UNIVERSIDAD SAN FRANCISCO DE QUITO

USFQ

Colegio de Ciencias e Ingenierías

A new method to compute Hecke eigenvalues for Classical Modular Forms.

Nicolás Coloma Carphio

Matemáticas

Trabajo de fin de carrera presentado como requisito

para la obtención del título de

Matemático

Cumbayá, 27 de mayo de 2020

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

HOJA DE CALIFICACIÓN DE TRABAJO DE FIN DE CARRERA

A new method to compute Hecke eigenvalues for Classical Modular Forms.

Nicolás Coloma Carphio

Calificación:

Nombre del profesor, Título académico: Nathan C. Ryan, Ph.D.

Firma del profesor .....

Cumbayá, 27 de mayo de 2020

DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante	.....
Nombres y apellidos:	Nicolás Coloma Carphio
Código:	00137654
Cédula de Identidad:	1718607201
Lugar y fecha:	Cumbayá, Mayo 2020

ACLARACÍON PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

[1]

[1] **Note:** The following document is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this document – in whole or in part – should not be considered a publication. For further information see Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

Para mi familia.

AGRADECIMIENTOS

Quiero empezar agradeciendo a mis padres y a mi hermana por el inigualable apoyo que me han brindado siempre. Han sido, son y serán mi motivación. Todo lo que he conseguido se los debo a ustedes. Quiero agradecer a todo el resto de mi familia por siempre estar dispuestos a brindarme un consejo y ayudarme en todo momento.

De la misma manera quisiera agradecer a Nathan Ryan, director de este trabajo de tesis. Muchas gracias por guiarme en todo lo relacionado a este trabajo y ayudarme en mi carrera. Además, quisiera aprovechar para dar un agradecimiento especial a John Skukalek y David Hervas, quienes convivieron conmigo durante prácticamente toda mi carrera, por enseñarme la belleza de las matemáticas desde mis primeros semestres en la USFQ, por todo el tiempo que me han dedicado, sus recomendaciones y nuestras pláticas; más allá de ser excelentes profesores son increíbles seres humanos. También quiero agradecer a Antonio Di Teodoro quien fue quien me inició en el mundo de la investigación y a toda la comunidad educativa de la Universidad San Francisco de Quito, en especial a Eduardo Alba, Svetlana Arbakova y Andrea Moreira quienes me guiaron estos años.

Gracias también a mi compañero Francisco Ponce, con quien compartí básicamente toda la carrera. Tampoco puedo olvidar a todas las personas que conocí en esta etapa quienes, de una u otra forma, me han ayudado a crecer todos estos años y con quienes he pasado varios de los mejores momentos en esta etapa.

Finalmente quiero agradecer a una persona muy especial que llegó a mi vida. A mi novia Lucía, gracias por el incondicional apoyo, paciencia y por ser una persona que saca lo mejor de mí. Porque aparte de impulsarme a ser un mejor matemático, me has hecho ser una mejor persona.

Durante estos años tuve la oportunidad de aprender, de visitar lugares sensacionales, de conocer gente increíble, y de hacer grandes amistades.

Muchas gracias a todos.

RESUMEN

En el presente trabajo se propone un nuevo método para calcular los autovalores de operadores de Hecke aplicados a formas modulares clásicas de nivel 1 basado en su evaluación analítica en puntos del plano superior. Utilizamos el hecho de que el espacio de formas modulares M_k es un espacio vectorial de dimensión finita sobre $\mathbb{Q}$ con una base formada de elementos de la forma $E_4^a E_6^b$ donde E_4 y E_6 son series de Eisenstein de peso 4 y 6 respectivamente. Nuestro enfoque funciona con precisión arbitraria, permite controlar el error y mejora los métodos exactos actuales.

Palabras Clave: Formas Modulares, Autovalores de Hecke, Evaluación Analítica, Aproximación Numérica, Algoritmo.

ABSTRACT

In the present work we propose a new method to calculate Hecke eigenvalues for classical modular forms of level 1 based of their analytic evaluation at points in the upper half plane. We use the fact that the space of modular forms M_k is a finite dimensional vector space over $\mathbb{Q}$ with a basis of elements of the form $E_4^a E_6^b$ where E_4 and E_6 are Eisenstein series of weight 4 and 6 respectively. Our approach works with arbitrary precision, allows for a strict control of the error in the approximation, and outperforms current exact computation methods.

Key Words: Modular Forms, Hecke eigenvalues, Analytic Evaluation, Numerical Approximation, Algorithm.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I
INTRODUCTION

Modular forms are well studied because they have many applications and connections with different areas of mathematics. Probably, the best known application of modular forms is in the study of elliptic curves and their usefulness for counting the points on an elliptic curve modulo a prime. The algorithms devised to do so have been proven useful not only in the field of number theory providing useful tools to solve diophantine equations, but they have also served in other fields such as cryptography. The connection between elliptic curves and the coefficients of modular forms have opened many new interesting possibilities for study and research. For instance, an entire book [1] is focused on showing and understanding the proof of the modularity theorem: All rational elliptic curves arise from modular forms (previously known as the Taniyama - Shimura conjectura). Andrew Wiles proved this result for a large class of elliptic curves, an approach that led him to achieve the proof of Fermat's last theorem after 350 years. The complete modularity theorem was proved later on.

For example, consider an elliptic curve E that can be defined by the equation,

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

The problem with this equation is that, while sometimes it may seem easy to find particular rational solutions, it becomes difficult to show the complete set of solutions, or even discuss wether it is finite or not. One way to work around is to consider, instead of the full set of solutions, just solutions modulo a prime p; if we keep a and b fixed,

then we only have to worry about p^2 number of cases and possible solutions. To show this consider the elliptic curve,

$$y^2 = x^3 - x$$

and let $p = 5$. Modulo 5 we see that the set of solutions is precisely:

$$\{(0,0), (1,0), (4,0), (2,1), (3,2), (3,3), (4,2)\}$$

every solution can be easily checked, for instance $3^2 \equiv 4 \equiv 3^3 - 3$ (mód 5). There are formulas to estimate the number of solutions modulo p and there is also a famous formula for taking into the account the "error" of this approximation. If we define N_p as the number of solutions modulo p then we can state an error term a_p as $a_p = N_p - p$. The fascinating connection between elliptic curves and modular forms is that, as we will see, modular forms can be expressed as a fourier series with coefficients c_i, the result is that for each modular form there exists an elliptic curve such that $a_p = c_p$ for all prime p.

Even though the exact definition of a modular form, which will be introduced later on, might be mystifying, it actually arises from a very natural way. Picture the real line. The functions sin and cos have very special properties: if you shift their argument by an integer multiple of 2π, you get the same value; in other words, sin and cos are periodic. This condition could be reestated as the following: sin and cos are invariant under the action of translations by integer multiples of 2π along the real line. Just like sin and cos have this special property, if instead of $\mathbb{R}$ one thinks of the upper half plane on $\mathbb{C}$, there exists a group of symmetries that act on this plane and a group of functions that are invariant over these group actions, such functions are known as weakly modular forms, once we add the requirement of holomorphy we get the modular

forms.

To give a more precise explanation, consider a lattice $\Lambda \subset \mathbb{C}$ defined as $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where ω_1 and ω_2 are linearly independent, i.e, $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Then we can identify an elliptic curve as the quotient group $\mathbb{C}/\Lambda$ and we want to find functions F such that $F(\Lambda)$ is preserved under certain actions. Multiplying a lattice by a non-zero complex scalar λ just amounts to rotating and reescaling the points on the lattice, so we want functions such that $F(\lambda\Lambda) = F(\Lambda)$ since $\mathbb{C}/\Lambda \cong \mathbb{C}/\lambda\Lambda$. Yet this equation imposes many unnecesary restrictions on our functions and instead we want to consider the equation

$$F(\lambda\Lambda) = \lambda^{-k} F(\Lambda) \tag{1}$$

The functions that satisfy (1) are called *weakly modular forms of weight k.*

Among the reasons why people study modular forms is that modular forms have a Fourier expansion and sometimes arithmetic information is contained in their Fourier coefficients, like for example, eigenvalues of Hecke operators and counting points on elliptic curves. As we mentioned, one can study elliptic curves by studying lattices $\Lambda \subset \mathbb{C}$. Modular forms can be in fact generalized as a function on the complex upper-half plane to an automorphic form as a function on a Lie Gruop G [2].

The space of modular forms is also of interest because given a weight k on a subgroup of $SL_2(\mathbb{Z})$, this space is finite dimensional and algorithmically computable. Also modular forms occur naturally in connections with problems arising in many other areas of mathematics [3]. If one wishes to see more applications of modular forms one can refer to [4].

In terms of Hecke operators, Hecke managed to determine all entire modular forms

with multiplicative coefficients by introducing a sequence of linear operators T_n called the Hecke operators. Hecke operators act on the space of automoprhic forms on a group G to form a commutative ring called the Hecke algebra [2]. These operators are still objects of current research and proof of that is that there still are conjectures about the action of Hecke operators on level 1 modular forms such as Maeda's Conjecture and the Gouvea-Mazur conjecture [5].

Last but not least, objects of extreme importance in this dissertation are the Eisenstein series. Ramanujan started studying Eisenstein series without knowing their connection to modular forms or even number theory. He then realized the coefficients of Eisenstein series in fact contain a lot of connections with other parts of number theory. In particular, it is not difficult to show, and we will later, that Eisenstein series are in fact modular forms. Ramanujan made many contributions to the theory and applications of Eisenstein series in [6], some of which where made within the theory of the divisor function, the partition function, and the number of representations of n as a sum of k squares [7]. Also, the coefficients of Eisenstein series hide very important mathematical objects such as the Bernoulli numbers, special values of the Riemann zeta function $\zeta(s)$ and the sums of powers of the divisors [8]. Such is the case that Eisenestein series of weight k have also been referred as 2-dimensional analogs of the Riemann zeta function [1].

Eisenstein series, are still objects of current research and study. As an example, Langland's study of Eisenstein series inspired his conjectures know as the Langlands program that dictate the role of modular forms (and their generalization known as automorphic forms) in modern number theory. The Langlands program is a set of influential conjetures that relate Galois groups in algebraic number theory to automorphic forms in representation theory.

There are many other fields which show the application of Eisenstein series such as in the theory of automorphic forms (L-functions arise out of the calculations of constant

termis of Eisenstein series along parabolic subgroups), representation theory (they aid to achieve the spectral decomposition of the space of L^2 functions), number theory, arithmetic geometry (aritmethically speaking, the p-divisibility of its coefficients helps in the construction of p-adic L-functions), etc. [9]. Eisenstein series are also helpful in proving analytic continuation and functional equations for L-functions. For example, the Siegel-Weil formula asserts that the Fourier coefficients of some Eisenstein series can be used to count the number of representations of a number by a quadratic form [10].

Up until now, Eisenstein series have provided many interesenting, seemingly unknown, connections. They have been studied since they show connections with crystals and lattice models, which are mathematical objects that first appeared in other context such as quantum groups and mathematical physics [11], an exploration which is just beginning.

While there are many applications, in this work we will focus in computing Fourier coefficients and Hecke eigenvalues of modular forms. This topic has been of interest especially because of the relations between the number of solutions on an elliptic curve modulo p and the coefficients of the modular form associated to that curve. A very important result for modular forms, that we will explain later, is that there exist modular forms that are eigenforms of the Hecke operators; furthermore, for these modular forms, the Fourier coefficients and Hecke eigenvalues agree. These eigenforms, suitably normalized, will be known as *newforms*. In this thesis we describe a new method to compute Hecke eigenvalues of eigenforms, as well as an implementation of the method.

As a motivation, consider the Ramanujan τ-function given by

$$\sum_{n\geq 1} \tau(n)q^n = q\prod_{n\geq 1}(1-q^n)^{24} = \Delta(z)$$

where $q = 2\pi iz$ and $\Im(z) > 0$; $\Delta(z)$ is the unique modular cusp form of level 1

and weight 12. In 1947 Lehmer conjectured [12] that the Fourier coefficients of $\Delta(z)$ never vanish. Since we mentioned that the Fourier coefficients of $\Delta(z)$ are also its Hecke eigenvalues, one of the oldest unsolved conjectures about modular forms can be studied by computing the Hecke eigenvalues of a modular form.

The usual way to compute Hecke eigenvalues is by the method of modular symbols implemented in Sage [13] and MAGMA [14], which will be briefly explained in section 3.1. One advantage of using modular symbols is that the method can be applied for a modular form of any given level and weight. However, one disadvantage is that, as the dimension of the space of modular forms increases, the linear algebra required for the computation of Hecke eigenvalues becomes difficult and inefficient. Recently, Wuthrich [15] proposed the computation of modular symbols which is faster for large level compared to traditional methods of computing modular symbols. Also recently, PARI/GP [16] has started to include methods to compute Hecke eigenvalues based on trace formulas [17].

A significant breakthrough appeared in the second half of the last decade with the work of Couveignes and Edixhoven and their collaborators [18]. Their main result is an algorithm that computes the Galois representation over a finite field attached to a modular eigenform of level one in time polynomial in the logarithm of the cardinality of the finite field. One can therefore compute the coefficients of such eigenforms (in characteristic zero) via a multimodular algorithm. Unfortunately, we are not aware of any implementations of this algorithm that are available for public use.

In this dissertation we propose another way to compute Hecke eigenvalues, one whose idea is relatively simple. For f a newform, if we apply a Hecke operator T_p on f with eigenvalue λ_p we get that $T_p f = \lambda_p f$. In other words, if we could evaluate $T_p f$ and f at some fixed point z_0 in the complex upper half-plane $\mathbb{H}$ at which f does not vanish, then

$$\lambda_p = \frac{T_p f(z_0)}{f(z_0)}.$$

One clear drawback to our proposed method is that we only get a numerical approximation to λ_p. However, this drawback is not too problematic. For example, in numerical experiments on $L(f, s)$, the L-function associated to f, we only need numerical approximations to the Dirichlet series coefficients (which are determined by the Hecke eigenvalues of f). If an exact representation of the Hecke eigenvalue is required, since the number field in which the Hecke eigenvalue lives is known, one can use LLL to find the Hecke eigenvalue exactly. The advantages of our method are that it allows us to compute some Hecke eigenvalues more quickly than using the traditional approach and that it can easily be made parallel.

In this dissertation we will focus on the special case of a level 1 eigenform f, we investigate a variant of the analytic evaluation method that writes any eigenform f of level 1 as an explicit polynomial in the Eisenstein series E_4 and E_6, and evaluates these Eisenstein series at relevant points as described above. The advantage of using this approach is that the Fourier expansions of Eisenstein series are easy to compute and there also exist computational packages such as ARB that will allow for the optimized evaluation of E_4 and E_6 [8], [19].

CHAPTER II
MATHEMATICAL BACKGROUND

2.1 Modular Forms

To get a better understanding of modular forms we will first define some concepts that will be used. We define the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ and the group

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc = 1 \right\}.$$

$\mathrm{SL}_2(\mathbb{R})$ acts on the upper half plane by linear fractional transformations of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d} \tag{2}$$

for $\tau \in \mathbb{H}$, it sends points in the upper half plane to points in the upper half plane. This can be seen from the simple equation,

$$Im\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{(ad - bc)Im(\tau)}{|c\tau + d|^2}$$

Since we know that $ad - bc = 1$ and $Im(\tau) > 0$ we see that $\frac{a\tau+b}{c\tau+d} \in \mathbb{H}$. For modular forms we are particularly interested in the group $SL_2(\mathbb{Z})$ which is defined just like $\mathrm{SL}_2(\mathbb{R})$

but with the entries now in $\mathbb{Z}$. We also define the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ to be,

$$\mathcal{F} = \left\{ z \in \mathbb{H} : |\Re(z)| \leq \tfrac{1}{2} \text{ and } |z| \geq 1 \right\}.$$

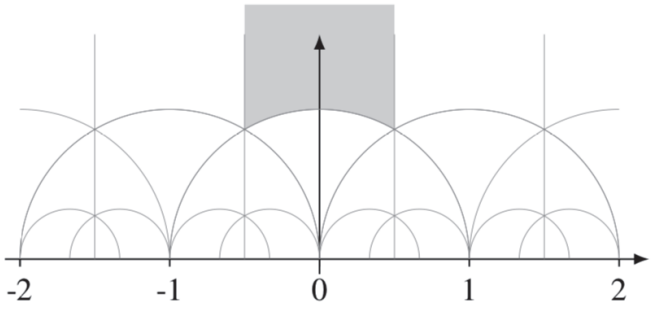

Figura 1: Fundamental domain for $SL_2(\mathbb{Z})$ [20]

Observe that $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$, in fact these two matrices are very important in our study because the group $SL_2(\mathbb{Z})$ is generated by the matrices T and S [1]. We will prove this result,

Lemma 1. *$SL_2(\mathbb{Z})$ is generated by the matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$*

Proof. First observe that $S^2 = -I$ and $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $G =< S, T >$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by S and T. Suppose without loss of generality that $c \neq 0$, and that $|a| \geq |c|$. By the division algorithm, $a = qc + r$ with $0 \leq r < |c|$. So, $T^{-q}A$ has $a - qc = r$ as its entry a_{11}. Now, mutiplication by S switches rows with a minus sign to the first row and now the entries $a_{11} = -c$ and $a_{21} = r$, we repeat this process again until we will get eventually that $a_{21} = 0$ and our matrix will have the form $A' = \begin{pmatrix} \pm 1 & m \\ 0 & \pm 1 \end{pmatrix}$, since $A \in \mathrm{SL}_2(\mathbb{Z})$. This matrix A' has to be $\pm T^m$ for some $m \in \mathbb{N}$. So, $\exists B \in G$ such that $BA = \pm T^m$ for some integer n. Since $T^n \in G$ and $S^2 = -I$ we have that $A = \pm B^{-1} T^n$, and the proof is complete. □

To illustrate the proof let us consider $A = \begin{pmatrix} 11 & 8 \\ 4 & 3 \end{pmatrix}$, we will express it in terms of S and T. Since $11 = 2 \cdot 4 + 3$, we have

$$T^{-2}A = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$$

Now, we multiply by S,

$$ST^{-2}A = \begin{pmatrix} -4 & -3 \\ 3 & 2 \end{pmatrix}$$

Since $-4 = (-2) \cdot 3 + 2$ we multiply by T^2,

$$T^2ST^{-2}A = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$$

Once again, we multiply by S to switch rows,

$$ST^2ST^{-2}A = \begin{pmatrix} -3 & -2 \\ 2 & 1 \end{pmatrix}$$

Now since $-3 = (-2) \cdot 2 + 1$ we multiply by T^2,

$$T^2ST^2ST^{-2}A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Switching rows,

$$ST^2ST^2ST^{-2}A = \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix}$$

We have that $-2 = (-2) \cdot 1 + 0$ and we have that,

$$T^2ST^2ST^2ST^{-2}A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

With our final switch of rows we have that

$$ST^2ST^2ST^2ST^{-2}A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I = S^2$$

Solving for A we finally arrive to,

$$A = T^2S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}S^2$$

Given that $S^{-1} = -S$ we get that,

$$A = -T^2ST^{-2}ST^{-2}ST^{-2}S$$

And thus, with this algorithm we are able to write any matrix in $\mathrm{SL}_2(\mathbb{Z})$ as a product of powers of T and S. Another important property about the action of $\mathrm{SL}_2(\mathbb{Z})$ is associativity, for $A, B \in \mathrm{SL}_2(\mathbb{Z})$ we have that

$$(AB)(\tau) = A(B(\tau)).$$

So that $f((AB)(\tau)) = f(A(B(\tau)))$. We will first state the definition of modular forms of level 1 and then we will generalize this idea to modular forms of higher levels.

Definition 1. A meromorphic function f on $\mathbb{H}$ is called a weakly modular function of weight $k \in \mathbb{Z}$ if for all $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and all $\tau \in \mathbb{H}$ we have that,

$$f(\tau) = (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right)$$

We will explain this condition when we define a modular function of any level and weight.

We now turn our attention to when $\tau \in \mathbb{H}$ tends to ∞, we want our function to be well behaved when this happens,

Definition 2. A modular function f of weight k is a weakly modular function of weight k that is meromorphic at ∞.

And now we define a modular function of weight k and level 1,

Definition 3. A modular form of weigth k and level 1 is a modular function of weight k that is holomorphic on all $\mathbb{H}$ and ∞.

Now, we extend this definitions and we define a modular form for any level N and weight k. First of all, let us examine the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 4. A congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is any subgroup that contains

$$\Gamma(N) = ker\left(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2\left(\mathbb{Z}/N\mathbb{Z}\right)\right)$$

for some positive N. The smallest such N is called the level of Γ.

The most important congruence subgroup is:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Now, we can safely define a modular form of weight k and level N to be the following.

Definition 5. A modular form of level N and weight k is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying the following:

- Modularity condition

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \tag{3}$$

  for all elements $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\Gamma_0(N)$ and all $\tau \in \mathbb{H}$.

- The function $f(\tau)$ is bounded as $Im(\tau)$ approaches infinity.

The space of all modular forms of weight k and level N is denoted $M_k(N)$.

One might find (3) particularly unmotivated since the factor $(c\tau + d)^k$ seems to appear from nowhere. However, we will show that it is actually natural to include it in the definition of a modular form once we recall our discussion in the Introduction about how modular forms arise from functions invariant over lattices $\Lambda \in \mathbb{C}$. Since we saw that the modularity condition implies that $f(\tau + 1) = f(\tau)$, we see that knowing the value of f in a strip of width 1 will give us the value of the function at any point in the upper half plane, that is why we only care about lattices of the form $\mathbb{Z} + \tau\mathbb{Z}$ and its multiples. Consider the equation

$$F(\lambda\Lambda) = -\lambda^k F(\Lambda)$$

and the lattices previously defined. We consider a lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$ and define a new function $F(\omega_1, \omega_2) = F\left(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\right)$, what we need is that,

$$F(\lambda\omega_1, \lambda\omega_2) = -\lambda^k F(\omega_1, \omega_2)$$

Now, it is known that two pair of complex numbers (ω_1, ω_2) and $(\omega_1^{'}, \omega_2^{'})$ generate the same lattice if $(\omega_1, \omega_2) = (a\omega_1^{'} + b, c\omega_2^{'} + d)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. This is precisely the action of $\mathrm{SL}_2(\mathbb{Z})$ in the upper-half plane. That is why we can only consider how the functions behaves in the lattice $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ where $\tau \in \mathbb{H}$, we can then define a function $f(\tau) = F(\Lambda)$ and for a general lattice we get that

$$\begin{aligned} F\left(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\right) &= F\left((\omega_2)\,\mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}\right) \\ &= (\omega_2)^{-k} F\left(\mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}\right) \end{aligned}$$

Now,

$$\begin{aligned} f\left(\tau\right) &= F\left(\mathbb{Z}\tau + \mathbb{Z}\right) \\ &= F\left(\mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d)\right) \\ &= (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right) \end{aligned}$$

This is the modularity condition.

Also, if we apply (2) to T and S we see the the action of these matrices are simply transformations that are equivalent to translation by a unit, $T(\tau) = \tau + 1$ and inversion of unit cirle plus a reflection on the real axis, $S(\tau) = -\frac{1}{\tau}$. However, also observe that $P = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2$ and so,

$$P(\tau) = (-1)^k P(\tau)$$

this simple equations shows that any modular forms of weight k, when k is odd, has to be the 0 function, one can check the zero function is in fact a modular form of any weight.

One of the conditions of modular functions can be reestated as follows, an entire modular form contains no-negative powers of x in its Laurent expansion. It is analytic everywhere and at $i\infty$ [21]. Since we saw that every modular function is holomorphic and satisfies the modularity condition, they admit a Fourier expansion that has to be of the form

$$f(q) = \sum_{n=0}^{\infty} a_n q^n, \tag{4}$$

where $q = exp(2\pi i\tau)$. Equation (4) is usually called the *q-expansion of* f. This representation of modular forms allow us to manipulate them more easily and it also let us define one kind of modular forms that we are particularly interested, cusp forms.

Definition 6. A cusp form of weight k and level N is a modular form f of weight k and level N that vanishes at the cusps. In other words, f is a cusp form if its Fourier expansion has constant term equal to 0: $f(q) = \sum_{n=1}^{\infty} a_n q^n$. We denote the space of all cusp forms of weight k and level N by $S_k(N)$.

2.2 Algebraic structure of $M_k(1)$ and $S_k(1)$

One of the reasons modular forms are so studied is because the space consisting of all modular forms of a given level and weight forms a vector space over $\mathbb{C}$. In fact, we define the operations in $M_k(1)$ as $(f+g)(\tau) = f(\tau)+g(\tau)$ and $(fg)(\tau) = f(\tau)g(\tau)$. In particular, consider two modular forms f and g of weight k and level 1. We know that the sum of two holomorphic functions is holomorphic, also, observe that,

$$\begin{aligned}(f+g)(\tau) &= f(\tau) + (g\tau) \\ &= (cz+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)(cz+d)^{-k} d\left(\frac{a\tau+b}{c\tau+d}\right) \\ &= (cz+d)^{-k}(f+g)\left(\frac{a\tau+b}{c\tau+d}\right)\end{aligned}$$

So that $f+g$ satisfies the modularity condition and $f+g$ is bounded as $\tau \to i\infty$ since both f and g are bounded. This shows that $f+g$ is also a modular form of weight k. Now let $f \in M_k(1)$ and $g \in M_l(1)$, and consider the following,

$$\begin{aligned}(fg)(\tau) &= f(\tau)(g\tau) \\ &= (cz+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)(cz+d)^{-l} d\left(\frac{a\tau+b}{c\tau+d}\right) \\ &= (cz+d)^{-(k+l)}(fg)\left(\frac{a\tau+b}{c\tau+d}\right)\end{aligned}$$

By similar reasons fg is holomorphic in $\mathbb{H}$ and $fg(\tau)$ is bounded at the cusps. This shows that fg is a modular form of weight $k+l$. Similar calculations also show that for $g \neq 0$, $\frac{f}{g}$ is a modular form of weight $k-l$.

It is also easy to see that $S_k(1)$ is a subspace of $M_k(1)$.

2.3 Modular forms of Level 1

We will now focus our attention to the structure of modular forms of level 1, i.e., modular forms on $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1) = \Gamma_1(1)$. First, we examine the first non-trivial example of a modular form.

2.3.1 Examples of Modular forms

Perhaps the most common non-trivial example of a modular form are Eisenstein series, as we saw that there are no nonzero modular forms of odd weight. We have the following proposition.

Proposition 1. *For even $k \geq 4$, the non-normalized weight k Eisenstein series is the function given by*

$$G_k(\tau) = \sum_{\substack{(m,n)\in\mathbb{Z}, \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^k}.$$

The function $G_k(\tau)$ is a modular form of weight k.

Proof. For a proof of the fact that $G_k(\tau)$ is an holomorphic function on $\mathbb{H}$ see [22, Chapter 7. Section 2.3]. It is also shown in [23, Section 1.4] that for $k \geq 4$, $G_k(\tau)$ is absolutely convergent. Now, what it is left for us to show is that $G_k(\tau+1) = G_k(\tau)$, $G_k\left(\frac{-1}{\tau}\right) = \tau^k G_k(\tau)$ and that $G_k(\tau)$ is bounded as $Im(\tau)$ approaches infinity. First observe that

$$\begin{aligned} G_k(\tau+1) &= \sum_{\substack{(m,n)\in\mathbb{Z}, \\ (m,n)\neq(0,0)}} \frac{1}{(m(\tau+1)+n)^k} \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}, \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+m+n)^k} \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}, \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+(m+n)^k}. \end{aligned}$$

Since (m,n) runs through all $\mathbb{Z}\setminus\{0,0\}$ then so does $(m,m+n)$ and we can rearrange this last terms because $G_k(\tau)$ is absolutely convergent. Thus,

$$G_k(\tau+1)=G_k(\tau).$$

Now also observe that,

$$\begin{aligned}G_k\left(\frac{-1}{\tau}\right)&=\sum_{\substack{(m,n)\in\mathbb{Z},\\(m,n)\neq(0,0)}}\frac{1}{\left(-\frac{m}{\tau}+n\right)^k}\\&=\sum_{\substack{(m,n)\in\mathbb{Z},\\(m,n)\neq(0,0)}}\frac{\tau^k}{\left(-m+n\tau\right)^k}\\&=\tau^k\sum_{\substack{(m,n)\in\mathbb{Z},\\(m,n)\neq(0,0)}}\frac{1}{\left(-m+n\tau\right)^k}.\end{aligned}$$

Similarly $(-m,n)$ also runs through all $\mathbb{Z}\setminus\{0,0\}$ and we can rearrange the terms and we get that,

$$G_k\left(\frac{-1}{\tau}\right)=\tau^kG_k(\tau).$$

Now, observe that if $\mathrm{Im}(\tau)\to\infty$ then

$$G_k\left(\tau\right)=\sum_{n\neq0}\frac{1}{n^k}+\sum_{m\neq0}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^k}=2\sum_{n\geq1}\frac{1}{n^k}+2\sum_{m\geq1}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^k},$$

every term in the sum $\frac{1}{(m\tau+n)^k}$ goes to 0 as τ goes to ∞. Thus,

$$\lim_{Im(\tau)\to\infty} G_k(\tau) = 2\sum_{n\geq 1}\frac{1}{n^k} < \infty$$

which proves that Eisenstein Series are in fact modular forms of weight k. □

This is the first example of a modular form and it also shows an important fact we previously discused about Eisenstein Series, when $\tau \to \infty$ we see that the Eisenstein Series tends to $2\sum_{n\geq 1}\frac{1}{n^k}$, we actually have that this sum equals to $2\zeta(k)$, where $\zeta(k)$ is the famous Riemann Zeta function.

Since Eisenstein series are modular forms we can think about their Fourier expansion, but first, we introduce an important function that will appear in this Fourier expansion,

Definition 7. For an integer $t \geq 0$ and a positive integer n, we define the sum of divisors function as,

$$\sigma_t(n) = \sum_{1\leq d|n} d^t.$$

In other words, $\sigma_t(n)$ is the sum of the t-th powers of positive divisors of n.

Now, we determine the Fourier expansion of an Eisenstein series.

Proposition 2. *For even $k \geq 4$ we have,*

$$G_k(\tau) = 2\zeta(k) + 2\cdot\frac{(2\pi i)^k}{(k-1)!}\sum_{n=0}^{\infty}\sigma_{k-1}(n)q^n$$

Proof. This proof can be found at [23, Theorem 1.4.6]. It can be shown that,

$$\frac{1}{\tau} + \sum_{d=1}^{\infty}\left(\frac{1}{\tau-d} + \frac{1}{\tau+d}\right) = \pi\cot(\pi\tau) = \pi i - 2\pi i\sum_{m=0}^{\infty} q^m \tag{5}$$

Then we will first prove that $\sum_{d\in\mathbb{Z}} \frac{1}{(\tau+d)^k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1}q^n$. Differentiating both sides of (5) with respect to τ we get that,

$$-\frac{1}{\tau^2} + \sum_{d=1}^{\infty}\left(\frac{-1}{(\tau-d)^2} + \frac{-1}{(\tau+d)^2}\right) = -(2\pi i)^2\sum_{d=1}^{\infty} dq^d$$

The series on the left hand side converges absolutely and therefore,

$$\sum_{d\in\mathbb{Z}} \frac{1}{(\tau+d)^2} = (2\pi i)^2\sum_{d=1}^{\infty} dq^d.$$

This proves the equation for $k = 2$, the general identity follows by induction by differentiating (5) $k-1$ times. Now we prove the general result we were after, we see that

$$G_k(\tau) = \sum_{n\neq 0}\frac{1}{n^k} + \sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^k} = 2\zeta(k) + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^k}$$

Using the identity we previously proved replacing m by mz we get that,

$$G_k(\tau) = 2\zeta(k) + 2\sum_{m=1}^{\infty}\left(\frac{(-2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty} d^{k-1}q^{dm}\right) = 2\zeta(k) + \frac{2(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{dm}$$

We know group the pairs in the inner sum that contribute to q^n, i.e., we are looking for the divisors of n, the pairs (m,d) such that $md = n$, thus using the sigma function we previusly defined we arrive to the result,

$$G_k(\tau) = 2\zeta(k) + 2\cdot\frac{(2\pi i)^k}{(k-1)!}\sum_{n=0}^{\infty}\sigma_{k-1}(n)q^n$$

□

However, we can still have another representation of this Fourier expansion once we introduce the Bernoulli numbers, this representation is useful in a computational point of view since Bernoulli numbers have a fast method of computation as implemented in Sage.

Definition 8. The Bernoulli number B_n for $n \geq 0$ is defined to be the number such that the following equality holds,

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$$

Expanding the power series one can get that the first values for B_n are

- $B_0 = 1$
- $B_1 = -\frac{1}{2}$
- $B_2 = \frac{1}{6}$
- $B_3 = 0$
- $B_4 = -\frac{1}{30}$
- $B_5 = 0$
- $B_6 = \frac{1}{42}$

Notice that the Bernoulli numbers with odd $n > 1$ are 0. Another interesting property about the Bernoulli numbers is that they give the value of the Riemann zeta function for positive even integers,

Proposition 3. *If $k \geq 2$ is an even integer,*

$$\zeta(k) = -\frac{(2\pi i)^k}{2k!} B_k$$

Proof. The proof can be found at [22, Chapter 7, section 4, prop 7]. Replacing $x = 2i\tau$ in the definition of the Bernoulli numbers we get that

$$\tau \cot(\tau) = 1 - \sum_{k=1}^{\infty} B_k \frac{2^k \tau^k}{k!}$$

Taking the logarithmic derivative of

$$\sin\tau = \tau \prod_{n=1}^{\infty} \left(1 - \frac{\tau^2}{n^2\pi^2}\right)$$

we get that,

$$\tau\cot(\tau) = 1 + 2\sum_{n=1}^{\infty} \frac{\tau^2}{\tau^2 - n^2\pi^2} = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \frac{\tau^{2k}}{n^{2k}\pi^{2k}}$$

Since,

$$1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \frac{\tau^{2k}}{n^{2k}\pi^{2k}} = 1 - \sum_{k=1}^{\infty} B_k \frac{2^k\tau^k}{k!}$$

we get the desired result. □

Often, it will be convenient to express a function in its Fourier expansion as a normalized series, i.e, with the coefficient of q equal 1. Therefore, we are able to introduce the normalized Eisenstein series as follows,

Definition 9. The normalized Eisenstein Series of even weight $k \geq 4$ is

$$\begin{aligned} E_k &= \frac{(k-1)!}{2\cdot(2\pi i)^k} G_k \\ &= -\frac{B_k}{2} + q + \sum_{n=2}^{\infty} \sigma_{k-1}(n) q^n \end{aligned}$$

Among other reasons, we want to use normalized series is that the eigenvalue of the n-th Hecke operator is the coefficient of q^n, as we will see later on.

As we have seen, Eisenstein series constitute the first example of a non-trivial modular form; however, cusp forms are also an object of study in this work and we will use eisenstein series to define a very important cusp form,

Theorem 1. *Delta (Δ) is a cusp of weight 12 defined by,*

$$\Delta = \frac{D}{(2\pi)^{12}},$$

where $D(z) = (60G_4(z))^3 - 27(140G_6(z))^2$. *Its q-expansion is given by,*

$$\Delta = q \cdot \prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Observe that $60G_4(i\infty) = 120\zeta(4)$ and that $140G_6(i\infty) = 280\zeta(6)$, then we get that,

$$60G_4(i\infty) = \frac{4}{3}\pi^4, 140G_6(i\infty) = \frac{8}{27}\pi^6$$

Therefore,

$$\Delta(i\infty) = \left(\frac{4}{3}\pi^4\right)^3 - 27\left(\frac{8}{27}\pi^6\right)^2 = 0,$$

which tells us indeed that Δ is a cusp form of level 12.

In [22, Chapter 7. Section 2], the author gives an explanation with lattices for where the discriminant D comes from. Let Γ be a lattice of $\mathbb{C}$, and let,

$$\vartheta_\Gamma(u) = \frac{1}{u^2} + \sum_{\gamma\in\Gamma}{}' \left(\frac{1}{(u-\gamma)^2} - \frac{1}{\gamma^2}\right)$$

be the corresponding Weierstrass function, in the Laurent expansion of $\vartheta_\Gamma(u)$ we will find Eisenstein series,

$$\vartheta_\Gamma(u) = \frac{1}{u^2} + \sum_{2}^{\infty}(2k-1)\,G_k(\Gamma)u^{2k-2}.$$

This function satisfies the differential equation $(f')^2 = 4f^3 - g_2 f - g_3$ and so, if we let $y = \vartheta'_\Gamma(u)$ and $x = \vartheta_\Gamma(u)$ we have that,

$$y^2 = 4x^3 - g_2 x - g_3,$$

where $g_2 = 60G_4(z)$ and $g_3 = 140G_6(z)$. So, up to some constant, Δ is in fact the discriminant of the polynomial $4x^3 - g_2 x - g_3$ which ends up showing one of the important properties that Δ possess: it never vanishes for points on the upper-half plane.

Among other properties of Δ we can find that its Fourier series also involves the Ramanujan τ function and it is given by

$$\Delta(z) = \sum_{n \geq 1} \tau(n) q^n,$$

Δ is perhaps one of the most important modular forms of level 1 and it is especially useful since we will prove that multiplication by Delta establishes an isomorphism between cusp forms and modular forms.

One of the reasons modular forms have been studied as much as they have is because of the structure they possess, especially when we are considering modular forms of level 1 like we are. We first define the $ord_w(f)$ to be the largest integer n such that $\frac{f(z)}{(w-z)^n}$ is holomorphic at w when f is a meromorphic function in $\mathbb{H}$. Observe that $ord_\infty(f)$ is the smallest positive integer for which the power of q in th q-expansion of f has a non-zero coefficient, i.e., $ord_\infty(f) = a_0$ if $f(\tau) = \sum_{n \geq a_0} a_n q^n$. Now, let $\rho = e^{\frac{2\pi i}{3}}$. Then we state the following theorem,

Theorem 2. *Valence Formula: Let k be any integer and suppose $f \in M_k(1)$ is nonzero.*

Then,

$$ord_\infty(f) + \frac{1}{2}ord_i(f) + \frac{1}{3}ord_\rho(f) + \sum_{w \in \mathcal{F}} ord_w(f) = \frac{k}{12} \tag{6}$$

where the sum ranges for the elements of $\mathcal{F}$ other than i and ρ.

Proof. The proof can be found in [22, Chapter 7. Section 3. Theorem 3]. □

Remember that $M_k(N)$ and $S_k(N)$ are the space of modular forms of weight k and level N and the space of cusp forms of level k and level N respectively. For ease of notation let $M_k := M_k(1)$ and $S_k := S_k(1)$. We now have the tools to prove the following theorem.

Theorem 3. *Multiplication by Δ defines an isomorphism between M_{k-12} and S_k*

Proof. The proof can be found in [4, Chapter 2. Theorem 2.14]. We know that Δ is never zero, so the holomorphy of Δ implies that multiplication by Δ establishes an injective map from $M_{k-12} \to S_k$. We only need to show that this map is also surjective, to do this consider a cusp form $f \in S_k$, we will prove that $\frac{f}{\Delta}$ is a modular form of level $k-12$. Define $g = \frac{f}{\Delta}$, g is holomorphic in $\mathbb{H}$ since Δ never vanishes and it is bounded as $\mathrm{Im}(\tau) \to \infty$ because

$$ord_\infty(g) = ord_\infty(f) - ord_\infty(\Delta) = ord_\infty(f) - 1 \geq 0.$$

We used the fact that $ord_\infty(\Delta) = 1$ but one can see this clearly from the q-expansion of Δ. We also used that $ord_\infty(f) \geq 1$ since f is a cuspform and it does not have a constant term. In section 2.2 one can see that the quotient of two modular forms of weight k and l respectively satisfy the modularity condition for $k - l$. This completes the proof. □

We have that the space of modular forms can be written as a direct sum of the space of cusp forms and the Eisenstein series. We state the following theorem,

Theorem 4. *If $k \geq 4$ is even, then $M_k = S_k \bigoplus \mathbb{C}G_k$.*

Proof. Let $f(\tau) \in M_k$ and consider $h(\tau) = f(\tau) - f(i\infty)\frac{G_k(\tau)}{G_k(i\infty)}$. It is well defined since $G_k(i\infty) \neq 0$. Now, observe that

$$h(i\infty) = f(i\infty) - f(i\infty)\frac{G_k(i\infty)}{G_k(i\infty)} = 0$$

This proves that $h \in S_k$. We have shown that any modular form of weight k can be written as the sum of a cusp form and a multiple of $G_k(\tau)$; which completes the proof. □

All the results we are stating are important since we want to arrive to the fact that the space of modular forms M_k is a vector space over $\mathbb{C}$, but most importantly, we want to show that its dimension is finite. If we can do this, we would like to find a basis for this space and carry on the evaluations of a modular form f expressed as a linear combination of the basis elements. We will show how strong the Valence Formula is when studying the dimension of the spaces of modular forms,

Lemma 2. *The dimension of M_k is zero for $k < 0$ and $k = 2$; furthermore, $S_k = 0$ for $k < 12$.*

Proof. Observe that the left-hand side of (6) is non-negative, thus the right-hand side must be non-negative as well and $k \geq 0$. If $k = 2$ we see that the right hand side is $\frac{1}{6}$, yet the left-hand side contains non-negative multiples of 1, $\frac{1}{2}$ and $\frac{1}{3}$ which makes the sum too big, so $k \neq 2$. The second part of the theorem is just a corollary of theorem 3 since $M_{k-12} \cong S_k$ we see that the dimensions agree, so $M_k = 0$ for $k < 0$ imply that $S_k = 0$ for $k < 12$. □

Now that we have used the Valence formula to take care of the cases $k < 0, k = 2$ for the space M_k, we are in position to show one of the important results of this section,

Theorem 5. *If $k < 0$ or k is odd, $M_k = 0$. For even $k \geq 2$, we have that,*

$$\dim(M_k) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor & \text{if } k \equiv 2 \pmod{12} \\ 1 + \left\lfloor \frac{k}{12} \right\rfloor & \text{if } k \not\equiv 2 \pmod{12} \end{cases} \tag{7}$$

Proof. For $k < 12$ using Theorem (3), observe that

$$\dim(M_k) = 1 + \dim(S_k) = 1 + \dim(M_{k-12}) = 1 + 0 = 1$$

. So, for $k = 0, 4, 6, 8, 10$ we have that $\dim(M_k) = 1$. Now, using again Theorem (3) we get that

$$\dim(M_k) = 1 + \dim(S_k) = 1 + \dim(M_{k-12})$$

Thus we see that when k is replaced by $k+12$ the dimension of M_k increases by 1, and the theorem is proved. □

This theorem tells us for instance that for $k = 0, 4, 6, 8, 10$ the space M_k has dimension 1 over $\mathbb{C}$. Also, the theorem tell us that $\dim(M_{38}) = \left\lfloor \frac{38}{12} \right\rfloor = 3$ and that $\dim(M_{42}) = 1 + \left\lfloor \frac{42}{12} \right\rfloor = 4$.

Now that we have proved that the space of modular forms is finite-dimensional, the right question to ask next should be about its basis. Is there an explicit basis for M_k? If so, how can we find a basis for M_k? If we were able to do this, as we have said before, we would be able to express any modular form as a linear combination of its basis, and we hope that it might be composed with elements that are more computationally accesible. The next theorem shows that all the things we discussed in this paragraph are true.

Theorem 6. *The space M_k has as basis the modular forms $E_4^a E_6^b$ where a,b run over all non-negative integers such that $4a + 6b = k$*

Proof. This proof uses [4, Chapter 2. Theorem 2.17] and [23, Corollary 1.6.10]. We will prove this result by induction. Fix an even integer k. We see that for $k \leq 10, k = 14$ for which $\dim(M_k) = 1$ the bases are 1,E_4,E_6,E_8,E_{10} and E_{14} respectively. Now choose $a, b \in \mathbb{Z}^+$ such that $4a + 6b = k$, then define $g = E_4^a E_6^b$, we see that g is not a cusp form since $g(\infty) \neq 0$. Now let $f \in M_k$ be such that $\exists \alpha \in \mathbb{C}$ so that $f - \alpha g \in S_k$. Thus, by Theorem 3 $\exists h \in M_{k-12}$ such that $f - \alpha g = h\Delta$, by our inductive hypothesis, h is a polynomial in E_4 and E_6 and so is Δ, since $\Delta = \frac{E_6^2 - E_4^3}{1728}$, and therefore, so is f. We have proved that $\left\{E_4^a E_6^b | (a, b) \geq 0, 4a + 6b = k\right\}$ spans M_k. All that is left to prove is that the polynomials are in fact linearly independent. We will also use induction on steps of 12, we want to show that the number of the monomials $E_4^a E_6^b$ that satisfy the condition agree with the dimension of M_k. For $k \leq 14$ calculations are straightforward. Now assume that $k > 14$, for each monomial $E_4^a E_6^b$ of weight $k - 12$ there exists one $E_4^a E_6^{b+2}$ of weight k. All those monomials are obtained in that way except those that are of the form E_4^a or $E_4^a E_6$. When $k \equiv 0 \pmod 4$ then $E_4^{k/4}$ is of weight k and when $k \equiv 2 \pmod 4$ then $E_4^{(k-6)/2} E_6$ is of weight k, in either case there is exactly one more monomial of weight k than there are of weight $k - 12$. This completes the proof. □

For instance, $\dim(M_{32}) = 3$ and we see that $2 \cdot 4 + 4 \cdot 6 = 32$, $5 \cdot 4 + 2 \cdot 6 = 32$ and $8 \cdot 4 = 32$, so $\{E_4^2 E_6^4, E_4^5 E_6^2, E_4^8\}$ is a basis for M_{32}. This theorem plays an essential role in the algorithm that we describe since expressing every modular form as a combination of Eisenstein series, whose coefficients are well known, will make the computations a lot easier.

As a result of these theorems we can state the following proposition.

Proposition 4. *$\mathbb{A} := \bigoplus_{k=0}^{\infty} M_k$ defines a graded $\mathbb{C}$-algebra and $\mathbb{A} \cong \mathbb{C}[x, y]$*

Proof. The fact that $\mathbb{A}$ is an algebra is easily checked, now Theorems 5 and 6 establish that the following map,

$$\pi : \mathbb{C}[x, y] \to \mathbb{A}$$

is an algebra isomorphism. This map sends x to E_4 and y to E_6, in that way we can identify elements in $\mathbb{A}$ as polynomials in E_4 and E_6. □

2.4 Hecke operators

Now that we have discussed the structure of the space of modular forms, we are particularly interested in a special type of modular forms known as newforms. But first, we have to introduce some other concepts. Hecke determined all entire modular forms with multiplicative coefficients by introducing a sequence of linear operators T_n, known as Hecke operators, which map M_k onto itself [21]. For a fixed k and $n = 1, 2, 3, \ldots$, the action of T_n on f is defined as,

$$(T_n f)(\tau) = n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{n\tau + bd}{d^2}\right). \tag{8}$$

If $n = p$ we see that the sum only contains two terms and (8) turns into

$$(T_p f)(\tau) = p^{k-1} f(p\tau) + \frac{1}{p} \sum_{b=0}^{p-1} f\left(\frac{\tau + b}{p}\right).$$

Among the intereseting properties of Hecke operators, we state the following proposition,

Proposition 5. *If $f \in M_k$ and has a Fourier expansion*

$$f(\tau) = \sum_{m=0}^{\infty} c(m) q^{2\pi i m \tau}$$

then $T_n f$ has a Fourier expansion

$$(T_n f)(\tau) = \sum_{m=0}^{\infty} b_n(m) q^{2\pi i m \tau}$$

where,

$$b_n(m) = \sum_{d|(n,m)} d^{k-1} c\left(\frac{mn}{d^2}\right)$$

Proof. For a proof of this fact refer to [21, Theorem 6.6]. □

Another very important fact about Hecke operators is that, as we should have expected, it maps modular forms into modular forms and cusp forms into cusp forms.

Theorem 7. *If $f \in M_k$, then $T_n f \in M_k$. Furthermore, if $f \in S_k$, then $T_n f \in S_k$.*

Proof. If $f \in M_k$ the definition of T_n shows that $T_n f$ is analytic everywhere on $\mathbb{H}$. Proposition 5 shows that $T_n f$ has the required q-form and that it is bound when $\mathrm{Im}(\tau) \to \infty$. For the second part of the theorem, Proposition 5 shows that $T_n f$ for $f \in S_k$ also vanishes at the cusp. To see a proof that $T_n f$ satisfies the modularity condition one can see [21, Chapter 6. Theorem 6.11]. □

Finally, we would like to have that Hecke operators are multiplicative and how we could decompose the operator T_n when we have p^n for some prime p. This is summarized in the following proposition.

Proposition 6. *On weight k modular functions we have that,*

$$T_{mn} = T_m T_n$$

if $gcd(m, n) = 1$ and that for p prime,

$$T_{p^n} = T_{p^{n-1}} T_p - p^{k-1} T_{p^{n-2}}$$

Now that we have defined the action of Hecke operators on a modular form, we can now turn our attention to a very particular kind of modular form. We are interested in

cuspforms, specifically in those that are Hecke eigenforms. Among Hecke eigenforms, we are particularly interested in newforms:

Definition 10. If $d_1 d_2 = N$ and $f \in M_k(d_1)$, then we also have $f \in M_k(N)$ and also $g(z) = f(d_2 z) \in M_k(N)$. The subspace of $S_k(N)$ spanned by the forms obtained in one of these ways are the old forms and the orthogonal complement, with respect to the Peterson inner product, of the oldforms are the newforms, denoted by $S_k(N)^{new}$.

Where the Peterson inner product comes given by,

Definition 11. Let f and g be two cuspforms of weight $2k, k > 0$.

$$\langle f, g \rangle = \int_F f(\tau)\overline{g(\tau)} y^{2k-2} dx dy.$$

Where $\tau = x + iy$ and F is the fundamental domain.

Another definition for newform might make more sense regarding what we are working with,

Definition 12. A non zero modular form $f \in M_k(N)$ that is an eigenform for the Hecke operator T_n for all $n \in \mathbb{Z}$ is an Hecke eigenfrom or simple eigenform. The eigenform $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ is normalized when $a_1 = 1$. A newform is a normalized eigenform in $S_k(N)^{new}$ [1].

One might wonder why we care at all about eigenforms or newforms in particular. The answer is relatively simple and it is explained in [22]. Let $f(\tau) = \sum_{n=0}^{\infty} a(n) q^n$ be a modular form of weight k. Assume that f is an eigenform as defined above, i.e.,

$$(T_n f)(\tau) = \lambda_n f(\tau)$$

for all $n \geq 1$. We have the following theorem,

Theorem 8. *Let f be a newform and let the coefficient $a(1)$ of q in f be different than zero. If f is normalized by having $a(1) = 1$, then we have that*

$$a(n) = \lambda_n$$

for all $n > 1$.

The theorem tell us that the Hecke eigenvalues agree with the Fourier coefficients of newforms. This is one of the most important results that we use since when computing Hecke eigenvalues we are actually computing the Fourier coefficients of classical modular forms.

CHAPTER III
COMPUTATIONAL BACKGROUND

In the following chapter we will give a brief introduction to modular symbols 3.1, the method currently used by SAGE to calculate Hecke eigenvalues. In section 3.2 we explain the computational package Arb which we use to make the analytic evaluation of our modular forms.

3.1 Modular Symbols

We saw in the previous section that we could explicitly construct a basis for each space M_k of modular forms of level 1, consisting of elements of the form $E_4^a E_6^b$ where $4a + 6b = k$. However, this is not so easy in general. The existing algorithm for computing eigenvalues of Hecke operators uses the method of modular symbols, which we will explain here.

First of all, we define the set of all cusps to be $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. We can define an action of $SL_2(\mathbb{Z})$ on the set of cusps as,

$$z \to \frac{az + b}{cz + d}$$

and $z \to \infty$ if $z = -\frac{d}{c}$, i.e., we identify the cusp ∞ with the fraction $\frac{1}{0}$. We say that two cusps α, β are equivalent mód Γ_0 if $\exists A \in \Gamma_0 \subset SL_2(\mathbb{Z})$ such that $A\alpha = \beta$, where Γ_0 contains $\Gamma_0(N)$ for some N. We can use this cusps to construct a homology class, in particular, the homology class of any oriented path from α to β. We define

this homology class as $\{\alpha, \beta\}$. Since we are considering oriented paths, we see that $\{\alpha, \beta\} = -\{\beta, \alpha\}$.

For now, let us focus on modular symbols of weight 2. We can then define a perfect map from the product of cusp forms of level 2 with the homology class of modular symbols to $\mathbb{C}$ as follows,

$$S_2(\Gamma_0) \times H_1(X_{\Gamma_0}, \mathbb{Z}) \to \mathbb{C},$$

$$(f, \{\alpha, \beta\}) \to 2\pi i \int_\alpha^\beta f(z)dz :=< \{\alpha, \beta\}, f > . \tag{9}$$

Where $X_{\Gamma_0} = {}^{\Gamma_0}\!/_{\mathbb{H}}$ is a Riemann surface. Observe that (9) is independent of path since f is holomorphic. However, we do require that f vanish at the cusps. It can actually be shown that this construction works even if α and β are not equivalent mód Γ_0. What we have done is that we define the modular symbol $\{\alpha, \beta\}$ to be the homology class in $H_1(X_{\Gamma_0}, \mathbb{Z})$ of the path between α and β. Thus, modular symbols give a representation of $H_1(X_{\Gamma_0}, \mathbb{Z})$ in terms of paths between cusps.

We now state some important properties of modular symbols,

$$\{\alpha, \beta\} = -\{\beta, \alpha\} \qquad \{\alpha, \beta\} = \{\alpha, \gamma\} + \{\gamma, \beta\} \qquad \{\alpha, \beta\} = \{g\alpha, g\beta\} g \in \Gamma_0 \tag{10}$$
$$\{\alpha, g\alpha\} \in H_1(X_{\Gamma_0}, \mathbb{Z}) \qquad \{\alpha, g\alpha\} = \{\beta, g\beta\}$$

The last two conditions tell us that we can safely define the map

$$\Gamma_0 \to H_1\left(X_{\Gamma_0}, \mathbb{Z}\right)$$

$$g \to \{\alpha, g\alpha\}$$

and that this map is independent of α. With these results, Manin managed to prove that if α, β are cusps of Γ_0, then $\{\alpha, \beta\} \in H_1\left(X_\Gamma, \mathbb{Q}\right)$ [24].

Now, define $\mathcal{M}_2(\Gamma_0)$ to be the $\mathbb{Q}$-vector space generated by $\{\alpha, \beta\}$ modulo the first three conditions of (10). We define a left action on $\mathcal{M}_2$ such as $g \in \Gamma$. $g\{\alpha, \beta\} = \{g(\alpha), g(\beta)\}$. We can consider the natural canonical homomorphism,

$$\mathcal{M}_2(\Gamma_0) \to H_1\left(X_{\Gamma_0}, \partial X_{\Gamma_0}, \mathbb{Z}\right)$$

Manin actually showed that we can construct an isomorphism from this space to the homology classes of $H_1\left(X_{\Gamma_0}, \partial X_{\Gamma_0}, \mathbb{Q}\right)$. Now define $\mathcal{B}_2(\Gamma_0)$ to be the $\mathbb{Q}$-vector space generated by the cusps of X_{Γ_0}. We define a very important map

$$\partial : \mathcal{M}_2(\Gamma_0) \to \mathcal{B}_2(\Gamma_0)$$

$$\{\alpha, \beta\} \to \{\beta\} - \{\alpha\}$$

With this map we now define the most important vector space we will use to compute with modular symbols. Let $\mathcal{S}_2(\Gamma) = \ker(\partial)$. This space is called the space of cuspidal modular symbols, Manin proved that this space actually captures the homology of X_{Γ_0} [24]. The above map induces a canonical isomorphism.

$$S_2(\Gamma_0) \to H_1(X_{\Gamma_0}, \mathbb{Z})$$

3.1.1 Hecke operators on modular symbols

Something surprising that will open a lot of possibilities with modular symbols is that the Hecke operators T_n act on the space of modular symbols, we define the action of a Hecke operator over a modular symbol. When p is a prime not dividing N we have that,

$$T_p\left(\{\alpha,\beta\}\right) = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\{\alpha,\beta\} + \sum_{r \mod p} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix}\{\alpha,\beta\}$$

If p divides N the definition is the same, the only change is that we don't add the first term. As we see, Hecke operators can act on modular symbols, but not only that. We have that

$$\langle T_n\{\alpha,\beta\}, f\rangle = \langle\{\alpha,\beta\}, T_n f\rangle\,. \tag{11}$$

Where $\langle\{\alpha,\beta\}, f\rangle = 2\pi i \int_\alpha^\beta f(\tau)d\tau$. What is really importante about (11) is that it tells us that if we can find engenvalues of Hecke operators in $\mathcal{S}_2(\Gamma_0)$, we can recover eigenvalues in $S_2(\Gamma_0)$, the space of cusp forms. Therefore, if we can find finite generators of $\mathcal{M}_2(\Gamma_0)$ we would have found a method to calculate Hecke eigenvalues.

Since we know that $\Gamma_0(N)$ has a finite index in $SL_2(\mathbb{Z})$. Let $r_0, r_1, \ldots, r_m$ be the right cosets representatives such that $SL_2(\mathbb{Z})$ is the disjoint union of these cosets.

$$SL_2(\mathbb{Z}) = \Gamma_0(N)r_0 \cup \cdots \cup \Gamma_0(N)r_m$$

To make our calculations easier, consider the symbol $[r_i]'$ and let $[r_i]$ be the modular symbol $r_i\{0,\infty\}$. We equip this symbols with the right action $[r_i]'g = [r_j]'$ where $\Gamma_0(N)r_j = \Gamma_0(N)r_ig$. The symbols $[r_i]'$ are known as Manin symbols. The key idea of using Manin symbols is that every modular symbol can be expressed as a linear combination of $r_i\{0,\infty\}$. In fact these modular symbols $r_i\{0,\infty\}$ generate $\mathcal{M}_2(\Gamma_0)$ [4].

Since $\{\alpha,\beta\} = \{0,\beta\} - \{0,\alpha\}$ in only suffices to consider modular symbols of the form $\{0,\frac{a}{b}\}$. This can be achieved by thinking of continued fractions, if we consider that $\left\{\frac{b_{k-1}}{a_{k-1}},\frac{b_k}{a_k}\right\} = g_k\{0,\infty\} = r_i\{0,\infty\}$. For instance, consider the fraction $\frac{20}{3}$ we see that

$$\frac{20}{3} = 6 + \frac{1}{1+\frac{1}{2}}$$

Therefore,

$$\left\{0,\frac{20}{3}\right\} = \{0,\infty\} + \{\infty,6\} + \{6,7\} + \left\{7,\frac{20}{3}\right\}$$

We know state the following theorem without proof (the proof can be found at [4, Theorem 3.13]).

Theorem 9. *Consider the quotient group M of the free abelian group on Manin symbols $[r_0]',\ldots,[r_m]'$ generated by the elements,*

$$[r_i]' + [r_i]'\sigma \qquad [r_i]' + [r_i]'\tau + [r_i]'\tau^2$$

Then, there is an isomorphism

$$\Phi : M \to \mathcal{M}_2(\Gamma_0(N))$$

given by $[r_i]' \to [r_i]$

Where $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. By default, Sage computes modular symbols spaces over $\mathbb{Q}$, and represents Manin symbols as pairs (c, d).

So, we have a finite computable model of $\mathcal{M}_2(\Gamma)$ and $\mathcal{S}_2(\Gamma)$, and an algorithm to compute Hecke operators and the space of modular symbols. Once we get the Manin symbols we can lift this to a modular symbol and thus, calculate the Hecke eigenvalue. This is the general outline of the method of modular symbols for modular forms of level 2.

This idea can be generalized for modular forms of higher degree if we consider $M_k := \mathbb{Q}[x, y]_{k-2} \otimes M_2$ and define the action of a $g \in \Gamma_0(K)$ on a $P \in \mathbb{Q}[x, y]_{k-2}$ as

$$(gP)(X, Y) = P\left(g^{-}1 \begin{pmatrix} -X \\ Y \end{pmatrix}\right) = P(dX - bY, -cX + aY)$$

and thus,

$$g\left(P \otimes \{\alpha, \beta\}\right) = gP \otimes \{g\alpha, g\beta\}$$

in this case, we also have spaces of modular symbols and cuspidal modular symbols if we consider the following maps,

$$\mathcal{M}_k(\Gamma_0) : {}^{M_k}\!/_{P \otimes \{\alpha, \beta\} - gP \otimes \{g\alpha, g\beta\}}$$

We define $\mathcal{B}_k$ to be $\mathbb{Q}[x, y]_{k-2} \otimes \mathcal{B}_2$ and finally, we get our boundary map

$$\partial : \mathcal{M}_k \to \mathcal{B}_2$$

$$\partial\left(P \otimes \{\alpha, \beta\}\right) = P \otimes \{\beta\} - P \otimes \{\alpha\}$$

We define our space of cuspidal modular symbols to be the kernel of ∂, $\mathcal{S}_k(L) := ker(\partial)$. If one wishes to dig deeper into the algoritm to compute with modular symbols, one can refer to chapters 3 and 8 in [4].

3.2 Arb Package

As we mentioned, we want to be able to evaluate the quotient $\frac{T_p f(z_0)}{f(z_0)}$ for a newform f of level 1. One of the advantages of using Theorem 6 is that we can express any newform f as a polynomial in E_4 and E_6 and the Arb Package, which we will talk about in this section, provides a method for the optimal evaluation of E_4 and E_6 allowing a computationally advantage when evaluating $T_p f(z_0)$ and $f(z_0)$.

Arb stands for 'Efficient Arbitrary-Precision Midpoint-Radius Interval Arithmetic' and we will explain it now. Arb is based on interval arithmetic that allows computing in a rigourous way while tracking the error in each step of the program. In this case, Arb uses midpoint-radius intervals in which a real number is represented by an interval $[m \pm r]$ where both m and r are floating numbers. The whole idea of Arb, as described by its creator Fredrik Johansson, is to provide a modern treatment of numerical evaluation that works in the whole domain of the functions; with arbitrary precision, rigorous error bounds and with efficiency.

The algorithms implemented in Arb use ball arithmetic internally for propagation of error bounds. The algorithms used to evaluate mathematical functions have two steps, if the first step they try to optimize the point of evaluation, then the second

step consists in the evaluation itself with the help of series expansion. Arb has already implemente algorithms to evaluate commonly-used modular forms as part of the open source Arb library. In particular, we will focus on its evaluations for E_4 and E_6. Arb first evaluates $G_4(\tau)$ and $G_6(\tau)$ on the fundamental domain using theta functions.

The q-series defined for modular forms in (4) always converges; however, this convergence could be slow depending on τ, for instance if $\Im(\tau)$ is close to zero. Therefore, in a first step we would like to be able to find a modular transformation that takes τ into the fundamental domain. This will ensure that $|q| \leq e^{-\pi\sqrt{3}}$ which makes the convergence extremely rapid [20]. This can be obtained by repeatedly applying T and S to τ.

Once we send τ to the fundamental domain, we continue by evaluating G_4 and G_6. For that, we define the following theta constants that will be of help:

$$\theta_2(\tau) = e^{\frac{\pi i \tau}{4}} \sum_{-\infty}^{\infty} q^{n(n+1)}, \qquad \theta_3(\tau) = \sum_{-\infty}^{\infty} q^{n^2}, \qquad \theta_4(\tau) = \sum_{-\infty}^{\infty} (-1)^n q^{n^2}.$$

where $q = e^{\pi i \tau}$. One can prove in fact that θ_2, θ_3 and θ_4 are in fact modular forms of half integer weight. The thing about the theta series is that Arb can evaluate them extremely quickly with high precision. Therefore we express the Eisenstein series as functions of these theta constants. In particular,

$$G_4(\tau) = \frac{\pi^4}{90}\left(\theta_2^8 + \theta_3^8 + \theta_4^8\right), \qquad G_6(\tau) = \frac{\pi^6}{945}\left(-3\theta_2^8\left(\theta_3^4 + \theta_4^4\right) + \theta_3^{12} + \theta_4^{12}\right).$$

The algorithm in detail for the evaluation of the theta constanst can be found in [20,

Sec 1.4.2, Algorithm 1].

To sum up, we see how the Arb package uses the midpoint - radius implementation and a complex ball field to evaluate G_4 and G_6 by evaluating them on the fundamental domain using theta functions. This allows an optimized evaluations of the Eisenstein series and therefore of $T_p f(z_0)$ and $f(z_0)$.

3.2.1 CBF and CIF

There is one more component we need to use in order to get an appropiate evaluation of Eisenstein series and that is CBF or the Complex Ball Field. In Sage, ComplexBall is bond to the Arb library for arbitrary precision computations. A ComplexBall represents a complex number with error bounds that use the midpoint-radius intervals. A given real number is represented as a midpoint-radius interval, which will be refered to as ball. Therefore, to represent an imaginary number we give a pair of real number or balls; one for the real part and one for the imaginary part of τ. Sage includes them in an interval with separate error bounds. Therefore, a ComplexBall is in fact a rectangle $[m_1 \pm r_1] + i[m_2 \pm r_2]$ in the complex plane. The whole idea of splitting the real and imaginary parts is precisely the convenience of implementing many operations in this way. The only drawback is that Sage does not work in general with Complex Balls, and thus, once we do our evaluations with Arb we have to come back and work with Complex Interval Fields or CIF which are handled by Sage.

Now, we can compute the evaluation of Eisenstein series in a given point doing the following, in this case we will evaluate $G_4\left(\frac{1+i\sqrt{3}}{2} + \sqrt{2}\right)$ and $G_6\left(\frac{1+i\sqrt{3}}{2} + \sqrt{2}\right)$. When we use in Sage the command $tau.eisenstein(n)$ we get the list $G_4(\tau), G_6(\tau), \ldots G_{2n}(\tau)$.

```
sage: CBF = ComplexBallField(1000)
sage: CIF = ComplexIntervalField(1000)
sage: tau = (1 + CBF(-3).sqrt())/2 + CBF(2).sqrt()
```

```
sage: tau.eisenstein(2)

[[4.1382034648504429813013564 86 +/- 5.73e-28]
                + [-1.2341037069589654291280297 47 +/- 2.74e-28]*I,
 [-2.0785635450616882972664698 0 +/- 1.65e-27]
                + [2.8615098183452639836317979 8 +/- 3.92e-27]*I]
sage: CIF(xx[0])
4.1382034648504429813013564 86? - 1.2341037069589654291280297 47?*I
sage: CIF(xx[1])
-2.0785635450616882972664698 0? + 2.8615098183452639836317979 8?*I
```

Which tells us that

$$G_4\left(\frac{1+i\sqrt{3}}{2}+\sqrt{2}\right) = (4{,}1382\cdots 6486 \pm 5{,}73\times 10^{-28}) + i(-1{,}2341\cdots 9747 \pm 2{,}74\times 10^{-28})$$

$$G_6\left(\frac{1+i\sqrt{3}}{2}+\sqrt{2}\right) = (-2{,}0785\cdots 6980 \pm 1{,}65\times 10^{-27}) + i(2{,}8615\cdots 9798 \pm 3{,}92\times 10^{-27})$$

CHAPTER IV
ALGORITHM

We now state the main novelty of our work. We are proposing a new algorithm to compute the eigenvalues of Hecke operators. The main idea is to obtain a numerical approximation by evaluating our operator at points in the upper half plane,

$$\lambda_p = \frac{T_p(f)(\tau_0)}{f(\tau_0)}$$

for any τ_0 such that $f(\tau_0) \neq 0$. The implemented algorithm works for modular forms of level 1 and requires the evaluation of our newform. So, the idea behind the our algorithm for level 1 is the following:

1. Take a newform f of weight k and identify a basis for M_{k-12} using Theorem 6.
2. Multiply this basis by Δ and by Theorem 4 we get a basis for S_k. Use the fact that $\Delta = \frac{E_6^2 - E_4^3}{1728}$.
3. Next, express f as a linear combination of the basis elements found in step 1.
4. Evaluate $x = E_4(\tau), y = E_6(\tau)$ and Δ and then evaluate $f(\tau)$ and $T_p f(\tau)$by taking the appropriate combinations of x and y.

This algorithm is accomplished by the functions presented below that can be found in [25]. The advantage is that E_4, E_6 and Δ coefficients are easy to calculate and to

evaluate.

4.1 Implementation Details

For simplicity, we do not describe all the algorithms implemented, we will just describe some important algorithms; the whole code can be found at [25].

Algorithm 1 Find the basis for M_{k-12}. findBasis(k)

Require: $k \geq 0$, $k \in \mathbb{Z}$.

Create a list L and a list M_k.
for $a = 0$ **to** $a < \left\lfloor \frac{k-12}{4} + 1 \right\rfloor$ **do**
  $b \leftarrow \frac{k-12-4a}{6}$
  if $b \in \mathbb{Z}$ **then**
    $(a, b) \rightarrow L$
  end if
end for
$x \leftarrow E_4 \qquad y \leftarrow E_6 \qquad d = \Delta$
for $i = 0$ **to** $i < \text{len}(L)$ **do**
  $x^a \cdot y^b \rightarrow M_k$
end for
for all $f \in M_k$ **do**
  $f \leftarrow \Delta f$
end for
return M_k

Algorithm 1 receives the weight of our modular form f and finds all nonnegative integers (a, b) such that $4a + 6b = k - 12$ to find a basis for modular forms of weight $k - 12$; then, it uses Theorems 4 and 6 to find the basis for cusp forms of weight k.

Algorithm 2 Find the coefficients of a newform f with the basis found in findBasis(k).

getCoeff(k)

Require: Weight k of the newform f. $k \geq 0$, $k \in \mathbb{Z}$

Create the newform f of weight k.

Define a number field F given by the first coefficient of f.

$M \leftarrow$ Matrix Space of dimension $\dim(S_k)$ over F

$bs \leftarrow$ findBasis(k)

Elements in bs will be q-expansions of the form $\sum_{n=0}^{\infty} a_n^i q^n$

$M = \begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_d^1 \\ a_1^2 & a_2^2 & \cdots & a_d^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^d & a_2^d & \cdots & a_d^d \end{pmatrix}$. Where a_n^i corresponds to the coefficient of the i-th element in the basis

b $\leftarrow$ coefficients of f.

$cf = M^{-1}b$

if $\dim(S_k) = 1$ **then**

Choose the only embedding of f and place it in emb

else if $\dim(S_k) > 1$ **then**

Choose the first embedding of f and place it in emb

end if

$cf \leftarrow emb(cf)$

return cf

Algorithm 2, which receives our function and its weight, uses the result of algorithm 1 to get the coefficients of the expression of f in our basis; in case of need, we used the first embedding of F. When we talk about embeddings of a modular form what we refer to is that the coefficients of f live in a field $\mathbb{Q}(\alpha)$ where α is the root of a polynomial and has various Galois conjugates, so we can define several embeddings $\mathbb{Q}(\alpha) \to \mathbb{C}$. In our case we always consider the first one.

Algorithm 3 Evaluate E_4 and E_6. eval_F_generators_E(F,τ)

Require: f a newform. $\tau \in \mathbb{H}$.

Optimize τ

Define ComplexBallField (CBF), Complex Interval Field(CIF) to desired precision

$\tau \leftarrow CBF(\tau)$

Evaluate $G_4(\tau)$ and $G_6(\tau)$

Normalize Eisenstein series in CIF.

return $E_4(\tau)$ and $E_6(\tau)$

Finally, algorithm 3 uses the Arb package to evaluate E_4 and E_6 which then use the previous algorithm implemented in order to get $T_p f(\tau_0)$ and $f(\tau_0)$ analytically and we then get the quotient. The algorithms presented here are the ones that allow us to evaluate a newform f and $T_p f$ for $\tau \in \mathbb{H}$ with $f(\tau) \neq 0$.

CHAPTER V
RESULTS

We show how to calculate, with our algorithm, some eigenvalues of modular forms. Consider a newform f of weight 24. We calculate the eigenvalues associated to T_{101} and T_{1009}.

```
sage: G=Newforms(1,24,names='a')[0]

sage: eigenvalue_Tp_generators2(G,next_prime(100))
 (1.362427808883252558788832382448654420866894317124782195984414214439
 989721159977865974321299145504843410467066280776018167392592854752046
 665384249018659339297162582850925783966692025278717381979128451009914
 428726050517942161595075898930649222794986028960978885550881258367559
 0038909?e23,
 3.093122555750734638171432620276759344465578788412526544717412652926
 961714422879900583715984500611086858537309739882901578616698522275957
 708386981452707873693837344962710734404531210961362412925271044266755
 307905048442330842474815087172320139760 91?e-35)

sage: eigenvalue_Tp_generators2(G,next_prime(1000))
 (3.570332419143301580456733796090858776004470511423155838585060511877
 799142428555308907371981468069502659407823568183953035879572737639815
 123875764806501337140274451435076554800040184585061817547773863803758
 194744251107032190938658909802890869548674015029152035277149 3?e34,
```

```
1.2581358060284765225517289374977487758757718529947498650901343414045926894759672858128480892345268368751059819203355399990191599738349294066646594511836964151053755182681446795412374899782802257951979603007088030770783939775921278?e-37)
```

this tells us that,

$$\lambda_{101} = 1{,}362427\cdots038909 \times 10^{23} \pm 3{,}093122\cdots976091 \times 10^{-35}$$
$$\lambda_{1009} = 3{,}570332\cdots771493 \times 10^{34} \pm 1{,}258135\cdots921278 \times 10^{-37}$$

are the eigenvalues for the Hecke operators T_{101} and T_{1009}, respectively. One can also see that the 101th fourier coefficient of f is λ_{101} and the 1009-th fourier coefficient is λ_{1009}.

We run calculations with our code and we achieved the following results which can be found at [26]. We compare the modular symbol method as implemented in Sage [13] to our method. For each p we compute the pth Hecke eigenvalue in both ways (using modular symbols and using our numerical approach).

In Table 1 we highlight some timings in which we computed Hecke eigenvalues using both methods.

level	weight	p	Modular symbols	Eisenstein
1	12	1 009	0,073	**0,071**
		10 007	0,967	**0,847**
		100 003	13,710	**9,274**
		1 000 003	163,515	**100,782**
1	24	1 009	0,158	**0,085**
		10 007	2,023	**0,935**
		100 003	27,190	**9,941**
		1 000 003	330,854	**108,923**
1	100	101	0,057	**0,013**
		1 009	0,918	**0,146**
		10 007	14,197	**1,913**
		100 003	186,873	**23,449**
1	200	101	0,171	**0,024**
		1 009	2,443	**0,347**
		10 007	36,195	**5,104**
		100 003	500,388	**69,916**

Cuadro 1: A summary of timings to compute Hecke eigenvalues using modular symbols and using our method.

The previous table shows a summary of timings (in seconds; the **bold** figures identify the shortest time in each row) to compute Hecke eigenvalues in different ways. The first uses the modular symbols method as implemented in Sage; the second way uses analytic evaluation of the Eisenstein series E_4 and E_6. The computations were done on one Intel i7-8550U core at 1.80GHz, on a machine with 16 GB RAM. As seen in table 1, our method outperforms the current algorithm implemented in Sage. It is quicker for large weights and primes.

CHAPTER VI
CONCLUSION

This worked served as an introduction to the theory of modular forms. The definition of a modular form as a holomorphic function in the upper half plane satisfying the modularity condition (3) is very abstract. However, we wish to carry out calculations with them. We defined all the things necessary to understand modular forms of level 1 and the algorithm implemented to calculate eigenvalues of Hecke operators. The code implemented helped us to find, numerically, the eigenvalues λ_p of Hecke operators such that

$$T_p f(\tau_0) = \lambda_p f(\tau_0)$$

for p a prime.

For this code, implemented for modular forms of level 1, we took advantage of the structure of the space of modular forms and cusp forms. We used the fact that there are some special modular forms called Eisenstein series which, when combined appropiately, forms a basis for the space of modular forms since, as we were able to see, M_k is in fact a vector space over $\mathbb{C}$; furthermore, M_k is finite dimensional. Once we found a basis for the space of modular forms of weight k, we used a very important cusp form Δ to establish an isomorphism between this space M_k and the space of cusp forms S_{k+12}. Once we did all that we evaluated f at points in the upper half plane $(f(\tau_0), T_P f(\tau_0))$ to get the quotient, and thus, an analytic evaluations for Hecke eigenvalues.

Computational methods such as modular symbols provide a practical and efficient

way of calculating Hecke eigenvalues of classical modular forms. However, when the dimension of the space gets too big, when either the weight of the modular form or the level or the p in T_p, increase, the calculations involved become impractical. An example of that is the magnitude of the Fourier coefficients that we found in Section V. Our algorithm was faster to evaluate because the Fourier coefficients of Eisenstein series are easier to calculate. In particular, the number of coefficients needed for large weight is much smaller than the number of coefficients needed to evaluate f using its Fourier expansion. Also, we used the ARB package that allowed for the optimal evaluation of E_4 and E_6 via theta functions. As ilustrated in Table 1, extensive benchmarks also show that our method exhibits performance that compares favorably with the modular symbol approach.

Therefore, the theoretical and experimental results of this work show that using Theorems 6 and 4 along with their implementation in Sage serve as a good method to obtain eigenvalues of Hecke operators T_p for large p. The approximations presented in this work are important, as they brought significant improvements in the time needed to calculate the eigenvalues, especially when p is large.

All in all, analytic evaluation of classical modular forms seem to be a promising new approach to overcome the present difficulties associated with the current computational methods. Even though our algorithm runs quickly, we do not yet know if it is the best we can do. We could optimize functions in between, or use parallel computing.

Future directions of the work would be to try to take advantage of the structure of the space of modular forms of higher level and establish some connections with modular symbols to use both approaches. Also, it would be nice if we maybe try to use our algorithm for other projects such as investigations of Lehmer's conjecture and Maeda's conjecture.

REFERENCES

[1] S. J. Diamond F., *A First Course in Modular Forms*, ép. Graduate Texts in Mathematics. Springer-Verlag, 2005.

[2] P. Fleig, H. P. A. Gustafsson, A. Kleinschmidt y D. Persson, "Eisenstein series and automorphic representations", arXiv:1511.04265, 2016. dirección: `https://arxiv.org/pdf/1511.04265`.

[3] D. Zagier, "Elliptic Modular Forms and Their Applications", en. oct. de 2008, págs. 1-103. DOI: `10.1007/978-3-540-74119-0_1`.

[4] W. A. Stein y P. E. Gunnells, *Modular forms, a computational approach*. American Mathematical Society Providence, RI, 2007, vol. 79.

[5] S. W. Ribet K., "Lectures on Modular Forms and Hecke Operators", 2011.

[6] S. Ramanujan, "On certain arithmetical functions", en *Collected Papers*, 1962, 136–-162.

[7] Y. A. J. Berndt B., "Ramanujan's Contributoins to Eisenstein Series, especially in his lost notebook", *Number Theoretic Methods*, vol. 8, págs. 31-53, 2002. DOI: `https://doi.org/10.1007/978-1-4757-3675-5_3`.

[8] H. Cohen, *An Introduction to Modular Forms*, ép. Notes from the International School on Computational Number Theory. 2018, págs. 3-62.

[9] K. S. T. Y. Gan W.T., *Eisenstein Series and Applications*. Birkhäuser, 2008.

[10] S. S. Kudla y T. H. Yang, "Eisenstein series for $SL(2)$", *Sci China Math*, vol. 53, n.º 9, 2275–2316, 2010. DOI: `10.1007/s11425-010-4097-1`. dirección: `https://doi-org.ezp.lib.unimelb.edu.au/10.1007/s40687-018-0155-z`.

[11] D Brubaker B. Bump y S. Friedberg, "Eisenstein Series, Crystals and Ice", *Notices of the American Mathematical Society*, vol. 58, n.º 11, 2011.

[12] D. H. Lehmer, "The vanishing of Ramanujan's function $\tau(n)$", *Duke Math. J*, vol. 14, págs. 429-433, 1947.

[13] W. Stein y col., *Sage Mathematics Software (Version 8.8)*, `http://www.sagemath.org`, The Sage Development Team, 2019.

[14] W. Bosma, J. Cannon y C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.*, vol. 24, n.º 3-4, págs. 235-265, 1997, Computational algebra and number theory (London, 1993), ISSN: 0747-7171. DOI: `10.1006/jsco.1996.0125`. dirección: `http://dx.doi.org/10.1006/jsco.1996.0125`.

[15] C. Wuthrich, "Numerical modular symbols for elliptic curves", *Math. Comp.*, vol. 87, n.º 313, págs. 2393-2423, 2018, ISSN: 0025-5718. DOI: 10.1090/mcom/3274. dirección: https://doi-org.ezp.lib.unimelb.edu.au/10.1090/mcom/3274.

[16] *PARI/GP version 2.11.2*, Available from http://pari.math.u-bordeaux.fr/, The PARI Group, Univ. Bordeaux, 2019.

[17] K. Belabas y H. Cohen, "Modular forms in Pari/GP", *Res. Math. Sci.*, vol. 5, n.º 3, Paper No. 37, 19, 2018, ISSN: 2522-0144. DOI: 10.1007/s40687-018-0155-z. dirección: https://doi-org.ezp.lib.unimelb.edu.au/10.1007/s40687-018-0155-z.

[18] B. Edixhoven y J.-M. Couveignes, eds., *Computational aspects of modular forms and Galois representations*, ép. Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 2011, vol. 176, págs. xii+425, ISBN: 978-0-691-14202-9. dirección: https://doi.org/10.1515/9781400839001.

[19] F. Johansson, "Arb: efficient arbitrary-precision midpoint-radius interval arithmetic", *IEEE Transactions on Computers*, vol. 66, págs. 1281-1292, 8 2017. DOI: 10.1109/TC.2017.2690633.

[20] ——, "Numerical Evaluation of Elliptic Functions, Elliptic Integrals and Modular Forms", arXiv:1806.06725, 2018. DOI: https://arxiv.org/pdf/1806.06725.pdf.

[21] T. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, ép. Graduate Texts in Mathematics. Springer-Verlag, 1990, vol. 2.

[22] J. Serre, *A course in Arithmetic*, ép. Graduate Texts in Mathematics. Springer-Verlag, 1973.

[23] M. Masdeu, *Modular Forms*, ép. Notes for a course on Modular forms offered at the University of Warwick. University of Warwick, 2014.

[24] P. Gunnels, *Modular Symbols*, ép. UNCG Summer Schools in Computational Number Theory. UNC Greensboro, 2014.

[25] D. Armendáriz, O. Colman, N. Coloma, A. Ghitza, N. C. Ryan y D. Terán, *SageMath code for the analytic calculation of the Hecke eigenvalues of classical modular forms*, https://github.com/nathancryan/analytic-evaluation-classical-modular-forms, [Online; accessed 29-Sep-2019], 2019.

[26] ——, "Analytic evaluation of Hecke eigenvalues for classical modular forms", arXiv:1806.01586, 2019. dirección: https://arxiv.org/abs/1806.01586.