1 & E \text{ has split mutiplicative reduction at } v \\ 1 - 2/|c_v| & E \text{ has nonsplit multiplicative reduction at } v \\ 1 - 2/|c_v| & E \text{ has multiplicative reduction in a quadratic extension at } v \\ 1 & E \text{ has potentially multiplicative reduction (non-quadratic)} \\ 1 & \text{otherwise} \end{cases}$$

and $|c_v|$ is the number of degree 2 extensions of K_v.

0.5 Comparison with Algebraic Results

0.5.1 Selmer Groups

On the other side of the Birch and Swinnerton-Dyer Theorem, there has been similar work by Zev Klagsbrun, Barry Mazur and Karl Rubin on the Selmer group of elliptic curves in a family of quadratic twists which we present here with a little bit of background about Selmer groups.

Let E be an elliptic curve over a number field K. Then the Galois group $G_{\bar{K}/K}$ acts on E (recal that E denotes the $\bar{K}$ -points of the elliptic curve) and the action preserves the 2-torsion of E, denoted $E[2]$. Indeed we have an exact sequence of $G_{\bar{K}/K}$-modules:

$$0 \to E[2] \to E \xrightarrow{2} E \to 0$$

Taking the Galois cohomology we form the fundamental short exact sequence:

$$0 \to E(K)/2E(K) \to H^1(K, E[2]) \to H^1(K, E)[2] \to 0$$

Where the notation $H^1(K, X)$ is shorthand for $H^1(G_{\bar{K}/K}, X)$. Next, we do a similar process for local fields. For each place v of K, fix an embedding $\bar{K}_v \subset \bar{K}$ which extends v, and a decomposition group $G_v \subset G_{\bar{K}/K}$. Then we may similarly form the exact sequence:

$$0 \to E(K_v)/2E(K_v) \to H^1(K_v, E[2]) \to H^1(K_v, E)[2] \to 0$$

Where the notation $H^1(K_v, X)$ is shorthand for $H^1(G_v, X)$. Note that the object $H^1(K, E)$ may be identified with the **Weil-Chatelet** group which is the group of homogenous spaces for E up to equivalence, giving it a more geometric meaning.

The natural restriction maps give the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & E(K)/2E(K) & \to & H^1(K, E[2]) & \to & H^1(K, E)[2] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \prod_v E(K_v)/2E(K_v) & \to & \prod_v H^1(K_v, E[2]) & \to & \prod_v H^1(K_v, E)[2] & \to & 0 \end{array}$$

Definition 99. The **2-Selmer group** of E/K is defined by:

$$S^{(2)}(E/K) := \ker \left\{ H^1(K, E[2]) \to \prod_v H^1(K_v, E) \right\}$$

Definition 100. The **Tate-Shafarevich group** of E/K is defined by

$$Ш(E/K) := \ker \left\{ H^1(K_v, E) \to \prod_v H^1(K_v, E) \right\}$$

The Tate-Shafarevich group of an elliptic curve can be understood to be the homogenous spaces for E modulo equivalence, that are everywhere locally trivial (they contain a K_v point). Thus the size of the Tate-Shafarevich group measures the failure of the Hasse "local-global" principal for the elliptic curve.

Theorem 101. *There is an exact sequence*

$$0 \to E(K)/2E(K) \to Sel^{(2)}(E/K) \to Ш(E/K)[2] \to 0$$

The Selmer group is easily shown to be finite and effectively computable. Furthermore, subtracting off the rank of $E(K)[2]$, it is an upper bound for the Mordell-Weil rank of E/K. If $Ш$ is finite, (which it has been conjectured to be and also proved in several cases) then the Selmer group is a good approximation to the Mordell-Weil rank of E/K. The Selmer group is rather easier to work with than the group $E(K)/2E(K)$ and much is known about the Selmer group, as compared to the actual group $E(K)$. For this reason, in an attempt to understand the rank of elliptic curves, mathematicians have turned to Selmer groups.

0.5.2 Selmer Groups in Quadratic Families

In the paper of Klagsbrun, Mazur and Rubin [11], they compute the proportion of elliptic curves in a family of quadratic twists that have odd rank. Recall the following notation

$C(K, X)$ is the group of (global) characters χ of K such that for any prime q which is ramified in χ $Nq < X$ and that E^χ is the elliptic curve "twisted" by χ. Then their results about the Selmer rank is identical to our result about the analytic rank:

Theorem 102. *Suppose E is an elliptic curve defined over a number field K. Then for all sufficiently large X , we have*

$$\frac{|\{\chi \in C(K,X) : \dim_{\mathbb{F}_2} Sel^{(2)}(E^\chi/K) \text{ is odd}\}|}{|C(K,X)|} = (1 - \delta(E/K))/2$$

Where $\delta = \prod \delta_v$ is a product of local factors.

They compute the local factors in several cases, tabulated here:

type of v	δ_v
real	0
complex	1
split multiplicative	$2/c_v - 1$
type I_v or I_v^*,$v > 0$, not split multiplicative	$1 - 2/c_v$
good reduction or type I_0^*,$v \nmid 2$	1
type II,IV,II^*,IV^*,$\Delta \in (K_v^\times)^2, v \nmid 2$	1
type II,IV,II^*,IV^*,$\Delta \notin (K_v^\times)^2, v \nmid 2$	0
type III,$III^{*,}$ $-1 \in (K_v^\times)^2, v \nmid 2$	1
type III,$III^{*,}$ $-1 \notin (K_v^\times)^2, v \nmid 2$	0

Which agree in the cases of overlap with our results.

0.5.3 Parity Conjectures

The analytic results of Theorem 92 and the results of Klagsbrun, Mazur and Rubin in Theorem 102 are separated by the elusive Birch and Swinnerton-Dyer conjecture. However, the equivalence of the two results depends not on the analytic and algebraic ranks but on the parity of the ranks alone. Recent work has been done on the so-called parity conjecture that brings the analytic and algebraic results much closer. Associated to an elliptic curve E/K is a Galois representation which has a so-called "root number" $\omega(E/K)$. Defining the root number does not require a functional equation for the Galois representation but via the local Langlands correspondence and the modularity conjecture, the root number $\omega(E/K)$ is the root number in the functional equation of the Jacquet-Langlands L-function associated to a modular elliptic curve. In fact, the following can be said[5]:

Theorem 103. *(Dokchitser, Dokchitser) Let E/K be an elliptic curve over a number field. For every degree 2 extension F/K,*

$$\dim_{\mathbb{F}_2} Sel^{(2)}(E/F) \equiv \omega(E/F) \ (mod\ 2)$$

In light of this result, our Theorem 92 follows from the earlier algebraic calculations in [11]. The analytic approach, however has some distinct advantages including the fact that it is a more convenient way of controlling the parity of the rank and a more direct approach. The main advantage of the approach using automorphic representations is the possible extension of the computations of the local factors to all cases. In the above, we have handled the reduction types except for the supercuspidal case. However, the supercuspidal calculations are within reach, as a classification of these representations and their epsilon factors have been worked out in [3], Chapter 6. In future work, the author plans to extend the results in this thesis to include elliptic curves which have local supercuspidal representations.

Bibliography

[1] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over q: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14, 2001.

[2] Daniel Bump. *Automorphic Forms and Representations*. Cambridge University Press, Cambridge, UK, 1998.

[3] C. Bushnell and G. Henniart. *The Local Langlands Conjecture for GL(2)*. Springer, Berlin Heidelberg, 2006.

[4] F. Diamond and J. Sherman. *A First Course in Modular Forms*. Springer, USA, 2005.

[5] Tim Dokchitser and Vladimir Dokchitser. Root numbers and the parity of ranks of elliptic curves. *J. Reine Angew. Math.*, 658, 2011.

[6] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular.

[7] Nuno Freitas and Samir Siksek. Modularity and the fermat equation over totally real fields. http://arxiv.org/abs/1307.3162, July 2013.

[8] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number Theory Carbondale 1979*, pages 108–118. Springer Berlin Heidelberg, 1979.

[9] Dorian Goldfeld and Joseph Hundley. *Automorphic Representations and L-functions for the General Linear Grouop*, volume 1. Cambridge University Press.

[10] H. Jacquet and R. Langlands. *Automorphic Forms on GL(2)*, volume 114 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1970.

[11] Zev Klagsbrun, Barry Mazur, and Karl Rubin. Disparity in selmer ranks of quadratic twists of elliptic curves. *Annals of Mathematics*, 178, 2013.

[12] Bao V. Le Hung. Modularity of some elliptic curves over totally real fields.

[13] John T. Tate. Fourier analysis in number fields, and hecke's zeta-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 305–347, Thompson, Washington, D.C, 1967.

[14] Shou-Wu Zhang. Elliptic curves, l-functions, and cm-points.