ROMA TRE
UNIVERSITÀ DEGLI STUDI

DIPARTIMENTO DI MATEMATICA E FISICA
Corso di Laurea Magistrale in Matematica

An Introduction to Elliptic Curves and Modular Forms

Summary

Relatore:
Prof. Francesco Pappalardi

Candidato:
Federico Campanini
n° matricola 428445

Anno Accademico 2014-2015
Ottobre 2015

AMS Classification: 11F06, 11F11, 11F25, 11G05, 11E05.
Keywords: elliptic curves, modular curves, modular groups, modular forms, Hecke operators.

Summary

The theory of *elliptic curves* and *modular forms* is one subject where the most diverse branches of Mathematics like complex analysis, algebraic geometry, representation theory and number theory come together. Our point of view will be number theoretic. A well-known feature of number theory is the abundance of conjectures and theorems whose statements are accessible to high school students but whose proofs either are unknown or, in some cases, are the culmination of decades of research and use some of the most powerful tools of twentieth century mathematics. In addressing problems such as these, which have no easy solution, it is essential to create strong tools that penetrate in different and apparently completely distinct branches of mathematics. The aim of this thesis is to explore the theory of elliptic curves and modular forms and to develop tools that are essential in the resolution of some remarkable problems, like the Ramanujan conjectures and the Fermat's Last Theorem.

Chapter 1 is devoted to the study of elliptic curves. We have chosen an analytic approach, due to Weierstrass, which involves the theory of elliptic functions. We talk about this topics before to give the definition of elliptic curves.

A **lattice** Λ is a subgroup of $\mathbb{C}$ which is free of dimension 2 over $\mathbb{Z}$ and which generates $\mathbb{C}$ over $\mathbb{R}$. If $\{\omega_1, \omega_2\}$ is a basis of Λ over $\mathbb{Z}$, then we also write $\Lambda = [\omega_1, \omega_2]$ or $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Moreover, we assume the normalizing convention that $Im(\omega_1/\omega_2) > 0$.

A **complex torus** is a quotient of the complex plane by a lattice,

$$\mathbb{C}/\Lambda = \{z + \Lambda \mid z \in \mathbb{C}\}.$$

An **elliptic function f with respect to** Λ is a meromorphic function on $\mathbb{C}$ which is Λ-periodic, i.e.

$$f(z+\omega) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

The most important example of a non-constant elliptic function with respect to a lattice Λ is the **Weierstrass $\wp$-function**, which is defined as

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right],$$

where $\Lambda^* = \Lambda \setminus \{0\}$. The power series development at the origin of this function is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2} z^{2n},$$

where

$$G_m(\Lambda) = G_m = \sum_{\omega \in \Lambda^*} \frac{1}{\omega^m}$$

is the **Eisenstein series of weight** m and it is an example of modular forms, as we will see later. $\wp$ satisfies the differential relation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

where $g_2 = 60G_4$ and $g_3 = 140G_6$, and so the points $(\wp(z), \wp'(z))$ lie on the curve defined by the equation

$$Y^2 = 4X^3 - g_2 X - g_3.$$

The cubic polynomial on the right-hand side has three distinct roots and so its discriminant $\Delta = g_2^3 - 27g_3^2$ does not vanish. Note that we have a map $z + \Lambda \mapsto (\wp(z), \wp'(z))$ from the torus $\mathbb{C}/\Lambda$ to the points of the curve $Y^2 = 4X^3 - g_2X - g_3$, because of the periodicity of $\wp$ and $\wp'$. If we want to embed the points in the projective space $\mathbb{P}^2_{\mathbb{C}}$, we can write $z + \Lambda \mapsto (\wp(z), \wp'(z), 1)$. In this way we obtain a map from the torus $\mathbb{C}/\Lambda$ to the set $E(\mathbb{C})$ of the complex projective points on the homogenized curve $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$, where the lattice points are the points going

to infinity on the curve. Namely, we have a map

$$\begin{aligned}\Phi\colon \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C})\\ 0+\Lambda &\mapsto (0,1,0)\\ z+\Lambda &\mapsto (\wp(z),\wp'(z),1)\end{aligned}$$

and it is easy to see that it is a bijection. Now we introduce the notion of *elliptic curve over* $\mathbb{C}$.

An **elliptic curve** over $\mathbb{C}$ is a cubic projective curve, defined over $\mathbb{C}$, given by the equation

$$E : Y^2Z = 4X^3 + a_2XZ^2 + a_3Z^3, \qquad a_2, a_3 \in \mathbb{C}. \tag{1}$$

Sometimes we write the equation in its non-homogeneous form, namely $E : Y^2 = 4X^3 + a_2X + a_3$. The equation (1) or its non-homogeneous form will be referred to as the **Weierstrass equation**. We say that E is **non-singular** if the cubic polynomial on the right-hand side has three distinct roots, i.e. its discriminant $\Delta = a_2^3 - 27a_3^2 \neq 0$. The set of the complex projective points on the curve is denoted by $E(\mathbb{C})$.

Let $P_z = \Phi(z+\Lambda)$ denotes a generic point in $E(\mathbb{C})$. We can use the one-to-one correspondence Φ to define a commutative group law on $E(\mathbb{C})$, namely for any $z_1 + \Lambda, z_2 + \Lambda$ in $\mathbb{C}/\Lambda$, we can define

$$P_{z_1} + P_{z_2} = P_{z_1+z_2}.$$

In this way we obtain an addition law that has two remarkable properties: first, there is a geometric interpretation for adding points on an elliptic curve and second, we can express the coordinates of $P_{z_1+z_2}$ as rational functions of the coordinates of P_{z_1} and P_{z_2}.

In this way, Φ defines an analytic group isomorphism between the complex torus $\mathbb{C}/\Lambda$ and the elliptic curve $E(\mathbb{C})$ defined by the equation $Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$. It follows that for any complex torus $\mathbb{C}/\Lambda$ there exists an elliptic curve $E(\mathbb{C})$ such that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. A result known as the **Uniformization Theorem** say us that the converse holds as well: in fact for any elliptic curve given by an equation $E : Y^2 = 4X^3 + a_2X + a_3$, there

exists a lattice Λ such that $a_2 = -g_2(\Lambda)$, $a_3 = -g_3(\Lambda)$ and $\mathbb{C}/\Lambda$ is isomorphic to $E(\mathbb{C})$ via Φ. The Uniformization Theorem allows us to treat complex analytic objects, like complex tori, and algebraic objects, like elliptic curves, in the same manner. So, the term "(complex) elliptic curve" can be used as synonym of "complex torus".

We are interested in class-isomorphism of elliptic curves. If Λ and Λ' are two lattices, then there exists an analytic group homomorphism from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\Lambda'$ if and only if there exists a non-zero element $m \in \mathbb{C}$ such that $m\Lambda \subseteq \Lambda'$ and such homomorphism is an isomorphism if and only if $m\Lambda = \Lambda'$. It follows that if $\Lambda = [\omega_1, \omega_2]$ is a lattice and if Λ_τ denotes the lattice of the form $[\tau, 1]$, then $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_\tau$, with $\tau = \omega_1/\omega_2$. Therefore for every lattice Λ there exists another one of the form $\Lambda_\tau = [\tau, 1]$ for some $\tau \in \mathbb{C}$ with $Im(\tau) > 0$ such that $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_\tau$. Moreover if $\Lambda = [\omega_1, \omega_2]$ and $\Lambda' = [\omega_1', \omega_2']$ are two lattices, then $\Lambda = \Lambda'$ if and only if there exists $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

where $SL_2(\mathbb{Z})$ denotes the **modular group**

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad - bc = 1 \right\}.$$

Combining these two results we can show that for any $\tau, \tau' \in \mathbb{C}$ with positive imaginary part, $\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'}$ if and only if there exists a matrix $M \in SL_2(\mathbb{Z})$ such that $\left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right) = M \left(\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right)$. The last condition can be rewritten by saying that there exist integers a, b, c, d such that $ad - bc = 1$ and $\tau' = \frac{a\tau + b}{c\tau + d}$.

This fact motivates the definition of an action of $SL_2(\mathbb{Z})$ on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$. The modular group acts on $\mathcal{H}$ through fractional linear transformations as follows:

$$Mz = \frac{az + b}{cz + d}, \qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \quad z \in \mathbb{C}.$$

In Chapter 2 we introduce the main results about this group action and about the action of some subgroups of $SL_2(\mathbb{Z})$ on $\mathcal{H}$. Let N be a positive

integer. The **principal congruence subgroup of level N** is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

(The matrix congruence is interpreted entrywise.) A subgroup Γ of $SL_2(\mathbb{Z})$ is a **congruence subgroup of level N** if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{Z}^+$. The most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

satisfying

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq SL_2(\mathbb{Z}).$$

The results in Chapter 1 show that every $\tau \in \mathcal{H}$ determinates an elliptic curve $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$. However the choice of τ is not unique, but $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'}$ if and only if there exists a matrix $M \in SL_2(\mathbb{Z})$ such that $\tau' = M\tau$. This fact motivates the definition of an equivalence relation between elements on $\mathcal{H}$ under the action of $SL_2(\mathbb{Z})$. We say that two points $\tau,\ \tau' \in \mathcal{H}$ are **equivalent relative to the modular group** $SL_2(\mathbb{Z})$ or $SL_2(\mathbb{Z})$**-equivalent** if there exists a matrix $M \in SL_2(\mathbb{Z})$ such that $\tau' = M\tau$. We write $\tau \sim \tau'$.

"$\sim$" defines an equivalence relation and the set of all equivalence classes is denoted by

$$Y(1) = SL_2(\mathbb{Z}) \setminus \mathcal{H},$$

to indicate that $SL_2(\mathbb{Z})$ acts on $\mathcal{H}$ on the left. So $Y(1)$ is the quotient space of orbit under $SL_2(\mathbb{Z})$ and it is a **modular curve**. Since $M\tau = (-M)\tau$, sometimes the equivalence relation is defined with respect to the quotient $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$. This group acts faithfully on $\mathcal{H}$. Clearly we can generalize this definition for any congruence subgroup Γ of $SL_2(\mathbb{Z})$. The

modular curve $Y(\Gamma)$ for Γ is defined as

$$Y(\Gamma) = \Gamma \setminus \mathcal{H} = \{\Gamma z \mid z \in \mathcal{H}\}.$$

and the special cases of modular curves for $\Gamma_0(N), \Gamma_1(N)$ and $\Gamma(N)$ are denoted by

$$Y_0(N) = \mathcal{H}/\Gamma_0(N), \quad Y_1(N) = \mathcal{H}/\Gamma_1(N), \quad Y(N) = \mathcal{H}/\Gamma(N).$$

We have seen that every class-isomorphism of elliptic curves corresponds to a point on $Y(1)$. The modular curves for congruence subgroups generalize this fact: the quotients of the upper half plane by congruence subgroups can be described by the sets of equivalence classes of elliptic curves enhanced by corresponding torsion data. The most important examples are discussed in Section (2.3) and we refer to it for details. A significant part of Chapter 2 is devoted to the proof of the fact that modular curves can be viewed as Riemann surfaces that can be compactified. Besides being a remarkable result, this fact allows us to study some important aspects of the action of the modular group and of its subgroups on $\mathcal{H}$. In particular we introduce the concept of **cusps**, the points that we need to add to $Y(\Gamma)$ to compactify it. The formal construction of these points is the following. We start to define the *extended half plane* as the union of $\mathcal{H}$ and a copy of the projective line over $\mathbb{Q}$, i.e.

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

The set $\{(s:1) \mid s \in \mathbb{Q}\}$ can be identified with $\mathbb{Q}$, while the point $(1:0)$ is the point at infinity, which we identify with "$i\infty$". We can extend the action of $SL_2(\mathbb{Z})$ on all $\mathcal{H}^*$. To do this, let $M \in SL_2(\mathbb{Z})$ and $(s:t) \in \mathbb{P}^1(\mathbb{Q})$. We define

$$M(s:t) = (as + bt : cs + dt) \in \mathbb{P}^1(\mathbb{Q}), \qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

This action is consistent with the previous definition of the action of $SL_2(\mathbb{Z})$ in $\mathcal{H}$. In fact, by the identification $(s:1) = s \in \mathbb{Q}$, if $cs + d \neq 0$ we obtain

$$M(s:1) = Ms = (as + b : cs + d) = (\frac{as+b}{cs+d} : 1) = \frac{as+b}{cs+d} \in \mathbb{Q},$$

while, if $cs + d = 0$, we obtain $M(s : 1) = (1 : 0) = i\infty$ and similarly, for the point at infinity we have

$$M(1 : 0) = (a : c) = \begin{cases} \frac{a}{c} \in \mathbb{Q} & \text{if } c \neq 0 \\ \infty & \text{if } c = 0. \end{cases}$$

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. The quotient $X(\Gamma) = \mathcal{H}^*/\Gamma$ is called the **modular curve** for Γ. The elements in $X(\Gamma)$ that have a representative in $\mathbb{P}^1(\mathbb{Q})$, i.e. the points Γz with $z \in \mathbb{P}^1(\mathbb{Q})$, are called the **cusps**. As we have said, these points allow us to compactify the modular curve $Y(\Gamma)$, and we note that we have just added only finitely many points. In fact the modular curve $X(1)$ has one cusp and for any congruence subgroup Γ of $SL_2(\mathbb{Z})$, the modular curve $X(\Gamma)$ has finitely many cusps.

Chapter 3 gives the basic definitions and the main results of modular forms which are complex analytic functions on the upper half-plane that are "essentially invariant" under the action of the modular group, in a sense that we explain hereinafter.

For any matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ define the **factor of automorphy** $j(M, z) \in \mathbb{C}$ for $z \in \mathcal{H}$ to be $j(M, z) = cz + d$, and for any integer k define the **weight-k operator** $[M]_k$ on functions $f : \mathcal{H} \to \mathbb{C}$ by

$$(f[M]_k)(z) = j(M, z)^{-k} f(Mz), \qquad z \in \mathcal{H}.$$

Since the factor of automorphy is never zero or infinity, f and $f[M]_k$ have the same zeros and poles. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is **weakly modular of weight k with respect to Γ** if

$$f[M]_k = f \quad \text{for all } M \in \Gamma.$$

When $\Gamma = SL_2(\mathbb{Z})$ we simply say that f is weakly modular of weight k. Necessary and sufficient condition for f to be weakly modular of weight k with respect to Γ is that this transformation law holds when M is each of the generators of Γ. In particular, since the modular group $SL_2(\mathbb{Z})$ is generated

by the two matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

which correspond to the transformations $z \mapsto z+1$ and $z \mapsto -1/z$, a function f is weakly modular of weight k if and only if $f(z+1) = f(z)$ and $f(-1/z) = z^k f(z)$. In particular f is $\mathbb{Z}$-periodic. We also observe that that if $M = -I$, then we obtain $f = (-1)^k f$ and so the only weakly modular function of any odd weight k is the zero function.

Now we want to introduce the concept of "*holomorphy at* $i\infty$". We have just seen that a weakly modular function f is $\mathbb{Z}$-periodic. Let D be the open complex punctured unit disk, i.e. $D = \{z \in \mathbb{C} \mid |z| < 1\} \setminus \{0\}$. Recall that the $\mathbb{Z}$-periodic holomorphic map $z \mapsto q = e^{2\pi i z}$ takes $\mathcal{H}$ to D. Thus, corresponding to f, the function $g : D \to \mathbb{C}$ where $g(q) = f(log(q)/2\pi i)$ is well defined even though the logarithm is only determinated up to $2\pi i\mathbb{Z}$, and $f(z) = g(e^{2\pi i z})$. If f is holomorphic on $\mathcal{H}$ then g is holomorphic on D, and so g has a Laurent expansion $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ for $q \in D$. Define f to be **holomorphic at** $i\infty$ if g can be extended holomorphically to the unit disk, i.e. the Laurent series sums over $n \in \mathbb{N}$. This means that f has a **Fourier expansion**

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

Since $q \to 0$ if and only if $Im(z) \to \infty$, to show that a weakly modular form f is holomorphic at $i\infty$ it suffices to verify that $lim_{Im(z)\to\infty} f(z)$ exists or even just that $f(z)$ is bounded as $Im(z) \to \infty$.

Let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a **modular form of weight k** if

1. f is holomorphic on $\mathcal{H}$;
2. f is weakly modular of weight k;
3. f is holomorphic at $i\infty$.

The set of modular forms of weight k forms a complex vector space which

is denoted by $\mathcal{M}_k(SL_2(\mathbb{Z}))$. A **cusp form** of weight k is a modular form of weight k whose Fourier expansion has leading coefficient $a_0 = 0$, i.e.

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

The complex vector subspace of cusp forms is denoted by $\mathcal{S}_k(SL_2(\mathbb{Z}))$.

We can define modular forms with respect to a congruence subgroup Γ in a similar way. Since Γ contains $\Gamma(N)$ for some N, Γ contains a translation $z \mapsto z + h$, i.e. an element of the form

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},$$

for some minimal $h > 0$ (note that h may properly divide N). If $f : \mathcal{H} \to \mathbb{C}$ is weakly modular with respect to Γ, then f is $h\mathbb{Z}$-periodic and thus has a corresponding function $g : D \to \mathbb{C}$ where again D is the open complex punctured unit disk, but now we have $f(z) = g(q_h)$, with $q_h = e^{2\pi i z/h}$. As before, if f is also holomorphic on the upper half plane then g is holomorphic on D and so it has a Laurent expansion. Define such f to be **holomorphic at** $i\infty$ if g extends holomorphically to $q = 0$. Thus f has a Fourier expansion

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

A function $f : \mathcal{H} \to \mathbb{C}$ is a **modular form of weight k with respect to** Γ if

1. f is holomorphic on $\mathcal{H}$;
2. f is weakly modular of weight k with respect to Γ;
3. $f[M]_k$ is holomorphic at $i\infty$ for all $M \in SL_2(\mathbb{Z})$.

If in addition

4. $a_0 = 0$ in the Fourier expansion of $f[M]_k$ for all $M \in SL_2(\mathbb{Z})$,

then we say that f is a **cusp form of weight k with respect to** Γ. The set of modular forms of weight k with respect to Γ forms again a complex vector space which is denoted by $\mathcal{M}_k(\Gamma)$, while the vector subspace of the cusp forms of weight k with respect to Γ is denoted by $\mathcal{S}_k(\Gamma)$.

Note that if f is weakly modular of weight k with respect to a congruence subgroup Γ, then for any $M \in SL_2(\mathbb{Z})$, $f[M]_k$ is weakly modular of weight k with respect to $M^{-1}\Gamma M$, which is again a congruence subgroup, and the condition (3) make sense. Moreover conditions (3) and (4) give us the holomorphy at the cusps in terms of holomorphy at ∞ in a natural way via the $[M]_k$ operators. For this reason we sometimes say that f is *holomorphic at the cusps* and *vanishes at the cusps* respectively.

An important example of modular forms are the **Eisentein series**. We have seen that if Λ is a lattice, the series

$$G_k(\Lambda) = \sum_{\omega \in \Lambda^*} \frac{1}{\omega^k}$$

appears in the Laurent expansion at the origin of $\wp_\Lambda$. For any lattice of the form $\Lambda_z = [z, 1]$ for some $z \in \mathcal{H}$, we set

$$G_k(z) = G_k(\Lambda_z) = \sum_{(0,0)\neq(c,d)\in\mathbb{Z}^2} \frac{1}{(cz+d)^k}.$$

This series defines a modular form of weight k for $SL_2(\mathbb{Z})$. The Fourier expansion of $G_k(z)$ is

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

where ζ denotes the Riemann zeta function and the n^{th}-coefficient is the arithmetic function

$$\sigma_{k-1}(n) = \sum_{m|n, m>0} m^{k-1}.$$

We can normalize the Eisenstein series by dividing by $2\zeta(k)$. We obtain the

normalized Eisenstein series

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

whose Fourier expansion at infinity has the constant term equal to one and the other coefficients equal to rational numbers with a common denominator. Another important example of modular form is the *discriminant function*. It is defined as

$$\Delta : \mathcal{H} \to \mathbb{C}, \qquad \Delta(z) = g_2^3(z) - 27 g_3^2(z).$$

where

$$g_2(z) = 60 G_4(z), \qquad \text{and} \qquad g_3(z) = 140 G_6(z).$$

The discriminant function is a cusp form of weight k and it has no zeros on $\mathcal{H}$. There is a useful result that allow us to study the vector spaces of modular forms and to compute the dimension formulas for $\mathcal{M}_k(SL_2(\mathbb{Z}))$. Let f be a weakly modular function of weight k for $SL_2(\mathbb{Z})$. For any $\tau \in \mathcal{H}$, let $v_\tau(f)$ denote the order of zero or minus the order of pole of f at the point τ. Let $v_\infty(f)$ denote the index of the first non-vanishing term in the Fourier expansion of f. Then

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_{\mu_3}(f) + \sum_{\tau \in SL_2(\mathbb{Z}) \setminus \mathcal{H},\ \tau \neq i, \mu_3} v_\tau(f) = \frac{k}{12}$$

(With $\tau \in SL_2(\mathbb{Z}) \setminus \mathcal{H},\ \tau \neq i, \mu_3$, we means that the sum is taken over all points $\tau \in \mathcal{H}$ modulo $SL_2(\mathbb{Z})$, not in the orbit of i or μ_3.) This formula has an important consequence. For any even integer k we have

1. The only modular forms of weight 0 for $SL_2(\mathbb{Z})$ are constants, i.e. $\mathcal{M}_0(SL_2(\mathbb{Z})) = \mathbb{C}$;
2. $\mathcal{M}_k(SL_2(\mathbb{Z})) = 0$ if $k < 0$ or $k = 2$;
3. $\mathcal{M}_k(SL_2(\mathbb{Z}))$ is one-dimensional, generated by E_k (i.e. $\mathcal{M}_k(SL_2(\mathbb{Z})) = \mathbb{C}E_k$), if k =4,6,8,10 or 14;
4. $\mathcal{S}_k(SL_2(\mathbb{Z})) = 0$ if $k < 12$ or $k = 14$; $\mathcal{S}_{12}(SL_2(\mathbb{Z})) = \mathbb{C}\Delta$ and for $k > 14$, $\mathcal{S}_k(SL_2(\mathbb{Z})) = \Delta \mathcal{M}_{k-12}(SL_2(\mathbb{Z}))$;
5. $\mathcal{M}_k(SL_2(\mathbb{Z})) = \mathcal{S}_k(SL_2(\mathbb{Z})) \oplus \mathbb{C}E_k$ for $k > 2$.

6. The dimension of $\mathcal{M}_k(SL_2(\mathbb{Z}))$ as a $\mathbb{C}$-vector space is finite and it is given by

$$\dim_{\mathbb{C}}(\mathcal{M}_k(SL_2(\mathbb{Z}))) = \begin{cases} 0 & \text{if } k < 0 \text{ or } k \text{ is odd;} \\ \left[\frac{k}{12}\right] & \text{if } k \geq 0,\ k \equiv 2 \pmod{12} \\ \left[\frac{k}{12}\right] + 1 & \text{otherwise} \end{cases}$$

where $[x]$ denotes the floor function. Moreover, for all integers k there exists an isomorphism of $\mathbb{C}$-vector spaces

$$\mathcal{M}_{2k-12}(SL_2(\mathbb{Z})) \xrightarrow{\sim} \mathcal{S}_{2k}(SL_2(\mathbb{Z})) \qquad f(z) \mapsto \Delta(z)f(z)$$

and in particular

$$\dim_{\mathbb{C}}(\mathcal{S}_{2k}(SL_2(\mathbb{Z}))) = \dim_{\mathbb{C}}(\mathcal{M}_{2k-12}(SL_2(\mathbb{Z}))).$$

In Chapter 4 we study the **Hecke operators**. Historically, this operators were used by Mordell in 1917 to prove that the **Ramanujan τ function** is a multiplicative function. Mordell used this operators in a paper on the special cusp form of Ramanujan, ahead of the general theory given by Hecke (1937). There are several ways to define the Hecke operators: in this thesis, we define them as **double coset operators**. For any Γ_1 and Γ_2 congruence subgroups of $SL_2(\mathbb{Z})$ and for any $A \in GL_2^+(\mathbb{Q})$ we define the **double coset** as the set

$$\Gamma_1 A \Gamma_2 = \{M_1 A M_2 \mid M_i \in \Gamma_i\}.$$

The group Γ_1 acts on the double coset by left multiplication, so we can write $\Gamma_1 A \Gamma_2$ as a disjoint union of its orbits $\Gamma_1 B_j$, for some representatives $B_j = M_{1,j} A M_{2,j}$. Moreover for each $B \in GL_2^+(\mathbb{Q})$ and $k \in \mathbb{Z}$ we can define the weight-k operator on functions $f : \mathcal{H} \to \mathbb{C}$ by

$$(f[B]_k)(z) = det(B)^{k-1} j(B,z)^{-k} f(Bz), \qquad z \in \mathbb{H}$$

where the factor of automorphy $j(B,z)$ and the action of $GL_2^+(\mathbb{Q})$ on $\mathcal{H}$ are defined as in the case of the modular group $SL_2(\mathbb{Z})$, i.e.

$$Bz = \frac{az+b}{cz+d}, \quad j(B,z) = cz+d, \quad \text{for all } B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{Q}).$$

The **weight-k $\Gamma_1 A \Gamma_2$ double coset operator** on $\mathcal{M}_k(\Gamma_1(N))$ is given by

$$f[\Gamma_1 A \Gamma_2]_k = \sum_j f[B_j]_k$$

where $\{B_j\}$ are orbit representatives for $\Gamma_1 A \Gamma_2$. The double coset operator is well defined since the set $\{B_j\}$ is finite and the definition is independent from the choice of this set.

The double coset operator takes modular forms with respect to Γ_1 to modular forms with respect to Γ_2 and takes cusp forms into cusp forms:

$$[\Gamma_1 A \Gamma_2]_k : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$$

and

$$[\Gamma_1 A \Gamma_2]_k : \mathcal{S}_k(\Gamma_1) \to \mathcal{S}_k(\Gamma_2).$$

We are interested in Hecke operators from $\mathcal{M}_k(\Gamma_1(N))$ to itself. The first type of Hecke operator we consider is the **diamond operator**. Let d be an integer such that $GCD(N, d) = 1$. The diamond operator on $\mathcal{M}_k(\Gamma_1(N))$ is given by

$$\langle d \rangle f = f[M]_k \quad \text{for any } M = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N) \text{ with } \delta \equiv d \pmod{N}.$$

The definition of the diamond operator can be extended for all n by defining $\langle n \rangle$ to be the zero operator if $GCD(n, N) > 1$ or $n = 0$. For all $n, m \in \mathbb{Z}$ we have $\langle nm \rangle = \langle n \rangle \langle m \rangle = \langle m \rangle \langle n \rangle$.

The second type of Hecke operators is again an operator on $\mathcal{M}_k(\Gamma_1(N))$. Let p be prime. The T_p operator is defined as

$$T_p = [\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N)]_k : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)).$$

We can extend the definition of T_p to T_n for all $n \in \mathbb{Z}$. First set $T_1 = Id$. Then for any prime powers, we define inductively

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}, \quad \text{for } r \geq 2.$$

Since $T_{p^r} T_{p^s} = T_{p^s} T_{p^r}$ for distinct primes and for any $r, s \geq 1$, it is well

defined for all $n \in \mathbb{Z}$

$$T_n = \prod_{i=1}^{m} T_{p_i^{e_i}} \quad \text{where } n = p_1^{e_1} \cdot ... \cdot p_m^{e_m}.$$

Clearly $T_m T_n = T_n T_m$ and in particular, $T_{nm} = T_n T_m$ if $GCD(m, n) = 1$.

We see that we can endow the space of cusp forms with an inner product. For any congruence subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$, the **Petersson inner product**

$$\langle \cdot\, , \cdot \rangle_\Gamma : \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \to \mathbb{C}$$

is given by

$$\langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(z)\overline{g(z)} Im(z)^k d\mu(z).$$

The Hecke operators $\langle n \rangle$ and T_n on $\mathcal{S}_k(\Gamma_1(N))$ are normal for $GCD(n, N = 1)$. From the Spectral Theorem of linear algebra, given a commuting family of normal operators on a finite-dimensional inner product space, the space has a orthogonal basis of simultaneous eigenvectors for the operators. Thus we have that the space $\mathcal{S}_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous **eigenforms** for the family of Hecke operators $\{\langle n \rangle\, , T_n \mid GCD(n, N) = 1\}$, where by an **eigenform for an Hecke operator** T we mean a cusp form $f \in \mathcal{S}_k(\Gamma_1(N))$ such that f is an eigenvector for T.

Now let d, N be integers, with $d \mid N$. Note there is a natural inclusion $\mathcal{S}_k(\Gamma_1(\frac{N}{d})) \subseteq \mathcal{S}_k(\Gamma_1(N))$, but there is another way to embed $\mathcal{S}_k(\Gamma_1(\frac{n}{d}))$ into $\mathcal{S}_k(\Gamma_1(N))$. In fact if we set

$$M_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \in GL_2^+(\mathbb{Q}),$$

then we have an injective linear map from $\mathcal{S}_k(\Gamma_1(\frac{N}{d}))$ to $\mathcal{S}_k(\Gamma_1(N))$:

$$[M_d]_k : \mathcal{S}_k(\Gamma_1(\frac{N}{d})) \to \mathcal{S}_k(\Gamma_1(N)), \qquad f(z) \mapsto (f[M_d]_k)(z) = d^{k-1} f(dz).$$

We can distinguish the part of $\mathcal{S}_k(\Gamma_1(N))$ coming from lower levels and the "new" one. For each divisor d of N, let i_d be the map

$$\mathcal{S}_k(\Gamma_1(\frac{N}{d})) \times \mathcal{S}_k(\Gamma_1(\frac{N}{d})) \longrightarrow \mathcal{S}_k(\Gamma_1(N))$$

given by

$$(f, g) \longmapsto f + g[M_d]_k.$$

The **subspace of old forms at level** N is

$$\mathcal{S}_k(\Gamma_1(N))^{old} = \sum_{p|N} i_p(\mathcal{S}_k(\Gamma_1(\frac{N}{p})) \times \mathcal{S}_k(\Gamma_1(\frac{N}{p})))$$

and the **subspace of new forms at level** N is defined as

$$\mathcal{S}_k(\Gamma_1(N))^{new} = (\mathcal{S}_k(\Gamma_1(N))^{old})^{\perp},$$

i.e. the orthogonal complement of the subspace of old forms with respect to the Petersson inner product. A **Hecke eigenform** or simply an **eigenform** is a non-zero modular form $f \in \mathcal{M}_k(\Gamma_1(N))$ that is an eigenform for the operators T_n and $\langle n \rangle$ for all $n \in \mathbb{Z}^+$. We say that $f = \sum_{n \geq 0} a_n(f) q^n$ is **normalized** when $a_1(f) = 1$. A **newform** is a normalized eigenform in $\mathcal{S}_k(\Gamma_1(N))^{new}$.

We conclude the Chapter by proving one of the most important results about the theory of the Hecke operators. Recall that the space $\mathcal{S}_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenforms for the family of Hecke operators $\{\langle n \rangle, T_n \mid GCD(n, N) = 1\}$. We see that we can eliminate the restriction $GCD(n, N) = 1$ for $\mathcal{S}_k(\Gamma_1(N))^{new}$. In fact if $f \in \mathcal{S}_k(\Gamma_1(N))^{new}$ is a non-zero eigenform for the Hecke operators T_n and $\langle n \rangle$ for all n with $GCD(n, N) = 1$, then f is a Hecke eigenform and it is a newform up to a suitable scalar multiple. Moreover the set of newforms is an orthogonal basis for the space $\mathcal{S}_k(\Gamma_1(N))^{new}$. Each such newform has the property that its Fourier coefficients are its T_n-eigenvalues. That is, every newform satisfies $T_n f = a_n(f) f$ for all $n \in \mathbb{Z}^+$.

In Chapter 5 we explain some applications of modular forms and Hecke operators. We prove two results concerning the **Ramanujan τ function**, which is an arithmetic function that, in the early twentieth century, evoked the curiosity of the great Indian mathematician Srinivasa Ramanujan. He proved or conjectured many of its properties and that is why this function is

named after him. This function is defined by the following identity:

$$\sum_{n\geq 1} \tau(n)q^n = (2\pi)^{-12}\Delta(z).$$

In other words, $\tau(n)$ is defined to be the n^{th}-coefficient in the Fourier expansion of $(2\pi)^{-12}\Delta(z)$. The first property that we prove is a famous congruence due to Ramanujan in 1916:

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

The second property of the τ function was proved by Mordell in 1917. By using the theory of the Hecke operators he proved that the τ function is a multiplicative function, i.e.

$$\tau(mn) = \tau(m)\tau(n) \quad \text{if } GCD(m,n) = 1.$$

There are some outstanding problems concerning the τ function. The most famous is the *Lehmer's conjecture*, which postulates that $\tau(n) \neq 0$ for all $n \in \mathbb{N}$. This assertion was conjectured by D.H. Lehmer in 1947 and it was verified by Derickx, van Hoeij, and Zeng for all $n < 816212624008487344127999$.

The last part of the thesis hints at the role of elliptic functions and modular forms in the proof of Fermat's last theorem. In 1994, Andrew Wiles proved a result known as the Taniyama-Shimura-Weil conjecture or the modularity theorem. This theorem states a strong link between elliptic curves and modular forms and it is certainly one of the most important results in Number Theory: to one hand the Taniyama-Shimura-Weil conjecture implies the Fermat's last theorem, whose proof turned out inaccessible even to the greatest mathematicians for over three centuries; to the other hand this result says us that the elliptic curves and the modular forms are closely related.

The fact that the theory of elliptic curves and modular forms has allowed us to solve such an important problem, as Fermat's Last Theorem is, gives us hope that these tools can be useful in the future to penetrate through the most insidious problems of Number Theory.

Bibliography

[AL70] A.O.L.Atkin and J.Lehner, "Hecke operators on $\Gamma_0(m)$", *Mathematishe Annalen*, **185:134-160** (1970).

[Apo76] T.M.Apostol, "Introduction to Analytic Number Theory", *Undergraduate Texts in Mathematics, Springer*, (1976).

[AZ95] A. N. Andrianov and V. G. Zhuravlev, "Modular Forms and Hecke Operators", *Translations of Mathematical Monographs, American Mathematical Society*, **145** (1995).

[BK07] B.C. Berndt and M.I.Knopp, "Hecke's Theory of Modular Forms and Dirichlet Series", *Monographs in Number Theory, World Scientific Pub Co Inc.*, (2007).

[CSS97] G.Cornell, J.H.Silverman and G.Stevens, "Modular Forms and Fermat's Last Theorem", *Papers from a conference held Aug.9-18,1995, at Boston University, Spingler-Verlag, New York*, (1997).

[DS05] F.Diamond and J.Shurman, "A First Course in Modular Forms", *Graduate Texts in Mathematics, Spingler, New York*, **228** (2005).

[Kil08] L.J.P.Kilford, "Modular Forms: A Classical and Computational Introduction", *Imperial College Press*, (2008).

[Kob93] N.Koblitz, "Introduction to Elliptic Curves and Modular Forms", *Graduate Texts in Mathematics, Spingler-Verlag, New York*, **97** (1993).

[Lan76] S.Lang, "Introduction to Modular Forms", *Grundl. Math. Wiss., Spingler-Verlag, Berlin, New York*, **222** (1976).

[Lan87] S.Lang, "Elliptic Functions", *Graduate Texts in Mathematics, Spingler-Verlag, Berlin, New York*, **112** (1987).

[Lan93] S.Lang, "Complex Analysis", *Graduate Texts in Mathematics, Spingler-Verlag, New York*, **103** (1993).

[Loz11] Á.Lozano-Robledo, "Elliptic Curves, Modular Forms, and Their L-functions", *Student Mathematical Library, American Mathematical Society*, (2011).

[Mil90] J.S.Milne, "Modular Functions and Modular Forms", (1990) **http://www.jmilne.org/math** .

[Miy89] T.Miyake, "Modular Forms", *Springer Monographs in Mathematics, Springer Berlin Heidelberg*, (1989).

[Mur93] M.Ram Murty, "Topics in Number Theory", *Lectures at Mehta Research Institute, Allahabad*, **211 002** (1993).

[Rib90] Kenneth Ribet, " From the Taniyama-Shimura conjecture to Fermat's last theorem", *Annales de la faculté des sciences de Toulouse* 5^e *Série*, **11 (1): 116–139** (1990).

[Rib90a] Kenneth Ribet, "On modular representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms", *Inven.math.*, **100: 431-476** (1990).

[Ser73] J.P.Serre, "A Course in Arithmetic", *Graduate Texts in Mathematics, Springer-Verlag*, **7** (1973).

[Shi11] G.Shimura, "Modular Forms: Basics and Beyond", *Springer Monographs in Mathematics, Springer*, (2011).

[Shi71] G.Shimura, "Introduction to the Arithmetic Theory of Automorphic Functions", *Iwanami Shoten and Princeton University Press*, (1971).

[Sil09] J.H.Silverman, "The Arithmetic of Elliptic Curves", *Graduate Texts in Mathematics, Springer*, **106** (2009).

[Was03] L.C.Washington, "Elliptic Curves, Number Theory and Cryptography", *CRC Press Series on Discrete Mathematics and its Applications, Chapman &Hall/CRC, New York*, **114** (2003).

[Wil95] Andrew Wiles, "Modular Elliptic Curves and Fermat's Last Theorem", *Annals of Mathematics*, **142 (3): 443–551** (1995).