A study of some Arithmetic Properties of Elliptic Curves

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Poornima B

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2019

Supervisor: Baskar Balasubramanyam

Certificate

This is to certify that this dissertation entitled A study of some Arithmetic Properties of Elliptic Curves towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Poornima B at Indian Institute of Science Education and Research under the supervision of Baskar Balasubramanyam, Associate Professor, Department of Mathematics , during the academic year 2018-2019.

Baskar Balasubramanyam

Committee:

Baskar Balasubramanyam

Vivek Mallick

This thesis is dedicated to everyone who inspired me to do math.

Declaration

I hereby declare that the matter embodied in the report entitled A study of some Arithmetic Properties of Elliptic Curves are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Baskar Balasubramanyam and the same has not been submitted elsewhere for any other degree.

Poornima B

Acknowledgments

I am immensely grateful to Dr. Baskar Balasubramanyam for providing me with many insights and for encouraging and patiently answering all my questions. I want to thank Dr. Vivek Mallick for being a wonderful advisor. I am thankful to the Mathematics department at IISER Pune for providing a very stimulating environment. I would also like to thank my friends Namrata, Sravya, and Narayanan for all the discussions on math and life and my family for the constant love and support.

Abstract

Finding the rank of an elliptic curve is a difficult problem. The Birch and Swinnerton-Dyer Conjecture relates the rank of an elliptic curve to the vanishing of a certain L-function attached to the elliptic curve. This thesis looks at the construction of Heegner points which prove the existence in some cases of points of infinite order. This provides some insight into solving the Birch and Swinnerton-Dyer conjecture. The construction of these points is explained in detail in the second chapter. The classical method of getting Heegner points is limited by assumption on the splitting of certain primes. Considering Shimura curves and imitating the construction leads to new algebraic points. The conjectures in the last two chapters suggest that the theory of Heegner point construction can be extended in various contexts.

Contents

Chapter 1

Introduction

An elliptic curve is a non-singular projective curve together with a group structure defined by regular maps. It can be defined over an algebraically closed field k (for $\text{char}(k) \neq 2, 3$) as the projective plane cubic curve over k of the form

$$y^2z = x^3 + axz^2 + bz^3 \text{ such that } 4a^3 + 27b^2 \neq 0$$

Let F be a number field and $E(F)$ the group of F-rational points on the elliptic curve, points with coordinates in the field F.

Theorem 1.0.1. *(Mordell-Weil) The group $E(F)$ is finitely generated,*

$$E(F) = \mathbb{Z}^r \bigoplus E(F)_{tors}$$

where r is the rank and $E(F)_{tors}$ is the set of torsion points.

Some bounds on the torsion points of elliptic curves are known. Bounding the rank of an elliptic curve is difficult. Any elliptic curve over the rational numbers can be described by the minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the coefficients a_i are integers and the discriminant is minimal. The reduced equation modulo a prime p describes another elliptic curve over $\mathbb{F}_p$ if p does not divide the discriminant. This is to ensure that the reduced curve is also elliptic. Such primes are called primes of good reduction. If the reduced curve has a cusp or a node, then the elliptic curve is said to have additive and multiplicative reduction respectively.

Define a_p to be the number

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

for primes p which do not divide the discriminant. Set $a_p = 0$ for primes of additive reduction and +1 and -1 for split and non-split multiplicative reduction respectively. Split and non-split reduction depends on slopes of the tangent curves. We can define the L-function associated to the elliptic curve $E/\mathbb{Q}$ of conductor N as

$$L(E, s) = \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p/N}(1 - a_p p^{-s})^{-1} = \sum a_n n^{-s}$$

where a_n's are obtained by expanding the product. The L-function converges for $\mathrm{Re}(s) > \frac{3}{2}$. Since the L-function has analytic continuation, we can make sense of it's value at $s = 1$.

Conjecture 1.0.1. *(Birch and Swinnerton-Dyer) The rank r of $E(\mathbb{Q})$ is equal to the order of vanishing of $L(E, s)$ at $s = 1$.*

For an elliptic curve defined over an imaginary quadratic field F, the L-fuction of E over the ring class field K factors as

$$L(E/K, s) = \prod_{\chi} L(E/F, \chi, s) \tag{1.1}$$

where χ ranges over complex characters on $\mathrm{Gal}(K/F) \longrightarrow \mathbb{C}^\times$. Ring class field is an abelian extension and will be defined precisely in the third chapter. It is known that $L(E/F, \chi, s) = L(E/F, \overline{\chi}, s)$. The L-function satisfies a functional equation relating s and $2-s$. $L(E/F, \chi, s) = 0$ for all $\chi \in \mathrm{Gal}(K/F) \longrightarrow \mathbb{C}^\times$ when a certain factor $\mathrm{sign}(E, F) = -1$. This factor does not depend on χ. Putting together the factorization of $L(E/K, s)$ and the vanishing of $L(E/F, \chi, s)$, we get the following inequality

$$\mathrm{ord}_{s=1} L(E/K, s) \geq [K : F].$$

The Birch and Swinnerton-Dyer conjecture leads to the following conclusion

$$\mathrm{rank}(E(K)) \geq [K : F].$$

The above inequality leads to the conjecture that if sign(E, F)=-1, then there is a collection of algebraic points attached to the elliptic curve E with complex multiplication by F. To gain more insight into the Birch and Swinnerton-Dyer conjecture, it might be helpful to examine these algebraic points called the Heegner points.

Chapter 2

Preliminaries

Modular forms form another essential component in the construction of Heegner points. This chapter introduces modular forms and explains the connection with Elliptic curves.

2.0.1 $SL_2(\mathbb{Z})$ and its congruence subgroups

The general linear group $GL_2(R)$ (R is a commutative ring) is the set of matrices with entries in R and whose determinant is invertible in R. The subgroup consisting of matrices of determinant one is denoted by $SL_2(R)$. Let $\tilde{\mathbb{C}} = \mathbb{C} \cup \infty$ be the complex plane with a point at infinity (Riemann sphere). An element of $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ acts on $z \in \mathbb{C}$ by

$$gz = \frac{az+b}{cz+d}$$

This map is called fractional linear transformation, and it defines a group action on $\mathbb{C}$. Identity matrix and negative of identity matrix both define the same action $z \in \mathbb{C}$. Therefore the quotient group $SL_2(\mathbb{R})/\pm I$ acts faithfully on $\mathbb{C}$, i.e., each element other than identity acts nontrivially.

Let $\mathcal{H} = \{z \in \mathbb{C} | \text{Im } z > 0\}$. Any $g \in SL_2(\mathbb{R})$ preserves $\mathcal{H}$ because of the following equality

$$Im(gz) = |cz + d|^{-2} Im(z)$$

The subgroup of $SL_2(\mathbb{R})$ with integer entries is $SL_2(\mathbb{Z})$ denoted by Γ. For a positive integer N define

$$\Gamma(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | a \equiv d \equiv 1 \mathrm{mod}(N), b \equiv c \equiv 0 \mathrm{mod}(N) \}$$

The subgroup $\Gamma(N)$ is a normal subgroup of Γ as it is the kernel of group homomorphism from Γ to $SL_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing entries modulo N. A subgroup of Γ is called congruence subgroup of level N if it contains $\Gamma(N)$. Two points $z_1, z_2 \in \mathbb{H}$ are G-equivalent to each other if $\exists g \in G$ such that $z_2 = gz_1$.

Definition 2.0.1. *A closed, simply connected region F is said to be a fundamental domain for subgroup G of Γ if every $z \in \mathcal{H}$ is G-equivalent to a point in F, but no two points in the interior of F are G-equivalent to each other.*

Proposition 2.0.1. *The fundamental domain for Γ, $F = \{z \in \mathbb{H} | -\frac{1}{2} \leq Re(z) \leq \frac{1}{2}$ and $|z| \geq 1\}$*

Proof. The group Γ is generated by two elements.

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \mapsto z + 1$$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : z \mapsto -1/z$$

Move a point $z \in \mathcal{H}$ inside the strip $-\frac{1}{2} \leq Re(z) \leq \frac{1}{2}$ by using multiple translations. If it does not land inside F then use S to invert the element i.e., to bring it outside unit circle and repeat the same procedure. □

2.1 Modular forms for $SL_2(\mathbb{Z})$

Let $f(z)$ be a meromorphic function in the upper half plane $\mathcal{H}$ satisfying the relation

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

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. In particular for $\gamma = T$ and S defined above, $f(z+1) = f(z)$ and $f(-1/z) = (-z)^k f(z)$. In addition if f is meromorphic at infinity, then $f(z)$ is called a modular function of weight k for $SL_2(\mathbb{Z})$. If $f(z)$ is holomorphic on $\mathcal{H}$ and at ∞, then $f(z)$ is called a modular form of weight k for $SL_2(\mathbb{Z})$. This set is denoted by $M_k(\Gamma)$.

We can map the upper half plane $\mathcal{H}$ to the punctured unit disc by $z \mapsto q = e^{2\pi iz}$ and $\infty \mapsto 0$. Given a function f of period 1, the Fourier series expansion of f is given by

$$f(z) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi iz} = \sum_{n\in\mathbb{Z}} a_n q^n$$

We say f is meromorphic at ∞ if the fourier expansion has atmost finitely many negative terms and f is holomorphic at ∞ if $a_n = 0$ for all negative n. If $a_0 = 0$, then the modular form vanishes at infinity and is called cusp form of weight k for Γ. This set of functions is denoted by $S_k(\Gamma)$.

Remarks 2.1.1. *1. For odd weight, there are no non-zero modular forms.*

2. Zero function is a modular form of every weight.

3. The set of modular forms of a given weight form a complex vector space.

Example 1. *Eisenstein series*

$$G_k(z) = \sum_{m,n} \frac{1}{(mz+n)^k}$$

where the summation is over pairs of integers m, n not both zero. For $k \geq 4$, the double sum is absolutely and uniformly convergent in a compact subset.

Theorem 2.1.1. *The meromorphic function $G_k(z) \in M_k(\Gamma)$*

Proof. $G_k(z+1) = \sum_{m,n} \frac{1}{(mz+m+n)^k} = \sum_{m,n'} \frac{1}{(mz+n')^k} = G_k(z)$

As m, n varies over $\mathbb{Z}^2 - \{(0,0)\}$, m, n' varies over $\mathbb{Z}^2 - \{(0,0)\}$ and the sum is absolutely convergent.

Similarly $G_k(-1/z) = \sum_{m,n} \frac{1}{(-(m/z)+n)^k} = \sum_{m,n} \frac{z^k}{(-m+nz)^k} = z^k G_k(z)$

Holomorphy at ∞ - $G_k(z)$ approaches a finite limit as $z \to i\infty$

$$G_k(z) = \sum_{n \neq 0} \frac{1}{n^k} + \sum_{m \neq 0} \sum_{n} \frac{1}{(mz+n)^k}$$

The second term goes to 0 and the first term is equal to $2\zeta(k)$. □

Example 2. *The discriminant modular form $\Delta(z)$. Let $g_2(z) = 60G_4(z)$ and $g_3(z) = 140G_6(z)$. Define*

$$\Delta(z) = g_3(z)^2 - 27g_3(z)^2 = \frac{(2\pi)^{12}}{1728}(E_4(z)^3 - E_6(z)^2)$$

$\Delta(z)$ is a modular function of weight 12 for Γ. Both $E_4(z)$ and $E_6(z)$ have constant term 1 in their q-expansions. Thus $\Delta(z)$ has constant term 0 and is therefore a cusp form of weight 12.

Proposition 2.1.2. *Let $f(z)$ be a nonzero modular function of weight k for Γ. For $P \in \mathbb{H}$, let $v_P(f)$ denote the order of zero of $f(z)$ at P. Let $v_\infty(f)$ denote the index of first non-vanishing term in the q-expansion of $f(z)$. Then*

$$v_\infty(f) + \tfrac{1}{2}v_i(f) + \tfrac{1}{3}v_\omega(f) + \sum_{P \neq i,\omega} v_P(f) = \tfrac{k}{12}$$

Proof. Counting the zeros and poles by integrating the logarithmic derivative of $f(z)$ along the boundary of fundamental domain F. □

Proposition 2.1.3. *Let k be an even integer, $\Gamma = SL_2(\mathbb{Z})$*

1. *The only modular forms of weight 0 for Γ are constants.*
2. *The space $M_k(\Gamma) = 0$ if k is negative or $k = 2$.*
3. *The space $M_k(\Gamma)$ is one-dimensional generated by E_k if k = 4,6,8,10 or 14; In other words $M_k(\Gamma) = \mathbb{C}E_k$ for the above values of k.*
4. *The space can be decomposed as $M_k(\Gamma) = S_k(\Gamma) \bigoplus \mathbb{C}E_k$ for $k > 2$.*

Proof. For modular forms the terms on left of the equation in the previous proposition are non-negative (by definition of modular form, could be 0's).

1. Let $f \in M_0(\Gamma)$ and let c be any value taken by $f(z)$. Then $f(z) - c$ is also a modular form of weight 0 and it has a zero. One of the terms in left of (4) is strictly positive and the right hand side is 0. Therefore $f(z) - c$ has to be the zero function.

2. The non-negative terms on the left of equation in the previous proposition cannot add to $k/12$ in these cases.

3. Equation in the previous proposition is satisfied if any two non-zero elements $f_1(z)$ and $f_2(z)$ have the same zeros. $f_1(z)/f_2(z)$ is a modular form of weight 0. Therefore by the first part of this proposition, $f_1(z)$ and $f_2(z)$ are proportional. ($f_1(z)/f_2(z)$-c=0 for some $c \in \mathbb{C}$). We can choose $f_2(z)$ to be $E_k(z)$, a modular form of weight k. Thus $M_k(\Gamma) = \mathbb{C}E_k$.

4. Since E_k does not vanish at infinity, given $f \in M_k(\Gamma)$ we can subtract a multiple of E_k such that the difference is in $S_k(\Gamma)$.

□

Proposition 2.1.4. *Any $f \in M_k(\Gamma)$ can be written in the form*

$$f(z) = \sum_{4i+6j=k} c_{i,j} E_4(z)^i E_6(z)^j.$$

Proof. By induction on k. For $k = 4, 6, 8, 10$ and 14 we know that $M_k(\Gamma) = \mathbb{C}E_k$. The modular forms E_4, E_6, E_4^2, E_4E_6 and $E_4^2E_6$ respectively span $M_k(\Gamma)$. For $k > 14$, k can be written in the form $4i + 6j$ for some $i, j \in \mathbb{Z}$ in which case $E_4^i E_6^j \in M_k(\Gamma)$. By the previous proposition, there exists $c \in \mathbb{C}$ such that $f - cE_4^i E_6^j \in S_k(\Gamma)$. Therefore $f = cE_4^i E_6^j + \Delta f_1$, where f_1 is a modular form of weight $k - 12$. By induction f is of the desired form. □

2.1.1 Modular forms for congruence subgroups

Let $f(z)$ be a function on $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ which takes values on $\mathbb{C}$, let $k \in \mathbb{Z}$ and let $\gamma \in \Gamma$. Define

$$f(z)|[\gamma]_k = (cz+d)^{-k} f(\gamma z)$$

for $\gamma \in \Gamma$. This condition is called the weak modularity condition. More generally for $\gamma \in GL_2^+(\mathbb{Q})$ consisting of matrices with positive determinants with entries in $\mathbb{Q}$, define

$$f(z)|[\gamma]_k = (det\gamma)^{k/2}(cz+d)^{-k} f(\gamma z)$$

Any modular function of weight k satisties $f(z)|[\gamma]_k = f(z)$ for all $\gamma \in \Gamma$. With the above notation, the following property is satisfied.

$$f|[\gamma_1\gamma_2]_k = (f|[\gamma_1]_k)|[\gamma_2]_k$$

for any $\gamma_1, \gamma_2 \in GL_2^+(\mathbb{Q})$. This can be proved by expanding on both sides.

Definition 2.1.1. *Let $f(z)$ be a meromorphic function on $\mathbb{H}$, let $\Gamma' \subset \Gamma$ be a congruence subgroup of level N. Let $k \in \mathbb{Z}$. f is a modular function of weight k for Γ' if $f(z)|[\gamma]_k = f$ for all $\gamma \in \Gamma'$ and if for any $\gamma_0 \in \Gamma$,*

$$f(z)|[\gamma_0]_k \text{ has the form } \sum a_n q_N^n \text{ with } a_n = 0 \text{ for } n \ll 0.$$

The above condition implies that the meromorphic function $f(z)$, in addition to satisfying weak modularity condition, also has a q_N-expansion ($q_N = e^{2\pi iz/N}$), where $a_n = 0$ for finitely many negative integers n.

Reason for existence of q_N-expansion - Let $g = f|[\gamma_0]_k$ for fixed $\gamma_0 \in GL_2^+(\mathbb{Q})$. If f is invariant under Γ', i.e., if $f|[\gamma]_k = f$ for all $\gamma \in \Gamma'$, then g is invariant under the group $\gamma_0^{-1}\Gamma'\gamma_0$ because for every $\gamma_0^{-1}\gamma\gamma_0 \in \gamma_0^{-1}\Gamma'\gamma_0$,

$$g|[\gamma_0^{-1}\gamma\gamma_0]_k = (f|[\gamma_0]_k)[\gamma_0^{-1}\gamma\gamma_0]_k = f|[\gamma\gamma_0]_k = f|[\gamma_0]_k = g$$

The group $\gamma_0^{-1}\Gamma'\gamma_0$ is conjugate of Γ' and therefore contains $\Gamma(N)$. Since $T^N \in \Gamma(N)$, $g(z+N) = g(z)$. Therefore $g(z)$ has Fourier series expansion in powers of q_N.

A modular function of weight k is called a modular form of weight k for a given congruence subgroup if it is holomorphic on $\mathbb{H}$ and if $\forall\gamma_0 \in \Gamma$, $a_n = 0$ for all negative n. It is called a cusp-form if in addition $a_0 = 0$.

2.1.2 Hecke operators

Any two subgroups Γ_1 and Γ_2 of a group G are called commensurable if their intersection has finite index in each group. If $\Gamma_1, \Gamma_2 \subset G$ and $\alpha \in G$, then the double coset $\Gamma_1\alpha\Gamma_2$ is the set of all elements of G of the form $\gamma_1\alpha\gamma_2$ with $\gamma_1 \in \Gamma_1$ and $\gamma_2 \in \Gamma_2$. Let $\Gamma' = \Gamma_1 \cap \alpha^{-1}\Gamma_1\alpha$ and $[\Gamma_1 : \Gamma'] = d$. Then $\Gamma_1\alpha\Gamma_1 = \cup_{j=1}^{d}\Gamma_1\alpha\gamma_j$ whenever $\Gamma_1 = \cup_{j=1}^{d}\Gamma'\alpha\gamma_j$.

Definition 2.1.2. *Let Γ' be a congruence subgroup of Γ, and let $\alpha \in GL_2^+(\mathbb{Q})$. Let $\Gamma'' = \Gamma' \cup \alpha^{-1}\Gamma'\alpha$, Let $d = [\Gamma' : \Gamma'']$, $\Gamma' = \cup_{j=1}^{d}\Gamma''\gamma_j'$. Let $f(z)$ be a function on H which is invariant under $[\gamma]_k$ for $\gamma \in \Gamma'$. Then*

$$f(z)|[\Gamma'\alpha\Gamma']_k = \textstyle\sum_{j=1}^{d} f(z)|[\alpha\gamma_j']_k$$

$f(z)|[\Gamma'\alpha\Gamma']_k$ does not depend on the choice of representative modulo the double coset. If $f \in M_k(\Gamma')$ then $f(z)|[\Gamma'\alpha\Gamma']_k \in M_k(\Gamma')$

Definition 2.1.3. *Let n be a positive integer and $f(z) \in M_k(\Gamma')$. Then*

$$T_n f = n^{(k/2)-1} \sum f(z)|[\Gamma'\alpha\Gamma']_k.$$

2.1.3 The Petersson scalar product

Let Γ be a congruence subgroup and $\mathcal{F}$ be a fundamental domain for Γ. For $f, g \in S_k(\Gamma)$ define the Petersson scalar product as

$$(f, g) = \tfrac{1}{[SL_2(\mathbb{Z}):\overline{\Gamma}]} \int\int_{\mathcal{F}} y^k f(z)\overline{g(z)}\tfrac{dxdy}{y^2}$$

This integral is well defined and independent of the choice of fundamental domain. The integral converges because f and g are cusp-forms. The integral converges even if just one of f or g is a cusp-form. It is easily seen that (f, g) is linear in f, is conjugate symmetric ($(f, g) = \overline{(g, f)}$) and $(f, f) > 0$ for any cusp form f. Therefore Petersson product defines a Hermitian inner product on $S_k(\Gamma)$. This makes the space of cusp forms a Hilbert space.

2.1.4 *L*-functions of Modular Forms

We can associate to every newform g of level N an L-function

$$L(g,s) = \sum_{n=1}^{\infty} a_n n^{-s} \tag{2.1}$$

where a_n is the nth Hecke eigenvalue. This L-function has Euler product expansion similar to that of elliptic curves and a functional equation. This similarity between L-functions lead to the Modularity conjecture which was later proved.

Theorem 2.1.5. *Let g be a normalized eigenform whose Fourier coefficients $a_n(g)$ are integers. Then there exists an elliptic curve E_g over $\mathbb{Q}$ such that*

$$L(E_g, s) = L(g, s) \tag{2.2}$$

The proof of this theorem involves constructing an elliptic curve as a quotient of the jacobian of the modular curve $X_0(N)$, where N is the level of the eigenform. This is referred to as the Eichler-Shimura construction. It was conjectured that every elliptic curve can be obtained from a modular form through the Eichler-Shimura construction. This was proved by Andrew Wiles.

Theorem 2.1.6. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Then there exists a newform $g \in S_2(\Gamma_0(N))$ such that*

$$L(g, s) = L(E, s) \tag{2.3}$$

and E is isogenous to the elliptic curve E_g obtained from the Eichler-Shimura construction.

As a corollary of the above theorem, we obtain an explicit complex uniformization

$$\Psi_N : \mathcal{H}/\Gamma_0(N) \longrightarrow E(\mathbb{C}). \tag{2.4}$$

2.2 Eichler Shimura Construction

The quotient $\mathcal{H}/\Gamma_0(N)$ can be given a compact Riemann surface structure. For any such compact Riemann surface X we can fix a base point x_0 and consider all the path integrals to some other point x with respect to a holomorphic differential.

$$x \longrightarrow (\omega \mapsto \int_{x_0}^{x} \omega)$$

This is a map from the Riemann surface to the set of all linear functions of holomorphic differentials on X modulo integration by loops. In particular for an elliptic curve, by uniformization theorem, there is an identification to $\mathbb{C}/\Lambda$ for some lattice Λ. We observe that the set $\{\int_0^{z+\lambda} d\zeta : \lambda \in \Lambda\} = z + \Lambda$ for any $z \in \mathbb{C}$. The integral is dependent on the path. Any two paths differ by a loop. If we mod out all the path integrals by integrals over loops, we get a group isomorphism using the translation invariant property of $d\zeta$.

Definition 2.2.1. *The Jacobian of X is the quotient group*

$$Jac(X) = \Omega^1_{hol}(X)/H_1(X, \mathbb{Z})$$

where $\Omega^1_{hol}(X)$ is the $\mathbb{C}$ vector space of maps from $\Omega^1_{hol}(X)$ to $\mathbb{C}$ and $H_1(X, \mathbb{Z})$ is the group of integer sums of integration over loops also called the first homology group of X.

The degree-0 divisor group of X is

$$\mathrm{Div}^0(X) = \{\textstyle\sum_{x \in X} n_x x : n_x \in \mathbb{Z}, \sum_x n_x = 0\}$$

where only finitely many n_x are non-zero. We can consider all the degree zero divisors modulo principal divisors which measures the extent by which degree 0 divisors fail to be principal. The latter quotient group is denoted by $\mathrm{Pic}^0(X)$. By choosing a base point $x_0 \in X$, we can embed X into $\mathrm{Pic}^0(X)$ by the map $x \mapsto [x - x_0]$, where $[x - x_0]$ denotes the equivalence class of degree 0 divisor $x - x_0$ in the Picard group. We have a well defined map from $\mathrm{Div}^0(X)$ to the Jacobian given by

$$\sum_x n_x x \mapsto \sum_x n_x \int_{x_0}^{x}$$

Theorem 2.2.1. *The above map dscends to divisor classes inducing an isomorphism* $Pic^0(X) \longrightarrow Jac(X)$.

If the genus of the Riemann surface is greater than 0, we have an embedding $X \longrightarrow \mathrm{Jac}(X)$ given by $x \mapsto \int_{x_0}^{x}$.

Let $h : X \longrightarrow Y$ be any holomorphic function between two Riemann surfaces. This map descends to a map between the Jacobians(h_J) and the Picard groups(h_P) of the respective Riemann surfaces such that the following diagram commutes.

$$\begin{array}{ccc} Pic^0(X) & \xrightarrow{h_P} & Pic^0(Y) \\ \downarrow & & \downarrow \\ Jac(X) & \xrightarrow{h_J} & Jac(Y) \end{array}$$

Theorem 2.2.2. *Let* $f \in S_2(\Gamma_1(N))$ *be a normalized eigenform for the Hecke operators* T_p. *Then the eigenvalues* $a_n(f)$ *are algebraic integers.*

The Hecke algebra $T_{\mathbb{Z}}$ over $\mathbb{Z}$ is the algebra of endomorphisms of $S_2(\Gamma_1(N))$ generated over $\mathbb{Z}$ by the Hecke operators.

Let $f \in S_2(\Gamma_1(N))$ be a newform and define the homomorphism $\lambda_f : T_{\mathbb{Z}} \longrightarrow \mathbb{C}$ given by $Tf = \lambda_f(T)f$ for any $T \in T_{\mathbb{Z}}$. Let $\ker\lambda_f = I_f$. The algebra $T_{\mathbb{Z}}$ acts on the Jacobian and preserves $I_f J_0(N)$. We have the following commutative diagram,

$$\begin{array}{ccc} J_0(N) & \xrightarrow{T_P} & J_0(N) \\ \downarrow & & \downarrow \\ A_f & \xrightarrow{a_p(f)} & A_f \end{array}$$

where $A_f = J_0(N)/I_f J_0(N)$ and $J_0(N)$ denotes the Jacobian of $\mathcal{H}/\Gamma_0(N)$.

Theorem 2.2.3. *For a non-singular projective curve* C *with good reduction at prime* p, *a map is induced on degree 0 divisors by reduction and the following diagram commutes:*

$$\begin{array}{ccc} Pic^0(C) & \xrightarrow{h_*} & Pic^0(C') \\ \downarrow & & \downarrow \\ Pic^0(\tilde{C}) & \xrightarrow{\tilde{h_*}} & Pic^0(\tilde{C'}) \end{array}$$

Theorem 2.2.4. *(Modularity theorem) Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then for some newform $f \in S_2(\Gamma_0(N))$ such that $a_p(f) = a_p(E)$ for all primes p.*

Theorem 2.2.5. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N_E. Let N be a positive integer and let*

$$\alpha : X_0(N) \longrightarrow E \tag{2.5}$$

be a non-zero morphism over $\mathbb{Q}$ of curves over $\mathbb{Q}$. Then for some newform $f \in S_2(\Gamma_0(M_f))$ such that M_f/N, we have

$$a_p(f) = a_p(E), \forall p \nmid N_E N$$

Proof. The correspondence between $a_p(f)$ and $a_p(E)$ can be understood by the following series of commutative diagrams. They are slight variants of the commutative diagrams described in this chapter.

$$\begin{array}{ccc} \oplus_{f,n} A'_f & \xrightarrow{a_p(f)} & \oplus_{f,n} A'_f \\ \downarrow & & \downarrow \\ J_0(N) & \xrightarrow{T_P} & J_0(N) \\ \downarrow & & \downarrow \\ Pic^0(X_0(N)) & \xrightarrow{T_p} & Pic^0(X_0(N)) \\ \downarrow & & \downarrow \\ Pic^0(X_0\tilde{(}N)) & \xrightarrow{\sigma} & Pic^0(X_0\tilde{(}N)) \end{array}$$

□

Chapter 3

Complex Multiplication and Heegner points

3.1 Elliptic curves with Complex Multiplication

We know that the endomorphism ring of an elliptic curve contains $\mathbb{Z}$ (Multiplication by m isogeny $\forall m \in \mathbb{Z}$). If the endomorphism ring is strictly greater than $\mathbb{Z}$, say some order in an imaginary quadratic field F, then the elliptic curve is said to have complex multiplication by that order. Order in F is defined as a subring of F which generates F as a $\mathbb{Q}$ vector space and is a finitely generated $\mathbb{Z}$-module. Any order is uniquely determined by it's conductor c, a unique integer such that $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}c\omega$ where $F = \mathbb{Q}(\omega)$.

Example 3. *Consider the elliptic curve $E : y^2 = x^3 + x$. The isogeny $(x, y) \mapsto (-x, iy)$ corresponds to the element $i \in \mathbb{Z}[i]$. E is said to have complex multiplication by $\mathbb{Z}[i]$.*

Let F be an imaginary quadratic field and R_F denote the ring of integers of F which is also the maximal order. Let $\mathcal{EL}(R)$ denote the set of all elliptic curves with endomorphism ring R upto isomorphism. By the uniformization theorem of elliptic curves, this is also equal to set of lattices Λ, with $\mathrm{End}(E_\Lambda) \cong R$ upto homothety of lattices.

Given F, it is easy to construct an elliptic curve with complex multiplication by R_F. Consider any ideal $\dashv$ in F. Any ideal in imaginary quadratic field is a 2 dimensional $\mathbb{Z}$-

module, therefore it can be viewed as a lattice. Hence we have an elliptic curve $E_{\mathfrak{a}}$ whose endomorphism ring is the set $\{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\}$ which is equal to R_F. Homothetic lattices give isomorphic elliptic curves. To get non-isomorphic elliptic curves, consider the set of fractional ideals modulo the principal ideals, which is the ideal class group. Denote the ideal class group by $\mathcal{CL}(R_F)$.

Let $[\mathfrak{a}]$ denote the equivalence class of a fractional ideal $\mathfrak{a}$ in $\mathcal{CL}(R_F)$. E_Λ denotes the elliptic curves in $\mathcal{EL}(R_F)$ associated to the lattice Λ. There is a well defined, simply transitive action of $\mathcal{CL}(R_F)$ on $\mathcal{EL}(R_F)$ given by

$$[\mathfrak{a}] \star E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}.$$

Theorem 3.1.1. *The j-invariants are algebraic numbers i.e., $j(\tau) \in \overline{\mathbb{Q}}$.*

Theorem 3.1.2. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by R_F and let $L = F(j(E), E_{tors})$, the field generated by the j-invariant of the elliptic curve and coordinates of all torsion points of E. Then L is an abelian extension of $F(j(E))$.*

There is a natural action of $\mathrm{Gal}(\overline{F}/F)$ on $\mathcal{EL}(R_F)$ defined by $\sigma \in \mathrm{Gal}(\overline{F}/F)$ sends isomorphism class of E to the isomorphism class of E^σ. But, simply transitive action of $\mathcal{CL}(R_F)$ on $\mathcal{EL}(R_F)$. Therefore there is a unique $[\mathfrak{a}] \in \mathcal{CL}(R_F)$ depending on σ such that $[\mathfrak{a}] \star E = E^\sigma$. This leads to the definition of a map

$$\mathcal{F} : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathcal{CL}(R_F)$$

characterized by $E^\sigma = \mathcal{F}(\sigma) \star E$, $\forall \sigma \in \mathrm{Gal}(\overline{F}/F)$.

This map $\mathcal{F}$ is also a homomorphism. This action of the Galois group commutes with the action of the class group which is captured precisely by the following proposition.

Proposition 3.1.3. *Let $E/\overline{\mathbb{Q}}$ be an elliptic curve representing an element of $\mathcal{EL}(R_F)$, let $\mathfrak{a} \in \mathcal{CL}(R_F)$ and $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then*

$$([\mathfrak{a}] \star E)^\sigma = [\mathfrak{a}]^\sigma \star E^\sigma.$$

3.2 Results from Class Field Theory

Let F be a totally imaginary number field and L be any abelian extension of F. Let R_L and R_F denote their ring of integers respectively. Let $\mathfrak{p}$ be a prime of F which does not ramify in L and β be a prime of L lying over $\mathfrak{p}$. We have a homomorphism from the decomposition group of β to the Galois group of the residue fields R_L/β over $R_F/\mathfrak{p}$. Since $\mathfrak{p}$ is unramified, the kernel of the homomorphism, called the inertia group is trivial. The Galois group of residue fields is generated by the Frobenius automorphism. There is a unique element $\sigma_\mathfrak{p} \in \mathrm{Gal}(L/F)$ which maps to the Frobenius. Let $\mathfrak{c}$ be an integral ideal of F divisible by all primes that ramify in L/F. Define $I(\mathfrak{c})$ to be the group of fractional ideals of K relatively prime to $\mathfrak{c}$.

We know that ring of integers of number fields are Dedekind domains. Therefore for any integral ideal $\mathfrak{a}$ in R_F, we have factorization of $\mathfrak{a}$ as

$$\mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}}.$$

Definition 3.2.1. *For every ideal in $\mathfrak{a} \in I(\mathfrak{c})$, define the Artin map to Gal(L/F) by*

$$(\mathfrak{a}, L/F) = \prod_\mathfrak{p} \sigma_\mathfrak{p}^{n_\mathfrak{p}}$$

.

Proposition 3.2.1. *There exists an integral ideal $c \in R_F$, divisible by only those primes that ramify in L such that all the principal ideals (α) in the kernel of the reciprocity map are such that $\alpha \cong 1(mod(c))$.*

The congruence above is defined multiplicatively, i.e. the prime factorization on both sides are equivalent. The maximal such c is called the conductor of the extension L/F.

Definition 3.2.2. *For an integral ideal c, a ray class field of F modulo c, F_c is an abelian extension such that if the conductor of that extension divides c, then the extension is contained in F_c.*

In other words, it is the largest abelian extension unramified outside the primes dividing the conductor. Class field theory asserts that the Artin map is surjective and guarantees the existence of ray class field. The Artin map induces an isomorphism to the Galois group of Hilbert Class field which is isomorphic to the ideal class group.

3.3 Heegner points

Theorem 3.3.1. *Main theorem of complex multiplication Let* $\mathfrak{t}$ *be an element of upper half plane which is quadratic over* $\mathbb{Q}$*. Then* $j(\mathfrak{t}) \in H$*, where* H *is the ring class field attached to the order* $\mathcal{O} = \mathcal{O}_{\mathfrak{t}}$*. In particular, for all* $\alpha \in Pic(\mathcal{O})$*, and* $\mathfrak{t} \in CM(\mathcal{O})$*,*

$$j(\alpha \star \mathfrak{t}) = rec(\alpha)^{-1} j(\mathfrak{t}).$$

Corresponding to every element in $\mathfrak{t} \in \mathcal{H}$, we have an order in $M_0(N)$, upper triangular modulo N

$$O_{\mathfrak{t}}^{(N)} = \{\gamma \in M_0(N) : \ \det(\gamma) \neq 0 \text{ and } \gamma\mathfrak{t} = \mathfrak{t}\} \cup \{0\}.$$

Theorem 3.3.2. *Let* $\mathfrak{t} \in \mathcal{H} \cap K$*. Let* $O_{\mathfrak{t}}^{(N)}$ *be the associated order and* H/F *be the ring class field attached to* $O_{\mathfrak{t}}^{(N)}$*. Then* $P_{\mathfrak{t}} := \Psi_N(\mathfrak{t}) \in E(H)$*.*

For any order O in F, define

$$\mathrm{CM}(O) = \{\mathfrak{t} \in \mathcal{H}/\Gamma_0(N) : O_{\mathfrak{t}}^{(N)} = O\}.$$

For any order O of discriminant prime to N, $\mathrm{CM}(O)$ is non-empty if and only if all primes dividing N are split in $F/\mathbb{Q}$. If $\mathrm{CM}(O)$ is non-empty then there exists $\mathfrak{t} \in \mathcal{H}/\Gamma_0(N)$ for which $O_{\mathfrak{t}}^{(N)} = O$. $O_{\mathfrak{t}}^{(N)}$ is a subgroup of $M_0(N)$. Therefore we have an embedding of O in $M_0(N)$ and a ring homomorphism $O \longrightarrow \mathbb{Z}/N\mathbb{Z}$.

Theorem 3.3.3. *Shimura Reciprocity If* $\alpha \in Pic(\mathcal{O})$*, and* $\mathfrak{t} \in CM(\mathcal{O})$*,*

$$\Psi_N(\alpha \star \mathfrak{t}) = rec(\alpha)^{-1} \Psi_N(\mathfrak{t}).$$

Shimura reciprocity will be a recurrent theme. It is important because it converts the algebraic action of the Galois group into the analytic action of multiplication of lattices. Lattice multiplication could be easier in many contexts. Especially when we are dealing with rings of integers which are Dedekind domains.

Chapter 4

Shimura Curves and Rigid Analytic parametrization

4.1 Modular forms on quaternion algebras

Definition Let F be a field ($\mathrm{char}(F) = 0$) , a quaternion algebra over F is a 4-dimensional central simple F-algebra $B(a,b) = F \oplus Fi \oplus Fj \oplus Fk$ with the multiplication defined by the relations : $i^2 = a, j^2 = b, ij = k = -ji$ where $a, b \in F^\times$. A quaternion algebra B over F is said to be split if it is isomorphic to $M_2(F)$, the ring of 2×2 matrices with entries in F. For any prime p in ring of integers of F, let F_p denote the completion with respect to the p-adic norm. Let $B_p = B \otimes F_p$, a quaternion algebra over F_p. B is split at p if B_p is a split quaternion algebra. Else B is said to be ramified at p.

The reduced norm map is defined as $x + yi + zj + wk \mapsto x^2 - ay^2 - bz^2 + abw^2$. This map is multiplicative.

Let B be a quaternion algebra over F, R be the ring of integers of F. An Eichler order O in B is the intersection of two maximal R-orders in B. The level m of O is the index of O in any maximal order containing it. A few theorems about the arithmetic of quaternion algebras will be assumed without proof in this section.

Example 4. *Let $B(1,1)$ be the quaternion algebra over $\mathbb{Q}$. We can embed it into $M_2(\mathbb{Q})$ by*

$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *and* $j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $O = M_2(\mathbb{Z})$ *is a maximal order in* $B(1,1)$.

Let B be a quaternion algebra over $\mathbb{Q}$ which splits at ∞. We have an identification $\iota : B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$. For a fixed order R in B, consider the image under this identification of all the invertible elements of reduced norm 1, i.e. $\Gamma = \iota(R_1^{\times})$. This is a subgroup of $SL_2(\mathbb{R})$ and acts properly discontinuously on $\mathcal{H}$ and the quotient is compact.

Definition 4.1.1. *A modular form of weight k on Γ is a holomorphic function f on $\mathcal{H}$ such that*

$$f(\gamma z) = (cz + d)^k f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Definition 4.1.2. *A factorization $N = N_1 N_2$ is called an admissible factorization if N_1 and N^- are coprime and N_2 is squarefree and product of even number of primes.*

To every admissible factorization of N, we can associate a discrete subgroup of $SL_2(\mathbb{R})$ as described below. Consider a quaternion algebra B over $\mathbb{Q}$ which is ramified only at primes dividing N_2. We require N_2 to be squarefree, product of even number of primes for guaranteeing the existence of such a quaternion algebra. Since B is ramified only at primes dividing N_2, it is split at ∞ and at all primes dividing N^+. The set of all elements in $M_2(\mathbb{Z})$ which are upper triangular modulo N_1 for an Eichler order R. With respect to the identification $\iota : B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$, define $\Gamma_{N_1,N_2} := \iota(R_1^{\times})$. Since Γ_{N_1,N_2} acts on $\mathcal{H}$ with compact quotient, there are no cusps. The space of modular forms of weight 2 denoted by $S_2(\Gamma_{N_1,N_2})$ can be identified with the space of holomorphic differential forms. This space is a Hilbert space and is also endowed with action of Hecke operators. Analogous to the classical case, we can define the notion of oldforms in $S_2(\Gamma_{N_1,N_2})$ as the forms arising from $S_2(\Gamma_{d,N_2})$ where d/N_1. The space of newforms is the orthogonal complement.

4.1.1 Shimura curves

The compact Riemann surface $\mathcal{H}/\Gamma_{N_1,N_2}$ can be interpreted as complex points on an algebraic curve over $\mathbb{Q}$ called the Shimura curve associated to the admissible factorization $N = N_1 N_2$.

4.1.2 Eichler Shimura for Shimura curves

Let $g \in S_2(\Gamma_{N_1,N_2})$ be an eigenform having integer Hecke eigenvalues $a_n(g)$.

Theorem 4.1.1. *There exists an elliptic curve E over $\mathbb{Q}$ such that $a_n(g) = a_n(E)$ for all integers $(n, N) = 1$.*

Theorem 4.1.2. *(Shimura-Taniyama-Weil) Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and let $N = N_1N_2$ be any admissible factorization of N. Then there exists a unique eigenform $g \in S_2(\Gamma_{N_1,N_2})$ such that $T_l(g) = a_l(E)g$, for all primes $l \nmid N$*

The above theorem follows from the Shimura Taniyama Weil conjecture in the classical case. Associated to $E/\mathbb{Q}$ with conductor N we have a newform $g \in \Gamma_0(N)$ and by Jacquet-Laglands correspondence we get an eigenform $f \in S_2(\Gamma_{N_1,N_2})$. As a corollary, we get a modular parametrization

$$\Psi_{N_1,N_2} : \mathrm{Div}^0(\mathcal{H}/\Gamma_{N_1,N_2}) \longrightarrow E(\mathbb{C})$$

Definition 4.1.3. *For any $\mathfrak{t} \in \mathcal{H}/\Gamma_{N_1,N_2}$, define the order associated to $\mathfrak{t}$,*

$$O_{\mathfrak{t}} = \{\gamma \in R : norm(\gamma) \neq 0, \iota(\gamma)(\mathfrak{t}) = \mathfrak{t}\} \cup \{0\}.$$

For a fixed order O, define $CM(O) = \{\mathfrak{t} \in \mathcal{H}/\Gamma_{N_1,N_2} : O_{\mathfrak{t}} = O\}$

Theorem 4.1.3. *(Complex Multiplication for Shimura curves) Let O be an order in an imaginary quadratic field F and let H/F be the ring class field associated to O. Then,*

$$\Psi_{N_1,N_2}(Div^0(CM(O))) \subset E(H)$$

4.2 Rigid analytic modular forms

Let $\Gamma \in SL_2(\mathbb{Q}_p)$ be a discrete subgroup such that $\mathcal{H}_p/\Gamma$ is compact.

Definition 4.2.1. *A form of weight k on $\mathcal{H}_p/\Gamma$ is a rigid analytic modular function on $\mathcal{H}_p$ if*

$$f(\gamma z) = (cz+d)^k f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Definition 4.2.2. *A factorization $N = pN^+N^-$ is called a p-admissible factorization if p,N^+ and N^- are pairwise coprime and N^- is squarefree and product of odd number of primes.*

To every p-admissible factorization of N, we can associate a discrete subgroup $\Gamma^p_{N^+,N^-}$ of $SL_2(\mathbb{Q}_p)$ as described below. Consider a quaternion algebra B over $\mathbb{Q}$ which is ramified only at primes dividing N^- and at ∞. The set of all elements in $M_2(\mathbb{Z})$ which are upper triangular modulo N^+ form an Eichler order R. With respect to the identification $\iota : B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p)$, define $\Gamma^p_{N^+,N^-} := \iota(R_1^\times)$. Since $\Gamma^p_{N^+,N^-}$ acts on $\mathcal{H}$ with compact quotient, there are no cusps.

4.2.1 Bruhat-Tits tree

Let p be a rational prime and $|\ |_p$ be the p-adic norm associated to p. $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to the p-adic norm. $\mathbb{Q}_p$ is not algebraically closed. For example 2 is not a square mod 3. Therefore $\sqrt{2}$ does not belong to $\mathbb{Q}_3$. We can consider the algebraic closure of $\mathbb{Q}_p$, but it is not complete.

We can consider the completion and denote it by $\mathbb{C}_p$. $\mathbb{C}_p$ and $\mathbb{C}$ are isomorphic as fields. The p-adic topology makes $\mathbb{C}_p$ a totally disconnected space. We need to define a new topology on $\mathbb{C}_p$ to be able to do analysis and Bruhat-Tits tree is a combinatorial approximation for a subspace defined as follows

Definition 4.2.3. *The p-adic upper half plane $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$.*

The space $\mathbb{P}_1(\mathbb{Q}_p)$ can be thought of as the boundary of the p-adic upper half plane analogous to $\mathbb{R}$ being the boundary of the complex upper half plane.

Two lattices L_1 and L_2 are said to be equivalent if $L_1 = \alpha L_2$ where $\alpha \in \mathbb{C}_p$. Consider the tree in which equivalence class of lattices form the vertices and two lattices L_1 and L_2 are joined by an edge if $pL_1 \subset L_2 \subset L_1$. This is an infinite, unordered tree and each vertex has a valency of $p+1$.

Holomorphic functions are replaced by rigid analytic functions. We have rigid analytic uniformization given by

$$\Phi^{(p)}_{N^+,N^-} : \mathrm{Div}^0(\mathcal{H}_p/\Gamma^{(p)}_{N^+,N^-}) \longrightarrow E(\mathbb{C}_p)$$

where $N = pN_+N_-$ is a p-admissible factorization of N and $\Gamma^{(p)}_{N^+,N_-}$ is as defined in the last section.

Chapter 5

Stark-Heegner points and Rigid Meromorphic Cocycles

5.1 Stark Heegner points

Let $N = pM$ such that $p \nmid M$. Fix an Eichler order $\mathcal{R}$ of level M Let F be a real quadratic field in which prime p remains inert. Fix an embedding of F into $\mathbb{R}$ and $\mathbb{C}_p$. Let $\psi : F \longrightarrow M_2(\mathbb{Q})$ be any algebra embedding and $\overline{\psi} : K \longrightarrow PGL_2(\mathbb{Q})$ be the homomorphism induced by ψ. Let $\Gamma = \overline{\psi}(\mathcal{R}_1^\times)$, where $\mathcal{R}_1^\times$ is the set of invertible elements of reduced norm 1.

For a general $\mathbb{Q}$ algebra embedding ψ, we say that ψ is optimal of conductor c if $O := \psi^{-1}(\mathcal{R})$ is a $\mathbb{Z}[1/p]$ order of conductor c such that $O = \{(u, v) : u \equiv v \bmod(c)\}$. The embedding is said to be oriented if there exists a ring homomorphism $\phi : O \longrightarrow \mathbb{Z}/M\mathbb{Z}$. For any factorization of M into two relatively prime integers, we can define an orientation by sending the tuple (u, v) to entries modulo the factors respectively. This defines a ring homomorphism to $\mathbb{Z}/M\mathbb{Z}$ as the two factors are relatively prime. We can also define an orientation associated to an optimal embedding by sending the upper left hand entry to it's class modulo M. An embedding is said to be oriented if the one arising from the embedding is equal to factorization $M = M \times 1$.

The group $\overline{\psi}(F^\times)$ acts on $\mathcal{H}_p$ with two fixed points z and $\overline{z}$ which are Galois conjugates of each other. Since p is inert, $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{Gal}(F_p/\mathbb{Q}_p)$. The group $\overline{\psi}(F^\times) \cap \Gamma$ is generated

by some element γ.

Define, for a fixed point $x \in \mathbb{P}(\mathbb{Q})$ and for a 2-form on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$

$$I_\psi := \int\!\!\!\!\!\!\times_{\overline{z}}^{z} \int_x^{\gamma x} \omega \in \mathbb{C}_p^\times \tag{5.1}$$

Γ acts on $\mathcal{H}_p$ and on $\mathcal{H}^* = \mathcal{H} \cup \infty$. The action on the product is properly discontinuous. We need to make precise the notion of integration with respect to the two-form on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$.

Definition Let z, $\overline{z} \in \mathcal{H}_p$ and x, $y \in \mathbb{P}(\mathbb{Q})$.

$$\int_{\overline{z}}^{z} \int_x^{\gamma x} \omega = \int_{\mathbb{P}(\mathbb{Q}_p)} \log(\frac{t-z}{t-\overline{z}}) d\mu_f\{x \to y\}(t) \tag{5.2}$$

where $\mu_f\{x \to y\}$ is a measure over $\mathbb{P}(\mathbb{Q}_p)$ and the integration over $\mathbb{P}(\mathbb{Q}_p)$ is as defined in the last chapter. To recall the setting we are in, $E/\mathbb{Q}$, an elliptic curve with conductor N. $\Phi : \mathcal{H}^*/\Gamma_0(N) \longrightarrow E(\mathbb{C})$ is the modular parametrization. We have the pull-back $\Phi^*(\omega_E) = 2\pi i c_\Phi f(z)dz$ where f is the modular form attached to the elliptic curve. Define a complex valued map from edges of the tree $\mathcal{T}$ as

$$k_f\{x \to y\}(e) := 2\pi i c_\Phi \int_x^y f_e(z)dz \tag{5.3}$$

Associated to $k_f\{x \to y\}$ we can define a distribution on $\mathbb{P}(\mathbb{Q}_p)$ as

$$\overline{\mu}\{x \to y\}(U(e)) = k_f\{x \to y\}(e)$$

where $U(e)$ is the open set associated to the edge e.

The double integral satisfies additive property for both the integrals.

Lemma 5.1.1. *I_ψ does not depend on the choice of x. It depends on the Γ-conjugacy class of ψ.*

Any element of the a field is said to be totally positive if for each embedding of the field into $\mathbb{R}$, the element has a positive image. Narrow class group can be defined as the quotient

of group of fractional ideals by the group of principal ideals which are generated by a totally positive element. The fixed field of this group is called the narrow class field.

Conjecture 5.1.1. *The local point*

$$S_\psi^- := \Phi_{Tate}(I_\psi)$$

is a global point in $E(K^+)$ where K is the narrow ring class field.

But these points do not satisfy the Shimura reciprocity law. We can tweak these points a little to obtain a correct generalization.

Define an indefinite multiplicative integral by fixing $x \in \mathbb{P}(\mathbb{Q})$ as follows

$$J_\psi := \int\!\!\!\!\!\!\times_x^z \int_x^{\gamma x} \omega \in K_p^\times / \mathcal{Q} \tag{5.4}$$

We can raise J_ψ to an appropriate power t such that J_ψ^t is a well defined element of $K_p^\times / q^{\mathbb{Z}}$.

Conjecture 5.1.2. *The local point*

$$S_\psi := \Phi_{Tate}(J_\psi^t)$$

is a global point in $E(K^+)$.

These points are the correct generalization as they satisfy a conjectural Shimura reciprocity and certain Galois actions like classical Heegner points.

Lemma 5.1.2. *An embedding ψ of conductor c exists iff there is a homomorphism from O to $\mathbb{Z}/M\mathbb{Z}$.*

For a fixed orientation $\phi : O \longrightarrow \mathbb{Z}/M\mathbb{Z}$, define Σ_O to be the set of all optimal embeddings $\psi : K \longrightarrow M_2(\mathbb{Q})$ of conductor c such that $\phi = \mathcal{O}_\psi$.

Proposition 5.1.3. *The orbits of Σ_O under conjugation by Γ are in natural bijection with $Pic^+(O)$.*

We therefore have an action of $\mathrm{Pic}^+(O)$ on Σ_O/Γ.

Conjecture 5.1.3. *The points $S_\psi \in E(K^+)$ satisfy the following property*

$$S_{c\star\psi} = rec(c)^{-1}(S_\psi)$$

for all $c \in Pic^+(O)$.

5.2 Rigid meromorphic cocycles

The results in this section try to generalize the techniques used previously to find analogues of Stark-Heegner points and the analogue of Shimura reciprocity law that these elements satisfy. The exposition will try to copy the order of results in the previous chapter.

Notation for this chapter -

1. $\mathcal{M}^\times$ - Rigid meromorphic functions on $\mathcal{H}_p$ i.e., ratios of rigid analytic functions whose denominator is non-zero.
2. $\Gamma = SL_2(\mathbb{Z}[1/p])$
3. RM points - Points of degree 2 over $\mathbb{Q}_p$

Definition 5.2.1. *A class in quasi parabolic elements of the first cohomology group $H^1(\Gamma, \mathcal{M}^\times)$ is called a rigid meromorphic cocycle.*

An element of $H^1(\Gamma, \mathcal{M}^\times)$ is parabolic if it's restriction to upper triangular matrices is trivial and is called quasi parabolic if this restriction is a constant in $\mathbb{C}_p^\times$.

Let τ be an RM-point in $\mathcal{H}_p$. Define the order associated to τ by

$$O_\tau := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}[1/p]) : a\tau + b = c\tau^2 + d\tau\}.$$

We can embed O_τ into the real quadratic field $K = \mathbb{Q}(\tau)$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto c\tau + d.$$

The generator of Γ_τ, the stabilizer of τ in Γ is denoted by γ_τ. To evaluate any rigid meromorphic cocycle (an element in $J \in H^1(\Gamma, \mathcal{M}^\times)$), $J(\gamma_\tau) \in \mathcal{M}^\times$ a ratio of meromorphic functions on $\mathcal{H}_p$ which can be evaluated at any RM-point τ. Therefore $J(\gamma_\tau)(\tau) \in \mathbb{C}_p \cup \infty$. τ can be a pole for $J(\gamma_\tau)$. It can be proved that $J(\gamma_\tau)(\tau)$ depends only on the class of J in the first cohomology group and on the Γ orbit of τ.

Let $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and define $j := J(S)$. Since $S^2 = -1$, j satisfies certain additional functional relations. Let $\mathcal{R}^\times$ denote the subset of $\mathcal{M}^\times$ which satisfy these functional relations.

Theorem 5.2.1. *The group $\mathcal{R}^\times$ is of infinite rank. The zeros and poles of any $j \in \mathcal{R}^\times$ are contained in finite union of Γ-orbits of τ.*

Let H_τ be the narrow ring class field associated to O_τ. The Galois group of this field is associated to $\mathrm{Pic}^+(O_\tau)$. Let H_j denote the composite of all H_τ for τ such that $j(\tau) = \infty$.

If J is a rigid meromorphic cocycle and $\tau \in \mathcal{H}_p$ is an RM-point, then the value $J[\tau]$ is algebraic belonging to the composite of fields H_J and H_τ.

Conjecture 5.2.1. *(Shimura reciprocity) Let $h = (h_1, h_2)$ be any element of G_{D_1,D_2}. Then $J_p(\tau_{h_1}, \tau_{h_2})$ belongs to H_{12} and, for all $g = (g_1, g_2) \in G_{D_1,D_2}$*

$$J_p(\tau_{g_1 h_1}, \tau_{g_2 h_2}) = J_p(\tau_{h_1}, \tau_{h_2})^{rec(g)^{-1}} \ (mod\ \epsilon_1^{\mathbb{Z}}).$$

The above conjecture is stated here only for the purpose of comparing it with the earlier We have the following parametrization similar to classical modular parametrization,

$$J_E^+ : \mathcal{H}_p^{\mathrm{RM}}/\Gamma \longrightarrow E(\mathbb{C}_p).$$

Conjecture 5.2.2. *Let E be an elliptic curve of prime conductor p. For an RM-point $\tau \in \mathcal{H}_p$, $J_E^+[\tau] \in E(\mathbb{C}_p)$ belongs to the ring class field of order O_τ.*

This conjecture predicts the existence of global points on E that can't be obtained through the previous methods. Below is a table summarizing the properties of all these points.

Property	**Heegner points**	**Stark-Heegner points**	**Conjectural equivalents**
j-invariant is algebraic	$j(\mathfrak{t})$ is an algebraic integer	-	$J[\mathfrak{t}]$ is algebraic belonging to the composite of fields H_J and $H_{\mathfrak{t}}$
Order associated to the point	$O_{\mathfrak{t}}^{(N)} = \{\gamma : \gamma\mathfrak{t} = \mathfrak{t}\} \cup \{0\}$	$O = \psi^{-1}(R)$	$O_{\mathfrak{t}} := \{\gamma \in M_2(\mathbb{Z}[1/p]) : \gamma\mathfrak{t} = \mathfrak{t}\}$
Existence theorem	$\Psi_N(\tau) \in E(H)$	$\Phi_{\mathrm{Tate}}(J_\psi^t) \in E(H^+)$	$J_E^+[\tau] \in E(H)$
Shimura Reciprocity	$\Psi_N(\alpha \star \mathfrak{t}) = \mathrm{rec}(\alpha)^{-1}\Psi_N(\mathfrak{t})$	$S_{c\star\psi} = \mathrm{rec}(c)^{-1}(S_\psi)$	$J_p(\tau_{g_1h_1}, \tau_{g_2h_2}) = J_p(\tau_{h_1}, \tau_{h_2})^{\mathrm{rec}(g)^{-1}}$

Bibliography

[1] Silverman, J.H., 1986. The arithmetic of elliptic curves (Graduate Texts in Mathematics).

[2] Silvermann, J.H., 1994. Advanced topics in the arithmetic of elliptic curves (Graduate Texts in Mathematics).

[3] Diamond, F., Shurman, J. (2005). A first course in modular forms (Vol. 228, pp. xvi-436). New York: Springer.

[4] Murty, M. R., Dewar, M., Graves, H. (2015). Problems in the theory of modular forms. Hindustan Book Agency.

[5] Darmon, H., Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications. Ann. of Math. (2)154 (2001), no. 3, 589639

[6] Darmon, H., Heegner points, Stark-Heegner points, and values of L-series. International Congress of Mathematicians. Vol. II, 313345, Eur. Math. So c., Zurich, 2006.

[7] Darmon, H. Rational points on modular elliptic curves. CBMS Regional Conference Series in Mathematics, 101. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI,2004.

[8] Shimura, G. (1994). Introduction to the arithmetic theory of automorphic functions (Vol. 1). Princeton university press.

[9] Koblitz, N. I. (2012). Introduction to elliptic curves and modular forms (Vol. 97). Springer Science Business Media.

[10] Bertolini, M., Darmon, H. (2001). The p-adic L-functions of modular elliptic curves. In Mathematics unlimited2001 and beyond (pp. 109-170). Springer, Berlin, Heidelberg.

[11] Darmon, H., Vonk, J. Singular moduli for real quadratic fields: a rigid analytic approach. Submitted, 1(2), 3.

[12] Bertolini, M., Darmon, H. (1996). Heegner points on MumfordTate curves. Inventiones mathematicae, 126(3), 413-456.

[13] Cox, D. A. (2011). Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication (Vol. 34). John Wiley Sons.