Modular Forms - A Master's Thesis

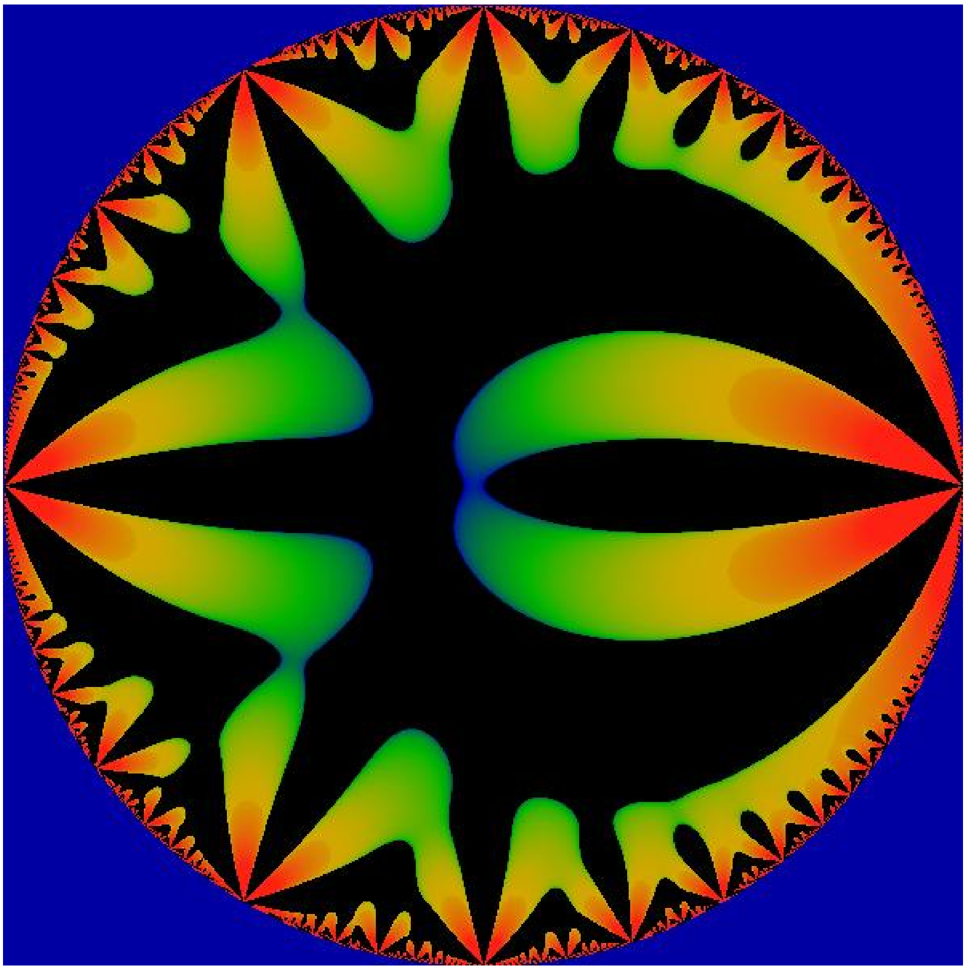


Figure 1: The real part of the Eisenstein series G_6 as a function of q on the unit disk. [10]

Mikkel Højlund Larsen

Aalborg Universitet
June 2020

AALBORG UNIVERSITET
STUDENTERRAPPORT

School of Engineering and Science
Skjernvej 4a
9220 Aalborg Øst
www.ses.aau.dk

Title:
Modular Forms - A Master's Thesis

Theme:
Complex Analysis &
Abstract Algebra

Project period:
Master's Thesis, Mathematics
Spring 2020

Project Group:
5.211c

Participants:
Mikkel Højlund Larsen

Supervisors:
Oliver Wilhelm Gnilke

Numbers printed: 1

Page count: 73

Finished: May 2020

Abstract

Målet med dette speciale er at finde et udtryk for antallet af repræsentationer af et naturligt tal n som en sum af fire kvadrater, altså

$$r(n,4) = |\{(a,b,c,d) \in \mathbb{Z} \mid n = a^2 + b^2 + c^2 + d^2\}.$$

Disse tal for ethvert naturligt n findes som koefficienter i den fjerde potens af Jacobi Theta funktionen, der er en uendelig række på formen

$$\theta(z)^4 = \sum_{n=0}^{\infty} r(n,4)q^n,$$

hvor $q = e^{2\pi iz}$ og $z \in \mathbb{H}$, hvor $\mathbb{H}$ er den øvre halvdel af det complekse plan med positiv imaginær del, $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$. Denne funktion tilhører en mængde af funktioner kaldet modulære former, hvis elementer udspænder et vektorrum med endelig dimension. Disse vektorrum har dermed et endeligt antal generatorer, og dermed kan $\theta(z)^4$ skrives som en linearkombination af disse generatorer.

For at finde disse generatorer introduceres læseren først til modulære former af heltals-vægt k med hensyn til matrix gruppen, $SL_2(\mathbb{Z})$; mængden af alle matricer med heltalsindgange og determinant 1, hvorved det konkluderes, at den eneste modulære form af ulige heltalsvægt k med hensyn til $SL_2(\mathbb{Z})$ er nul-funktionen, $f(z) = 0$. Eksempler på ikke-trivielle modulære former af vægt k med hensyn til $SL_2(\mathbb{Z})$ gives i form af den k'te Eisenstein række,

$$G_k = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^k},\ z \in \mathbb{H},$$

for $k \geq 3$. Disse er identisk 0 for ulige vægte k. Fourier-udvidelsen for den k'te Eisenstein række udledes i specialet til at være

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

hvor $\zeta(k) = \sum_{n>0,n\in\mathbb{Z}} \frac{1}{n^k}$ og $\sigma_k(n) = \sum_{d>0,d|n} d^k$. Det konkluderes efterfølgende, at vektorrum af modulære former med hensyn til $SL_2(\mathbb{Z})$, M_k, for enhver heltals vægt $k \geq 0$, er genereret af linearkombinationer af produkter af potenser af E_4 og E_6; den henholdsvis fjerde og sjette normaliserede Eisenstein række, således at for potenserne a og b gælder $4a + 6b = k$.

Da $\theta(z)^4$ ikke er svagt modulær med hensyn til $SL_2(\mathbb{Z})$, men er svagt modulær med hensyn til mængden $\left\{\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\4 & 1\end{bmatrix}\right\}$, introduceres læseren dernæst til modulære former med hensyn til kongruens delgrupper af $SL_2(\mathbb{Z})$. Specielt vises det, at hvis en funktion er svagt modulær med hensyn til en mængde af matricer, så er funktionen også svagt modulær med hensyn til den gruppe, elementerne i mængden genererer med matrix multiplikation. Specielt findes det at kongruens delgruppen

$$\Gamma_0(4) = \left\{\gamma = \begin{bmatrix}a & b\\c & d\end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix}a & b\\c & d\end{bmatrix} \equiv \begin{bmatrix}a & b\\0 & d\end{bmatrix} \mod 4\right\}$$

er genereret af $\left\{\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\4 & 1\end{bmatrix}\right\}$, og det følger dermed at $\theta(z)^4$ er svagt modulær med hensyn til $\Gamma_0(4)$.

Det vises i det efterfølgende, at $\theta(z)^4$ er en modulær form af vægt 2 med hensyn til $\Gamma_0(4)$, og en yderligere analyse af vektorrummet bestående af alle modulære former af vægt 2 med hensyn til $\Gamma_0(4)$, $M_2(\Gamma_0(4))$, at dette rum er to-dimensionelt og er genereret af de to lineært uafhængige elementer $G_{2,2}(z) = G_2(z) - 2G_2(2z)$, $G_{2,4}(z) = G_2(z) - 4G_2(4z)$.

Dermed er $\theta(z)^4$ en linearkombination af disse to elementer, og det findes at

$$\theta(z)^4 = -\frac{1}{\pi^2} G_{2,4}(z).$$

Efter påvisning af Fourier udvidelsen

$$G_{2,4}(z) = -\pi^2 \left(1 + 8 \sum_{n=1}^{\infty} \left(\sum_{d>0, d|n, d \notin 4\mathbb{Z}} d \right) q^n \right),$$

konkluderes det slutteligt ved ækvivalens af koefficienter, at

$$r(n,4) = 8 \sum_{d>0, d|n, 4 \nmid d} d,$$

og målet med specialet er nået.
Som forsættelse af specialet, er der flere resultater at finde for antallet af representationer af et naturligt tal som en sum af k kvadrater for naturlige tal k, altså

$$r(n,k) = |\{(v_1, v_2, \ldots, v_k) \in \mathbb{Z}^k \mid n = v_1^2 + v_2^2 + \ldots + v_k^2\}|.$$

I specialet er det vist, at $r(n,k)$ er koefficienterne i den k'te potens af Jacobi Theta funktionen,

$$\theta(z)^k = \sum_{n=0}^{\infty} r(n,k) q^n,$$

samt at enhver naturlig, endelig, lige potens, $2k$, $k \geq 1$ af $\theta(z)$ er holomorf på $\mathbb{H}$, holomorf ved uendelig og svagt modulær af vægt k med hensyn til $\Gamma_0(4)$. Man kan dernæst påvise, hvorvidt $\theta(z)^{2k}$ er en modulær form af vægt k med hensyn til $\Gamma_0(4)$, finde det korresponderende vektorrums dimension, $dim(M_k(\Gamma_0(4)))$ (Dette viser sig at være endeligt dimensionelt for endelige k. Se [4][Theorem 3.5.1 og Theorem 3.6.1] for mere), finde generatorer for dette vektorrum, og slutteligt finde et andet udtryk for $\theta(z)^k$ i form af en linearkombination af disse generatorer.

Contents

Preface

The author of this project is Mikkel Højlund Larsen.

The overall theme of this thesis is modular forms. In this theme, we try to derive the Four Square Theorem using modular forms and, in the process, give a good introduction to the theory of modular forms both with respect to the full matrix group $SL_2(\mathbb{Z})$ and congruence subgroups of $SL_2(\mathbb{Z})$. With this, we will give an analysis of the structure and dimension of the vector spaces that the modular forms with respect to $SL_2(\mathbb{Z})$ span, and for the Four Square Theorem, we shall focus on a specific vector space of modular forms with respect to the congruence subgroup $\Gamma_0(4)$, which will be described in the thesis.

The chapters of this thesis are enumerated with sections and subsections that are enumerated internally in chapters. The end of a proof will be marked by $\square$. References will be shown with a number, that refers to the enumerated references in the reference chapter placed in the end of the project.

The thesis is written under the assumption that the reader has a higher understanding of Abstract Algebra and Complex Analysis, however, most of the relevant results and definitions used from these fields are found in the Appendix with proofs provided for some of the results.

As a final note, I would like to thank my supervisor, Oliver Wilhelm Gnilke, for all the help he has given me throughout the last 3 semesters, and this thesis would not be possible without it. It is truly appreciated.
Enjoy.

Aalborg Universitet June 2020.

Mikkel Højlund Larsen

Chapter 1 | Introduction

In this these, we shall derive a formula for computation of how many different ways there are to write a nonnegative integer n, as the sum of four squares of integers

$$n = a^2 + b^2 + c^2 + d^2, \ a, b, c, d \in \mathbb{Z}.$$

The following is based on the introduction in [4].
Generally we define the representations of n as a sum of k squares as the following, and the case of $k = 4$ is within this definition:

Definition 1.1. (Representations of n as the sum of k squares)
For integers $n \geq 0$ and $k \geq 1$, we define **the number of representations of n as a sum of k squares** as the function

$$r(n, k) = \left| \left\{ (v_1, \dots, v_k) \in \mathbb{Z}^k \mid n = \sum_{i=1}^{k} v_i^2 \right\} \right|,$$

If $n = 0$ this implies $r(0, k) = 1$ for all k. That is, $n = 0$ only has the trivial solution $0 = 0^2 + \dots 0^2$. Now, if $i + j = k$ then

$$r(n, k) = \sum_{l+m=n} r(l, i) r(m, j),$$

summing over the nonnegative integer values of m, l that add to n. This is seen as, if $k = i + j$, and $n = m + l$, then

$$m = \sum_{r=1}^{j} a_r^2$$
$$l = \sum_{t=1}^{i} b_t^2$$
$$n = m + l = \sum_{r=1}^{j} a_r^2 + \sum_{t=1}^{i} b_t^2,$$

and thus for one way of representing m as the sum of j squares, there are $r(l, i)$ ways of representing n as a sum of k square with this representation of m, so going through all representations of m as j squares, there are in total $\sum_{l+m=n} r(l, i) r(m, j)$ ways to represent n as a sum of k squares and vice versa.
This result is of the form

$$c_n = \sum_{l+m=n} a_l b_m,$$

with $c_n = r(n, k)$, $a_l = r(l, i)$ and $b_m = r(m, j)$. If we view c_n as coefficients in a power series $S = \sum_{n=0}^{\infty} c_n q^n$, we see that this power series is a product of two power series

$$\left(\sum_{l=0}^{\infty} a_l q^l \right) \left(\sum_{m=0}^{\infty} b_m q^m \right) = \sum_{n=0}^{\infty} c_n q^n = S,$$

with $m + l = n$.
The power series with $r(n, 1)$ as coefficients is called the Jacobi theta series, which we will define and analyse further in the following section.

1.1 Jacobi theta series

Definition 1.2. (Jacobi theta series)
The **Jacobi Theta series** is the function

$$\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \ldots,$$

where $z \in \mathbb{H}$ and $q = e^{2\pi i z}$.

Now, we see that

$$\begin{aligned}\theta(z)^2 &= (\sum_{a\in\mathbb{Z}} q^{a^2})(\sum_{b\in\mathbb{Z}} q^{b^2})\\ &= \sum_{a\in\mathbb{Z}}\sum_{b\in\mathbb{Z}} q^{a^2+b^2}\\ &= \sum_{n=0}^{\infty} r(n,2)q^n,\end{aligned}$$

with the substitution $n = a^2 + b^2$. With this approach we see the following pattern:

Corollary 1.3. We have

$$\theta(z)^k = \sum_{n=0}^{\infty} r(n,k)q^n$$

Proof
For any k, we have

$$\begin{aligned}\theta(z)^k &= (\sum_{a_1\in\mathbb{Z}} q^{a_1^2}) \cdot \ldots \cdot (\sum_{a_k\in\mathbb{Z}} q^{a_k^2})\\ &= \sum_{a_1\in\mathbb{Z}} \cdots \sum_{a_k\in\mathbb{Z}} q^{a_1^2+\ldots+a_k^2}\end{aligned}$$

Now, with the substitution of $n = a_1^2 + \ldots + a_k^2$, we obtain

$$\theta(z)^k = \sum_{n=0}^{\infty} r(n,k)q^n.$$

□

Likewise, one naturally sees that with the substitution $n = a^2$, we have $\theta(z) = \sum_{n=0}^{\infty} r(n,1)q^n$, which fits the definition of $\theta(z) = 1 + 2q + 2q^4 + 2q^9 \ldots$, as the number of ways to represent a natural number n as a square of an integer. This is only possible if n is a square number $(1, 4, 9, 16, \ldots)$, and if a is a solution to $n = x^2$, then $-a$ is aswell. In fact these are the only two solutions, so if $r(n,1)$ is non-zero, we must have $r(n,1) = 2$ with the exception of $r(0,1) = 1$.
We are specifically interested in the case of $\theta(z)^4$ since the coefficients in this series is $r(n,4)$, and we wish to derive a formula for these coefficients. We shall see that $\theta(z)^4$ belongs to a set of special functions called **modular forms**. These are functions that satisfy certain holomorphicity conditions and certain functional equations under fractional linear transformations $\gamma(z) = \frac{az+b}{cz+d}$, where $ad - bc = 1$. We shall therefore in this thesis study modular forms in order to derive results about $\theta(z)^4$ and thus also $r(n,4)$, so we shall return to the θ^4 function in this thesis, whenever we have the appropriate results to analyse it.

Chapter 2 | Fractional Linear Transformations

This chapter is based on [5][Section 2.1] and [3][Sections 1.1, 1.2].
With the introduction behind us, we shall start by describing fractional linear transformations. We denote $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

Definition 2.1. (Fractional Linear Transformations)
Fractional linear transformations, (FLT) are rational functions $f: \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form

$$f(z) = \frac{az+b}{cz+d}, \; a, b, c, d \in \mathbb{Z}, \; ad - bc \neq 0$$

where we define $\frac{az+b}{0} = \infty$, $f(\infty) = \frac{a}{c}$ for $c \neq 0$, and $f(\infty) = \infty$ for $c = 0$.

Remark 2.2. Note, that the fractional linear transformations are rational functions with polynomials of degree 1 in both enumerator and denominator and are thus holomorphic on an open set S of $\mathbb{C}$. There is only one pole for each fractional linear transformation at $z = -\frac{d}{c}$, since we have the condition $ad - bc \neq 0$, which implies that c and d cannot simultaneously be 0 in this case, but with the addition of ∞ to the complex plane the functions are holomorphic everywhere and thus entire on $\hat{\mathbb{C}}$.
Also, if $ad = bc$ in the above, the fractional linear transformations would be constant as we have

$$f(z) = \frac{az+b}{cz+d} = \frac{a(cz+d)}{c(cz+d)} - \frac{ad-bc}{c(cz+d)} = \frac{a}{c}.$$

Proposition 2.3. The set of all fractional linear transformation, FLT, is a group under the composition of functions

Proof
We will show that FLT, together with the composition of functions, satisfies the group axioms.
1. We will show that the group is closed under the composition of functions. For $f = \frac{az+b}{cz+d}, g = \frac{a'z+b'}{c'z+d'} \in FLT$, we have

$$\begin{aligned} g \circ f(z) &= \frac{a'(\frac{az+b}{cz+d}) + b'}{c'(\frac{az+b}{cz+d}) + d'} \\ &= \frac{a'(az+b) + b'(cz+d)}{c'(az+b) + d'(cz+d)} \\ &= \frac{a'az + a'b + b'cz + b'd}{c'az + c'd + d'cz + d'd} \\ &= \frac{(a'a + b'c)z + a'b + b'd}{(c'a + d'c)z + c'd + d'd}. \end{aligned}$$

What is left to show is that $(a'a + b'c)(c'd + d'd) - (a'b + b'd)(c'a + d'c) \neq 0$, such that the composition is again a fractional linear transformation. We see that

$$(a'a + b'c)(c'd + d'd) - (a'b + b'd)(c'a + d'c) = a'ac'd + a'ad'd + b'cc'd + b'cd'd - a'bc'a - a'bd'c - b'dc'a - b'dd'c$$

$$
\begin{aligned}
&= (ad-bc)a'd' + (bc-ad)b'c' \\
&= (ad-bc)(a'd'-b'c') \\
&\neq 0
\end{aligned}
$$

So the composition of two fractional linear transformations must form a fractional linear transformation.

2. The composition of functions is always associative.

3. FLT contains the neutral element $f(z) = \frac{1\cdot z+0}{0\cdot z+1} = z \in FLT$

4. Let $f(z) = \frac{az+b}{cz+d}$. We have that the inverse of $f(z)$ is $g(z) = \frac{dz-b}{-cz+a} \in FLT$, as

$$
\begin{aligned}
g(f(z)) &= \frac{df(z)-b}{-cf(z)+a} \\
&= \frac{d(\frac{az+b}{cz+d})-b}{-c(\frac{az+b}{cz+d})+a} \\
&= \frac{\frac{daz+db}{cz+d}-b}{\frac{-caz-cb}{cz+d}+a} \\
&= \frac{daz+db-b(cz+d)}{-caz-cb+a(cz+d)} \\
&= \frac{daz-bcz}{ad-bc} \\
&= \frac{(ad-bc)z}{ad-bc} \\
&= z.
\end{aligned}
$$

Likewise, we can show that the inverse of g is f, as

$$
\begin{aligned}
f(g(z)) &= \frac{ag(z)+b}{cg(z)+d} \\
&= \frac{a(\frac{dz-b}{-cz+a})+b}{c(\frac{dz-b}{-cz+a})+d} \\
&= \frac{\frac{daz-ab}{-cz+a}+b}{\frac{cdz-cb}{-cz+a}+d} \\
&= \frac{daz-ab+b(-cz+a)}{cdz-cb+d(-cz+a)} \\
&= \frac{daz-bcz}{ad-bc} \\
&= \frac{(ad-bc)z}{ad-bc} \\
&= z.
\end{aligned}
$$

□

Proposition 2.4. *FLT is isomorphic to $PGL_2(\mathbb{C})$. That is, there exists an isomorphism $\tilde{\phi}: \ PGL_2(\mathbb{C}) \to FLT$.*

Proof

There exists a surjective group homomorphism $\phi: \ GL_2(\mathbb{C}) \to FLT$ with $\phi(A)(z) = \frac{az+b}{cz+d}$ for $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in GL_2(\mathbb{C})$, then $AB = \begin{bmatrix} a'a + c'b & b'a + d'b \\ a'c + c'd & b'c + d'd \end{bmatrix} \in GL_2(\mathbb{C})$. Then we have

$$\begin{aligned} \phi(AB)(z) &= \frac{(a'a + c'b)z + b'a + d'b}{(a'c + c'd)z + b'c + d'd} \\ &= \frac{a'az + c'bz + b'a + d'b}{a'cz + c'dz + b'c + d'd} \\ &= \frac{a(a'z + b') + b(c'z + d')}{c(a'z + b') + d(c'z + d)} \\ &= \frac{a(\frac{a'z+b'}{c'z+d'}) + b}{c(\frac{a'z+b'}{c'z+d'}) + d} \\ &= \phi(A) \circ \phi(B)(z), \end{aligned}$$

and the map is clearly surjective.
The center of $GL_2(\mathbb{C})$ was shown in Example B.14 to be the set of all scalar multiples of I_2.
We have that the center $Z(GL_2(\mathbb{C})) \subseteq Ker(\phi)$, as for $\alpha \in \mathbb{C}$, we have

$$\phi(\alpha \cdot I_2)(z) = \frac{\alpha z}{\alpha} = z.$$

Thus we have the induced map

$$\tilde{\phi} : GL_2(\mathbb{C})/Z(GL_2(\mathbb{C})) = PGL_2(\mathbb{C}) \to FLT,$$

It only remains to show that $Z(GL_2(\mathbb{C})) = Ker\phi$. The kernel of ϕ contains the matrices that map to the fractional linear transformation with a pole at $z = \infty$ and a zero at $z = 0$. So let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then we have $\phi(A)(z) = \frac{az+b}{cz+d}$, and recall that a fractional linear transformation has one zero at $z = -\frac{b}{a}$ and one pole at $z = -\frac{d}{c}$. So we have the equation $-\frac{b}{a} = 0$, which implies $b = 0$. This means $\phi(A)(z) = \frac{az}{cz+d}$. Now, assume $\phi(A)(\infty) = \infty$. If $a \neq 0$ and $c \neq 0$, we have defined for a fractional linear transformation $f(z) = \frac{az+b}{cz+d}$ that $f(\infty) = \frac{a}{c}$. So $c = 0$ such that $\phi(A)(\infty) = \infty$. So we have $b = 0, c = 0$ and we must have $a = d$ for $\frac{az}{d} = z$ and therefore A must be a scalar multiple of I. So we must have $Z(GL_2(\mathbb{C})) = Ker\phi$.
Thus by the first isomorphism theorem, we have

$$\hat{\phi}: \ PGL_2(\mathbb{C}) \to FLT$$

is a well-defined group isomorphism. □

Definition 2.5. (Upper Half Plane)
The **upper half plane** is the subset

$$\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}.$$

Proposition 2.6. Let $f \in FLT$ with $ad - bc = 1$. Then for $z \in \mathbb{C}$, we have

$$Im(f(z)) = \frac{Im(z)}{|cz+d|^2}.$$

Proof
We have

$$\begin{aligned} f(z) &= \frac{az+b}{cz+d} \\ &= \frac{(az+b)(d+c\bar{z})}{|cz+d|^2} \\ &= \frac{ac|z|^2 + 2(ad+bc)Re(z) + (ad-bc)Im(z)}{|cz+d|^2} \\ &= \frac{ac|z|^2 + 2(ad+bc)Re(z) + Im(z)}{|cz+d|^2}. \end{aligned}$$

Thus

$$Im(f(z)) = \frac{Im(z)}{|cz+d|^2}.$$

□

Proposition 2.7. Let $Aut(\mathbb{H})$ denote the set of invertible maps $f : \mathbb{H} \to \mathbb{H}$. The restriction of FLT to $\mathbb{H}$ is a subgroup of $Aut(\mathbb{H})$.

Proof
A fractional linear transformation maps $\mathbb{R} \cup \{\infty\} \to \mathbb{R} \cup \{\infty\}$ and maps complex numbers with positive imaginary part to complex numbers with positive imaginary part. Therefore it must map all of $\mathbb{H}$ to itself, and as it was shown, all fractional linear transformations have a mutual inverse fractional linear transformation, so they are indeed invertible maps. Hence we have $FLT_{|\mathbb{H}} \subseteq Aut(\mathbb{H})$. What remains to show is that $Aut(\mathbb{H})$ is a group, which follows as the composition of functions is always associative, it contains the identity function $f(z) = z$, which is it's own mutual inverse and thus invertible, all functions in $Aut(\mathbb{H})$ are invertible and thus the mutual inverse is also contained in $Aut(\mathbb{H})$, and the composition of two invertible functions $f, g : \mathbb{H} \to \mathbb{H}$, must again be invertible. So $FLT_{|\mathbb{H}}$ must indeed be a subgroup of $Aut(\mathbb{H})$.

□

We will be focusing on the matrix group $SL_2(\mathbb{Z})$ in the coming chapters, so we will divert our attention to this group now. Since $SL_2(\mathbb{Z})$ contains the elements $-I_2$ and I_2, which fix any $z \in \mathbb{H}$, we can instead consider the quotient group

$$SL_2(\mathbb{Z})/\{\pm I_2\}.$$

The center of $SL_2(\mathbb{Z})$ is exactly $\{\pm I_2\}$. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in SL_2(\mathbb{Z})$. we will look at the two products AB and BA and see, what conditions on one of them, in order for these matrices to commute.

So,

$$AB = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

$$BA = \begin{bmatrix} ae+cf & eb+df \\ ag+ch & bg+dh \end{bmatrix}.$$

Now, for $AB = BA$, we must have either $b, c = 0$ and $a = d$, $f, g = 0$ and $e = h$, or $A = B$. But since $ad - bc = 1, eh - fg = 1$, we must have that either $A = \pm I$ or $B = \pm I$, and thus we must have $Z(SL_2(\mathbb{Z})) = \{\pm I_2\}$. Thus we see that this quotient group is in fact the **projective special linear group with integer entries**

$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I_2\}.$$

This group is generated by $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, and we see that

$$S^2 = [I_2]$$
$$T^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$
$$(ST)^3 = [I_2]$$

Thus S has order 2, T has infinite order and ST has order 3 and the group action of these two elements on $\mathbb{H}$ is defined by

$$S: \; z \mapsto -\frac{1}{z}$$
$$T: \; z \mapsto z+1.$$

We have shown that $PGL_2(\mathbb{C}) \cong FLT$, but if we introduce the set of fractional linear transformations with $ad - bc = 1$, where $a, b, c, d \in \mathbb{Z}$ as FLT_1, we get another interesting result:

Proposition 2.8. FLT_1 is isomorphic to $PSL_2(\mathbb{Z})$. That is, there exists an isomorphism $\tilde{\phi}: \; PSL_2(\mathbb{Z}) \to FLT_1$.

Proof
The approach of the proof is absolutely the same as in the proof of Proposition 2.4.

□

With this result, we thus have for any $\gamma \in PSL_2(\mathbb{Z})$ there is a corresponding fractional linear transformation $\gamma(z) \in FLT_1$. Now, since any $\pm\gamma \in SL_2(\mathbb{Z})$ are equivalent in $PSL_2(\mathbb{Z})$, we thus have for any $\pm\gamma \in SL_2(\mathbb{Z})$ there is a corresponding frational linear transformation $\gamma(z) \in FLT_1$. We can therefore see matrices in $SL_2(\mathbb{Z})$ as fractional linear transformations.

2.1 The Fundamental Domain for the group action of $SL_2(\mathbb{Z})$

We are now interested in analysing how these fractional linear transformations act on the upper half plane. For this, we can consider the set of orbits $\mathbb{H}/SL_2(\mathbb{Z}) = \{SL_2(\mathbb{Z})z \mid z \in \mathbb{H}\}$, where $SL_2(\mathbb{Z})$ acts on $\mathbb{H}$ by fractional linear transformations. What we are interested in is to find the elements of this set, as we can then generate all of $\mathbb{H}$ using elements from this set by the group action of $SL_2(\mathbb{Z})$, as points in $\mathbb{H}$ in the same $SL_2(\mathbb{Z})$-orbit are equivalent in $\mathbb{H}/SL_2(\mathbb{Z})$. This set is equivalent to the fundamental domain for the group action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ and we will now define a fundamental domain for a group action on $\mathbb{H}$:

Definition 2.9. (Fundamental domain for a group action)
A **fundamental domain** for a group action of a group Γ on $\mathbb{H}$ is an open subset $D \subset \mathbb{H}$ so that the closure of D, $\overline{D} = D \cup \delta D$ with δD being the boundary of D, satisfies

1. $\Gamma \overline{D} = \mathbb{H}$.
2. For $d_1, d_2 \in D$ with $d_1 \neq d_2$, we have $\Gamma d_1 \neq \Gamma d_2$.
3. For any point $p \in \delta D$ and $d \in D$ we have $\Gamma p \neq \Gamma d$ and there are only finitely many points $p_1, \dots p_n \in \delta D$ such that $\Gamma p = \Gamma p_i$, $i = 1, \dots, n$.

Proposition 2.10. The set

$$F = \left\{ z \in \mathbb{H} \mid |z| > 1, \ |Re(z)| < \frac{1}{2} \right\}$$

is the fundamental domain for the group action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$.

Proof
Throughout this proof, we use the property for a matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ has $det(\gamma) = ad - bc = 1$.

(1):
Let $z \in \mathbb{H}$. Then $\{mz + n \mid m, n \in \mathbb{Z}\}$ is a lattice in $\mathbb{C}$. Every lattice must have a non-zero vector of minimal length, therefore this lattice must have a point of minimal modulus and there are only finitely many points with $|cz + d|^2 < 1$ in this lattice. Let $cz + d$ be such a point. This requires c and d to be relatively prime, since if we had $gcd(c, d) = a$ for some $a \in \mathbb{Z}$, $\frac{cz+d}{a} = bz + r$, where b and r are integers, would have even smaller modulus, which would contradict our choice of $cz + d$ as a point of minimal modulus.
Since c and d are relative prime, there must exist $a, b \in \mathbb{Z}$ such that $ad - bc = 1$ and hence there exists a matrix $\gamma_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$. By the transformation property from Proposition 2.6, we have $Im(\gamma(z)) = \frac{Im(z)}{|cz+d|^2}$.
Now, since this modulus is minimal by the transformation of γ_1, we must have that $Im(\gamma_1(z))$ is a maximal member in the set $\{Im(\gamma(z)) \mid \gamma \in SL_2(\mathbb{Z})\}$.
Now, set $z^* = T^n(\gamma_1(z)) = \gamma_1 z + n$, where n is such that $|Re(z^*)| \leq \frac{1}{2}$. Clearly, since n is an integer, $Im(z^*)$ is still maximal. We cannot have that $|z^*| < 1$, as

$$Im(S(z^*)) = Im\left(-\frac{1}{z^*}\right) = Im\left(\frac{z^*}{|z^*|^2}\right) > Im(z^*),$$

which would contradict the maximality of $Im(z^*)$. So since $|Re(z^*)| \leq \frac{1}{2}$ and since $|z^*| \geq 1$, we have $z^* \in \overline{F}$, and z is equivalent to z^* under the group action of $SL_2(\mathbb{Z})$ (they are in the same orbit). Thus we have shown that any point in $z \in \mathbb{H}$ is in the same orbit as some point $z^* \in \overline{F}$ which satisfies (1) in the definition.

(2):
Now, suppose we have two points $z_1, z_2 \in F$ in the same orbit $z_2 = \gamma z_1$ with $\gamma_1 \neq \pm I_2$. This implies that there is an inverse transformation $z_1 = \gamma_2 z_2$. These γ_1 and γ_2 cannot be on the form T^n for any $n \geq 1$ since this would contradict the assumption of $|Re(z_1)|, |Re(z_2)| < \frac{1}{2}$, so $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $c \neq 0$, as $c = 0$ implies $a, b = \pm 1$ and this is equivalent to γ being a power of T (could be negative) or being negative T^n (of which we know $\pm T^n$ are equivalent as fractional linear tranformations). Now, since for a point $z \in F$, we must have $|Re(z)| < \frac{1}{2}$ and $|z| > 1$, we have

$$|z| = \sqrt{(Im(z))^2 + (Re(z))^2} = \sqrt{Im(z)^2 + |Re(z)|^2} > 1.$$

Now since the imaginary part is minimized in the boundary of F, we have that

$$\sqrt{Im(z)^2 + \frac{1}{4}} = 1$$
$$\Updownarrow Im(z) = \frac{\sqrt{3}}{2}.$$

Hence for $z \in F$, we have $Im(z) > \frac{\sqrt{3}}{2}$.
Now, from the transformation property in Proposition 2.6, we get

$$\begin{aligned}\frac{\sqrt{3}}{2} &< Im(z_2)\\ &= \frac{Im(z_1)}{|cz_1 + d|^2}\\ &= \frac{Im(z_1)}{c^2 Im(z_1)^2 + (cRe(z_1) + d)^2}\\ &\leq \frac{Im(z_1)}{c^2 Im(z_1)}\\ &< \frac{2}{c^2\sqrt{3}}.\end{aligned}$$

This inequality is only satisfied for the integer value $c = \pm 1, 0$. Without loss of generality we may assume $Im(z_1) \leq Im(z_2)$, however for $c = \pm 1$ we have

$$|\pm z_1 + d| = \sqrt{Im(z_1)^2 + (\pm Re(z_1) + d)^2} = \sqrt{|z_1|^2 + d^2 \pm 2Re(z_1)d},$$

and since $|Re(z_1)| < \frac{1}{2}$, we have

$$|\pm z_1 + d| = \sqrt{|z_1|^2 + d^2 \pm 2Re(z_1)d} \geq |z_1|$$

for all $d \in \mathbb{Z}$ which contradicts the transformation property as $Im(z_2) = \frac{Im(z_1)}{|\pm z_1 + d|^2} < Im(z_1)$. The same argument can be made for $Im(z_1) \geq Im(z_2)$ for the inverse transformation. Hence, no two points in F can be in the same orbit and (2) in the definition is shown.

(3):

If we have $c = 0$, we must have $d = \pm 1$, which in turn implies $a = \pm 1$ and b can be any integer. Due to the constraint $|Re(z)| < \frac{1}{2}$, the two points z_1 and z_2 can then only be in the same orbit if they are both on the boundary lines of $Re(z) = \pm\frac{1}{2}$ and hence we must have $z_1, z_2 \in \delta F$ and we have $Im(z_1) = Im(z_2)$, as $Im(z_2) = \frac{Im(z_1)}{|cz+d|^2} = \frac{Im(z_1)}{|\pm 1|^2} = Im(z_1)$ and vice versa for the inverse transformation. Thus there is a unique point on the opposite real boundary line in the same orbit.
Without loss of generality, we assume for $c = 1$ for the case $c = \pm 1$. Then we need $|z_1 + d| \leq 1$. If $d = 0$, we have $|z_1| = 1$ and so $b = -1$ for unit determinant. In this case $|z_1|$ is on the unit arc of the boundary. We then have the transformation

$$z_2 = \gamma(z_1) = \frac{az_1 - 1}{z_1} = a - \frac{1}{z_1} = a - \frac{\bar{z_1}}{|z_1|^2} = a - \bar{z_1}.$$

Now, since we have $|Re(z_1)| \leq \frac{1}{2}$, we must have that if $|Re(z_1)| = \frac{1}{2}$ that $a = \pm 1$, so every point at the intersection of the boundary lines for the real part and the unit arc $|z_1| = 1$ is in the same orbit as the unique point $Re(z_2) = -Re(z_1)$ with $|z_1| = |z_2| = 1$.
For $|Re(z_1)| < \frac{1}{2}$, we must have $a = 0$ and then we have

$$z_2 = \gamma(z_1) = -\frac{1}{z_1} = -\frac{\bar{z_1}}{|z_1|^2} = -\bar{z_1}.$$

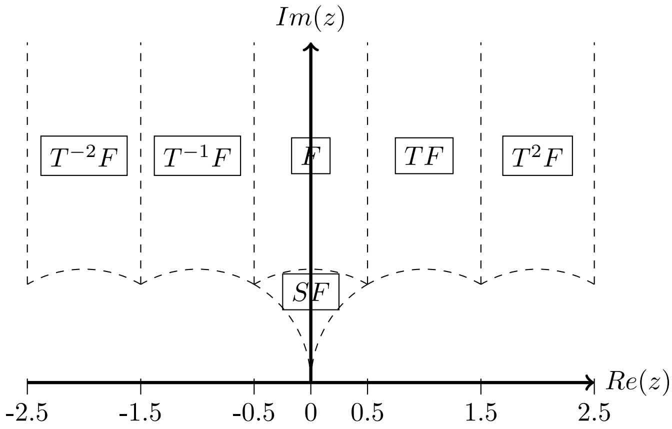
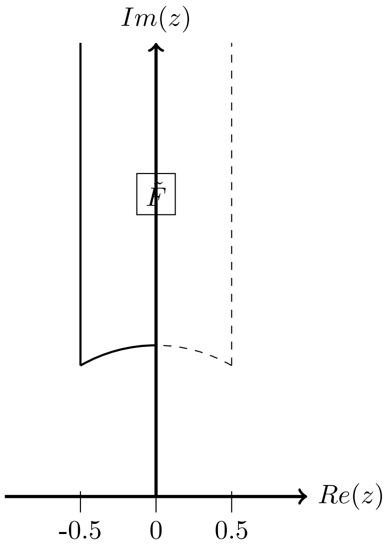


Figure 2.1: The Fundamental Domain F for the group action of $SL_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}$

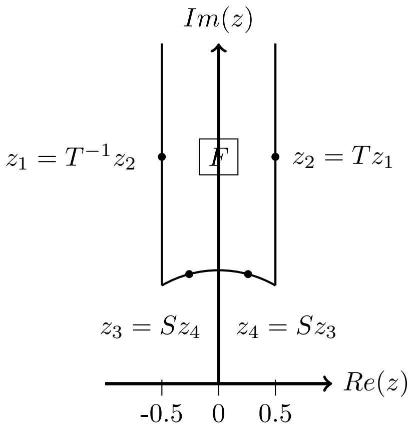
Hence any point on the arc, but not on the real boundary lines at $\pm\frac{1}{2}$ is in the same orbit as the unique point with $Re(z_1) = -Re(z_2)$ by $S(z_1) = z_2 = -\bar{z_1}$ as shown in Figure (b) below.

Therefore, any point in δF is in the same orbit as a unique point in δF, and therefore finitely many. This shows (3).

□



(a) The semi-closure of F, $\tilde{F}$



(b) Boundary points in the same orbit

Remark 2.11. As stated in the proof, all points on the two lines $Re(z) = \pm\frac{1}{2}$ with $|z| \geq 1$ are equivalent under the action of $T: \; z \mapsto z+1$. Also, the points on the left and right halves of the arc $|z| = 1$ are equivalent under the action of $S: \; z \mapsto -\frac{1}{z}$ and these are the only two equivalences for the boundary of F. We can therefore define the semi-closure $\tilde{F}$, which is the set consisting of all of F and the boundary points of F with non-positive real part. This way any point in $\mathbb{H}$ is $SL_2(\mathbb{Z})$-equivalent to a unique point of $\tilde{F}$. See Figure (a) above for $\tilde{F}$.

Corollary 2.12. We have $SL_2(\mathbb{Z}) = \langle S, T\rangle$.

Proof
Let $G = \langle S, T\rangle$, $\gamma \in SL_2(\mathbb{Z})$ and $g \in G$ If $z \in F$, then z has a point in it's $SL_2(\mathbb{Z})$-orbit $\gamma(z) \in \mathbb{H} \setminus \bar{F}$, but any point in $\mathbb{H} \setminus \bar{F}$ is in the same G-orbit as some point in $g(\gamma(z))$ by the above proof. We have since G is a subgroup of $SL_2(\mathbb{Z})$, then $g\gamma \in SL_2(\mathbb{Z})$. Let $g\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and assume without loss of generality that $z = 2i$. Then

$$Im((g\gamma)(2i) = \frac{2}{4c^2 + d^2} > \frac{\sqrt{3}}{2}.$$

We must then have $c = 0$. Then $ad = 1$ for unit determinant, so $a = d = \pm 1$ and

$$(g\gamma)(2i) = \frac{2ai + b}{d} = 2i \pm b.$$

Now since $g(\gamma(2i)) \in F$, we must have $|Re((g\gamma)(2i))| < \frac{1}{2}$, which forces $b = 0$, so

$$g\gamma = \pm I_2.$$

Therefore $\gamma = \pm g^{-1}$ and since $-I_2 = S^2 \in G$, we conclude $\gamma \in G$. So $SL_2(\mathbb{Z}) = \langle S, T\rangle$. ([9][Theorem 1.1])

□

Chapter 3 | Introduction to Modular Forms

This chapter is based on [4][section 1.1], [5][Sections 2.2, 3.1] and [3][Sections 1.1, 1.2, 2.1].
With the description of the group action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$, we will now describe **weakly modular functions**. Transformation by fractional linear transformation in FLT_1 of the domain of these functions corresponds to scaling the function by a factor determined by the given fractional linear transformation. We have the following definition for functions that satisfy these:

Definition 3.1. (Weakly Modular Functions)
Let $SL_2(\mathbb{Z})$ act on the upper half plane by fractional linear transformations and let k be an integer. Suppose $\gamma \in SL_2(\mathbb{Z})$ with $\gamma(z) = \frac{az+b}{cz+d}$. A **weakly modular function of weight** k is a complex meromorphic function $f : \mathbb{H} \to \mathbb{H}$, satisfying

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

We call $(cz+d)^k$ the **automorphy factor of** f **given** γ.

If a function is weakly modular of weight 0, this corresponds to complete $SL_2(\mathbb{Z})$-invariance as

$$f(\gamma(z)) = f(z),$$

for all $\gamma \in SL_2(\mathbb{Z})$.

Proposition 3.2. The only weakly modular function of odd weight is

$$f(z) = 0.$$

Proof
Let f be a weakly modular function of odd weight k. Then by applying the matrix $-I_2$, we see

$$f(-I_2(z)) = f(z) = (-1)^k f(z) = -f(z),$$

which in turn implies $f(z) = 0$.

□

Example 3.3. The zero function $f(z) = 0$ is a weakly modular function of any weight $k \in \mathbb{Z}$ as

$$f(\gamma(z)) = (cz+d)^k \cdot f(z) = f(z) = 0.$$

The constant functions $f(z) = C$ are weakly modular functions of weight 0 as

$$f(\gamma(z)) = (cz+d)^0 f(z) = f(z).$$

Recall that $S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ both generate all of $SL_2(\mathbb{Z})$ by Corollary 2.12.
Now, since we consider even k, we see that the automorphy factor $(cz+d)^k$ is in fact unchanged when considering $\pm\gamma \in SL_2(\mathbb{Z})$ as

$$\begin{aligned} f(-\gamma(z)) &= (-cz - d)^k f(z) \\ &= ((-1)(cz + d))^k f(z) \\ &= (cz + d)^k f(z). \end{aligned}$$

For a weakly modular function of weight k, f. Therefore, by associativity of fractional linear transformations, it is enough to check that a function is weakly modular of weight k for S and T, as any other $\pm\gamma \in SL_2(\mathbb{Z})$ is some product of powers of these two matrices. So a function f is weakly modular of weight k with respect to $SL_2(\mathbb{Z})$ precisely when we have

$$f(T(z)) = f(z + 1) = f(z) f(S(z)) = f\left(-\frac{1}{z}\right) = z^k f(z)$$

for all $z \in \mathbb{H}$.
Now, recall that the Laurent series of a complex function $f(z)$ around $i\infty$ is equivalent to the Laurent series of $f\left(\frac{1}{z}\right)$ around 0, so we have the following

Definition 3.4. (Meromorphic and holomorphic function at infinity)
A function $f:\ \mathbb{H} \to \mathbb{C}$, satisfying $f(z + 1) = f(z)$ is **meromorphic at infinity** if for the Laurent series of f around $i\infty$,

$$f\left(\frac{1}{z}\right) = \sum_{n=-\infty}^{\infty} a_n z^{-n},$$

we have $a_n = 0$ for all $n \leq N$ for some $N \in \mathbb{Z}$. Equivalently, we say that f has a pole of order N at $i\infty$
If we have for the Laurent series that $a_n = 0$ for all $n < 0$, then f is said to be **holomorphic at infinity**. Equivalently, we say that f has a removable singularity at $i\infty$.

Definition 3.5. (Modular function)
A **modular function of weight** k is a weakly modular function of weight k $f:\ \mathbb{H} \to \mathbb{C}$ that is meromorphic at infinity.

Definition 3.6. (Modular form)
A **modular form of weight** k is a weakly modular function of weight k $f:\ \mathbb{H} \to \mathbb{C}$ that is holomorphic on $\mathbb{H}$ and holomorphic at infinity.

Example 3.7. The zero function is obviously holomorphic on all of $\mathbb{H}$. Since $f(\infty) = 0$ and since the zero function is weakly modular of any weight k, it must be a modular form of any weight $k \in \mathbb{Z}$.
The constant functions are modular forms of weight 0 as their derivatives exists on all of $\mathbb{H}$ with $f'(z) = 0$ and we have that $f(\infty) = C$.

Since a modular form, f, is holomorphic on $\mathbb{H}$, holomorphic at infinity and satisfies $f(z + 1) = f(z)$, f has a convergent Laurent series around $i\infty$ with:

$$f(z) = \sum_{n=0}^{\infty} a_n z^{-n}.$$

We can also represent this Laurent series with respect to the complex exponential $q = e^{2\pi iz}$, which we will now show.
We shall denote the complex unit disk $D = \{z \in \mathbb{C} \mid |z| < 1\}$ and the punctured unit disk $D^* = D \setminus \{0\}$.

Lemma 3.8. If $f : \mathbb{H} \to \mathbb{C}$ is holomorphic, holomorphic at infinity and satisfying $f(z) = f(z+1)$, then there exists $a_n \in \mathbb{C}$ for $n \geq 0$ such that

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

for all $z \in \mathbb{H}$ and $q = e^{2\pi iz} \in D^*$.

Proof
For $z \in \mathbb{H}$ set

$$q(z) = e^{2\pi iz}.$$

If we write $z = x + iy$, we have $q(z) = e^{2\pi ix}e^{-2\pi y}$, and we note that $|e^{2\pi ix}| = 1$ and $0 < |e^{-2\pi y}| < 1$, as y is positive. So q is a point in the punctured unit disc D^*. Conversely, each point in $q_0 \in D^*$ can be written as $e^{2\pi iz_0}$ for a point $z_0 \in \mathbb{H}$ with $-\frac{1}{2} < Re(z_0) \leq \frac{1}{2}$ (remember that $e^{2\pi iRe(z)}$ is 1-periodic, so the interval can be interval of length 1).
So the mapping $q : \mathbb{H} \to D^*$ is surjective and locally invertible, as if we write $q_0 \in D^*$ as $q_0 = e^{2\pi iz_0}$, then any q sufficiently close to q_0 can be written $q = e^{2\pi iz}$ for a unique $z \in \mathbb{H}$ sufficiently close to z_0.
Now, convert the function $f : \mathbb{H} \to \mathbb{C}$ to function $\tilde{f} : D^* \to \mathbb{C}$ by defining $\tilde{f}(q) = f(z)$ for any $z \in \mathbb{H}$ for which $e^{2\pi iz} = q$. This is well-defined because if for some other $z' \in \mathbb{H}$, we also have $e^{2\pi iz'} = q$, then $z' = z + n$ for some $n \in \mathbb{Z}$. Since f is holomorphic, we can prove that $\tilde{f}$ is holomorphic by computing the derivative. So, for each $q_0 \in D^*$ write $q_0 = e^{2\pi iz_0}$. Then any q near q_0 is $q = e^{2\pi iz}$ for a unique z near z_0, and $q \to q_0$ is equivalent to $z \to z_0$. So

$$\begin{aligned}\frac{\tilde{f}(q) - \tilde{f}(q_0)}{q - q_0} &= \frac{f(z) - f(z_0)}{q - q_0} \\ &= \frac{f(z) - f(z_0)}{z - z_0} \frac{z - z_0}{e^{2\pi iz} - e^{2\pi iz_0}}.\end{aligned}$$

As $z \to z_0$, the first fraction tends to $f'(z_0)$ and the second fraction tends to $\frac{1}{(e^{2\pi iz_0})'} = \frac{1}{2\pi ie^{2\pi iz_0}}$, so in total, this tends to $\frac{f'(z_0)}{2\pi iq_0}$.
Now, since $f(z)$ is holomorphic at infinity, it must by Riemann's removable singularity theorem (Theorem A.27) be bounded at $i\infty$, and since $z \to i\infty$ implies $q \to 0$, we have that $\tilde{f}(q)$ must be bounded as $q \to 0$, and must thus be holomorphic at $q = 0$. Thus $\tilde{f}$ has a Laurent series around 0 with

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

and since $\tilde{f}(q)$ is holomorphic on the open unit disc $D = \{q \in \mathbb{C} \mid |q| < 1\}$, this Laurent series must converge on all of D. Therefore

$$f(z) = \tilde{f}(q) = \sum_{n=0}^{\infty} a_n e^{2\pi inz}$$

for all $z \in \mathbb{H}$.

□

Definition 3.9. (Fourier expansion)
For a function $f: \mathbb{H} \to \mathbb{C}$ that is holomorphic on $\mathbb{H}$, holomorphic at infinity and satisfying $f(z+1) = f(z)$, we call the series expansion

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

the **Fourier expansion of** f.

Recall, that any weakly modular function satisfies $f(z) = f(z+1)$ as

$$f(z+1) = f(Tz) = 1^k f(z) = f(z).$$

Since modular forms are holomorphic on $\mathbb{H}$, holomorphic at infinity and are weakly modular functions, these must, by Lemma 3.8, have a Fourier expansion of the form

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

for all $z \in \mathbb{H}$.
We can introduce a special case of modular forms; cusp forms:

Definition 3.10. (Cusp Form)
A modular form of weight k with respect to $SL_2(\mathbb{Z})$, f, is called a **cusp form of weight k with respect to $SL_2(\mathbb{Z})$** if for the constant term a_0 in the Fourier expansion of f, we have $a_0 = 0$.

Now, since $z \to i\infty$ implies that $q \to 0$, we have that $a_0 = f(i\infty)$, as a_0 is the constant term in the Fourier expansion of f, and the complex exponentials vanish at $i\infty$. Hence a cusp form with respect to $SL_2(\mathbb{Z})$ is to be interpretted as a modular form that vanishes at infinity.

3.1 Holomorphicity of θ^4

We now return to the function $\theta(z)^4$. We would like to determine if this is a modular form with respect to $SL_2(\mathbb{Z})$, and to summarize, the requirements for this is the following:

1) It must be holomorphic on $\mathbb{H}$.
2) It must be holomorphic at infinity.
3) It must be weakly modular of weight k with respect to $SL_2(\mathbb{Z})$ for some integer k.

We will now check if the holomorphicity conditions are satisfied. The following is based on [4][Exercise 4.9.2] with some hints found in the back of the book.
Now, we will show that not only is $\theta(z)^4$ holomorphic on $\mathbb{H}$ and at infinity, but that this applies generally for $\theta(z)^k$. Recall that

$$\theta(z)^k = \sum_{a_1 \in \mathbb{Z}} \cdots \sum_{a_k \in \mathbb{Z}} q^{a_1^2 + \ldots + a_k^2}.$$

We can view this sum, as a sum over a vector $l \in \mathbb{Z}^k$, where the exponent of q corresponds to $|l|^2$. So if we define the set

$$S_m = \{l \in \mathbb{Z}^k \mid |l| = m\}$$

for some nonnegative, real m (for example, if n is a prime then the square root of n is irrational). We then have $S_0 = \{0\}$, only containing the zero vector. Then if $l \in S_m$ this implies that $l = \begin{bmatrix} a_1 \\ \vdots \\ a_k \end{bmatrix}$ is a solution vector to $m^2 = n = a_1^2 + \ldots + a_k^2$. Conversely if n has a representation as a sum of k squares $n = a_1^2 + \ldots + a_k^2$, then there exists some positive, real square root of n, $m = \sqrt{n}$, such that $m = \sqrt{a_1^2 + \ldots + a_k^2}$, which is the norm of some integral vector $l = \begin{bmatrix} a_1 \\ \vdots \\ a_k \end{bmatrix} \in \mathbb{Z}^k$ and hence $n = a_1^2 + \ldots + a_k^2$ implies that $l \in S_m$. It then follows that $|S_m| = r(n, k)$. We have the following upper bound on S_m for all nonnegative integers m:

Lemma 3.11. Let $S_m = \{n \in \mathbb{Z}^k \mid |n| = m\}$. For all nonnegative integers m and for all natural numbers k, we have

$$|S_m| \leq (2m+1)^k$$

Proof
If $n \in S_m$ then

$$|n|^2 = \sum_{i=1}^{k} a_i^2 = m^2$$

and thus we have the constraint

$$-m \leq a_i \leq m.$$

There are then $2m + 1$ possible integer values for each a_i of which there are k. Hence

$$|S_m| \leq (2m+1)^k.$$

□

We wish to use this to show that $\theta(z)^k$ converges uniformly and absolutely on every compact subset $K \subset \mathbb{H}$, but we need another result for this:

Lemma 3.12. Let $K \subset \mathbb{H}$ be compact. We have that for any $z \in K$ and $l \in S_m$, there exists a $y_0 > 0$ such that

$$|e^{2\pi i |l|^2 z}| \leq e^{-2\pi m^2 y_0}$$

Proof
Since K is compact, there must exists some $y_0 > 0$ such that $Im(z) \geq y_0$ for all $z \in K$. Now, for all $l \in S_m$, we have

$$|l| = m \Leftrightarrow |l|^2 = m^2,$$

and since

$$\begin{aligned} |e^{2\pi i |l|^2 z}| &= |e^{2\pi i |l|^2 Re(z)}||e^{-2\pi |l|^2 Im(z)}| \\ &= e^{-2\pi |l|^2 Im(z)} &= e^{-2\pi m^2 Im(z)}, \end{aligned}$$

we must have that if $Im(z) \geq y_0$ for all $z \in K$, that

$$|e^{2\pi i |l|^2 z}| \leq e^{-2\pi m^2 y_0},$$

since the exponential is monotonically decreasing with increasing $Im(z)$. This proves the Lemma.

□

Lemma 3.13. Let $K \subset \mathbb{H}$ be compact. We have for any $z \in K$, there exists a natural number M_0 such that for any $M \geq M_0$, the corresponding tail of the series $\theta(z)^k$ satisfies

$$\sum_{l \in \mathbb{Z}^k |l| \geq M} |e^{2\pi i |l|^2 z}| < \sum_{m=M} e^{-m} = e^{-M}(1 - e^{-1})^{-1}.$$

Proof
We have from Lemma 3.12 that there exists some $y_0 > 0$, such that $Im(z) \geq y_0$ for all $z \in K$, and

$$|e^{2\pi i |l|^2 z}| \leq e^{-2\pi m^2 y_0}$$

for all $l \in S_m$. We can rewrite this series as

$$\sum_{l \in \mathbb{Z}^k} |e^{2\pi i |l|^2 z}| = \sum_{m=0}^{\infty} |S_m||e^{2\pi i m^2 z}|.$$

Now, combining Lemma 3.11, Lemma 3.12 and using that for some $M \geq M_0$, we have $(2M+1)^k < e^M$ and $2\pi m^2 y_0 > 2m$, we have that

$$\begin{aligned}\sum_{l \in \mathbb{Z}^k} |e^{2\pi i |l|^2 z}| &= \sum_{m=0}^{\infty} |S_m||e^{2\pi i m^2 z}| \\ &\leq \sum_{m=0}^{\infty} (2m+1)^k e^{-2\pi m^2 y_0},\end{aligned}$$

for all $z \in K$ and $l \in S_m$. Hence for any $M \geq M_0$, we have for the corresponding tails of the series $\theta(z)^k$, that

$$\begin{aligned}\sum_{\substack{l \in \mathbb{Z}^k \\ |l| \geq M}} |e^{2\pi i |l|^2 z}| &\leq \sum_{m=M}^{\infty} (2m+1)^k e^{-2\pi m^2 y_0} \\ &< \sum_{m=M}^{\infty} e^m e^{-2m} \\ &= \sum_{m=M}^{\infty} e^{-m} \\ &= e^{-M}(1 - e^{-1})^{-1},\end{aligned}$$

where the last step follows as the sum can be viewed as a geometric series. This proves the Lemma.

□

Lemma 3.14. We have that $\theta(z)^k$ converges absolutely and uniformly on every compact subset $K \subset \mathbb{H}$.

Proof
We showed with Lemma 3.13 that for any compact subset $K \subset \mathbb{H}$, there exists a natural number M_0 such that for all $M \geq M_0$ and $z \in K$ we have

$$\sum_{\substack{l \in \mathbb{Z}^k \\ |l| \geq M}} |e^{2\pi i |l|^2 z}| < \sum_{m=M} e^{-m} = e^{-M}(1 - e^{-1})^{-1}.$$

The right hand side of this inequality is less than arbitrary $\epsilon > 0$ for large enough M independently of z, showing that the series converges absolutely and uniformly on compact subsets of $\mathbb{H}$.

□

Theorem 3.15. $\theta(z)^k$ is holomorphic on $\mathbb{H}$ for any $k \in \mathbb{N}$.

Proof
We have shown that $\theta(z)^k$ converges uniformly and absolutely on every compact subset $K \subset \mathbb{H}$, and since each of the summands in the previous lemmas are holomorphic, the entire sum must be holomorphic by Theorem A.21. Thus $\theta(z)^k$ is holomorphic on $\mathbb{H}$.

□

Theorem 3.16. $\theta(z)^k$ is holomorphic at infinity for any $k \in \mathbb{N}$.

Proof
Since all terms with a q dependence in $\theta(z)^k$ vanish as $Im(z) \to \infty$ (the exponential decays faster as $z \to i\infty$, than $r(n,k)$ grows with $n \to \infty$ for fixed k, since $r(n,k)$ is $O(n^{k/2})$), we must have that the limit of $\theta(z)^k$ as $Im(z) \to \infty$ exists and is finite, as it is $r(0,k) = 1$. Hence $\theta(z)^k$ is bounded as $Im(z) \to \infty$ and by Riemann's removable singularity theorem (Theorem A.27) it must then be holomorphic at $i\infty$.

□

3.2 Functional Equations of θ^4

Now, we only need to check if θ^4 is weakly modular of weight k with respect to $SL_2(\mathbb{Z})$ for some integer k. We have the following results for θ and θ^4:

Proposition 3.17. The function $\theta(z)$ satisfies the two functional equations

$$\theta(z+1) = \theta(z), \tag{3.1}$$

$$\theta\left(\frac{-1}{4z}\right) = \sqrt{\frac{2z}{i}}\theta(z) \tag{3.2}$$

for all $z \in \mathbb{H}$.

Proof
The first equation follows as θ only depends on q and q is 1-periodic.
For the second equation, we can use the Poisson summation formula, that is

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n),$$

where $\hat{f}$ is the Fourier transform of f,

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{2\pi ixy} f(x)dx.$$

Applying this to the function $f(t) = e^{-\pi tx^2}$, where $t \in \mathbb{R}$ with $t > 0$, we get

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-\pi tx^2 + 2\pi ixy} dx$$

$$= \int_{-\infty}^{\infty} e^{-(\sqrt{\pi}\sqrt{t}(x-iy/t))^2-\pi y^2/t}dx$$
$$= e^{-\pi y^2/t}\int_{-\infty}^{\infty} e^{-\pi(\sqrt{t}(x-iy/t))^2}dx$$

Now, substituting with $u = \sqrt{t}(x - iy/t)$, we get

$$e^{-\pi y^2/t}\int_{-\infty}^{\infty} e^{-\pi(\sqrt{t}(x-iy/t))^2}dx = \frac{e^{-\pi y^2/t}}{\sqrt{t}}\int_{-\infty}^{\infty} e^{-\pi u^2}du$$
$$= \frac{e^{-\pi y^2/t}}{\sqrt{t}}.$$

Thus by the formula, we obtain

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} = \frac{1}{\sqrt{t}}\sum_{n\in\mathbb{Z}} e^{-\pi n^2/t},$$

and this proves the relation for $z = \frac{it}{2}$, which lies on $\mathbb{H}$ since $t > 0$ and the general case follows by analytic continuation. ([3][Section 3.1, Proposition 9])

□

We have the following functional equation for θ^4:

Corollary 3.18. We have

$$\theta\left(\frac{z}{4z+1}\right)^4 = (4z+1)^2\theta(z)^4.$$

Proof

To check this, it suffices to check that $\theta\left(\frac{z}{4z+1}\right) = \sqrt{4z+1}\theta(z)$ as the result follows by taking the fourth power. We have

$$\theta\left(\frac{z}{4z+1}\right) = \theta\left(-\frac{1}{-4-\frac{1}{z}}\right)$$
$$= \theta\left(-\frac{1}{4(-\frac{1}{4z}-1)}\right)$$
$$= \sqrt{2\frac{\frac{1}{(-4z)}-1}{i}}\theta\left(\frac{1}{4z}-1\right)$$
$$= \sqrt{2i\left(\frac{1}{4z}+1\right)}\theta\left(\frac{1}{4z}-1\right),$$

Now, recall that θ satisfies $\theta(z+1) = \theta(z)$, so we finally have

$$\theta\left(\frac{z}{4z+1}\right) = \sqrt{2i(\frac{1}{4z}+1)}\theta\left(\frac{1}{4z}\right)$$
$$= \sqrt{2i(\frac{1}{4z}+1)}\sqrt{\frac{2z}{i}}\theta(z)$$
$$= \sqrt{2i(\frac{1}{4z}+1)\cdot\frac{2z}{i}}\theta(z)$$

$$= \sqrt{4z+1}\theta(z)$$

([5][Corollary 6.0.12])

□

Since the set $\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\}$ does not generate all of $SL_2(\mathbb{Z})$, we can conclude that θ^4 is indeed not weakly modular of weight 2 with respect to $SL_2(\mathbb{Z})$, so θ^4 is not a modular form of weight 2 with respect to $SL_2(\mathbb{Z})$. We do, however, see that these functional equations hold for the subgroup generated by $\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\}$, and we will later define modular forms with respect to subgroups of $SL_2(\mathbb{Z})$.

3.3 Eisenstein Series

We have only presented some trivial examples of modular forms with respect to $SL_2(\mathbb{Z})$, but now we will present the Eisenstein series, which will be shown to be modular forms. These will play an important role in our analysis of modular forms and θ^4 later in the thesis.

Definition 3.19. (Eisenstein Series)
Let $k \geq 3$ be an integer. **The Eisenstein series of weight** k is a function $G_k : \mathbb{H} \to \mathbb{C}$ with

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^k}$$

Remark 3.20.
We note that for odd k we will have $G_k(z) = 0$ for all z as the contribution from $(-m, -n)$ to the sum will cancel out the one from (m, n).

Definition 3.21. (Riemann Zeta Function)
The **Riemann zeta function** is defined to be

$$\zeta(z) = \sum_{n\in\mathbb{Z},n>0} n^{-z}.$$

This series is absolutely convergent in $\{z \in \mathbb{C} \mid Re(z) > 1\}$ and in $\{z \in \mathbb{R} \mid z > 1\}$.
Another expression of the Riemann zeta function on the natural numbers is by the Bernoulli numbers

$$\zeta(2k) = (-1)^{k-1} B_{2k} \frac{(2\pi)^{2k}}{(2k-1)!}.$$

The Bernoulli numbers are defined by the generating function

$$\sum_{k=0}^{\infty} \frac{B_k x^k}{k!} = \frac{x}{e^x - 1}$$

Now, we wish to show that the Eisenstein series is a modular form of weight k for $k \geq 3$. For this, we need to show that: *(1) The Eisenstein series is a weakly modular function of weight k. That is, it satisfies the*

transformation equations in the definition.
(2) The Eisenstein series is holomorphic on $\mathbb{H}$.
(3) The Eisenstein series is holomorphic at infinity.

Lemma 3.22. The Eisenstein series G_k is weakly modular of weight k for $k \geq 3$.

Proof
We need to show $G_k(z+1) = G_k(z)$ and $G_k(-\frac{1}{z}) = z^k G_k(z)$. Clearly $G_k(z+1) = G_k(z)$ as

$$\begin{aligned} G_k(z+1) &= \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m(z+1)+n)^k} \\ &= \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n+m)^k}, \end{aligned}$$

and by setting $n = n + m$, we get the equivalent series for $G_k(z)$.
For the second part, we have

$$\begin{aligned} G_k\left(-\frac{1}{z}\right) &= \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(-\frac{m}{z}+n)^k} \\ &= (-z)^k \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m+nz)^k} \\ &= (-z)^k \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^k} \\ &= (-z)^k G_k(z). \end{aligned}$$

For odd k, we have $G_k(z) \equiv 0$ for all z, so the property is satisfied, and for even k, we have $(-z)^k = z^k$, which again ensures that the property is satisfied.

□

Now define the t'th partial sum of the Eisenstein series by

$$f_t(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0),|m|<t,|n|<t} \frac{1}{(mz+n)^k}.$$

We wish to show that the sequence of partial sums $\{f_t\}$ converge uniformly to $G_k(z)$ on every compact set of $\mathbb{H}$. Since $f_t(z)$ is clearly holomorphic on $\mathbb{H}$ for any finite t, it will then follow that G_k is holomorphic on $\mathbb{H}$ by Theorem A.21 as we will have the uniform convergence $\{f_t\} \to G_k$ as $t \to \infty$. The following is based on [4][Exercise 1.1.4] with hints found in the back of the book.

Lemma 3.23. The series

$$S = \sum_{(c,d)\in\mathbb{Z}^2\setminus(0,0)} (\sup\{|c|,|d|\})^{-k}$$

converges absolutely for $k \geq 3$.

Proof
We can do a substitution by considering the set $S_n = \{(c,d) \in \mathbb{Z}^2 \setminus (0,0) \mid \sup\{|c|,|d|\} = n\}$. That is,

$$\sum_{(c,d)\in\mathbb{Z}^2\setminus(0,0)} (\sup\{|c|,|d|\})^{-k} = \sum_{n=1}^{\infty} \frac{|S_n|}{n^k}.$$

Now, if $|d| = n$, then $-n \leq c \leq n$, so there are $2n+1$ possible values of c, and we have the double of that since if $|d| = n$, then both d and $-d$ are solutions. So this yields at least $4n+2$ solutions. Likewise if $|c| = n$ there are $4n$ solutions (we have already counted the end points $|d| = n$ and $|c| = n$), so in total we have $|S_m| = 8n + 2 < 8(n+1)$, and thus

$$\begin{aligned}\sum_{(c,d)\in\mathbb{Z}^2\setminus(0,0)} (\sup\{|c|,|d|\})^{-k} &= \sum_{m=1}^{\infty} \frac{|S_n|}{n^k} \\ &< 8\sum_{n=1}^{\infty} \frac{(n+1)}{n^k} \\ &= 8(\sum_{n=1}^{\infty} \frac{1}{n^{k-1}} + \sum_{n=1}^{\infty} \frac{1}{n^k}) \\ &= 8(\zeta(k-1) + \zeta(k)).\end{aligned}$$

Since $k \geq 3$, we have $k - 1 \geq 2$, so the zeta functions converges absolutely and so must their sum, and since the sum S is majorized by these, we must have that the sum converges. Now, since the terms in S are strictly positive, we must have that S converges absolutely by definition (Appendix A, section 4).

□

Lemma 3.24. Let A and B be positive real numbers and let

$$\Omega = \{z \in \mathbb{H} \mid |Re(z)| \leq A,\ Im(z) \geq B\}.$$

There exists a constant $C > 0$ such that $|z + \delta| > C \sup\{1, |\delta|\}$ for all $z \in \Omega$ and $\delta \in \mathbb{R}$.

Proof
We can split this into four cases:
1) $|\delta| < 1$.
2) $1 \leq |\delta| \leq 3A$ *and* $Im(z) > A$.
3) $1 \leq |\delta| \leq 3A$ *and* $B \leq Im(z) \leq A$.
4) $|\delta| > 3A$.

1):
We have

$$|z + \delta| \geq B = B \sup\{1, |\delta|\}$$

for all $z \in \Omega$.

2):
We have

$$|z + \delta| > A \geq \frac{1}{3}|\delta| = \frac{1}{3}\sup\{1, |\delta|\}$$

for all $z \in \Omega$.

3):
The quantity $|z+\delta|/|\delta|$ takes a non-zero minimum m, so we have

$$|z+\delta| \geq m|\delta| = m\sup\{1, |\delta|\}$$

for all $z \in \Omega$.

4):
We have

$$|z+\delta| \geq |\delta| - A \geq \frac{2}{3}|\delta| = \frac{2}{3}\sup\{1, |\delta|\}$$

for all $z \in \Omega$.

To conclude, we can use any positive C such that

$$0 < C < inf\left\{B, \frac{1}{3}, m\right\}.$$

□

For the next result, we note that we can write

$$G_k(z) = 2\zeta(k) + \sum_{m\in\mathbb{Z}\setminus\{0\}, n\in\mathbb{Z}} \frac{1}{(mz+n)^k}.$$

as for $m = 0$, we have the sum

$$\sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^k} = 2\sum_{n=1}^{\infty} \frac{1}{n^k} = 2\zeta(k).$$

The first equality follows for even k. The sum is summetric so for odd k it is 0.

Lemma 3.25. The Eisenstein series G_k is holomorphic on $\mathbb{H}$ for $k \geq 3$.

Proof
We write

$$G_k(z) = 2\zeta(k) + \sum_{m\in\mathbb{Z}\setminus\{0\}, n\in\mathbb{Z}} \frac{1}{(mz+n)^k}.$$

Now, for $m \neq 0$, we can write

$$|mz+n| = |m||z+\delta|,$$

where $\delta = \frac{n}{m}$. We have by Lemma 3.24 that there exists a constant $C > 0$ such that

$$|z+\delta| > C\sup\{1, |\delta|\}$$

for all $z \in \Omega$ and $\delta \in \mathbb{R}$, where $\Omega = \{z \in \mathbb{H} \mid |Re(z)| \leq A, Im(z) \geq B\}$. Therefore, we have

$$\begin{aligned} |m||z+\delta| &> C|m|\sup\{1, |\delta|\} \\ &= C\sup\{|m|, |n|\}, \end{aligned}$$

for all $z \in \Omega$. By taking the exponent $-k$, we then have

$$|m|^{-k}|z+\delta|^{-k} < C^{-k}|m|^{-k}(\sup\{1,|\delta|\})^{-k}$$
$$= C^{-k}(\sup\{|m|,|n|\})^{-k},$$

for all $z \in \Omega$. For the Eisenstein series, we then have

$$G_k = 2\zeta(k) + \sum_{m\in\mathbb{Z}\setminus\{0\}, n\in\mathbb{Z}} \frac{1}{(mz+n)^k}$$
$$= 2\zeta(k) + \sum_{m\in\mathbb{Z}\setminus\{0\}, n\in\mathbb{Z}} \frac{1}{|m|^k|z+\delta|^k}$$
$$< C \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} (\sup\{|m|,|n\})^{-k},$$

for all $z \in \Omega$. So in Ω, the Eisenstein series is majorized by the series from Lemma 3.23, which was shown to converge absolutely for $k \geq 3$, and since the series $S = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)}(\sup\{|m|,|d|\})^{-k}$ has only positive terms, we have by the Weierstrass M-test (Theorem A.20), that G_k must converge absolutely and uniformly on Ω. Now, since any compact subset of $\mathbb{H}$ is contained in some suitable Ω, we must have that G_k converges absolutely and uniformly on any compact subset of $\mathbb{H}$. Since the partial sums f_t are holomorphic on $\mathbb{H}$ and has limit G_k as $t \to \infty$, It follows by Theorem A.21 that G_k is holomorphic on $\mathbb{H}$.

□

Corollary 3.26. The Eisenstein series, $G_k(z)$, converges absolutely for $k \geq 3$ on $\mathbb{H}$

Proof
Since $G_k(z)$ converges absolutely on $\Omega = \{z \in \mathbb{H} \mid |Re(z)| \leq A, Im(z) \geq B\}$ we can choose A and B such that Ω contains the closure of the fundamental domain $\bar{F}$, and G_k is weakly modular of weight k, so G_k must converge absolutely on all of $\mathbb{H}$, since $\bar{F}$ covers $\mathbb{H}$.

□

Now, we wish to show that the Eisenstein series is holomorphic at infinity for $k \geq 3$.

Lemma 3.27. For $k \geq 3$ the Eisenstein series, G_k, is holomorphic at infintiy and the value of G_k as $z \to i\infty$ is

$$\lim_{z\to i\infty} G_k(z) = 2\zeta(k)$$

for even k and

$$\lim_{z\to i\infty} G_k(z) = 0$$

for odd k.

Proof
By Riemann's removable singularity theorem (Theorem A.27), it suffices to check that G_k is bounded in some neighborhood of $i\infty$. By the previous Lemma we showed that G_k is bounded on $\Omega = \{z \in \mathbb{H} \mid |Re(z)| \leq A, Im(z) \geq B\}$. Now, since there are points $z \in \Omega$ that lies in a neighborhood of $i\infty$ ($\mathbb{H}$ is open and$i\infty$ is on the boundary), and since $G_k(z+1) = G_k(z)$, we must have that $G_k(z)$ is bounded in some neighborhood of $i\infty$ and thus $G_k(z)$ is holomorphic at infinity.
Now, since the series is absolutely convergent on $\mathbb{H}$, we can check its value at infinity by it's term by term limit. That is

$$G_k(i\infty) = \lim_{Im(z)\to\infty} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^k}$$

$$= \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \lim_{Im(z)\to\infty} \frac{1}{(mz+n)^k}$$
$$= \sum_{n\in\mathbb{Z}\setminus\{0\}} n^{-k}.$$

The last equality is due to the fact that the terms go to 0 for all $m \neq 0$, and the remaining terms $(0, n)$ form the series $\sum_{n\in\mathbb{Z}\setminus\{0\}} n^{-k}$.
Now, for odd k, the n'th and $-n$'th term will cancel out, so the sum will be 0. For even k however, we can rewrite this

$$\sum_{n\in\mathbb{Z}\setminus\{0\}} n^{-k} = 2 \sum_{n\in\mathbb{Z},n>0} n^{-k}$$
$$= 2\zeta(k),$$

and we are done.

□

Corollary 3.28.
The Eisenstein series of weight k, $G_k(z)$, is a modular form of weight k for $k \geq 3$.

Proof
For $k \geq 3$ the Eisenstein series is weakly modular of weight k, holomorphic on $\mathbb{H}$ and holomorphic at infinity and is therefore a modular form of weight k.

□

One can normalize the Eisenstein series by division with $2\zeta(k)$ to obtain a 1 in the constant term of the series. That is:

$$E_k(z) = \frac{G_k(z)}{2\zeta(k)}.$$

Another normalization that would prove useful is multiplying the series with $\frac{(k-1)!}{2(2\pi i)^k}$. We shall denote this

$$\mathbb{G}_k(z) = \frac{(k-1)!}{2(2\pi i)^k} G_k(z).$$

We will give explicit examples of these normalized series after we have presented the Fourier expansion of the Eisenstein series.

Chapter 4 | The Fourier Series of an Eisenstein Series

This chapter is based on [3][Section 2.2].
Recall that the Eisenstein series of weight k is a modular form of weight k, and that modular forms with respect to $SL_2(\mathbb{Z})$ has a Fourier expansion.
We will in this chapter derive the Fourier expansion of the Eisenstein series for any given $k \geq 4$, $k \in 2\mathbb{Z}$, and we will see in the next chapter that the coefficients in these Fourier expansions have number-theoretic applications.

Definition 4.1. (Divisor function)
The **divisor function** is the function

$$\sigma_k(n) = \sum_{d|n, d>0} d^k.$$

That is, for a given positive integer n, $\sigma_k(n)$ is the sum of all k-th powers of the positive divisors of n.

Theorem 4.2. For $k \geq 4$, $k \in 2\mathbb{Z}$, the Fourier expansion of $G_k(z)$ is

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

We will prove this, but first, we need to establish some identities of sums [8][Section 1.5]:

Lemma 4.3. We have

$$\pi cot(\pi z) = \sum_{n \in \mathbb{Z}} \frac{1}{z+n}, \ z \in \mathbb{C} \setminus \mathbb{Z}.$$

Proof
Let $L(z)$ and $R(z)$ denote the left hand side and the right hand side respectively. Both of these functions are meromorphic in $\mathbb{C}$, as their poles are located in all the integers, and they are both 1-periodic. In a neighborhood of 0, we have that the Laurent series of $L(z)$ is of the form $L(z) = \frac{1}{z} + h_1(z)$, where $h_1(z)$ is a holomorphic function that vanishes at 0. Since we can write

$$R(z) = \sum_{n \in \mathbb{Z}} \frac{1}{z+n} = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{1}{z+n} + \frac{1}{z-n},$$

we have that $R(z) = \frac{1}{z} + h_2(z)$, where h_2 also is a holomorphic function that vanishes at 0 due to the symmetry around 0. So we must have that $L - R$ is bounded in a neighborhood of 0 by Riemann's removable singularity theorem. By the periodicity of L and R, we must have that $L - R$ is bounded at each point $z \in \mathbb{Z}$.
Now, since both L and R are bounded away from the integers, since the integers are poles for these functions, we must have that $L - R$ is bounded. But $L - R$ is an entire function, as it is holomorphic on all of $\mathbb{C}$. Thus by Liouville's Theorem, we have that $L - R$ must be constant, and since both h_1 and h_2 vanish at 0, we must have

$$L - R = 0,$$

and thus $L = R$, which proves the Lemma. □

Lemma 4.4. We have

$$\pi cot(\pi z) = \pi - 2\pi i \sum_{m=0}^{\infty} e^{2\pi imz} = \pi - 2\pi i \sum_{m=0}^{\infty} q^m, \ z \in \mathbb{C} \setminus \mathbb{Z},$$

where $q = e^{2\pi iz}$.

Proof
Consider a small neighborhood of a point z_0. We can in a small neighborhood consider the square roots

$$q^{\pm 1/2} = exp(\pm \pi iz) = cos(\pi z) \pm isin(\pi z).$$

We have by definition of the cotangent

$$\begin{aligned} cot(\pi z) = \frac{cos(\pi z)}{\sin(\pi z)} &= \frac{2icos(\pi z)}{2i\sin(\pi z)} \\ &= \frac{i(q^{1/2} + q^{-1/2})}{q^{1/2} - q^{-1/2}} \\ &= \frac{i(q+1)}{q-1}. \end{aligned}$$

Now, since we work in a small neighborhood, $\frac{1}{q-1}$ is equal to the negative geometric series $-\sum_{m=0}^{\infty} q^m$, so we get

$$cot(\pi z) = \frac{i(q+1)}{q-1} = -i(q+1)\sum_{m=0}^{\infty} q^m = 1 - 2i\sum_{m=0}^{\infty} q^m,$$

and multiplying with π yields the wanted result.

□

Corollary 4.5. We have

$$\pi - 2\pi i \sum_{m=0}^{\infty} q^m = \sum_{n\in\mathbb{Z}} \frac{1}{z+n}, \ z \in \mathbb{C} \setminus \mathbb{Z}.$$

Proof
Follows by transitivity of the other Lemmas.

□

Now we are ready to prove Theorem 4.2:

Proof
We differentiate the equation in Corollary 4.5 $(k-1)$ times and obtain

$$(-1)^{k-1}(k-1)!\sum_{d\in\mathbb{Z}} \frac{1}{(z+d)^k} = -(2\pi i)^k \sum_{m=0}^{\infty} m^{k-1}q^m.$$

As for odd k, we have $G_k \equiv 0$, so we consider even k and we multiply through:

$$\sum_{d\in\mathbb{Z}} \frac{1}{(z+d)^k} = \frac{(2\pi i)^k}{(k-1)!} \sum_{m=0}^{\infty} m^{k-1}q^m.$$

Now we have for the Eisenstein series of weight k with k even:

$$\begin{aligned} G_k(z) &= 2\zeta(k) + \sum_{c\in\mathbb{Z}\setminus\{0\}} \sum_{d\in\mathbb{Z}} \frac{1}{(cz+d)^k} \\ &= 2\zeta(k) + 2\sum_{c=1}^{\infty} \sum_{d\in\mathbb{Z}} \frac{1}{(cz+d)^k} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{c=1}^{\infty} \sum_{m=0}^{\infty} m^{k-1} q^{cm}. \end{aligned}$$

Now, if we write $cm = N$ and use the fact that $m = 0$ yields a zero term in the series, which can be omitted, we then obtain

$$\begin{aligned} G_k(z) &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{c=1}^{\infty} \sum_{m=1}^{\infty} m^{k-1} q^{cm} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{N=1}^{\infty} \left(\sum_{m|N, m\geq 1} m^{k-1} \right) q^N, \end{aligned}$$

but the m-sum is exactly the divisor function $\sigma_{k-1}(N)$ (This argument is from the proof of Theorem 4.7 in [6]), so we finally get

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

□

With the Fourier expansion of the Eisenstein series and the expression of the Riemann zeta function by Bernoulli numbers, we see that

$$\begin{aligned} E_k(z) &= 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \\ \mathbb{G}_k(z) &= -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \end{aligned}$$

Example 4.6. The first 4 coefficients of $E_k(z)$ and $\mathbb{G}_k(z)$ for $k = 4, 6, 8, 10, 12, 14$ will now be given [6][Page 17]. The values B_k for the given k are $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$, $B_{14} = \frac{7}{6}$. Thus we get

$$\begin{aligned} E_4(z) &= 1 + 240q + 2160q^2 + 6720q^3 + \dots \\ E_6(z) &= 1 - 504q - 16632q^2 - 122976q^3 - \dots \\ E_8(z) &= 1 + 480q + 61920q^2 + 1050240q^3 + \dots \\ E_{10}(z) &= 1 - 264q - 135432q^2 - 5196576q^3 - \dots \\ E_{12}(z) &= 1 + \frac{65520}{691}q + \frac{134250480}{691}q^2 + \frac{11606736960}{691}q^3 + \dots \\ E_{14}(z) &= 1 - 24q - 196632q^2 - 38263776q^3 \dots, \end{aligned}$$

and

$$\mathbb{G}_4(z) = \frac{1}{240} + q + 9q^2 + 28q^3 + \dots$$

$$\begin{aligned}
\mathbb{G}_6(z) &= -\frac{1}{504} + q + 33q^2 + 244q^3 + \ldots \\
\mathbb{G}_8(z) &= \frac{1}{240} + q + 129q^2 + 2188q^3 + \ldots \\
\mathbb{G}_{10}(z) &= -\frac{1}{264} + q + 513q^2 + 19684q^3 + \ldots \\
\mathbb{G}_{12}(z) &= \frac{691}{65520} + q + 2049q + 177148q^3 + \ldots \\
\mathbb{G}_{14}(z) &= -\frac{1}{24} + q + 8193q + 1594324q^3 + \ldots
\end{aligned}$$

If we compare the coefficients of the given E_k in the example, it suggests the identities

$$\begin{aligned}
E_4(z)^2 &= E_8(z) \\
E_4(z)E_6(z) &= E_{10}(z) \\
E_6(z)E_8(z) &= E_4(z)E_{10}(z) \\
&= E_{14}(z).
\end{aligned}$$

We cannot however conclude that these identities hold by only comparing the coefficients. However, we will see in the next chapter that these identities do in fact hold, because of the dimensions of the corresponding spaces of modular forms.

Chapter 5 | The Space of Modular Forms

This chapter is based on [5] Now, Let $M_k(SL_2(\mathbb{Z}))$ denote the set of all modular forms of weight k with respect to $SL_2(\mathbb{Z})$, and we recall that for odd k we have $M_k = \{0\}$.

Proposition 5.1. $M_k(SL_2(\mathbb{Z}))$ is a vector space over $\mathbb{C}$ for all $k \in \mathbb{Z}$.

Proof
Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ and $f, g \in M_k(SL_2(\mathbb{Z}))$. Then we have

$$\begin{aligned}(f+g)(\gamma(z)) &= f(\gamma(z)) + g(\gamma(z)) \\ &= (cz+d)^k f(z) + (cz+d)^k g(z) \\ &= (cz+d)^k (f+g)(z)\end{aligned}$$

and since both f and g are holomorphic and holomorphic at infinity, the sum must also be holomorphic and holomorphic at infinity, and we have $(f+g) \in M_k(SL_2(\mathbb{Z}))$.
Also, we have for $m \in \mathbb{C}$

$$\begin{aligned}(mf)(\gamma(z)) &= mf(\gamma(z)) \\ &= m(cz+d)^k f(z) \\ &= (cz+d)^k (mf)(z)\end{aligned}$$

Which is again a modular form of weight k.

□

Recall that the **order of vanishing** for a holomorphic function f at a point z_0, denoted $ord_{z_0}(f)$ is the maximum integer n such that we can write

$$f(z) = g(z)(z - z_0)^n$$

for g holomorphic.

Lemma 5.2. The order of vanishing is a valuation. That is, we can write for holomorphic functions f, g at a point z_0

$$\begin{aligned}ord_{z_0}(f \cdot g) &= ord_{z_0}(f) + ord_{z_0}(g) \\ ord_{z_0}(f+g) &\leq ord_{z_0}(f) + ord_{z_0}(g),\end{aligned}$$

where $ordz_0(f+g) = ord_{z_0}(f) + ord_{z_0}(g)$ if and only if $ord_{z_0}(f) = ord_{z_0}(g) = 0$.

Proof
Let f, g be holomorphic functions with $ord_{z_0}(f) = n$ and $ord_{z_0}(g) = m$. Then

$$\begin{aligned}f(z) &= v(z)(z - z_0)^n \\ g(z) &= w(z)(z - z_0)^m\end{aligned}$$

with v, w holomorphic. Then

$$f(z) \cdot g(z) = v(z)w(z)(z - z_0)^{n+m}$$

and we must have the product $v(z)w(z)$ is holomorphic. Since $u(z) = v(z)w(z)$ has a finite limit that exists, we must have $n + m$ to be the maximum integer for $f \cdot g$ such that $f \cdot g = u(z)(z - z_0)^{m+n}$.
Now, since

$$\begin{aligned} f(z) + g(z) &= v(z)(z - z_0)^n + w(z)(z - z_0)^m \\ &= (v(z) + w(z)(z - z_0)^{m-n})(z - z_0)^n \\ &= (v(z)(z - z_0)^{-m} + w(z)(z - z_0)^{-n})(z - z_0)^{n+m} \end{aligned}$$

Now, since $v(z)$ and $w(z)$ are both holomorphic with order of vanishing 0, we must have that the right hand side goes to infinity for $m, n > 0$, so $ord_{z_0}(f + g) < ord_{z_0}(f) + ord_{z_0}(g)$, but for $m = n = 0$ the right hand side is finite and exists, and we have

$$ord_{z_0}(f + g) = 0 = ord_{z_0}(f) + ord_{z_0}(g),$$

and we conclude

$$ord_{z_0}(f + g) \leq ord_{z_0}(f) + ord_{z_0}(g).$$

□

Lemma 5.3. Let f be a modular form of weight k and $\gamma \in SL_2(\mathbb{Z})$. If $q \in \mathbb{H}$ and $p = \gamma(q) = \frac{az+b}{cz+d}$ we have $ord_p(f) = ord_q(f)$. That is, we have a well-defined value $ord_t(f)$ for $t \in \mathbb{H}/SL_2(\mathbb{Z})$.

Proof
Since for a modular form, we have $f(\gamma(z)) = (cz + d)^k f(z)$ and since $ord_p(cz + d) = 0$, we have by the property $ord_{z_0}(f \cdot g) = ord_{z_0}(f) + ord_{z_0}(g)$, we have

$$ord_{\gamma(p)}(f) = ord_p(f) + ord_p(cz + d) = ord_p(f),$$

which proves the lemma.

□

For our next result, we now recall from chapter 2 that the fundamental domain of $\mathbb{H}$ under the group action of $SL_2(\mathbb{Z})$ is $F = \left\{z \in \mathbb{H} \mid |Re(z)| < \frac{1}{2},\ |z| > 1\right\}$. For any point $z \in F$, the stabilizer of this group action only contains I_2. If we include the boundary, we see that the same is true for all points except for the points $z = i$ and $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, as we have $S(i) = \frac{-1}{i} = \frac{i}{i(-i)} = i$ and $ST(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) = \frac{-1}{-\frac{1}{2} + \frac{\sqrt{3}}{2}i + 1} = \frac{-1}{\frac{1}{2} + \frac{\sqrt{3}}{2}i} = \frac{-\frac{1}{2} + \frac{\sqrt{3}}{2}i}{|\frac{\sqrt{3}}{2}i - \frac{1}{2}|^2} = \frac{\sqrt{3}}{2}i - \frac{1}{2}$.
If we denote e_p as the **order of the stabilizer** of a point $p \in \mathbb{H}$, then by the above, we have $e_p = 1$ for all $z \neq i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and since the order of S is 2 in $PSL_2(\mathbb{Z})$ (recall that the group actions by fractional linear transformations of $SL_2(\mathbb{Z})$ and $PSL_2(\mathbb{Z})$ are equivalent ($\pm\gamma$ act equivalent on $\mathbb{H}$)) and order of ST is 3 in $PSL_2(\mathbb{Z})$, so $e_i = 2$ and $e_{\frac{1}{2}(-1+\sqrt{3}i)} = 3$.
With that in mind, we are ready for the next result:

Theorem 5.4. For a non-zero modular form of weight k with respect to $SL_2(\mathbb{Z})$, we have

$$ord_\infty(f) + \sum_{p \in \mathbb{H}/SL_2(\mathbb{Z})} \frac{1}{e_p} ord_p(f) = \frac{k}{12}.$$

Proof
To prove this, we shall integrate the function $\frac{d}{dz}log(f(z)) = \frac{f'(z)}{f(z)}$. We first note, that since f is a non-zero modular form, there is some neighborhood of $i\infty$ where it has no zeroes. We shall call this neighborhood N. These zeroes are exactly the poles of $\frac{f'(z)}{f(z)}$ and the residue of $\frac{f'(z)}{f(z)}$ is the multiplicity of these zeroes. Now we define the domain $D = \bar{F} \setminus N$. This domain is closed and bounded in the imaginary direction for some sufficiently small $\epsilon > 0$ such that for $z \in D$, $Im(z) \leq Y = \epsilon^{-1}$. So D is compact and f must then have finitely many zeroes in D. We will compute the integral $\int_{\delta D} \frac{f'(z)}{f(z)} dz$ to show the result.
Now, let $A = \frac{1}{2}(-1 + \sqrt{3}i)$, $B = i$ and $C = \frac{1}{2}(1 + \sqrt{3}i)$. If there are poles on the boundary other than A, B and C they will come in pairs which are reflections about the real axis. We can then simply integrate along semicircles of them and take the limit as the radius approaches 0, and we note that $\frac{f'(z)}{f(z)}$ has the same residue at both points as $f(z) = f(z+1)$ and $f(-\frac{1}{z}) = z^k f(z)$.
Now, if there is a pole at B, we can replace the contour going through B by a circle of small radius going around B and in the limit that radius goes to 0, the circle approaches a half-circle and the integration along around it is

$$\frac{1}{2} Res_B \left(\frac{f'(z)}{f(z)} \right) = \frac{1}{2} ord_B(f).$$

Next, we know that there is a pole at A if and only if there is a pole at C, as $f(z) = f(z+1)$. If we do the analogous with A and C, we see that in the limit that radius goes to 0, the circles approach $\frac{1}{6}$ of a circle. Hence together the two points contribute

$$\frac{1}{6} Res_A \left(\frac{f'(z)}{f(z)} \right) + \frac{1}{6} Res_C \left(\frac{f'(z)}{f(z)} \right) = \frac{1}{3} Res_A \left(\frac{f'(z)}{f(z)} \right) = \frac{1}{3} ord_A(f).$$

Using Cauchy's residue theorem and adding the poles inside the contour, we get that

$$\int_{\delta D} \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{p \in \mathbb{H}/SL_2(\mathbb{Z})} \frac{1}{e_p} ord_p(f).$$

It just remains to show that this integral also equals $2\pi i(-ord_\infty(f) + \frac{k}{12})$.
Now let $G = \frac{1}{2} + iY$ and $E = -\frac{1}{2} + iY$ with Y defined as previously. Now, we rewrite δD as the union of continuously differentiable curves CG, GE, EA, AB, BC. Then we observe that

$$\int_{EG} \frac{f'(z)}{f(z)} dz = 2\pi i ord_\infty(f),$$

because when we transform the upper half plane to the unit circle by the logarithm, the EG travels around the origin exactly once and since the residues in the other residues in the region are zero, we obtain $\int_{EG} \frac{f'(z)}{f(z)} dz = 2\pi i Res_\infty \left(\frac{f'(z)}{f(z)} \right) = 2\pi i ord_\infty(f(z))$ and since GE has the opposite orientation, we get a change of sign in the integral.
What remains to show is that $\int_{EA,AB,BC,CG} \frac{f'(z)}{f(z)} dz = 2\pi i \frac{k}{12}$. First, observe that since $f(z) = f(z+1)$, we have

$$\int_{EA} \frac{f'(z)}{f(z)} dz = -\int_{GC} \frac{f'(z)}{f(z)} dz$$

as they have opposite orientation, and so

$$\int_{EA,CG} \frac{f'(z)}{f(z)} dz = 0.$$

Now, since $f(-\frac{1}{z}) = z^k f(z)$, we can use the change of variable $y = -\frac{1}{z}$ and we obtain

$$\begin{aligned}\int_A^B \frac{f'(z)}{f(z)} dz &= \int_A^B \frac{kz^{k-1} f(-\frac{1}{z}) + z^k f'(-\frac{1}{z})}{z^k f(-\frac{1}{z})} \frac{1}{z^2} dz \\ &= \int_C^B \frac{f'(y)y^k - ky^{k-1} f(y)}{y^k f(y)} dy \\ &= \int_C^B \frac{f'(y)}{f(y)} + \int_B^C -k\frac{1}{y} dy\end{aligned}$$

Therefore,

$$\begin{aligned}\int_{AB,BC} \frac{f'(z)}{f(z)} dz &= \int_B^C \left[\frac{f'(y)}{f(y)} - \frac{f'(y)}{f(y)} + \frac{k}{y}\right] dy \\ &= k \int_B^C \frac{dy}{y} \\ &= \int_{\frac{i\pi}{3}}^{\frac{i\pi}{2}} k dz \\ &= 2\pi i \frac{k}{12}\end{aligned}$$

as was wanted. So to sum up, we have

$$\int_{\delta D} \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{p \in \mathbb{H}/SL_2(\mathbb{Z})} \frac{1}{e_p} ord_p(f) = 2\pi i(-ord_\infty(f) + \frac{k}{12}),$$

and therefore

$$ord_\infty(f) + \sum_{p \in \mathbb{H}/SL_2(\mathbb{Z})} \frac{1}{e_p} ord_p(f) = \frac{k}{12}.$$

□

Corollary 5.5. The dimension of $M_k(SL_2(\mathbb{Z}))$ for even $k \in \mathbb{N}$ is

$$dim(M_k(SL_2(\mathbb{Z}))) \leq \begin{cases} \lfloor \frac{k}{12} \rfloor + 1 & k \not\equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor & k \equiv 2 \mod 12 \end{cases}$$

Proof

Let $m = \lfloor \frac{k}{12} \rfloor + 1$ and choose m distinct point in $p_1, \ldots, p_m \in \mathbb{H}/SL_2(\mathbb{Z})$ that are not in the same orbit as i and $\frac{1}{2}(\pm 1 + \sqrt{3}i)$. Given any $m+1$ modular forms $f_1, \ldots, f_{m+1}$ we can find a linear combination f, which vanishes in all of the p_i's, but then f must be the zero-function by definition, since $m > \frac{k}{12}$ and the f_i must form a linearly dependent set. Hence $dim(M_k) \leq m$.
If $k \equiv 2 \mod 12$, we notice, that the only way to satisfy $ord_\infty(f) + \sum_{p \in \mathbb{H}/SL_2(\mathbb{Z})} \frac{1}{e_p} ord_p(f) = \frac{k}{12}$ is to have at

least a zero of multiplicity 1 at i and a zero of multiplicity 2 at $\frac{1}{2}(-1+\sqrt{3}i)$ yielding a contribution of $\frac{1}{2}+\frac{2}{3}=\frac{7}{6}$ to the orders at p and thus together with

$$\frac{k}{12}-\frac{7}{6}=m-1$$

zeroes, we get $dim(M_k) \leq m-1$.

□

5.1 The function space of cusp forms

Let $M_k^0(SL_2(\mathbb{Z}))$ denote the set of cusp forms of weight k.

Proposition 5.6. $M_k^0(SL_2(\mathbb{Z}))$ is a vector space over $\mathbb{C}$ for all $k \in \mathbb{Z}$.

Proof
A cusp form is also a modular form, so the sum and product of two cusp forms satisfy the transformational equation of modular forms and are still holomorphic on $\mathbb{H}$ and at infinity. What differs is, that cusp forms have $a_0 = 0$ in their Fourier expansion at ∞.
Then we must have that for $f, g \in M_k^0$ with Fourier expansion at $\hat{f}(q) = \sum_{n=-\infty}^{\infty} a_n q^n, \hat{g}(q) = \sum_{n=-\infty}^{\infty} b_n q^n$ at infinity, that $a_0 = b_0 = 0$ and so $a_0 + b_0 = 0$, as we sum and match appropriate terms of each Fourier expansion. Also for $m \in \mathbb{C}$, we get $ma_0 = 0$. So $M_k^0(SL_2(\mathbb{Z}))$ is indeed a vector space over $\mathbb{C}$.

□

Now, denote $\Delta = 60^3(G_4(z))^3 - 27 \cdot 140^2(G_6(z))^2$.

Lemma 5.7. $\Delta \in M_{12}^0(SL_2(\mathbb{Z}))$.

Proof
Clearly $(G_4(z))^3$ is a modular form of weight $3 \cdot 4 = 12$ as

$$\left(G_4\left(-\frac{1}{z}\right)\right)^3 = (z^4 G_4(z))^3 = z^{12}(G_4(z))^3,$$

and

$$(G_4(z+1))^3 = (G_4(z))^3,$$

and the product of three holomorphic functions is still holomorphic by the product rule and linearity of differentiation. The same can be observed for $(G_6(z))^2$ and this is indeed also a modular form of weight 12.
So Δ is a modular form of weight 12, so all that is left to check, is that it's value at ∞ is 0. That is,

$$\begin{aligned}\Delta(\infty) &= 60^3(G_4(\infty))^3 - 27 \cdot 140^2(G_6(\infty))^2 \\ &= 60^3(2\zeta(4))^3 - 27 \cdot 140^2(2\zeta(6))^2 \\ &= 60^3\left(\frac{\pi^4}{45}\right)^3 - 27 \cdot 140^2\left(\frac{2\pi^6}{945}\right)^2 \\ &= 0\end{aligned}$$

So $\Delta \in M_{12}^0(SL_2(\mathbb{Z}))$.

□

5.2 Characterizations of the space of modular forms

From this section and forward, we denote $M_k(SL_2(\mathbb{Z})) = M_k$ and only use the other notation, where the matrix group is not obvious.

Corollary 5.8. For $k < 0$, we have $M_k = 0$ (the space containing only the zero-function).

Proof
By Theorem 5.4, we must have $ord_p(f) < 0$ or $ord_\infty(f) < 0$, however, since any $f \in M_k$ is holomorphic on $\mathbb{H}$ and holomorphic at infinity, we cannot by definition have a negative order of vanishing.

□

Corollary 5.9. $M_2 = 0$.

Proof
This follows immediately from Corollary 5.5 as $dim(M_2) \leq 0$, and by definition of dimension of a vector space, we must have $dim(M_2) = 0$.

□

Recall that for a point x_0 and a function f, a functional is a mapping from a function to an evaluation of a function, that is $f \mapsto f(x_0)$.

Lemma 5.10. For $k \in 2\mathbb{Z}$, if $M_k^0 \neq 0$, then $M_k \cong M_k^0 \bigoplus \mathbb{C} \cdot G_k$.

Proof
Define the functional $\xi : M_k \to \mathbb{C}$ by $\xi(f) = f(i\infty)$. This map is linear as $\xi(f+g) = f(i\infty) + g(i\infty)$ and $\xi(c \cdot f) = cf(i\infty)$. By definition, we must have M_k^0 is the elements that map ξ to 0, since for $f \in M_k^0$, we have $\xi(f) = f(i\infty) = 0$. In the case where $M_k^0 \neq 0$, we have since $dim(Range(\xi)) = 1$, as $Range(\xi) = \mathbb{C}$ and $dim(\mathbb{C}) = 1$. The fact that $Range(\xi) = \mathbb{C}$ is due to M_k being closed under scalar multiplication, and thus ξ is surjective. Thus by rank nullity, we have

$$dim(M_k) = 1 + dim(M_k^0).$$

Now since $G_k \notin M_k^0$, as $G_k(i\infty) = 2\zeta(k) \neq 0$ for all $k > 0$, $k \in 2\mathbb{Z}$, we can generate M_k by linear combination of the basis of M_k^0 and $\mathbb{C}G_k$, and we have $M_k \cong M_k^0 \bigoplus \mathbb{C}G_k$.

□

Lemma 5.11. We have $M_{k-12} \cong M_k^0$. That is, there exists an isomorphism $\nu : M_{k-12} \to M_k^0$ defined by $f \mapsto \Delta \cdot f$.

Proof
Clearly the map $\nu : M_{k-12} \to M_k^0$ is well-defined by $f \mapsto \Delta \cdot f$, as the product of a modular form and a cusp form, must be a cusp form, as this termwise corresponds to a zero-constant term in the Fourier expansion of the product, and the product is thus a cusp form of weight $k - 12 + 12 = k$, so the $Range(\nu) = M_k^0$.
By Theorem 5.4, we have $ord_\infty(\Delta) + \sum_{p \in \mathbb{H}/SL_2(\mathbb{Z})} \frac{1}{e_p} ord_p(\Delta) = 1$, and since Δ has a zero at infinity, as it is a cusp form, it cannot have any other zeroes by this equation. Therefore, we can define an inverse map by division $\eta : M_k^0 \to M_{k-12}$, $g \mapsto \frac{g}{\Delta}$. This map is again well-defined, as for any $g \in M_k^0$, we have $g(\infty) = 0$, and since Δ has a zero of order 1 at infinity, $\frac{g}{\Delta}$ cannot have a pole at infinity. Furthermore, since Δ is holomorphic

and non-vanishing on $\mathbb{H}$ (it has no zeroes on $\mathbb{H}$), we must have that $\frac{g}{\Delta}$ is also holomorphic on $\mathbb{H}$. Therefore $\frac{g}{\Delta}$ is holomorphic on $\mathbb{H}$, holomorphic at infinity and is the quotient of two modular forms. Hence $\frac{g}{\Delta}$ is a modular form of weight $k-12$.
Now, since ν and η are mutual inverse maps and each of them are bijective, we must have, that ν defines an isomorphism.

□

Theorem 5.12. We have the following:
1. For odd k, $k<0$ and $k=2$, we have $M_k = 0$.
2. For $k=0$, we have $M_k \cong \mathbb{C}$.
3. For $k=4,6,8,10$, we have $M_k \cong \mathbb{C}\cdot G_k$.
4. For $k \geq 12$, we have $M_k \cong \mathbb{C}\cdot G_k \bigoplus \Delta \cdot M_{k-12}$.

Proof
1. This is already proved throughout the project.

2. We know that any modular form must be holomorphic on $\mathbb{H}$, holomorphic at infinity and satisfy $f(-\frac{1}{z}) = z^k f(z)$, $f(z+1) = f(z)$. We know that $dim(M_0) \leq 1$ by Corollary 5.5, but we have already shown that the constant functions are modular forms of weight 0. So we get $M_0 \cong \mathbb{C}$.

3. For $k=4,6,8,10$, we know that $\dim(M_k) \leq 1$ by Corollary 5.5, but since we know that G_k are non-zero modular forms, we must have $dim(M_k) = 1$ and $M_k \cong \mathbb{C}\cdot G_k$.

4. For $k \geq 12$, we have from Lemma 5.11 that $M_k^0 \cong \Delta \cdot M_{k-12}$, and from Lemma 5.10, we know that there is only 1 linearly independent non-cusp form by the rank nullity. This non-cusp form is G_k, as for $k>0$, $k \in 2\mathbb{Z}$, we have $\zeta(k) \neq 0$. Thus we must have by combination of the two Lemma's that

$$M_k \cong \mathbb{C}\cdot G_k \bigoplus \Delta \cdot M_{k-12}.$$

□

Corollary 5.13. For $k>0$, we have

$$dim(M_k) = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor + 1 & k \equiv 0,4,6,8,10 \mod 12 \\ 0 & otherwise \end{cases}$$

Proof
Theorem 5.12 tells us that this is true for $0<k<12$. By recursion, we see that the dimension counting must hold, as we have

$$M_k \cong \mathbb{C}\cdot G_k \bigoplus \Delta \cdot M_{k-12} \cong \mathbb{C}\cdot G_k \bigoplus \Delta(\mathbb{C}\cdot G_{k-12} \bigoplus \Delta M_{k-24}) \cong ....$$

Thus with each recursive step, we see that for any $k = m + 12n$, we have that the dimension increases by 1, when n increases by 1. □

Corollary 5.14. For $k \geq 0$, the set $\left\{E_4^a E_6^b \mid a,b \geq 0, 4a+6b=k\right\}$ is a basis of M_k.

Proof
Since $M_k = 0$ for odd k, we may assume k is even.
Let N_k be the number of solutions to $4a + 6b = k$ in non-negative integers a and b. By a direct check, we see that $N_k = dim(M_k)$ for $k \leq 12$, as $N_0 = 1$, $N_2 = 0$, $N_4 = 1$, $N_6 = 1$, $N_8 = 1$, $N_{10} = 1$, $N_{12} = 2$. Now, since $N_k = 1 + N_{k-12}$ for all k, and since the dimension of the space of modular forms follow the same pattern, we must have $N_k = dim(M_k)$ for all $k \geq 0$. So the proposed basis has the correct size.
What remains to show is that the set is linearly independent. To show this, we may assume $k \geq 14$. Let

$$\sum_{4a+6b=k,a,b\geq 0} c_{a,b} E_4(z)^a E_6(z)^b = 0$$

for all $z \in \mathbb{H}$. If there is a pure $E_4(z)$ term, say $c_{A,0}E_4(z)^A$, then setting $z = i$, we obtain

$$c_{A,0}E_4(i)^A = 0,$$

since $E_6(i) = 0$, as for any modular form of weight 6, we have $f\left(-\frac{1}{z}\right) = z^6 f(z)$, and thus $f(i) = f\left(-\frac{1}{i}\right) = i^6 f(i) = -f(i)$, which implies $f(i) = 0$.
However $E_4(i) > 0$, so we must have $c_{A,0} = 0$. Therefore all non-zero terms in the sum have $b \geq 1$. Division by $E_6(z)$ gives

$$\sum_{4a+6b=k,a,b\geq 0} c_{a,b} E_4(z)^a E_6(z)^{b-1} = 0.$$

Continuing this procedure then gives that the remaining coefficients must be 0 by induction. Hence the set is linearly independent.

□

5.3 Identities of divisor functions using Eisenstein series

This section is based on [3][Section 2.2.1] and the identities of divisor functions not shown in the reference are done by hand by yours truly.
Now given Corollary 5.14 we know that any modular form of positive, even weight k can be written as some linear combination of $E_4(z)^a$ and $E_6(z)^b$ with $4a + 6b = k$. In chapter 5.3 we suggested the identities

$$\begin{aligned} E_4(z)^2 &= E_8(z) \\ E_4(z)E_6(z) &= E_{10}(z) \\ E_6(z)E_8(z) &= E_4(z)E_{10}(z) \\ &= E_{14}(z), \end{aligned}$$

by comparing the first few coefficients of these series. We now know that the dimensions of M_8, M_{10} and M_{14} are all 1, so since $E_4(z)^2$ is a modular form of weight 8 and so is $E_8(z)$, they must be linearly dependent. That is, they must be scalar multiples of one another, and thus since the first few coefficients are equivalent, they must all be, such that the identity holds. The same argument can be used for the other two identities.
Now, let's look at the first relation and insert the Fourier expression of $E_4(z)$ and $E_8(z)$:

$$\begin{aligned} E_4(z)^2 &= (1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m)^2 \\ &= 1 + 2 \sum_{m=1}^{\infty} [240^2 \sum_{i=1}^{m-1} \sigma_3(i)\sigma_3(m-i) q^m] + 240\sigma_3(m) q^m \end{aligned}$$

$$E_8(z) = 1 + 480 \sum_{m=1}^{\infty} \sigma_7(m) q^m$$

Looking at the n'th term and cancelling out the constant term of 1 and the powers of q, we get

$$480\sigma_7(n) = 57600[\sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)] + 480\sigma_3(n)$$

Equivalently, we obtain

$$\frac{\sigma_7(n) - \sigma_3(n)}{120} = \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Using the same method for the other Eisenstein relations we obtain:

$$\sum_{m=1}^{n-1} \sigma_5(m)\sigma_3(n-m) = \frac{264}{120960}\sigma_9(n) + \frac{1}{504}\sigma_3(n) - \frac{1}{240}\sigma_5(n)$$
$$\sum_{m=1}^{n-1} \sigma_3(m)\sigma_9(n-m) = \frac{\sigma_{13}(n) - 11\sigma_9(n) + 10\sigma_3(n)}{2640}$$

More relations between the Eisenstein series can be found for higher k even though the corresponding space M_k is not of dimension 1. For example, the space M_{12} is 2-dimensional and contains the three modular forms $E_4(z)E_8(z)$, $E_6(z)^2$ and E_{12}. By comparing the first 4 coefficients in the Fourier expression of E_4, E_6, E_8 and E_{12} in Example 4.6, we find the relation

$$441E_4(z)E_8(z) + 250E_6(z)^2 = 691E_{12}(z).$$

We will now derive an identity for the corresponding sums of divisor functions. We have

$$\begin{aligned}
E_4(z)E_8(z) &= (1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m)(1 + 480 \sum_{m=1}^{\infty} \sigma_7(m) q^m) \\
&= 1 + \sum_{m=1}^{\infty} \left[\sum_{i=1}^{m-1} 240 \cdot 480 \sigma_3(i)\sigma_7(m-i) q^m \right] + q^m(240\sigma_3(m) + 480\sigma_7(m)) \\
E_6(z)^2 &= (1 - 504 \sum_{m=1}^{\infty} \sigma_5(m) q^m)^2 \\
&= 1 + 2 \sum_{m=1}^{\infty} \left[\sum_{i=1}^{m-1} 504^2 \sigma_5(i)\sigma_5(m-i) q^m \right] - 504\sigma_5(m) q^m
\end{aligned}$$

So we have

$$\begin{aligned}
441E_4(z)E_8(z) + 250E_6(z)^2 = 691 + \sum_{m=1}^{\infty} [\sum_{i=1}^{m-1} &\left[441 \cdot 240 \cdot 480 \sigma_3(i)\sigma_7(m-i) q^m + 2 \cdot 250 \cdot 504^2 \sigma_5(i)\sigma_5(m-i)\right] q^m \\
&+ 441 q^m(240\sigma_3(m) + 480\sigma_7(m)) - 250 q^m(1008\sigma_5(m))] \\
&= 691E_{12}
\end{aligned}$$

$$= 691 + 65520 \sum_{m=1}^{\infty} \sigma_{11}(m) q^m$$

Now, eliminating the q's and seeing that all the constant terms cancel out due to $441 + 250 = 691$, we get at the n'th term

$$65520\sigma_{11}(n) = 50803200 \sum_{m=1}^{n-1} [\sigma_3(m)\sigma_7(n-m)] + 127008000 \sum_{m=1}^{n-1} [\sigma_5(m)\sigma_5(n-m)]$$
$$+ 105840\sigma_3(n) + 211680\sigma_7(n) - 252000\sigma_5(n).$$

Equivalently, the relation is

$$\frac{65520\sigma_{11}(n) - 105840\sigma_3(n) - 211680\sigma_7(n) + 252000\sigma_5(n)}{25401600} = \sum_{m=1}^{n-1} \left[2\sigma_3(m)\sigma_7(n-m) + 5\sigma_5(m)\sigma_5(n-m)\right].$$

Chapter 6 | Congruence subgroups of $SL_2(\mathbb{Z})$

This chapter is based on [4][Section 1.2] We have presented and analysed modular forms on $SL_2(\mathbb{Z})$ of weight k, but we will now define modular forms on subgroups of $SL_2(\mathbb{Z})$. Specifically, we shall discuss subgroups containing matrices of $SL_2(\mathbb{Z})$ that satisfy certain arithmetic congruences in the entries of these matrices. We shall start by defining the principal subgroup of level N:

Definition 6.1. (Principal subgroup of level N)
The **principal subgroup of level** N is denoted

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

where the congruence modulo N is taken entry-wise.

Lemma 6.2. $\Gamma(N)$ is the kernel of the surjective homomorphism $\phi : \; SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} [a] & [b] \\ [c] & [d] \end{bmatrix}$.

Proof
This is a homomorphism as for $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in SL_2(\mathbb{Z})$ since

$$\phi(AB) = \begin{bmatrix} [a'a + c'b] & [b'a + d'b] \\ [a'c + c'd] & [b'c + d'd] \end{bmatrix} = \begin{bmatrix} [a'][a] + [c'][b] & [b'][a] + [d'][b] \\ [a'][c] + [c'][d] & [b'][c] + [d'][d] \end{bmatrix} = \phi(A)\phi(B).$$

We will show that this map is surjective.
Let $[\gamma] = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$ and let $\gamma = \begin{bmatrix} a + eN & b + fN \\ c & d + gN \end{bmatrix} = \begin{bmatrix} a' & b' \\ c & d' \end{bmatrix} \in M_2(\mathbb{Z})$, where $e, f, g \in \mathbb{Z}$ will be specified. We have $ad - bc - mN = 1$ for some $m \in \mathbb{Z}$ since $det([\gamma]) \equiv 1 \mod N$ and therefore $gcd(c, d, N) = 1$. Hence there exists a $g \in \mathbb{Z}$ such that $gcd(c, d + gN) = 1$. We then have

$$det(\gamma) = a'd' - b'c = ad - bc + N(ed' - fc) = 1 + (m + ed' - fc)N.$$

Now, since $gcd(c, d') = 1$ there exist $f, e \in \mathbb{Z}$ such that $m = cf - ed'$, hence we have $det(\gamma) = 1$ and $\gamma \in SL_2(\mathbb{Z})$. Hence the map is surjective.
We have that $\Gamma(N)$ is the kernel of ϕ, since $\Gamma(N)$ corresponds to all the matrices $A \equiv I_2 \mod N$ with the modulo taken entry-wise, and since a matrix A is in $Ker(\phi)$ if and only if $A \equiv I_2 \mod N$, then we must have $\Gamma(N) = ker(\phi)$.

□

To have some idea of the relative size of $\Gamma(N)$ in comparison to the supergroup $SL_2(\mathbb{Z})$, we have the following result on the index:

Corollary 6.3. We have
$$[SL_2(\mathbb{Z}) : \Gamma(N)] < \infty.$$

Proof
We first note that since $\Gamma(N)$ is the kernel of the surjective homomorphism ϕ, there exists an isomorphism
$$\tilde{\phi}: \ SL_2(\mathbb{Z})/\Gamma(N) \to SL_2(\mathbb{Z}/N\mathbb{Z}),$$
and since $\mathbb{Z}/N\mathbb{Z}$ is finite (it contains N elements), we must have that $SL_2(\mathbb{Z}/N\mathbb{Z})$ is finite as each entry has N possible values, but with the further constraint of unit determinant, we have even fewer elements ($\phi(N)$ for coprimes of N). Hence there must be a finite amount of cosets $A\Gamma(N)$ with $A \in SL_2(\mathbb{Z})$ since there is a one-to-one correspondence with these cosets and elements in $SL_2(\mathbb{Z}/N\mathbb{Z})$.

□

The lemma, corollary and proofs above are from [7][Exercise 3.a]. The principal subgroup of level N is to be interpretted as the identity element under a congruence modulo N of $SL_2(\mathbb{Z})$, so since other congruence subgroups of $SL_2(\mathbb{Z})$ must contain the identity element, we define congruence subgroups of level N of $SL_2(\mathbb{Z})$ by the following:

Definition 6.4. (Congruence subgroup of level N)
A **congruence subgroup of level** N of $SL_2(\mathbb{Z})$ is a group Γ with $\Gamma(N) < \Gamma < SL_2(\mathbb{Z})$.

Example 6.5. The two subgroups of $SL_2(\mathbb{Z})$ defined by
$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mod N \right\} \tag{6.1}$$
$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mod N \right\} \tag{6.2}$$
are both congruence subgroups of level N of $SL_2(\mathbb{Z})$ with $\Gamma(N) < \Gamma_1(N) < \Gamma_0(N) < SL_2(\mathbb{Z})$.

Lemma 6.6. The map $\chi: \ \Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto b \mod N$ is a surjective homomorphism with kernel $\Gamma(N)$.

Proof
Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in \Gamma_1(N)$. Then
$$\begin{aligned} \chi(AB) &= [ab' + bd'] \\ &= [b' + b] \\ &= [b'] + [b] \\ &= \chi(A) + \chi(B), \end{aligned}$$
since $a, d' \equiv 1 \mod N$, so the map is a homomorphism. The map is surjective as for any $b \in \mathbb{Z}$, $\begin{bmatrix} 1 & [b] \\ 0 & 1 \end{bmatrix} \in \Gamma_1(N)$. Any matrix in $\Gamma_1(N)$ is in the kernel of χ if and only if $b \equiv 0 \mod N$, which is exactly the matrices in $\Gamma(N)$. So the kernel of χ is $\Gamma(N)$.

□

It follows that $\Gamma(N)$ is a normal subgroup of $\Gamma_1(N)$ and a normal subgroup of $SL_2(\mathbb{Z})$, but there is one more result to be found:

Lemma 6.7. The map $\psi: \ \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \mod N$ is a surjective homomorphism with kernel $\Gamma_1(N)$.

Proof
Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in \Gamma_0(N)$. Then

$$\begin{aligned} \psi(AB) &= [b'c + d'd] \\ &= [d'd] \\ &= [d'][d] \\ &= \psi(A)\psi(B), \end{aligned}$$

so the map is a homomorphism.
For $[d] \in (\mathbb{Z}/N\mathbb{Z})^*$ we set $[d]^{-1} = [a]$. Then by the same approach as in the proof of Lemma 6.2 we can find representatives $a, b, c, d \in \mathbb{Z}$, such that modulo N these are the elements $[a], [0], [0], [d]$ and we have $ad - bc = 1$. Then the matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ is mapped to $[d]$ and the map is surjective.
Now, let $\gamma = \begin{bmatrix} a & b \\ cN & d \end{bmatrix} \in \Gamma_0(N)$. We always have $[1] = [ad - bcN] = [ad] = [a][d]$. We have that γ is in the kernel of ψ if and only if $[d] = 1$. This is the case if and only if $[1] = [a][d] = [a]$, so γ is in the kernel of ψ if and only if $\gamma \in \Gamma_1(N)$. Hence $\Gamma_1(N)$ is the kernel of ψ.

□

The two lemmas and corresponding proofs above are from [7][Exercises 3.b, 3.c].
So, to summarize, we have that $\Gamma(N) \lhd \Gamma_1(N) \lhd \Gamma_0(N)$ and $\Gamma(N) \lhd SL_2(\mathbb{Z})$. Since ψ is a surjective homomorphism with kernel $\Gamma_1(N)$, there exists an isomorphism

$$\tilde{\psi}: \ \Gamma_0(N)/\Gamma_1(N) \to (\mathbb{Z}/N\mathbb{Z})^*,$$

and since the number of units in $Z/N\mathbb{Z}$ is the Euler totient of N, $\varphi(N)$, we have $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$.
Now, we still need some notation before we start defining modular forms with respect to congruence subgroups of $SL_2(\mathbb{Z})$:

Definition 6.8. (Factor of automorphy)
Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. For any matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ we define the **factor of automorphy**, $j(\gamma, z) \in \mathbb{C}$ for $z \in \mathbb{H}$ to be

$$j(\gamma, z) = cz + d$$

Definition 6.9. (Weight k operator)
For $\gamma \in \Gamma$ and any integer k define the weight k operator $[\gamma]_k$ on functions $f : \mathbb{H} \to \mathbb{C}$ by

$$(f[\gamma]_k)(z) = j(\gamma, z)^{-k} f(\gamma(z)),$$

where $\gamma(z) = \frac{az+b}{cz+d}$.

Since the factor of automorphy is never 0 or ∞ for any $z \in \mathbb{H}$ or $\gamma \in SL_2(\mathbb{Z})$ this implies that if f is meromorphic, so is $f[\gamma]_k$, and they share the same poles and zeroes. (Follows from the fact that $j(\gamma, z)$ has a pole at ∞ and a zero at 0 both of which are not points in $\mathbb{H}$).

Definition 6.10. (Weakly modular function with respect to a subset of $SL_2(\mathbb{Z})$)
Let $\Gamma \subset SL_2(\mathbb{Z})$. A meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is said to be a **weakly modular function of weight k with respect to** Γ if

$$f[\gamma]_k = f,$$

for all $\gamma \in \Gamma$.

This shows that $\theta(z)^4$ is indeed weakly modular of weight 2 with respect to the set $\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\}$.

Proposition 6.11. If f is weakly modular of weight k with respect to some subset $\Gamma \subseteq SL_2(\mathbb{Z})$, then f is weakly modular of weight k with respect to the group generated by Γ (with matrix multiplication).

Proof
This follows indirectly from Proposition 2.4. We have $\phi : GL_2(\mathbb{C}) \to FLT$ with $\phi(A)(z) = \frac{az+b}{cz+d}$ for $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a surjective homomorphism, and $\phi_{|SL_2(\mathbb{Z})}$ is still surjective onto the fractional linear transformations with $ad - bc = 1$. Even further we can restrict ϕ to Γ and since $\phi(A)\phi(B) = \phi(AB)$ for $A, B \in \Gamma$, we get that if f is weakly modular of weight k with respect to Γ, then

$$f[AB]_k = j(AB, z)^{-k} f(z) = j(A, \phi(B)(z))^{-k} j(B, z)^{-k} f(z),$$

where the last step follows from associativity of FLT, and since $\phi(B)(z)$ covers all of $\mathbb{H}$ by the fundamental domain of $SL_2(\mathbb{Z})$, we get

$$f[AB]_k = f[A]_k[B]_k = (f[A]_k)[B]_k = f[B]_k = f.$$

□

By this proposition, just like it was showed for the case of $\Gamma = SL_2(\mathbb{Z})$, it is enough to check that the weak modularity condition is satisfied for the generators of a given congruence subgroup Γ of $SL_2(\mathbb{Z})$ to conclude that f is weakly modular of weight k with respect to Γ.

It follows that $\theta(z)^4$ is weakly modular of weight 2 with respect to the group generated by the matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}$, for which we have the following result:

Proposition 6.12. The group $\Gamma_0(4)$ is generated by the matrices $\pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}, \pm\begin{bmatrix}1 & 0\\ 4 & 1\end{bmatrix}$

Proof
Let $\begin{bmatrix}a & b\\ c & d\end{bmatrix} \in \Gamma_0(4)$. It suffices to show that this matrix can be formed by products of the mentioned matrices. We have the identity

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}^n = \begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix} = \begin{bmatrix}a & b'\\ c & nc+d\end{bmatrix}.$$

By this identity, if $c \neq 0$, we may choose an appropriate n such that $|nc+d| \leq |c|/2$ and since $c \equiv 0 \mod 4$ and the fact that d must be odd (so must a) for the determinant to be 1, the inequality must be strict, $|nc+d| < |c|/2$. If on the other hand $c = 0$, we must have that for the determinant to be 1, the matrix must have 1's in the diagonal and b can be any reduction modulo 4, so the matrix must be a power of $\pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$. So assume $c \neq 0$, then as we established, we must have $|d| < |c|/2$. Now, we have the identity

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & 0\\ 4 & 1\end{bmatrix}^n = \begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & 0\\ 4n & 1\end{bmatrix} = \begin{bmatrix}a' & b\\ 4nd+c & d\end{bmatrix}.$$

By the same argument, we may choose an appropriate n such that $|c+4nd| < 2|d|$. So we can rearrange $|c|/2 < |d|$. Now, since we can perform matrix multiplications of the two forms that reduces either $|c|$ or $|d|$ at each step, we can after finitely many steps arrange for $c = 0$, and then the matrix is generated by some power of $\pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$. Hence we must have that $\Gamma_0(4)$ is generated by these two matrices. ([5][Theorem 7.0.13])

□

From this, it follows that $\theta(z)^4$ is a weakly modular function of weight 2 with respect to $\Gamma_0(4)$, since $\Gamma_0(4)$ is generated by $\pm\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}, \pm\begin{bmatrix}1 & 0\\ 4 & 1\end{bmatrix}$ and by Proposition 6.11 it suffices to check for these matrices that $\theta^4[\gamma]_2 = \theta^4$, for which we now know that

$$\theta^4\left[\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\right]_2 = 1^{-2}\theta^4(z+1) = \theta^4$$
$$\theta^4\left[\begin{bmatrix}1 & 0\\ 4 & 1\end{bmatrix}\right]_2 = (4z+1)^{-2}\theta^4\left(\frac{1}{4z+1}\right) = \theta^4.$$

Lemma 6.13. For all congruence subgroups Γ of $SL_2(\mathbb{Z})$ of any level N there exists a number $h \in \mathbb{Z}$ such that the matrix

$$m_h = \begin{bmatrix}1 & h\\ 0 & 1\end{bmatrix} \in \Gamma.$$

Proof
Any congruence subgroup by definition contains a principal congruence subgroup of level N, $\Gamma(N)$ which contains elements of the form $\begin{bmatrix}1 & bN\\ 0 & 1\end{bmatrix}$, for any $b \in \mathbb{Z}$, but we can have some $h \in \mathbb{Z}$, such that $h \mid N$, which gives $m_h \in \Gamma$.

□

We will denote the minimal h such that $m_h \in \Gamma$ as $h(\Gamma)$.

Remark 6.14. With this Lemma, we know that any weakly modular form of weight k with respect to a congruence subgroup Γ, f, must be $h(\Gamma)$-periodic, as Γ must contain $m_{h(\Gamma)}$ and thus

$$f[m_h]_k = f,$$

which in turn by definition implies that

$$f[m_h](z) = f(z+h) = f(z).$$

Lemma 6.15. If $f : \mathbb{H} \to \mathbb{C}$ is holomorphic, holomorphic at infinity and satisfying $f(z) = f(z+h)$, then there exists $a_n \in \mathbb{C}$ for $n \geq 0$ such that

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

for all $z \in \mathbb{H}$ and $q_h = e^{2\pi i z/h} \in D^*$.

Proof
The proof has the same approach as in Lemma 3.8 if one instead defines the coordinate $q_h(z) = e^{2\pi i z/h}$ and f is now h-periodic.

□

From now on, we consider the q_h-expansion $q = e^{2\pi i z/h(\Gamma)}$ for weakly modular functions of weight k with respect to Γ. Now we will define modular forms of weight k with respect to Γ:

Definition 6.16. (Modular form with respect to congruence subgroups)
Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. A function $f : \mathbb{H} \to \mathbb{C}$ is a **modular form of weight k with respect to** Γ if f is holomorphic on $\mathbb{H}$, f is weakly modular of weight k with respect to Γ and $f[\alpha]_k$ is holomorphic at infinity for all $\alpha \in SL_2(\mathbb{Z})$.

Since, modular forms are weakly modular, we have that $f[\gamma]_k = f$ for $\gamma \in \Gamma$, and thus since $f[\alpha]_k$ is holomorphic at infinity for all $\alpha \in SL_2(\mathbb{Z})$, then so must f be, as Γ is a subgroup of $SL_2(\mathbb{Z})$. Therefore modular forms with respect to a congruence subgroup Γ are holomorphic on $\mathbb{H}$, holomorphic at infinity and are weakly modular functions, these must, by Lemma 6.15, have a Fourier expansion of the form

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

for all $z \in \mathbb{H}$.
Likewise, we can define cusp forms analogously:

Definition 6.17. (Cusp form with respect to congruence subgroups)
If f is a modular form of weight k with respect to a congruence subgroup Γ of $SL_2(\mathbb{Z})$, we say that f is a **cusp form of weight k with respect to** Γ if $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$.

The conditions that $f[\alpha]_k$ is holomorphic at infinity for all $\alpha \in SL_2(\mathbb{Z})$ and the cusp form condition are both independent of the given congruence subgroup, but since we can decompose $SL_2(\mathbb{Z})$ into a finite union $SL_2(\mathbb{Z}) = \cup_j \Gamma\alpha_j$ (remember that $\Gamma(N)$ has finite index with $SL_2(\mathbb{Z})$, and that any congruence subgroup of level N contains $\Gamma(N)$) and since $f[\gamma\alpha]_k = f[\alpha]_k$ for $\gamma \in \Gamma$ for weakly modular f of weight k with respect to Γ,

we only have to check the condition on finitely many coset representatives α_j.
One can show by the exact same approach as in Chapter 5, that the set of all modular forms of weight k with respect to Γ, $M_k(\Gamma)$, forms a vector space over $\mathbb{C}$ for all $k \in \mathbb{Z}$ and likewise with cusp forms. We will describe these vector spaces further, but first, we need a result:

Lemma 6.18. Let $f : \mathbb{H} \to \mathbb{C}$ be holomorphic on $\mathbb{H}$, satisfying $f(z+N) = f(z)$. If there exist positive constants C, r such that the coefficients in the Fourier expansion of f satisfies $|a_n| < Cn^r$ for all n. Then

$$|f(z)| \leq C_0 + C\left(\int_{t=0}^{\infty} t^r e^{-2\pi t y/N} dt\right) + \frac{C}{y^r},$$

where C_0 is some appropriate constant.

Proof
First, write $z = x + iy$, and assume $|a_n| < Cn^r$ for some positive constants C, r. We have that

$$|f(z)| = |\sum_{n=0}^{\infty} a_n e^{2\pi i n z/N}| \leq \sum_{n=0}^{\infty} |a_n||e^{2\pi i n(x+iy)}| = \sum_{n=0}^{\infty} |a_n||e^{2\pi i n x/N} \cdot e^{-2\pi n y/N}| < \sum_{n=0}^{\infty} Cn^r e^{-2\pi n y/N}.$$

Defining $g(t) = t^r e^{-2\pi t y/N}$, we have that $g'(t) = t^{r-1}e^{-2\pi t y/N}(r + t \cdot (-\frac{2\pi y}{N}))$ by the product rule. We then observe that

$$g'(t) > 0 \text{ for } t \in \left(0, \frac{rN}{2\pi y}\right) \text{ and } g'(t) < 0 \text{ for } t > \frac{rN}{2\pi y}.$$

Let $k = \lfloor \frac{rN}{2\pi y} \rfloor$.
Since $g(t)$ is monotonically increasing and positive on$(0, k)$ it follows that

$$\sum_{n=0}^{k-1} n^r e^{-2\pi n y/N} = \sum_{n=0}^{k-1} g(n) < \int_{t=0}^{k} g(t) dt,$$

and since $g(t)$ is monotonically decreasing and positive on $(k+1, \infty)$ it follows that

$$\sum_{n=k+1}^{\infty} n^r e^{-2\pi n y/N} = \sum_{n=k+1}^{\infty} g(n) < \int_{t=k}^{\infty} g(t) dt.$$

Combining these, we get

$$\begin{aligned}
\sum_{n=1}^{\infty} n^r e^{-2\pi n y/N} &= (k-1)^r e^{-2\pi(k-1)y/N} + k^r e^{-2\pi k y/N} + \sum_{n=1}^{k-1} n^r e^{-2\pi n y/N} + \sum_{n=k+1}^{\infty} n^r e^{-2\pi n y/N} \\
&< (k-1)^r e^{-2\pi(k-1)y/N} + k^r e^{-2\pi k y/N} + \int_{t=0}^{k} g(t) dt + \int_{t=k}^{\infty} g(t) dt \\
&= (k-1)^r e^{-2\pi(k-1)y/N} + k^r e^{-2\pi k y/N} + \int_{t=0}^{\infty} g(t) dt.
\end{aligned}$$

Since $k > \frac{rN}{2\pi y} - 1$, we have $e^{-2\pi k y/N} \approx e^{-\frac{2\pi y r N}{2\pi y N}} = e^{-r}$, and since $(k-1)^r$ and k^r is $O(y^{-r})$, if we choose C_0 large enough to bypass this constant e^{-r}, we finally obtain

$$|f(z)| \leq |a_n| + C\left(\int_{t=0}^{\infty} g(t) dt + O(y^{-r})\right)$$

$$\leq C_0 + C\left(\int_{t=0}^{\infty} t^r e^{-2\pi t y/N} dt\right) + \frac{C}{y^r}.$$

([5][Lemma 5.4.1])

□

We will now show, that given certain conditions, there exists modular forms of weight k with respect to congruence subgroups of $SL_2(\mathbb{Z})$.

Theorem 6.19. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. Let $f: \mathbb{H} \to \mathbb{C}$ be a weakly modular function of weight k with respect to Γ and holomorphic on $\mathbb{H}$ and holomorphic at infinity. If there exists positive constants C, r such that for the coefficients of the Fourier expansion of f, we have $|a_n| < Cn^r$ for all n, then $f \in M_k(\Gamma)$.

Proof
By definition of modular forms with respect to congruence groups, all we need to show is that given the above conditions, $f[\alpha]_k$ is holomorphic at infinity for all $\alpha \in SL_2(\mathbb{Z})$.
Now, since Γ contains $\Gamma(N)$ for some N, f satisfies the conditions from the previous Lemma, so we have

$$|f(z)| \leq C_0 + C\left(\int_{t=0}^{\infty} t^r e^{-2\pi t y/N} dt\right) + \frac{C}{y^r}.$$

If we substitute $u = 2\pi y t/N$, we get $dt = \frac{N du}{2\pi y}$ and

$$\begin{aligned}|f(z)| &\leq C_0 + C\left(\int_{u=0}^{\infty} \left(\frac{Nu}{2\pi y}\right)^r e^{-u}\frac{N}{2\pi y} du\right) + \frac{C}{y^r}\\ &= C_0 + \frac{CN^{r+1}}{(2\pi y)^{r+1}}\left(\int_{u=0}^{\infty} u^r e^{-u} du\right) + \frac{C}{y^r}.\end{aligned}$$

Now, since the integral is the Γ-function, that is $\Gamma(z) = \int_{x=0}^{\infty} x^{z-1}e^{-x}dx$, which converges for all $z \in \mathbb{C}$, $Re(z) > 0$, we have that, the right hand side is only dependant on y, and since

$$|f(z)| \leq C_0 + O(y^{-(r+1)}) + O(y^{-r}),$$

for all $y \in \mathbb{R}$ with $y > 0$, we have that $|f(z)|$ is bounded as $y \to \infty$.
Now, since $(f[\alpha]_k)(z+N) = f[\alpha]_k(z)$ we may estimate $|f[\alpha_k](z)|$ as $q_N = e^{-2\pi i z/N} \to 0$ by letting $y \to \infty$ and $0 \leq x < N$ for $z = x + iy$. We have that

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

and by the previous Lemma, we have that

$$|f(\alpha(z))| \cdot |cz+d|^{-k} \leq (C_0 + O(Im(\alpha(z))^{-r})|cz+d|^{-k},$$

and by recalling that $Im(\alpha(z)) = \frac{Im(z)}{|cz+d|^2}$ for all $\alpha \in SL_2(\mathbb{Z})$, we get

$$|(f[\alpha]_k)(z)| \leq (C_0 + O(Im(z)^{-r}|cz+d|^{2r}))|cz+d|^{-k} = (C_0 + O(Im(z)^{-r})O(Im(z)^{2r})O(Im(z)^{-k}),$$

so we get that for some constant $C > 0$

$$|(f[\alpha]_k)(z)| \leq Cy^{r-k}.$$

Now, since for every $\alpha \in SL_2(\mathbb{Z})$, $(f[\alpha]_k)(z)$ is holomorphic on $\mathbb{H}$ and weight k-invariant under $\alpha\Gamma\alpha^{-1}$, it must have a Laurent expansion

$$(f[\alpha]_k)(z) = \sum_{n\in\mathbb{Z}} a'_n q_N^n.$$

To show that $f[\alpha]_k$ is holomorphic at infinity, it is equivalent to show that $a'_n = 0$ for $n < 0$, for which it suffices to show that

$$lim_{q_N\to 0}(f[\alpha]_k)(z) \cdot q_N = 0,$$

as if for some $n < 0$, $a'_n \neq 0$ this limit would be infinite. Combining what we have, we see that

$$lim_{q_N\to 0}|(f[\alpha]_k)(z) \cdot q_N| \leq C \lim_{q_N\to 0} y^{r-k}|q_N|.$$

Now, since for $z = x + iy$, we have $q_N = e^{2\pi i(x+iy)/N} = e^{-2\pi y/N} \cdot e^{2\pi ix/N}$. And thus

$$|q_N| = e^{-2\pi y/N},$$

and since the exponential term dominates the polynomial in y for all r and k, we must have that

$$lim_{q_N\to 0}|(f[\alpha]_k)(z) \cdot q_N| = 0,$$

and we are done. (This proof is based on [4][Exercise 1.2.6] with hints found in the back of the book)

□

Now, we have the appropriate conditions to determine if $\theta(z)^4$ is not only a weakly modular function, but in fact a modular form of weight 2 with respect to $\Gamma_0(4)$.

Corollary 6.20. We have

$$\theta(z)^4 \in M_2(\Gamma_0(4))$$

Proof

We have showed in Theorem 3.15 and Theorem 3.16 that θ^4 is holomorphic on $\mathbb{H}$ and holomorphic at infinity. Since $\theta(z)^4$ is a Fourier expansion, we require the coefficients $a_n = r(n,4)$ to satisfy $|r(n,4)| \leq Cn^r$ for all n and some appropriate constants C and r. We will now show that $\theta(z)^4$ is a modular form of weight 2 with respect to $\Gamma_0(4)$.

So, recall from Lemma 3.11 that $r(n,2k) = |S_m| \leq (2m+1)^{2k}$, and that $|S_m| = r(n,2k)$. But since m is a real, positive square root of n, we have

$$r(n,2k) \leq (2\sqrt{n}+1)^{2k},$$

and the right hand side is $O(n^k)$. Thus we can choose some appropriate constant C and an exponent $r \geq k$ such that this is satisfied.

□

Chapter 7 | The Eisenstein Series of weight 2

We established in the previous chapter that the only modular form of weight 2 with respect to $SL_2(\mathbb{Z})$ is the zero-function. Therefore the Eisenstein series of weight 2 is not in M_2. However, this series still satisfy some modular properties that have applications. We will therefore describe this series further in detail in this chapter. As we established in Corollary 3.26, the Eisenstein series for $k \geq 3$ converges absolutely on $\mathbb{H}$, but $G_2(z)$ does not. If we however consider the Fourier expression of the normalization

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

this function converges rapidly for $q \to 0$ (equivalently for $Im(z) \to i\infty$) and defines a holomorphic function on $\mathbb{H}$, also for $k = 2$. So we can define, with $B_2 = \frac{1}{6}$

$$\mathbb{G}_2(z) = -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

Using the fact that $G_k(z) = \frac{2(2\pi i)^k}{(k-1)!}\mathbb{G}_k(z)$, we can define the Eisenstein series of weight 2 as

$$G_2(z) = -8\pi^2 \mathbb{G}_2(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n,$$

and

$$E_2(z) = \frac{3}{\pi^2} G_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

Now, at first, we defined the Eisenstein series of weight k by

$$G_2(z) = \sum_{(c,d \in \mathbb{Z}^2, (c,d) \neq (0,0)} \frac{1}{(cz+d)^2} = \sum_{d \in \mathbb{Z} \setminus 0} \left[\frac{1}{d^2}\right] + \sum_{c \in \mathbb{Z} \setminus 0} \sum_{d \in \mathbb{Z}} \frac{1}{(cz+d)^2},$$

and if we carry out the summation over d first and then c, the proof of Theorem 4.2 still holds, so the Fourier expression of G_2 is indeed as stated:

$$G_2(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

The double sum over c and d is however not absolutely convergent, but conditionally convergent, so we cannot change the order of summation. The consequence of this is that the step used in the proof of Theorem 3.28 is not valid, so $G_2(z)$ does not satisfy the functional equation $G_2\left(-\frac{1}{z}\right) = z^2 G_2(z)$. The equation $G_2(z) = G_2(z+1)$ of course still holds since the sums are over all the integers.

7.1 The Almost-invariance of $G_2(z)$

We established that a weakly modular function of weight k with respect to $SL_2(\mathbb{Z})$ satisfies the equation

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

for all $\gamma \in SL_2(\mathbb{Z})$, that is, a weakly modular function is in a sense invariant under γ up to an automorphy factor $(cz+d)^k$. The Eisenstein series of weight 2 is not a weakly modular form of weight 2, however for arguments $z \in \mathbb{H}\backslash SL_2(\mathbb{Z})$ the series does have a pattern.

Proposition 7.1. For $z \in \mathbb{H}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ we have

$$G_2(\gamma(z)) = (cz+d)^2 G_2(z) - \pi i c(cz+d).$$

Proof
The series $\sum_{(c,d\in\mathbb{Z}^2,(c,d)\neq(0,0)} \frac{1}{(cz+d)^k}$ does not converge for $k=2$, however it converges for any real number $k>2$. We therefore modify the sum slightly by introducing an $\epsilon > 0$:

$$G_{2,\epsilon} = \sum_{(c,d\in\mathbb{Z}^2,(c,d)\neq(0,0)} \frac{1}{(cz+d)^2|cz+d|^{2\epsilon}}.$$

This series converges absolutely and transforms by

$$G_{2,\epsilon}\left(\frac{az+b}{cz+d}\right) = (cz+d)^2|cz+d|^{2\epsilon} G_{2,\epsilon}(z).$$

What we need to show is that the limit of $G_{2,\epsilon}$ as $\epsilon \to 0$ exists and equals $G_2(z) - \frac{\pi}{2y}$ where $y = Im(z)$.
So, to prove this we define a function I_ϵ by

$$I_\epsilon(z) = \int_{-\infty}^{\infty} \frac{dt}{(z+t)^2|z+t|^{2\epsilon}},\ z \in \mathbb{H}.$$

Then for $\epsilon > 0$ we can write

$$G_{2,\epsilon}(z) - \sum_{c=1}^{\infty} I_\epsilon(cz) = 2\sum_{d=1}^{\infty} \frac{1}{d^{2+2\epsilon}} + \sum_{c=1}^{\infty}\sum_{d=-\infty}^{\infty}\left[\frac{1}{(cz+d)^2|cz+d|^{2\epsilon}} - \int_n^{n+1} \frac{dt}{(cz+d)^2|cz+d|^{2\epsilon}}\right].$$

Both sums on the right hand side converge absolutely and locally uniformly for $\epsilon > -1/2$. The first sum is equal to $\zeta(s)$ with $s = 2+2\epsilon$, which converges absolutely for all real $s > 1$. The second sum is $O((cz+d)^{-3-2\epsilon})$ by the mean value theorem, which states that for any differentiable function f, the difference $f(t) - f(n)$ is bounded in $n \leq t \leq n+1$ by $max_{n\leq u\leq n+1}|f'(u)|$. Hence, the limit of the expression on the right hand side exists and can be obtained by setting $\epsilon = 0$ in each term where it reduces to $G_2(z)$.
However, for $\epsilon > -1/2$ we have

$$I_\epsilon(x+iy) = \int_{-\infty}^{\infty} \frac{dt}{(x+t+iy)^2((x+t)^2+y^2)^\epsilon}$$

$$= \int_{-\infty}^{\infty} \frac{dt}{(t+iy)^2(t^2+y^2)^\epsilon}$$
$$= \frac{I(\epsilon)}{y^{1+2\epsilon}},$$

where $I(\epsilon) = \int_{-\infty}^{\infty}(t+i)^{-2}(t^2+1)^{-\epsilon}dt$, so $\sum_{c=1}^{\infty} I_\epsilon(cz) = I(\epsilon)\zeta(1+2\epsilon)/y^{1+2\epsilon}$ for $\epsilon > 0$. Now, we have $I(0) = 0$, as the integral vanishes due to symmetry and

$$I'(0) = -\int_{-\infty}^{\infty} \frac{log(t^2+1)}{(t+i)^2} dt$$
$$= \left[\frac{1+log(t^2+1)}{t+i}\right]_{-\infty}^{\infty}$$
$$= -\pi$$

and since $\zeta(1+2\epsilon) = \frac{1}{2\epsilon} + O(1)$, the product $I(\epsilon)\zeta(1+2\epsilon)/y^{1+2\epsilon} \to -\pi/2y$ as $\epsilon \to 0$. This proves the proposition. □

Now, given this transformation equation for $G_2(z)$, we can define the functions

$$G_2^*(z) = G_2(z) - \pi/2Im(z)$$
$$E_2^*(z) = E_2(z) - 3/\pi Im(z)$$
$$\mathbb{G}_2^*(z) = \mathbb{G}_2(z) + 1/8\pi Im(z).$$

These three functions each satisfy the weakly modular transformation equations for weight 2, however, they are not holomorphic on $\mathbb{H}$, so they are not modular forms of weight 2 with respect to $SL_2(\mathbb{Z})$ (of which there are non other than the zero function).

Chapter 8 | The space $M_2(\Gamma_0(4))$

This chapter is based on [5][Section 5.5]. Since we have determined that $\theta(z)^4$ is in fact a modular form of weight 2 with respect to $\Gamma_0(4)$, we wish to analyse the space containing these functions further. We start with the following result involving the Eisenstein series of weight 2:

Proposition 8.1. For any $N \in \mathbb{N}$, we have

$$G_{2,N}(z) = G_2(z) - NG_2(Nz) \in M_2(\Gamma_0(N)).$$

Proof

First note that for $N = 1$, we have $G_{2,1} \equiv 0 \in M_2(SL_2(\mathbb{Z}))$. For $N > 1$, we note that for $\gamma = \begin{bmatrix} a & b \\ Nc & d \end{bmatrix}, \eta = \begin{bmatrix} a & Nb \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$, we can write

$$N\gamma(z) = \frac{aNz + Nb}{Ncz + d} = \eta(Nz).$$

Thus for $\gamma \in \Gamma_0(N)$, we have

$$\begin{aligned} G_{2,N}[\gamma]_2 &= (Ncz+d)^{-2}\left(G_2(\gamma(z)) - NG_2(N\gamma(z))\right) \\ &= (Ncz+d)^{-2}(G_2(\gamma(z))) - (Ncz+d)^{-2}(NG_2(N\gamma(z))) \\ &= G_2(z) - \frac{\pi i Nc}{Ncz+d} - (Ncz+d)^{-2}(NG_2(\eta(Nz)) \\ &= G_2(z) - \frac{\pi i Nc}{Ncz+d} - \left(N\left(G_2(Nz) - \frac{\pi i c}{(cN)z+d}\right)\right) \\ &= G_2(z) - NG_2(Nz), \end{aligned}$$

where the transformation property of G_2 is used in the last three steps. To shows that this difference is holomorphic, we know that G_2 has a convergent Fourier expansion, and thus so must $N(G_2(Nz))$, and the difference of two holomorphic functions is holomorphic.
To show that this difference is holomorphic at infinity, we have Theorem 6.19. We know that the coefficients a_n of the Fourier expansion of $G_{2,N}$ is bounded above by $8\sigma_1(n)$, at least for $n > 1$. So it suffices to show that $\sigma_1(n) < Cn^r$, but since $\sigma_1(n) < \sum_{i=1}^{n} n^2$, we are done. So $G_{2,N} \in M_2(\Gamma_0(N))$.

□

Now, with this result, we can conclude that $G_{2,4} \in M_2(\Gamma_0(4))$ and that $G_{2,2} \in M_2(\Gamma_0(2))$. Now, since $M_2(\Gamma_0(2)) \subset M_2(\Gamma_0(4))$, since the smaller subgroup $\Gamma_0(4)$ allows more weakly modular functions of weight 2, and the other conditions are invariant of the given congruence subgroup, we must have that $G_{2,2} \in M_2(\Gamma_0(4))$. We will now give further results on these specific modular forms and use them to describe the space $M_2(\Gamma_0(4))$.

Lemma 8.2. The functions $G_{2,2}$ and $G_{2,4}$ have series expansions

$$G_{2,2}(z) = -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{d>0, d|n, d\notin 2\mathbb{Z}} d\right) q^n\right)$$

$$G_{2,4}(z) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{d>0, d|n, d\notin 4\mathbb{Z}} d\right) q^n\right)$$

Proof
From the previous chapter, we have that

$$G_2(z) = \frac{\pi^2}{3} - 8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^n,$$

so we can write

$$\begin{aligned}
G_{2,2}(z) &= G_2(z) - 2G_2(2z) \\
&= \left(\frac{\pi^2}{3} - 8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^n\right) - 2\left(\frac{\pi^2}{3} - 8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^{2n}\right) \\
&= -\frac{\pi^2}{3} - 8\pi^2\left(\sum_{n=1}^{\infty}\sigma_1(n)q^n - 2\sigma_1(n)q^{2n}\right) \\
&= -\frac{\pi^2}{3} - 8\pi^2\left(\sum_{n=1}^{\infty}\sigma_1(n)q^n - \left(\sum_{d>0, d|n, 2|d} d\right) q^n\right) \\
&= -\frac{\pi^2}{3} - 8\pi^2\sum_{n=1}^{\infty}\left(\sum_{d>0, d\nmid n, d\notin 2\mathbb{Z}} d\right) q^n \\
&= -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{d>0, d\nmid n, d\notin 2\mathbb{Z}} d\right) q^n\right)
\end{aligned}$$

and with the same approach we arrive at

$$G_{2,4} = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{d>0, d\nmid n, d\notin 4\mathbb{Z}} d\right) q^n\right).$$

□

Proposition 8.3. The two Eisenstein series $G_{2,2}(z)$ and $G_{2,4}(z)$ are linearly independent.

Proof
From the series expansions of the two, the sums of the odd divisors and sum of divisors that are not a multiple of 4 will ensure that the only solution to

$$aG_{2,2} + bG_{2,4} = 0$$

is $a = 0, b = 0$.

□

Theorem 8.4. We have
$$dim(M_2(\Gamma_0(4))) = 2$$

Proof
The proof is long and technical and requires another background than we have focused the scope of this thesis to. The build-up to the proof and the proof itself can found seen in [4][Chapter 3]. Theorem 3.5.1 is the general case.

□

Now, since $M_2(\Gamma_0(4))$ is two-dimensional and we have found two linearly independent elements of this space, we have the following consequence:

Corollary 8.5. $\{G_{2,2}(z), G_{2,4}(z)\}$ is a basis for $M_2(\Gamma_0(4))$

Chapter 9 | The Four Square Theorem

This section is based on [4][Section 1.2] and [5][Chapter 7].
Now, we have found that $\theta(z)^4 \in M_2(\Gamma_0(4))$ (Corollary 6.20), and that $M_2(\Gamma_0(4))$ is a two-dimensional space (Theorem 8.4) with basis $\{G_{2,2}, G_{2,4}\}$ (Corollary 8.5). Se must have that $\theta(z)^4$ is a linear combination of these two basis elements, that is

$$\theta(z)^4 = aG_{2,2}(z) + bG_{2,4}(z),$$

with not both a and b zero and for all $z \in \mathbb{H}$, since $\theta(z)^4$ is a non-zero modular form. We then have the following observation:

Proposition 9.1. We have

$$\theta(z)^4 = -\frac{1}{\pi^2} G_{2,4}(z)$$

for all $z \in \mathbb{H}$.

Proof
By checking the first few terms we find that

$$\theta(z)^4 = 1 + 8q + \dots,$$

and since

$$G_{2,4} = -\pi^2(1 + 8q + \dots),$$

we get the relation

$$\theta(z)^4 = -\frac{1}{\pi^2} G_{2,4}(z),$$

given independently of z. □
Now, recall from Corollary 1.3 that

$$\theta(z)^k = \sum_{n=0}^{\infty} r(n,k) q^n,$$

and especially for the case of $k = 4$, we have $r(n, 4)$ as coefficients in $\theta(z)^4$. We have that the equality

$$\theta(z)^4 = -\frac{1}{\pi^2} G_{2,4}(z)$$

holds for all $z \in \mathbb{H}$ by Proposition 9.1. So we can compare the coefficients of $\theta(z)^4$ and $G_{2,4}(z)$ to finally reach our goal and present the four square theorem:

Theorem 9.2. (The Four Square Theorem)
The number of representations of $n \geq 1$ as a sum of four squares,

$$r(n,4) = |\{(a,b,c,d) \in \mathbb{Z}^4 \mid n = a^2 + b^2 + c^2 + d^2\}|,$$

is given by

$$r(n,4) = 8 \sum_{d>0,\ d|n,\ 4\nmid d} d$$

Proof
Since $G_{2,4}(z) = -\pi^2(1 + 8\sum_{n=1}^{\infty}(\sum_{d>0,\ d|n,\ 4\nmid d} d)q^n$ by Lemma 8.2 and $\theta(z)^4 = -\frac{1}{\pi^2}G_{2,4}(z)$ by Proposition 9.1, we obtain

$$\theta(z)^4 = 1 + \sum_{n=1}^{\infty} 8(\sum_{d>0,\ d|n,\ 4\nmid d} d)q^n,$$

and since $\theta(z)^4 = 1 + \sum_{n=1}^{\infty} r(n,4)q^n$, we conclude by matching coefficients that

$$r(n,4) = 8 \sum_{d>0,\ d|n,\ 4\nmid d} d,$$

for $n \geq 1$. □

Now, obviously if 4 does not divide n, then 4 does not divide any of the divisors d of n, so we have the following consequence:

Corollary 9.3. For $n \geq 1$, $4 \nmid n$, $r(n,4)$ reduces to

$$r(n,4) = 8\sigma_1(n).$$

Chapter 10 | Conclusion

The aim of this thesis was to derive a formula for the amount of representations of a natural number n as the sum of four squares

$$r(n,4) = |\{(a,b,c,d) \in \mathbb{Z}^4 \mid n = a^2 + b^2 + c^2 + d^2\}|,$$

to have other methods than going through all the different representations.
For this, we presented the Jacobi Theta function: a power series with $r(n,1)$ as coefficients defined on the upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$,

$$\theta(z) = \sum_{n=0}^{\infty} r(n,1)q^n, \ z \in \mathbb{H}, \ q = e^{2\pi i z}.$$

We found that for the k'th power of this series, the coefficients would be $r(n,k)$, that is

$$\theta(z)^k = \sum_{n=0}^{\infty} r(n,k)q^n,$$

and it followed that $\theta(z)^4$ has coefficients $r(n,4)$. To derive a formula for these coefficients, we would have to find an equivalent series with other coefficients to then be able to establish an equality of coefficients between the two series. For this, we found that $\theta(z)^4$ was a modular form of weight 2 with respect to the congruence subgroup of $SL_2(\mathbb{Z})$,

$$\Gamma_0(4) = \left\{ \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mod 4 \right\},$$

where modulo N is taken entry-wise.
The set of modular forms of weight 2 with respect to $\Gamma_0(4)$ forms a vector space and has finite dimension and is thus generated by finitely many linearly independent modular forms. It follows that $\theta(z)^4$ must be a linear combination of these generators.
To find these generators, we gave an introduction to modular forms with respect to $SL_2(\mathbb{Z})$ and found non-trivial modular forms of integral weight $k \geq 3$,

$$G_k = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(mz+n)^k}, \ z \in \mathbb{H}.$$

The set of modular forms of weight k was shown to also form a vector space for all $k \geq 0$, and it was found that for any k, these spaces have finite dimension and are generated by linear combinations of products of powers of G_4 and G_6. This was used to show that one can find relations between sums of divisor functions, $\sigma_k(n) = \sum_{d|n,d>0} d^k$, such as

$$\frac{\sigma_7(n) - \sigma_3(n)}{120} = \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Then, we went back on track to show that $\theta(z)^4$ was indeed a modular form of weight 2 with respect to $\Gamma_0(4)$, and for this, we introduced the reader to the theory of modular forms with respect to congruence subgroups of $SL_2(\mathbb{Z})$. The space of modular forms of weight 2 with respect to $\Gamma_0(4)$, $M_2(\Gamma_0(4))$, was then analyzed, and it was shown that this space contained the two elements

$$G_{2,2} = G_2(z) - 2G_2(2z)$$

$$G_{2,4} = G_2(z) - 4G_2(4z).$$

These two elements were shown to be linearly independent and $M_2(\Gamma_0(4))$ was shown to be 2-dimensional, and thus $\theta(z)^4$ is a linear combination of these two elements

$$\theta(z)^4 = aG_{2,2}(z) + bG_{2,4}(z).$$

We then found the relation

$$\theta(z)^4 = -\frac{1}{\pi^2}G_{2,4}(z),$$

and since the Fourier expansion of $G_{2,4}(z)$ was given by

$$G_{2,4}(z) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{d>0, d|n, 4\nmid d} d\right)q^n\right),$$

we finally found

$$\theta(z)^4 = 1 + \sum_{n=1}^{\infty} r(n,4)q^n = \left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{d>0, d|n, 4\nmid d} d\right)q^n\right),$$

whereafter we concluded by equivalence of coefficients that

$$r(n,4) = 8\sum_{d>0,\ d|n,\ 4\nmid d} d.$$

Since if 4 does not divide n, 4 does not divide the divisors d, we finally had for $n \in \mathbb{N}$ with $4 \nmid n$ that

$$r(n,4) = 8\sigma_1(n).$$

For further work, one could use a similar approach to find other formulas for the number of representations of a natural number as a sum of k squares

$$r(n,k) = |\left\{(v_1, v_2, \ldots, v_k) \in \mathbb{Z}^k \mid n = v_1^2 + v_2^2 + \ldots + v_k^2\right\}|.$$

We showed in the thesis that not only is $\theta(z)^4$ holomorphic on $\mathbb{H}$, holomorphic at infinity and weakly modular of weight 2 with respect to $\Gamma_0(4)$. In fact, any even integral power $2k$, $k \geq 1$ of $\theta(z)$ is holomorphic on $\mathbb{H}$, holomorphic at infinity and weakly modular of weight k with respect to $\Gamma_0(4)$, so one only needs to use Theorem 6.19 to show whether a given even integral power $2k$, $k \geq 1$, of theta is a modular form of weight k with respect to $\Gamma_0(4)$.
It even turns out that the space of modular forms of finite weight k with respect to any congruence subgroup of $SL_2(\mathbb{Z})$ is finite dimensional ([4][Theorem 3.5.1 and Theorem 3.6.1]), that includes those with respect to $\Gamma_0(4)$, hence we can again find finitely many generators and find that $\theta(z)^{2k}$ is a linear combination of these. So a continuation of this thesis could include an analysis of other spaces and find other identities for $r(n, 2k)$.

Bibliography

[1] Ravi P. Agarwal, et al., Springer Science+Business Media, 2011.
An Introduction to Complex Analysis

[2] Niels Lauritzen, Cambridge University Press, 2003
Concrete Abstract Algebra - From Numbers to Gröbner Bases.

[3] Jan Henrik Bruinier, et al., Springer-Verlag Berlin Heidelberg, 2008
The 1-2-3 of Modular Forms

[4] Fred Diamond and Jerry Shurman, Springer Science+Business Media New York, 2005, (corrected 2016)
A First Course in Modular Forms

[5] Aaron Landesman, Stanford University
Modular Forms and the Four Square Theorem https://web.stanford.edu/~aaronlan/assets/landesman_junior_paper.pdf

[6] Keith Conrad, Course material for Connecticut Summer School in Number Theory, 2016
Modular Forms https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/CTNTmodularforms.pdf

[7] Arpád Tóth, Eötvös Loránd University, 2013
Solutions to Course Exercises in Modular Forms
https://www2.math.ethz.ch/education/bachelor/lectures/fs2013/math/modular_forms/solutions1.pdf

[8] Rich Schwartz, Brown University, 2017
Notes on Fourier Series and Modular Forms https://www.math.brown.edu/~res/MathNotes/modular.pdf

[9] Keith Conrad
$SL_2(\mathbb{Z})$ https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf

[10] *Wikipedia photo of* G_6
https://en.wikipedia.org/wiki/Eisenstein_series

Appendix A | Complex Analysis

A.1 Introduction to complex functions

This section is based on the book [1]. Recall that the **complex numbers** $\mathbb{C}$ are

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\},$$

where $i = \sqrt{-1}$ is called the **imaginary unit**, and $\mathbb{C}$ is a field. We call a the **real part** and b the **imaginary part** of a complex number and denote these $a = Re(z)$ and $b = Im(z)$ for a complex number $z = a + bi$.
Recall that the **modulus of a complex number** $z = a + bi$ is $|z| = \sqrt{a^2 + b^2}$.
We will now define complex functions:

Definition A.1. (Complex function)
Let $S \subseteq \mathbb{C}$ be a set of complex numbers. A **complex function** f defined on S is a rule that assigns to each $z = x + iy \in S$ a unique complex number $w = u + iv$ and written as $f : S \to \mathbb{C}$.
The set S is called the **domain** of f, the set $W = \{f(z) \mid z \in S\}$ is called the **codomain** (sometimes also range or image) of f and f is said to map S **onto** W. That is, f maps the domain S to the whole codomain W.
The function $w = f(z)$ is said to be from S **into** $\mathbb{W}$ if the range, W, of f is a proper subset of $\mathbb{W}$.
A function f is called **injective** on a set S if the equation $f(z_1) = f(z_2)$ implies that $z_1 = z_2$. That is, no two distinct elements of S are mapped to the same element in W by f.

Now, as every complex number c is characterized by two real numbers, $a, b \in \mathbb{R}$ such that $c = a + bi$, a complex function f of the complex variable $z = x + iy$ can be specified by two real functions $u = u(x, y)$ and $v = v(x, y)$, where x and y are real arguments. We usually write

$$f(z) = u(x, y) + iv(x, y).$$

An example of this is the complex exponential function $f(z) = e^z$ with $z = x + iy$, which can be written

$$f(z) = e^x cos(y) + ie^x sin(y),$$

where $u(x, y) = e^x cos(y)$ and $v(x, y) = e^x sin(y)$.
We have tools to analyse the behaviour of real functions: the limit of a function, continuity, differentiability, etc., and we shall now present the complex analogues.

Definition A.2. (Limit of a complex function)
Let f be a complex function defined in some neighborhood of $z_0 \in \mathbb{C}$, with the possible exception of the point z_0 itself. We say that the **limit** of $f(z)$ as z approaches z_0 (independent of path) is the number w_0 if

$$|f(z) - w_0| \to 0 \ as \ |z - z_0| \to 0,$$

and we write $\lim_{z \to z_0} f(z) = w_0$. With this, $f(z)$ can be made arbitrarily close to w_0 if we choose z sufficiently close to z_0.
Equivalently, we say that w_0 is the **limit** of f as z approaches z_0 if, for any given real $\epsilon > 0$, there exists a real $\delta > 0$ such that

$$0 < |z - z_0| < \delta \implies |f(z) - w_0| < \epsilon.$$

Formally, when we let $z \to \infty$, this is understood as $|z| \to \infty$ and equivalently $f(z) \to \infty$ is $|f(z)| \to \infty$, since a complex number can approach infinity in either the real part, the imaginary part or both simultaneously.

Definition A.3. (Continuous Complex function)
Let f be a function defined in a neighborhood of z_0. Then, f is **continuous at** z_0 if

$$\lim_{z \to z_0} f(z) = f(z_0).$$

Equivalently, f is continuous at z_0 if for any given real $\epsilon > 0$, there exists a $\delta > 0$ such that

$$|z - z_0| < \delta \implies |f(z) - f(z_0)| < \epsilon.$$

A function is said to be **continuous on a set** S if it is continuous at each element of S. If f is continuous on the domain, we call f **continuous**.

Continuity on the domain can be seen interpretted as the following: any arbitrarily small change in the variable z will imply an arbitrarily small change in function value.

Definition A.4. (Derivative and Differentiability)
Let f be a function defined in a neighborhood of a point z_0. Then, the **derivative** of f at z_0 is given by

$$\frac{d}{dz} f(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0},$$

provided this limit exists. Such a function f is said to be **differentiable at the point** z_0. Alternatively, f is differentiable at z_0 if and only if it can be written as

$$f(z) = f(z_0) + A(z - z_0) + \eta(z)(z - z_0),$$

where $A = f'(z_0)$ and $\eta \to 0$ as $z \to z_0$.

Remark A.5. For a real function f with one real variable x defined in a neighborhood of a point x_0, x can approach x_0 from two directions. That is from the right side of the axis from the point and from the left. On the complex plane however, z can approach z_0 in infinitely many ways from all angles in the interval $[0; 2\pi)$.

Definition A.6. (Holomorphic Functions)
A function f of a complex variable is said to be **holomorphic** in an open set S if it has a derivative at every point of S. If f is holomorphic on the entire complex plane (without infinity), we say f is an **entire function**.

Example A.7. All polynomials of a complex variable have existing derivatives on the whole complex plane and are thus entire functions.
The rational function $f(z) = \frac{p(z)}{q(z)}$, with polynomials q and p of a complex variable are holomorphic in an open set. The rational function is not defined in the roots of q, say $\{\alpha_1, \ldots, \alpha_r\}$, but in the open set $S = \mathbb{C} \setminus \{\alpha_1, \ldots, \alpha_r\}$ and by the quotient rule the derivative $f'(z)$ is defined and f is thus holomorphic in S.
The complex exponential functions $f(z) = ae^{bz}$, $a, b \in \mathbb{C}$ are entire functions. The function is defined on all of $\mathbb{C}$ and the derivative $f'(z) = abe^{bz}$ exists at every point in $\mathbb{C}$. When $a = 0$ the function is the zero function, which is entire and when $b = 0$ the function is a constant, which is entire.

Recall that a complex function, $f(z)$, is said to be bounded on a domain $D \subseteq \mathbb{C}$ if there exists some $M \in \mathbb{R}$ such that

$$|f(z)| \leq M$$

for all $z \in D$.

Theorem A.8. (Cauchy's Inequality)
Let f be a holomorphic function inside and on a circle γ_R of radius R centered at z_0. If $|f(z)| \leq M$ for all z on γ_R, then the following inequality holds:

$$|f^{(n)}(z_0)| \leq \frac{n!M}{R^n}, \; n = 1, 2, \ldots.$$

Theorem A.9. (Liouville's Theorem)
The only bounded entire functions are the constant functions

A.2 Complex logarithm

Recall that a complex number, $z = a + bi$ can be written on polar form by

$$z = r(cos(\theta) + isin(\theta)),$$

where $r = |z| = \sqrt{a^2 + b^2}$ and θ is a number satisfying

$$cos(\theta) = \frac{x}{r} \text{ and } sin(\theta) = \frac{y}{r}.$$

We call θ the argument of z, denoted $arg(z)$, and since $\theta \pm 2n\pi$ is also a valid argument, we call the value $-\pi < arg(z) \leq \pi$ of $arg(z)$ the **principal value of the argument**, denoted $Arg(z)$.

Definition A.10. (Complex logarithm)
Let z be a complex number. If $z \neq 0$, then we define the complex logarithm $log(z)$ to be any of the infinitely many values

$$log(z) = log(|z|) + iarg(z) = log(|z|) + iArg(z) + 2k\pi i,\ k \in \mathbb{Z}.$$

Remark A.11. Note, that $log(|z|)$ behaves like the real logarithm, as $|z|$ takes values in $\mathbb{R} \setminus (-\infty; 0]$.

Remember that for the real logarithm, we have for a positive real number x, that

$$e^{log(x)} = x.$$

The same relationship can be found for the complex logarithm and exponential function. Let $z = r(cos(\theta) + isin(\theta) = re^{i\theta} \neq 0$. Then $|z| = r$ and $arg(z) = \theta$. Hence $log(z) = log(r) + i\theta$, and we see

$$e^{log(z)} = e^{log(r)+i\theta} = e^{log(r)}e^{i\theta} = re^{i\theta} = z.$$

Theorem A.12. The logarithm $log(z)$ is holomorphic in the domain consisting of all points of the complex plane except those lying on the nonpositive real axis $D^* = \mathbb{C} \setminus (-\infty, 0]$. Furthermore,

$$\frac{d}{dz} log(z) = \frac{1}{z}$$

for $z \in D^*$.

Proof
Set $w = log(z)$. Let $z_0 \in D^*$ and $w_0 = log(z_0)$. We have to show that the limit

$$w'(z_0) = \lim_{z \to z_0} \frac{log(z) - log(z_0)}{z - z_0}$$

exists and is equal to $\frac{1}{z_0}$. Since $log(z)$ is continuous on D^*, $w \to w_0$ as $z \to z_0$. Thus it follows:

$$\begin{aligned} lim_{z \to z_0} \frac{log(z) - log(z_0)}{z - z_0} &= lim_{w \to w_0} \frac{w - w_0}{e^w - e^{w_0}} \\ &= lim_{w \to w_0} \frac{1}{\frac{e^w - e^{w_0}}{w - w_0}} \\ &= \frac{1}{e^{w_0}} \\ &= \frac{1}{e^{log(z_0)}} \\ &= \frac{1}{z_0} \end{aligned}$$

Note that the third step follows from the differentiation of the complex exponential function. □

A.3 Complex contours and curves

Definition A.13. (Curve in the complex plane)
Let $x(t)$ and $y(t)$ be continuous real-valued functions defined on the interval $[a, b]$. A **curve** γ in the complex plane is the range of the continuous function $z: [a, b] \to \mathbb{C}$ given by

$$z(t) = x(t) + iy(t).$$

The point $z(a)$ is called the **initial point** of the curve and $z(b)$ is called the **terminal point** of the curve. If we write $z(t) = x(t) + iy(t)$ in parametric form $z(t) = (x(t), y(t))$, then the curve γ is the set of points

$$\gamma = \{z(t) = (x(t), y(t)) \mid t \in [a, b]\},$$

called the **track** of γ. A curve is called **simple** if for all different $t_1, t_2 \in [a, b]$ $z(t_1) \neq z(t_2)$. That is, the curve does not cross itself.
A curve is said to be **closed** if $z(a) = z(b)$, that is the terminal point is the initial point of the curve.

Definition A.14. (Piecewise Continuous and Smooth Curves)
A curve γ given by the range of $z: [a, b] \to \mathbb{C}$ is said to be **piecewise continuous** if

1. $z(t)$ exists and is continuous for all but finitely many points in (a, b)
2. At any point $c \in (a, b)$ where z fails to be continuous, both the left limit and right limit

$$\lim_{t \to c^-} z(t) \text{ and } \lim_{t \to c^+} z(t)$$

exist and are finite.

3. At the end points the right limit $\lim_{t \to a^+} z(t)$ and the left limit $\lim_{t \to b^-} z(t)$ exist and are finite.

The curve is called piecewise smooth if z and z' are both piecewise continuous.

If all left and right limits in (a, b) exist, are equal and finite and the mentioned limits in the end points exist and are finite, the curve is said to be **continuous on** $[a, b]$. Likewise if z and z' both are continuous, γ is said to be **smooth on** $[a, b]$.

Definition A.15. (Contour)
A **contour** γ is a sequence of smooth curves $\{\gamma_1, \ldots, \gamma_n\}$ such that the terminal point of γ_k coincides with the initial point of γ_{k+1} for $1 \leq k \leq n-1$. In this case, we write

$$\gamma = \gamma_1 + \ldots + \gamma_n.$$

A contour is clearly a piecewise smooth curve, as it consists of a collection of smooth curves.

A.4 Sequences and series

Recall that a sequence of complex numbers is a function whose domain is the set of non-negative integers and whose range is a subset of complex numbers, and denote a complex sequence as $\{z_n\}_{n=0}^{\infty}$. A sequence is said to have a limit z if for any $\epsilon > 0$ there exists an integer N, such that

$$|z_n - z| < \epsilon$$

for all $n > N$. Equivalently we write $z_n \to z$ as $n \to \infty$ or $\lim_{n \to \infty} z_n = z$. If a sequence has a limit it is called a **convergent sequence** and the sequence is said to **converge** to the limit z. If the sequence does not have a

limit, it is said to **diverge** and is called a **divergent sequence**
A sequence $\{z_n\}$ is called a **Cauchy sequence** if for any $\epsilon > 0$ there exists an integer $N > 0$ such that $n, m \geq N$ implies that

$$|z_n - z_m| < \epsilon,$$

and since $\mathbb{C}$ is a complete metric space, we have that every $\{z_n\}$ is a Cauchy sequence if and only if $\{z_n\}$ is convergent.
Now, recall that a **complex infinite series** is a formal expression of the form $z_0 + z_1 + \ldots$ or equivalently $\sum_{j=0}^{\infty} z_j$, where $z_j \in \mathbb{C}$ for all $j = 0, 1, 2, \ldots$. We denote the n-th partial sum as $s_n = \sum_{j=0}^{n} z_j$. If the sequence of partial sums $\{s_n\}_{n=0}^{\infty}$ has a limit s, the series is said to **converge**, or **sum**, to s, and we write

$$s = \sum_{j=0}^{\infty} z_j.$$

A series that does not converge is said to **diverge**.
Even further, if the series $\sum_{j=0}^{\infty} |z_j|$ converges, then $\sum_{j=0}^{\infty} z_j$ is said to be **absolutely convergent**. A series that is convergent, but not absolutely convergent is called **conditionally convergent**.

Example A.16. The geometric series $\sum_{j=0}^{\infty} ac^j$ with $|c| < 1$ is co. This is seen as in the n-th partial sum, we have the identity

$$\frac{a}{1-c} - (a + ac + ac^2 + \ldots + ac^n) = \frac{ac^{n+1}}{1-c},$$

and since $|c| < 1$ we have $|a||c|^{n+1}/|1-c| \to 0$ as $n \to \infty$, and thus we have

$$\lim_{n\to\infty} |\frac{a}{1-c} - \sum_{j=0}^{n} ac^n| = 0.$$

A.5 Sequences and series of complex functions

Let $\{f_n(z)\}_{n=0}^{\infty}$ be a sequence of complex functions defined on a domain $D \subseteq \mathbb{C}$. Suppose that for any $z \in D$ that the complex sequence $\{f_n(z)\}$ converges and define the limit $f(z) = \lim_{n\to\infty} f_n(z)$ for any $z \in D$. In this case, we say that $\{f_n(z)\}$ **converges pointwise** on D. If we have further, that for every $\epsilon > 0$ there exists an integer $N > 0$ such that $n \geq N$ implies

$$|f_n(z) - f(z)| < \epsilon$$

for all $z \in D$, $\{f_n(z)\}$ is said to **converge uniformly** on D. Note that uniform convergence implies that the same N can be used for all $z \in D$.
The series $\sum_{j=0}^{\infty} f_j(z)$ converges uniformly to $s(z)$ on D if the sequence of partial sums, $\{s_n(z)\}_{n=0}^{\infty}$ with $s_n(z) = \sum_{j=0}^{n} f_j(z)$, converges uniformly to $s(z)$ on D.
Now for some results on sequences and series of complex functions:

Theorem A.17. (Cauchy's Criterion)
The sequence $\{f_n(z)\}$ converges uniformly on the domain D to $f(z)$ if and only if for any $\epsilon > 0$ there exists an $N(\epsilon) > 0$ such that, for all $z \in D$, $n \geq N$, and any $m \in \mathbb{N}$, the inequality

$$|f_{n+m}(z) - f_n(z)| < \epsilon$$

holds.

Equivalently for a series of complex functions, we have:

Corollary A.18. The series $\sum_{j=0}^{\infty} f_j(z)$ converges uniformly on a domain D to $s(z)$ if and only if for any $\epsilon > 0$ there exists an $N(\epsilon) > 0$ such that, for all $z \in D$, $n \geq N$, and any $m \in \mathbb{N}$, the inequality

$$|s_{n+m}(z) - s_n(z)| < \epsilon$$

holds.

Now for a result on sequences of continuous functions:

Theorem A.19. If the sequence $\{f_n(z)\}$ converges uniformly on a domain D to $f(z)$ and each of the $f_n(z)$ is continuous on D, then $f(z)$ is continuous on D.

There is an equivalent result for uniformly convergent series of continuous functions.

Theorem A.20. (Weierstrass' M-test)
Let $\sum_{j=0}^{\infty} M_j$ be a convergent series of positive numbers. Suppose that $|f_j(z)| \leq M_j$ for all z on a domain D and for $j \geq 0$. Then, $\sum_{j=0}^{\infty} f_j(z)$ converges uniformly and absolutely on D.

Now for sequences of holomorphic functions on a domain D, we have the following:

Theorem A.21. Let $\{f_n(z)\}$ be a sequence of holomorphic functions on a domain D. If $\{f_n(z)\}$ converges uniformly to $f(z)$ on D, then $f(z)$ is holomorphic on D.

A.6 Singularities and poles

Definition A.22. (Singular points and isolated points)
A point z_0 is called a **singular point** (or a singularity) of the function $f(z)$ if $f(z)$ is not holomorphic at z_0, but is holomorphic at some point in $B(z_0, \epsilon)$ for all $\epsilon > 0$.
A singular point is called **isolated** if there exists $R > 0$ such that $f(z)$ is holomorphic on some punctured open disk $0 < |z - z_0| < R$.

Example A.23. The function $f(z) = Log(z)$ is holomorphic in $\mathbb{C} \setminus (-\infty, 0]$. Each point in $(-\infty, 0]$ is a singular point of $f(z)$ but not an isolated singularity by definition.

Remark A.24. If a function is holomorphic everywhere except for the singular point at z_0, and the limit $\lim_{z \to z_0} f(z) = a_0$ exists and is finite, we can remove the singularity by defining $f(z_0) = a_0$.

Example A.25. For the function $sinc(z) = \frac{sin(z)}{z}$ there is a singularity at $z = 0$, however we have $\lim_{z \to 0} sinc(z) = 1$, so we can define $sinc(0) = 1$ and remove the singularity such that the function is defined in this point.

Now, recall that a function that is holomorphic in an annulus domain $A = \{z \mid R_1 < |z - z_0| < R_2\}$ can be represented by a Laurent series

$$f(z) = \sum_{j=-\infty}^{\infty} a_j (z - z_0)^j.$$

If z_0 is a isolated singularity, the function has a Laurent series in a punctured disk around z_0, and if the singularity is removable, we have that $a_j = 0$ for $j < 0$, since else f would not have a finite limit. Now, since $(z - z_0)^j \to 0$ for $z \to z_0$, we also have, that if z_0 is a removable singularity

$$\lim_{z \to z_0} f(z) = a_0.$$

Definition A.26. (Pole of order m)
Let z_0 be an isolated singularity of f. If for the Laurent series of f around z_0, we have $a_{-m} \neq 0$ for some positive integer m but $a_j = 0$ for $j < -m$, we say that z_0 is a **pole of order** m. A pole of order 1 is called a **simple pole**.

Theorem A.27. (Riemann's Removable Singularity Theorem)
The function $f(z)$ has a removable singularity at z_0 if and only if any one of the following conditions hold:
1). $f(z)$ has a (finite) limit as $z \to z_0$.
2). $f(z)$ can be redefined at z_0 such that the new function is holomorphic at z_0.
3). $\lim_{z \to z_0}(z - z_0)f(z) = 0$
4). $f(z)$ is bounded in some punctured neighborhood of z_0.

Proof
Recall that if $f(z)$ has a removable singularity at z_0 then the Laurent series of f at z_0 takes the form

$$f(z) = a_0 + \sum_{n=1}^{\infty} a_n(z - z_0)^n, \ 0 < |z - z_0| < R.$$

Thus we see that conditions 1)-3) follows as $\lim_{z \to z_0} f(z) = a_0$, we can redefine $f(z_0) = a_0$ and

$$\lim_{z \to z_0}(z - z_0)f(z) = 0 \cdot a_0 = 0.$$

For 4), let z_0 be a removable singularity of $f(z)$. Then from the above, it is clear that the function

$$g(z) = \begin{cases} f(z), & 0 < |z - z_0| < R \\ a_0, & z = z_0 \end{cases}$$

is holomorphic on $|z - z_0| < R$, and hence bounded in some punctured neighborhood of z_0.
Conversely, suppose there is a punctured neighborhood $0 < |z - z_0| < r < R$ and a finite M such that on this neighborhood $|f(z)| \leq M$. Now, we have for the (negatively indexed) coefficients in the Laurent series of f around z_0, that $b_j = \frac{1}{2\pi i}\int_\gamma f(\xi)(\xi - z_0)^{j-1}d\xi, \ j = 1, 2, \ldots$, where γ is any positively oriented, simple, closed contour around z_0 in an annulus $R_1 \leq |z - z_0| \leq R_2$. If we let γ be the sphere of radius R_1, then the length of γ is $2\pi R_1$ and the integrand in the expression of b_j is bounded by MR_1^{j-1}, so we have that $|b_j| \leq MR_1^j$, and letting $R_1 \to 0$, we obtain $b_j = 0$ for all $j = 1, 2, \ldots$. Thus the Laurent series of f around z_0 reduces to the above case, and $f(z)$ has a removable singularity at z_0. ☐

Appendix B | Abstract Algebra

This chapter is based on [2].

B.1 Groups and Subgroups

To describe modular forms, we need to cover select results from group theory and to introduce some special groups. So let us first define a group:

Definition B.1. (Group)
A pair $(G, \circ)$ consisting of a set G and a composition $\circ : G \times G \to G$ is called a **group** if it satisfies the following three properties:

1. The set G is closed under the composition of $\circ$. That is, for all $x, y \in G$, we have

$$x \circ y \in G$$

2. The compositions is associative:

$$s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$$

for every $s_1, s_2, s_3 \in G$.

3. There is a neutral element $e \in G$ such that

$$e \circ s = s \circ e = s$$

for every $s \in G$.

4. For every $s \in G$ there is an inverse element $t \in G$ such that

$$s \circ t = t \circ s = e$$

A group $(G, \circ)$ is called **abelian** if $x \circ y = y \circ x$ for every $x, y \in G$ (commutativity). The number of elements $|G|$ in G is called the **order** of G.

An example of a composition is addition, multiplication, function composition, matrix multiplication, etc. By the definition $(\mathbb{N}, +)$ is not a group, as $\mathbb{N}$ does not contain the neutral element 0 or negative numbers, so no additive inverse exists for any element in $\mathbb{N}$.
$(\mathbb{Z}, \cdot)$ is not a group. $\mathbb{Z}$ does contain the neutral element 1, but does not contain any multiplicative inverses, as there are no fractions in $\mathbb{Z}$. For example the inverse of $2 \in \mathbb{Z}$ is $\frac{1}{2} \notin \mathbb{Z}$.
When the composition of the group is presented, we usually omit the symbol (for example if matrix multiplication is implied, then we just write AB for two matrices A and B of compatible dimensions)
In this project, we are interested in matrix groups. The set of all 2×2 matrices with real entries (the same holds for complex entries),

$$M_2(\mathbb{R}) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\},$$

does not form a group under the composition of matrix multiplication. The neutral element is the identity matrix I_2 which is certainly contained in $M_2(\mathbb{R})$, however, recall that a matrix A is invertible if and only if it is non-singular, that is $det(A) \neq 0$. Since $M_2(\mathbb{R}$ also contains singular matrices, which are not invertible, there are no inverse elements of these matrices. Thus by definition $M_2(\mathbb{R})$ (and $M_2(\mathbb{C})$) does not form a group under the composition of matrix multiplication.

Now that we have presented a condition for the existence of inverse elements for matrices, we now observe the set of all non-singular 2×2 matrices of real entries (again, the same holds for complex entries)

$$GL_2(\mathbb{R}) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R},\ det(A) = ad - bc \neq 0 \right\}.$$

Now, since we have for the determinant

$$det(AB) = det(A)det(B) \neq 0$$

for $A, B \in GL_2(\mathbb{R})$, we must have that any product of non-singular matrices must result in a non-singular matrix. Thus $GL_2(\mathbb{R})$ is closed under the composition of multiplication, and since it is associative under matrix multiplication, it contains the identity matrix and every element has a corresponding inverse, $GL_2(\mathbb{R})$ is a group under composition of matrix multiplication. This group is called the **general linear group** (of 2×2 matrices with real entries).

Definition B.2. (Subgroup)
A **subgroup** of a group G is a non-empty subset $H \subseteq G$ such that the composition of G makes H into a group. That is H is a subgroup of G if and only if

1. $e \in H$
2. $x^{-1} \in H$ for every $x \in H$
3. $xy \in H$ for every $x, y \in H$

We sometimes denote that H is a subgroup of G by $H \leq G$ (for proper subgroups we write $H < G$. That is when $H \subset G$)

Example B.3. We know that $GL_2(\mathbb{C})$ is a group under matrix multiplication. We have that $GL_2(\mathbb{R}) < GL_2(\mathbb{C})$, since $I_2 \in GL_2(\mathbb{R})$, every real non-singular matrix is invertible with a corresponding real inverse, and the product of real non-singular matrices yield a real non-singular matrix.

Note that every inverse of a 2×2 non-singular matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is on the form

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Now, we see that $GL_2(\mathbb{Q}) < GL_2(\mathbb{R})$, since $I_2 \in GL_2(\mathbb{Q})$, the determinant of a rational matrix is rational and thus every rational non-singular matrix has a corresponding rational inverse and the product of rational non-singular matrices yield a rational non-singular matrix, as the inner products of the rational column/row vectors will each be rational. Lastly, we have that $GL_2(\mathbb{Z})$ is not a group nor a subgroup, as for non-unit determinant the entries of the corresponding inverse can be rational and not integers.

With the same arguments, we have that $SL_2(\mathbb{C}) > SL_2(\mathbb{R}) > SL_2(\mathbb{Q})$, but even further, we have $SL_2(\mathbb{Z}) < SL_2(\mathbb{Q})$, since $I_2 \in SL_2(\mathbb{Z})$, the determinant of each element is 1 so the corresponding inverses have integer entries and exist, and a product of unit-determinant integer matrices yield a unit-determinant integer matrix. Lastly, we note that $SL_2(\mathbb{N})$ is nor a group or a subgroup of $SL_2(\mathbb{Z})$, since the corresponding inverse of a natural matrix can contain negative entries.

Definition B.4. (Cosets)
Let H be a subgroup of G and $g \in G$. Then the subset

$$gH = \{gh \mid h \in H\} \subseteq G$$

is called a **left coset** of H. Similarly we call the subset

$$Hg = \{hg \mid h \in H\} \subseteq G$$

a **right coset** of H. The set of left cosets of H is denoted G/H. The set of right cosets of H is denoted $H \setminus G$.

Definition B.5. (Normal Subgroup)
A subgroup N of a group G is called **Normal** if

$$gNg^{-1} = \{gng^{-1} \mid n \in N\} = N$$

for every $g \in G$. We sometimes denote this $N \trianglelefteq G$ ($N \triangleleft G$ for proper subgroups).

B.2 Group Homomorphisms and Isomorphisms

Definition B.6. (Group Homomorphism)
Let G and K be groups. A map $f: G \to K$ is called a **group homomorphism** if $f(xy) = f(x)f(y)$ for every $x, y \in G$.
We say that a group homomorphism f is **surjective** if $f(G) = K$ and that f is **injective** if $f(x) = f(y)$ implies that $x = y$. A group homomorphism that is surjective and injective (also called **bijective**) is called a **group isomorphism**.

The determinant is a group homomorphism $det: GL_2(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$, where $\cdot$ denotes multiplication, since

$$det(AB) = det(A)det(B) \neq 0$$

for $A, B \in GL_2(\mathbb{R})$.

Definition B.7. (Kernel)
The **Kernel** of a group homomorphism $f: G \to K$ is

$$Ker(f) = \{g \in G \mid f(g) = e\},$$

where e denotes the identity element in K.

The kernel of the determinant is the set of all 2×2 matrices with real entries of determinant 1, that is

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

We call this **the special linear group** (of 2×2 matrices with real entries)

Proposition B.8. Let $f:\ G \to K$ be a group homomorphism. We have:
1. The image $f(G) \subseteq K$ is a subgroup of K.
2. The kernel $Ker(f) \subseteq G$ is a normal subgroup of G
3. f is injective if and only if $Ker(f) = \{e\}$, where e is the identity element in G.

Proof
1. Since $f(e) = f(ee) = f(e)f(e)$ it follows that $e = f(e)$. This shows that $e \in f(G)$. Let $x \in G$. Then

$$e = f(e) = f(xx^{-1}) = f(x)f(x^{-1}),$$

and

$$e = f(e) = f(x^{-1}x) = f(x^{-1})f(x),$$

and thus $f(x^{-1}) = f(x)^{-1}$. Thus if $f(x) \in f(G)$ then $f(x)^{-1} \in f(G)$. Finally, if $f(x), f(y) \in f(G)$ then

$$f(x)f(y) = f(xy) \in f(G),$$

and thus $f(G)$ is a subgroup of K.
2. We now know that $e \in Ker(f)$ since $f(e) = e$. If $x \in Ker(f)$ then $e = f(x) = f(x)^{-1} = f(x^{-1})$ and thus $x^{-1} \in Ker(f)$. If $x, y \in Ker(f)$ then

$$f(xy) = f(x)f(y) = ee = e,$$

so $x, y \in Ker(f)$ implies that $xy \in Ker(f)$. So the kernel is a subgroup of G.
Let $N = Ker(f)$. Then for every $g \in G$ and $x \in N$, we have

$$f((gx)g^{-1}) = (f(g)f(x))f(g^{-1}) = f(g)ef(g)^{-1} = e.$$

This shows that $gNg^{-1} \subseteq N$. The inclusion $N \subseteq gNg^{-1}$ for every $g \in G$ follows from the fact that we have the inclusion $gNg^{-1} \subseteq N$ for every $g \in G$.
3. Since $f(e) = e$ it follows that $Ker(f) = \{e\}$ if f is injective. Conversely, assume $Ker(f) = \{e\}$ and $f(x) = f(y)$, then

$$f(y)^{-1}f(x) = f(y^{-1})f(x) = f(y^{-1}x) = e,$$

which implies that $y^{-1}x \in Ker(f)$. This implies that $y^{-1}x = e$ or $x = y$. □ From this proof it follows that $SL_2(\mathbb{R})$ is a normal subgroup of $GL_2(\mathbb{R})$.

Theorem B.9. (First Isomorphism Theorem)
Let G and K be groups and $f:\ G \to K$ a group homomorphism with kernel $N = Ker(f)$. Then

$$\tilde{f}:\ G/N \to f(G)$$

given by $\tilde{f}(gN) = f(g)$ is a well defined map and a group isomorphism.

Proof
First, we know from the previous proof that $f(x) = f(y)$ if and only if $y^{-1}x \in Ker(f) = N$ for every $x, y \in G$. This implies that $x \in yN$ and $y \in xN$ and thus $xN \subseteq yN$ and $yN \subseteq xN$ resulting in $xN = yN$ if and only if $f(x) = f(y)$. Thus $\tilde{f}$ given by $\tilde{f}(gN) = f(g)$ is a well defined and injective map. It is a group homomorphism since

$$\begin{aligned}\tilde{f}((g_1N)(g_2N)) &= \tilde{f}((g_1g_2)N)\\ &= f(g_1g_2)\end{aligned}$$

$$= f(g_1)f(g_2)$$
$$= \tilde{f}(g_1N)\tilde{f}(g_2N)$$

for $g_1N, g_2N \in G/N$. It is surjective because f is surjective onto $f(G)$. Thus $\tilde{f}$ is a group isomorphism. $\square$
Recall that $SL_2(\mathbb{R})$ is the kernel of the determinant map $det:\ GL_2(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$. Thus we have a group isomorphism

$$\tilde{f}:\ GL_2(\mathbb{R})/SL_2(\mathbb{R}) \to det(GL_2(\mathbb{R})).$$

B.3 Group Actions

Definition B.10. (Group Action)
Let $(G, \circ)$ be a group and S be a set. We will say that G **acts**(from the left) on S if there is a map

$$\alpha:\ G \times S \to S,$$

such that

1. $\alpha(e, s) = s$ for every $s \in S$, with $e \in G$ being the identity element.
2. $\alpha((g \circ h), s) = \alpha(g, \alpha(h, s))$ for every $g, h \in G$ and every $s \in S$.

Definition B.11. (Orbit and Stabilizer)
Let $\alpha:\ G \times S \to S$ be an action of G on S, $X \subseteq S$ a subset of S and $s \in S$ an element of S. Then

$$Gs = \{\alpha(g, s) \mid g \in G\}$$

is called the **orbit** of s (under the action of G). The **set of orbits** is denoted

$$S/G = \{Gs \mid s \in S\}.$$

Let $gX = \{\alpha(g, x) \mid x \in X\}$, where $g \in G$. Then

$$G_X = \{g \in G \mid gX = X\}$$

is called the **stabilizer** of X.

Example B.12. Matrix-vector products are group actions, where a matrix group acts on a vector space. For example, the matrix-vector product on the form $Av = w$, $A \in GL_2(\mathbb{R})$ and $v, w \in \mathbb{R}^2$ is indeed an action as
1. $I_2v = v$ for all $v \in \mathbb{R}^2$
2. $(AB)v = A(Bv)$ for all $A, B \in GL_2(\mathbb{R})$, $v \in \mathbb{R}^2$.
The stabilizer of this action contains only the identity matrix, while the orbits of each vector in $\mathbb{R}^2$ is all of $\mathbb{R}^2$, since all the matrices are non-singular and thus of full rank.

Definition B.13. (Group Center)
Let $(G, \circ)$ be a group. The **Center** of G is the set

$$Z(G) = \{g \in G \mid g \circ x = x \circ g \text{ for every } x \in G\},$$

that is the set of elements in G that commute with every element in G.

Example B.14. The center of $GL_2(\mathbb{R})$ is the set of all scalar matrices

$$Z(GL_2(\mathbb{R})) = \{A \in GL_2(\mathbb{R}) \mid A = b \cdot I_2,\ b \in \mathbb{R}\}.$$

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in GL_2(\mathbb{R})$. We will look at the two products AB and BA and see, what conditions on one of them, in order for these matrices to commute.
So,

$$AB = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}.$$

$$BA = \begin{bmatrix} ae + cf & eb + df \\ ag + ch & bg + dh \end{bmatrix}.$$

Now, for $AB = BA$, we must have either $b, c = 0$ and $a = d$, or $f, g = 0$ and $e = h$. This was arbitrarily shown, so this is also the center for $GL_2(\mathbb{C})$.

Definition B.15. (Projective General Linear Group) The **projective general linear group of** 2×2 **matrices with real entries** is the set

$$PGL_2(\mathbb{R}) = GL_2(\mathbb{R})/Z(GL_2(\mathbb{R})$$

under the composition of matrix multiplication. That is, the set of all left cosets of the center of the general linear group.

One can define the **projective special linear group** likewise with $SL_2(\mathbb{R})$ and $Z(SL_2(\mathbb{R}))$.