UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

El efecto de la torsión en la distribución de Sha de los twists cuadráticos de una curva elíptica.

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Patricia L. Quattrini.

Director de tesis: Dr. Fernando Rodriguez Villegas.

Director Asistente: Dr. Ariel Pacetti.

Consejero de Estudios: Dr. Pablo Solerno.

Buenos Aires, año 2008.

El efecto de la torsión en la distribución de Sha de los twists cuadráticos de una curva elíptica.

Resumen

Sea $E/\mathbb{Q}$ una curva elíptica de conductor primo N. Consideramos la familia $\{E_d\}$ de *twists* cuadráticos imaginarios de E y analizamos la distribución de los valores de $|Ш_d|$ obtenidos dentro de la familia. Los datos obtenidos evidencian que esta distribución es "perturbada" precisamente cuando la curva elíptica E tiene un punto de torsión definido sobre $\mathbb{Q}$.

Sea $f = \sum_{n>0} a_n q^n$ la forma modular de peso 2 y nivel N, asociada a la curva E, y sea

$$e_2(z) = \sum_n b_n q^n$$

la serie Eisenstein de peso 2 y nivel N, normalizada.

Si E tiene un punto de torsión de orden primo ℓ, impar y definido sobre $\mathbb{Q}$, se tiene entonces una congruencia $f \equiv e_2$ módulo ℓ. Mostramos que esta congruencia da origen a una congruencia, módulo ℓ, entre formas modulares de peso 3/2. Esta congruencia en peso 3/2 nos permite relacionar la distribución de números de clases de cuerpos cuadráticos imaginarios $\mathbb{Q}(\sqrt{-d})$, con la distribución de valores de $|Ш_d|$ obtenidos en la familia de twists de E, $\{E_d\}$. Damos una heurística precisa para la densidad de valores de $|Ш|$ que son divisibles por el primo ℓ, basada en una heurística dada por Cohen y Lenstra para números de clases de cuerpos cuadráticos imaginarios.

Luego analizamos el caso de curvas elípticas E de conductor N libre de cuadrados y damos evidencia numérica para este caso.

Palabras clave: Curvas elípticas, distribución de Ш analítico, formas modulares, puntos de torsión, representaciones ℓ-adicas.

The effect of torsion on the distribution of Sha among quadratic twists of an elliptic curve.

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor N. We consider the family $\{E_d\}$ of negative quadratic twists of E and analyze the distribution of $|Ш_d|$-values obtained within the family. The data obtained shows that this distribution isx "disturbed" precisely when the elliptic curve E has a torsion point defined over $\mathbb{Q}$.

Let $f = \sum_{n>0} a_n q^n$ be the weight 2 and level N, modular form associated to E, and

$$e_2(z) = \sum_n b_n q^n$$

be the normalized Eisenstein series of weight 2 and level N.

If E has a torsion point of odd prime order ℓ, defined over $\mathbb{Q}$, then there is a congruence $f \equiv e_2$ modulo ℓ. We show that this congruence gives rise to a congruence, modulo ℓ, among modular forms of weight $3/2$. This congruence in weight $3/2$ permits us to relate the distribution of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$, to the distribution of $|Ш_d|$ values obtained in the family of twists of E, $\{E_d\}$. We give a precise heuristics for the density of those $|Ш|$ values being divisible by the prime ℓ, based on heuristics given by Cohen and Lenstra for class numbers of imaginary quadratic fields.

Next we analyze and give numerical evidence for the case of elliptic curves E of square free conductor N.

Keywords: Elliptic curves, distribution of analytic Ш, modular forms, torsion points, ℓ-adic representations.

Agradecimientos

A Fernando Rodriguez Villegas por su claridad, su incondicional apoyo para cada uno de mis viajes y su gran dedicación durante ellos. A Ariel Pacetti por estar siempre dispuesto a responder mis preguntas, por las largas y numerosas charlas que me permitieron aclarar mis dudas y seguir adelante. A la universidad de Texas por permitirme mantener mi cuenta en la que he corrido muchos programas. A Flavia Bonomo por su ayuda con el Latex y con el C. A Eduardo, que siempre apoyó mis viajes. A los ricos mates de Mariana que tanto me acompañaron mientras escribía esta tesis. A mis compañeras de oficina, Constanza, Flavia y Mariana por la alegría de encontrarlas cada mañana y por el aliento y los abrazos con que recibieron mis múltiples cambios de humor durante todos estos años. A Alejandra, Silvana y Mariela por las palabras justas en el momento indicado. Y a todos los que me olvido, que es sabido, mi memoria siempre fue un desastre!

A mis hijos, Simon y Milan,
por su alegría y por todo lo
que dia a dia, me enseñan.

Introduction

An elliptic curve E is a curve of genus 1 together with a rational point. Elliptic curves have a natural structure of abelian group. Over the rationals this group, which will be denoted by $E(\mathbb{Q})$, is finitely generated by a theorem of Mordell. Thus $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$ where T denotes the *torsion* subgroup of $E(\mathbb{Q})$ (a finite group) and r is the *rank* of the elliptic curve $E/\mathbb{Q}$.

An important invariant associated to an elliptic curve is the *Tate-Shafarevich* group, usually denoted by the russian letter Ш. This group appears naturally when one wants to compute the rank r of an elliptic curve.

The group Ш, which is extremely difficult to calculate, is certain cohomology group that measures the obstruction of *local-global* principle for curves of genus one.

The Birch and Swinnerton-Dyer conjecture relates the order of Ш, as well as other arithmetic information of an elliptic curve, with the central value of its L-series.

The *analytic Sha* is the order of Ш one obtains as from the L-series, assuming the conjecture of Birch and Swinnerton-Dyer.

The investigation of this thesis focuses on the distribution of the values of the analytic Ш in certain families of elliptic curves. For simplicity, assume we have an elliptic curve E given by an equation

$$E : y^2 = x^3 + ax + b.$$

Given a discriminant d of a quadratic field we let the d-quadratic twist of E be the elliptic curve E_d given by the equation $dy^2 = x^3 + ax + b$.

The first part of this work is to consider families of elliptic curves which are quadratic twists of a fixed curve E by negative discriminants and study the numerical distribution of the analytic $Ш_d$ values obtained within the family.

The main observation arising from the numerical evidence is that when the base elliptic curve E has a nontrivial torsion point of some prime order ℓ, defined over $\mathbb{Q}$, then the analytic Ш values divisible by ℓ are more frequent that in the general situation, when l does not divide the order of the torsion group of E.

The fact that something different occurred in the distribution of central values of L-series among quadratic twists of an elliptic curve had already been noted by many authors.

In [6] C. Delaunay gives an heuristics on the probability of Ш being divisible by a prime p in families of quadratic twists of elliptic curves.

Conrey, Keating, Rubinstein and Snaith in [4] use *random matrix theory* to study the distribution of central values of L-series. They observe that when a prime ℓ divides the order of the group of torsion points of an elliptic curve, the statistics they obtain in the family of its negative quadratic twists, deviate form Delaunay's predictions in a way they cannot explain.

In the present work we explain this fact.

In his work [33], J. L. Waldspurger relates the central values of L-series associated to twists of modular forms with the coefficients of the Fourier expansion of certain

modular form g of half-integer weight. The d-coefficient in the Fourier expansion of g is related to the central value $L(E_d, 1)$ of the L-series of the $-d$ quadratic twist of E.

B. Gross in [9] gives an explicit construction of the modular form g involved in Waldspurger's formula, when the conductor N of the elliptic curve E is prime.

This construction, which involves a quaternion algebra B ramified at the prime N and at infinity, is the fundamental basis for the numerical investigation done on the distribution of Sha in the family of negative quadratic twists of an elliptic curve E. Further, it permits us to relate the distribution of Ш values to those of class numbers of imaginary quadratic fields.

This is as follows.

A congruence among modular forms of weight 3/2 occur when the elliptic curve E has nontrivial torsion. This observation made by Gross (see [9]) for the elliptic curve of conductor $N = 11$ is general. For prime level N we have the following result.

Theorem. *Let E be an elliptic curve of prime conductor N. Suppose E has a rational torsion point of prime order $\ell > 2$. Then the proportion of* Ш *values divisible by ℓ in the family of imaginary quadratic twists of E is the same as the proportion of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ divisible by ℓ.*

If we assume the Cohen-Lenstra heuristics on the probability of class numbers being divisible by a prime then this proportion is equal to

$$f(\ell) = 1 - \prod_{i \geq 0} (1 - \frac{1}{\ell^i}) = \frac{1}{\ell} + \frac{1}{\ell^2} - \frac{1}{\ell^3} - \frac{1}{\ell^7} \ldots$$

The congruence among modular forms of weight 3/2 arises form a congruence among modular forms of weight 2. For prime level N we have that if the elliptic curve E has a rational ℓ-torsion point, then the modular form $f = \sum a_n q^n$ associated to the curve E is congruent modulo ℓ to the weight 2 Eisenstein series

$$e_2(z) = \sum \sigma(n)_N q^n$$

where $\sigma(n)_N = \sum_{d|n;(d,N)=1} d.$

This congruence translates into a congruence modulo ℓ between the corresponding eigenvectors of all Brandt matrices in the quaternion algebra ramified at N and infinity. In turn this yields a congruence among the weight 3/2 modular g, related to f, and the Cohen-Eisenstein modular form $\mathcal{H}_{3/2}$ of prime level N, related to e_2. The coefficients of the Cohen-Eisenstein modular form $\mathcal{H}_{3/2}$ are known to be related to class numbers of imaginary quadratic fields.

In [1] Bocherer and Schulze-Pillot generalized Gross' construction for nonprime levels N. In the last part of this work we analyze the situation for square free levels.

In this case, the space of Eisenstein series is no longer one dimensional and this fact makes thing more complicated. In addition, Bocherer and Schulze-Pillot generalization of Gross' method only lead us to a proportion of the negative quadratic twists of the curve E. However, numerical examples calculated show us that the same phenomena occurs on the distribution of Ш.

Outline.

The thesis is organized as follows.

The first four chapters are of background material. We have chosen to develop these topics for the sake of self-containness and because we consider them as relevant results in the foregoing work.

In chapter 1 we introduce, following Serre [27], ℓ-adic representations

$$\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to T_\ell(E)$$

where $T_\ell(E)$ is the Tate module of an elliptic curve E.

We explain, by means of Galois representations, why the presence of a rational ℓ-torsion point on the group of the elliptic curve gives rise to a congruence modulo ℓ among its modular form and certain Eisenstein series.

In chapter 2 we recall the definition of modular forms and work out the analytic continuation and q-expansion for an Eisenstein series of weight 2 for the group $\Gamma_0(N)$.

In chapter 3 we define modular forms of half integer weight and derive the transformation formula for the Theta series, following Shimura [29] and Ogg [21]. The important fact proved in this chapter is that the Θ-series of a quadratic form in n variables is a modular form of weight $n/2$.

In chapter 4, following Pizer [24] we introduce the quaternion algebras and its relation to elliptic curves or, more precisely, to modular forms.

Chapter 5 and 6 are the central part of this work. Here, following [9] we explain how to construct the modular forms of weight 3/2 involved in Waldspurger theorem and show how the congruence obtained among the Eisenstein series of weight 2 and the modular form f corresponding to our elliptic curve E can be lifted, through a certain quaternion algebra, to a congruence modulo the prime ℓ among the modular form g involved in Waldspurger's formula and a certain weight 3/2 Eisenstein series $\mathcal{H}$. The form g is related to the central values of the L-series of the negative quadratic twists of f and the form $\mathcal{H}$ to class numbers of quadratic extensions of $\mathbb{Q}$. This permits us to relate the density of Ш-values if the family of negative quadratic twists of f divisible by the prime ℓ to the density of class numbers of fields $\mathbb{Q}(\sqrt{-d})$ divisible by ℓ.

In chapter 7 we analyze the case of square free levels. Recall in this case the space of Eisenstein series is no longer one dimensional. A numerical analysis of the case $N = pq$, lead us to certain Eisenstein series, depending on N, which we show to be congruent to f modulo ℓ for general square free N. Here f is, as before, the modular form associated to an elliptic curve having an ℓ-torsion point defined over $\mathbb{Q}$. Next we analyze multiplicity one and give some numerical examples.

Table of Contents

Elliptic curves: definition and group law

An elliptic curve E is an algebraic curve of genus one, together with a point defined over the ground field. It can be seen that, taking that selected point to infinity, and by means of projective transformations, every elliptic curve can be taken to an equation in *Weierstrass form*, which in affine coordinates is given by:

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

We say that E is defined over a field K if the numbers $a_i \in K$.

Elliptic curves can be given a group law. Think of a non-singular cubic (remember the additional point at infinity), then a line through two points P and Q defined over K (with possibly $P = Q$), will intersect the curve again in a point defined over K. The group law can be defined as *three points in a line add up to zero*. The zero element for this group law is the point at infinity $\mathcal{O}$. Geometry is especially nice if we take the curve to an equation of the type $y^2 = x^3 + ax + b$, which can be done for every field of characteristic $\neq 2$ or 3. We assume the reader is acquainted with this group law and we will not go into further detail.

One important fact is that, over the rationals, this group is finitely generated.

Theorem 0.0.1. *The group of rational points of an elliptic curve defined over $\mathbb{Q}$ is finitely generated.*

This is *Mordell*'s finite basis theorem, which was generalized by *Weil* to number fields.

Then we can write this group as $T \oplus \mathbb{Z}^r$. T is the group of torsion points of the elliptic curve. This is the *easy* part of the story. The number r is known as the *rank* of the elliptic curve. It is not easy to determine r, even for a particular given curve. Moreover, it is a difficult problem to determine whether r is zero or not in general.

One of the *natural* groups that appears when one wants to determine the rank of an elliptic curve is the group of *Tate-Shafarevich* denoted by the Russian letter Ш.

The *analytic* Ш, defined in the introduction, is the central object we are studying in this work.

CHAPTER 1

Frobenius on the Tate module of E

In this section we derive the congruence

$$a_p \equiv 1 + p \mod \ell \tag{1.1}$$

for any elliptic curve E having an ℓ torsion point defined over $\mathbb{Q}$, and for every prime p of good reduction for E. This will result in a congruence between modular forms, as we will see in the next section.

To derive (1.1), roughly, it goes as follows.

Let ℓ be a prime number and K a field of characteristic $\neq \ell$. The Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on the Tate module $T_\ell(E)$ of an elliptic curve E/K and gives rise to an ℓ-adic representation $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}\, T_\ell(E)$.

In particular, for $K = \mathbb{F}_p$ with $p \neq \ell$ and E_p an elliptic curve over $\mathbb{F}_p$, we have the Frobenius morphism $\mathcal{F}_p \in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ acting on the module $T_\ell(E_p)$. By means of the Weil pairing it can be seen that the determinant of $\mathcal{F}_p$ acting on $T_\ell(E_p)$ is p and its trace is a_p.

Consider now an elliptic curve $E/\mathbb{Q}$, a prime $p \neq \ell$ of good reduction for E and denote E_p the reduced curve modulo p.

We have a representation $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, T_\ell(E)$.

Let $\mathcal{P} \in \overline{\mathbb{Q}}$ be a prime above p. We have the decomposition and inertia groups $D, I \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and $\mathcal{F}_\mathcal{P} \in D/I$ the corresponding Frobenius morphism. If p is a prime of good reduction, then $\rho_\ell(I)$ is trivial and the representation ρ_ℓ factors through D/I. Thus we have a morphism $\rho(\mathcal{F}_\mathcal{P}) \in \mathrm{Aut}\, T_\ell(E)$. Further, the reduction mod $\mathcal{P}$ map gives an isomorphism among $T_\ell(E)$ and $T_\ell(E_p)$, and $\rho(\mathcal{F}_\mathcal{P})$ corresponds to the usual Frobenius $\mathcal{F}_p$ acting on $T_\ell(E_p)$. Then the determinant and trace of $\rho(\mathcal{F}_\mathcal{P})$ are, respectively, p and a_p.

When the elliptic curve E has an ℓ-torsion point defined over $\mathbb{Q}$ then, after fixing a base of $T_\ell(E)$, $\rho(\mathcal{F}_\mathcal{P})$ is given by some matrix

$$\begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix}$$

which gives

$$a_p \equiv 1 + p \mod \ell.$$

This, in detail, is what we are going to describe in this chapter.

The results in this chapter are taken mostly from the following texts: [27], [19], [18], [31].

For further definitions, notation and algebraic background see the appendix.

1.1 Infinite Galois extensions

Let L/K denote an arbitrary algebraic extension of K in $\overline{K}$. We denote $\mathrm{Gal}(L/K)$ the *Galois group* of L over K, that is the group of automorphisms σ of L such that $\sigma|_K = \mathrm{id}$. Recall that the extension L/K is called *Galois* if it is normal and separable. For a subgroup H of $\mathrm{Gal}(L/K)$ we denote $L^H = \{e \in L : \sigma(e) = e \ \forall \sigma \in H\}$.

Let us recall the main theorem for finite Galois extensions.

Theorem 1.1.1. *Let L/K be a finite Galois extension with Galois group G. The set of subfields of L containing K and the set of subgroups of G are in a one-to-one correspondence as follows: to a subgroup H of G it is associated the field $F = L^H$ and to a subfieldF of L it is associated the group $H = \mathrm{Gal}(L/F)$. Then $H = \mathrm{Gal}(L/L^H)$ and $F = L^{\mathrm{Gal}(L/F)}$. The subgroup H is normal in G if and only if F/K is a Galois extension.*

For infinite Galois extensions it is no longer true that for any subgroup H of $\mathrm{Gal}(L/K)$ we have $H = \mathrm{Gal}(L/L^H)$. The application $H \mapsto L^H \mapsto \mathrm{Gal}(L/L^H)$ is not necessarily injective. If a topology is considered on Galois groups, then a correspondence can be defined between subfields of L/K and *closed* subgroups of $\mathrm{Gal}(L/K)$.

Consider the following topology on the automorphism groups:
If L is a field, $\sigma \in \mathrm{Aut}(L)$ and Λ a finite subset of L, define $U(\sigma, \Lambda)$ as the set

$$U(\sigma, \Lambda) = \{\tau \in \mathrm{Aut}(L) : \tau|_\Lambda = \sigma|_\Lambda\}.$$

Take on $\mathrm{Aut}(L)$ the topology generated by the sets $U(\sigma, \Lambda)$, that is, a subset U of $\mathrm{Aut}(L)$ will be open if for any $\sigma \in U$ there is a finite set Λ such that $U(\sigma, \Lambda) \subset U$.

This topology turns $\mathrm{Aut}(L)$ into a Hausdorff topological group.

Note that for a subset H of $\mathrm{Aut}(L)$, its closure is

$$\overline{H} = \{\sigma \in \mathrm{Aut}(L) : \text{ for each finite } \Lambda \subset L, \exists \tau \in H \text{ such that } \tau|_\Lambda = \sigma|_\Lambda\}$$

and if F is a subfieldof L/K then $\mathrm{Aut}_F(L)$ is a closed subgroup of $\mathrm{Aut}(L)$.

Let us remark that any $U(\sigma, \Lambda) = \sigma U(\Lambda)$, where

$$U(\Lambda) = \{\tau \in \mathrm{Aut}(L) : \tau|_\Lambda = id\}$$

is a neighborhood of the identity. Thus we can describe the topology by just giving a base of neighborhoods of the identity and these can also be taken as the subgroups $H \subset \mathrm{Gal}(L/K)$ that fix a finite extension of K or, equivalently, as the subgroups H of finite index in $\mathrm{Gal}(L/K)$.

Let us state some basic facts on topological groups.

Proposition 1.1.2. *Let G be a topological group, H a subgroup. Then*

(1) If H is open, then it is closed.

(2) If H is closed and of finite index, then it is open.

(3) Suppose G is compact. Then H is open $\iff$ H is closed and of finite index.

Now we state the main theorem for infinite Galois extensions:

Theorem 1.1.3. *Let L/K be a Galois extension with Galois group G. The set of subfields of L containing K and the set of closed subgroups of G are in a one-to-one correspondence as follows: to a closed subgroup H of G it is associated the field $F = L^H$ and to a subfield F of L it is associated the group $H = \mathrm{Gal}(L/F)$. Then $H = \mathrm{Gal}(L/L^H)$ and $F = L^{\mathrm{Gal}(L/F)}$. The closed subgroup H is normal in G if and only if F/K is a Galois extension.*

1.1.1 Galois groups as inverse limits.

Let K be a perfect field and $L = \overline{K}$. Let I be the set of all finite Galois extensions of K contained in L. If F_2 and F_1 are extensions of K, $F_2 \supseteq F_1$ we denote $\mathrm{Res}_{F_2F_1}$ the restriction map from $\mathrm{Gal}(F_2/K)$ to $\mathrm{Gal}(F_1/K)$.

Consider the injective morphism:

$$\psi : \mathrm{Gal}(L/K) \to \prod_{F\in I} \mathrm{Gal}(F/K)$$

$$\sigma \mapsto \{\sigma_F\} = \mathrm{Res}_{L,F}(\sigma)_{F\in I}.$$

The image of ψ is the set of all *compatible* elements $\{\sigma_F\}_{F\in I}$, that is, the elements such that for all $F_2, F_1 \in I$

$$\mathrm{Res}_{F_2,F_2\cap F_1}(\sigma_{F_2}) = \mathrm{Res}_{F_1,F_1\cap F_2}(\sigma_{F_1}).$$

Endow each factor $\mathrm{Gal}(F/K)$ with the discrete topology, and the product with the product topology. Then endow $\psi(\mathrm{Gal}(L/K))$ with the induced topology. Considering $\mathrm{Gal}(L/K)$ as a subset of the product of finite Galois extensions, this topology, known as the *krull topology*, is the topology described before.

Formally, we have:

Let $(I, \leq)$ be a partially ordered set. I is called a *directed set* if for any $i, j \in I$ there is a $k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 1.1.4. *Let I be a directed set and $\{G_i\}_{i\in I}$ a set of groups (or ring, or modules, etc). For all $j \geq i$, let $g_{ji} : G_j \to G_i$ be a homomorphism of groups (or rings, or modules, etc). The set $\{G_i\}_{i\in I}$ together with the homomorphisms $\{g_{ji}\}_{j\geq i}$ is called a projective system or an inverse system if $\forall\, j \geq i \geq k$, $g_{jk} = g_{ji} \circ g_{ik}$, and $g_{ii} = id$.*

The set I of all finite Galois extensions of L/K with the order in I given by inclusion is an example of a directed set. The system of Galois groups $\{G_F\}_{F\in I}$ with the restriction homomorphisms $\{\mathrm{Res}_{F_2,F_1}\}_{F_2\geq F_1}$ is a projective system.

Definition 1.1.5. *Let $\{G_i\}_{i\in I}$ be a projective system of groups (or ring, or modules, etc). The projective limit of this system is the subgroup Γ of the product $\prod_{i\in I} G_i$ (or subring, submodule, etc.) of the elements $\gamma=(\gamma_i)_{i\in I}$ such that for all $j\geq i$ $g_{ji}(\gamma_j)=\gamma_i$. This group is denoted by $\varprojlim(G_i)$.*

We can say that the Galois group $\mathrm{Gal}(L/K)$ is isomorphic to the projective limit of the system of finite Galois groups $\{\mathrm{Gal}(F/K)\}_{F\in I}$. A group that is a projective limit of a system of finite groups is called a *profinite group.*

Let us mention without proof the following theorem:

Theorem 1.1.6. *Let G be a topological group. The following are equivalent:*

a) G is the Galois group of some field extension.

b) G is a profinite group.

c) G is compact, Houssdorf and totally disconnected.

The projective limit Γ comes endowed with natural maps $g_i:\Gamma\to G_i$, for all $i\in I$ where g_i is the restriction to Γ of the natural projection map from $\prod G_k$ to G_i.

If H is any group, morphisms from H to Γ are seen to be

$$\mathrm{Hom}(H,\varprojlim(G_i))\cong\varprojlim(\mathrm{Hom}(H,G_i)).$$

For $\{H_i\}_{i\in I}$ and $\{G_i\}_{i\in I}$ two projective systems indexed by the same set I, and $\{h_{ji}\}_{j\geq i}$, $\{g_{ji}\}_{j\geq i}$ the corresponding group homomorphisms, a *morphisms of projective systems* is defined as a set $\{f_i\}_{i\in I}$ of morphisms $f_i:H_i\to G_i$ such that $g_{ji}\circ f_j=f_i\circ h_{ji}$. A morphism of projective systems defines a group homomorphism $f:\varprojlim(H_i)\to\varprojlim(G_i)$.

1.1.2 $\hat{\mathbb{Z}}$: The profinite completion of $\mathbb{Z}$.

Let I be the set of natural numbers $\mathbb{N}$ with the partial ordering $\leq$ given by $i\leq j$ if and only if $i\mid j$. For each $n\in\mathbb{N}$ denote H_n the ring $\mathbb{Z}/n\mathbb{Z}$. If $n\mid m$ denote h_{mn} the natural quotient map $h_{mn}:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$. The rings $\{H_n\}_{n\in\mathbb{N}}$ with the maps $\{h_{mn}\}$ define a projective system of rings. The projective limit of the system $\{\mathbb{Z}/n\mathbb{Z}\}$ is a ring called the *profinite completion* of $\mathbb{Z}$ and it is denoted $\hat{\mathbb{Z}}$.

The system of compatible maps $\{\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\}_{n\in\mathbb{N}}$ defines an embedding of $\mathbb{Z}$ into $\hat{\mathbb{Z}}$. Identifying $\mathbb{Z}$ with its image in $\hat{\mathbb{Z}}$, $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$ with the krull topology.

If $\{G_i\}_{i\in I}$ is a projective system and J is a subset of I such that the partial ordering on I induces a structure of a directed set on J, the projective system $\{G_j\}_{j\in J}$ may also be considered. Denote by Γ_I and Γ_J the projective limits of these two systems. The projection map $\prod_I G_i\to\prod_J G_j$ induces a group homomorphism of $\Gamma_I\to\Gamma_J$.

For example, let $\hat{\mathbb{Z}}$ be the profinite completion of Z as before, and consider for a prime ℓ the set $J=\{\ell^m\}_{m\in\mathbb{N}}\subset I=\mathbb{N}$. The ring Γ_I is $\hat{\mathbb{Z}}$, and the ring Γ_J is the ring of *ℓ-adic integers* $\mathbb{Z}_\ell$. Thus $\mathbb{Z}_\ell=\varprojlim\mathbb{Z}/\ell^n\mathbb{Z}$. Note that the krull topology coincides with the usual ℓ-adic topology, and that $\mathbb{Q}_\ell=\mathbb{Z}_\ell[\frac{1}{\ell}]$.

1.1.3 The Tate module and ℓ-adic representations.

Let us consider now an elliptic curve E/K, and let $m \geq 2$ be an integer prime to $\mathrm{char}(K)$ if $\mathrm{char}(K) \neq 0$. Recall that $E[m]$ denotes the kernel of the multiplication by m map in $E(\overline{K})$, and that

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

Each element σ of the Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$ in the usual way: $P = (x, y) \mapsto P^\sigma = (\sigma(x), \sigma(y))$, thus we have a representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$$

where the last isomorphism involves choosing a basis for $E[m]$.

By this we mean just a morphism from $\mathrm{Gal}(\overline{K}/K)$ to $\mathrm{Aut}(E[m])$. Note that this morphism is a *continuous* one: consider on the finite set $\mathrm{Aut}(E[m])$ the discrete topology. As this is a morphism among topological groups, it is enough to see that the inverse image of any one point, for example, the identity, is an open set in $\mathrm{Gal}(\overline{K}/K)$. But this amounts saying that the kernel of the map is a set of finite index, which is an obvious task, as the image is finite. Let H denote the kernel of this representation. By the Galois theorem for infinite Galois extensions, the subgroup H corresponds to a finite extension of K which will be denoted by $K(E[m])$ and it is easy to see that $K(E[m])$ is the extension of K generated by the coordinates of the points in $E[m]$. On taking the quotient $\mathrm{Gal}(\overline{K}/K)$ by H we obtain an injective representation

$$\rho : \mathrm{Gal}(K(E[m])) \to GL_2(\mathbb{Z}/m\mathbb{Z})$$

1.1.4 Example.

Let E be the elliptic curve $y^2 = x^3 - 2x$. Then $E[2] = \{(0,0), (\sqrt{2}, 0), (-\sqrt{2}, 0), \mathcal{O}\}$ and $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{2})$. Fix for a base of $E[2]$ the points $\{(0,0), (\sqrt{2}, 0)\}$. Note that on E the points $(0,0)$ and $(\sqrt{2}, 0)$ add to $(-\sqrt{2}, 0)$. Thus, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, $\rho(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ if $\sigma(\sqrt{2}) = \sqrt{2}$ and $\rho(\sigma) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ if $\sigma(\sqrt{2}) = -\sqrt{2}$. This defines the injective representation $\rho : \mathrm{Gal}(\mathbb{Q}(E[2])) \to GL_2(\mathbb{Z}/2\mathbb{Z})$ or the representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/2\mathbb{Z})$ that depends only on how σ acts on $\sqrt{2}$.

It is more convenient to deal with rings of characteristic 0 so these representations will be somehow fit together.

As before, let E be an elliptic curve over a field K and ℓ a prime distinct from $\mathrm{char}(K)$.

Definition 1.1.7. *The ℓ-adic Tate module of E is the group*

$$T_\ell(E) = \varprojlim E[\ell^n]$$

the projective limit being taken with respect to the natural maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$$

Since each $E[\ell^n]$ has a natural structure of $\mathbb{Z}/\ell^n\mathbb{Z}$-module, the Tate module $T_\ell(E)$ gains a natural structure as a $\mathbb{Z}_\ell$ module, with the product given coordinate by coordinate.

Note that by the krull topology on $T_\ell(E)$, a point $\mathbb{P} \in T_\ell(E)$ is "near" zero, if and only if $P_n = \pi_n(\mathbb{P}) \in E[\ell^n]$ is equal to $\mathcal{O}$ for a big value of n. This means that $P_k = \pi_k(\mathbb{P}) \in E[\ell^k]$ equals $\mathcal{O}$ for any $k \leq n$ and, as the multiplication by ℓ-maps are surjective, that we can write $\mathbb{P} = \ell^n\mathbb{S}$ with $\mathbb{S} \in T_\ell(E)$. Thus, the neighborhoods of the identity are the sets $\ell^n\, T_\ell(E)$. Further, this shows that this topology is the same as the topology inherited on $T_\ell(E)$ by being a $\mathbb{Z}_\ell$-module in which two points $\mathbb{P}$ and $\mathbb{S}$ are near if their difference is divisible by a large power of ℓ.

The following proposition is a direct consequence of proposition 1.15 and the definition of inverse limits.

Proposition 1.1.8. *As a $\mathbb{Z}_\ell$-module, the Tate module has the following structure*
a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *if* $\ell \neq \mathrm{char}(K)$
b) $T_p(E) \cong \{0\}$ *or* $\mathbb{Z}_p$ *if* $p = \mathrm{char}(K) > 0$

The action of $\mathrm{Gal}(\overline{K}/K)$ on each $E[\ell^m]$ commutes with the multiplication by ℓ-map used to form the inverse limit, so $\mathrm{Gal}(\overline{K}/K)$ also acts on $T_\ell(E)$. Since the pro-finite group $G_{\overline{K}/K}$ acts continuously on each finite discrete group $E[\ell^m]$ the resulting action on $T_\ell(E)$ is also continuous.

Definition 1.1.9. *The ℓ-adic representation of* $\mathrm{Gal}(\overline{K}/K)$ *on E, denoted by ρ_ℓ, is the map*

$$\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E))$$

giving the action of $\mathrm{Gal}(\overline{K}/K)$ *on $T_\ell(E)$ as described above.*

If we choose a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$ we obtain a representation

$$\mathrm{Gal}(\overline{K}/K) \to GL_2(\mathbb{Z}_\ell)$$

and by the natural inclusion $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ we have a 2-dimensional representation

$$\mathrm{Gal}(\overline{K}/K) \to GL_2(\mathbb{Q}_\ell)$$

over a field of characteristic 0.

In general, let K be any field, which we assume to be perfect for simplicity, G the Galois group of $\overline{K}/K$ and $\mathbb{V}$ a finite n-dimensional vector space over $\mathbb{Q}_\ell$. The group $\mathrm{Aut}(\mathbb{V})$ is isomorphic to $GL_n(\mathbb{Q}_\ell)$. We have the following

Definition 1.1.10. *An ℓ-adic representation of G or, by abuse of language, of K is a continuous homomorphism $\rho : G \to \mathrm{Aut}(\mathbb{V})$.*

1.1.5 The Tate module of a field K.

Let K be a field and, as usual, $\mathrm{char}(K) \neq \ell$. Let $\mu_{\ell^n} \subset \overline{K}^*$ be the group of ℓ^n-roots of unity. Raising to the ℓ-power give morphisms $\mu_{\ell^{n+1}} \xrightarrow{(\ )^\ell} \mu_{\ell^n}$ and we can take the inverse limit to form the *Tate module of* K

$$T_\ell(\mu) = \varprojlim \mu_{\ell^n}$$

As an abstract group $T_\ell(\mu) \cong \mathbb{Z}_\ell$.

Further, the group $\mathrm{Gal}(\overline{K}/K)$ acts on each μ_{ℓ^n}, so we have a one-dimensional representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(\mu)) \cong \mathbb{Z}_\ell^*.$$

The $\mathbb{Q}_\ell$ vector space $V_\ell(\mu) = T_\ell(\mu) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is one dimensional, and the homomorphism $\chi_\ell : G \to \mathrm{Aut}(V_\ell) = \mathbb{Q}_\ell^*$ defined by the action of G on V_ℓ is a 1-dimensional ℓ-adic representation of G. The character χ_ℓ takes its values in the group of units of $\mathbb{Z}_\ell$.

We will later relate this character to the representation ρ_ℓ defined before.

1.1.6 The Tate module and Isogenies.

Let $\phi : E_1 \to E_2$ be an isogeny. Then ϕ gives a map $\phi : E_1[\ell^n] \to E_2[\ell^n]$ and so it induces a $\mathbb{Z}_\ell$-linear map $\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$. Thus we have a homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1)), T_\ell((E_2)).$$

We will need the following result:

Proposition 1.1.11. *Let E_1, E_2 be elliptic curves. The map*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

$$\phi \mapsto \phi_\ell$$

is injective.

Choosing $\mathbb{Z}_\ell$ basis for $T_\ell(E_1)$ and $T_\ell(E_2)$ we have

$$\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) \cong M_2(\mathbb{Z}_\ell).$$

An isogeny is said to be defined over K if it commutes with the action of $\mathrm{Gal}(\overline{K}/K)$. Similarly, we define $\mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$ to be the group of $\mathbb{Z}_\ell$-linear maps from $T_\ell(E_1)$ to $T_\ell(E_2)$ which commute with the action of $\mathrm{Gal}(\overline{K}/K)$ as given by the ℓ-adic representation.

Theorem 1.1.12. *The natural map*

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$$

is an isomorphism if K is a finite field or K is a number field.

1.2 The Weil pairing.

Let E/K be an elliptic curve. Fix an integer $m \geq 2$ prime to $\mathrm{char}(K)$ if this is not zero. Let us recall that $\sum n_P P$ is the divisor of a function if and only if $\sum n_P = 0$ and $\sum [n_P]P = \mathcal{O}$ in E.

For any $T \in E[m]$, there is a function $f \in \overline{K}(E)$ such that $\mathrm{div}(f) = mT - m\mathcal{O}$. Let $T' \in E$ such that $[m]T' = T$, then there is a function $g \in \overline{K}(E)$ such that

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(\mathcal{O}) = \sum_{R \in E[m]} ((T' + R) - R)$$

note that $\#E[m] = m^2$ and $[m^2]T' = \mathcal{O}$.

As the functions $f \circ [m]$ and g^m have the same divisor, we may assume (multiplying f by an element of $\overline{K}^*$ if necessary), that $f \circ [m] = g^m$.

Let S be another m-torsion point. For any point $X \in E$,

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

We can define a *pairing* $e_m : E[m] \times E[m] \to \mu_m$ by setting $e_m(S, T) = g(X + S)/g(X)$, where X is any point such that both $g(X + S), g(X)$ are defined and non-zero.

This pairing is known as the *Weil e_m- pairing*. We state its basic properties:

Proposition 1.2.1. *The Weil e_m- pairing is*

a) bilinear: $e_m(S_1+S_2, T) = e_m(S_1, T)e_m(S_2, T)$, and $e_m(S, T_1+T_2) = e_m(S, T_1)e_m(S, T_2)$.
b) alternating: $e_m(T, T) = 1$, so in particular $e_m(S, T) = e_m(T, S)^{-1}$.
c) non-degenerate: If $e_m(S, T) = 1$ for all $S \in E[m]$, then $T = O$.
d) Galois invariant: For all $\sigma \in G_{\bar{K}/K}$, $e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma)$.
e) compatible: If $S \in E[mm']$ and $T \in E[m]$, then $e_{mm'}(S, T) = e_m([m']S, T)$.

Corollary 1.2.2. *The e_m pairing is surjective: there exists points $S, T \in E[m]$ such that $e_m(S, T)$ is a primitive m-th root of unity. In particular, if $E[m] \subset E(K)$, then $\mu_m \subset K^*$.*

Recall that if $\phi : E_1 \to E_2$ is an isogeny, then we have its dual isogeny $\hat{\phi} : E_2 \to E_1$.

Proposition 1.2.3. *Let $S \in E_1[m], T \in E_2[m]$ and $\phi : E_1 \to E_2$ an isogeny. Then*

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

Let ℓ be a prime number different from $\mathrm{char}(K)$. We would like to fit together the pairings

$$e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$$

for all $n = 1, 2, 3...$ to give an *ℓ-adic Weil pairing* on the Tate module

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu).$$

To show that the e_{ℓ^n}-pairings are compatible with taking the inverse limit, we must show that, for any $S, T \in E[\ell^{n+1}]$

$$e_{\ell^{n+1}}(S,T)^\ell = e_{\ell^n}([\ell]S, [\ell]T).$$

By linearity we have $e_{\ell^{n+1}}(S,T)^\ell = e_{\ell^{n+1}}(S, [\ell]T)$ and applying proposition (1.2.1) e) with $m = \ell^n$ and $m' = \ell$ we get the desired property. Then e is well defined and it inherits the properties stated in (1.2.1) and (1.2.3). Thus we have the following

Proposition 1.2.4. *There exists a bilinear, alternating, non-degenerate, Galois invariant pairing*

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu).$$

Further, if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and its dual isogeny $\hat{\phi}$ are adjoints for the pairing.

1.3 The Trace and Determinant of Frobenius on $T_\ell(E)$.

Let E be an elliptic curve, ℓ a prime different from $\mathrm{char}(K)$. Recall that we have a representation

$$\mathrm{End}(E) \to \mathrm{End}(T_\ell(E))$$

$$\phi \mapsto \phi_\ell.$$

If we choose a $\mathbb{Z}_\ell$ basis for $T_\ell(E)$, we can write ϕ_ℓ as a 2×2 matrix and, in particular, we can compute $\det \phi_\ell$ and $\mathrm{Tr}\, \phi_\ell$ which are in $\mathbb{Z}_\ell$. Of course, they do not depend on the choice of the basis.

Proposition 1.3.1. *Let $\phi \in \mathrm{End}(E)$. Then*

a) $\det \phi_\ell = \deg \phi$.
b) $\mathrm{Tr}\, \phi_\ell = 1 + \deg \phi - \deg(1 - \phi)$.
In particular, $\det \phi_\ell, \mathrm{Tr}\, \phi_\ell$ *are in* $\mathbb{Z}$ *and are independent of* ℓ.

Proof:

Let v_1, v_2 be a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$ and write the matrix for ϕ_ℓ in this basis:

$$\phi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

For the Weil pairing $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$, let us compute:
$e(v_1, v_2)^{\deg \phi} = e([\deg \phi]v_1, v_2) = e(\hat{\phi}_\ell \phi_\ell v_1, v_2) = e(\phi_\ell v_1, \phi_\ell v_2)$
$= e(av_1 + cv_2, bv_1 + dv_2) = e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det \phi_\ell}$
As e is non-degenerate, we conclude that $\deg \phi = \det \phi_\ell$.
Finally, for any 2×2 matrix A, $\mathrm{Tr}(A) = 1 + \det(A) - \det(I - A)$.

□

We will now consider $\phi = \mathcal{F}_p$, the Frobenius morphism, in what was said beforehand.

Let p be a prime number and $\mathbb{F}_p$ the field of p elements. Choose a Weierstrass equation for the elliptic curve E_p, with coefficients in $\mathbb{F}_p$. Denote by

$$\begin{aligned} \mathcal{F}_p : E_p &\longrightarrow E_p \\ (x, y) &\mapsto (x^p, y^p) \end{aligned}$$

the p-th power Frobenius morphism.

The Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is generated by the Frobenius map on $\overline{\mathbb{F}}_p$ and we have seen that $\#E_p(\mathbb{F}_p) = \deg(1 - \mathcal{F}_p)$ (see (A.8.2)).

For $\ell \neq p$, let us denote by $\mathcal{F}_{p,\ell}$ the morphism induced by the Frobenius map $\mathcal{F}_p$ on the Tate module of E_p, $T_\ell(E_p)$. Then by proposition (1.3.1) and (A.8.2) we have,

a) $\det \mathcal{F}_{p,\ell} = p$

b) $\#\mathcal{E}(\mathbb{F}_p) = 1 + p - \mathrm{Tr}(\mathcal{F}_{p,\ell})$

or, otherwise stated

$$\det \mathcal{F}_{p,\ell} = p \quad \text{and} \quad a_p = \mathrm{Tr}\, \mathcal{F}_{p,\ell}$$

where, as usual, a_p is defined by $\#E_p(\mathbb{F}_p) = p + 1 - a_p$.

1.4 Elliptic curves: good and bad reduction.

Consider an elliptic curve $E/\mathbb{Q}$ given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

Let p be a prime number and v the p-adic valuation.

Suppose the coefficients a_i are not p-integral. The transformation $(x, y) \mapsto (u^{-2}x, u^{-3})$ makes each a_i to become $u^i a_i$. Thus choosing an appropriate u we may suppose the coefficients of our Weierstrass equation are p-integral. The discriminant Δ, which is a polynomial in the a_i's, will then satisfy $v(\Delta) \geq 0$.

Recall that any transformation on (x, y) that preserves the Weierstrass equation, makes Δ to become $u^{12}\Delta$. Then we can look for an equation with $v(\Delta)$ as small as possible (and $v(\Delta) \geq 0$).

Definition 1.4.1. *Let E be an elliptic curve with Weierstrass equation* (1.2)*. Then the equation is said to be minimal at v if $v(\Delta)$ is minimized subject to the condition a_i is p-integral for every i.*

Having chosen a minimal equation for E at v, we can reduce its coefficients modulo p to obtain a, possibly singular, elliptic curve $\widetilde{E}_p$ over $\mathbb{F}_p$. Suppose P is a point in $E(\mathbb{Q})$. We can choose integer projective coordinates $[x : y : z]$ for P such that at least one coordinate is non-zero modulo p. The reduced point $\widetilde{P} = [\tilde{x} : \tilde{y} : \tilde{z}]$ lies in $\widetilde{E}_p(\mathbb{F}_p)$.

This defines the *reduction map* $E(\mathbb{Q}) \to \widetilde{E}_p(\mathbb{F}_p)$. If $\widetilde{E}_p$ is nonsingular, then this map is a group homomorphism.

A prime p is a prime of *good reduction* if the reduced curve $\widetilde{E}_p$ is non-singular, that is, it is an elliptic curve.

If the curve $\widetilde{E}_p$ is singular, p is said to be a prime of *bad reduction*. In this case the reduced curve has one singular point S and is either a *node* or a *cusp*. The set of non-singular points in $\widetilde{E}_p$, which is $\widetilde{E}_p(\mathbb{F}_p) - \{S\}$, still form a group. It can be seen that this group is isomorphic to:

- $\mathbb{F}_p^+$ which has order p; when $\widetilde{E}_p$ has a cusp. In this case we say that E has *additive reduction* at p.
- $\mathbb{F}_p^\times$, which has order $p-1$; when $\widetilde{E}_p$ has a split node. We say that E has *split multiplicative* reduction at p.
- A subgroup of order $p+1$ of the multiplicative structure of a quadratic extension of $\mathbb{F}_p$; when $\widetilde{E}_p$ has a non-split node. We say that E has *non-split multiplicative* reduction at p.

Thus, if we keep our definition $a_p = p + 1 - N_p$,where N_p is the number of points of $\widetilde{E}_p(\mathbb{F}_p)$ (singular or not) then

$$a_p = \begin{cases} 1 & \text{if } \widetilde{E}_p \text{ has a split node} \\ -1 & \text{if } \widetilde{E}_p \text{ has a non-split node} \\ 0 & \text{if } \widetilde{E}_p \text{ has a cusp} \end{cases}$$

1.5 The action of Galois on the Tate module of E.

Let K be a number field, that is, a finite extension of $\mathbb{Q}$, and let $K/\mathbb{Q}$ be Galois. Denote Σ_K the set of all prime ideals in the ring $\mathcal{O}_K$ of integers of K, or, alternatively, the set of all normalized discrete valuations of K. Let $\mathcal{P} \in \Sigma_K$ and $(p) = \mathcal{P} \cap \mathbb{Q}$ the restriction of $\mathcal{P}$ to $\mathbb{Q}$. Denote by $k_\mathcal{P}$ the residue field $\mathcal{O}_K/\mathcal{P}$ and $\mathbb{F}_p = \mathbb{Z}/(p)$. The residue field $k_\mathcal{P}$ of a prime ideal $\mathcal{P} \in \Sigma_K$ is a finite field with $N(\mathcal{P}) = p^{\deg(\mathcal{P})}$ elements, where $p = \mathrm{char}(k_\mathcal{P})$ and $\deg(\mathcal{P})$ is the degree of $k_\mathcal{P}$ over the finite field $\mathbb{F}_p$. The ramification index $e_\mathcal{P}$ of $\mathcal{P}$ is the ramification index of p, that is the valuation $v_\mathcal{P}(p)$.

Let G denote the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. For any prime ideal $\mathcal{P}$ of $\mathcal{O}_K$, that is $\mathcal{P} \in \Sigma_K$, the *Decomposition group of* $\mathcal{P}$, is the subgroup of G defined by

$$D_\mathcal{P} = \{\sigma \in G : \sigma\mathcal{P} = \mathcal{P}\}.$$

Any $\sigma \in D_\mathcal{P}$ induces a morphism $\widetilde{\sigma} : \mathcal{O}_K/\mathcal{P} \to \mathcal{O}_K/\mathcal{P}$ that fixes $\mathbb{Z}/(p)$.
The group $D_\mathcal{P}$ is mapped homomorphically *onto* the Galois group of the finite extension $k_\mathcal{P}/\mathbb{F}_p$. The kernel of the application $D_\mathcal{P} \to \mathrm{Gal}(k_\mathcal{P}/\mathbb{F}_p)$ is the *inertia group of* $\mathcal{P}$:

$$I_\mathcal{P} = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod \mathcal{P}\ \forall \alpha \in \mathcal{O}_\mathcal{K}\}.$$

The quotient group $D_\mathcal{P}/I_\mathcal{P}$ is isomorphic to $\mathrm{Gal}(k_\mathcal{P}/\mathbb{F}_p)$ and it is thus a finite cyclic group generated by an element called the *Frobenius element* $\mathcal{F}_\mathcal{P}$. Note that, $\mathcal{F}_\mathcal{P}$ is the element of $D_\mathcal{P}/I_\mathcal{P}$ that corresponds to the Frobenius automorphism $\mathcal{F}_p \in \mathrm{Gal}(k_\mathcal{P}/\mathbb{F}_p)$: for all $\lambda \in k_\mathcal{P}$, $\mathcal{F}_p(\lambda) = \lambda^p$.

The prime $\mathcal{P}$ (or, the valuation $v_{\mathcal{P}}$) is called *unramified* if $I_{\mathcal{P}} = \{1\}$. Recall that the prime $p \in \mathbb{Z}$, $p = \mathcal{P} \cap \mathbb{Q}$, is said to be unramified in the Galois extension K if the ramification index $e_{\mathcal{P}} = 1$. It is known (see, for example [16] Theorem 28) that $e_{\mathcal{P}} = \#I_{\mathcal{P}}$. Thus $\mathcal{P}$ is unramified if and only if p is unramified in K.

If $I_{\mathcal{P}}$ is trivial, that is, if $\mathcal{P}$ is unramified, then $\mathcal{F}_{\mathcal{P}} \in G = \mathrm{Gal}(K/\mathbb{Q})$ denotes the unique element such that

$$\mathcal{F}_{\mathcal{P}}(\alpha) \equiv \alpha^p \mod \mathcal{P}$$

for all $\alpha \in \mathcal{O}_K$. If $\mathcal{P}'$ is a prime ideal conjugate to $\mathcal{P}$, the corresponding Frobenius morphisms are conjugate by an element of G. The conjugacy class of $\mathcal{F}_{\mathcal{P}}$ depends only on p and it is denoted $\mathcal{F}_p$.

Let now K be an arbitrary Galois extension of the rational numbers $\mathbb{Q}$, $\mathcal{O}_K$ its ring of integers. An ideal $\mathcal{P}$ is prime if $\mathcal{O}_K/\mathcal{P}$ is an integral domain. Σ_K will denote the set of all prime ideals of K and it is equal to the projective limit of the sets Σ_F, where F ranges over all the finite subextensions of $K/\mathbb{Q}$. Then if $K/\mathbb{Q}$ is an arbitrary Galois extension and $\mathcal{P} \in \Sigma_K$ one defines as above the groups $D_{\mathcal{P}}$, $I_{\mathcal{P}}$ and the Frobenius morphism $\mathcal{F}_{\mathcal{P}}$.

Definition 1.5.1. *Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathbb{V})$ be an ℓ-adic representation of $\mathbb{Q}$, and let p be a prime. Then ρ is said to be unramified at p if $\rho(I_{\mathcal{P}}) = \{1\}$ for any $\mathcal{P}$ of $\overline{\mathbb{Q}}$ extending p.*

Note that for different primes $\mathcal{P}$ and $\mathcal{P}'$ of $\overline{\mathbb{Q}}$ extending p, the subgroups $I_{\mathcal{P}}$ and $I_{\mathcal{P}'}$ are conjugate and, as ρ is a morphism, this means that $\rho(I_{\mathcal{P}}) = \{1\}$ if and only if $\rho(I_{\mathcal{P}'}) = \{1\}$.

If the representation ρ is unramified at p, then the restriction of ρ to $D_{\mathcal{P}}$ factors through $D_{\mathcal{P}}/I_{\mathcal{P}}$ for any $\mathcal{P} \mid p$ and $\rho(\mathcal{F}_{\mathcal{P}}) \in \mathrm{Aut}(\mathbb{V})$, the *Frobenius of $\mathcal{P}$ in the representation ρ* is defined and denoted by $\mathcal{F}_{\mathcal{P},\rho}$. The conjugacy class of $\mathcal{F}_{\mathcal{P},\rho}$ in $\mathrm{Aut}(\mathbb{V})$ depends only on p and it is denoted by $\mathcal{F}_{p,\rho}$.

Now, let $K/\mathbb{Q}$ be the extension that corresponds to $H = \mathrm{Ker}(\rho) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we have an injective representation

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\operatorname{Ker}\rho \xrightarrow{\bar{\rho}} \mathrm{Aut}(\mathbb{V})$$

and $\bar{\rho}$ is unramified at p if and only if $\bar{\rho}(I_{\mathcal{P}}) = \{1\} \Leftrightarrow I_{\mathcal{P}} = \{1\}$, for any prime $\mathcal{P}$ in K extending p, and this amounts saying that the prime p is unramified in the extension $K/\mathbb{Q}$.

Let us consider now an elliptic curve E defined over $\mathbb{Q}$. For a prime ℓ, let

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathbb{V}_\ell(E))$$

where $\mathbb{V}_\ell(E) = T_\ell(E) \otimes \mathbb{Q}_\ell$, be the corresponding ℓ-adic representation of $\mathbb{Q}$.

Let $p \in \mathbb{Z}$ be a prime, $p \neq \ell$, $\mathbb{F}_p$ its residue field and suppose the elliptic curve E has good reduction at p. Denote $\tilde{E}_p$ the reduction of E at p. This is a curve defined over the finite field $\mathbb{F}_p$. As before $\mathcal{F}_p$ denotes its Frobenius endomorphism.

1.5.1 Properties of $\mathbb{V}_\ell$ related to good reduction.

Recall that $E[\ell^m]$, $T_\ell(E)$ and $\mathbb{V}_\ell(E)$ are of rank two over $\mathbb{Z}/\ell^m\mathbb{Z}$, $\mathbb{Z}_\ell$, and $\mathbb{Q}_\ell$, respectively.

With the above setting, denote $\mathcal{P}$ some extension of p to $\overline{\mathbb{Q}}$, D its decomposition group and I the inertia group.

If E has good reduction at p, the reduction mod $\mathcal{P}$ map $\pi_\mathcal{P}$ is injective and thus, by cardinality, an isomorphism of $E[\ell^m]$ onto the corresponding module for the reduced curve $\widetilde{E}_p$,

$$E[\ell^m] \xrightarrow{\pi_\mathcal{P}} \widetilde{E}_p[\ell^m]$$

(see, for example [31] proposition 3.1).

In particular, this means that the representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell^m])$ is unramified at p. For, suppose $\sigma \in I_\mathcal{P}$, then $\rho(\sigma)$ is just σ acting on the points of $E[\ell^m]$ and the condition $\sigma \in I_\mathcal{P}$ says that for any point $P \in E[\ell^m]$, $P^\sigma \equiv P \mod \mathcal{P}$. But this means, precisely, that σ acts trivially on the points $\widetilde{E}_p[\ell^m]$ of the reduced curve, and thus, it acts trivially in $E[\ell^m]$. Then $\rho(I_\mathcal{P}) = \{1\}$.

Further, the reduction mod $\mathcal{P}$ map induces isomorphisms among the respective modules $T_\ell(E)$, $\mathbb{V}_\ell(E)$ and $T_\ell(\widetilde{E}_p)$ and $\mathbb{V}_\ell(\widetilde{E}_p)$; and the respective representations are unramified.

Consider the extension $K_\ell/\mathbb{Q}$ corresponding to $\mathrm{Ker}(\rho)$. Thus K_ℓ is the Galois extension of $\mathbb{Q}$ obtained by adjoining all the coordinates of the points in $T_\ell(E)$ and $\mathrm{Gal}(K_\ell/\mathbb{Q}) \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Ker}(\rho)$. Consider

$$\begin{array}{ccccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho} & \mathrm{Aut}(T_\ell(E)) & \xrightarrow[\simeq]{\pi_\mathcal{P}} & \mathrm{Aut}(T_\ell(\widetilde{E}_p)) \\ \downarrow & \nearrow_{\bar\rho} & & & \\ \mathrm{Gal}(K_\ell/\mathbb{Q}) & & & & \end{array}$$

As $\bar\rho$ is injective and unramified, $I_\mathcal{P} = \{1\}$ in K_ℓ, that is, p is unramified in K_ℓ. Take any Frobenius automorphism $\mathcal{F}_\mathcal{P} \in \mathrm{Gal}(K_\ell/\mathbb{Q})$. Then the automorphism $\rho(\mathcal{F}_\mathcal{P})$ of $T_\ell(E)$ corresponds to the Frobenius endomorphism $\mathcal{F}_{p,\ell}$ of $\widetilde{E}_p$. Hence we have, by abuse of language,

$$\det(\rho(\mathcal{F}_\mathcal{P})) = \det(F_{p,\ell}) = p$$

and

$$\det(1 - \rho(\mathcal{F}_\mathcal{P})) = \det(1 - \mathcal{F}_{p,\ell}) = 1 - \mathrm{Tr}(\mathcal{F}_{p,\ell}) + p$$

is equal to the number of $\mathbb{F}_p$-points of $\widetilde{E}_p$.

This means that once fixed a base for $T_\ell(E)$, $\mathrm{Aut}(T_\ell(E)) \simeq GL_2(\mathbb{Z}_\ell)$ and we can compute

$$\det(\rho(\mathcal{F}_\mathcal{P})) = p$$

$$\mathrm{Tr}(\rho(\mathcal{F}_\mathcal{P})) = a_p$$

Note that this means that, for any $p \nmid \ell N$, $\det(\rho(\mathcal{F}_\mathcal{P}))$ and $\mathrm{Tr}(\rho(\mathcal{F}_\mathcal{P}))$ are in $\mathbb{Z}$ and do not depend on the prime ℓ.

1.6 A congruence for a_p on E with an ℓ $\mathbb{Q}$-torsion point.

Suppose we have an elliptic curve E defined over $\mathbb{Q}$, with an ℓ-torsion point P defined over $\mathbb{Q}$. Consider as usual the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\mathbb{Z}/\ell\mathbb{Z}$-module $E[\ell]$.

Recall we have an injective representation

$$\rho : \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[\ell]) \simeq GL_2(\mathbb{Z}/\ell\mathbb{Z})$$

where $\mathbb{Q}(E[\ell])$ is the extension that corresponds to $\mathrm{Ker}(\rho)$ and it is generated by the coordinates of the ℓ-division points.

Now, let $p \neq \ell$ be a prime of good reduction, and $\widetilde{E}_p$ the reduced curve.

As we come to see, if E has good reduction at p, we have an isomorphism of $E[\ell]$ onto the corresponding module $\widetilde{E}_p[\ell]$ and the Frobenius automorphism of $E[\ell]$, $\rho(\mathcal{F}_\mathcal{P})$, where $\mathcal{P}$ is any prime in $\mathbb{Q}(E[\ell])$ above p, corresponds to the Frobenius endomorphism $\mathcal{F}_p$ of $\widetilde{E}_p[\ell]$. Further we have

$$\det(\rho(\mathcal{F}_\mathcal{P})) = p$$

$$\mathrm{Tr}(\rho(\mathcal{F}_\mathcal{P})) = a_p$$

this, in $\mathbb{Z}/\ell\mathbb{Z}$.

Suppose the elliptic curve E has a point P of order ℓ defined over $\mathbb{Q}$. Let Q be any independent point in $E[\ell]$, so that $\{P, Q\}$ is a base of $E[\ell]$.

With this choice of a base the representation ρ above can be written as

$$\rho : \sigma \longmapsto \begin{pmatrix} 1 & b(\sigma) \\ 0 & d(\sigma) \end{pmatrix}$$

Let $\sigma = \mathcal{F}_\mathcal{P}$. Then $\det(\rho(\mathcal{F}_\mathcal{P})) = p$ and $\mathrm{Tr}(\rho(\mathcal{F}_\mathcal{P})) = a_p$ gives

$$\rho(\mathcal{F}_\mathcal{P}) = \begin{pmatrix} 1 & b(\sigma) \\ 0 & p \end{pmatrix}$$

and

$$a_p \equiv 1 + p \mod \ell$$

for any prime $p \nmid \ell N$

We still have to work out the primes of bad reduction, and the prime ℓ.

Suppose the prime ℓ is a prime of good reduction.

Thus we have an elliptic curve E with a torsion point of prime order ℓ. By the theorem of Nagell-Lutz, torsion points have integer coordinates. If p is a prime of good reduction and $p \neq 2$ then the reduction mod p map is injective. In particular, the reduction mod ℓ map takes the ℓ-torsion point to an ℓ torsion point on the reduced curve. Thus ℓ must divide N_ℓ which is the order of the group $\widetilde{E}_\ell(\mathbb{F}_\ell)$. Then we have

$$a_\ell = \ell + 1 - N_\ell \equiv 1 \mod \ell.$$

We can include this case with the previous one and state:

Proposition 1.6.1. *Let E be an elliptic curve define over $\mathbb{Q}$, $\ell \neq 2$ a prime number, and suppose that E has an ℓ-torsion point defined over $\mathbb{Q}$. Set $a_p = p + 1 - N_p$ where N_p is the number of points of the reduced curve $\widetilde{E}_p$ modulo the prime p.*

Then, for any p of good reduction for E, we have

$$a_p \equiv 1 + p \mod \ell.$$

We will postpone the treatment for the primes of bad reduction till the end of the next chapter.

CHAPTER 2

Eisenstein series of weight 2 on $\Gamma_0(N)$.

In this chapter we define modular forms and Eisenstein series. The space of Eisenstein series of weight $k \geq 4$ for $\Gamma = Sl_2(\mathbb{Z})/\{\pm\}$ is one dimensional, generated by a series E. We expose here how to find the q-expansion for E. With this, we find the q-expansion of an Eisenstein series for $\Gamma_0(N)$. When N is a prime this space is also one dimensional. This is not the case for non-prime N.

Next we face the problem for $k = 2$ in which we do not have absolute convergence, and workout the q-expansion of the *non-holomorphic* Eisenstein series of weight 2 for Γ.

After this, following the example for $k \geq 4$ we define an Eisenstein series $e_2(z)$ of weight 2 for $\Gamma_0(N)$, with N prime, whose q-expansion is

$$e_2(z) = \frac{N-1}{24} + \sum_{n=1}^{\infty} \sigma(n)_N \, q^n.$$

Next we put together chapters one and two and show the following result:

Proposition 2.0.2. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor N, f its associated weight 2 and level N modular form. If E has an ℓ-torsion point defined over $\mathbb{Q}$ then $f \equiv e_2 \mod \ell$, where $e_2(z)$ is the Eisenstein series just defined.*

Remark: Throughout this section E will *not* denote an elliptic curve, but mostly, an Eisenstein series.

2.1 Some general and known facts on Modular Forms.

Let us recall some general and known facts on modular forms and set the notation.

The group $\Gamma = SL_2(\mathbb{Z})$ acts on the upper half-plane $\mathcal{H} = \{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0\}$ by the usual transformation:

$$z \mapsto \gamma z = \frac{az+b}{cz+d} \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

A subgroup G of Γ is called a *congruence subgroup* of level N if it contains the group $\Gamma(N)$ defined by

$$\Gamma(N) = \{\gamma \in \Gamma : \gamma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod N\}.$$

The congruence subgroup we will be mostly concerned with is

$$\Gamma_0(N) = \{\gamma \in \Gamma : c \equiv 0 \bmod N\}.$$

Call $\bar{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ and extend the action of Γ by $\gamma(\infty) = a/c$ and $\gamma(-d/c) = \infty$, with γ as before. The points $\mathbb{Q} \cup \{\infty\}$ are called *cusps*. Γ permutes the cusps transitively, so there is only one equivalence class of cusps under the action of Γ: we refer to this by saying that Γ has *one cusp*: ∞. If $G \subset \Gamma$ is a subgroup, G permutes the cusps, but there will be, in general, more than one G-equivalence class among the points in $\mathbb{Q} \cup \{\infty\}$. By a cusp of G we will mean a G-equivalence class of cusps. Thus, for example, $\Gamma_0(p)$ with p prime, has two cusps: ∞ and 0.

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2^+(\mathbb{Q})$ we denote $f|_{[\gamma]_k} = \det \gamma^{k/2}(cz+d)^{-k} f(\gamma z)$. Note that if $\gamma \in \Gamma$ this reduces to $f|_{[\gamma]_k} = (cz+d)^{-k} f(\gamma z)$ and that for any $\gamma_1, \gamma_2 \in GL_2(\mathbb{Q})$ we have:

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

Now we come to the definition of modular forms.
Let G be a congruence subgroup, a *modular form* for G is a holomorphic function on $\mathcal{H}$ such that

(1) $f|_{[\gamma]_k} = f \quad \forall \gamma \in G$

plus additional holomorphy conditions at *cusps* which we will now state.
As G contains $\Gamma(N)$ for some $N \in \mathbb{N}$, then condition (1) says that $f(z+N) = f(z)$. This, together with the fact that f holomorphic on $\mathcal{H}$, gives a Fourier expansion

$$f(z) = \sum_{n \in \mathbb{Z}} a_n \, e^{2\pi i z/N}$$

with

$$a_n = \frac{1}{N} \int_{z_0}^{z_0+N} f(z) \, e^{-2\pi i n z/N} \, dz$$

where z_0 is any point in $\mathcal{H}$.

We say that f is holomorphic at ∞ if in the above expansion $a_n = 0$ for all $n < 0$. Recall that $z \to e^{2\pi i z/N}$ maps the region $\{0 \le \mathrm{Re}(z) < N, \ \mathrm{Im}(z) > 0\}$ to the punctured

disc $\{0 < |z| < 1\}$. For a different cusp $x \in \mathbb{Q} \cup \{\infty\}$, we take $\gamma_0 \in \Gamma$ such that $x = \gamma_0 \infty$, then we say that f is holomorphic at x if $f|_{[\gamma_0]_k}$ has a Fourier expansion with no negative terms. This condition only depends on the G- equivalence class of x.

Then the holomorphy condition at cusps can be stated as:

(2) $f|_{[\gamma_0]_k}$ has the form $\sum a_n e^{-2\pi i n z/N}$ with $a_n = 0 \ \ \forall n < 0$ and for any $\gamma_0 \in \Gamma$.

We will denote $\mathcal{M}_k(N)$ the space of modular forms for the group $\Gamma_0(N)$. Observe that if $N \mid M$ then $\mathcal{M}_k(N) \subset \mathcal{M}_k(M)$.

Proposition 2.1.1. *Suppose f has the property* **(2)** *above for all $\gamma_0 \in \Gamma$. Then f has the same property for all $\alpha \in GL_2^+(\mathbb{Q})$, that is, $f|_{[\alpha]_k}$ can be written as a Fourier series $\sum a_n q_N^n$ with $a_n = 0 \ \ \forall n < 0$, for some $N \in \mathbb{N}$.*

Proof: We can assume that α has integer entries, as multiplying α by a scalar does not change the action $f|_{[\alpha]_k}$. It is easy to see that there exists a matrix $\gamma_0 \in \Gamma$ such that $\gamma_0^{-1}\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. We want to see that $f|_{[\alpha]_k}$ has a $q-$expansion with no negative terms.

$$f|_{[\alpha]_k} = f|_{[\gamma_0]_k}|_{[\gamma_0^{-1}\alpha]_k} = f|_{[\gamma_0]_k}|[\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)]_k \underset{\text{(by def)}}{=} \det(\alpha)^{k/2} d^{-k} f|_{[\gamma_0]_k}(\frac{az+b}{d})$$

As $\gamma_0 \in \Gamma$, we know $f|_{[\gamma_0]_k}$ has an expansion

$$f|_{[\gamma_0]_k} = \sum_{n=n_0}^{\infty} a_n \, q_N^n \qquad q_N = e^{2\pi i z/N}$$

for some $n_0 \geq 0$ and some $N \in \mathbb{N}$. Then,

$$f|_{[\alpha]_k} = \det(\alpha)^{k/2} d^{-k} \sum_{n=n_0}^{\infty} a_n \, e^{2\pi i n(az+b)/Nd}$$

which is of the desired form.

□

2.2 Eisenstein series.

There are essentially two ways to define *Eisenstein* series.

Eisenstein series can be defined either by summing over the elements of a lattice or by summing over the cosets of a group.

Let G denote a subgroup of Γ of finite index. Let $\{j_\gamma(z) : \gamma \in G\}$ be a collection of holomorphic nowhere vanishing functions on $\mathcal{H}$ satisfying

$$j_{\beta\gamma}(z) = j_\beta(\gamma z) j_\gamma(z) \quad \forall \beta, \gamma \in G.$$

We wish to construct a holomorphic function $f(z)$ on $\mathcal{H}$ such that

$$f(\gamma z) = j_\gamma(z) f(z) \ \forall \gamma \in G.$$

Let $h(z)$ be a holomorphic function on $\mathcal{H}$ and write formally

$$f(z) = \sum_{\gamma \in G} \frac{h(\gamma z)}{j_\gamma(z)}. \tag{2.1}$$

Then

$$f(\beta z) = \sum_{\gamma \in G} \frac{h(\gamma\beta z)}{j_\gamma(\beta z)} = \sum_{\gamma \in G} \frac{h(\gamma\beta z)}{j_{\gamma\beta}(z)} j_\beta(z) = j_\beta(z) \sum_{\gamma \in G} \frac{h(\gamma\beta z)}{j_{\gamma\beta}(z)} = j_\beta(z) f(z).$$

If the series converges absolutely and uniformly on compact subsets of $\mathcal{H}$, then $f(z)$ is holomorphic and the formal computations become legitimate. However, if there are infinitely many γ's in G for which $j_\gamma(z) = 1$ identically, the sum will contain many 'redundant' terms and will not be convergent.

Let $G_0 = \{\gamma \in G : j_\gamma(z) = 1\}$ and R a set of coset representatives of G modulo G_0,

$$G = \bigcup_{\gamma \in R} G_0 \gamma$$

Suppose $h(z)$ is invariant under G_0 : $h(\beta z) = h(z)\,(\forall \beta \in G_0)$, and take

$$f(z) = \sum_{\gamma \in R} \frac{h(\gamma z)}{j_\gamma(z)} = \sum_{\gamma \in G_0 / G} \frac{h(\gamma z)}{j_\gamma(z)}. \tag{2.2}$$

Then $f(z)$ is independent of the coset representatives chosen and for any $\beta \in G$, $f(\beta z) = j_\beta(z) f(z)$. If this series converges absolutely and uniformly on compacts subsets of $\mathcal{H}$, then it defines a holomorphic function on $\mathcal{H}$ with the desired property.

2.3 Eisenstein for Γ, $k \geq 4$.

Let us take $j_\gamma(z) = (cz + d)^k$, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$.

Thus we have $j_{\gamma\gamma'}(z) = j_\gamma(\gamma' z) j_{\gamma'}(z)$.

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and k even, when is $j_\gamma(z) = 1$?

$$j_\gamma(z) = (cz + d)^k = 1 \Leftrightarrow (cz + d) = \pm 1 \Leftrightarrow c = 0 \;\&\; d = \pm 1$$

Then $\gamma \in \{\pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) : h \in \mathbb{Z}\}$.

When $\gamma_1, \gamma_2 \in \Gamma$ are equivalent modulo the subgroup $\Gamma_\infty = < \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) >$?

$$\gamma_1 \sim \gamma_2 \Leftrightarrow \gamma_1 = \pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \gamma_2 = \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} a + hc & b + hd \\ c & d \end{smallmatrix}\right)$$

Now $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ if and only if $\det \gamma = ad - bc = 1$. If, for any pair c, d with c and d coprime, a and b is a solution, then every solution is $(a + hc, b + hd)$, which gives a matrix

$$\left(\begin{smallmatrix} a + hc & b + hd \\ c & d \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mod \Gamma_\infty$$

Moreover, if $c \neq 0$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right) \mod \Gamma_\infty$. Thus if we are looking for non-equivalent matrices, we can assume $c \geq 0$ and $d \in \mathbb{Z}$ coprime with c.

Then a set of representatives for $\Gamma \mod \Gamma_\infty$ is the set of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where d, c run through the integers, with c and d coprime, $c \geq 0$, and a, b is (any) one solution of $ad - bc = 1$.

Now returning to equation (2.2) with $h(z) = 1$ and $j_\gamma(z) = (cz + d)^k$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\Gamma \mod \Gamma_\infty$, we have that for $k > 2$ the series:

$$E_k(z) = \sum_{\substack{(c,d)=1 \\ c \geq 0, d \in \mathbb{Z}}} \frac{1}{(cz + d)^k}$$

converges absolutely and uniformly on compact sets of $\mathcal{H}$ and defines a weight-k *Eisenstein* series.

With $c = 0$ we only have one term corresponding to $d = 1$ and (say) $a = b = 1$. Then,

$$E_k(z) = 1 + \sum_{\substack{(c,d)=1 \\ c > 0, d \in \mathbb{Z}}} \frac{1}{(cz + d)^k} = 1 + \sum_{n=1}^{\infty} \sum_{\substack{d \in \mathbb{Z} \\ (n,d)=1}} \frac{1}{(nz + d)^k}$$

2.4 The q-expansion of $E_k(z)$, $k \geq 4$.

In this section we will find the q-expansion of the Eisenstein series $E_k(z)$ defined above.

Recall $\zeta(k) = \sum_{a \in \mathbb{N}} \frac{1}{a^k}$. Then,

$$\begin{aligned} \zeta(k) E_k(z) =& \zeta(k) + \sum_{a \in \mathbb{N}} \frac{1}{a^k} \sum_{n=1}^{\infty} \sum_{\substack{d \in \mathbb{Z} \\ (n,d)=1}} \frac{1}{(nz + d)^k} \\ =& \zeta(k) + \sum_{a=1}^{\infty} \sum_{n=1}^{\infty} \sum_{\substack{d \in \mathbb{Z} \\ (n,d)=1}} \frac{1}{(anz + ad)^k} \end{aligned} \tag{2.3}$$

Now the sum over all pairs

$$\{(an, ad) \quad a, n \in \mathbb{N},\ d \in \mathbb{Z} \text{ with } (d, n) = 1\}$$

equals the sum over

$$\{(m, D) \;\; m \in \mathbb{N},\; D \in \mathbb{Z}\}$$

and the equation (2.3) can be re-written as

$$\zeta(k)E_k(z) = \zeta(k) + \sum_{\substack{m\in\mathbb{N}\\ D\in\mathbb{Z}}} \frac{1}{(mz+D)^k}$$

We want the q-expansion of this last expression.

As it is well known, and can be found in any book on modular forms, we have for $k \geq 3$

$$\sum_{D\in\mathbb{Z}} \frac{1}{(z+D)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1}\, q^n \qquad q = e^{2\pi i z}$$

Then,

$$\sum_{m\geq 1} \sum_{D\in\mathbb{Z}} \frac{1}{(mz+D)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m\geq 1} \sum_{n=1}^{\infty} n^{k-1}\, q^{mn}$$

and, grouping powers of q,

$$\sum_{\substack{m\geq 1\\ D\in\mathbb{Z}}} \frac{1}{(mz+D)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m\geq 1} (\sum_{d|m} d^{k-1})\, q^m = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m\geq 1} \sigma_{k-1}(m)\, q^m$$

Thus we get the well known expression

$$\zeta(k)E_k(z) = \zeta(k) + \sum_{\substack{m\in\mathbb{N}\\ D\in\mathbb{Z}}} \frac{1}{(mz+D)^k} = \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n$$

After normalizing we get the following Eisenstein series, which we will denote again $E_k(z)$:

$$E_k(z) = \frac{(k-1)!\zeta(k)}{(2\pi i)^k} \;+\; \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n$$

For $k \geq 4$ it is a modular form for $\Gamma = SL_2(\mathbb{Z})$.

□

We can obtain modular forms for $\Gamma_0(N)$ from modular forms for Γ, as the following proposition shows.

Proposition 2.4.1. *Let $k > 0$, and l any positive integer. Take*

$$\delta_l = \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})^+$$

and for $f \in \mathcal{M}_k(N)$ consider $f(lz)$. Then $f(lz) = l^{-k/2}(f|_{[\delta_l]k})(z) \in \mathcal{M}_k(lN)$.

Proof: [20]

Put $g = f|_{[\delta_l]k}$ and let $\gamma = \begin{pmatrix} a & b \\ clN & d \end{pmatrix} \in \Gamma_0(lN)$

Then $\delta_l \gamma \delta_l^{-1} = \begin{pmatrix} a & lb \\ cN & d \end{pmatrix} \in \Gamma_0(N)$

$$g|_{[\gamma]k} = (f|_{[\delta_l]k})|_{[\gamma]k} = (f|_{[\delta_l]k})|_{[(\gamma\delta_l^{-1})\delta_l]k} = (f|_{[\delta_l\gamma\delta_l^{-1}]k})|_{[\delta_l]k} = f|_{[\delta_l]k} = g$$

It remains to see that $g|_{[\gamma_0]_k}$ has a Fourier expansion with no negative terms, for any $\gamma_0 \in \Gamma$. But this is straightforward as

$$g|_{[\gamma_0]_k} = f|_{[\delta_l]_k}|_{[\gamma_0]_k} = f|_{[\delta_l\gamma_0]_k}$$

$\delta_l\gamma_0 \in GL_2^+(\mathbb{Q})$ and f is holomorphic at the cusps.

□

2.5 An Eisenstein series for $\Gamma_0(N)$, N prime and $k \geq 4$.

Proposition 2.5.1. *Let $k \geq 4$, $E_k(z) = \dfrac{(k-1)!\,\zeta(k)}{(2\pi i)^k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)\ q^n$ be the Eisenstein series for Γ, and N a prime integer. We will consider*

$$e_k(z) = E_k(z) - N^{k-1}\ E_k(Nz)$$

Then $e_k(z) \in \mathcal{M}_k(N)$ and has q-expansion

$$e_k(z) = \frac{(k-1)!\,\zeta(k)}{(2\pi i)^k}\ (1 - N^{k-1}) + \sum_{n=1}^{\infty} \sigma_{k-1}(n)_N\ q^n$$

where

$$\sigma_{k-1}(n)_N = \sum_{\substack{d|n \\ (d:N)=1}} d^{k-1}.$$

Proof:
For any integer M and any $d \mid M$, the series $E_k(dz) \in \mathcal{M}_k(d) \subset \mathcal{M}_k(M)$ as d is a divisor of M.

Thus we only have to see that the q-expansion is the one given above.

Let us put $c = \dfrac{(k-1)!\ \zeta(k)}{(2\pi i)^k}$ to simplify the notation. If $N = p$ is prime, then we have

$$e_k(z) = E_k(z) - p^{k-1}E_k(pz) = c(1 - p^{k-1}) + \sum_{n=1}^{\infty} \sigma_{k-1}(n)\ q^n - \sum_{n=1}^{\infty} p^{k-1}\sigma_{k-1}(n)\ q^{pn}$$

Now we group by powers of q and denote $a(n)$ the coefficient of q^n:
for $(n : p) = 1$ only the first sum is involved and $a(n) = \sigma_{k-1}(n) = \sigma_{k-1}(n)_p$. If $p \mid n$ then $a(n) = \sigma_{k-1}(n) - p^{k-1}\sigma_{k-1}(\frac{n}{p})$. If we write $n = mp^r$ then the divisors d of n will

be the divisors of m, for those coprime to p and p times a divisor of $n \mid p$ for those not coprime to p. This gives

$$\sigma_{k-1}(n) = \sum_{d|m} d^{k-1} + \sum_{d|\frac{n}{p}} (pd)^{k-1} = \sigma_{k-1}(m) + p^{k-1}\sigma_{k-1}(\frac{n}{p})$$

so $a(n) = \sigma_{k-1}(m) = \sigma_{k-1}(n)_N$.

□

2.6 The non-holomorphic Eisenstein series of weight 2.

For $k = 2$, if we set $\sum_{\Gamma_\infty/\Gamma} \frac{1}{(cz+d)^2}$ or $\sum'_{m,n\in\mathbb{Z}} \frac{1}{(cz+d)^2}$ then we do not have absolute convergence and its value depends on the order of summation. Under a modular substitution any order of summation is disturbed and the series above would not lead to a useful definition.

The following procedure introduces a summability factor and a limiting process.

Let us consider the function

$$G(z,s) = \sum'_{m,n\in\mathbb{Z}} \frac{1}{(mz+n)^2} \frac{1}{|mz+n|^{2s}}$$

for $s > 0$ and define $G_2(z) = \lim_{s\to 0} G(z,s)$.

The series in $G(z,s)$ is absolutely and uniformly convergent for $2 + 2s \geq 2 + \epsilon$.

For $s > 0$ and because of absolute convergence, we have that under a modular substitution $z \mapsto \gamma z = \frac{az+b}{cz+d}$, with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

$$\begin{aligned} G(\gamma z, s) =& (cz+d)^2 |cz+d|^{2s} \sum'_{m,n\in\mathbb{Z}} \frac{1}{((ma+nc)z+(mb+nd))^2} \frac{1}{|(ma+nc)z+(mb+nd)|^{2s}} \\ =& (cz+d)^2 |cz+d|^{2s} G(z,s) \end{aligned}$$

because $(ma+nc, mb+nd)$ goes through $\mathbb{Z}\times\mathbb{Z} - \{(0,0)\}$ as (m,n) do.

Thus, if we define $G_2(z) = \lim_{s\to 0} G(z,s)$, supposing this limit exists, then we will have $G_2(\gamma z) = (cz+d)^2 G_2(z)$ for any $\gamma \in \Gamma$. Notice, however, that the functions $G(z,s)$ are not holomorphic functions of z.

Let us re-write

$$G(z,s) = 2\,\zeta(2+2s) \;+\; 2\sum_{m=1}^{\infty} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2} \frac{1}{|mz+n|^{2s}}$$

and study the function

$$\Psi(z,s) = \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} \frac{1}{|z+n|^{2s}} \qquad \mathrm{Im}(z) > 0$$

considering s as complex variable.

2.6.1 Poisson Summation Formula

Let $f : \mathbb{R} \to \mathbb{C}$ be a twice continuously differentiable function in $-\infty < x < \infty$ and such that

$$\int_{-\infty}^{\infty} f(x)\ dx \qquad \text{and} \qquad \int_{-\infty}^{\infty} |f''(x)|\ dx$$

both exist. Then

$$S = \sum_{n=-\infty}^{\infty} f(n) = \sum_{k=-\infty}^{\infty} \widehat{f}(k)$$

where $\widehat{f}$ is the Fourier transform of f:

$$\widehat{f}(k) = \int_{-\infty}^{\infty} f(x)\ e^{-2\pi i k x}\ dx$$

Proof: see, for example, [25] §35 Theorem A.

Now we apply Poisson summation formula to $f(x) = \dfrac{1}{(z+x)^2}\dfrac{1}{|z+x|^{2s}}$; recall that for $2+2\,\mathrm{Re}(s) > 1$ this function belongs to L^1 as a function of x and therefore it exists its Fourier transform:

$$\Psi(z,s) = \sum_{n\in\mathbb{Z}} A_n(z,s)$$

where $A_n(z,s) = \widehat{f}(n) = \displaystyle\int_{-\infty}^{\infty} \frac{e^{-2\pi i n x}}{(z+x)^2|z+x|^{2s}}\ dx.$

Now,

$$A_n(z,s) \quad = \int_{-\infty}^{\infty} \frac{e^{-2\pi i n x}}{(z+x)^2|z+x|^{2s}}\ dx \underset{x=-t}{=} \int_{-\infty}^{\infty} \frac{e^{2\pi i n t}}{(z-t)^2|z-t|^{2s}}\ dt$$

$$\underset{\xi=-iz}{=} i\int_{-\infty}^{\infty} \frac{e^{2\pi i n t}}{(\xi+it)^2|\xi+it|^{2s}}\ idt \underset{w=\xi+it}{=} ie^{2\pi i n z} \int_{\mathrm{Re}(w)=\rho} \frac{e^{2\pi n w}}{w^2\ |w|^{2s}}\ dw$$

where $\mathrm{Re}(w) = \mathrm{Re}(\xi) = \mathrm{Im}(z) = \rho > 0$.

Notice that on the path of integration, $|w|^2 = w\bar{w} = w(2\rho - w)$, therefore we could re-write this integral as:

$$A_n(z,s) \quad = ie^{2\pi i n z} \int_{\mathrm{Re}(w)=\rho} \frac{e^{2\pi n w}}{w^2\ w^s(2\rho-w)^s}\ dw$$

$$\underset{w=\rho\omega}{=} i\frac{e^{2\pi i n z}}{\rho^{1+2s}} \int_{\mathrm{Re}(\omega)=1} \frac{e^{2\pi n\rho\omega}}{\omega^{2+s}\ (2-\omega)^s}\ d\omega$$

This integral represents a holomorphic function for $2 + 2\,\mathrm{Re}(s) > 1$, or $\mathrm{Re}(s) > -\frac{1}{2}$. Therefore it is holomorphic at $s = 0$.

Let us write

$$G(z,s) = 2\zeta(2+2s) \ + \ 2\sum_{m=1}^{\infty} \Psi(mz,s) = 2\zeta(2+2s) \ + \ 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}} A_n(mz,s)$$
$$= 2\zeta(2+2s) \ + \ 2\sum_{m=1}^{\infty}\sum_{n<0} A_n(mz,s) \ + \ 2\sum_{m=1}^{\infty}\sum_{n\geq 1} A_n(mz,s) \ + \ 2\sum_{m=1}^{\infty} A_0(mz,s)$$

this, provided we can show the three sums in the last expression converge separately for $s > 0$.

We will be interested in the convergence of the above series near $s = 0$, thus we will be interested in bounding the $A_n(z,s)$, as well as in the limit $\lim_{s\to 0} A_n(z,s)$.

We have three cases here:

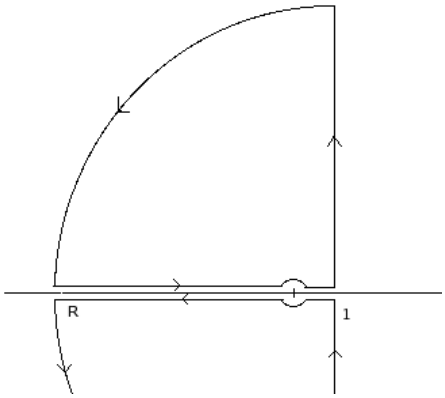

Figure 2.1:

I) $n > 0$: Note that if we take an arch $w = Re^{it}$ in the upper half-plane, from $\mathrm{Re}(w) = 1$ to the point $-R$ in the negative real axis (figure (2.1)), we have $|e^{2\pi n\rho w}| = e^{2\pi n\rho R\cos(t)}$, and over this arch $-R \leq R\cos(t) \leq 1$ as $\cos(t) = \dfrac{1}{R}$ in the intersection $|w| = R$ and $\mathrm{Re}(w) = 1$. So we can bound $e^{2\pi n\rho R\cos(t)} \leq e^{2\pi n\rho}$ and easily see that the integral over this arch goes to zero as R goes to infinity. Then we can change the integral on $\mathrm{Re}(w) = 1$ from 1 to $1 + i\infty$, by the integral on the real axis from $-\infty$ to 1, avoiding the 0 with half an arch of radio $\epsilon < 1$. It is to be understood here that $\arg(w) = \pi$ on the negative real axis. Similarly, we change the integral from $1 - i\infty$ to 1 by the integral on the real axis from $-\infty$ to 1, avoiding the 0 with half an arch of radio $\epsilon < 1$, this time on the lower half-plane and taking into account now that $\arg(w) = -\pi$ on the negative real axis.

After noting that the two integrals from ϵ to 1 over the positive real axis cancel each other, this results in a "loop" integral from $-\infty$ to 0^+ in the positive direction, as shown in figure (2.2). This gives us

$$A_n(z,s) = i\frac{e^{2\pi inz}}{\rho^{1+2s}} \oint_{-\infty}^{0^+} \frac{e^{2\pi n\rho\omega}}{\omega^{2+s}\ (2-\omega)^s}\ d\omega$$

Now the right hand side is defined and holomorphic for every s and gives an analytic continuation of $A_n(z,s)$, as it coincides with it for s real and positive.

It is easy to bound this integral for s real and positive and find out

$$|A_n(z,s)| \leq C\ \frac{e^{-\pi n\rho}}{\rho^{1+2s}} \left(\frac{4}{3}\right)^s$$

for some constant C, independent of n. Remember $\rho = \mathrm{Im}(z)$.

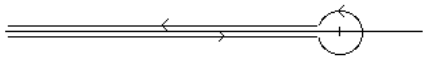

Figure 2.2:

Take $\epsilon = \dfrac{1}{2}$ in figure (2.2). As s is real, $|w^{2+s}(2-w)^s| = |w|^{2+s}|2-w|^s \geq \left(\dfrac{1}{2}\right)^{2+s}\left(\dfrac{3}{2}\right)^s$ for any w on the path of integration. Then we have:

$$\begin{aligned}|A_n(z,s)| &\leq \frac{e^{-2\pi n\rho}}{\rho^{1+2s}} \left(2\ \int_{1/2}^{+\infty} \frac{e^{-2\pi n\rho x}}{(\frac{1}{2})^{2+s}\ (\frac{3}{2})^s}\ dx\ + \int_0^{2\pi} \frac{e^{\pi n\rho\cos t}}{(\frac{1}{2})^{1+s}\ (\frac{3}{2})^s}\ dx\right) \\ &\leq \frac{e^{-2\pi n\rho}}{\rho^{1+2s}} \left(2\ \frac{e^{-\pi n\rho}}{\rho\,(\frac{1}{2})^{2+s}\ (\frac{3}{2})^s}\ + 2\pi\frac{e^{\pi n\rho}}{(\frac{1}{2})^{1+s}\ (\frac{3}{2})^s}\right) \leq C\ \frac{e^{-\pi n\rho}}{\rho^{1+2s}} \left(\frac{4}{3}\right)^s\end{aligned}$$

for some constant C, as desired.

II) $n < 0$: Analogously to the case $n > 0$, we "bend" the path of integration into a loop around the real axis from 2^- to $+\infty$ in the negative direction and find the estimate

$$|A_n(z,s)| \leq C\ \frac{e^{-\pi|n|\rho}}{\rho^{1+2s}} \left(\frac{4}{3}\right)^s$$

III) $n = 0$:

$$A_0(z,s) = i\frac{1}{\rho^{1+2s}} \int_{\mathrm{Re}(\omega)=1} \frac{1}{\omega^{2+s}\ (2-\omega)^s}\ d\omega$$

and then

$$|A_0(z,s)| \leq \frac{1}{\rho^{1+2s}} \int_{-\infty}^{\infty} \frac{1}{(1+t^2)^{\frac{2+s}{2}}\ (1+t^2)^{s/2}}\ dt$$

$$\leq \frac{1}{\rho^{1+2s}} \int_{-\infty}^{\infty} \frac{dt}{(1+t^2)^{1+s}} \leq \frac{\pi}{\rho^{1+2s}} \qquad \text{for } s \geq 0$$

Putting things together we can majorize

$$2\sum_{m=1}^{\infty}\ \sum_{n<0} A_n(mz,s)\ +\ 2\sum_{m=1}^{\infty}\ \sum_{n\geq 1} A_n(mz,s)\ +\ 2\sum_{m=1}^{\infty}\ A_0(mz,s)$$

by

$$2C\sum_{m=1}^{\infty}\ \sum_{n<0} \frac{e^{-\pi|n|m\rho}}{(m\rho)^{1+2s}}\,(\frac{4}{3})^s\ +\ 2C\sum_{m=1}^{\infty}\ \sum_{n\geq 1} \frac{e^{-\pi nm\rho}}{(m\rho)^{1+2s}}\,(\frac{4}{3})^s +\ 2C\sum_{m=1}^{\infty}\ \frac{1}{(m\rho)^{1+2s}}$$

Then the three sums converge absolutely for $s > 0$, the two double sums are uniformly convergent for $0 \leq s \leq 1$ and we can therefore perform the limit for $s \to 0$ and write:

$$G_2(z) = 2\zeta(2)\ +\ 2\sum_{m=1}^{\infty}\ \sum_{n<0} A_n(mz,0)\ +\ 2\sum_{m=1}^{\infty}\ \sum_{n\geq 1} A_n(mz,0)\ +\ \lim_{s\to 0}\ 2\sum_{m=1}^{\infty}\ A_0(mz,s)$$

We will now prove the following two facts:

Fact 1:

$$A_n(mz,0) = \begin{cases} 0 & \text{for } n < 0 \\ -(2\pi)^2 n e^{2\pi i n m z} & \text{for } n \geq 1 \end{cases}$$

Fact 2:

$$\lim_{s\to 0}\ 2\sum_{m=1}^{\infty}\ A_0(mz,s) = \frac{-2\pi i}{z-\bar{z}}$$

which, together with the well known result $\zeta(2) = \dfrac{\pi^2}{6}$, will give us

$$G_2(z) = \frac{\pi^2}{3}\ -8\pi^2\ \sum_{m=1}^{\infty}\ \sum_{n\geq 1} n e^{2\pi i n m z}\ -\frac{2\pi i}{z-\bar{z}}$$

Proof of Fact 1:

Recall that $A_n(z,s) = i\dfrac{e^{2\pi i n z}}{\rho^{1+2s}} \int_{\mathrm{Re}(\omega)=1} \dfrac{e^{2\pi n\rho\omega}}{\omega^{2+s}\ (2-\omega)^s}\ d\omega$, so we have

$$A_n(mz,0) = i\frac{e^{2\pi i n m z}}{m\rho} \int_{\mathrm{Re}(\omega)=1} \frac{e^{2\pi nm\rho\omega}}{\omega^2}\ d\omega$$

Suppose first $m < 0$ and replace the integral $\displaystyle\int_{1-iR}^{1+iR} \frac{e^{2\pi nm\rho\omega}}{\omega^2}\, d\omega$ by the integral over a half disc $|w-1| = R, -\pi/2 \le \arg(w-1) \le \pi/2$.
We can bound this integral by $\dfrac{\pi}{R}\, e^{2\pi nm\rho}$ which goes to zero as $R \to \infty$. Thus $A_n(mz, 0) = 0$ for $m < 0$.

For $m > 0$, replace $\xi = 2\pi nm\rho w$ in the integral to get

$$A_n(mz,0) = i\frac{e^{2\pi inmz}}{m\rho}\, 2\pi nm\rho \int_{\mathrm{Re}(\xi)=a} \frac{e^{\xi}}{\xi^2}\, d\xi$$

where $a = 2\pi nm\rho > 0$. The last integral is (see Hankel's lemma, in the appendix to this section below): $\dfrac{2\pi i}{\Gamma(2)}$ which gives

$$A_n(mz,0) = ie^{2\pi inmz}\, 2\pi n\, 2\pi i = -4\pi^2\, n\, e^{2\pi inmz}$$

which completes the proof of **1**.

Proof of Fact 2:

We have to calculate the limit $\lim\limits_{s\to 0}\ 2\sum\limits_{m=1}^{\infty}\ A_0(mz,s)$.

$$2\sum_{m=1}^{\infty}\ A_0(mz,s) = \sum_{m=1}^{\infty}\ \frac{2i}{(m\rho)^{1+2s}} \int_{\mathrm{Re}(w)=1}\ \frac{dw}{w^{2+s}\,(2-w)^s} = \frac{2i}{\rho^{1+2s}} I(s)\zeta(1+2s)$$

where $I(s)$ denotes the integral

$$I(s) = \int_{\mathrm{Re}(w)=1}\ \frac{dw}{w^{2+s}\,(2-w)^s}$$

We now calculate this integral.

As in **(III)** the path can be bended to a loop around $(2,\infty)$ in the negative direction,

$$I(s) = \oint_{\infty}^{2^-}\ \frac{dw}{w^{2+s}\,(2-w)^s}$$

To evaluate this integral we take a small disc around 2, thus the path of integration comes form $+\infty$ to $2+\epsilon$ on the lower part of the real axis, then a disc of radius ϵ around 2 in the negative direction, and finally from $2+\epsilon$ to $+\infty$ on the upper part of the real axis. Here $\arg(2-w) = \pi$ on the lower part of the axis, and $\arg(2-w) = -\pi$ on the upper part, as we are taking the branch of the logarithm that is positive when $w(2-w)$ is positive.

$$I(s) = \int_{\infty}^{2+\epsilon}\ \frac{dx}{x^{2+s}\,(x-2)^s\, e^{i\pi s}} + \int_{2+\epsilon}^{\infty}\ \frac{dx}{x^{2+s}\,(x-2)^s\, e^{-i\pi s}} + \int_{(|w-2|=\epsilon)^-}\ \frac{dw}{w^{2+s}\,(2-w)^s}$$

The last integral goes to zero as ϵ tends to zero,

$$\left|\int_{(|w-2|=\epsilon)^-}\ \frac{dw}{w^{2+s}\,(2-w)^s}\right| \ \le\ \int_0^{2\pi}\ \frac{\epsilon\, dt}{(2-\epsilon)^{2+s}\,\epsilon^s}\ \le\ \frac{2\pi\epsilon}{(2-\epsilon)^{2+s}\,\epsilon^s}\ \underset{\epsilon\to 0}{\longrightarrow} 0$$

for $0 \leq s < 1$. The other two integrals permit the limit $\epsilon \to 0$ as they converge for $0 \leq s < 1$. Thus we get, gathering the two integrals

$$I(s) = 2i\sin(\pi s) \int_2^\infty \frac{dx}{x^{2+s}\,(x-2)^s} \underset{x=2(u+1)}{=} \frac{i\sin(\pi s)}{2^{2s}} \int_0^\infty \frac{du}{(u+1)^{2+s}\,u^s}$$

This last expression is

$$\int_0^\infty \frac{u^{-s}\,du}{(u+1)^{2+s}} = \frac{\Gamma(1-s)\,\Gamma(1+2s)}{\Gamma(2+s)}$$

For the last equality, see the identities for the Gamma function in the appendix to this section below.

We have calculated

$$2\sum_{m=1}^{\infty} A_0(mz,s) = \frac{2i}{\rho^{1+2s}} I(s)\zeta(1+2s) = \frac{2i}{\rho^{1+2s}} \frac{i\sin(\pi s)}{2^{2s}} \frac{\Gamma(1-s)\,\Gamma(1+2s)}{\Gamma(2+s)}\,\zeta(1+2s)$$

Thus,

$$\lim_{s\to 0} 2\sum_{m=1}^{\infty} A_0(mz,s) = \frac{-2}{\rho} \frac{\Gamma(1)\,\Gamma(1)}{\Gamma(2)} \lim_{s\to 0} \sin(\pi s)\,\zeta(1+2s) = \frac{-\pi}{\rho} = \frac{-2\pi i}{z-\bar{z}}$$

as $\lim_{s\to 0} s\zeta(1+2s) = \frac{1}{2}$ for, having $\zeta(s)$ a simple pole with residue 1 at $s=1$, $\zeta(1+2s)$ has a simple pole at $s=0$ with residue $1/2$.
Recall $\Gamma(n) = (n-1)!$ for $n \in \mathbb{N}_0$.

Thus our definition lead us to

$$\begin{aligned} G_2(z) &= \frac{\pi^2}{3} - 8\pi^2 \sum_{m=1}^{\infty} \sum_{n\geq 1} n e^{2\pi i n m z} - \frac{2\pi i}{z-\bar{z}} \\ &= \frac{\pi^2}{3} - 8\pi^2 \sum_{m=1}^{\infty} \sigma(m) e^{2\pi i m z} - \frac{2\pi i}{z-\bar{z}} \end{aligned}$$

This function, though invariant for Γ, it is not a holomorphic function of z, due to the non-holomorphic term $\dfrac{2\pi i}{z-\bar{z}}$.

Remark: Note that we can take for any integer $k \geq 3$

$$G_{(k)}(z,s) = \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(mz+n)^k} \frac{1}{|mz+n|^{2s}}$$

for $s > 0$ and define $G_k(z) = \lim_{s\to 0} G_{(k)}(z,s)$. We can apply exactly the same procedure we have done for $k=2$, but with the difference now that for $k \geq 3$ the sum $2\sum_{m=1}^{\infty} A_0(mz,s) = \frac{2i}{\rho^{k+2s}}\, I(s)\,\zeta(k-1+2s) = 0$. We have seen that $I(s)$ vanishes at $s=0$ and being $\zeta(k-1+2s)$ holomorphic at $s=0$ for $k \geq 3$ this leads to $\lim_{s\to 0} 2\sum_{m=1}^{\infty} A_0(mz,s) = 0$. Thus we obtain a holomorphic function of the variable z.

2.6.2 Appendix to this section:

1) Identities with Gamma function

For $0 < p$ and $0 < \mathrm{Re}(s) < p$

$$\int_0^\infty \frac{\xi^{s-1}}{(1+\xi)^p}\, d\xi \;=\; \frac{\Gamma(s)\Gamma(p-s)}{\Gamma(p)}$$

Another version is:
For $\mathrm{Re}(p), \mathrm{Re}(q) > 0$

$$\int_0^\infty \frac{\xi^{p-1}}{(1+\xi)^{p+q}}\, d\xi \;=\; \beta(p,q) \;=\; \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)}$$

2)Hankel's integral

For a a positive real number and $\mathrm{Re}(s) > 1$, we have:

$$\int_{a-i\infty}^{a+i\infty} \frac{e^\omega}{\omega^s}\, d\omega = \oint_{-\infty}^{0^+} \frac{e^\omega}{\omega^s}\, d\omega = \frac{2\pi i}{\Gamma(s)}$$

Where the first integral is over $\mathrm{Re}(\omega) = a$ and the second over a loop in the positive direction "around" the negative real axis.
For $n < 0$,

$$\int_{a-i\infty}^{a+i\infty} \frac{e^{n\omega}}{\omega^s}\, d\omega = 0$$

Proofs: [25], §37 and §24.

Recall: The Riemann zeta-function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ extends to a holomorphic function on the whole complex plane, except for a simple pole at $s = 1$ with residue 1.

2.7 Eisenstein series $e_2(z)$ for $\Gamma_0(N)$, N prime.

We now consider the normalized Eisenstein series

$$E_2(z) = \frac{-1}{24} + \sum_{n=1}^{\infty} \sigma(n)\, q^n + \frac{1}{8\pi y}$$

defined for $z = x + iy$ on the upper half-plane, non holomorphic due to the term $\frac{1}{8\pi y}$, and invariant for the action of Γ.

Let N be a prime integer. Following the example for $k \geq 4$, define

$$e_2(z) = E_2(z) - N\; E_2(Nz).$$

We want to prove that $e_2(z) \in \mathcal{M}_k(N)$ and has q-expansion

$$e_2(z) = \frac{-1}{24}\,(1-N) + \sum_{n=1}^{\infty} \sigma(n)_N\; q^n$$

The proof for the q-expansion is the same as for $k \geq 4$ except that we have to show that the term with $\frac{1}{8\pi y}$ vanishes. But this is immediate since we have

$$\frac{1}{8\pi y} - N\frac{1}{8\pi N y} = 0$$

Further, we need to prove that $e_2(z)$ is holomorphic on $\mathcal{H}$ and that it is holomorphic at every cusp of $\Gamma_0(N)$, rather than ∞.

To accomplish this we state the following

Theorem 2.7.1. *see [20] Theorem 2.1.4*

Suppose f is holomorphic on $\mathcal{H}$ and $f|\gamma = f$, $\forall \gamma \in G$, where G is a congruence subgroup. If there exists a positive real number ν such that $f(z) = O(\mathrm{Im}(z)^{-\nu})$ for $\mathrm{Im}(z) \to 0$ uniformly with respect to $\mathrm{Re}(z)$, then f belongs to $\mathcal{M}_k(G)$.

Proof:

If $G\backslash\mathcal{H}$ is compact, the assertion is obvious. Suppose G has cusps and let $x \in \mathbb{Q}$ be a cusp of G. Take $\sigma \in GL_2(\mathbb{Q})$ such that $\sigma x = \infty$ and let

$$f|_{[\sigma^{-1}]_k}(z) = \sum_{n=-\infty}^{\infty} a_n\, e^{2\pi i n z/N}$$

for some $N \in \mathbb{N}$.

The Fourier coefficient a_n being expressed as

$$a_n = \frac{1}{N}\int_{z_0}^{z_0+N} f|_{[\sigma^{-1}]_k}(z)\, e^{-2\pi i n z/N}\, dz$$

for any fixed $z_0 \in \mathcal{H}$.

Now take $\sigma^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

We have

$$\mathrm{Im}(\sigma^{-1}z) = \frac{\mathrm{Im}(z)}{|cz+d|^2} = O(\frac{1}{\mathrm{Im}(z)}) \text{ for } \mathrm{Im}(z) \to \infty, \text{ uniformly on } |\mathrm{Re}(z)| \leq N/2$$

As $\mathrm{Im}(\sigma^{-1}z) \to 0$ when $\mathrm{Im}(z) \to \infty$, we have by the assumption on f: $f(\sigma^{-1}z) = O((\mathrm{Im}\, z)^{\nu})$. So,

$$f|_{[\sigma^{-1}]_k}(z) = f(\sigma^{-1}z)j(\sigma^{-1},z)^{-k} = f(\sigma^{-1}z)(cz+d)^{-k} = O(\mathrm{Im}(z)^{\nu-k})$$

for $\mathrm{Im}(z) \to \infty$ uniformly on $|\mathrm{Re}(z)| \leq N/2$. Thus

$$|a_n| \leq \frac{C}{N}\int_{z_0}^{z_0+N} \mathrm{Im}(z)^{\nu-k}|e^{-2\pi i n z/N}|\,|dz| \leq C\,(\mathrm{Im}(z))^{\nu-k}\, e^{2\pi n\,\mathrm{Im}\, z}$$

for $\mathrm{Im}(z) \to \infty$, and having taken $z_0 = iy - N/2$.

Thus for $n < 0$ we have $a_n = 0$, therefore f is holomorphic at the cusp x.

For the cusp ∞, there is a $\gamma \in G$ such that $\gamma\infty = x$, a real cusp, equivalent to ∞.

□

Proposition 2.7.2. *see [20] Lemma 4.3.3*
For a sequence $\{a_n\}_{n=0}^{\infty}$ of complex numbers, put

$$f(z) = \sum_{n=0}^{\infty} a_n\, e^{2\pi i n z} \qquad z \in \mathcal{H}$$

If $a_n = O(n^\nu)$ for some $\nu > 0$, then the series is absolutely and uniformly convergent on compact subsets of $\mathcal{H}$ and $f(z)$ is holomorphic on $\mathcal{H}$. Moreover $f(z) = O(\mathrm{Im}(z)^{-\nu-1})$ for $\mathrm{Im}(z) \to 0$ uniformly on $\mathrm{Re}(z)$.

Proof: For $\nu > 0$ we have $\lim_{n\to\infty} \dfrac{n^\nu}{(-1)^n\binom{-\nu-1}{n}} = \Gamma(\nu+1)$. Then, there exists a constant L such that $|a_n| \leq L\,(-1)^n \dfrac{n^\nu}{(-1)^n\binom{-\nu-1}{n}} \quad \forall n \geq 0$.

For $z = x + iy$,

$$\sum_{n=0}^{\infty} |a_n|\,|e^{2\pi i n z}| \leq L \sum_{n=0}^{\infty} (-1)^n \binom{-\nu-1}{n} e^{-2\pi n y} = L\,(1 - e^{-2\pi y})^{\nu-1}$$

This says that the series defining f is absolutely and uniformly convergent on compact subsets of $\mathcal{H}$, and, as $1 - e^{-2\pi y} = O(y)$, $|f(z)| = O(y^{-\nu-1})$.

□

Now we finish our proof for $e_2(z)$.

Take $a_n = \sum_{d|n,(d:N)=1} d$. It is clear that $a_n = O(n^2)$. Then, by the previous lemma, the defined series

$$e_2(z) = E_2(z) - \ N\ E_2(Nz) = \frac{-1}{24}\ (1 - N) + \ \sum_{n=1}^{\infty} \sigma(n)_N\ q^n$$

is a modular form of weight 2 for $\Gamma_0(N)$.

2.8 A congruence among modular forms of weight 2.

In this short section we recall the L-series of an elliptic curve and put together the two previous chapters: we show that if f the modular form associated to an elliptic curve E, of prime conductor N, and E having an ℓ $\mathbb{Q}$-torsion point, then there is a congruence modulo ℓ between f, and the Eisenstein series e_2 just defined.

2.8.1 A modular form for E.

Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. The L-series of E is defined, for $\mathrm{Re}(s) > 3/2$, by means of the following *Euler product*

$$L(E,s) = \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - a_p p^{-s})^{-1} = \sum_{n\geq 0} a_n n^{-s}$$

where $a_1 = 1$, for p prime a_p has been previously defined, and for any n, a_n is determined by the Euler product. That is, $a_{nm} = a_n a_m$ if n is prime to m, and for prime powers we have the recursions

$$a_{p^k} = a_p a_{p^{k-1}} - p a_{p^{k-2}} \quad \text{for } k \geq 2 \text{ and } p \nmid N$$
$$a_{p^k} = a_p^k \quad \text{for } k \geq 1 \text{ and } p \mid N.$$

Thanks to the work of Wiles and others, it is known that $L(E,s)$ extends to a holomorphic function on the whole complex plane and has a functional equation

$$\Lambda(E,s) = \omega \Lambda(E, 2-s) \tag{2.4}$$

where $\omega = \pm 1$ is the *sign of functional equation* and

$$\Lambda(E,s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(E,s).$$

The conjecture of Birch and Swinnerton-Dyer relates the central value $s = 1$ of this functional equation to arithmetic information of the curve. We will come back to this in the future.

Consider a normalized cusp form $f = \sum a_n q^n$, of level N and weight 2, that is an eigenfunction of all Hecke operators T_p: $T_p(f) = a_p f$. Its L-series is defined as

$$L(f,s) = \sum a_n n^{-s}.$$

L-series of modular forms were known to have Euler products and functional equations.

Eichler and Shimura proved that if the Fourier coefficients a_n are integers, then there exists an elliptic curve E_f defined over $\mathbb{Q}$ such that

$$L(E_f, s) = L(f, s).$$

The Shimura-Taniyama-Weil conjecture, now a theorem of Wiles, went in the other direction:

Theorem 2.8.1. *Let E be an elliptic curve of conductor N, defined over $\mathbb{Q}$. There exists a newform $f \in S_2(N)$ such that $L(E,s) = L(f,s)$. The curve E is isogenous to the elliptic curve E_f obtained by the Eichler-Shimura construction.*

The selected curve E_f in the isogeny class of E is known as the *strong Weil curve.*

The sign of the functional equation.

For more details see [13], chapter IX, §4.

Let $\alpha_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$.

Conjugation by α_N preserves $\Gamma_0(N)$.

The Atkin-Lehner involution is defined by

$$(W_N f)(z) = f|_{[\alpha_N]2} = \frac{1}{Nz^2} f(-1/Nz).$$

Then W_N preserves $M_2(\Gamma_0(N))$ and $S_2(\Gamma_0(N))$. Further, it is an involution.

Proposition 2.8.2. *Let $f \in S_2(\Gamma_0(N))$. Then $W_N f = -\epsilon f$ where ϵ is the sign of the functional equation* (2.4).

For a proof see [13] Theorem 9.8.

Note that, if the sign of the functional equation is -1 then the L-series $L(E, s)$ vanishes trivially at $s = 1$.

In the sequel, we will only consider elliptic curves with sign equal $+1$ at their functional equation. Thus, for these curves, the sign of the Atkin-Lehner involution is -1: $W_N f = -f$.

If N is composite, we have more operators of this kind. Suppose for simplicity that N is a square free integer. Then for each prime p dividing N we have an involution W_p given by the action of α_p on f. Set $\epsilon_p = \pm 1$ to be the sign in $W_p f = f|_{[\alpha_p]} = \epsilon_p f$ and $\epsilon_N = -\epsilon$ to be the sign of W_N. Then we have

$$\epsilon_N = \prod_{p|N} \epsilon_p. \tag{2.5}$$

If the sign of the functional equation is $+1$, then we will have an odd number of primes $p \mid N$ such that $\epsilon_p = -1$. In particular for N prime we have just one involution W_N with sign equal to -1.

2.8.2 Primes of bad reduction.

Now we can deal with primes of bad reduction, postponed in chapter 1.

The *conductor* N of an elliptic curve is defined as follows: if p is a prime, then the exponent of the conductor at p is

$$\begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2+e & \text{if } E \text{ has additive reduction at } p \end{cases}$$

where e is some number that depends on p and is 0 if $p \neq 2, 3$.

Then the set of primes that divides the conductor and the discriminant is the same, and p is of bad reduction if and only if $p \mid N$. Further, E has multiplicative reduction at p if and only if $\mathrm{ord}_p(N) = 1$.

Thus if N is square-free, E can only have multiplicative reduction at a bad prime p.

For primes of bad reduction we have the following

Proposition 2.8.3. *Let p be a prime dividing the conductor N, and W_p the corresponding Atkin-Lehner involution.*

Then $W_p(f) = \epsilon_p f$ and we have

$$a_p = \begin{cases} -\epsilon_p & p^2 \nmid N \\ 0 & p^2 \mid N \end{cases}$$

2.8.3 The congruence for N prime

We showed in the previous section that if $E/\mathbb{Q}$ is an elliptic curve of conductor N, having an ℓ torsion point, then for any prime p of good reduction,

$$a_p \equiv \sigma(p)_N.$$

Suppose the sign ϵ of the functional equation for the elliptic curve E is $+1$. If the conductor N is prime, then we only have one prime of bad reduction and

$$a_N = -\epsilon_N = \epsilon = 1$$

Then we also have $a_N \equiv \sigma(N)_N = 1 \mod \ell$.

Thus the modular form f of our elliptic curve E is congruent modulo the prime ℓ to the Eisenstein series e_2 defined above. That is

$$f \equiv e_2 \mod \ell$$

CHAPTER 3

The theta functions.

In this chapter we define modular forms of half integer weight, and give a proof, following Shimura's work [29], that Theta-series attached to a quadratic form in n-variables are modular forms of weight $n/2$.

3.1 Modular forms of half integer weight and the Theta series.

We will now define modular forms of *half integer weight* with the aid of the *Theta function*

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 \tau}.$$

For $\gamma \in SL_2(\mathbb{Z})$, set $j(\gamma, z) = (cz + d)$. It is a holomorphic function on the upper half plane $\mathcal{H}$, and it is a *1-cocycle*, that is

$$j(\gamma\beta, z) = j(\gamma, \beta z)j(\beta, z). \tag{3.1}$$

Thus a holomorphic function on the upper half plane is a modular form of integer weight k, if

$$\frac{f(\gamma z)}{f(z)} = j(\gamma, z)^k \tag{3.2}$$

plus holomorphy conditions at the cusps. Note that, if there is a function f that satisfies (3.2), j must satisfy (3.1).

In defining modular forms of half integer weight one is tempted to put $j(\gamma, z) = \sqrt{cz + d}$ as the square of such a form should be a modular form of integer weight. Here $\sqrt{\cdot}$ denotes the principal branch of the square root: we take $-\frac{\pi}{2} < \arg(\sqrt{z}) \leq \frac{\pi}{2}$. However, the fact that $\sqrt{zw}$ is not always $\sqrt{z}\sqrt{w}$ spoils it. Consider the two matrices

$$\alpha = \begin{pmatrix} N+1 & N \\ -N & 1-N \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 0 \\ -N & 1 \end{pmatrix}$$

both in $\Gamma(N)$, and thus in any congruence subgroup of level N.

Then $\alpha\beta = \begin{pmatrix} N+1-N^2 & N \\ -2N+N^2 & 1-N \end{pmatrix}$ and $j(\alpha\beta, z) = j(\alpha, \beta z)j(\beta, z)$ would give

$$\underbrace{\sqrt{(-2N+N^2)z+(1-N)}}_{\in\mathcal{H}} = \underbrace{\sqrt{-N\frac{Nz}{-Nz+1}+(1-N)}}_{\in 4\text{th quad}} \underbrace{\sqrt{-Nz+1}}_{\in 4\text{th quad}}$$

Thus the product in the right hand side lies in the lower half plane.

To fix this we need first to consider modular forms of integer weight with a character: for $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times$ a character, and f holomorphic on $\mathcal{H}$,

$$M_k(N,\chi) = \{f : f(\gamma z) = \chi(d)(cz+d)^k f(z) \forall \gamma \in \Gamma_o(N)\}$$

plus holomorphy conditions at cusps. Here, as usual $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. $M_k(N,\chi)$ will be the space of modular forms of weight k, level N and character χ. Then the square of a modular form of half integer weight, though we have no given a definition yet, will be a modular form of integer weight with a character.

3.2 Theta function.

We will first study the *Theta-function* and a transformation formula for it.

Recall the following properties of the Fourier transform $\widehat{f}$ of a function $f : \mathbb{R} \to \mathbb{C}$, twice continuously differentiable and rapidly decreasing at infinity.

- for $f(x) = e^{-\pi x^2}$ we have $\widehat{f} = f$
- $\widehat{f(ax)} = \frac{1}{a}\widehat{f}(\frac{x}{a})$
- $\widehat{f(x+a)} = e^{2\pi i a.x}\widehat{f}(x)$
- Poisson summation formula: $\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)$ (see (2.6.1)).

3.2.1 Transformation formula for θ.

Take a parameter $t > 0$ and consider the function $f_t(x) = e^{-2\pi t x^2}$, we have $\widehat{f_t}(y) = \frac{1}{\sqrt{2t}} e^{-2\pi y^2/4t}$.

The *theta-function* is defined for $\mathrm{Im}(\tau) > 0$ by

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 \tau}.$$

This series is absolutely and uniformly convergent in any $\mathrm{Im}(\tau) \geq t_0 > 0$ and it defines a holomorphic function for $\mathrm{Im}(\tau) > 0$.

Consider for $t > 0$, $\tau = it$, then $\theta(it) = \sum e^{-2\pi t n^2}$.
Then $\theta(it) = \sum f_t(n)$ and Poisson Summation formula gives

$$\sum_{n\in\mathbb{Z}} f_t(n) = \sum_{n\in\mathbb{Z}} \widehat{f}_t(n)$$

$$\theta(it) = \sum_{n\in\mathbb{Z}} e^{-2\pi t n^2} = \frac{1}{\sqrt{2t}} \sum_{n\in\mathbb{Z}} e^{-2\pi n^2/4t} = \frac{1}{\sqrt{2t}}\, \theta(\frac{-1}{4it}).$$

Consider now this last equation for $\tau \in \mathbb{C}$ and $\mathrm{Im}(\tau) > 0$

$$\theta(\tau) = \frac{1}{\sqrt{-2i\tau}}\ \theta(\frac{-1}{4\tau}) \tag{3.3}$$

where $\sqrt{\cdot}$ will always denote the principal branch of the square root. This equality still holds for *any* τ with $\mathrm{Im}(\tau) > 0$ as both sides are analytic functions on $\mathcal{H}$ and coincide when $\mathrm{Re}(\tau) = 0$.

Moreover, it is clear from the definition that $\theta(\tau + 1) = \theta(\tau)$. This is the "natural" candidate for a modular form of weight 1/2.

If we square both sides of the identity (3.3) we get that, for $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 4 & 0 \end{smallmatrix}\right) \in GL_2(\mathbb{Q})^+$

$$\theta^2|_{[\gamma]_1} = -i\theta^2.$$

Recall that $f|_{[\gamma]_k} = (\det\gamma)^{k/2}\,(c\tau + d)^{-k}\, f(\gamma\tau)$ if $\det\gamma \neq 1$.

Proposition 3.2.1. *The function θ^2 lies in $M_1(4, \chi)$, with $\chi(d) = (\frac{-1}{d})$.*

The group $\Gamma_0(4)$ is generated by $-I, T, ST^4S = \left(\begin{smallmatrix} -1 & 0 \\ 4 & -1 \end{smallmatrix}\right)$. It is clear that θ^2 has period 1 and that $\theta^2|_{[-I]_1} = -\theta^2 = \chi(-1)\theta^2$. As for $\left(\begin{smallmatrix} -1 & 0 \\ 4 & -1 \end{smallmatrix}\right)$, consider the matrix $\alpha_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Then $\alpha_N^{-1} = \frac{-1}{N}\alpha_N$ and

$$\begin{pmatrix} -1 & 0 \\ 4 & -1 \end{pmatrix} = -\alpha_4 T \alpha_4^{-1} = \frac{1}{4}\alpha_4 T \alpha_4$$

we have already proved that $\theta^2|_{[\alpha_4]_1} = -i\theta^2$. Thus we have

$$\theta^2|_{\alpha_4(T\alpha_4)} = (\theta^2|_{\alpha_4})|_{T\alpha_4} = -i\theta^2|_{T\alpha_4} = -i\theta^2|_{\alpha_4} = (-i)^2\theta^2 = -\theta^2 = (-1)^{-1}\theta^2.$$

So θ^2 has behaves correctly under the action of $\Gamma_0(4)$.

We still have to prove the cusp condition: that is, $\theta^2|_{[\gamma]_1}$ is finite at ∞ for every $\gamma \in \Gamma$. This depends only on the classes modulo $\Gamma_0(4)$, which has three cusps: $0, \infty, -1/2$. It is clear that θ^2 is holomorphic at 0 and ∞. We should check by hand the cusp $-1/2$; note that $TST^{-2}S(\frac{-1}{2}) = \infty$, where as usual $T : z \to z + 1$ and $S : z \to \frac{-1}{z}$. We thus should need a transformation formula for $\theta^2(\frac{-1}{z})$.

We will not prove this here, as we are going for a more general results.

Define

$$j(\gamma, z) = (\frac{c}{d})\, \epsilon_d^{-1}\, \sqrt{cz+d} \tag{3.4}$$

where

$$\epsilon_d = \left(\frac{-1}{d}\right)^{1/2} = \begin{cases} 1 & d \equiv 1(4) \\ i & d \equiv 3(4) \end{cases}$$

Proposition 3.2.2.

$$\theta(\gamma z) = j(\gamma, z)\theta(z), \text{ for every } \gamma \in \Gamma_0(4)$$

This will be a corollary of proposition 3.3.1.

Definition 3.2.3. *A holomorphic function on the upper half plane $\mathcal{H}$ is a modular form of half integer weight $k/2$ and level N if for every $\gamma \in \Gamma_0(N)$, $f(\gamma z) = j(\gamma, z)^k f(z)$ and it is holomorphic at the cusps of $\Gamma_0(N)$.*

We would like to prove a general result on theta series attached to quadratic forms. Roughly, the theta series of a positive definite integral quadratic form in n variables, will be a modular form of weight $n/2$.

3.2.2 Quadratic forms and Theta series.

Let $Q(x) = \frac{1}{2} x A x^t$ be a positive definite integral quadratic form in n variables (that is, A is an integral symmetric $n \times n$ matrix). The theta function associated to Q (or to A) is

$$\Theta_A(z) = \sum_{x \in \mathbb{Z}^n} e^{2\pi i Q(x) z} = 1 + \sum_{n=1}^{\infty} a_Q(n)\, e^{2\pi i n z}.$$

For Q, a quadratic form in n variables, $\Theta_A(z)$ is a modular form of weight $k = n/2$, a certain level N and some character.

Note that, as Q is positive definite there is a constant C such that $Q(x) \geq C \sum_{i=1}^n x_i$. Let $z = \sigma + iy$. Then we have

$$\left| e^{2\pi i Q(x) z} \right| = e^{-2\pi y Q(x)} \leq \sum_{i=1}^{n} e^{-2\pi y C x_i^2}$$

and this gives

$$\left| \sum_{x \in \mathbb{Z}^n} e^{2\pi i Q(x) z} \right| \leq \sum_{x \in \mathbb{Z}} (e^{-2\pi y C x^2})^n$$

Then $\Theta_A(z)$ is absolutely and uniformly convergent in any region $\mathrm{Im}(z) \geq y_0 > 0$ and it defines a holomorphic function on the upper half plane $\mathcal{H}$.

We will see transformation formulas for $\Theta_A(\tau)$, under the action of $\gamma \in \Gamma_0(N)$, that will give us the following

Proposition 3.2.4. *Let $Q(x) = x^t Ax/2$ be a positive definite integral quadratic form in n variables. Then the* Theta-series *attached to Q, or to A*

$$\Theta_A = \sum_{m \in \mathbb{Z}^n} e^{2\pi i z m^t A m/2}$$

is a modular form of weight $n/2$, level N equal to the level of A, and some character. If n is even, the character is trivial.

This will be a corollary of proposition 3.3.1 below.

3.3 Transformation formula for Θ_A.

We need to extend the definition of the Kronecker symbol for any $a \in \mathbb{Z}$ and any *odd* non-zero integer b.

- if $(a, b) > 1$ then $\left(\frac{a}{b}\right) = 0$
- if b is an odd prime, then $\left(\frac{a}{b}\right)$ is the ordinary quadratic residue symbol.
- for $b > 0$, the map $a \to \left(\frac{a}{b}\right)$ defines a character modulo b.
- if $a \neq 0$, then the map $b \to \left(\frac{a}{b}\right)$ defines a character modulo a divisor of $4a$, whose conductor is the discriminant of $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$.
- $\left(\frac{a}{-1}\right) = 1$ or -1 according as $a > 0$ or $a < 0$.
- $\left(\frac{0}{\pm 1}\right) = 1$

Note that this does not agree with the traditional symbol with the property $\left(\frac{a}{b}\right) = \left(\frac{a}{|b|}\right)$. In fact we have $\left(\frac{a}{b}\right) = \eta\left(\frac{a}{b}\right)$ where $\eta = 1$ unless *both* a and b are negative.

We have the following setting:

Let n be a positive integer. A will be a positive definite symmetric matrix of size n, with integer entries, and N a positive integer. All vectors will be n-column vectors.

For a fixed $h \in \mathbb{Z}^n$ consider the theta-function

$$\theta(z; h, A, N) = \sum_{m \equiv h(N)} e^{2\pi i z m^t A m/2N^2}$$

the summation being over all $m \in \mathbb{Z}^n$ with $m \equiv h(N\mathbb{Z}^n)$.

We impose the following conditions: A and NA^{-1} have coefficients in $\mathbb{Z}$, and $Ah \in N\mathbb{Z}^n$. We will request the diagonal entries of A to be even. However we will not ask NA^{-1} to have even diagonal. Thus the *level* of the matrix A may be as well N or $2N$.

Note that $NA^{-1} \in \mathbb{Z}^{n \times n}$ implies that $\det(A)$ is a divisor of N^n. We put $D = \det(A)$.

Following [29], we will prove the following result.

Proposition 3.3.1. *Let $\theta(z;h,A,N)$ be the theta series just defined, under the conditions on A,h,N stated. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, with c even and $c \equiv 0(N)$. Then the following transformation formula holds:*

$$\theta(\gamma z;h,A,N) = e^{2\pi i a b h^t A h/2N^2} \left(\frac{D}{d}\right) \left(\frac{2c}{d}\right)^n \epsilon_d^{-n} (cz+d)^{n/2} \theta(z;ah,A,N)$$

where ϵ_d is 1 or i according as $d \equiv 1$ or 3 modulo 4. Note that d is odd as $\det\gamma = 1$ and c is even.

If also NA^{-1} has even diagonal entries, then the equality holds for all $\gamma \in \Gamma_0(N)$.

If we set $h = 0$ in the above formula we have:

$$\theta(z;0,A,N) = \sum_{m \equiv 0(N)} e^{2\pi i z m^t A m/2N^2} = \sum_{m \in \mathbb{Z}^n} e^{2\pi i z m^t A m/2}$$

which is the theta-function θ_A associated to the quadratic form A, of level N or $2N$. The proposition then gives us

$$\theta_A(\gamma z) = (\frac{D}{d}) \left(\frac{2c}{d}\right)^n \epsilon_d^{-n} (cz+d)^{n/2} \theta_A(z)$$

for all $\gamma \in \Gamma_0(2N)$.

If, in particular, $n = 1$ and $A = (2)$ we have that A has level 4, and 2 is the least N such that NA^{-1} has integer entries; $D = \det(A) = 2$, and θ_A is the ordinary theta-function $\sum_{m \in \mathbb{Z}} e^{2\pi i m^2 z}$. The following transformation rule holds for $\gamma \in \Gamma_0(4)$:

$$\theta(\gamma z) = (\frac{c}{d})\, \epsilon_d^{-1} (cz+d)^{1/2}\, \theta(z).$$

3.3.1 Three transformation formulas.

The following transformation formulas will be needed in the proof of proposition (3.3.1).

1. $\theta(-1/z;h,A,N) = D^{-1/2}(-iz)^{n/2} \sum_{\substack{k \bmod N \\ Ak \equiv 0(N)}} e^{2\pi i k^t A h/N^2} \theta(z;k,A,N)$

2. $\theta(z+a;h,A,N) = e^{2\pi i a h^t A h/2N^2} \theta(z;h,A,N)$
   for any $a \in \mathbb{Z}$, if A has even diagonal.

3. $\theta(z;h,A,N) = \sum_{\substack{g \bmod cN \\ g \equiv h(N)}} \theta(cz;g,cA,cN)$
   for any $c \neq 0$.

Remark 3.3.2. *Note that this means that for any $\gamma \in SL_2(\mathbb{Z})$ the functions $\theta(z, h, A, N)$ are holomorphic functions at infinity. Any of these acted by a γ can be expressed, by applying (1) and (2) a finite number of times, as a linear combination of $\theta' s(z, *, A, N)$, (all with period 1 as A has even diagonal), and thus have a Fourier expansion with no negative terms.*

These transformation formulas give us the holomorphy condition at cusps.

Proofs

1. $\theta(-1/z; h, A, N) = D^{-1/2}(-iz)^{n/2} \sum_{\substack{k \bmod N \\ Ak \equiv 0(N)}} e^{2\pi i k^t Ah/N^2} \theta(z; k, A, N)$

We will apply Poisson summation formula to the function $f : \mathbb{R}^n \to \mathbb{C}$, $f(x) = e^{2\pi i z(x+\frac{h}{N})^t A(x+\frac{h}{N})/2}$. The transformation formula will follow from the equality

$$\sum_{m\in\mathbb{Z}^n} f(m) = \sum_{m\in\mathbb{Z}^n} \widehat{f}(m).$$

Note that

$$\begin{aligned}\sum_{m\in\mathbb{Z}^n} f(m) &= \sum_{m\in\mathbb{Z}^n} e^{2\pi i z(m+\frac{h}{N})^t A(m+\frac{h}{N})/2} = \sum_{m\in\mathbb{Z}^n} e^{2\pi i z(mN+h)^t A(mN+h)/2N^2} \\ &= \sum_{r\equiv h(N)} e^{2\pi i z r^t Ar/2N^2} = \theta(z; h, A, N).\end{aligned}$$

Believe for a moment that $\widehat{f}(x) = (\frac{i}{z})^{n/2} \frac{1}{\sqrt{D}} e^{2\pi i u.x} e^{-\pi i x^t A^{-1} x/z}$ (for a proof of this result look at the appendix (3.3.3) at the end of this chapter).

Then

$$\begin{aligned}\theta(z; h, A, N) &= \sum_{m\in\mathbb{Z}^n} \widehat{f}(m) \\ &= \left(\frac{i}{z}\right)^{n/2} \frac{1}{\sqrt{D}} \sum_{m\in\mathbb{Z}^n} e^{2\pi i h^t m/N} e^{-\pi i m^t A^{-1} m/z}\end{aligned}$$

and, changing z by $-1/z$

$$\begin{aligned}\theta(\frac{-1}{z};h,A,N) &= (\frac{(-iz)^{n/2}}{\sqrt{D}}\sum_{m\in\mathbb{Z}^n} e^{2\pi i h^t m/N}\ e^{2\pi i z m^t A^{-1} m/2}\\ &\underset{(\mathbf{1})}{=} (\frac{(-iz)^{n/2}}{\sqrt{D}}\sum_{\substack{r\in\mathbb{Z}^n\\ Ar\equiv 0(N)}} e^{2\pi i h^t Ar/N^2}\ e^{2\pi i z (Ar)^t A^{-1} Ar/2N^2}\\ &\underset{(\mathbf{2})}{=} (\frac{(-iz)^{n/2}}{\sqrt{D}}\sum_{\substack{k \bmod N\\ Ak\equiv 0(N)}}\ \sum_{r\equiv k(N)} e^{2\pi i h^t Ar/N^2}\ e^{2\pi i z r^t Ar/2N^2}\\ &\underset{(\mathbf{3})}{=} (\frac{(-iz)^{n/2}}{\sqrt{D}}\sum_{\substack{k \bmod N\\ Ak\equiv 0(N)}} e^{2\pi i h^t Ak/N^2}\ \sum_{r\equiv k(N)} e^{2\pi i z r^t Ar/2N^2}\\ &= (\frac{(-iz)^{n/2}}{\sqrt{D}}\sum_{\substack{k \bmod N\\ Ak\equiv 0(N)}} e^{2\pi i h^t Ak/N^2}\ \theta(z;k,A,N).\end{aligned}$$

In (**1**) we write $m = \frac{1}{N}A(NA^{-1}m)$ and set $r = NA^{-1}m$. Note that $r \in Z^n$ as NA^{-1} has integer entries, and $Ar \equiv 0(N)$ as $Ar = Nm$. The set of vectors $m \in \mathbb{Z}^n$ corresponds with the set of vectors $r \in \mathbb{Z}^n$ such that $Ar \equiv 0(N)$. Thus we can replace in the left hand side of (1) m by $\frac{1}{N}Ar$ and sum over all the $r \in \mathbb{Z}^n$ with $Ar \equiv 0(N)$.

In (**2**) we separate in classes modulo k. Note that if $r \equiv k(N)$, $Ar \equiv 0(N)$ if and only if $Ak \equiv 0(N)$.

In (**3**) note that $e^{2\pi i h^t Ar/N^2}$ depends only on $r \bmod N$ as if $r = Nm + k$, $e^{2\pi i h^t A(mN+k)/N^2} = e^{2\pi i h^t Am/N}\ e^{2\pi i h^t Ak/N^2}$ and as $h^t A/N$ is integer by assumption, the first factor of the last equality is equal to 1.

2. $\theta(z+a;h,A,N) = e^{2\pi i a h^t Ah/2N^2}\theta(z;h,A,N)$
if either we assume the diagonal of the matrix A is even, or, the integer a is even.

Let a be an integer.
$\theta(z+a;h,A,N) = \sum_{m\equiv h(N)} e^{2\pi i(z+a)m^t Am/2N^2} = \sum_{m\equiv h(N)} e^{2\pi i z m^t Am/2N^2} e^{2\pi i a m^t Am/2N^2}$
As $m \equiv h(N)$ write $m = h + rN$, then

$$\begin{aligned}am^t Am/2N^2 &= a(h+rN)^t A(h+rN)/2N^2\\ &= ah^t Ah/2N^2 + 2aNr^t Ah/2N^2 + aN^2 r^t Ar/2N^2.\end{aligned}$$

The last term, $ar^t Ar/2$, is clearly an integer if the diagonal of A is even or $a = 2\alpha$ is even. The term $2aNr^t Ah/2N^2 = ar^t Ah/N$ is always integer, as $Ah \equiv 0(N)$. Then $e^{2\pi i a m^t Am/2N^2} = e^{2\pi i a h^t Ah/2N^2}$ if A has even diagonal or the integer a is an even number, and the result follows,

$$\theta(z+a;h,A,N) = e^{2\pi i a h^t Ah/2N^2}\sum_{m\equiv h(N)} e^{2\pi i z m^t Am/2N^2} = e^{2\pi i a h^t Ah/2N^2}\theta(z;h,A,N).$$

3. $\theta(z;h,A,N) = \sum_{\substack{g \bmod cN \\ g\equiv h(N)}} \theta(cz;g,cA,cN)$

Let c be a positive integer

$$\begin{aligned}\theta(z;h,A,N) &= \sum_{m\equiv h(N)} e^{2\pi i z m^t Am/2N^2} = \sum_{m\equiv h(N)} e^{2\pi i (cz) m^t (cA) m/2(cN)^2} \\ &\underset{(\mathbf{1})}{=} \sum_{\substack{g \bmod Nc \\ g\equiv h(N)}} \sum_{m\equiv g(cN)} e^{2\pi i (cz) m^t (cA) m/2(cN)^2} \\ &= \sum_{\substack{g \bmod Nc \\ g\equiv h(N)}} \theta(cz;g,cA,cN)\end{aligned}$$

For (**1**), the sum on the left is over all $m = Nr + h$, with any $r \in \mathbb{Z}^n$. separate on congruences modulo Nc writing every such m as $m = (Nc)k + Na + h$ with k any integer vector, and a in a set of vector classes modulo c. The classes mod cN equivalent to h modulo N, are the vector classes of $\{(Na + h)\}$.

3.3.2 Proof of proposition 3.3.1.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Note that $c\gamma(z) = a + \frac{-1}{cz+d}$ and apply the transformation formulas (3), (2) and (1) of the last section, in the order mentioned, to $\theta(\gamma z;h,A,N)$:

$$\begin{aligned}\theta(\gamma z;h,A,N) &= \sum_{\substack{g \bmod cN \\ g\equiv h(N)}} \theta(c\gamma z;g,cA,cN) = \sum_{\substack{g \bmod cN \\ g\equiv h(N)}} \theta(a + \frac{-1}{cz+d};g,cA,cN) \\ &= \sum_{\substack{g \bmod cN \\ g\equiv h(N)}} e^{2\pi i a g^t cAg/2(cN)^2} \theta(\frac{-1}{cz+d};g,cA,cN)\end{aligned}$$

And, applying (1) this equals

$$= \frac{(-i(cz+d))^{n/2}}{c^{n/2}\sqrt{D}} \sum_{\substack{g \bmod cN \\ g\equiv h(N)}} e^{2\pi i a g^t Ag/2cN^2} \sum_{\substack{k \bmod cN \\ cAk\equiv 0(cN)}} e^{2\pi i k^t Ag/cN^2} \theta(cz+d;k,cA,cN)$$

Now, $cAk \equiv 0(cN)$ if and only if $Ak \equiv 0(N)$, applying (2) to $\theta(cz+d;k,cA,cN)$,

inverting the order of summation and gathering the exponentials, we get

$$\theta(\gamma z;h,A,N) = \frac{(-i(cz+d))^{n/2}}{c^{n/2}\sqrt{D}} \times \sum_{\substack{(k \mod cN)\\ Ak\equiv 0(N)}} \sum_{\substack{(g \mod cN)\\ g\equiv h(N)}} e^{2\pi i(ag^tAg+2k^tAg+dk^tAk)/2cN^2}\theta(cz;k,cA,cN) \tag{3.5}$$

And as $\theta(cz;k,cA,cN)$ does not depend on g we can write

$$\theta(\gamma z;h,A,N) = \frac{(-i(cz+d))^{n/2}}{c^{n/2}\sqrt{D}} \sum_{\substack{(k \mod cN)\\ Ak\equiv 0(N)}} \theta(cz;k,cA,cN)\ \Phi(h,k)$$

where $\Phi(h,k)$ depends on c, N and A and is defined by

$$\Phi(h,k) = \sum_{\substack{(g \mod cN)\\ g\equiv h(N)}} e^{2\pi i(ag^tAg+2k^tAg+dk^tAk)/2cN^2}$$

Believe for a moment that $\Phi(h,k)$ depends only on $k \mod N$ and not on $k \mod cN$, then we split the sum

$$\sum_{\substack{(k \mod cN)\\ Ak\equiv 0(N)}} \Phi(h,k)\ \theta(cz;k,cA,cN) = \sum_{\substack{(g \mod N)\\ Ag\equiv 0(N)}} \Phi(h,g) \sum_{\substack{(k \mod cN)\\ k\equiv g(N)}} \theta(cz;k,cA,cN)$$

and applying (3)

$$\sum_{\substack{(k \mod cN)\\ Ak\equiv 0(N)}} \Phi(h,k)\ \theta(cz;k,cA,cN) = \sum_{\substack{(g \mod N)\\ Ag\equiv 0(N)}} \Phi(h,g)\ \theta(z;g,A,N)$$

Gathering with equation (3.5)

$$\theta(\frac{az+b}{cz+d};h,A,N) = \frac{(-i(cz+d))^{n/2}}{c^{n/2}\sqrt{D}} \sum_{\substack{(g \mod N)\\ Ag\equiv 0(N)}} \Phi(h,g)\ \theta(z;g,A,N) \tag{3.6}$$

Replace z by $-1/z$ in (3.6)

$$\theta(\frac{bz-a}{dz-c};h,A,N) = \frac{(-i(c\frac{-1}{z}+d))^{n/2}}{c^{n/2}\sqrt{D}} \sum_{\substack{(g \mod N)\\ Ag\equiv 0(N)}} \Phi(h,g)\ \theta(\frac{-1}{z};g,A,N) \tag{3.7}$$

apply (1)

$$\theta(\frac{-1}{z};g,A,N) = \frac{(-iz)^{n/2}}{\sqrt{D}} \sum_{\substack{(\ell \mod N)\\ A\ell\equiv 0(N)}} e^{2\pi i\ell^tAg/N^2}\ \theta(z,\ell,A,N)$$

We insert this in (3.7) and change the order of summation.

From here on we will assume c to be positive. This condition is not restrictive, as we will see at the end of the proof.

Note that, for $c > 0$, $((-i)(\frac{-c}{z} + d))^{1/2}(-iz)^{1/2} = (\mathrm{sg}(d)i)(dz - c)^{1/2}$ (see section (3.3.3) 3.).

$$\theta(\frac{bz-a}{dz-c}; h, A, N) = \frac{(-\mathrm{sg}(d)i)^n (dz-c)^{n/2}}{c^{n/2} D} \times \sum_{\substack{(\ell \bmod N) \\ A\ell \equiv 0(N)}} \{ \sum_{\substack{(g \bmod N) \\ Ag \equiv 0(N)}} e^{2\pi i \ell^t Ag/N^2} \ \Phi(h,g)\} \theta(z, \ell, A, N) \tag{3.8}$$

Now, (see section (3.3.3) 2.)

$$\Phi(h,g) = e^{-b2\pi i(dg^t Ag + 2g^t Ah)/2N^2} \ \Phi(h + dg, 0).$$

Suppose that $d \equiv 0(N)$, then $dg^t Ag/2N^2$ is an integer as $Ag \equiv 0(N)$ and thus $e^{-b2\pi i dg^t Ag/2N^2} = 1$ and

$$\Phi(h + dg, 0) = \sum_{\substack{k \bmod cN \\ k \equiv h + dg(N)}} e^{2\pi i a k^t Ak}/2cN^2 = \sum_{\substack{k \bmod cN \\ k \equiv h(N)}} e^{2\pi i a k^t Ak}/2cN^2 = \Phi(h,0)$$

Then $\Phi(h,g) = e^{-b2\pi i g^t Ah/N^2} \ \Phi(h,0)$ and replacing this in the inner summand of equation (3.8) we have:

$$\sum_{\substack{g \bmod N \\ Ag \equiv 0(N)}} e^{2\pi i \ell^t Ag/N^2} \ \Phi(h,g) = \sum_{\substack{g \bmod N \\ Ag \equiv 0(N)}} e^{2\pi i \ell^t Ag/N^2} \ e^{-b2\pi i g^t Ah/N^2} \ \Phi(h,0)$$
$$= \Phi(h,0) \sum_{\substack{g \bmod N \\ Ag \equiv 0(N)}} e^{2\pi i (\ell - bh)^t Ag/N^2}$$

Note that (see section (3.3.3) 4.)

$$\sum_{\substack{g \bmod N \\ Ag \equiv 0(N)}} e^{2\pi i (\ell - bh)^t Ag/N^2} = \begin{cases} D = \det(A) & \text{if } \ell \equiv bh(N) \\ 0 & \text{if } \ell \not\equiv bh(N) \end{cases}$$

We replace in (3.8),

$$\theta(\frac{bz-a}{dz-c}; h, A, N) = \frac{(-\mathrm{sg}(d)i)^n (dz-c)^{n/2}}{c^{n/2}} \ \Phi(h,0) \underbrace{\sum_{\substack{(\ell \bmod N) \\ A\ell \equiv 0(N), \ell \equiv bh(N)}} \theta(z, \ell, A, N)}_{\theta(z, bh, A, N)}$$

as $\Phi(h,0)$ does not depend on ℓ, and the sum

$$\sum_{\substack{(\ell \bmod N) \\ A\ell \equiv 0(N), \ell \equiv bh(N)}} \theta(z, \ell, A, N) = \theta(z, bh, A, N)$$

as there is only one term $\ell \equiv bh \mod N : bh$. Recall that $Ah \equiv 0(N)$ by assumption.

Therefore, writing $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $\begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$ we have, for $d < 0$, $c \equiv 0(N)$ and even:

$$\theta(\frac{az+b}{cz+d}; h, A, N) = (-\operatorname{sg}(c)i)^n (cz+d)^{n/2}\ W\theta(z, ah, A, N) \tag{3.9}$$

where $W = \dfrac{1}{|d|^{n/2}} \displaystyle\sum_{\substack{g \mod dN \\ g \equiv h(N)}} e^{-b2\pi i g^t Ag/2|d|N^2}$.

As $ad - bc = 1$, $ad \equiv 1(N)$. Write $g = adh + Nu$ where u is a vector modulo d. The exponent in the sum in W now becomes

$g^t Ag = (adh + Nu)^t A(adh + Nu) = (ad)^2 h^t Ah + \underbrace{2adNh^t Au}_{\equiv 0(2dN^2) \text{ as } Ah \equiv 0(N)} + N^2 u^t Au$

which gives

$$W = |d|^{-n/2} e^{-b2\pi i (ad)^2 h^t Ah/2|d|N^2} \sum_{u \mod d} e^{-b2\pi i u^t Au/2|d|}$$

Further, $\frac{-b(ad)^2}{|d|} = ab(ad)$ and, as $ad \equiv 1(N)$ and $Ah \equiv 0(N)$, $e^{-b2\pi i (ad)^2 h^t Ah/2|d|N^2} = e^{2\pi i abh^t Ah/2N^2}$, so (3.9) becomes

$$\theta(\frac{az+b}{cz+d}; h, A, N) = (-\operatorname{sg}(c)i)^n (cz+d)^{n/2}\ e^{2\pi i abh^t Ah/2N^2} \omega(-b, |d|)\theta(z, ah, A, N) \tag{3.10}$$

where we have set

$$\omega(-b, |d|) = |d|^{-n/2} \sum_{u \mod d} e^{-b2\pi i u^t Au/2|d|}$$

We will now investigate $\omega(-b, |d|)$.

Recall $d < 0$, c is even and $\equiv 0(N)$, $ad - bc = 1$. If $c = 0$, then $d = -1$ and $\omega(-b, |d|) = 1e^0 = 1$. Thus, let us suppose $c \neq 0$, and change z by $z + 4m$ in (3.10): thus, for

$$\theta(\frac{az+b+4am}{cz+d+4cm}; h, A, N)$$

we can simply replace z by $z+4m$ in both sides of equality (3.10), or we can suppose we are acting by the matrix

$$\begin{pmatrix} a & b+4am \\ c & d+4cm \end{pmatrix} \in SL_2(\mathbb{Z})$$

where we impose $cm < 0$ (then $d + 4cm < 0$). Comparing these two equalities gives

$$\omega(-b, |d|) = \omega(-b - 4am, |d + 4cm|)$$

As c is even, d is an odd integer and thus coprime to $4c$. Take m such that $-(d+4cm)=p$ is a prime number, and set $\beta=-b-4am$. Note

$$\begin{pmatrix} a & -\beta \\ c & -p \end{pmatrix} = \begin{pmatrix} a & b+4am \\ c & d+4cm \end{pmatrix}, \quad \text{then } -ap+\beta c = 1$$

Thus p is prime to β, c and then to N and $\det(A)$. Note also that $p=-d-4cm \equiv -d(4N)$ as $c\equiv 0(N)$; and $p\equiv -d(4c)$.

Now we analyze

$$\omega(\beta,p) = p^{-n/2} \sum_{u \mod p} e^{2\pi i \beta u^t A u/2p}.$$

We have

- A can be diagonalized modulo p. Suppose $2q_1,...,2q_n$ are the diagonal elements, then

$$\omega(\beta,p) = p^{-n/2} \left(\frac{(2\beta)^n q_1...q_n}{p}\right) g_\chi^n$$

where g_χ is the Gauss sum $g_\chi(1)$ associated to the character $\chi(n)=(\frac{n}{p})$:

$$g_\chi = \sum_{x=0}^{p-1} (\frac{n}{p})\ e^{2\pi i x/p}$$

For a (very short) summary on Gauss sums see section (3.3.3) 5.

As $\det A$ is prime to p, there exist a matrix $S\in M_n(\mathbb{Z})$, $(\det(S),p)=1$ such that $A \underset{\mod p}{\equiv} S^t D S$, where D is a diagonal matrix with entries $2q_1,...,2q_n$. Thus

$$\sum_{\substack{x \mod p \\ x\in\mathbb{Z}^n}} e^{2\pi i\beta (Sx)^t D(Sx)/2p} \underset{y=Sx}{=} \sum_{\substack{y \mod p \\ y\in\mathbb{Z}^n}} e^{2\pi i\beta(\sum q_i y_i^4)/p} = \prod_{i=1}^n \left(\sum_{y=1}^p e^{2\pi i\beta q_i y^2/p}\right)$$

Now

$$\sum_{y=1}^p e^{2\pi i\beta q_i y^2/p} = \sum_{x=1}^p \left(1+\left(\frac{x}{p}\right)\right)\ e^{2\pi i\beta q_i x/p} = \sum_{x=1}^p \left(\frac{x}{p}\right)\ e^{2\pi i\beta q_i x/p}$$

as being $\psi(x)=e^{2\pi i\beta q_i x/p}$ a primitive character mod p, its sum over the integers mod p equals zero. For the sum

$$\sum_{x=1}^p \left(\frac{x}{p}\right)\ e^{2\pi i\beta q_i x/p} = g_\chi(\beta q_i) = \left(\frac{\beta q_i}{p}\right)\ g_\chi.$$

With this the result follows, that is

$$w(\beta,p) = p^{-n/2}\left(\frac{\beta^n q_1...q_n}{p}\right) g_\chi^n = p^{-n/2}\left(\frac{(2\beta)^n 2q_1...2q_n}{p}\right)$$

- $g_\chi = \epsilon_p p^{1/2}$, thus we have
$$p^{-n/2}\, g_\chi^n = \epsilon_p^n$$

Then
$$\omega(\beta, p) = \epsilon_p^n \left(\frac{(2\beta)^n 2q_1 ... 2q_n}{p}\right) = \epsilon_p^n \left(\frac{(2\beta)^n D}{p}\right)$$

$D = \det(A) \underset{(p)}{\equiv} \det(S)^2 2q_1 ... 2q_n$.

For any $a \neq 0$, $(\frac{a}{\cdot})$ is a character of conductor a divisor of $4a$. Write $D = D_0 K^2$. As D divides N^n, D_0 must divide N.

Thus
$$\left(\frac{D}{p}\right) = \left(\frac{D_0}{p}\right) \underset{(\mathbf{1})}{=} \left(\frac{D_0}{-d}\right) = \left(\frac{D}{-d}\right) = \left(\frac{D}{|d|}\right) \underset{(\mathbf{2})}{=} \left(\frac{D}{d}\right)$$

(**1**): $(\frac{D_0}{\cdot})$ has conductor dividing $4D_0$ and $p \equiv -d(4N)$ implies that $p \equiv -d(4D_0)$

(**2**): $D > 0$ as A is a positive definite matrix (see the definition of $\left(\frac{a}{b}\right)$)

For $\left(\frac{2\beta}{p}\right)$ note that $\beta c^2 = c + apc$ and $p \equiv -d(4c)$

$$\left(\frac{2\beta}{p}\right) = \left(\frac{2c}{p}\right) = \left(\frac{2c}{-d}\right) = \left(\frac{2c}{|d|}\right) = \mathrm{sg}(c) \left(\frac{2c}{d}\right)$$

Note that $p \equiv -d(4) \Rightarrow \epsilon_p = \epsilon_{-d}$

Thus we have

$$\omega(\beta, p) = \epsilon_{-d}^n \,\mathrm{sg}(c)^n \left(\frac{2c}{d}\right)^n \left(\frac{D}{d}\right) \underset{(*)}{=} \epsilon_d^{-n} (\mathrm{sg}(c) i)^n \left(\frac{c}{d}\right)^n \left(\frac{D}{d}\right)$$

$(*)$: $\epsilon_{-d} = i\epsilon_d^{-1}$

Inserting this in (3.10) we obtain the result

$$\theta(\frac{az+b}{cz+d}; h, A, N) = e^{2\pi i abh^t Ah/2N^2} \left(\frac{D}{d}\right) \left(\frac{2c}{d}\right)^n \epsilon_d^{-n} (cz+d)^{n/2}\ \theta(z, ah, A, N)$$

for c even and $\equiv 0 \mod N$. If $d > 0$ the formula can be obtained replacing γ by $-\gamma$. □

Now take $h = 0$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then we have the following

Proposition 3.3.3. *Let A be the matrix of an integral positive definite quadratic form in n variables. Let N be the least integer such that NA^{-1} has integer even entries and let $D = \det(A)$. Then the theta-series attached to A verifies*

$$\Theta_A(\gamma z) = \left(\frac{2^n D}{d}\right) \left(\frac{c}{d}\right)^n \epsilon_d^{-n} (cz+d)^{n/2}\ \Theta_A(z)$$

or

$$\Theta_A(\gamma z) = \left(\frac{2^n D}{d}\right) j(\gamma, z)^n \, \Theta_A(z)$$

for any γ in $\Gamma_0(N)$. Further, as we have already seen that this theta-function is holomorphic at cusps, it is a modular form of weight $n/2$, level N equal to the level of the matrix A and character $\chi(d) = \left(\frac{2^n D}{d}\right)$.

3.3.3 Appendix to this chapter.

1. **The Fourier transform of $f(x) = e^{2\pi i z(x+\frac{h}{N})^t A(x+\frac{h}{N})/2}$**

   Consider $g(x) = e^{2\pi i z x^t A x/2}$. Thus $f(x) = g(x + \frac{h}{N})$, and so $\widehat{f}(x) = e^{2\pi i \frac{h}{N}.x} \, \widehat{g}(x)$. Thus we calculate $\widehat{g}(x)$.

$$\widehat{g}(x) = \int_{\mathbb{R}^n} e^{2\pi i z s^t A s/2} \, e^{-2\pi i x^t s} \, ds = \int_{\mathbb{R}^n} e^{\pi i z (s^t A s - \frac{2}{z} s^t x)}$$

   Completing the square in $s^t A s - \frac{2}{z} s^t x$ we have
   $s^t A s - \frac{2}{z} s^t x = s^t A s - 2 s^t A (A^{-1}\frac{x}{z}) + x^t A^{-1} x/z^2 - x^t A^{-1} x/z^2 = (s - A^{-1}\frac{x}{z})^t A (s - A^{-1}\frac{x}{z}) - x^t A^{-1} x/z^2$, which gives

$$\begin{aligned} \widehat{g}(x) &= \int_{\mathbb{R}^n} e^{\pi i z (s - A^{-1}\frac{x}{z})^t A (s - A^{-1}\frac{x}{z})} \, e^{-\pi i z x^t A^{-1} x/z^2} \, ds \\ &= e^{-\pi i x^t A^{-1} x/z} \int_{\mathbb{R}^n} e^{\pi i z (s - A^{-1}\frac{x}{z})^t A (s - A^{-1}\frac{x}{z})} \, ds \end{aligned}$$

   Write $A = B^t B$ with B a real invertible matrix. Then $(s - A^{-1}\frac{x}{z})^t A (s - A^{-1}\frac{x}{z}) = (Bs - BA^{-1}\frac{x}{z})^t (Bs - BA^{-1}\frac{x}{z})$. Put $w = BA^{-1}\frac{x}{z}$ and $u = Bs$. Thus $du = \det B \, ds = \sqrt{\det A} \, ds$ and

$$\int_{\mathbb{R}^n} e^{\pi i z (s - A^{-1}\frac{x}{z})^t A (s - A^{-1}\frac{x}{z})} \, ds = \frac{1}{\sqrt{\det A}} \int_{\mathbb{R}^n} e^{\pi i z (u+w)^t (u+w)} \, du$$

   Which, separating the integral in n integrals $\int_{\mathbb{R}} e^{\pi i z (u_i + w_i)^2} du_i$, and by Cauchy's theorem on the following contour

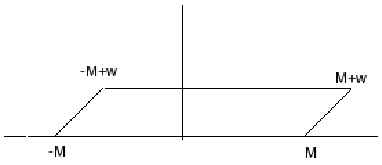

Figure 3.1:

we have

$$\widehat{g}(x) = \frac{e^{-\pi i x^t A^{-1} x/z}}{\sqrt{\det A}} \left(\int_{\mathbb{R}} e^{\pi i z u^2} \, du \right)^n$$

as the integrals on each of the line segments $\pm M + tw_i$, $t \in [0,1]$, $w = (w_1, ..., w_n)^t$, go to zero as $M \to \infty$ for $\mathrm{Im}(z) > 0$. Call $I = \int_{\mathbb{R}} e^{\pi i z u^2} \, du$, then, as usual, change to polar coordinates to calculate $I^2 = \int_{\mathbb{R}} e^{\pi i z (u^2+v^2)} \, du dv \; = \; \frac{i}{z}$

Write $z = a + bi$ and note that $\mathrm{Re}(I) > 0$ as well as $\mathrm{Re}(\frac{i}{z}) > 0$, which gives $I = \sqrt{\frac{i}{z}}$.

Putting things together gives

$$\widehat{f}(x) = e^{2\pi i \frac{h}{N}.x} \; \frac{e^{-\pi i x^t A^{-1} x/z}}{\sqrt{\det A}} \left(\frac{i}{z} \right)^{n/2}$$

2. **An equality for $\Phi(h,k)$**

$$\Phi(h,k) = \sum_{\substack{g \bmod cN \\ g \equiv h (N)}} e^{2\pi i (a g^t A g + 2 k^t A g + d k^t A k)/2cN^2}$$

We try to complete the square in $a g^t A g + 2 k^t A g + d k^t A k$. Write:

$a(g+dk)^t A (g+dk) = a g^t A g + 2ad k^t A g + (ad) d k^t A k \overset{ad=1+bc}{=} a g^t A g + 2 k^t A g + d k^t A k + 2bc k^t A g + bcd k^t A k$. Then

$$\Phi(h,k) = \sum_{\substack{g \bmod cN \\ g \equiv h (N)}} e^{2\pi i (a(g+dk)^t A (g+dk)/2cN^2} \; e^{-b 2\pi i (d k^t A k + 2 k^t A g)/2N^2}$$

The last exponential depends only on g mod N (as $k^t A \in N\mathbb{Z}^n$), and can be taken out of the sum giving

$$\Phi(h,k) = e^{-b 2\pi i (d k^t A k + 2 k^t A h)/2cN^2} \; \Phi(h + dk, 0)$$

with $\Phi(h+dk,0) = \sum_{\substack{g \bmod cN \\ g \equiv h + dk (N)}} e^{2\pi i a g^t A g}/2N^2$.

Note that, in particular, $\Phi(h,k)$ depends only on $k \mod N$.

3. **The equality $((-i)(\frac{-c}{z} + d))^{1/2} (-iz)^{1/2} = (-\,\mathrm{sg}(d) i)(dz - c)^{1/2}$**

We will assume that $c > 0$. Recall that $z \in \mathcal{H}$, and so $\frac{-1}{z} \in \mathcal{H}$.

Recall that $z^{1/2} = e^{i \log(z)/2} = e^{i(\ln|z| + i \arg(z))/2}$ with $-\pi < \arg(z) < \pi$.

Observe that if $z \in \mathcal{H}$ and $w \in \{\mathrm{Im}(w) < 0\}$ then $\sqrt{zw} = \sqrt{z}\sqrt{w}$:
as $0 < \arg z < \pi, -\pi < \arg w < 0$, we have

$$-\pi < \arg(w) < \arg(w) + \arg(z) < \pi + \arg(w) < \pi$$

then $\arg(zw) = \arg(w) + \arg(z)$ and so $\sqrt{zw} = \sqrt{z}\sqrt{w}$.

Taking the left hand side of the equality we get:
$((-i)(\frac{-c}{z} + d))^{1/2} = (-i)^{1/2}(\frac{-c}{z} + d)^{1/2}$ and
$(-iz)^{1/2} = (-i)^{1/2}z^{1/2}$ gives
$((-i)(\frac{-c}{z} + d))^{1/2}(-iz)^{1/2} = (-i)z^{1/2}(\frac{-c}{z} + d)^{1/2}$.
Now we look under which conditions we can say
$z^{1/2}(\frac{-c}{z} + d)^{1/2} = (z(\frac{-c}{z} + d))^{1/2} = (dz - c)^{1/2}$.
Suppose $d \geq 0$. We have $\arg(\frac{-c}{z} + d) \leq \arg(\frac{-c}{z})$ as $(w \to w + d)$ is a translation to the right; and, as $c > 0$, $\arg(\frac{-c}{z}) = \arg(\frac{-1}{z}) = \pi - \arg(z)$. Then, as both z and $(\frac{-c}{z} + d)$ are in $\mathcal{H}$,

$$0 < \arg(z) + \arg(\frac{-c}{z} + d) \leq \arg(z) + \arg(\frac{-c}{z}) = \arg(z) + \arg(\frac{-1}{z}) = \pi.$$

Then $\arg(z(\frac{-c}{z} + d)) = \arg(z) + \arg(\frac{-c}{z} + d)$ and $z^{1/2}(\frac{-c}{z} + d)^{1/2} = (z(\frac{-c}{z} + d))^{1/2}$.
If $d < 0$, $(w \to w + d)$ is a translation to the left, and $\arg(\frac{-c}{z} + d) > \arg(\frac{-c}{z})$. Thus we get $\arg(z) + \arg(\frac{-c}{z} + d) > \pi$ and $\arg(z(\frac{-c}{z} + d)) = \arg(z) + \arg(\frac{-c}{z} + d) - 2\pi$. Thus $(z(\frac{-c}{z} + d))^{1/2} = z^{1/2}(\frac{-c}{z} + d)^{1/2}(-1)$, from which the result follows.

4.

$$\sum_{\substack{g \bmod N \\ Ag \equiv 0(N)}} e^{2\pi i(\ell - bh)^t Ag/N^2} = \begin{cases} D = \det(A) & \text{if } \ell \equiv bh(N) \\ 0 & \text{if } \ell \not\equiv bh(N) \end{cases}$$

Let $G = \{g \mod N : Ag \equiv 0(N)\}$, which is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^n$, and $\chi(g) = e^{2\pi i(\ell - bh)^t Ag/N^2}$. Then $\chi : G \to \mathbb{C}$ is a character, that is $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$ and

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi \text{ is the trivial character} \\ 0 & \text{otherwise} \end{cases}$$

It remains to see that $|G| = \det(A)$:

We may suppose A is diagonal, as otherwise we can write $A = UDV$ with U and V integer matrices of determinant equal to 1; and $G = \{g \mod N : Dg \equiv 0(N)\}$. Moreover NA^{-1} has integer entries if and only if ND^{-1} has, and if $\alpha_1, ..., \alpha_n$ are the diagonal entries of D, then $ND^{-1} \in \mathbb{Z}^{n \times n}$ means that α_i/N, for $i = 1, ..., n$.

Thus $Dg \equiv 0(N)$, $g = (g_1, ..., g_n)^t$ if and only if $\alpha_i g_i \equiv 0(N)$. Each equation having $\alpha_i = (\alpha_i, N)$ solutions $g_i \mod N$, gives $|G| = \alpha_1 ... \alpha_n = \det(A)$.

5. **Gauss Sums**

Let χ be a character of conductor m, that is χ is primitive modulo m: it is not a character modulo a proper divisor of m. For $n \in \mathbb{Z}/n\mathbb{Z}$ the Gauss sum of χ is defined as

$$g_\chi(n) = \sum_{x \mod m} \chi(x) e^{2\pi i x n/m}$$

Denote $g_\chi = g_\chi(1)$. It is easy to see that

- $g_\chi(n) = \overline{\chi}(n) g_\chi$
- $m = g_\chi \overline{g_\chi} = \chi(-1) g_\chi^2$, then $|g_\chi| = \sqrt{m}$.

Note that

$$\left(\frac{-1}{p}\right)^{1/2} = \left\{ \begin{matrix} 1 & p \equiv 1(4) \\ i & p \equiv 3(4) \end{matrix} \right\} = \epsilon_p$$

Thus, the previously defined ϵ_p is the (principal) square root of the character $(\frac{\cdot}{p})$.

We have the following important relation:

- For an odd prime p,

$$g_\chi = \sum_{k=1}^{p} \left(\frac{k}{p}\right) e^{2\pi i k/p} = \epsilon_p \, p^{1/2}$$

CHAPTER 4

Modular forms and Quaternion Algebras.

In this chapter we give some general theory on quaternion algebras and Brandt matrices. We show the connection among quaternion algebras and modular forms; and Brandt matrices and Hecke operators. For reference on this see [24].

To an order of level N in a definite quaternion algebra B defined over $\mathbb{Q}$ and ramified at some specific primes, one can attach certain theta series which, by the results exposed in the last chapter, turn out to be modular forms of weight 2 and level N. Each newform f of level N is represented in this space of theta series. The Brandt matrices of level N act on this space as the Hecke operators $\{T_p\}$ act on $M_2(N)$. If $f = \sum a_n q^n$ is a normalized newform, we have that $T_p f = a_p f$. Let B_p denote the Brandt matrix of prime degree p, then there is a dimension one eigenspace such that $B_p v = a_p v$, for every prime p.

In the next chapter we will see, in the prime level case, how to construct modular forms of weight $3/2$ within the quaternion algebra B and how this dimension one eigenspace, will permit us to "select" a modular form of weight $3/2$ under Shimura correspondence to f. This explicit construction is crucial for the numeric work done.

4.1 Background on Quaternion Algebras.

F will denote the fields $\mathbb{Q}, \mathbb{Q}_p$ or $\mathbb{R}$. A quaternion algebra B over F can be defined as the set with basis, over F, $\{1, i, j, k\}$ and multiplication given by the following relations: 1 is the identity, $i^2 = a$, $j^2 = b$ with $a, b \in F^\times$ and $ij = -ji = k$. That is,

$$B = \{w + xi + yj + zk : w, x, y, z \in F,\ i^2 = a, j^2 = b \text{ and } ij = k = -ji\}.$$

For $F = \mathbb{Q}$ this quaternion algebra B will be denoted (a, b). For $F = \mathbb{Q}_p$, $p \leq \infty$ and $\mathbb{Q}_\infty = \mathbb{R}$, it will be denoted $(a, b)_p$.

If B is a quaternion algebra over $\mathbb{Q}$, then $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a quaternion algebra over $\mathbb{Q}_p$, for any $p \leq \infty$.

Over $\mathbb{Q}_p$ there are, up to isomorphism, only two quaternion algebras: the matrix algebra $M_2(\mathbb{Q}_p)$ or a unique quaternion division algebra.

Set $(a,b)_p = 1$ if $(a,b)_p$ is the 2×2 matrices and $(a,b)_p = -1$ if $(a,b)_p$ is a division algebra. Then $(a,b)_p$ becomes the Hilbert symbol which is defined by

$$(a,b)_p = \begin{cases} 1 & \text{if } w^2 - ax^2 - by^2 - abz^2 \text{ represents zero in } \mathbb{Z}_p \\ -1 & \text{if } w^2 - ax^2 - by^2 - abz^2 \text{ does not represent zero in } \mathbb{Z}_p \end{cases}$$

The number of primes such that the quadratic form $w^2 - ax^2 - by^2 - abz^2$ does *not* represent zero in $\mathbb{Z}_p$ is finite: for any $p \neq 2$ not dividing ab the equation $w^2 - ax^2 - by^2 - abz^2 = 0$ always has a nontrivial solution in $\mathbb{Z}_p$. Further, the primes such that the above equation is not solvable in $\mathbb{Z}_p$ is even in number, as we have the following well known *Product Formula*:

$$\prod_{p \leq \infty} (a,b)_p = 1.$$

For reference on quadratic forms see [2] chapter I, §6.

Let $B = (a,b)$ be a quaternion algebra over $\mathbb{Q}$. A prime $p \leq \infty$ is said to *ramify* in B if B_p is a division algebra. If B_p is a matrix algebra, then the prime p is said to *split* in B.

Thus the set of primes ramifying in a quaternion algebra B is finite and even in number. Determining which primes ramify in a given quaternion algebra is an exercises of evaluating Hilbert symbols.

Further, given any finite set of an even number of primes, there is, up to isomorphism, a unique quaternion algebra ramified precisely at those primes.

Let $\alpha = w + xi + yj + zk \in B$, the conjugate of α is defined as $\overline{\alpha} = w - xi - yj - zk$. The reduced *norm* and *trace* are defined by $N(\alpha) = \alpha\overline{\alpha}$, $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$.

The norm N will be viewed as a quadratic form on the four dimensional vector space B over F. If $B = (a,b)$ is a quaternion algebra over $\mathbb{Q}$, then N is positive definite if and only if ∞ is ramified in B if and only if $a < 0$ and $b < 0$.

4.1.1 Example.

Suppose the quaternion algebra B is given by the matrices, $B = M_2(F)$.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then we have $\overline{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ is the adjoint matrix of A; the norm N is the determinant, and Tr is the usual trace of the matrix A.

As an example suppose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix such that $A^2 = \lambda\,\mathrm{id}$. A simple calculation shows that $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. Let us take, for example, a matrix with $a \neq 0$, $I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and any other linearly independent with I, for example $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, then $K = IJ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. For any $A \in B$ we can write $A = \frac{a+d}{2}\,\mathrm{id} + \frac{a-d}{2}I + \frac{b-c}{2}J + \frac{b+c}{2}K$, then $\overline{A} = \frac{a+d}{2}\,\mathrm{id} - \frac{a-d}{2}I - \frac{b-c}{2}J - \frac{b+c}{2}K = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. □

Let B be a quaternion algebra over $\mathbb{Q}$ (or $\mathbb{Q}_p$). A *lattice* on B is a free $\mathbb{Z}$ (or $\mathbb{Z}_p$) submodule of B of rank four. An *order* $\mathcal{O}$ of B is a lattice on B which is also a subring containing the identity.

• If α belongs to some order of B, then $\mathrm{Tr}(\alpha)$ and $N(\alpha)$ are in $\mathbb{Z}$ (respectively $\mathbb{Z}_p$): Suppose $\{v_1, \ldots, v_4\}$ is a $\mathbb{Z}$-base of $\mathcal{O}$ and A the matrix $A = (\mathrm{Tr}(v_i\bar{v_j}))$ associated to the quadratic form N. Then for any $\alpha = x_1v_1 + \cdots + x_4v_4 \in \mathcal{O}$, $N(\alpha) = x\frac{1}{2}Ax^t$ where $x = (x_1, \ldots, x_4) \in \mathbb{Z}^4$. This means, in particular, that the denominators of the norms of the elements $\alpha \in \mathcal{O}$ are bounded by the least common multiple of those in $(\mathrm{Tr}(v_i\bar{v_j}))$. Thus if for $\alpha \in \mathcal{O}, N(\alpha) \notin \mathbb{Z}$, as $\mathcal{O}$ is a ring, $\alpha^n \in \mathcal{O}$ for any n, and the rational numbers $N(\alpha^n)$ do not have bounded denominators, so $N(\alpha)$ must be an integer. Similarly, the denominator of any $\mathrm{Tr}(\alpha)$, $\alpha \in \mathcal{O}$ must be bounded as $\mathcal{O}$ is of finite rank over $\mathbb{Z}$. Thus, if $\mathrm{Tr}(\alpha) \notin \mathbb{Z}$, as $\mathcal{O}$ is a ring $\alpha^2 \in \mathcal{O}$ and $\mathrm{Tr}(\alpha^2) = \mathrm{Tr}^2(\alpha) - 2N(\alpha)$ has a bigger denominator than α. Recall that $N(\alpha) \in \mathbb{Z}$. We can repeat this for $(\alpha^2)^2$, and so on, getting non-bounded denominators for the elements in $\mathcal{O}$.

In what follows B will always be a quaternion algebra over $\mathbb{Q}$, unless explicitly stated. We will give some more definitions and state some facts on orders in quaternion algebras. For proofs see [24] or references therein.

• For a lattice L in B, L_p will denote the lattice $L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ of B_p. Let N be the norm form and $\mathrm{Tr}(x\bar{y}) = N(x + y) - N(x) - N(y)$ the bilinear form associated to N. If $\{v_1, \ldots, v_4\}$ is a $\mathbb{Z}$-basis for a lattice L then the *discriminant* of L is $\mathrm{disc}(L) = \det(\mathrm{Tr}(v_i\bar{v_j}))$.

• An order $\mathcal{O}$ of B is said to be *maximal* if it is not properly contained in any other order of B. An order $\mathcal{O}$ of B is maximal if and only if $\mathcal{O}_p$ is a maximal order of B_p for all $p < \infty$, that is, for all "finite" or non-Archimedian primes.

If B_p is a division algebra ($p < \infty$), there is a unique maximal order $= \{x \in B_p : N(x) \in \mathbb{Z}_p\}$. If B_p is split, then all maximal orders of B_p are conjugate to the order $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ by an element of $B_p^\times$. Any order is contained in a maximal order.

• Let p be a finite prime and F the unique unramified quadratic field extension of $\mathbb{Q}_p$: $F = \mathbb{Q}_2(\sqrt{5})$ if $p = 2$ and $F = \mathbb{Q}_p(\sqrt{u})$ for $p > 2$ where $u \in \mathbb{Z}$ is a quadratic nonresidue mod p. Consider the $\mathbb{Q}_p$-subalgebra of $M_2(F)$ given by

$$A = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix}, \quad \alpha, \beta \in F \right\}$$

where σ is conjugation in $F/\mathbb{Q}_p$. A direct calculation shows that A is a quaternion division algebra over $\mathbb{Q}_p$. The norm N and trace Tr are the determinant and trace of $M_2(F)$ restricted to A. Denote R the ring of integers of F: $R = \mathbb{Z}_2 + \mathbb{Z}_2\frac{1+\sqrt{5}}{2}$ for $p = 2$ and $R = \mathbb{Z}_p + \mathbb{Z}_p\sqrt{u}$ for $p > 2$. The set

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix}, \quad \alpha, \beta \in R \right\}$$

is the unique maximal order of A since if γ belongs to an order, then $N(\gamma) = N(\alpha) - pN(\beta) \in \mathbb{Z}_p$ which implies $\gamma \in \mathcal{O}$:

Suppose first that $p \neq 2$. Then, as u is a nonresidue mod p, we have that the p-valuation of any number $a^2 - ub^2$, with $a, b \in \mathbb{Q}_p$ must be even and, secondly, if the number $a^2 - ub^2 \in \mathbb{Z}_p$ then a and b must be in $\mathbb{Z}_p$ for otherwise we would have that u is a square mod p.

Now, if $N(\gamma) = (a^2 - ub^2) - p(c^2 - ud^2) \in \mathbb{Z}_p$ then $a^2 - ub^2$ and $c^2 - ud^2$ must be in $\mathbb{Z}_p$ as no cancellation is possible if the parity of the p-valuations of the numbers $(a^2 - ub^2)$ and $p(c^2 - ud^2)$ is opposite.

A similar reasoning goes for $p = 2$.

• Fix a prime p and let B be the quaternion algebra over $\mathbb{Q}$ ramified precisely at p and ∞. Let r be a non negative integer and M any positive integer prime to p. An order $\mathcal{O}$ is said to have *level* $N = p^{2r+1}M$ if $\mathcal{O}_q$ is isomorphic over $\mathbb{Z}_q$ (ie conjugate by an element of $B_q^\times$) to $\begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ N\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}$ for all $q \neq p$ and $\mathcal{O}_p$ is isomorphic over $\mathbb{Z}_p$ to $\left\{ \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in R \right\}$ where B_p is identified with the $\mathbb{Q}_p$-algebra A defined before.

An order of level $N = p^{2r+1}M$ is maximal if and only if $r = 0$ and $M = 1$. $\mathcal{O}$ has level $N = p^{2r+1}M$ if and only if $\mathrm{disc}(\mathcal{O}) = (p^{2r+1}M)^2$.

We will now be considering a fixed quaternion algebra B ramified exactly at a prime p and ∞, $N = p^{2r+1}M$ as before, $\mathcal{O}$ an order of level N in B.

A *left $\mathcal{O}$-ideal* I is a lattice on B such that for all $p < \infty$, $I_p = \mathcal{O}_p b_p$ for some $b_p \in B_p^\times$. Two left $\mathcal{O}$-ideals I and J are said to be equivalent if $I = Jb$ for some $b \in B^\times$. We have the analogous definitions for right $\mathcal{O}$-ideals.

The *class number* of left-ideals for an order $\mathcal{O}$ of level N is the number of distinct classes and it is denoted by $H(N)$. The *type number* of orders of level N in B is the number of isomorphism classes of orders of level N in B and it is denoted by $T(N)$. The class number is finite and independent of the particular order of level N used in its definition. The type number always satisfies $T(N) \leq H(N)$. Explicit formulas for type number and class number exist.

We will later relate orders of level N in the quaternion algebra B over the rationals, ramified at some prime and ∞, to cusps forms of level N.

Let I be an ideal for an order $\mathcal{O}$ of level N in B. The *right order of I* is defined as the set $\{b \in B : Ib \subset I\}$. Similarly we have the *left order of I*: $\{b \in B : bI \subset I\}$. If I is a left ideal of an order $\mathcal{O}$ of level N, its right and left orders are orders of level N, and its left order is $\mathcal{O}$.

The *Norm* of an ideal I, $N(I)$, is the positive rational number that generates the $\mathbb{Q}$-ideal $\{N(a) : a \in I\}$. The *conjugate* of an ideal I is the ideal $\bar{I} = \{\bar{a} : a \in I\}$ and the *inverse* of I is given by $I^{-1} = \{b \in B : IbI \subset I\}$.

Proposition 4.1.1. *Let $\mathcal{O}$ be an order of level N, $\{I_1, \ldots, I_H\}$ a complete set of representatives of left ideals of $\mathcal{O}$. Let $\mathcal{R}_j$ be the right order of I_j, then $\{I_j^{-1}I_1, \ldots, I_j^{-1}I_H\}$ is a complete set of representatives of left ideals of $\mathcal{R}_j$. Further, the $\mathcal{R}_j$ represent all the types of orders of level N in B, with possible duplication.*

4.1.2 Ideals and Quadratic Forms.

A quadratic form $Q(x)$ is said to be *integral* if $Q(x) \in \mathbb{Z}$ for any $x \in \mathbb{Z}^r$.

To a positive definite integral quadratic form $Q(x)$ in an even number $r = 2k$ of variables we associate a matrix A, which is the matrix of the associated bilinear form $(x, y) = Q(x + y) - Q(x) - Q(y)$. Then $Q(x) = \frac{1}{2}xAx^t$ and $A = (a_{ij})$ is a positive definite symmetric matrix with integer coefficients and $a_{ii} \equiv 0 \mod 2$.

The *discriminant* of Q is $\mathrm{disc}(Q) = (-1)^k \det(A)$. The *level* of Q, or A, is defined as the least positive integer N such that the matrix NA^{-1} has integer entries with even integers in the diagonal. The *adjoint* form to Q is the form $Q^*(x) = \frac{1}{2}xNA^{-1}x^t$.

Proposition 4.1.2. *Let B be a positive definite (that is, ramified at infinity), quaternion algebra over $\mathbb{Q}$; $\mathcal{O}$ an order of level N and I a left $\mathcal{O}$-ideal. Then the quadratic form $\frac{N(x)}{N(I)}$ is a positive definite integral quadratic form in B, of level N and discriminant N^2. That is, if $\{v_1, \ldots, v_4\}$ is a $\mathbb{Z}$-basis for I, then $Q(x) = \dfrac{N(x_1v_1 + \cdots + x_4v_4)}{N(I)}$ is positive definite, integral, of level N and discriminant N^2.*

Proof:

First, $Q(x)$ is positive definite for B is ramified at ∞ and it is integral because, by definition of $N(I)$, $N(I)$ divides $N(x)$ for all $x \in I$. Let A be the matrix associated to Q. The level N is a positive integer so it is enough to determine it locally at every prime $q < \infty$. Recall that B is ramified precisely at p and ∞. Thus, for a prime $q \neq p$, B_q is isomorphic to $M_2(\mathbb{Q}_q)$ and $I_q = \mathcal{O}_q\beta$ for some $\beta \in B_q^\times = GL_2(\mathbb{Q}_q)$. Now,

$$\mathcal{O}_q = \alpha \begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ N\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix} \alpha^{-1}$$

for some $\alpha \in GL_2(\mathbb{Q}_q)$. Let $e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $e_2 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $e_3 = \left(\begin{smallmatrix} 0 & 0 \\ N & 0 \end{smallmatrix}\right)$, $e_4 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $\{\alpha e_1\alpha^{-1}\beta, \ldots, \alpha e_4\alpha^{-1}\beta\}$ is a $\mathbb{Z}_q$-basis for I_q. Note that $N(I) = N(\beta)$, so the matrix A associated to the form Q is calculated by:

$$\begin{aligned} A &= \frac{1}{N(I)}(\mathrm{Tr}(\alpha e_i\alpha^{-1}\beta\ \overline{\alpha e_j\alpha^{-1}\beta})) = \frac{1}{N(I)}(\mathrm{Tr}(\alpha e_i\alpha^{-1}\beta\bar{\beta}\bar{\alpha}^{-1}\bar{e_j}\bar{\alpha})) \\ &= \frac{N(\beta)N(\alpha^{-1})}{N(I)}(\mathrm{Tr}(\alpha e_i\bar{e_j}\bar{\alpha})) = N(\alpha^{-1})(\mathrm{Tr}(\alpha e_i\bar{e_j}\alpha^{-1}\alpha\bar{\alpha})) \\ &= N(\alpha^{-1})N(\alpha)(\mathrm{Tr}(\alpha e_i\bar{e_j}\alpha^{-1})) = (\mathrm{Tr}(e_i\bar{e_j})) \\ &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -N & 0 \\ 0 & -N & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Then A has clearly level N and has discriminant $-\det(A) = N^2$ in $\mathbb{Z}_q$.

For $q = p$ we have:

$$B_p \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix}, \quad \alpha, \beta \in F \right\}$$

where $F = \mathbb{Q}_p(v)$ with $v = \begin{cases} \sqrt{u} & u \text{ a non-residue mod } p, \text{ for } p \neq 2 \\ \frac{1+\sqrt{5}}{2} & \text{for } p = 2 \end{cases}$

and $\mathcal{O}_p$ is the ideal

$$\left\{ \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in R \right\}$$

$R = \mathbb{Z}_p \oplus \mathbb{Z}_p v$, the ring of integers of F.

A similar calculation to the one done for $q \neq p$, now with basis $e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $e_2 = \left(\begin{smallmatrix} v & 0 \\ 0 & v^\sigma \end{smallmatrix}\right)$, $e_3 = \left(\begin{smallmatrix} 0 & p^r \\ p^{r+1} & 0 \end{smallmatrix}\right)$, $e_4 = \left(\begin{smallmatrix} 0 & p^r v \\ p^{r+1}v^\sigma & 0 \end{smallmatrix}\right)$ leads to the matrices

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2v & 0 & 0 \\ 0 & 0 & -2p^{2r+1} & 0 \\ 0 & 0 & 0 & 2p^{2r+1}v \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & -2p^{2r+1} & -p^{2r+1} \\ 0 & 0 & -p^{2r+1} & 2p^{2r+1} \end{pmatrix}$$

for $p \neq 2$ and $p = 2$, respectively. Clearly they have level p^{2r+1} and discriminant $p^{2(2r+1)}$.

□

We will come back on this quadratic norm forms related to an order $\mathcal{O}$ of level N. These will give us a connection to modular forms, as we already have seen in the last chapter that theta series attached to such quadratic forms are modular forms for $\Gamma_0(N)$.

4.2 Hecke operators.

We will denote the complex vector space of modular forms of weight k for $\Gamma_0(N)$ by $M_k(N)$. We have that $M_k(N) = S_k(N) \oplus E_k(N)$ where $S_k(N)$ is the space or cusp forms and $E_k(N)$ the space of Eisenstein series.

We will restrict our attention to forms of weight $k = 2$. Thus from now on we will only be considering the space $M_2(N)$ and operators therein.

The main tool in studying cusp forms is the notion of *Hecke operators* T_n, which are linear mappings on the finite dimensional space $S_2(N)$.

We can define the Hecke operators acting on $M_2(N)$ as follows.

Let R be a commutative ring and consider the operators $T_p : R[[q]] \to R[[q]]$ for p prime formally defined by:

Suppose f is given by its q-expansion: $f = \sum a_n q^n$. For p prime to the level N, we define

$$T_p f = \sum a_{pn}\, q^n + p \sum a_n\, q^{pn} = \sum (a_{pn} + p a_{n/p})\, q^n$$

with the convention that $a_{n/p} = 0$ if $p \nmid n$.

For the primes p dividing the level N, we define

$$T_p f = \sum a_{pn}\, q^n$$

Proposition 4.2.1. *The Hecke operators satisfy the following properties:*

a) $T_{nm} = T_n T_m$ *for* $(n, m) = 1$. *In particular,* T_n *and* T_m *commute.*

b) If p *is a prime that divides* N, $T_{p^r} = T_p^r$.

c) If p *is a prime not dividing* N, *and* $r \geq 2$

$$T_{p^r} = T_{p^{r-1}} T_p - p T_{p^{r-2}}.$$

Let $\mathbb{V}$ be a finite-dimensional vector space and T a linear operator on $\mathbb{V}$. The operator T is *semisimple* if for any T-invariant subspace $\mathbb{U}$ there is a T-invariant subspace $\mathbb{W}$ such that $\mathbb{V} = \mathbb{U} \oplus \mathbb{W}$. For a (finite-dimensional) vector space $\mathbb{V}$ over an algebraically closed field, an operator T is semisimple if and only if it can be diagonalized. Further, if we have a commutative set of diagonalizable operators, they can all be diagonalized in the same basis of eigenfunctions.

We have the following important theorem of Hecke-Peterson

Theorem 4.2.2. *The Hecke operators* T_n, *for* $(n, N) = 1$ *acting on the complex vector space* $S_2(N)$ *generate a commutative, semisimple ring. Thus there exist a basis* $(f_i(\tau))_{1 \leq i \leq \dim S_2(N)}$ *of* $S_2(N)$ *consisting of eigenfunctions for all* T_n *with* $(n, N) = 1$.

Recall that for N and M positive integers, M dividing N and $d \mid \frac{N}{M}$, any cusp form f on $\Gamma_0(M)$ is also a cusp form on $\Gamma_0(N)$ and $f(d\tau)$ is also a cusp form on $\Gamma_0(N)$. Let $C^-(N)$ denote the subspace of $S_2(N)$ generated by all the $f(d\tau)$ where $f(\tau)$ is a cusp form on some $\Gamma_0(M)$, M, d as before. Denote by $S_2^0(N)$ the orthogonal complement of $C^-(N)$ with respect to the Paterson inner product on $S_2(N)$. By Atkin and Lehner, the space $S_2^0(N)$ is called the *space of newforms* on $\Gamma_0(N)$. A *newform* on $\Gamma_0(N)$ is a form on $S_2^0(N)$ that is an eigenfunction for all the Hecke operators.

4.3 Connection with modular forms on $\Gamma_0(N)$.

4.3.1 Brandt matrices.

Let B be a quaternion algebra over $\mathbb{Q}$ ramified at p and ∞, $\mathcal{O}$ an order of level $N = p^{2r+1}M$, $(p, M) = 1$ in B. Let $\{I_1, \ldots, I_H\}$ a set of representatives of left ideals classes for $\mathcal{O}$, $\mathcal{R}_j$ the right order of I_j and e_j the number of units of $\mathcal{R}_j$, that is, elements $x \in \mathcal{R}_j$ such that $N(x) = 1$. Then e_j is the number of times the positive definite quadratic form $N(x)$, $x \in \mathcal{R}_j$ represents 1, and it is thus a finite number. It can be seen that $e_j \leq 24$ and it is usually 2.

Define for any positive integer n and $1 \leq i, j \leq H$

$$b_{ij}(n) = \frac{1}{e_j} \#\{x \in I_j^{-1} I_i : \tfrac{N(I_j)}{N(I_i)} N(x) = n\}$$

and $b_{ij}(0) = \frac{1}{e_j}$. Thus $b_{ij}(n)$ is $\frac{1}{e_j}$ the number of times the positive definite quadratic form $\frac{N(I_j)}{N(I_i)} N(x)$ represents n in the ideal $I_j^{-1} I_i$.

Definition 4.3.1. *The Brandt matrices $B_n = B_n(p^{r+1}, M)$, for $n \geq 0$ are the $H \times H$ matrices defined by*

$$B_n = (b_{ij}(n))$$

where H is the class number of left ideal classes of an order $\mathcal{O}$ of level $N = p^{r+1}M$, $p \nmid M$, in the quaternion algebra B defined over $\mathbb{Q}$ and ramified at p and ∞.

Theorem 4.3.2. *The entries of the Brandt matrix series*

$$\Theta(\tau) = \sum_{n=0}^{\infty} B_n q^{n\tau}$$

are modular forms of weight 2, level N and trivial character.

Proof:

For i, j fixed, we have

$$\theta(\tau) = \theta_{ij}(\tau) = \frac{1}{e_j} \sum_{x \in I_j^{-1} I_i} q^{\tau N(x) \frac{N(I_j)}{N(I_i)}} = \sum_{n=0}^{\infty} b_{ij}(n)\ q^n$$

where $q = e^{2\pi i \tau}$.

By proposition 4.1.1 $I_j^{-1} I_i$ is a left ideal for the order $\mathcal{R}_j$ of level N. Its norm form is a positive definite integral quadratic form in 4 variables, of level N by 4.1.2. Then proposition 3.2.4 gives us the desired result.

□

None of these θ_{ij} are cusp forms as the zero Fourier coefficient at $i\infty$ is $\frac{1}{e_j}$.

The difference of any two of these forms lying in the same column is a cusp form: $f(\tau) = \theta_{ij}(\tau) - \theta_{kj}(\tau)$ is a cusp form for all $1 \leq i, j, k \leq H$. For a proof we have to see that $f(\tau)$ vanishes at all other cusps of $\Gamma_0(N)$, rather than $i\infty$. However theta series of quadratic forms in the same genus behave equally at all cusps, thus their difference is a cusp form (see [30]).

Proposition 4.3.3. *([24] lemma 2.18 and theorem 2.28.)*

Consider the Brandt matrices $B_n = B_n(p^{r+1}, M) = (b_{ij}(n))$. Then

a) $b_{ij}(0) = \frac{1}{e_j}$

b) $e_j b_{ij}(n) = e_i b_{ji}(n)$ *for all* $1 \leq i, j \leq H$ *and all* $n \geq 0$.

c) The row sums of the Brandt matrices are constant, ie.

$$\sum_{j=1}^{H} b_{ij}(n) = b(n)$$

is independent of i.

d) When $N = p$ is prime, we have (see [9] Proposition 2.7):

$$b(n) = \sigma_N(m) = \sum_{d|n, (d,N)=1} d$$

The most important fact about Brandt matrices is that they give a representation of the Hecke operators on a space of theta series.

Fix $N = pM$, $p \nmid M$. The Brandt matrices $B_n = B_n(p, M)$ with $(n, N) = 1$ generate a commutative semisimple ring and satisfy the same identities as the Hecke operators:

Proposition 4.3.4.

a) $B_{nm} = B_n B_m$ *for* $(n, m) = 1$.

b) If the quaternion algebra B *is ramified at* p, $B_{p^r} = B_p^r$.

c) If p *is a prime not dividing* $N = pM$, *and* $r \geq 2$

$$B_{p^r} = B_{p^{r-1}} B_p - p B_{p^{r-2}}.$$

c) The matrices B_n *for* $n \geq 1$ *generate a commutative semisimple ring* $\mathbb{B}$.

Proof: see [7] §6 Theorem 2 or [24] Proposition 2.22.

Eichler proved that the operators T_n and the Brandt matrices B_n have the same traces for $(n, N) = 1$.

Two representations of a semisimple ring are equivalent if and only if their traces are equal.

Let $\Theta(\tau) = (\theta_{ij}(\tau))$ be the Brandt matrix series. Then the action of the Hecke operators T_n, $(N, n) = 1$ on the θ_{ij} is given formally by B_n, that is $T_n(\theta_{ij})$ is the ij entry of the matrix

$$\sum_{m=0}^{\infty} B_n B_m q^m$$

As the Brandt matrices generate a commutative semisimple ring, they can be simultaneously diagonalized. If we conjugate the matrices $B_n = (b_{ij}(n))$ by a determined fixed matrix A we reduce them to block in the following form:

$$C_n = \begin{pmatrix} b(n) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B'_n & \\ 0 & & & \end{pmatrix}$$

where $b(n) = \sum_{j=1}^{h} b_{ij}(n)$ (independent of i) and $c_{ij}(n) = b_{ij}(n) - b_{1j}(n)$ for $2 \leq i, j \leq h$.

Then the entries of the modified Brandt matrix series

$$\Theta(\tau) = \sum_{n=0}^{\infty} B'_n \; q^n$$

are cusp forms of weight 2 on $\Gamma_0(N)$.

We can diagonalize simultaneously the matrices B'_n, for all $(n, N) = 1$.

Let $\Phi_2(N)$ denote the set of cusp forms appearing on the diagonal of the diagonalized modified Brandt matrix series

$$\sum_{n=0}^{\infty} PB'_nP^{-1}q^n$$

Then all elements of $\Phi_2(N)$ are eigenforms for all T_n with $(n, N) = 1$. Since the Hecke operators T_n commute they will be eigenforms for all T_n.

Set $\Phi_2(N) = \{\theta_1(\tau), ..., \theta_d(\tau)\}$, $d = h - 1$, we then have

$$S_2(N) \cong < \theta_1(\tau) > \oplus \quad ... \quad \oplus < \theta_d(\tau) >$$

where the $\cong$ is as modules for the Hecke algebra $\mathbb{T}$ generated by T_n.

4.3.2 Jacket-Langlands correspondence.

A particular case of the Jacquet-Langlands correspondence says roughly as follows.

Let N be a square-free integer, and f a normalized newform of level N. That is, $f \in S_2(N)$ the space of cusp forms of weight 2 for the congruence subgroup $\Gamma_0(N)$. Further, f is "new" and it is an eigenfunction of all the Hecke operators T_p:

$$\begin{cases} f = \sum_{n=1}^{\infty} a_n q^n \qquad (a_1 = 1) \\ T_p(f) = a_p f \end{cases}$$

Let B be a quaternion algebra ramified at infinity and at some set of finite primes. Let $\mathcal{O}$ be an order of level N, and B_p the Brandt matrices associated to the order $\mathcal{O}$.

To each of these newforms f corresponds an eigenvector of the Brandt matrices of square free level N: there is a dimension-one space of eigenvectors v such that $B_p v = a_p v$ for all prime $p \nmid N$.

As for the primes $q \mid N$, the Brandt matrices B_q commute with all B_p $(p, N) = 1$ and thus v will also be an eigenvector for B_q. We cannot assert, in the most general situation, that $B_q v = a_q v$. This will be so, if the level N is square free.

In the next chapter we will explain the method described in [9] to construct, for an elliptic curve E of prime conductor N, a modular form of weight 3/2 whose coefficients are related to the central values of the L-series of the family of imaginary quadratic twists of E. We use this construction to analyze the distributions of the orders of the Tate-Shafarevich groups in the family.

CHAPTER 5

Distribution of Ш among twists of elliptic curves.

Now we put together what we have seen in the previous chapters and begin with what is the purpose of this thesis.

Given an elliptic curve E, we consider the family of negative quadratic twists of E. We want to calculate, and analyze, how the orders of the Tate-Shafarevich groups distribute within this family. A series of numerical experiments have been done for this, which we expose in this chapter. The main observation gleaned from the experimental data obtained is that the distribution of the Ш values, obtained in the family of negative quadratic twists of an elliptic curve E, was not "smooth" (in a sense we will explain below) exactly when the elliptic curve E had a nontrivial torsion point.

We remark on the fact that, in this case, we have a congruence among a modular form of weight 3/2 that corresponds to the elliptic curve E and an Eisenstein series. From this congruence we obtain the following result:

Theorem 5.0.5. *Let E be an elliptic curve of prime conductor N. Suppose E has a rational torsion point of prime order $\ell > 2$. Then the proportion of* Ш *values divisible by ℓ in the family of imaginary quadratic twists of E, with $\left(\frac{-d}{N}\right) \neq 1$, is the same as the proportion of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ divisible by ℓ, with $\left(\frac{-d}{N}\right) \neq 1$.*

If we assume the Cohen-Lenstra heuristics on the probability of class numbers being divisible by a prime, and assume that being divisible by a prime is an independent fact from having a determinate Kronecker symbol, then this proportion is equal to

$$f(\ell) = 1 - \prod_{i \geq 0} (1 - \frac{1}{\ell^i}) = \frac{1}{\ell} + \frac{1}{\ell^2} - \frac{1}{\ell^3} - \frac{1}{\ell^7} \ldots$$

The experimental data obtained, shows that this situation clearly differs from the general case. The proportion of Ш values divisible by a prime number ℓ among the negative quadratic twists of an elliptic curve E is significantly bigger when E has an ℓ torsion point defined over $\mathbb{Q}$, than the general case where $\ell \nmid |E(\mathbb{Q})_{\mathrm{Tor}}|$.

As for the general situation, the proportion we obtain numerically seems to adjust to Delaunay's predictions given in [6]. However, for this predictions, Delaunay orders elliptic curves by conductor which differs from taking an elliptic curve and its family of twists. Though this fact seems not to affect the general case, it does represent a difference when we have a rational ℓ-torsion point, as it will be seen in the tables below.

This deviation was already observed in [4], without having an explanation for it.

5.1 Twists of Elliptic Curves.

Let E be an elliptic curve defined over $\mathbb{Q}$. Let us suppose, for simplicity, that E is given by an equation

$$y^2 = x^3 + b_2x + 8b_4x + 16b_6.$$

Let d be an integer. The *d-quadratic twist* of E is the Elliptic Curve defined by the equation

$$dy^2 = x^3 + b_2x + 8b_4x + 16b_6 \tag{5.1}$$

or, more precisely, by

$$y^2 = x^3 + b_2dx + 8b_4d^2x + 16b_6d^3 \tag{5.2}$$

This *twisted* elliptic curve, is clearly isomorphic to E over $\mathbb{Q}(\sqrt{d})$.

Denote a_p as usual, and a_p^d the "a_p's" for the twisted curve E_d. That is,

$$N_p^d = p + 1 - a_p^d$$

is the number of points of the reduced curve $(\widetilde{E_d})_p$ modulo p. Then $a_p^d = \left(\frac{d}{p}\right) a_p$.

If we suppose, when considering equation (5.1) or (5.2), that it is minimal at p, then this last assertion is roughly as follows: if $p \mid d$ then the equation (5.2) is singular modulo p and reduces to a cusp, thus $a_p^d = 0$.

If d is a square modulo p then equation (5.1) is isomorphic to $\widetilde{E}_p$ and thus they have the same number of points.

If d is not a square modulo p then by equation (5.1) we see that if $x \in \mathbb{F}_p$ is such that the right hand side of (5.1) is a non-zero square then it will give 2 solutions on $\widetilde{E}_p$ and none on $(\widetilde{E_d})_p$ and, if it is a non-square then it gives 2 solutions on $(\widetilde{E_d})_p$ and none on $\widetilde{E}_p$. Further, each root of the polynomial on the right of (5.1) gives one point in each of the curves $\widetilde{E}_p$ and $\widetilde{E_{dp}}$. Then we have, adding one point at infinity for each curve,

$$N_p + N_p^d = 2p + 2$$

which gives

$$N_p^d = 2p + 2 - N_p = p + 1 + a_p = p + 1 - \left(\frac{d}{p}\right) a_p.$$

□

Now let $f = \sum_{n\geq 1} a_n\, q^n$ be the modular form corresponding to the elliptic curve E. To the d-quadratic twist of E, E_d, corresponds the *twist of* f given by

$$f_d = \sum_{n\geq 1} \left(\frac{d}{n}\right) a_n\, q^n$$

and denoted usually by $f \otimes \epsilon_d$.

Remark on notation: As we will only be considering *negative* quadratic twists, by E_d we will denote the $(-d)$-quadratic twist of E.

5.2 Experimental Approach.

Let $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ be an elliptic curve of prime conductor N and rank zero, that is, an elliptic curve with a finite number of points. Recall that E has an L-series which is defined for $\mathrm{Re}(s) > 3/2$ by

$$L(E,s) = \sum_{n\geq 1} a_n n^{-s}.$$

By the recent work of Wiles and others it is known that if we set

$$f = \sum_{n=1}^{\infty} a_n q^n \qquad q = e^{2\pi i\tau}$$

this is a cusp form of weight 2, level N, and $L(E,s) = L(f,s)$ (see 2.8.1 for definitions).

Moreover, f is an eigenfunction for all the Hecke operators T_n acting on $M_2(\Gamma_0(N))$. If we have normalized to have $a_1 = 1$, then the Fourier coefficients a_n are the eigenvalues: $T_n f = a_n f$.

Given E, we will be considering its imaginary quadratic twists. Let d be a positive integer such that $-d \equiv 0, 1 \bmod 4$ and denote by ϵ_{-d} the quadratic character of $(\mathbb{Z}/d\mathbb{Z})^*$ determined by $\epsilon_{-d}(p) = \left(\frac{-d}{p}\right)$ for primes p. Here $\left(\frac{\cdot}{p}\right)$ is the usual Legendre symbol. Then

$$f \otimes \epsilon_{-d} = \sum_{m\geq 1} a_m \epsilon_{-d}(m) q^m$$

the twist of f, is the weight 2, level dividing Nd^2, modular form of the $(-d)$-quadratic twist of the curve E, which we denote E_d; and $L(E_d,s) = L(f\otimes\epsilon_{-d},s)$.

In the early 80's Waldspurger [33] proved a remarkable result in which he relates the central values of L-series, associated to twists of modular forms of integer weight, to the coefficients of the Fourier expansion of certain modular form of half integer weight.

B. Gross in [9] states a special case of the Waldspurger's formula concerning the twists of modular forms of weight 2 and conductor N prime. This formula relates the product $L(f,1)L(f\otimes\epsilon_{-d},1)$ to the squared $d-$coefficient of a weight $3/2$ modular form g, under Shimura correspondence to f.

Moreover, given a modular form f of weight 2 and prime level N, he states an explicit procedure for constructing the modular form g of weight 3/2 involved in the Waldspurger formula.

We remark here that by the Birch and Swinnerton-Dyer conjecture we have, for an elliptic curve E_d of rank zero,

$$L(E_d, 1)c_d = |Ш_d|$$

where c_d can be explicitly calculated. A direct calculation of $L(E_d, 1)$ by the standard analytic method of braking the integral in two, which expresses $L(E_d, 1)$ as a series, will give us the exact $|Ш_d|$ with $O(d)$ terms. Doing this for all d in an interval $0 \leq d \leq X$ requires $O(X^2)$ operations.

The construction mentioned above, gives us, roughly, the order of $Ш_d$ as the square of the d-coefficient of certain modular form of weight 3/2. This amounts counting how many times a certain positive definite ternary quadratic form represents d, with some additional congruence conditions. This permits to calculate $|Ш_d|$ for $0 \leq d \leq X$ in $O(X^{3/2})$ operations.

We now explain briefly the method described in [9], following Gross' notation. The procedure, comes from the connection between modular forms on $\Gamma_0(N)$ and the quaternion algebra B ramified at N and ∞ (recall that now N is a prime number).

Basically, one constructs the theta series associated to certain rank-3 lattices in the quaternion algebra B. These theta series are then modular forms of weight 3/2, by proposition 3.2.4. The weight 3/2 modular form g corresponding to the weight 2 modular form f, will be a linear combination of the theta series just mentioned. The coefficients of this linear combination are given by an eigenvector v of the Brandt matrices of prime level N.

The construction is as follows.

Consider a maximal order $\mathcal{O}$ in the quaternion algebra B set above. For B ramified at a single prime N, a maximal order will be an order of prime level N. Let $\{I_1, ..., I_n\}$ be a set of left ideal classes for the order $\mathcal{O}$. Let R_i denote the right (maximal) order for the ideal I_i.

For each right order R_i, one constructs the theta series g_i of the following rank three $\mathbb{Z}$-lattices:

define S_i^0 as the subgroup of elements of trace zero in the R_i-suborder $\mathbb{Z} + 2R_i$. Let $\mathbb{N}$ denote the norm form, which is positive definite, then define the theta series g_i by

$$g_i(\tau) = \frac{1}{2} \sum_{b \in S_i^0} q^{\mathbb{N}b} = \frac{1}{2} + \sum_{d>0} a_i(d) q^d \qquad i = 1, \ldots, n$$

This is the theta series of a quadratic form in three variables, and by the results exposed in 3.2.4 are modular forms of weight 3/2.

Recall that T is the type number in B, that is, the number of distinct conjugacy classes of maximal orders in B. Then one gets T different theta series g_i.

These theta series g_i have level $4N$, trivial character, and their coefficients a_d satisfy

$$a_d = 0 \text{ unless } -d \equiv 0 \pmod 4 \text{ and } \left(\frac{-d}{N}\right) \neq 1$$

This is the *Kohnen* subspace of modular forms of weight 3/2. It has dimension T and it is stable under Hecke algebra. The theta series defined above lie in a lattice of rank T, denoted by M^*, which consists of those forms that, in addition to the condition just stated, have integral coefficients except, possibly, for a_0 that lies in $\frac{1}{2}\mathbb{Z}$.

Let $f \in S_2(\Gamma_0(N))$ be a newform. By Jacquet-Langlands correspondence, to f corresponds an eigenvector of the Brandt matrices of prime level N: there is a dimension-one space of eigenvectors $< v >$ such that $B(N,p)v = a_p v$ for all prime p (and for all $n \in \mathbb{N}$).

Let $v = (v_1, ..., v_n)$ be the (up to constant factor) eigenvector of the Brandt matrices of prime level N corresponding to our $f \in S_2(\Gamma_0(N))$ coming from the elliptic curve E.

Define $e_f = (e_1, ..., e_n) = (v_1/w_1, ..., v_n/w_n)$. Where w_i is one half the number of units of the order R_i. We can assume e_f has integer coordinates, and is primitive.

Then

$$g = \sum_{i=1}^{n} e_i g_i = \sum_{d>0} m_d q^d$$

is the weight 3/2 modular form that corresponds to the weight 2 modular form f. And this is the form involved in the Waldspurger formula, as related by B. Gross.

5.3 A special case of Waldspurger's formula.

We state here the special case of Waldspurger formula as given in [9].

Let N be a prime number, f a cusp form of weight 2 and trivial character for $\Gamma_0(N)$. Recall $f \otimes \epsilon_{-d}$ is the twist of f by the character ϵ_{-d} of $(\mathbb{Z}/d\mathbb{Z})^*$ determined by $\epsilon_{-d}(p) = \left(\frac{-d}{p}\right)$ for primes p.

For d a positive integer such that $-d$ is a fundamental discriminant and $\left(\frac{-d}{N}\right) \neq 1$ we have:

$$L(f,1)\ L(f \otimes \epsilon_{-d}, 1) = k_d\ \frac{(f,f)\, m_d^2}{\sqrt{d} < e_f, e_f >} \tag{5.3}$$

where $k_d = 2$ if $d \equiv 0\ (N)$, otherwise it is 1.

The product $< ., . >$ is given by:
If $v = \sum_{i=1}^n v_i e_i$ and $u = \sum_{i=1}^n u_i e_i$, then

$$< v, u >= \sum_{i=1}^{n} w_i v_i u_i$$

and (f, f) is the Peterson inner product, defined on the space of cusp forms $S_k(\Gamma_0(N))$ as

$$(f, h) = \int_{\Gamma_0(N)/\mathcal{H}} f(z)\,\overline{h(z)}\,y^k\,\frac{dxdy}{y^2}$$

where $z = x + iy$.

5.4 Restatement and Procedure.

We will restate the above formula in a more convenient way.

5.4.1 Periods and the Peterson inner product.

Let E be an elliptic curve. Over the complex numbers E is a compact Riemann surface. We won't go into detail with this part of the theory but we will briefly state some facts as we don't want to leave the periods undefined.

The following results can be found in [31] (5.1.1, 5.2):

Proposition 5.4.1. *There exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, and a complex analytic isomorphism*

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \qquad \phi(z) = [\wp(z) : \wp'(z) : 1]$$

of complex Lie groups (that is, an isomorphism of Riemann surfaces which is a group homomorphism). Here $\wp$ is the Weierstrass function associated to the lattice Λ.

Proposition 5.4.2. *Let E be an elliptic curve defined over $\mathbb{C}$ with Weierstrass coordinate functions x, y.*

a) Let α and β be paths on $E(\mathbb{C})$ giving a basis for the homology $H_1(E, \mathbb{Z})$. Then the periods

$$\omega_1 = \int_\alpha \frac{dx}{y} \quad \text{and} \quad \omega_2 = \int_\beta \frac{dx}{y}$$

are $\mathbb{R}$-linearly independent.

b) Let $\Lambda \subset \mathbb{C}$ be the lattice generated by ω_1, ω_2. Then the map

$$F : E(\mathbb{C}) \to \mathbb{C}/\Lambda \qquad F(P) = \int_{\mathcal{O}}^{P} \frac{dx}{y} \mod \Lambda$$

is a complex analytic isomorphism of Lie groups. Its inverse is the map given in proposition 5.4.1

By the work of Weil, Shimura and Taniyama, for every elliptic curve E defined over $\mathbb{Q}$, of conductor N, there is a non-constant map $\varphi : \Gamma_0(N)\backslash\mathcal{H}^* \to E$. The map φ is called the *modular parametrization*. The pullback of the unique (up to scalar multiple) holomorphic differential on E is of the form $2\pi i f(z)dz$ where f is a holomorphic cusp form of weight 2 for $\Gamma_0(N)$. This is the cusp form associated to the elliptic curve E.

We will replace the Peterson product (f, f) in the formula (5.3), taking E to be a strong-Weil curve and using the following result which can be found in Cremona [5], and which, for simplicity, we will enunciate differently.

Proposition 5.4.3. *Let E be an elliptic curve, and $f(\tau)$ the corresponding normalized new form of weight 2 for $\Gamma_0(N)$. Recall that E is isomorphic to $\mathbb{C}/\Lambda$, for some lattice Λ. Let $\varphi : X = \Gamma_0(N)\backslash\mathcal{H}^* \longrightarrow \mathbb{C}/\Lambda$ the associated modular parametrization. Then*

$$4\pi^2\|f\|^2 = \deg(\varphi)\,\mathrm{Vol}(E)$$

where

$$\|f\|^2 = \int_X |f(\tau)|^2 dudv \qquad \tau = u + iv$$

Further, if we write the lattice Λ as generated by $\Omega(1,\tau)$ where Ω is the real period of E and $\tau = \frac{\omega_2}{\omega_1} \in \mathcal{H}$ then:

$$\mathrm{Vol}(E) = \Omega^2\,\mathrm{Im}(\tau)$$

where $\mathrm{Im}(\tau)$ denotes the imaginary part of τ.

Replacing this in Waldspurger's formula and rearranging in a convenient way, we have the following identity:

Proposition 5.4.4. *Let E be an elliptic curve of prime conductor N, f its corresponding weight 2, level N, modular form, Ω_f its real period, e_f, m_d, k_d as in* (5.3). *Then*

$$\frac{L(f,1)}{\Omega_f}\;\frac{L(f\otimes\epsilon_{-d},1)}{\frac{2\Omega_f\,\mathrm{Im}(\tau)}{\sqrt{d}}} = k_d\,\frac{\deg(\varphi)\,m_d^2}{< e_f, e_f >} \qquad \text{for } \left(\frac{-d}{N}\right) \neq 1 \tag{5.4}$$

The degree of the modular parametrization $\deg(\varphi)$ can be taken from Cremona's tables.

The factor $\dfrac{L(f,1)}{\Omega_f}$ on the left is a rational number which can be calculated with PARI-GP.

$\dfrac{2\Omega_f\,\mathrm{Im}(\tau)}{\sqrt{d}}$ is "almost" the real period of the $(-d)$-twist of f, $f\otimes\epsilon_{-d}$. That is, it is a rational computable multiple of it, which is either constant or depends on d modulo 8.

5.5 The Birch and Swinnerton-Dyer conjecture for elliptic curves of rank zero.

For an elliptic curve E, of rank zero, the Birch and Swinnerton-Dyer conjecture states that

$$\frac{L(E,1)}{\Omega} = \frac{|Ш|\prod_p c_p}{|\,\mathrm{Tor}(E)|^2}$$

where $\mathrm{Tor}(E)$ is the torsion group of E, and Ω is the integral over $E(\mathbb{R})$ of the invariant differential $\dfrac{dx}{2y + a_1x + a_3}$. This is the real period of E or twice the real period, depending on whether the polynomial $p(x)$ defining E in $y^2 = p(x)$, has negative or

positive discriminant. The product $\prod_p c_p$ is a power of two, and each c_p for p a prime of bad reduction is related to the group of non singular points of the reduced curve. For primes of good reduction $c_p = 1$.

For E_d, the $(-d)$-twist of the elliptic curve E, $L(f \otimes \epsilon_{-d}, 1) = L(E_d, 1)$. We replace the equality above given by the Birch and Swinnerton-Dyer conjecture, in Waldspurger's formula. We have

$$\frac{L(E,1)}{\Omega} \; \frac{|Ш_d| \prod_p c_{p,d}}{|\operatorname{Tor}(E_d)|^2} \; q_d = \frac{k_d 2 \deg(\varphi) m_d^2}{< e_f, e_f >}. \tag{5.5}$$

At this point we make some remarks on calculations. Remember that we want the value $|Ш_d|$ in equation (5.5) above, so the other factors in the equality should be easy to calculate.

- The order $|\operatorname{Tor}(E_d)|$ is constant, at least for $d \geq b$, for some small bound b.
- q_d is the rational multiple that comes from the quotient $\Omega_d / \frac{\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}$. In the examples calculated q_d is constant equal to 2, or it equals 2 or 4 depending on the divisibility of d by 8.
- The quotient between $L(E,1)$ and the period Ω, as well as the product of the fudge factors $\prod_p c_{p,d}$ can be calculated with PARI-GP.

With identity (5.5) and the considerations just mentioned, we calculate the order of $Ш_d$, for a family of imaginary quadratic twists of the elliptic curve E, having previously calculated the weight 3/2 modular form g:

$$g(\tau) = \sum_{d>0} m_d \; q^d.$$

Moreover, as it is known, the order of the Tate-Shafarevich group is a square. Thus what we get is a *signed square root* of $|Ш_d|$, with the sign given by the sign of the coefficient m_d of the weight 3/2 modular form g.

5.6 An example.

We will write explicitly all calculations for the prime conductor $N = 17$.

From Cremona's tables we see that there is one isogeny class of elliptic curves of conductor $N = 17$ and rank zero. We take the curve number one in the class, that is, the strong Weil curve, in order to use the above formula to calculate (f, f).

This is, in the format $[a_1, a_2, a_3, a_4, a_6]$ given by

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

the curve $E = [1, -1, 1, -1, -14]$; its group of torsion points has 4 elements and the degree of the modular parametrization φ is 1.

To this curve we have to associate a modular form g of weight 3/2. It will be a linear combination of the theta series g_i associated to the lattices S_i^0, constructed from right orders R_i in the quaternion algebra B, ramified at 17 and ∞.

5.6.1 Calculation of the theta series g_i.

Remark. *We will use routines from* `qalgmodforms`*, written by A. Pacetti [22] for doing arithmetic over quaternion algebras and from* `qftheta3`*, written by G. Tornaria [32], that run under PARI-GP.*

Notation. $[b_0, b_1, b_2, b_3]$ *stands for* $b_0 + b_1 i + b_2 j + b_3 k$*, in the quaternion algebra* B*.*

We have to take a maximal order $\mathcal{O}$, in the quaternion algebra ramified at $N = 17$ and ∞, and calculate a set of representatives $I_1, ..., I_n$ of left ideals for the order $\mathcal{O}$. For each of these ideals I_i, we calculate the right (maximal or, equivalently, of level 17) orders R_i.

We then take the trace-zero elements of the lattices $\mathbb{Z} + 2R_i$. The modular forms g_i will be the theta series of these lattices.

This can be done in the following way with routines from the packages above:

`qsetprime(17)` sets the quaternion algebra ramified at $N = 17$ and ∞, and returns a maximal order $\mathcal{O}$ in it.

$$\mathcal{O} = \left[[\tfrac{1}{2}, 0, \tfrac{1}{2}, 0], [0, \tfrac{1}{2}, 0, \tfrac{1}{2}], [0, 0, \tfrac{1}{3}, \tfrac{1}{3}], [0, 0, 0, 1], 1\right]$$

`qdef` tells us which is the quaternion algebra we are in:

$$\texttt{qdef} = [-17, -3]$$

That is, the quaternion algebra ramified at $N = 17$ and ∞ is

$$B = \{b_0 + b_1 i + b_2 j + b_3 k, b_i \in \mathbb{Q}, i^2 = -17, j^2 = -3\}$$

We then have to calculate a set of representatives of left ideals for the maximal order $\mathcal{O}$:

$$\begin{aligned}\texttt{qidcl}(\mathcal{O}) = \big[\big[[\tfrac{1}{2}, 0, \tfrac{1}{2}, 0], [0, \tfrac{1}{2}, 0, \tfrac{1}{2}], [0, 0, \tfrac{1}{3}, \tfrac{1}{3}], [0, 0, 0, 1], 1\big]\ ,\\ \big[\big[1, 0, 1, 0], [1, 0, -1, 0], [0, 0, \tfrac{-1}{3}, \tfrac{-1}{3}], [\tfrac{1}{2}, \tfrac{-1}{2}, \tfrac{1}{6}, \tfrac{1}{6}], 2\big]\big]\end{aligned}$$

Thus, in this case, we have 2 different ideal classes. That is, the class number H is 2, and the left ideals classes are represented by:

$$\begin{aligned}I_1 &= \left[[\tfrac{1}{2}, 0, \tfrac{1}{2}, 0], [0, \tfrac{1}{2}, 0, \tfrac{1}{2}], [0, 0, \tfrac{1}{3}, \tfrac{1}{3}], [0, 0, 0, 1], 1\right]\\ I_2 &= \left[[1, 0, 1, 0], [1, 0, -1, 0], [0, 0, \tfrac{-1}{3}, \tfrac{-1}{3}], [\tfrac{1}{2}, \tfrac{-1}{2}, \tfrac{1}{6}, \tfrac{1}{6}], 2\right]\end{aligned}$$

We calculate the right orders:

$R_i =$ `qrorder(`I_i`)` gives a (maximal) right order for the ideal I_i

$$\begin{aligned}R_1 &= \left[[1, 0, 0, 0], [\tfrac{-1}{2}, 0, \tfrac{-1}{2}, 0], [\tfrac{-1}{2}, \tfrac{-1}{2}, \tfrac{1}{6}, \tfrac{1}{6}], [\tfrac{1}{2}, \tfrac{-1}{2}, \tfrac{-1}{6}, \tfrac{-1}{6}], 1\right]\\ R_2 &= \left[[1, 0, 0, 0], [\tfrac{-1}{2}, 0, \tfrac{1}{3}, \tfrac{-1}{3}], [\tfrac{-1}{2}, 0, \tfrac{2}{3}, \tfrac{1}{6}], [0, \tfrac{-1}{2}, \tfrac{-1}{2}, 0], 1\right]\end{aligned}$$

To calculate the lattices S_i^0 we have to take the trace-zero elements of $\mathbb{Z} + 2R_i$.

$\mathbb{Z} + 2R_i$ are generated by

$$\begin{aligned}\mathbb{Z} + 2R_1 &= \left[[1, 0, 0, 0], [0, 0, -1, 0], [0, -1, \tfrac{1}{3}, \tfrac{1}{3}], [0, -1, \tfrac{-1}{3}, \tfrac{-1}{3}], 1\right]\\ \mathbb{Z} + 2R_2 &= \left[[1, 0, 0, 0], [0, 0, \tfrac{2}{3}, \tfrac{-1}{3}], [0, 0, \tfrac{4}{3}, \tfrac{1}{3}], [0, -1, -1, 0], 1\right]\end{aligned}$$

Then we have:

$$S_1^0 = \left[[0,0,-1,0],[0,-1,\tfrac{1}{3},\tfrac{1}{3}],[0,-1,\tfrac{-1}{3},\tfrac{-1}{3}],1\right]$$
$$S_2^0 = \left[[0,0,\tfrac{2}{3},\tfrac{-1}{3}],[0,0,\tfrac{4}{3},\tfrac{1}{3}],[0,-1,-1,0],1\right]$$

and the corresponding theta series

$$g_i(\tau) = \frac{1}{2}\sum_{b\in S_i^0} q^{\mathbb{N}b} = \frac{1}{2}\sum_{x\in\mathbb{Z}^3} q^{x^t A_i x}$$

where A_i is one half the matrix of the bilinear form $\mathrm{Tr}(x\overline{y})$ restricted to the lattice S_i^0. More precisely, if f_1, f_2, f_3 is a $\mathbb{Z}$-basis for a lattice L then the matrix A of the bilinear form is given by

$$A = \frac{1}{2}\left(\mathrm{Tr}(f_i\overline{f_j})\right)$$

With $\mathtt{qgram}(\mathtt{S_i^0})/2$ we have the corresponding quadratic forms $A_i = \frac{1}{2}\mathtt{qgram}(\mathtt{S_i^0})$

$$A_1 = \begin{bmatrix} 3 & -1 & 1 \\ -1 & 23 & 11 \\ 1 & 11 & 23 \end{bmatrix}; \quad A_2 = \begin{bmatrix} 7 & -3 & -2 \\ -3 & 11 & -4 \\ -2 & -4 & 20 \end{bmatrix}$$

Next, we have to calculate the coefficients of the series

$$g_i(\tau) = \frac{1}{2}\sum_{x\in\mathbb{Z}^3} q^{x^t A_i x} \qquad i = 1, 2.$$

These are computed by the routine $\mathtt{qfminim3}(A_i, b, 0, 3)$ which returns a smallvector of length $b+1$ whose $k+1$ component is the number of elements of norm k, that is the $k-$ coefficient of the theta series given by the norm form A_i.

We calculate 10,000,000 coefficients of the modular forms g_i with
$\frac{1}{2}\mathtt{qfminim3}(\mathtt{A_i}, \mathtt{10000000}, \mathtt{0}, \mathtt{3})$.

5.6.2 Calculation of the weight 3/2 form g, under Shimura correspondence to f.

Once we have these forms, we need the "right" linear combination of them.

The number of units in the order R_i, which is the number of times "1" is represented in R_i, is calculated with $\mathtt{qrepnum}(R_i, 1)$. We have

$$w_1 = \mathtt{qrepnum}(\mathtt{R1}, \mathtt{1})/2 = 3$$
$$w_2 = \mathtt{qrepnum}(\mathtt{R2}, \mathtt{1})/2 = 1.$$

Now we look for the eigenvector of the Brandt's matrices corresponding to the modular form f defined above:

We know there exists a dimension one eigenspace $< v >$ of all the Brandt's matrices of prime level 17, such that $B_p(v) = a_p v$ for all prime p. Recall a_p are the eigenvalues of our normalized modular form f, under the action of the Hecke operators T_p.

With the PARI-GP routine `ellap(E,p)` we calculate:

$$a_2 = -1, a_3 = 0, a_5 = -2, a_7 = 4...$$

Next we calculate the Brandt matrix B_2:

$$B_2 = \texttt{brandt}(\mathcal{O}, 2) = \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix}.$$

Take, for example, $a_2 = -1$ and look for the kernel of

$$\texttt{B}_2 - (-\texttt{matid}(2)) = \begin{bmatrix} 1 & 3 \\ 1 & 3 \end{bmatrix}.$$

This kernel has already dimension one. We take any vector in it, for example $v = (-3, 1)$, and this will be an eigenvector of *all* Brandt matrices with the required eigenvalues.

If the above eigenspace had not been of dimension one, we would have needed to intersect with the kernel of $B_3 - a_3 I$ and so on, until we get a one dimensional eigenspace.

We divide the coordinates of the eigenvector $v = (-3, 1)$ by the respective number of units $w_1 = 3$, $w_2 = 1$ and set $e_f = (\frac{v_1}{w_1}, \frac{v_2}{w_2}) = (-1, 1)$. Thus, the weight 3/2 modular form we want, is

$$g = g_{\mathbf{17}} = \frac{v_1}{w_1} g_1 + \frac{v_2}{w_2} g_2 = -g_1 + g_2.$$

5.6.3 A formula for $|Ш_d|$.

Now we go for the $|Ш_d|$ values of the $(-d)$-quadratic twists of E. If m_d is the d-coefficient of the modular form $g_{\mathbf{17}}$, then we know that

$$\frac{L(f,1)}{\Omega_f} \; \frac{L(f \otimes \epsilon_{-d}, 1)}{\frac{2\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}} = \frac{\deg(\varphi) m_d^2}{< e_f, e_f >}.$$

We have:

- $< e_f, e_f >= w_1 (e_{f1})^2 + w_2 (e_{f2})^2 = 3(-1)^2 + 1.1^2 = 4.$

- From Cremona's tables we get $\deg(\varphi) = 1$.

- With PARI-GP we calculate $L(f,1)/\Omega_f = 1/4$ (we know this number is rational).

So the terms $L(f,1)/\Omega_f$ on the left cancels with $\deg(\varphi)/ < e_f, e_f >$ on the right. The ratio $\Omega_d / \frac{2\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}$ does not depend on d, in this particular case, and we have

$$\Omega_d = 2 \; \frac{\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}$$

The polynomials $p_d(x)$ defining the equations of the twisted curves E_d: $y^2 = p_d(x)$ have negative discriminant. Thus the real period Ω_d (and not twice of it) is what goes

in the equality of the Birch and Swinnerton-Dyer conjecture, applied now to the curve E_d (see 5.5 and recall that we have denoted by Ω the *real period* of E, see for this the first paragraph after 5.4.3).

So we have

$$\frac{L(f\otimes\epsilon_{-d})}{\frac{2\Omega_f\,\mathrm{Im}(\tau)}{\sqrt{d}}}=\frac{L(f\otimes\epsilon_{-d})}{\Omega_d}=\frac{|Ш_d|\prod_p c_{p,d}}{|\,\mathrm{Tor}(E_d)|^2}$$

The order of the group of torsion points of the $(-d)$-twists of E, is constantly equal to two: $|\,\mathrm{Tor}(E_d)|=2$.

Putting all this together, we get

$$|Ш_d|=\frac{4m_d^2}{\prod_p c_{p,d}}$$

This gives us a way for calculating, with the coefficients of the form $g_{\mathbf{17}}$, the values of $|Ш_d|$. Moreover, as the order of Ш is known to be a square, we write

$$\sqrt{|Ш_d|}=\frac{m_d}{\sqrt{\frac{\prod_p c_{p,d}}{4}}}.$$

This gives us a *signed-square root* of $|Ш_d|$, with the sign given by the sign of the coefficient m_d.

With the data obtained we make an histogram that consists simply on the orders of Ш obtained for the different values of d on the x-axis and the density or total amount, of each of them, on the y-axis.

This gives us the following figure

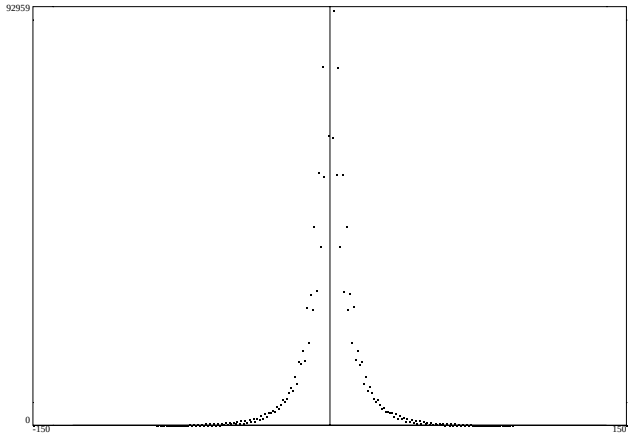

Figure 5.1: density distribution of S_d for $N=17$, $|\,\mathrm{Tor}(E)|=4$

5.7 Experiment and Observations.

As described in the above section, we have calculated the signed square-root of the analytic sha-values $|Ш_d|$, for the imaginary $(-d)$ quadratic twists E_d, of a strong

Weil curve E of prime conductor N, and rank zero, for the following conductors: $N = 11, 17, 19, 37, 67, 73, 89, 109, 139$ and for $N = 307$, this last one, in the four existing isogeny classes of curves, all of rank zero.

To be more precise, we picked a strong Weil curve E of prime conductor N and rank zero, and calculated from 3 to 10 million coefficients of the weight 3/2 modular form g associated to the weight 2 modular form f of the elliptic curve E.

For those d such that $(-d)$ is a fundamental discriminant and $\left(\frac{-d}{N}\right) \neq 1$ (that is, the sign of the functional equation is $+1$), we have, by Gross' formula and the Birch and Swinnerton-Dyer's conjecture, that either both $L(E_d, 1)$ and m_d equal zero, or both are nonzero and we get a relationship $|Ш_d| = q_d^2 m_d^2$, where q_d is a rational number that involves the product of the fudge factors $c_{p,d}$. Then the (integer) number $q_d m_d$ is a signed square root of the order of the Tate-Shafarevich group $Ш_d$, with the sign given by the coefficient m_d. We will denote by S_d this number:

$$\mathrm{S}_d = \begin{cases} q_d\, m_d & \mathrm{if} L(E_d, 1) \neq 0 \\ 0 & \mathrm{if} L(E_d, 1) = 0 \end{cases}$$

The zero coefficients m_d with $(-d)$ a fundamental discriminant and $\left(\frac{-d}{N}\right) \neq 1$ correspond to non-trivial zeros of $L(E_d, 1)$, so we can also obtain the density of nontrivial vanishing L-series, within the family.

From this information we made graphs for the density distribution of the S_d values obtained (over the total of d's with $(-d)$ fundamental and $\left(\frac{-d}{N}\right) \neq 1$).

5.7.1 Observations:

We will first state a number of observations made from the data obtained and then concentrate on the main point of this work which concerns the distribution of S_d under the presence of a nontrivial torsion point on the elliptic curve E.

From the graphs obtained, it is clear that there is a symmetry in the behavior of the positive-negative S_d values. The sign of S_d seems to play no role. For this reason, we will mostly restrict our attention to the positive part in further analysis.

In all examples, the density graphs split essentially in two pointed curves. This splitting responds to the parity of the S_d values. The two density-pointed-curves we get correspond to odd values of S_d and to even values of S_d.

Further, when the base elliptic curve E has nontrivial torsion point, of prime order ℓ, these two density-pointed-curves show some "noise", or "shadow" (see figures 5.2 and 5.3).

The *shape* or behavior of the curves in the graphs made, are ruled by the order of the group of torsion points of $E(\mathbb{Q})$. We describe these situations.

- **Curves E with trivial torsion.**

  These correspond to conductors $N = 67, 109, 139$, and 307. In each case the torsion group of the elliptic curves E is trivial and we get, among its twists, two well differentiated density-pointed-curves.

These correspond to odd values of S_d for the upper density-curve and even values of S_d for the bottom one. Odd values of Ш are more occurring than even ones. See figure 5.2.

- **Elliptic curves E with odd nontrivial torsion.**

These correspond to the elliptic curves of conductors $11, 19$ and 37. The groups of torsion points of $E(\mathbb{Q})$ have, respectively, orders $5, 3$ and 3. These are the only elliptic curves of prime conductor with a nontrivial odd torsion point. It is known that for prime conductors, the order of the group of torsion points is one or two (when the conductor is 64+ a square), except for $N = 11, 19, 37$ and for $N = 17$ in which the order of torsion is 4 (see [9]).

This situation is different from the one above. In the density graphs of these three elliptic curves, is that we observe the "noise" introduced by a nontrivial torsion point of prime order ℓ.

Graphically, we remark that some points distinguish from their neighbors by having more density. These points correspond to those values of Ш divisible by the order of the group of torsion points. As an example of what is observed, pick the graph for the curve of conductor $N = 11$. Pick up a point in the density graph of (say) odd values of S_d, that has 'slightly' a bigger density than its neighbors points in the same 'odd value curve'. The next point on the left with the same 'property' will be the fifth, and so on. See figure 5.3. This is clearly corroborated by the data obtained.

It goes analogously for $N = 19, 37$ and three.

We will afterward return on this.

Here too, odd values of Ш are more occurring than even ones. Of the two density-pointed-curves, the one above corresponds to odd values of S_d, while the one below corresponds to even values.

It is to remark here that none of these curves has a torsion point of even order.

- **Curves E with even torsion.**

The behavior of the graphs for elliptic curves of conductors $N = 17, 73$ and 89 is different in the following sense. There are also two density-pointed-curves corresponding to even and odd values of S_d. However, they cross each other. This, is different. The other significant difference is that now even values of Ш are more frequent than the odd ones. *Small* even values of S_d are more frequent than the odd ones, as for *big* values of S_d the odd ones are more frequent than even ones. This 'crossing' of the even/odd density curves is clearly seen in the logarithm-graph, as shown in picture 5.4.

The orders of the groups of torsion points of the elliptic curves considered are, respectively, 4, 2 and 2.

Here, we again remark on some *noise* produced by the torsion of E, as those S_d divisible by $|\operatorname{Tor}(E)| = 4$ or 2, (for $N = 17$ or $N = 73, 89$, respectively) distinguish from their neighbors by having a greater density.

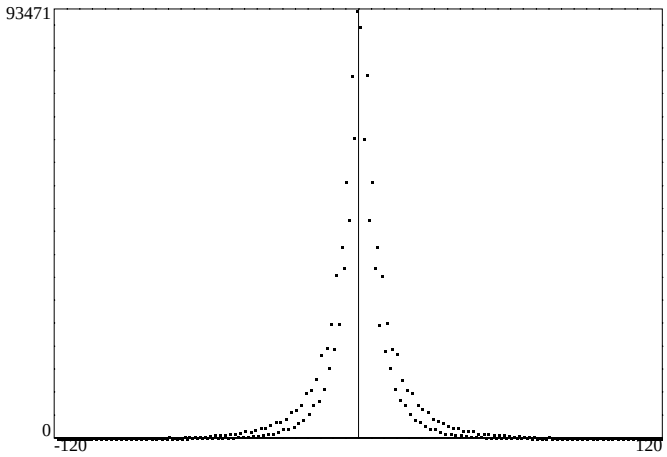

Figure 5.2: density distribution of S_d for $N = 67$, $|\mathrm{Tor}(E)| = 1$

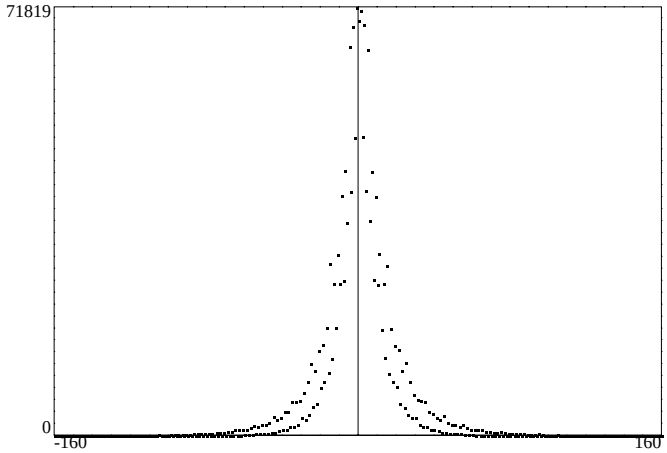

Figure 5.3: density distribution of S_d for $N = 11$, $|\mathrm{Tor}(E)| = 5$

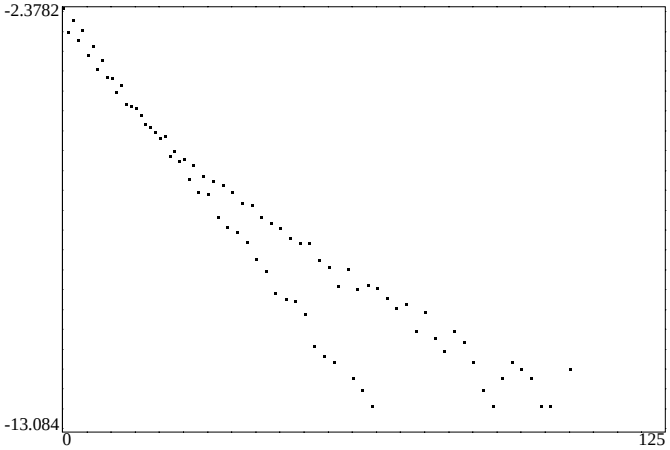

Figure 5.4: Logarithm-graph for curve E of conductor N=17 of even torsion.

The graphs and the data obtained arise the following questions:

What role plays the presence of an ℓ torsion point on the elliptic curve E? What can we say about the density of Ш values divisible by a prime p, among imaginary quadratic twists of a fixed elliptic curve E?

When the curve E has a torsion point of prime order ℓ, there seem to be a greater proportion of S_d values divisible by ℓ than in the general case. Can we give some reason for this?

5.7.2 What happens with Ш?

In [6] C. Delaunay gives an heuristic for the probability of Ш being divisible by a prime number p among twists of elliptic curves. It is important to mention here that Delaunay orders the elliptic curves and its twists by conductor. This can make a significant difference from picking an elliptic curve and all its twists.

In [4] Conrey, Keating, Rubinstein and Snaith obtain conjectures for the value distribution of the Fourier coefficients m_d, based on conjectures from random matrix theory for the value distribution of $L(E_d, 1)$. They observe that, for primes p dividing the order of the torsion group of E, the probability that the Fourier coefficient m_d is divisible by p, deviates from Delaunay's prediction for the probability of $|Ш|$ being divisible by a given prime.

In [26] Rubinstein makes a graph of the distribution of the coefficients m_d of the modular form of weight 3/2, normalized by the product of the fudge factors, for the elliptic curve of conductor $N = 11$. He points out that in the histogram it is seen that primes 2 and 5 behave differently. He also compares the density of coefficients divisible by primes p, with Delaunay's prediction [6] for the probability of $|Ш|$ being divisible by p among elliptic curves of rank zero.

In Table 1 below, we show, for each conductor N, the density of S_d divisible by small primes p, among twists of an elliptic curve or conductor N. We have added $p = 4$ to the table, in order to have in the list all the orders of the groups of torsion points of the elliptic curves analyzed.

`T` is the order of the group of torsion points, `I` denotes the isogeny class, `mult n` stands for the density of curves E_d whose S_d-value is multiple of n; `zeros` is the density of curves E_d with positive analytic rank, that is, the density of those curves in which the corresponding L-series vanishes non-trivially at the symmetry center $s = 1$ (recall that we are only looking at quadratic twists in which the sign of the functional equation is $+1$) and finally `tot` is the total number of twists calculated.

`CL` is a Cohen-Lenstra heuristics on class numbers which we will explain later and `D` is Delaunay's heuristics for $|Ш|$ being divisible by a prime p.

If we read this table by columns, we remark on the following.

There is, in general, around 40% of even S_d-values among the twists of an elliptic curve. However, this percentage increases to more than 50% exactly when the elliptic curve E has even torsion ($N = 17, 73, 89.$).

If we look now at S_d-values divisible by 3 there are, in the examples calculated, about 35% of them. This, except for conductors $N = 19$ and $N = 37$ in which the

N	T	I	zeros	mult 2	mult 3	mult 4	mult 5	mult 7	mult 11	m
11	5	A	0.042	0.369	0.353	0.185	0.234	0.146	0.097	10
17	4	A	0.079	0.592	0.353	0.303	0.210	0.156	0.115	10
19	3	A	0.065	0.371	0.407	0.189	0.206	0.150	0.105	3
37	3	B	0.054	0.440	0.413	0.223	0.207	0.149	0.101	10
67	1	A	0.058	0.403	0.355	0.204	0.208	0.150	0.103	10
73	2	A	0.086	0.539	0.356	0.269	0.212			3
89	2	B	0.072	0.507	0.354	0.257	0.209			3
109	1	A	0.076	0.391	0.322	0.199	0.208	0.153	0.109	3
139	1	A	0.073	0.394	0.354	0.192	0.209			3
307	1	A	0.091	0.390	0.354	0.200	0.210			3
307	1	B	0.087	0.405	0.354	0.208	0.210			3
307	1	C	0.076	0.391	0.354	0.199	0.207			3
307	1	D	0.071	0.401	0.354	0.205	0.209			3
D	-	-	-	**0.580**	**0.360**	-	**0.206**	**0.145**	**0.091**	
CL	-	-	-	-	**0.439**	-	**0.239**	**0.163**	**0.099**	
26	3	A	0.043	-	0.415	-	0.207	0.147	0.098	10
26	7	B	0.036	-	0.353	-	0.207	0.160	0.095	10

Table 5.1: density of S_d values divisible by $2, 3, 4, 5, 7, 11$

group of torsion points of the elliptic curve E has order 3. Here this percentage increases to 40%. Something similar is seen for S_d-values divisible by 4 and 5.

In what follows we will explain the reason for this behavior and give a precise heuristic for the density of S_d values divisible by the prime ℓ when the elliptic curve E has an ℓ torsion point.

5.7.3 A congruence between modular forms of weight $3/2$.

Remark on notation: For this section we are going to drop the subscript $3/2$ in $\mathcal{H}_{3/2}$ and replace it instead, by the conductor N. Thus by $\mathcal{H}_{11}$ we mean the Eisenstein series of weight $3/2$ and level $N = 11$.

B. Gross in [9] mentions, for $N = 11$, the following congruence between the corresponding modular form of weight $3/2$, $g_{\mathbf{11}}$ and the weight $3/2$ Eisenstein series $\mathcal{H}_{\mathbf{11}}$:

$$2g_{\mathbf{11}} = -2g_1 + 2g_2 \equiv 3g_1 + 2g_2 = 6\mathcal{H}_{\mathbf{11}} \qquad (5M^*)$$

This gives, in particular, that the coefficients of both modular forms are congruent modulo 5, which is the order of the torsion group of the elliptic curve of conductor 11. The interest in this congruence, is that *we know* how the coefficients of the weight $3/2$ Eisenstein series $\mathcal{H}_N$ are. They are related to class numbers of quadratic extensions of $\mathbb{Q}$. We will exploit this fact.

We can check by hand that a similar situation occurs for conductors $N = 19$ and $N = 37$ and the prime $\ell = 3$. However, this congruence modulo ℓ among the weight

3/2 modular forms should reflect that we can *lift* through the quaternion algebra B a well known congruence among weight 2 modular forms.

We are going to leave this for the next chapter, and analyze here the information we can obtain on $|Ш|$ from the before mentioned congruences, among the respective weight 3/2 modular forms and Eisenstein series.

5.7.4 Ш divisibility by ℓ, for conductor N prime.

For a prime conductor N there are three elliptic curves with a nontrivial torsion point of odd prime order ℓ. These are the elliptic curves of conductors $N = 11, 19, 37$ which have, respectively, a torsion point of order $5, 3$ and 3.

We have the following congruences:

- For $N = 11$, we have the following congruence between the modular form of weight 3/2 and level 11, g, and the weight 3/2, level 11 Eisenstein series $\mathcal{H}_{11}$:

$$2g = -2g_1 + 2g_2 \equiv 3g_1 + 2g_2 = 6\mathcal{H}_{11} \mod 5$$

  or $g \equiv 3\mathcal{H}_{11} \mod 5$. Further, $|Ш_d| = \dfrac{m_d^2}{2^*}$

- Similarly we have for $N = 19$, $N = 37$ and their respective modular forms:

$$g \equiv \mathcal{H}_* \mod 3$$

  and, again $|Ш_d| = \dfrac{m_d^2}{2^*}$.

By 2^* we mean some power of 2 which, anyhow, does not affect divisibility by odd primes.

What we see is that the order of the group of Tate-Shafarevich of the $-d$-quadratic twist of an elliptic curve E is given by the square of the d-coefficient of the corresponding weight 3/2 modular form g, m_d, divided by some power of 2. Thus for ℓ odd, $|Ш_d|$ is divisible by the prime ℓ if and only if the coefficient m_d is divisible by ℓ. Further, by the congruence modulo ℓ above, m_d is divisible by ℓ if and only if the d-coefficient of $\mathcal{H}_*$ is divisible by ℓ.

The coefficients of the Eisenstein series $\mathcal{H}_*$ are related to class numbers of quadratic fields $\mathbb{Q}(\sqrt{-d})$ in a way we are going to explain below.

Thus we can give heuristics for the density of Ш values divisible by the order of the group of torsion points for conductors 11, 19 andv 37 by applying the Cohen-Lenstra [3] heuristics on class groups of number fields.

Before explaining this fact, we need to define *Hurwitz's class number*.

5.7.5 The Hurwitz's class number.

Let $-d$ be a negative discriminant, and K the imaginary quadratic extension of $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{-d})$. Let $\mathcal{O}$ be an order of discriminant $-d$ in K, denote $h(\mathcal{O})$ the order of the finite group $Pic(\mathcal{O})$ and $u(\mathcal{O})$ the order of $\mathcal{O}^*/\mathbb{Z}^*$. Then $u(\mathcal{O}) = 1$ unless $d = -3, -4$ which gives $3, 2$, respectively.

Hurwitz's class number is given by

$$H(d) = H(\mathcal{O}) = \sum_{\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_K} \frac{h(\mathcal{O}')}{u(\mathcal{O}')}$$

Gross, in [9], uses the prime N to define the modified invariant $H_N(d)$ by

$$H_N(d) = \begin{cases} 0 & \text{if } N \text{ splits in } \mathcal{O} \\ H(\mathcal{O}) & \text{if } N \text{ is inert in } \mathcal{O} \\ \frac{1}{2}H(\mathcal{O}) & \text{if } N \text{ is ramified in } \mathcal{O} \text{ but does not divide the conductor of } \mathcal{O} \\ H_N(d/N^2) & \text{if } N \text{ divides the conductor of } \mathcal{O} \end{cases}$$

This number $H_N(d)$ is zero unless $-d \equiv 0, 1\ (4)$ and $\left(\frac{-d}{N}\right) \neq 1$. For $W = \prod_{i=1}^{n} w_i$, we have that $WH_N(d)$ is integral.

If d is such that $(-d)$ is a fundamental discriminant, which is a condition we request for, otherwise, we would be repeating twisted curves, then $\mathcal{O} = \mathcal{O}_d$ and $H(\mathcal{O}_d) = h(d)/u(\mathcal{O}_d)$, where $\mathcal{O}_d$ is the ring of integers in K and $h(d)$ its class number of K.

Furthermore, if we request that $\left(\frac{-d}{N}\right) \neq 1$, which we do for, otherwise, the L-series of the twisted curve E_d vanishes trivially, then N is either inert or ramifies in $\mathcal{O}_d$ and then $H_N(d)$ becomes:

$$H_N(d) = \begin{cases} \dfrac{h(d)}{u(\mathcal{O}_d)} & \text{if } N \text{ is inert in } K \\ \dfrac{1}{2}\dfrac{h(d)}{u(\mathcal{O}_d)} & \text{if } N \text{ is ramified in } K \end{cases}$$

Recall that $u(\mathcal{O}_d) = 1$, except for exactly 2 values of d.

Thus $H_N(d)$ is the class number $h(d)$ of $\mathbb{Q}(\sqrt{-d})$ or $\frac{1}{2}h(d)$ except for, at most, 2 values of d.

Let $\mathcal{H}_N$ be the weight $3/2$ Eisenstein series defined by

$$\mathcal{H}_N = \sum_{i=1}^{n} \tfrac{1}{w_i}\, g_i$$

where g_i are the theta series of the lattices S_i^0 in the quaternion algebra ramified at N and ∞ and w_i half the number of units of the right orders R_i, as stated before.

B. Gross proves that $\mathcal{H}_N$ has Fourier expansion

$$\mathcal{H}_N = \frac{N-1}{24} + \sum_{d>0} H_N(d)\ q^d$$

5.7.6 The Cohen Lenstra heuristics and $|Ш|$ divisibility by 5 for conductor $N = 11$

To ease the notation, we are going to fix on the elliptic curve of conductor 11, which has a 5-torsion point. Anything said in this section goes for any other congruence $g \equiv c\mathcal{H} \mod \ell$ as long as c is prime to ℓ, ℓ is odd, and $|Ш_d|$ is given by m_d^2 times any constant prime to ℓ (which, usually, will be 1 over a power of 2). Here $g = \sum m_d q^d$.

From the congruence $g \equiv 3\mathcal{H}_{11} \mod 5$ we have, in particular

$$m_d \equiv 3H_{11}(d)\ (5). \tag{5.6}$$

We are to use now this congruence and the Cohen-Lenstra heuristics for class numbers to explain the density of $|Ш|$ divisible by 5 in the family of quadratic twists of the elliptic curve $[0, -1, 1, -10, -20]$ of conductor 11.

The order of $Ш_d$ is given by m_d^2 divided by a power of 2. So, the density of S_d values divisible by 5 is the density of m_d's divisible by 5.

The congruence (5.6) shows that

$$\{d : m_d \equiv 0\ (5)\} = \{d : h(d) \equiv 0\ (5)\}$$

where both sets are taken over d's with $-d$ a fundamental discriminant and $\left(\frac{-d}{11}\right) \neq 1$.

If we make the assumption that a class number being divisible by a prime p and having a particular Kronecker symbol are independent facts, which numerically it is so, then we have:

$$\frac{\left|\left\{0 < d < X : -d \in F, h(d) \underset{5}{\equiv} 0 \text{ and } \left(\frac{-d}{11}\right) \neq 1\right\}\right|}{|\left\{0 < d < X : -d \in F \text{ and } \left(\frac{-d}{11}\right) \neq 1\right\}|} \sim \frac{\left|\left\{0 < d < X : -d \in F, h(d) \underset{5}{\equiv} 0\right\}\right|}{|\left\{0 < d < X : -d \in F\right\}|}$$

where F is the set of fundamental discriminants and by $\sim$ we intend that the quotient goes to 1 as X goes to infinity.

In [3], Cohen and Lenstra give heuristics for the probability that the class number of a quadratic imaginary extension of $\mathbb{Q}$ is divisible by a prime p, as follows:

$$\lim_{X\to\infty} \frac{|\left\{0 < d < X : -d \in F \text{ and } h(d) \equiv 0\,(p)\right\}|}{|\left\{0 < d < X : -d \in F\right\}|} = f(p)$$

$$f(p) = 1 - \prod_{i\geq 0}(1 - \frac{1}{p^i}) = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^7} + \dots$$

By the assumption made above we can say that $f(5) \sim 0.239$ is the probability of S_d being divisible by 5 among negative quadratic twists for conductor $N = 11$.

5.7.7 $|Ш|$ divisibility by 3 for N=19 and N=37

This exact argument explains the density of Ш values divisible by 3 for conductors $N = 19$ and $N = 37$ as we have the following congruency holds among the respective weight 3/2 modular form and Eisenstein series, for both conductors:

$$g \equiv \mathcal{H}_*\,(3M^*)$$

Then we have in these two cases, the density of Ш- values divisible by 3 is $f(3) \sim 0.439$.

These examples complete the case of prime conductors. We have proved

Theorem 5.7.1. *Let E be an elliptic curve of prime conductor N. Suppose E has a rational torsion point of prime order $\ell > 2$. Then the proportion of* Ш *values divisible by ℓ in the family of imaginary quadratic twists of E, with $\left(\frac{-d}{N}\right) \neq 1$, is the same as the proportion of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ divisible by ℓ, with $\left(\frac{-d}{N}\right) \neq 1$.*

If we assume the Cohen-Lenstra heuristics on the probability of class numbers being divisible by a prime, and assume that being divisible by a prime is an independent fact from having a determinate Kronecker symbol, then this proportion is equal to

$$f(\ell) = 1 - \prod_{i \geq 0} (1 - \frac{1}{\ell^i}) = \frac{1}{\ell} + \frac{1}{\ell^2} - \frac{1}{\ell^3} - \frac{1}{\ell^7} \ldots$$

However, we want to prove that this congruence in weight 3/2 is arized by a congruence in weight 2. This will permit us to generalize the situation for non-prime conductors N.

5.7.8 Further comments

In table 5.1 we have included the densities of $|Ш|$ divisible by p for curves $26A$ and $26B$ (as in Cremona's tables), which have, respectively, group of torsion points of orders 3 and 7. The ternary forms and linear combination that gives the weight 3/2 modular forms, have been taken from Tornaria's data at the web [32]. We restricted for simplicity to d's coprime to the conductor and we have an additional restriction on the sign of $\left(\frac{-d}{p}\right)$, for primes p dividing N.

It is clearly seen that $p = 3$ and $p = 7$ have bigger density for curves $26A$ and $26B$ respectively, and though the size of the experiment is rather small, this densities are not far from Cohen-Lenstra's prediction. We did not take into account $p = 2$ as we have not divisible by the fudge factors to obtain the order of Ш. The situation for non-prime conductors will be analyzed in chapter 7.

For completeness we compared also with Delaunay's heuristics for the probability of order of Ш being divisible by a prime p. We remark that Delaunay's heuristics are for elliptic curves of rank zero, ordered by conductor. However for small odd primes p this prediction seem to be applicable to families of negative quadratic twists, even rank, of an elliptic curve. This density is denoted by **D** in table 5.1. Though for $p = 2$ this prediction does not seem to apply, as in general the density of even values of Ш is less than 50%, it does seem to be applicable for $N = 17$. If we are to suppose that if a prime p divides $\mathrm{Tor}(E)$ then the density of $|Ш|$ values divisible by p is bigger than if it does not, then this case goes in the same direction, as the group of torsion points of E is of order 4.

CHAPTER 6

The Lift of a congruence for prime conductor N.

For elliptic curves E of prime conductor N, it is a known fact that when E has a point of prime torsion ℓ, the weight 2 modular form f attached to E is congruent modulo ℓ to the normalized Eisenstein series in $M_2(N)$. Thus, the congruence among the respective weight 3/2 modular forms we have seen in the last chapter, should be a reflection of the situation occurring in weight 2.

We show that, in fact, this is what happens. The congruence occurring in weight 2 can be lifted, through the quaternion algebra, to a congruence modulo the prime ℓ among a modular form of weight 3/2, under Shimura correspondence to f, and an Eisenstein series $\mathcal{H}_{3/2}$.

We have seen in the last chapter that the relevance of this situation, in what concerns Ш, is that Eisenstein series are known to be related to class numbers of quadratic fields.

6.1 A congruence among two weight two modular forms.

In §2.7 we defined, for N prime, a series

$$e_2(z) = E_2(z) - NE_2(Nz)$$

where E_2 is the non holomorphic Eisenstein series of weight 2 and level 1. We showed that $e_2(z)$ is a modular form of weight 2 for $\Gamma_0(N)$ and that it has q-expansion

$$e_2(z) = \frac{N-1}{24} + \sum_{n\geq 1} \sigma(n)_N \, q^n.$$

Recall that $\sigma(n)_N$ denotes the sum of the divisors of n which are prime to N. The space of Eisenstein series in $M_2(N)$, for N prime, is one dimensional, and it is thus generated by $e_2(z)$.

Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor N, with a torsion point of prime order ℓ.

Let $f = \sum_{n\geq 1} a_n\, q^n$ be the modular form of weight 2 and level N associated to E.

We have seen in proposition 1.6.1 that for any prime p of good reduction, thus for any $p \neq N$,

$$a_p \equiv 1 + p \mod \ell.$$

In 2.8.2 and 2.8.3, we studied the primes of bad reduction and obtained, in particular, $a_N = 1$. This gave us the congruence $f \equiv e_2 \mod \ell$.

We will state this fact in a separate proposition, as it is the departure step in our chain of congruences.

Proposition 6.1.1. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor N. Assume E has a torsion point defined over $\mathbb{Q}$, of odd prime order ℓ. Let f be the weight 2, level N modular form associated to E and $e_2(z)$ the weight 2 normalized Eisenstein series for $\Gamma_0(N)$. Then $f \equiv e_2(z) \mod \ell$.*

6.2 A congruence among eigenvectors of Brandt matrices.

By the work of Jacquet and Langlands, we know that to each modular form $f \in M_2(N)$, which is a newform, and thus an eigenfunction for all Hecke operators, with $T_p f = a_p f$, corresponds a one dimensional eigenspace $< v >$ of the Brandt matrices of prime level N, in the quaternion algebra ramified at N and ∞, such that

$$B_p v = a_p v.$$

This last equality valid, in principle, for $p \neq N$ is also true for $p = N$.

To the Eisenstein series e_2 defined above, corresponds the eigenvector $u = (1, 1, ..., 1)$, as we know by proposition 4.3.3 that the row sums of the Brandt matrices B_n are $\sigma(n)_N$. Thus

$$B_p u = \sigma(p)_N u.$$

When E has a rational point of torsion ℓ, the eigenvalues a_p and $\sigma(p)_N$ turn out to be congruent modulo ℓ for all p. What can we say about the eigenvectors v and u modulo ℓ ?

Suppose we know that the Brandt matrices reduced modulo ℓ have one dimensional eigenspace for the reduced eigenvalues $\sigma(p)_N$. Then we would have $\lambda v \equiv u \mod \ell$, which is the relation we need to deduce that the respective modular forms of half integer weight are congruent modulo ℓ.

6.2.1 Multiplicity one.

In this section we are going to see that this is in fact the case. If we consider the reduced Brandt matrices modulo the prime ℓ, there is a dimension one eigenspace for the system of eigenvalues $\sigma(n)_N$.

We will need some results on the *Eisenstein Ideal* which can be found in the work of Mazur [17] §5, §9.

Consider the weight 2 Eisenstein series for $\Gamma_0(N)$

$$e_2(z) = \frac{N-1}{24} + \sum_{n\geq 1} \sigma(n)_N \, q^n$$

Remove the constant term and consider the formal power series

$$\delta = \sum_{n\geq 1} \sigma(n)_N q^n$$

By the work of Mazur [17] chapter II §5, δ is a modular form modulo an integer m if and only if m divides $\frac{N-1}{2}$ and it is a cusp form if m divides the exact numerator, n, of $\frac{N-1}{12}$.

Note that, if $f \equiv e_2 \mod \ell$, for a prime ℓ and a cusp form f, then δ is clearly a cusp form modulo ℓ and thus ℓ divides n.

Let R be the ring $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$, and $M(R)$, $S(R)$ the space or modular forms and cusp forms, of weight 2 and level N, with coefficients in R. If $f \in S(R)$ is an eigenvector for all T_p, $p \neq N$ and for T_N then f is determined, up to a scalar, by the eigenvalues.

By the Hecke algebra $\mathbb{T}$ we shall mean the algebra generated by T_p for $p \nmid N$ and T_N.

Let $\mathcal{M} \subset \mathbb{T}$ be a maximal ideal with residue field k of characteristic p. Denote $S(\mathbb{F}_p)[\mathcal{M}]$ the kernel of the ideal $\mathcal{M}$. This may be viewed as a k-vector space.

Proposition 6.2.1. *$S(\mathbb{F}_p)[\mathcal{M}]$ is of dimension one over k.*

The *Eisenstein ideal* $\mathcal{I} \subset \mathbb{T}$ is the ideal generated by the elements $1 + p - T_p$ and $1 - T_N$. Thus any element in $S(R)[\mathcal{I}]$ is an eigenvector for the operators T_p $(p \neq N)$ and T_N, with eigenvalues $c_p = 1 + p$ $(p \neq N)$ and $c_N = 1$.

In $R[[q]]$ the generating eigenvector for these c_p eigenvalues is the power series δ. Thus the q-expansion of any element in the R-module $S(R)[\mathcal{I}]$ is a scalar multiple of δ.

Proposition 6.2.2. *(Mazur)*

1) *Let m be any integer divisible by n = the exact numerator of $\frac{N-1}{12}$. Then $S(\mathbb{Z}/m\mathbb{Z})[\mathcal{I}]$ is a cyclic group of order n, generated by $\frac{m}{n}\delta$.*

2) *$\mathbb{T}/\mathcal{I} = \mathbb{Z}/n\mathbb{Z}$; the Eisenstein ideal $\mathcal{I}$ contains the integer n.*

For details on this see [17] §9.

A prime ideal $\mathcal{M}$ in the support of the Eisenstein ideal is called an Eisenstein prime. The Eisenstein primes $\mathcal{M}$ are in one-to-one correspondence with the primes $p \mid n$. For $p \mid n$ the Eisenstein prime corresponding to p is given by $\mathcal{M} = (\mathcal{I}, p)$. Then $\mathbb{T}/\mathcal{M} = \mathbb{F}_p$ and $\mathcal{M}$ is a maximal ideal and it is the unique Eisenstein prime whose residue field is of characteristic p.

Let $\mathcal{X}$ denote the free $\mathbb{Z}$ module of divisors supported on the set of singular points of the curve $X_0(N)$. The Hecke algebra $\mathbb{T}$ acts on the module $\mathcal{X}$. Let $\mathcal{M}$ be an Eisenstein

prime of residue characteristic ℓ. As part of a stronger result, Emerton proves in [8], that the $\mathbb{T}/\mathcal{M}$-module $\mathcal{X}/\ell\mathcal{X}[\mathcal{M}]$ is of rank one (see the proof of Theorem 4.2). Recall that $\mathbb{T}/\mathcal{M} \simeq \mathbb{F}_\ell$, thus the set of points in $\mathcal{X}/\ell\mathcal{X}$ annihilated by the Eisenstein prime $\mathcal{M}$ is one dimensional over $\mathbb{F}_\ell$. This is what we need.

We will rephrase this last paragraph in a way more familiar to our present setting.

We can think the module $\mathcal{X}$ as the $\mathbb{Z}$-module generated by the ideal classes $I_1, ..., I_n$ of the maximal order $\mathcal{O}$ in the quaternion algebra B ramified at N and at ∞. We will denote this $\mathbb{Z}$-module by $\mathcal{X}(\mathcal{O})$. The action of the Hecke algebra $\mathbb{T}$ on $\mathcal{X}$ corresponds to the action of the Brandt matrices in $\mathcal{X}(\mathcal{O})$ as follows:

Let $x = \sum_{i=1}^n m_i I_i$, then B_n acts by multiplication: if $(s_1, ..., s_n)^t = B_n(m_1, ..., m_n)^t$, then $B_n.x = \sum_{i=1}^n s_i I_i$.

To see that these two settings are parallel situations see, for example, [8] and [23].

The eigenvectors u and v correspond to the elements $X = \sum I_i$ and $Y = \sum v_i I_i$ in $\mathcal{X}(\mathcal{O})$, whose eigenvalues are congruent modulo ℓ. Let us denote by $\mathbb{B}$ the $\mathbb{Z}$-algebra generated by the Brandt matrices. Consider the maximal Eisenstein prime $\mathcal{M}$ of $\mathbb{B}$ given by $\mathcal{M} =< B_p - (p+1)\,\mathrm{id}, B_N - \mathrm{id}, \ell >$. Then $\mathbb{B}/\mathcal{M} = \mathbb{F}_\ell$.

Call $\bar{u}$, $\bar{v}$ the reductions of u and v modulo ℓ. Thus $\bar{u}$ and $\bar{v}$ correspond to the elements $\bar{X}, \bar{Y}$ in $\mathcal{X}(\mathcal{O})/\ell\mathcal{X}(\mathcal{O})$ that are in the kernel of the action of $\mathcal{M}$. Then $\bar{X}, \bar{Y} \in \mathcal{X}(\mathcal{O})/\ell\mathcal{X}(\mathcal{O})[\mathcal{M}]$ which is a $\mathbb{B}/\mathcal{M}$-module of rank one. That is, the $\mathbb{F}_\ell$ vector space $\mathcal{X}(\mathcal{O})/\ell\mathcal{X}(\mathcal{O})[\mathcal{M}]$ is of dimension one and $\bar{X} = \lambda\bar{Y}$. Thus $u \equiv \lambda v \mod \ell$ for some $\lambda \in \mathbb{F}_\ell^\times$.

6.3 A congruence among modular forms of weight $3/2$.

Recall how we construct the weight $3/2$ modular form g corresponding to our f, once we have the eigenvector $v = (v_1, ..., v_n)$.

$$g = \sum \frac{v_i}{w_i} g_i$$

where g_i are theta series of weight $3/2$ and level $4N$.

To the Eisenstein series e_2 corresponds the weight $3/2$ Eisenstein series

$$\mathcal{H}_{3/2} = \sum \frac{1}{w_i} g_i.$$

If the eigenvectors v and u are proportional modulo ℓ, that is, $u \equiv \lambda v \mod \ell$, then we automatically have $\lambda g \equiv \mathcal{H}_{3/2} \mod \ell$. This, provided that the number of units w_i in the right orders R_i are prime to ℓ. For $\ell = 5, 7$ there is nothing to do, as $w_i/12$.

It is known that (see [9] §1) the product $\prod_{i=1}^n w_i$ is independent of the choice of $\mathcal{O}$ and equals the exact denominator of $\dfrac{N-1}{12}$.

Suppose $\ell = 3$. Then E has a point P of order 3 which reduces to a non-singular point in $\widetilde{E}_N$.

We saw in 1.4 the structure of the group of non-singular points in $\widetilde{E}_p$ for primes of bad reduction. In particular, $\widetilde{E}_N$ has order $N-1$ as the sign of the Atkin-Lehner at

N is -1. Thus 3 divides $N-1$ and it cannot divide the denominator in $\dfrac{N-1}{12}$. Then we have,

$$3 \nmid \prod_{i=1}^{n} w_i.$$

and

$$\lambda g \equiv \mathcal{H}_{3/2} \mod \ell \quad (\lambda \in \mathbb{F}_\ell^\times).$$

For N prime we know the q-expansion of $\mathcal{H}_{3/2}$ and how its coefficients are related to class numbers of imaginary quadratic number fields. We rewrite here this result from last chapter

$$\mathcal{H}_{3/2} = \frac{N-1}{24} + \sum_{d>0} H_N(d)\ q^d$$

where

$$H_N(d) = \begin{cases} \dfrac{h(d)}{u(\mathcal{O}_d)} & \text{if } N \text{ is inert in } K \\ \dfrac{1}{2}\dfrac{h(d)}{u(\mathcal{O}_d)} & \text{if } N \text{ is ramified in } K \end{cases}$$

and $h(d)$ is the class number of $\mathbb{Q}(\sqrt{-d})$.

CHAPTER 7

N square free.

In this chapter we analyze the situation for an elliptic curve E with square free conductor N. We give an Eisenstein series congruent to the weight 2 modular form f corresponding to E, when this last has an ℓ torsion point. Recall that we are assuming $\ell > 2$.

We show this Eisenstein series is represented in the quaternion algebra B ramified at exactly those primes $p \mid N$ for which the Atkin-Lehner involution W_p has sign equal to -1.

We believe that the situation in the last chapter is general, and this congruence in weight 2 can be lifted to a congruence in weight 3/2. This reduces to a problem of *multiplicity one* modulo the prime ℓ. The congruence can be lifted, if there is a one dimensional eigenspace of the Brandt matrices associated to the eigenvector $(1, 1, ..., 1)$ corresponding to the Eisenstein series mentioned before. If this is the case, the weight 3/2 modular form under Shimura correspondence to f, is congruent modulo ℓ to certain weight 3/2 Eisenstein series, whose coefficients are related to class numbers of imaginary quadratic twists.

We give numerical examples concerning this situation and conjecture an analog result as in theorem 5.7.1.

7.1 Generalities.

As before, E will be an elliptic curve of rank zero and conductor N, which we will assume to be square free. The sign of the functional equation for the L-series of E must be $+1$ or, equivalently, the sign of the Atkin-Lehner W_N is -1. As the sign of W_N equals the product of the signs of the Atkin-Lehner at each prime $p \mid N$ (see (2.5)), we have that there is an odd number of primes $p \mid N$ for which the sign of $W_p = -1$.

Along this chapter we will write $N = DM$, where D is the product of those primes $p \mid N$ such that the Atkin-Lehner involution W_p acting on f has sign -1, while M is the product of those acting on f with sign $+1$.

We will work in the quaternion algebra B ramified exactly at those primes $p \mid D$. Note that, as this number of primes is odd, B is also ramified at infinity and the norm form in B is positive definite.

As in the prime case, we want to consider the family of negative quadratic twists E_d of E, for those d such that $-d$ is a fundamental discriminant and $\left(\frac{-d}{N}\right) \neq 1$ (otherwise, the sign of the functional equation for E_d is -1 and its L-series vanishes trivially).

We consider an order $\mathcal{O}$ of level N in the quaternion algebra B and construct the Brandt matrices. Let $f = \sum a_n q^n$ be the weight 2 and level N modular form associated to E. We have seen in 4.3.2 that there is a one dimensional eigenspace $< v >$ such that for each p, prime to N, $B_p v = a_p v$.

To this eigenvector, corresponds a weight $3/2$ modular form g whose Fourier coefficients are related to the central values $L(E_d, 1)$.

There is, as in the prime level case, a weight 2 Eisenstein series $e_2(z)$, whose coefficients are congruent modulo ℓ to those of f, under the assumption that E has an ℓ-torsion point defined over $\mathbb{Q}$. This Eisenstein series corresponds to the eigenvector $u = (1, ..., 1)$ of the Brandt matrices. Thus the eigenvalues turn out to be congruent mod ℓ. If, under some additional hypothesis, we can affirm that the eigenvectors u and v must be linearly dependent modulo ℓ, then we will have a congruence among the respective weight $3/2$ modular forms. As before we will relate this weight $3/2$ Eisenstein series to class numbers of imaginary quadratic fields. This will give us some relation among them and Ш, which is what we are looking for.

7.1.1 How to construct weight $3/2$ modular forms.

In [1], Bocherer and Shulze-Pillot generalized Gross' construction for square-free level N.

They consider a definite quaternion algebra B ramified at some set of primes $\{p_1, ..., p_r\}$ and split at all other primes. Put $D = p_1...p_r$ and let $N = DM$ be any square free integer.

As before take $\mathcal{O}$ an order of level N, $I_1, ..., I_n$ representatives of left-ideal classes, and $R_1, ..., R_n$ the respective right orders (of level N) of each ideal I_i.

For each R_i take the rank three lattice $L_i = \mathbb{Z} + 2R_i$ and S_i^0 the elements of trace zero in L_i. Define, as before, g_i to be the theta series

$$g_i = \frac{1}{2} \sum_{b \in S_i^0} q^{\mathbb{N}(b)}$$

where $\mathbb{N}$ is the norm form and $q = e^{2\pi i \tau}$.

The forms g_i are in the *Kohnen* subspace $M^{3/2}(N)$ which are those modular forms of weight $3/2$ on $\Gamma_0(4N)$ whose Fourier coefficient a_n is zero unless $-n \equiv 0, 1 \mod 4$.

Let w_i be the number of units in $R_i^\times / \{\pm 1\}$.

Recall we had an eigenvector $v = (v_1, ..., v_n)$ of the Brandt matrices, corresponding to our modular form f. Then

$$g = \sum_{i=1}^{n} \frac{v_i}{w_i} g_i$$

is in $M^{3/2}(N)$ and corresponds to f under Shimura map.

The form g is trivially zero unless we have

$$\operatorname{sg} W_p = \begin{cases} -1 & \text{for } p \mid D \\ 1 & \text{for } p \mid M \end{cases}$$

where $\operatorname{sg} W_p$ denotes the sign of W_p acting on f (see [1] for details).

This *lift* from modular forms of weight 2 to modular forms of weight 3/2 is also valid for Eisenstein series. Thus take

$$\mathcal{H}_{3/2} = \sum \frac{1}{w_i} g_i$$

this is a weight 3/2 *Eisenstein* series corresponding to the eigenvector u, and thus to an Eisenstein series of weight 2. If $W = \prod w_i$, then $W\mathcal{H}_{3/2} \in M^{3/2}(N)$.

7.1.2 Walspurger 's formula.

A similar special case of Waldspurger's formula to that described in [9] is valid for square-free levels, as shown in [1].

Let $f \in S_2(N)$ be a normalized newform of square-free level N, with sign $+1$ in the functional equation for $L(f, s)$. Let $-d$ be a fundamental discriminant and $f \otimes \epsilon_d$ the $-d$-quadratic twist of f.

Let $g = \sum m_d q^d$ be the weight 3/2 modular form corresponding to f as constructed above, in the definite quaternion algebra B ramified at those primes $p \mid D$, and $e_f = (\frac{v_1}{w_1}, ..., \frac{v_n}{w_n})$ where $v = (v_1, ..., v_n)$ is the eigenvector of the Brandt matrices in B corresponding to f.

We have

$$\prod_{p \mid \frac{N}{gcd(N,d)}} \left(1 + \left(\frac{-d}{p}\right) \operatorname{sg} W_p\right) L(f, 1)\, L(f \otimes \epsilon_d, 1) = 2^{\nu} \frac{(f, f)\, m_d^2}{\sqrt{d} < e_f, e_f >} \tag{7.1}$$

where ν is the number of prime divisors of N.

Note that the left hand side is zero unless $\left(\frac{-d}{p}\right) \operatorname{sg} W_p \neq -1, 0$ for every prime $p \mid N$.

This means that m_d is zero unless for every $p \mid N$, $\left(\frac{-d}{p}\right)$ coincides with the sign of W_p, or, it is zero. Thus we will only get a proportion of the twists of f by this construction.

7.2 $N = pq$, some numerics.

We want to extend the results of last chapter to the case of non prime conductor. More specifically, we would like to obtain a similar heuristic result for the proportion of Ш values divisible by a prime ℓ among twists of an elliptic curve having an ℓ-torsion point.

We will consider, in this section, an elliptic curve E of conductor $N = pq$, p, q primes. Suppose that $\operatorname{sg} W_p = -1$ and $\operatorname{sg} W_q = 1$. Further, suppose that E has an ℓ-torsion point defined over $\mathbb{Q}$.

We know that $M_2(N) = S_2(N) \oplus E_2(N)$, but for non prime N the space of Eisenstein series is not one dimensional. Thus, we would like to have:

- An Eisenstein series $e_2 = \sum c_n q^n$ such that for every prime p (and thus for every n), $a_p \equiv c_p \mod \ell$. Here $f = \sum a_n q^n$ is the modular form of the elliptic curve E, as usual.
- The eigenvectors of the Brandt matrices corresponding f and e_2 to be linearly dependent modulo ℓ.
- The relation among the coefficients of the corresponding weight 3/2 Eisenstein series $\mathcal{H}_{3/2}$ and the class numbers of imaginary quadratic number fields.

We will begin all this by analyzing some examples.

- $N = 14$

  We have the elliptic curve $E = [1, 0, 1, 4, -6]$ of conductor $N = 14$ and rank zero. The group of torsion points of E has order 6. Thus we have a 3-torsion point, and a 2-torsion point.

  The signs of the Atkin-Lehner at the primes $p = 7$ and $p = 2$ are, respectively, -1 and $+1$.

  We work with an order $\mathcal{O}$ of level 14 in the quaternion algebra ramified at the prime 7 and at ∞. There are 2 left ideal classes, thus we have two right orders $\mathcal{R}_1$ and $\mathcal{R}_2$. One half the units in each order R_i are $w_1 = 2$ and $w_2 = 1$.

  The first Fourier coefficients for the modular form f attached to E are

  $$a_2 = -1, a_3 = -2, a_5 = 0, a_7 = 1, ...$$

  The eigenvector of the Brandt matrices corresponding to f is $v = (-2, 1)$. Let $u = (1, 1)$. Clearly $v \equiv u \mod 3$.

  Thus the eigenvalues must be equivalent modulo 3. We know that for any $p \neq 2, 7$ $a_p \equiv p + 1 \mod 3$ as E has a 3-torsion point defined over $\mathbb{Q}$. Further we know that the row sums of the Brandt matrices B_p is $p + 1$ for any $p \neq 2, 7$, that is $B_p u = (p + 1)u$ as long as $p \nmid 14$.

We want to see what happens for $p = 2$ and $p = 7$.

$B_7 = \mathrm{id}$, thus $B_7 u = u$. In general B_p for any *ramified* p will be a permutation matrix, thus the row sums will be equal to one and $B_p u = u$.

For $p = 2$ we have

$$B_2 = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}$$

Thus $B_2 u = 5u = 2 \times 2 + 1$.

- $N = 26$

We have two elliptic curves of level 26 and rank 0.

(26A) $E = 26A = [1, 0, 1, -5, -8]$ with $|\operatorname{Tor}(E)| = 3$.
The signs of the Atkin-Lehner at the primes dividing 26 are -1 at $p = 13$ and $+1$ at $p = 2$. We work in the definite quaternion algebra ramified at 13, and calculate the Brandt matrices for an order of level 26, and the eigenvector v corresponding to f (and to E).

We have $a_2 = -1, a_3 = 1, a_5 = -3, \ldots$. The eigenvector for E is $v = (-2, 1, 1)$ which again is clear that $v \equiv u = (1, 1, 1) \mod 3$.

At primes $p = 2$ and $p = 13$ we have

$$B_2 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix} \qquad B_{13} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Thus $B_2 u = 2 \times 2 + 1$ and $B_{13} u = u$

(26B) $E = 26B = [1, -1, 1, -3, 3]$ with $|\operatorname{Tor}(E)| = 7$.
The signs of the Atkin-Lehner at the primes dividing 26 are -1 at $p = 2$ and $+1$ at $p = 13$. We work in the definite quaternion algebra ramified at 2.

We have $a_2 = 1, a_3 = -3, a_5 = -1, \ldots$. The eigenvector for E is $v = (-4, 3, 3)$ which again is clear that $v \equiv 3 * u = (3, 3, 3) \mod 7$.

At primes $p = 2$ and $p = 13$ we have

$$B_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad B_{13} = \begin{pmatrix} 11 & 8 & 8 \\ 12 & 8 & 7 \\ 12 & 7 & 8 \end{pmatrix}$$

Thus $B_2 u = u$ and $B_{13} u = 27u = (2 \times 13 + 1)u$.

- $N = 77$

We have $E = 77B = [0, 1, 1, -49, 600]$ with $|\operatorname{Tor}(E)| = 3$.
The signs of the Atkin-Lehner at the primes dividing 77 are -1 at $p = 7$ and $+1$ at $p = 11$. We work in the definite quaternion algebra ramified at 7.

The eigenvector for E is $v = (4, 1, -2, 1, -2, -2)$ and $v \equiv u \mod 3$.

At primes $p = 7$ and $p = 11$ we have

Thus $B_7 u = u$ and $B_{11} u = 23u = (2 \times 11 + 1)u$.

- $N = 30 = 2.3.5$

  The curve $E = [1, 0, 1, 1, 2]$ has rank zero, conductor $N = 30$, and $|\operatorname{Tor}(E)| = 6$. Has sign -1 for the Atkin-Lehner at exactly $p = 3$. The Brandt matrices B_p of level 30 in the definite quaternion algebra ramified at $p = 3$, for $p = 2, 3, 5$ are

$$B_2 = \begin{pmatrix} 0 & 3 & 1 & 1 \\ 3 & 0 & 1 & 1 \\ 2 & 2 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix} \qquad B_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad B_5 = \begin{pmatrix} 4 & 3 & 2 & 2 \\ 3 & 4 & 2 & 2 \\ 4 & 4 & 2 & 1 \\ 4 & 4 & 1 & 2 \end{pmatrix}$$

  The eigenvector for E is $v = (-1, -1, 2, 2)$.

  Then $-v \equiv u \mod 3$; and $B_3 u = u, B_2 u = (2 \times 2 + 1)u, B_5 u = (2 \times 5 + 1)u$.

- $N = 58 = 2.29$

  $E = [1, 1, 1, 5, 9]$ has rank 0, $|\operatorname{Tor}(E)| = 5$. Sign of $W_2 = -1$. Then B is the quaternion algebra ramified at 2 and ∞.

  Eigenvector for E: $v = (-4, 1, 1)$, $v \equiv u \mod 5$. As for the eigenvalues of u we have $B_2 u = u$ and $B_{29} u = 59u$.

7.3 The row sums of Brandt matrices.

Here, as before, B is a definite quaternion algebra and $\mathcal{O}$ an order of level $N = DM$. Denote by $B_n = B(n, D, M)$ the corresponding Brandt matrices.

The *zeta function* of $\mathcal{O}$ is the sum

$$\zeta_{\mathcal{O}} = \sum \frac{1}{\mathbb{N}(I)^{2s}}$$

where the sum extends over all integral $\mathcal{O}$-left ideals I.

Eichler in [7] §6 proves that the row sums of the Brandt matrices B_n equals the n-coefficient of the zeta function of $\mathcal{O}$. That is, if

$$\zeta_{\mathcal{O}} = \sum_{n=1}^{\infty} \frac{b(n)}{n^{2s}}$$

then $b(n)$ is the sum of (any) row in the matrix B_n.

The zeta function can be expressed as an Euler product ([7] §2) with local factor at a prime given as follows:

$$\begin{aligned} \zeta_p(s) &= (1 - p^{-2s})^{-1}(1 - p^{1-2s})^{-1} && \text{for } p \nmid DM \\ \zeta_p(s) &= (1 - p^{-2s})^{-1} && \text{for } p \mid D \\ \zeta_p(s) &= (1 + p^{1-2s})(1 - p^{-2s})^{-1}(1 - p^{1-2s})^{-1} && \text{for } p \mid M \end{aligned}$$

Which we can re-write as follows

$$\begin{aligned}
\zeta_p(s) &= (1-(p+1)p^{-2s}+pp^{-4s})^{-1} && \text{for } p \nmid DM\\
\zeta_p(s) &= (1-p^{-2s})^{-1} && \text{for } p \mid D\\
\zeta_p(s) &= 2\,(1-(p+1)p^{-2s}+pp^{-4s})^{-1} - (1-p^{-2s})^{-1} && \text{for } p \mid M
\end{aligned}$$

Put

$\alpha_p = p+1$	$d_p = -p$	$p \nmid DM$	$\beta_p = p+1$	$h_p = -p$	$p \nmid DM$
$\alpha_p = 1+p$	$d_p = -p$	$p \mid M$	$\beta_p = 1$	$h_p = 0$	$p \mid M$
$\alpha_p = 1$	$d_p = 0$	$p \mid D$	$\beta_p = 1$	$h_p = 0$	$p \mid D$

Then

$$\begin{aligned}
\zeta_{\mathcal{O}}(s) &= \prod_p \zeta_p(s) = 2\prod_p (1-\alpha_p p^{-2s} - d_p p^{-4s})^{-1} - \prod_p (1-\beta_p p^{-2s} - h_p p^{-4s})^{-1}\\
&= 2\sum_{n\geq 0}\frac{u(n)}{n^{2s}} - \sum_{n\geq 0}\frac{v(n)}{n^{2s}} = \sum_{n\geq 0}\frac{b(n)}{n^{2s}}
\end{aligned}$$

and we have the following recursion formulas:

$u(p) = 1$	$u(p^k) = 1 (\forall k)$	for $p \mid D$
$u(p) = p+1$	$u(p^k) = u(p)u(p^{k-1}) - pu(p^{k-2})$	for $p \nmid D$
$v(p) = 1$	$v(p^k) = 1 (\forall k)$	for $p \mid DM$
$v(p) = p+1$	$v(p^k) = v(p)v(p^{k-1}) - pv(p^{k-2})$	for $p \nmid DM$

Thus $b(n) = 2u(n) - v(n)$ satisfies

$$b(p) = \begin{cases} 1 & \text{for } p \mid D\\ p+1 & \text{for } p \nmid DM\\ 2p+1 & \text{for } p \mid M \end{cases} \tag{7.2}$$

and the following recursion formula

$b(p^k) = 1$	for $p \mid D$
$b(p^k) = b(p)b(p^{k-1}) - pb(p^{k-2})$	for $p \nmid DM$
$b(p^k) = 2u(p^k) - 1$	for $p \mid M$

7.4 A congruence for E.

Let E be an elliptic curve defined over $\mathbb{Q}$ with an ℓ torsion point P defined over $\mathbb{Q}$, where $\ell > 2$ is prime.

Recall that $a_p = p+1-N_p$, where N_p is the number of points of the reduced curve modulo the prime p.

We saw in proposition 1.6.1, that for any prime p of good reduction (including the prime ℓ if necessary), we have a congruence:

$$a_p \equiv 1 + p \mod \ell$$

For a prime p of bad reduction we have (see 2.8.2):

$$a_p = -\operatorname{sg} W_p$$

The ℓ-torsion point P reduces to a nonsingular point in the reduced curve $\widetilde{E}_p$. We saw in 1.4 that the nonsingular points in $\widetilde{E}_p$ form a group. This group has order

$p-1$ if $a_p = 1$, that is E has split multiplicative reduction at p
$p+1$ if $a_p = -1$, that is E has non-split multiplicative reduction at p

Thus ℓ must divide $p+1$ if $a_p = -1$ or, equivalently, $\operatorname{sg} W_p = 1$, and ℓ must divide $p-1$ if $a_p = 1$ or $\operatorname{sg} W_p = -1$.

Suppose E has square free conductor $N = DM$. Let B be the definite quaternion algebra ramified at those primes $p \mid D$. The vector $u = (1, 1, ..., 1)$ is an eigenvector of the Brandt matrices of level N. As the row sums of the Brandt matrices B_n is a constant $b(n)$, we have $B_n u^t = b(n)u^t$, for all $n \in \mathbb{N}_0$. If we take, in the Brandt matrix series $\Theta = (\theta_{ij}) = \sum B_n q^n$, the sum of any row

$$\sum_j \theta_{ij}(\tau)$$

this is an Eisenstein series whose q-expansion is given by

$$e_2(z) = b(0) + \sum_{n \geq 1} b(n) q^n.$$

The Fourier coefficient $b(p)$ at each prime p was given in the previous section, as well as the recursion formulas for $b(n)$. The zero-coefficient is (see[7] p.95 for details)

$$b(0) = \sum_{i=1}^{n} \frac{1}{2w_i} = \frac{1}{24} \prod_{p|D} (p-1) \prod_{q|M} (q+1) \tag{7.3}$$

Note that ℓ divides each factor in the numerator of (7.3).

The series $e_2(z)$ is a modular form of weight 2 and level N, as it is a linear combination of theta series that are modular forms of weight 2 and level N. Further, for this Eisenstein series we have

- $b(p) \equiv a_p \mod \ell$ for any $\ell \nmid DM$
- $b(p) = 1 = a_p$. In particular, $b(p) \equiv a_p \mod \ell$ for any $p \mid D$
- $2q + 1 = b(q) \equiv a_q = -1 \mod \ell$ if and only if $\ell \mid 2(q+1)$ which we know to be true as the group of nonsingular points $\widetilde{E}_q$ has order $q+1$ and a point of order ℓ.

From the recursion formulas for a_n and $b_n = b(n)$ it follows that $a_n \equiv b_n$ modulo ℓ for every n. As the coefficients a_n and b_n are multiplicative, it is enough to check this for n equal to a prime power. Further, for any prime $p \nmid DM$ the recursion formulas for a_{p^k} and b_{p^k} are the same, and there is nothing to check. For $p \mid D$, $a(p^k) = b(p^k) = 1$. Thus we only need to see that $b(q^k) \equiv a(q^k)$ modulo ℓ, for primes $q \mid M$.

Here $u(q) = q + 1 \equiv 0 \mod \ell$, $u(1) = 1$ and $-q \equiv 1 \mod \ell$, and the recursion formula for $u(q^k) = u(q)u(q^{k-1}) - qu(q^{k-2})$ give

$$u(q^k) \underset{\ell}{\equiv} \begin{cases} 1 & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd} \end{cases}$$

This gives

$$b(q^k) = 2u(q^k) - 1 \underset{\ell}{\equiv} \begin{cases} 1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd} \end{cases}$$

which is the same as $a(q^k) = (-1)^k$. This gives $b_n \equiv a_n \mod \ell$ for every $n \in \mathbb{N}$.

Further, the zero-coefficient $b(0)$ is divisible by the prime ℓ. Thus we have

$$f \equiv e_2(z) \mod \ell \tag{7.4}$$

7.5 Multiplicity one $\mod \ell$?

We know that the Brandt matrices B_p for p prime to the level, act as the Hecke operators T_p on the space of newforms. We know further, that to a newform f corresponds an eigenvector v such that, for $(p, N) = 1$,

$$B_p v = a_p v$$

In fact we have that this equality holds for *every* prime p, as we will now show.

Take the Brandt matrix series

$$\Theta(z) = \sum_{m=0}^{\infty} B_m q^n.$$

Recall this is an $n \times n$ matrix whose entries are the theta series θ_{ij} defined in 4.3.1.

$$\Theta v = (\sum_{m \geq 0} B_m q^m) v$$

We have,

$$T_p(\Theta v) = (\sum_{m \geq 0} B_p B_m q^m) v = \sum_{m \geq 0} B_m (B_p v) q^m = a_p (\sum_{m \geq 0} B_m q^m) v = a_p(\Theta v)$$

Thus $\sum_j \theta_{ij} v_j$ if it is non zero, it is an eigenfunction for all the Hecke operators T_p with eigenvalue a_p; at least for p prime to the level N.

We know that there is a basis of $S_k(N)$ whose elements are eigenforms for all the T_n with $(n, N) = 1$. The *multiplicity one* statement says that, restricting our attention to *newforms*, to each set of eigenvalues $\{a_n\}$ for n prime to the level, corresponds a one-dimensional eigenspace $< f >$. As the operators T_p commute for all p, f will be an eigenfunction for *all* T_p and it is determined by the Fourier coefficients a_p with $(p, N) = 1$.

This means that $\sum_j \theta_{ij} v_j = \lambda_i f$, for some λ_i. Further, we have: λ_i is the coefficient of q in the Fourier expansion of

$$\theta_{ij} v_j = \sum_m (\sum_j \theta_{ij}(m) v_j) q^m$$

which is $\sum_j \theta_{ij}(1) v_j = v_i$ as B_1 is the identity matrix.

Consider a prime $p \mid N$, and some index i, such that $v_i \neq 0$. Thus $v_i f = \sum_j \theta_{ij} v_j$ and the Hecke operator T_p acts on $v_i f$ as

$$T_p(\sum_j \theta_{ij} v_j) = \sum_j T_p \theta_{ij} v_j = \sum_j T_p(\sum_m \theta_{ij}(m) q^m) v_j = \sum_j \sum_m \theta_{ij}(pm) v_j q^m$$

$$a_p v_i f = \sum_m (\sum_j \theta_{ij}(pm) v_j) q^m$$

Comparing coefficients for $m = 1$,

$$a_p v_i = \sum_j \theta_{ij}(p) v_j$$

which means that

$$a_p v = B_p v$$

This shows that the coefficients $\{a_p\}$ are the eigenvalues of v, for *every* prime p, and thus for every n. Then the congruence (7.4) shows up in the quaternion algebra B as a congruence among eigenvalues, as we state in the following

Proposition 7.5.1. *Let E be an elliptic curve of conductor $N = DM$ as above, having a rational ℓ-torsion point, ℓ odd. Let $e_2 = \sum b(n) q^n$ with $b(n)$ as in* (7.2) *and* (7.3) *and let f be the modular form of level N, corresponding to E. Let v be the eigenvector of the Brandt matrices, corresponding to f, and u the one corresponding to e_2. Then, for every n, the respective eigenvalues, of the Brandt matrices B_n, of v and u, are equivalent modulo ℓ.*

As in the last chapter, we would like to have $\lambda v \equiv u$ modulo ℓ, for some $\lambda \in \mathbb{F}_\ell^\times$. This will be so if the eigenspace associated to u is one dimensional modulo ℓ.

Numerically, we have checked this for a number of elliptic curves of conductors $N = pM$, such that W_p acts on E with -1 sign, and W_q with sign $+1$ for every other prime $q \mid M$. This means that we work in a quaternion algebra ramified at exactly one finite prime.

We believe that, in this case, the results of Emerton in [8], for non-prime levels, will conduce us, under some restrictions, to a positive answer in what concerns multiplicity one modulo ℓ for the space of Eisenstein series. It is a technical matter to check whether we are under the hypothesis of his results, and we plan to do this in a near future.

7.6 Examples.

Suppose we have multiplicity one, then If $g = \sum \frac{v_i}{w_i} g_i$ and $\mathcal{H}_{3/2} = \sum \frac{1}{w_i} g_i$ we have

$$g \equiv \mathcal{H}_{3/2} \mod \ell.$$

We will analyze the Fourier coefficients of the weight $3/2$ modular form $\mathcal{H}_{3/2}$. In what follows we will consider an elliptic curve E of level N, with exactly one Atkin-Lehner W_p acting on f with sign -1.

We will drop the subscript 3/2 in $\mathcal{H}_{3/2}$ and write $\mathcal{H}_N$ for the Eisenstein series of weight 3/2 obtained for the elliptic curve E of level N.

- $N = 14$**.** Recall that we have an elliptic curve E, with a 3-torsion point. W_7 has sign -1 and W_2 has sign $+1$.

  We already saw that the eigenvector v, corresponding to f, is equivalent to u mod 3.

  We want to see how are the coefficients of the weight 3/2 Eisenstein series $\mathcal{H}_{14}$. For this, we calculate the form $\sum \frac{1}{w_i} g_i$ and compare the coefficients with the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$.

  Let $K_d = \mathbb{Q}(\sqrt{-d})$, $\mathcal{O}_d$ its ring of integers, and $h(d)$ its class number. Recall $u(\mathcal{O}_d) = 1$ except for $d = 3, 4$ which have, respectively, 3 and 2 units. Recall that a prime $p \in \mathbb{Z}$ is inert, splits or ramifies in $\mathcal{O}_d$ if the Kronecker symbol $\left(\frac{-d}{p}\right)$ is, respectively, -1, 1, 0.

  We have, for d such that $-d$ is a fundamental discriminant and $\left(\frac{-d}{7}\right) \neq 1$ and $\left(\frac{-d}{2}\right) \neq -1$:

$$H_{14}(d) = \begin{cases} 2h(d) \text{ if 7 is inert and 2 splits in } \mathcal{O}_d \\ \dfrac{h(d)}{u(\mathcal{O}_d)} \text{ if 7 is inert and 2 ramifies in } \mathcal{O}_d \\ h(d) \text{ if 7 is ramified and 2 splits in } \mathcal{O}_d \\ \dfrac{1}{2}h(d) \text{ if 7 and 2 ramify in } \mathcal{O}_d \end{cases} \tag{7.5}$$

  Note that, as $u(\mathcal{O}_d) = 1$ for every $d \neq 3, 4$ we will not detect numerically if we have to divide by $u(\mathcal{O}_d)$ unless 3 or 4 is in the class of congruences we are considering. Further, as neither 3 or 4 is a product of 2 distinct primes, we can equally write $\frac{1}{2}\frac{h(d)}{u(\mathcal{O}_d}$) in the last row of (7.5).

- $N = 26A$**.** The elliptic curve $26A$ has a 3-torsion point defined over $\mathbb{Q}$. The signs of the involutions W_p acting on f are: W_{13} has sign -1 and W_2 has sign $+1$.

  The eigenvector v corresponding to f is equivalent to $u \mod 3$.

  For the coefficients of the weight 3/2 Eisenstein series $\mathcal{H}_{26A}$, we obtain numerically, for d such that $-d$ is a fundamental discriminant and $\left(\frac{-d}{13}\right) \neq 1$ and $\left(\frac{-d}{2}\right) \neq -1$ exactly the same coefficients as in (7.5) replacing 7 by 13.

- $N = 26B$**.** The elliptic curve $26B$ has a 7-torsion point defined over $\mathbb{Q}$. The signs of the involutions W_p acting on f are: W_2 has sign -1 and W_{13} has sign $+1$.

  The eigenvector v corresponding to f is equivalent to $u \mod 7$.

  As for the coefficients of $\mathcal{H}_{26B}$ we can correct the equation (7.5), in what concerns dividing by the the units in $\mathcal{O}_d$:

$$H_{26B}(d) = \begin{cases} 2\dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if 2 is inert and 13 splits in } \mathcal{O}_d \\ \dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if 2 is inert and 13 ramifies in } \mathcal{O}_d \\ \dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if 2 ramifies and 13 splits in } \mathcal{O}_d \\ \dfrac{1}{2}\dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if 13 and 2 ramify in } \mathcal{O}_d \end{cases}$$

- $N = 30$**.** We have an elliptic curve E of rank zero and a 3-torsion point defined over $\mathbb{Q}$. The signs of the involutions W_p acting on f are: W_3 has sign -1; and W_2, W_5 have sign $+1$.

  The eigenvector v corresponding to f is equivalent to $u \mod 3$.

  For the coefficients of $\mathcal{H}_{30}$ recall that we will only consider $\left(\frac{-d}{3}\right) \neq 1$ and $\left(\frac{-d}{p}\right) \neq -1$ for $p = 2, 5$. We obtain

$$H_{30}(d) = \begin{cases} 2^2\dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if 3 is inert and } 2,5 \text{ split in } \mathcal{O}_d \\ 2\dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if exactly one of the primes } 2,3,5 \text{ ramify in } \mathcal{O}_d \\ \dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if exactly two of the primes } 2,3,5 \text{ ramify in } \mathcal{O}_d \\ \dfrac{1}{2}\dfrac{h(d)}{u(\mathcal{O}_\mathcal{K})} & \text{if } 2,3 \text{ and } 5 \text{ all ramify in } \mathcal{O}_d \end{cases}$$

Gathering the information obtained for N prime, a product of two primes and $N = 30$, we expect the following formula for $\mathcal{H}_N(d)$ to be true, following the results of Eichler in [7], but we have not yet filled in all the details.

Let B be a definite quaternion algebra ramified at exactly one finite prime p, and let $N = pM$ be square free integer. Denote by $\mathcal{H}_N$ the weight 3/2 Eisenstein series constructed in the quaternion algebra B as explained in 7.1.1.

Let $d \in \mathbb{N}$ such that $-d$ is a fundamental discriminant such that

- $\left(\frac{-d}{p}\right) \neq 1$
- $\left(\frac{-d}{q}\right) \neq -1$ for every $q \mid M$.

Let $h(d)$ be the class number in $\mathbb{Q}(\sqrt{-d})$, $\mathcal{O}_d$ its ring of integers and $u(\mathcal{O}_d)$ the number of units in $\mathcal{O}_d$.

Set r to be the number of (distinct) primes that divide N and $s(d)$ the number of primes that divide N and ramify in $\mathbb{Q}(\sqrt{-d})$. Then

$$H_N(d) \stackrel{?}{=} \frac{2^{r-1}}{2^{s(d)}} \frac{h(d)}{u(\mathcal{O}_d)}. \tag{7.6}$$

Recall that we want to analyze the distribution of Ш among negative quadratic twists of elliptic curves E, with associated modular form f. It can be seen numerically that the order of $Ш_d$ is "essentially" the coefficient m_d^2 of the modular form g of weight $3/2$ under Shimura correspondence to f, divided by a power of 2.

Thus, considering what we have exposed, we have the following

Proposition 7.6.1. *Let E be an elliptic curve of rank zero and square free conductor N. Suppose the sign of W_p acting on f is -1 for exactly one prime $p \mid N$. Consider the family $\{E_d\}$, of negative quadratic twists of E, satisfying the Kronecker conditions above. Suppose E has a torsion point defined over $\mathbb{Q}$, of odd prime order ℓ. Then, assuming multiplycity one and* (7.6)*, the proportion of $Ш_d$ in the family, divisible by ℓ, is the same as the proportion of class numbers $h(d)$ divisible by ℓ in the family of negative quadratic fields $\mathbb{Q}(\sqrt{-d})$, with the same Kronecker conditions.*

APPENDIX A

Some Algebraic Background.

This appendix has been included in order to ease the reading and set the notation. It has to be taken as a summary of the algebraic background we need and will be using throughout the text, mainly in chapter 1, in which we will consider the action of Frobenius on the Tate module of an elliptic curve.

For reference, look at the book of Silverman [31].

A.1 Varieties: algebraic and projective.

Let's recall some elementary facts of algebraic geometry.

Let K be a field, which we will assume to be perfect for simplicity, $\overline{K}$ its algebraic closure, and let I be an ideal in $\bar{K}[X] = \bar{K}[X_1, ..., X_n]$. An algebraic set $V \subset \mathbb{A}^n = \mathbb{A}^n(\bar{K})$ is the set of common zeroes of functions in I. An algebraic set V is a *variety* if $I(V) = \{f \in \bar{K}[X] : f(P) = 0 \ \forall P \in V\}$ is a prime ideal in $\overline{K}[X]$. A variety is said to be defined over K if the ideal $I(V)$ can be generated by polynomials in $K[X]$. We will note this by V/K, and by $V(K)$ its K-rational points.

If V/K is a variety, its (affine) coordinate ring is defined by $K[V] = K[X]/I(V/K)$ and its quotient field $K(V)$ is called the *function field* of V/K.

The *dimension* of the variety V is the transcendence degree of $\overline{K}(V)$ over $\overline{K}$.

Let V be a variety and $f_1, ..., f_m \in \bar{K}[X]$ a set of generators for $I(V)$. V is said to be *smooth* or *non singular* at P if the m x n matrix

$$(\partial f_i/\partial X_j(P))_{1 \leq i \leq m, 1 \leq j \leq n}$$

has rank $n - \dim(V)$.

Similarly we define *projective varieties*. Let $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$ denote the projective n-space. Consider a *homogeneous* ideal I in $\overline{K}[X] = \overline{K}[X_0, ..., X_n]$, that is, an ideal generated by homogeneous polynomials. A projective set V is one of the form

$$V = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}.$$

V is a *projective variety* if the homogeneous ideal

$$I(V) = \{f \in \overline{K}[X] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}$$

is a prime ideal in $\overline{K}[X]$. As above, we say that V is defined over K, if its ideal $I(V)$ can be generated by homogeneous polynomials in $K[X]$, and we denote it V/K. The set $V(K)$ is the set of K-rational points in the variety, that is, the points defined over K.

Let's recall that $\mathbb{P}^n$ can be covered by open sets $U_i = \{p = [x_0, ..., x_n] \in \mathbb{P}^n : x_i \neq 0\}$ and that we have the usual bijections $\phi_i : \mathbb{A}^n \to U_i \subset \mathbb{P}^n$ defined by $(x_1, ..., x_n) \xrightarrow{\phi_i} [x_1, ..., x_{i-1}, 1, x_i, ..., x_n]$.

If V is a projective variety with homogeneous ideal $I = I(V)$, we will write $V \cap \mathbb{A}^n$ for $\phi_i^{-1}(V \cap U_i)$, for any i such that this set is nonempty. This is an algebraic variety with ideal $I(V \cap \mathbb{A}^n)$ which is the ideal generated by the dehomogenization with respect to X_i of the homogeneous polynomials $f \in I$.

If, instead, V is an algebraic variety with ideal $I(V)$, we can consider it as a subset of $\mathbb{P}^n$ by the embedding $\phi_i : V \to U_i$. The *projective closure of* V, denoted $\overline{V}$, is the projective variety with homogeneous ideal $I(\overline{V})$ generated by the homogenization with respect to X_i of the polynomials $f \in I(V)$.

If V is an affine variety, $V = \overline{V} \cap \mathbb{A}^n$.
If V is a projective variety, $V \cap \mathbb{A}^n = \emptyset$ or $V = \overline{V \cap \mathbb{A}^n}$.

By a *variety* we will always mean a projective variety. If a set of non homogeneous equations is given as definition, it is meant the algebraic closure of the affine variety given.

For a projective variety V/K, the *dimension* of V is defined as the dimension of $V \cap \mathbb{A}^n$ whenever this is nonempty. The *function field* of V, denoted $K(V)$ is the function field of $V \cap \mathbb{A}^n$. If $P \in V$, then V is non-singular at P if $V \cap \mathbb{A}^n$ is non-singular at P.

The function field of a projective variety V can also be defined as the field of rational functions $f(X)/g(X)$ where f and g are homogeneous polynomials of the same degree, $g \notin I(V)$ and $f/g = \tilde{f}/\tilde{g}$ if and only if $f\tilde{g} - \tilde{f}g \in I(V)$.

Let V_1 and V_2 be projective varieties. A *rational map* $\phi : V_1 \to V_2$ is an application $\phi = [\phi_0, ..., \phi_n]$, where each $\phi_i \in \overline{K}(V_1)$ and for each $P \in V_1$ at which every ϕ_i is defined, $\phi(P) \in V_2$. A rational map is said to be *regular* or *defined* at P if there is a function $g \in \overline{K}(V_1)$ such that each $g\phi_i$ is defined at P and for some i, $g\phi_i(P) \neq 0$. A *morphism* is a rational map that is regular at every point. Note that for regularity it may be necessary to take different functions g for different points P.

An alternative definition of rational map $\phi : V_1 \to V_2$, "clearing denominators" in the above definition, is the following: is a map $\phi = [\phi_0, ..., \phi_n]$ where ϕ_i are homogeneous polynomials of the same degree, not all in $I(V_1)$; and, for every $g \in I(V_2)$, $g(\phi_0(X), ..., \phi_n(X)) \in I(V_1)$. A rational map ϕ as above is defined or regular at $P \in V_1$ if there are homogeneous polynomials $\psi_0, ...\psi_n$ all of the same degree, such that for all i, j, $\phi_i\psi_j \equiv \phi_j\psi_i(\mod I(V_1))$ and $\psi_i(P) \neq 0$ for some i. A morphism is a rational map that is everywhere regular.

A.2 Valuations.

Let K be a field. A *valuation* defined over K is a function $\nu : K \to \mathbb{Z}$ such that
1) $\nu(x)$ takes all the values in $\mathbb{Z}$ when $x \neq 0$, and $\nu(0) = \infty$.
2) $\nu(xy) = \nu(x)\nu(y)$
3) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$
The set $A = \{x : \nu(x) \geq 0\} \cup \{0\}$ is a ring known as the *valuation ring* of ν.
The ring A is integrally closed in K. It is a *local ring*. Its maximal ideal m is the set of elements $x \in K$ such that $\nu(x) > 0$.

Examples:
1) $K = \mathbb{Q}$, p a prime in $\mathbb{Z}$ and $\nu_p(x) = a$ if $x = p^a y$ with numerator and denominator in y coprime to p. This is the *p-adic valuation* of $\mathbb{Q}$. The valuation ring of ν_p is the local ring $\mathbb{Z}_{(p)}$.
2) K a number field with ring of integers $\mathcal{O}_K$. A prime $\pi \in \mathcal{O}_K$ defines a valuation ν_π in a complete analogous manner as in the previous example.
3) $K = k(X)$, where k is a field and X an indeterminate. Let f be an irreducible polynomial in $k(X)$ and define a valuation ν_f as in 1). The valuation ring of ν_f is the local ring of $k(X)$ with respect to the prime ideal (f).

An integral domain A is called a *discrete valuation ring* if there is a valuation ν defined over its field of fractions K such that A is the valuation ring of ν.

Suppose now that A is a discrete valuation ring.
Note that two element x, y of A with the same valuation generate the same ideal.
Let $a \neq 0$ be an ideal in A, there is a least positive integer k such that $\nu(x) = k$ for some $x \in a$. Then a contains every y with $\nu(y) \geq k$. This means that the only non-trivial ideals of A can be described by $m_k = \{y : \nu(y) \geq k\}$. These form a unique chain $m \supset m_2 \supset m_3 ...$, and so A is a noetherian ring.
As ν is a surjective function, there is an x such that $\nu(x) = 1$, then $m = (x)$, and $m_k = (x^k)$ $(k \geq 1)$. So that m is the unique prime nontrivial ideal of A, A is a local noetherian domain of dimension one and every ideal $(\neq 0)$ of A is a power of the maximal ideal. Most of these properties are characteristics of discrete valuation rings.
Let A be a local ring, with maximal ideal m, and residue field $k = A/m$.
Let's recall that if M is a finitely generated A-module, M/mM is annihilated by m and is naturally an A/m-modulo, that is, a k vector space and as that it is finite dimensional.
If, in particular, M is an ideal of A, as it is the maximal ideal m, then we have that m/m^2 is an $k = A/m$-vector space of finite dimension.

Another characterization of smoothness.

Let V be an algebraic variety. Consider in the ring $\overline{K}[V]$ the ideal m_P defined by $m_P = \{f \in \overline{K}[V] : f(P) = 0\}$. Then m_P is a maximal ideal and we can consider the local ring $\overline{K}[V]_{(m_P)}$.

Definition A.2.1. *The local ring of V at P, denoted $\overline{K}[V]_P$ is the localization of $\overline{K}[V]$ at m_P, that is*

$$\overline{K}[V]_P = \{H \in \overline{K}(V), H = f/g \text{ with } f, g \in \overline{K}[V] \text{ and } g(P) \neq 0\}$$

Functions in $\overline{K}[V]_P$ are said to be *regular* or defined at P.

The residue field $\overline{K}[V]_P/m_P \cong \overline{K}$, the isomorphism given by $H \mapsto H(P)$. Then m_P/m_P^2 is a finitely generated $\overline{K}$-vector space.

Thus we come to an alternate and useful condition for non-singularity:

Theorem A.2.2. *A point $P \in V$ is non-singular if and only if*
$$\dim_{\bar{K}} m_P/m_P^2 = \dim V$$

Let us go back to algebraic varieties and the definition of smoothness, to give a more intuitive version.

Recall the Zariski topology in $\mathbb{A}^n$: closed subsets are the algebraic sets, that is, the common zeroes of a set of polynomials. This induces a topology on a variety V in $\mathbb{A}^n$.

Let V be an affine variety, Y an open set of V and $f : Y \to K$ a function. f is said to be *regular* at P if there is an open neighborhood U of P, $U \subset Y$, and polynomials $g, h \in K[X_1, ..., X_n]$ such that en U, $h \neq 0$ and $f = g/h$.

We can associate to an affine variety V the following rings of functions: $\mathcal{O}(V)$ will be the ring of all regular functions on V. For $P \in V$, $\mathcal{O}_P$, the *local ring of P on V* is the ring of germs of regular functions on V. Its maximal ideal m is the set of germs of regular functions that vanish at P, and the residue field $\mathcal{O}_P/m$ is isomorphic to $\overline{K}$.

It can be easily seen (see [11]) that $\mathcal{O}(V)$ is isomorphic to the ring $\overline{K}[V]$; and, if we consider the maximal ideal m_P of $\overline{K}[V]$ then the local ring $\overline{K}[V]_{(m_P)}$ is isomorphic to $\mathcal{O}_P$ and has dimension $\dim \mathcal{O}_P = \dim V$.

We have the analog theorem for smoothness:

Theorem A.2.3 (Hartshorne I.5.1)**.** *Let V be an affine variety, $P \in V$ a point. Then V is non-singular at P if and only if the local ring $\mathcal{O}_P$ is a regular local ring: if m is its maximal ideal and $k = \mathcal{O}_P/m$ its residue field, then $\dim_k m/m^2 = \dim \mathcal{O}_P$.*

A.3 Curves.

A *Curve* is a projective variety of dimension 1. If C is a curve and $P \in C$ is a smooth point, then $\overline{K}[C]_P$ is a *discrete valuation ring*. The valuation on $\overline{K}[C]_P$ is given by $\mathrm{ord}_P(f) = \max\{k : f \in m_P^k\}$ for $f \in \overline{K}[V]_P$ and extended to $\overline{K}(C)$ in the natural way.

A *uniformizer* for C at P is a function $t \in \overline{K}(C)$ such that $\mathrm{ord}_P(t) = 1$, that is, a generator of m_P.

If $f \in \overline{K}(C)$, $\mathrm{ord}_P(f)$ is the *order of f at P*. f has a zero at P if $\mathrm{ord}_P(f) > 0$, a pole if $\mathrm{ord}_P(f) < 0$. f is said to be *regular* at P if $\mathrm{ord}_P(f) \geq 0$, otherwise f has a pole at P and we write $f(P) = \infty$.

If C is a smooth curve and $f \in \overline{K}(C)$, the number of points of C at which f has a zero or a pole is finite. If f has no poles, then $f \in \overline{K}$.

Proposition A.3.1. *Let C/K be a curve, and $t \in K(C)$ a uniformizer at some non-singular point $P \in C$. Then $K(C)$ is a finite separable extension of $K(t)$.*

A.3.1 Maps between curves.

Let C be a curve, $V \subset \mathbb{P}^n$ a variety and $\phi : C \to V$ a rational map. If $P \in C$ is a smooth point, then the map ϕ is regular at P. In particular, if C is smooth, ϕ is a morphism. Thus, for a smooth curve, a rational map is always defined at every point.

Now consider two curves C_1 and C_2 defined over a field K and a non constant rational map $\phi : C_1 \to C_2$ defined over K. Then ϕ is a surjective map. Composition with ϕ induces an injection ϕ^* of the respective function fields: $K(C_2) \xrightarrow{\phi^*} K(C_1)$ defined by $f \mapsto f \circ \phi$.

If ϕ is non-constant, then $K(C_1)$ is a finite extension of $\phi^*K(C_2)$. The *degree* of ϕ is defined as the degree of the extension field $K(C_1)/\phi^*K(C_2)$. For a constant map ϕ, the degree is defined to be zero. The map ϕ is said to be *separable, inseparable or purely inseparable* if the corresponding extension field is separable, inseparable or purely inseparable. We define correspondingly the separable and inseparable degrees $\deg_s \phi, \deg_i \phi$ as the separable and inseparable degrees of the extension $K(C_1)/\phi^*K(C_2)$.

If $\phi : C_1 \to C_2$ is a map of degree one, then ϕ is an isomorphism.

A.3.2 Behavior of a map in the neighborhood of a point.

Definition A.3.2. *Let $\phi : C_1 \to C_2$ be a non constant map of smooth curves, $P \in C_1$ a point, and $t_{\phi(P)} \in K(C_2)$ a uniformizer at $\phi(P)$. The ramification index of ϕ at P, denoted by $e_\phi(P)$, is defined by*

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)}).$$

We have $e_\phi(P) \geq 0$ and we say that ϕ is unramified at P if $e_\phi(P) = 1$. By ϕ is *unramified* we mean that ϕ is unramified at every $P \in C_1$.

Proposition A.3.3. *Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves,*

a) For every $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

b) For all but finitely many $Q \in C_2$,

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

c) Let $\psi : C_2 \to C_1$ be another non-constant map. Then for all $P \in C_1$

$$e_{\psi \circ \phi}(P) = e_\psi(\phi(P)) e_\phi(P).$$

Then a map $\phi : C_1 \to C_2$ is unramified if and only if $\#\phi^{-1}(Q) = \deg \phi$ for all $Q \in C_2$.

A.4 The Frobenius map.

Suppose K is a field of characteristic p, and let $q = p^r$. For each polynomial f consider the polynomial $f^{(q)}$ obtained by raising each coefficient of f to the q-th power. For any curve C/K consider the curve $C^{(q)}/K$ defined by the ideal $I^{(q)} = \{f^{(q)} : f \in I(C)\}$.

The q^{th}-power *Frobenius morphism* is the map $\mathcal{F}_q : C \to C^{(q)}$ defined by

$$\mathcal{F}_q([x_0, ..., x_n]) = [x_0^q, ..., x_n^q]$$

Let us state the basic properties of the Frobenius map.

Suppose now K is a perfect field of characteristic $p > 0$, and $q = p^r$ as before. Let C/K be a curve and consider the Frobenius morphism $\mathcal{F}_q : C \to C^{(q)}$. Then,

1) $\mathcal{F}_q^* K(C^{(q)}) = K(C)^q = \{f^q : f \in K(C)\}$.

2) $\mathcal{F}_q$ is purely inseparable.

3) $\deg \mathcal{F}_q = q$.

Every map $\psi : C_1 \to C_2$ of smooth curves over a field of characteristic $p > 0$ factors as:

$$C_1 \xrightarrow{\mathcal{F}_q} C_1^{(q)} \xrightarrow{\lambda} C_2$$

where $q = \deg_i(\psi)$, $\mathcal{F}_q$ is the q-th power Frobenius map, and λ is separable.

A.5 The divisor group of a curve.

The divisor group of a curve C, denoted by $\mathrm{Div}(C)$, is the free abelian group generated by the points of C, in the algebraic closure of K. Thus a divisor D is a formal sum $D = \sum_{P \in C} n_P P$, where n_P are integers, finitely many $\neq 0$. The degree of D is the sum $\deg D = \sum_{P \in C} n_P$.

The subgroup of divisors of degree 0 will be denoted by $\mathrm{Div}^0(C)$.

Suppose C is defined over K. The Galois group $G_{\overline{K}/K}$ acts on the group of divisors and on the subgroup of divisors of degree zero in the obvious way:

if $D = \sum_{P \in C} n_P P$, then $D^\sigma = \sum_{P \in C} n_P P^\sigma$.

Thus, a divisor D is defined over K if $D^\sigma = D$. Let $\mathrm{Div}_K(C)$ denote the group of divisors defined over K, and $\mathrm{Div}_K^0(C)$ the group of divisors of degree 0 defined over K.

Consider now a smooth curve C and a map $f \in \overline{K}(C)^\times$. We can associate to f a divisor, which is defined by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$$

It is clear that for $\sigma \in G_{\bar{K}/K}$, $\mathrm{div}(f^\sigma) = \mathrm{div}(f)^\sigma$. Thus, if $f \in K(C)$, then $\mathrm{div}(f) \in \mathrm{Div}_K(C)$.

The map $\mathrm{div} : \overline{K}(C)^\times \to \mathrm{Div}(C)$ is a homomorphism of abelian groups, analogous to the map that sends an element of a number field to the corresponding fractional ideal.

Further, a divisor is said to be *principal* if it is of the form $D = \mathrm{div}(f)$ for some $f \in \overline{K}(C)^\times$. Two divisors are said to be equivalent $D_1 \sim D_2$ if $D_1 - D_2$ is principal. The *divisor class group* or *Picard group* of C, denoted $\mathrm{Pic}(C)$, is the quotient of $\mathrm{Div}(C)$ by the subgroup of principal divisors. $\mathrm{Pic}_K(C)$ will denote the subgroup of $\mathrm{Pic}(C)$ fixed by the Galois group $G_{\bar{K}/K}$. This is *not* the quotient of $\mathrm{Div}_K(C)$ by its subgroup of principal divisors.

Proposition A.5.1. *If C is a smooth curve and $f \in \overline{K}(C)^\times$, then we have*

1) $\mathrm{div}(f) = 0$ *if and only if* $f \in \overline{K}^\times$

2) $\deg \mathrm{div}(f) = 0$.

The *degree* 0 *part of the divisor class group of* C, denoted by $\mathrm{Pic}^0(C)$, is the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors. $\mathrm{Pic}^0_K(C)$ denotes the subgroup of $\mathrm{Pic}^0(C)$ fixed by $G_{\bar{K}/K}$.

Let $\phi : C_1 \to C_2$ be a non-constant map among smooth curves. We have seen that ϕ induces a map $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$. Similarly it induces a map on the divisor groups: $\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ defined on a single point as

$$Q \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\, P$$

and extended by $\mathbb{Z}$-linearity to arbitrary divisors.

Now suppose we have an *elliptic curve* E defined over K. Recall that an elliptic curve is a curve of genus 1, with a rational point on it, and that the points of E have an abelian group law. We will denote by $\mathcal{O}$ the point at infinity and identity for this group law.

We have the following

Proposition A.5.2. *Let E be an elliptic curve with zero element $\mathcal{O}$.*

For every divisor $D \in \mathrm{Div}^0(E)$, there exists a unique point $P \in E$ such that $D \sim P - \mathcal{O}$. Let $\sigma : \mathrm{Div}^0(E) \to E$ be the map given by this association. Then

a) σ is surjective.

b) $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. Thus, it induces a bijection of sets

$$\sigma : \mathrm{Pic}^0(E) \to E$$

with inverse $\kappa : E \to \mathrm{Pic}^0(E)$, that maps

$$P \mapsto \text{ the class of } P - \mathcal{O}.$$

c) κ is a group isomorphism.

From this it is easy to see that if E is an elliptic curve and $D = \sum n_P P \in \mathrm{Div}(E)$, then D is principal if and only if $\sum n_P = 0$ and $\sum [n_P]P = 0$ in E.

A.6 Isogenies.

Definition A.6.1. *Let E_1 and E_2 be elliptic curves. An isogeny $\phi : E_1 \to E_2$ is a morphism sending zero to zero.*

Two elliptic curves are said to be *isogenous* if there is an isogeny among them.

Any non-constant isogeny ϕ, being a morphism among curves, satisfies $\phi(E_1) = E_2$. Hence we have the usual injection of the respective function fields $\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$ and we have defined the degrees $\deg \phi$, $\deg_s(\phi)$ and $\deg_i(\phi)$.

A.6.1 Example:

For an elliptic curve E and for each $m \in \mathbb{Z}$, we have a *multiplication by m* map, which will be denoted by $[m]$. By the expression of the addition of points on E it is easily seen that $[m]$ is an isogeny and that it is non-constant.

Proposition A.6.2. *The degree of the multiplication-by-m map is m^2.*

By $[0]$ we denote the constant morphism $P \mapsto \mathcal{O}$. As with any constant map, by convention $\deg[0] = 0$.

Theorem A.6.3. *Let $\phi : E_1 \to E_2$ be an isogeny between elliptic curves. Then ϕ is a homomorphism for the respective group laws.*

Then if ϕ is a non-zero isogeny, its kernel $\operatorname{Ker} \phi = \phi^{-1}(\mathcal{O})$ is finite, as there are at most $\deg \phi$ elements in the fiber of any point, and it is thus a finite subgroup of E_1.

Theorem A.6.4. *Let $\phi : E_1 \to E_2$ be a non-zero isogeny.*

a) For every $Q \in E_2$,

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

Further, for every $P \in E_1$, $e_\phi(P) = \deg_i(\phi)$.

b) If ϕ is separable, then ϕ is unramified, $\#\operatorname{Ker}(\phi) = \deg \phi$ and $\overline{K}(E_1)$ is a Galois extension of $\phi^*\overline{K}(E_2)$.

A.6.2 The dual isogeny.

Let $\phi : E_1 \to E_2$ be a non-constant isogeny. We have seen that ϕ induces a map $\phi^* : \operatorname{Pic}^0(E_2) \to \operatorname{Pic}^0(E_1)$ and that for $i = 1, 2$ there are group isomorphisms $\kappa_i : E_i \to \operatorname{Pic}^0(E_i)$. Thus there is a homomorphism going in the opposite direction to ϕ given by:

$$E_2 \xrightarrow{\kappa_2} \operatorname{Pic}^0(E_2) \xrightarrow{\phi^*} \operatorname{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1$$

This map can be computed as follows: for $Q \in E_2$ pick any $P \in E_1$ such that $\phi(P) = Q$. Then $\kappa_1^{-1} \circ \phi^* \circ \kappa_2(Q) = [\deg \phi](P)$.

It is worth mentioning that it is not straightforward that the map $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$ is given by a rational map, as the process of finding P such that $\phi(P) = Q$ involves taking roots of many polynomial equations.

However, we state the result

Theorem A.6.5. *Let $\phi : E_1 \to E_2$ be an isogeny of degree m.*
There exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [m]$.
As a group homomorphism, $\hat{\phi}$ equals the composition

$$E_2 \longrightarrow \mathrm{Div}^0(E_2) \xrightarrow{\phi^*} \mathrm{Div}^0(E_1) \xrightarrow{sum} E_1$$

$$Q \mapsto Q - O \qquad \sum n_P P \mapsto \sum [n_P]P.$$

The *dual isogeny* to ϕ is the isogeny $\hat{\phi}$ given in the above theorem.
Note: This assumes $\phi \neq [0]$. If $\phi = [0]$ we set $\hat{\phi} = [0]$.

The basic properties of the dual isogeny are given in the following

Theorem A.6.6. *Let $\phi : E_1 \to E_2$ be an isogeny of degree m.*
a) $\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2.
b) If $\psi : E_2 \to E_3$ is another isogeny, then $\widehat{\psi \circ \phi} = \hat{\psi} \circ \hat{\phi}$.
c) If $\psi : E_1 \to E_2$ is another isogeny, then $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$.
d) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.
e) $\deg \hat{\phi} = \deg \phi$.
f) $\hat{\hat{\phi}} = \phi$.

A.7 The group of Torsion Points of $E(\overline{K})$.

Let E be an elliptic curve, $m \in \mathbb{N}$. $E[m] = \{P \in E : [m]P = \mathcal{O}\}$ is the m- torsion subgroup of E.

$$E_{\mathrm{Tor}} = \bigcup_{m=1}^{\infty} E[m]$$

is the torsion subgroup of E. If E is defined over K then $E_{\mathrm{Tor}}(K)$ denotes the points of finite order in $E(K)$.

Proposition A.7.1. *Let K be an algebraically closed field. If $\mathrm{char}(K) = 0$ or if $\mathrm{char}(K)$ is prime to m, then*

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

If $\mathrm{char}(K) = p$, then we have one of the two following situations

$$E[p^r] \cong \begin{cases} \{0\} & \forall r = 1, 2, \ldots \text{ or} \\ \mathbb{Z}/p^r\mathbb{Z} & \forall r = 1, 2, \ldots \end{cases}$$

A.8 More on Frobenius.

Suppose K is a field of characteristic $p > 0$, and $q = p^r$. Let E/K be an elliptic curve given by a Weierstrass equation, that is, an equation of the type $y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then we have the Frobenius morphism $\mathcal{F}_q : E \to E^{(q)}$ that maps (x, y) to (x^q, y^q). If K is the finite field $\mathbb{F}_q$, then $E^{(q)} = E$ and $\mathcal{F}_q$ is an endomorphism of E, called the *Frobenius endomorphism*. The set of points fixed by $\mathcal{F}_q$ is exactly the finite group $E(\mathbb{F}_q)$.

Proposition A.8.1. *Let* $\mathrm{char}(K) = p > 0$, *and* E *an elliptic curve defined over* $\mathbb{F}_q$. *Let* $\mathcal{F}_q : E \to E$ *be the* q*-th power endomorphism, and* $m, n \in \mathbb{Z}$. *Then the map* $m + n\,\mathcal{F}_q : E \to E$ *is separable if and only if* $p \nmid m$. *In particular, the map*

$$1 - \mathcal{F}_q$$

is separable.

Note that

$$E(\mathbb{F}_q) = \mathrm{Ker}(1 - \mathcal{F}_q) = (1 - \mathcal{F}_q)^{-1}(\mathcal{O})$$

and so we have

$$\#E(\mathbb{F}_q) \underset{(A.6.4)}{=} \deg_s(1 - \mathcal{F}_q) \underset{(A.8.1)}{=} \deg(1 - \mathcal{F}_q)$$

For further reference we will rewrite the following facts on Frobenius.

Proposition A.8.2. *Let* E_p *be an elliptic curve defined over* $\mathbb{F}_p$ *and* $\mathcal{F}_p : E \to E$ *be the* p*-th power Frobenius endomorphism. Then,*

a) $\deg \mathcal{F}_p = p$.

b) $\#E(\mathbb{F}_p) = \deg(1 - \mathcal{F}_p)$.

Bibliography

[1] S. Bocherer and R. Schulze-Pillot, On a theorem of waldspurger and on eisenstein series of klingen type, *Math. Ann.* **288** (1990), 361–388.

[2] Z. I. Borevich and I. R. Chafarevich, *Theorie des nombres*, Gauthier-Villars, Paris, 1967.

[3] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields, In: *Number Theory* (H. Jager, ed.), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

[4] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, *Random matrix theory and the Fourier coefficients of half-integral weight forms*, arXiv:math.NT/0412083 v2, 4 Dec 2004.

[5] J. E. Cremona, Computing the degree of the modular parametrization of a modular elliptic curve, *MatComp* **64** (1995), 1235–1250.

[6] C. Delaunay, Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$, *Experimental Mathematics* **10** (2001), 191–196.

[7] M. Eichler, The basis problem for modular forms and the trace of the hecke operators, In: *Modular Functions of One Variabe I*, LNM, vol. 320, Springer-Verlag, Berlin, 1972, pp. 75–151.

[8] M. Emerton, Supersingular elliptic curves, theta series and weight two modular forms., *J. Amer. Math. Soc.* **15** (2002), 671–714.

[9] B. Gross, Heights and the special values of L-series, *CMS Conference Proceedings*, vol. 7, AMS, 1987.

[10] L. C. Gunning, Lectures on modular forms, In: *Annals of Mathematics Studies*, vol. 48, Princeton University Press, 1962.

[11] R. Hartshorne, Algebraic geometry, GTM, vol. 52, Springer Verlag, 1977.

[12] J. Tate J. Silverman, In: *Rational Points on Elliptic Curves*, UTM, Springer, 1992.

[13] A. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, 1992.

[14] N. Koblitz, Introduction to elliptic curves and modular forms, In: *LNM*, vol. 97, Springer Verlag, 1984.

[15] D. Lorenzini, An invitation to arithmetic geometry, GSM, vol. 9, American Mathematical Society, 1996.

[16] D. A. Marcus, *Number fields*, Editorial Board, Springer Verlag, 1977.

[17] B. Mazur, Modular curves and the eisenstein ideal., *Publications mathmatiques del Inst. Hautes Etud. Sci.* **47** (1977), 33–186.

[18] J. Milne, *Course notes: Elliptic curves*, http://www.jmilne.org/math/.

[19] J. Milne, *Course notes: Fields and galois theory*, http://www.jmilne.org/math/.

[20] T. Miyake, *Modular forms*, Springer-Verlag, 1989.

[21] A. Ogg, *Modular forms and dirichlet series*, W. A. Benjamin, 1969.

[22] A. Pacetti, *qalgmodforms*, http://www.ma.utexas.edu/users/villegas/cnt/cnt-frames.html.

[23] A. Pacetti and G. Tornaria, Shimura correspondence for level p^2 and the central values of l-series, *Journal of Number Theory* **124** (2007), 396–414.

[24] A. Pizer, An algorithm for computing modular forms on $\Gamma_0(N)$, *JALG* **64** (1980), 340–390.

[25] H. Rademacher, *Topics in analytic number theory*, Springer-Verlag, 1973.

[26] M. O. Rubinstein, 1992, Private communication.

[27] J. P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, 1968.

[28] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[29] G. Shimura, On modular forms of half integral weight, *AnnMatSec* **97** (1973), 440–481.

[30] C. Siegel, über die analytische theory der quadratic formen, gesammelte abhandlungen, vol. Band I, Springer-Verlag, Berlin/New York, 1967.

[31] J. Silverman, The arithmetic of elliptic curves, GTM, vol. 106, Springer, 1992.

[32] G. Tornaria, *Data about the central values of the L-series of (imaginary and real) quadratic twists of elliptic curves*, http://www.ma.utexas.edu/users/tornaria/cnt, 2004.

[33] J. L. Waldspurger, Sur les coefficients de fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.* **60** (1981), 375–484.