Modular forms and congruences

Breki Pálsson

13. february 2023

Motivation

A classical application of modular forms is to find equalities of arithmetical functions, by finding modular forms whose Fourier coefficients are those arithmetical functions, and then finding identities of modular forms which follow from dimensional considerations. Our goal for this session will be to prove the following well know identities:

$$\sigma_7(n) = \sigma_3(n) + \sum_{i=1}^{n-1} \sigma_3(i)\sigma_3(n-i)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040\sum_{i=1}^{n-1} \sigma_3(i)\sigma_5(n-i)$$

$$\sigma_{13}(n) = 21\sigma_5(n) - 20\sigma_7(n) + 10080\sum_{i=1}^{n-1} \sigma_5(i)\sigma_7(n-i)$$

We note that these identities can be proved without using modular forms, but once we have set up enough of the theory of modular forms, results like these follow almost immediately.

> entre deux vérités du domaine réel, le chemin le plus facile et le plus court passe bien souvent par le domaine complex.
>
> -Paul PainLevé.

1 Introduction to Modular Forms

We define the *full modular group*

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

Exercise 1.1. Show that
$$\Gamma/\{\pm 1\} \cong \langle S, T | S^2 = I, (ST)^3 = I \rangle$$
Where $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Next we can define an action of elements of Γ on the Riemann sphere $\widehat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ by

$$f(z) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}(z) = \frac{az+b}{cz+d}, z \in \mathbb{C}$$

And we extend this to the whole Riemann sphere by defining $f(-d/c) = \infty$ and $f(\infty) = a/c$. These transformations are known as *Mobius transformations*.

We define the *Poincaré upper half plane* as

$$\mathcal{H} = \{z \in \mathbb{C} | \Im(z) > 0\}$$

Exercise 1.2. Proof that $\gamma z \in \hat{\mathcal{H}} := \mathcal{H} \cup \{\infty\}$ for $\gamma \in \Gamma$ and $z \in \hat{\mathcal{H}}$.

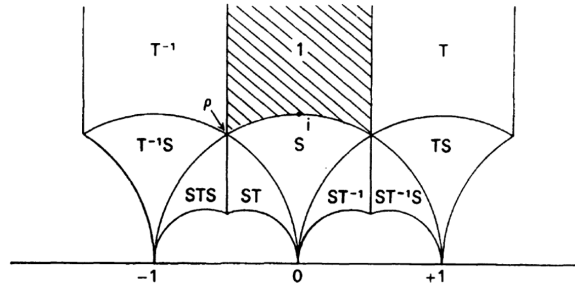$\{1, T, TS, ST^{-1}S, S, ST, STS, T^{-1}S, T^{-1}\}$ of the group G.

Figure 1: Above we can see a visual representation of the action of the group $G := \Gamma$ on the striped area.

If $f : \mathcal{H} \to \mathbb{C}$ is a meromorphic function which satisfies the transformation formula

$$f(\gamma z) = (cz + d)^k f(z), \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma, z \in \mathcal{H}$$

then we say that f is *weakly modular of weight k for Γ* in particular

$$f(Sz) \quad = f(-1/z) = (-z)^k f(z) f(Tz) \quad = f(z+1) = f(z)$$

The second equation tells us that f has a Fourier expansion of the following form in a suitable neighborhood of the origin, wit the origin removed:

$$f(q) = \sum_{n \in \mathbb{Z}} a_n q^n, \quad \text{with } q := e^{2\pi i z};$$

If there exists a m such that $a_n = 0$ for $n < m$ we say that f is *meromorphic at ∞*. If in addition to this $a_n = 0$ for all $n < 0$, then we say that f *holomorphic at ∞*

We call $f(q)$ the *Fourier expansion of f at ∞*, or simply the *Fourier expansion of f*.

Definition 1.1 (Modular form)

Let k be an integer. We say that a meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight k for Γ* if

1. f is weakly modular of weight k for Γ

2. f is holomorphic on $\mathcal{H}$

3. f is holomorphic at ∞

We call the set of all modular forms of weight k for Γ, denoted $M_k(\Gamma)$ or simply M_k.

We define the value of f at ∞ to be the limit $f(z)$ as $z \to i\infty$, and write it as $f(\infty)$. If f is zero at infinity then we call f a *cusp form*.The set of cusp forms for Γ, denoted $S_k(\Gamma)$ or simply S_k.

Exercise 1.3. Let $f \in M_k(\Gamma)$ and $g, h \in M_l(\Gamma)$ then $fg \in M_{k+l}(\Gamma)$, also note that $cg \in M_l(\Gamma)$, for all $c \in \mathbb{C}$ and $g + h \in M_l(\Gamma)$. This gives the set of modular forms of weight k a structure of a $\mathbb{C}$ vector space and in addition gives the set of all modular forms on Γ, denoted $M(\Gamma)$ a structure of a graded $\mathbb{C}$-algebra.

Show a similar result for S_k.

One other way to look at S_k is that it is the kernel of the map $M_k \to \mathbb{C}, f \to f(\infty)$.

The condition for a function to be a modular form is rather strong and one naturally can ask what are examples of them.

First we can note that if f is a modular form of weight k then

$$f\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} z\right) = f(z) = (-1)^k f(z)$$

so if k is an odd number then $f(z) = -f(z)$ and therefore f must be the zero function. In the next section we will see an example of a nontrivial modular form.

2 Eisenstein series

Proposition 2.1 (Eisenstein series)

Let k be an even integer which is at least 4 and let $z \in \mathcal{H}$. The function

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

is a modular form of weight k for Γ.

Proof

First we show that $G_k(z)$ is holomorphic on $\mathcal{H}$ and at ∞. Fix $A, B \in \mathbb{R}_+$ and then define $\mathscr{D}_{A,B}$ to be the set of $z \in \mathcal{H}$ such that $Im(z) > A$ and $|Re(z)| < B$ It's possible to show that there exists a $C > 0$ such that for all $(\nu, \mu) \in \mathbb{R}^2 - \{0\}$ and all $z \in \mathscr{D}_{A,B}$ then $|\nu z + \mu| > C \sup(|\nu|, |\mu|)$. Note that the number of elements of $\mathbb{Z}^2$ such that the taxicab norm is equal to a given number $s \in \mathbb{N}_+$ is equal to $8s$. Now we have

$$|G_k(z)| \leq \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (n,m)\neq(0,0)}} \frac{1}{|mz+n|^k} \leq \frac{1}{C^k} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (n,m)\neq(0,0)}} \frac{1}{\sup(n,m)^k} \leq \frac{1}{C^k} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (n,m)\neq(0,0)}} \frac{8s}{s^k}$$

This means that the series converges normally on $\mathscr{D}_{A,B}$ and therefore $G_k(z)$ is a holomorphic function on $\mathcal{H}$. By absolute convergence of $G_k(z)$ along with the bijection

$$(n,m) \to (m, n+m), \ \ (n,m) \to (n, -m)$$

give us the relations

$$G_k(z+1) = G_k(z), \ \ G_k(-1/z) = z^k G_k(z)$$

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

To show that $G_k(z)$ is finite at ∞, we will show that $G_k(z)$ approaches an explicit finite limit as $z \to i\infty$. The terms of $G_k(z)$ are of the form $1/(mz+n)^k$, those which have $m \neq 0$ will contribute 0 to the sum, while those which have $m = 0$ each contribute $1/n^k$. Therefore we have

$$\lim_{z \to i\infty} G_k(z) = \sum_{0 \neq n \in \mathbb{Z}} \frac{1}{n^k} = 2\zeta(k)$$

Now let us suppose that z satisfies $|z| \geq 1$ and $\Re(z) \leq 1/2$; we

■

Exercise 2.1. Proof that there exists a $C > 0$ such that for all $(\nu, \mu) \in \mathbb{R}^2 - \{0\}$ and all $z \in \mathscr{D}_{A,B}$ then $|\nu z + \mu| > C \sup(|\nu|, |\mu|)$ We can see from the proof that $G_k(z)$ is not zero at infinity.

3 Bernoulli numbers

Definition 3.1 (Bernouilli numbers)

We will define the *Bernouilli numbers*, B_n, to be the numbers that satisfy the equation

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!}$$

Exercise 3.1. Show that $B_1 = -1/2, B_2 = 1/6, B_3 = 0$ and $B_4 = -1/30$ and that $B_{2r+1} = 0$ for $r \geq 1$.

If a prime does not divide the numerator of any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ then it is said to be a *regular prime* and *irregular* otherwise. Ernst Kummer proved that for all regular primes Fermat's equation with regular prime exponents is unsolvable.

Siegel conjectured has that about 61% of primes are regular, which would lead to the statement that there are infinitely many regular primes however no one has been able to prove the two conjectures. Jensen however proved in a short paper in 1915 that there are infinitely many irregular primes.

Another interesting fact about Bernoulli numbers are their relations to the Riemann zeta function via euler's celebrated formulas

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

4 Fourier expansions of Modular forms

The Fourier expansions of modular forms are very arithmetically interesting, for example, many modular forms have Fourier coefficients which are multiplicative or satisfy recurrence relations.

We have already seen that a modular form f has a Fourier expansion in some suitable neighborhood of the origin. We also computed the first coefficient a_0 of the Fourier expansion of $G_k(z)$. We will now exhibit the complete Fourier expansion of $G_k(z)$.

Proposition 4.1

Let $k \geq 4$ be an even integer, and let $z \in \mathcal{H}$. The modular form $G_k(z)$ has Fourier expansion

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

where we define $\sigma_k(n)$ to be the function

$$\sigma_k(n) := \sum_{0<m|n} m^k$$

Proof

Using the identity $\frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right) = \frac{\pi}{\tan(\pi z)}$ we will proof the result, note that the series on the left is absolutely convergent. The function on the right is periodic of period 1 and therefore has a Fourier expansion given by

$$\frac{\pi}{\tan(\pi z)} = \pi \frac{\cos(\pi z)}{\sin(\pi z)} = \pi i \frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}} = -\pi i \frac{1+q}{1-q} = 2\pi i \left(\frac{1}{2} + \sum_{r=1}^{\infty} q^r \right),$$

where $q = e^{2\pi i z}$. Using this relation and differentiating the first equation $k - 1$ times and divide

by $(-1)^{k-1}(k-1)!$ to get

$$\frac{1}{z^k} \sum_{n=1}^{\infty} \left(\frac{1}{(z+n)^k} + \frac{1}{(z-n)^k} \right)$$

now for the Fourier expansion of $G_K(z)$

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

$$= \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} r^{k-1} q^{mr}$$

$$= \frac{(2\pi i)^k}{(k-1)!} \left(-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n \right)$$

∎

Exercise 4.1. Show that $\frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right) = \frac{\pi}{\tan(\pi z)}$ using the formula $\sin(x) = x^2 \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2 \pi^2} \right)$

A standard notation for Eisenstein series is to write

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

this is called the *normalized Eisenstein series of weight k*. For these modular forms the following identities hold:

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

$$E_4(q) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n$$

$$E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)q^n$$

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

$$E_{10}(q) = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n)q^n$$

$$E_{12}(q) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n)q^n$$

$$E_{14}(q) = 1 + 240 \sum_{n=1}^{\infty} \sigma_{13}(n)q^n$$

We saw that if $k = 2$ then the sum in G_2 does not converge but what we can do to give E_2 some meaning is to define by following the pattern and defining it by its Fourier expansion

There is a holomorphic function E_2 which has Fourier expansion at ∞

$$E_2(q) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n,$$

which satisfies the following transformation formula

$$E_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 E_2(z) + \frac{12}{2\pi i} c(cz+d)$$

We will not proof this proposition but one can be found in [3]

5   Ramanujan Δ function

In the early 20th century Srinvasa Ramanujan studied the explicit Fourier expansions of considerations well-known modular forms, such as the Δ function, given by

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

where $q = e^{2\pi i z}$. We can expand the product in the definition to get

$$\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^8 - 113643q^9 + \ldots$$

Ramanujan observed in 1915 that $\tau(n)$ is multiplicative, i.e. $\tau(mn) = \tau(m)\tau(n)$ for coprime n and m.

The function $\Delta(z)$ is a cusp form of weight 12.

Proof

Since $\Delta(z) \neq 0$, we can consider its logarithmic derivative. We find

$$\frac{1}{2\pi i}\frac{d}{dz}log(\Delta(z)) = \frac{1}{2\pi i}\frac{d}{dz}\left(q \prod_{n=1}^{\infty}(1-q^n)^{24}\right) = \frac{1}{2\pi i}\frac{d}{dz}\left(log(q) + 24\sum_{n=1}^{\infty}log(1-q^n)\right)$$

Since $q = e^{2\pi i z}$ we have $\frac{1}{2\pi i}\frac{d}{dz}$ and therefore

$$\frac{1}{2\pi i}\frac{d}{dz}log(\Delta(z)) = 1 - 24\sum_{n=1}^{\infty}n\frac{q^n}{1-q^n} = 1 - 24\sum_{n=1}^{\infty}n\sum_{d=1}^{\infty}q^{dn} = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n = E_2(z).$$

Now we have already seen that

$$E_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 E_2(z) + \frac{12}{2\pi i}c(cz+d).$$

Combining the equations above and using the fact that

$$\frac{d}{dz}\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^2}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we deduce that

$$\frac{1}{2\pi i}\frac{d}{dz}log\left(\frac{\Delta\left(\frac{az+b}{cz+d}\right)}{(cz+d)^{12}\Delta(z)}\right) = \frac{1}{(cz+d)^2}E_2\left(\frac{az+b}{cz+d}\right) - \frac{12}{2\pi i}\frac{c}{cz+d} - E_2(z) = 0.$$

In other words, $log(\Delta\left(\frac{az+b}{cz+d}\right)) = log(s(\gamma))log((cz+d)^{12}\Delta(z))$, where $s(\gamma)$ is a non zero constant that depends only on γ that is

$$\Delta\left(\frac{az+b}{cz+d}\right) = s(z)(cz+d)^{12}\Delta(z)$$

we want to show that $s(\gamma) = 1$ for all $\gamma \in \Gamma$.

First note that for $\gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ with $\gamma_3 := \gamma_1\gamma_2 = \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$ we have

$$s(\gamma_1)s(\gamma_2)\Delta(z) = s(\gamma_1)\Delta(\gamma_2 z)(c_2 z + d_2)^{-12} = \Delta(\gamma_1\gamma_2 z)(c_3 z + d_3)^{-12} = s(\gamma_1\gamma_2)\Delta(z).$$

Therefore $s : \Gamma \to \mathbb{C}$ is a homomorphism so we just need to prove that $s(T) = s(S) = 1$.

By definition we have $\Delta(Tz) = \Delta(z)$ so $s(T) = 1$ and to show that $s(S) = 1$ put $z = i$ in the equation $z^{-12}\Delta(\frac{-1}{z}) = s(S)\Delta(z)$.

■

6 Dimension of $M_k(\Gamma)$ and $S_k(\Gamma)$

We have already seen that M_k and S_k have a structure of a $\mathbb{C}$ vector space. In this section we will look at the dimension of the $\mathbb{C}$ vector spaces of modular forms of weight k and cusp forms of weight k.

First let us define the order of a meromorphic function $f : \mathcal{H} \to \mathbb{C}$ at a given point $x \in \mathcal{H}$, denoted $v_x(f)$, as the integer n such that $f(z)/(z-x)^n$ is holomorphic and non null. We can furthermore define $v_\infty(f)$ as the order of f in the Fourier expansion at $q = 0$. This integer is necessarily positive since it counts the number of poles of f at x.

When f is a modular form of weight k then the identity

$$f(z) = (cz+d)^{-k}f(\frac{az+b}{cz+d})$$

shows us that $v_x(f) = v_{\gamma x}(f)$ if $\gamma \in \Gamma$. Thus we can define $v_{\bar{x}}(f)$ where $\bar{x}$ is in the quotient $\mathcal{H}/\Gamma$ because $v_x(f)$ does not depend on the representative of x in $\mathcal{H}/\Gamma$.

now for a lemma that is very useful when studying the dimension of $M_k(\Gamma)$ will be stated without proof but the reader is encouraged to see [7] for a complete proof.

Theorem 6.1 (The $k - 12$ lemma)

Let f be a modular form of weight k that is not the zero function, then we have the equation:

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{x\in\mathcal{H}/G} v_x(f) = \frac{k}{12}$$

Using this lemma we proof the proposition

Proposition 6.1 (Formulae for the full modular group)

Let k be an integer. Then

- $M_0(\Gamma) = \mathbb{C}$

- $M_2(\Gamma) = 0$, and if $k < 0$ or if k is odd then $M_k(\Gamma) = 0$

- If $k \in \{4, 6, 8, 10, 14\}$, then $M_k(\Gamma) = \mathbb{C}E_k$

- If $k < 12$ or $k = 14$ then $S_k(\Gamma) = 0$, $S_{12}(\Gamma) = \mathbb{C}\Delta$ and if $k \geq 16$ then $S_k(\Gamma) = \Delta M_{k-12}(\Gamma)$

- If $k \geq 4$ then $M_k(\Gamma) = S_k(\Gamma) \oplus \mathbb{C}E_k$

Proof

i) We know that the constant functions are elements of M_0 and we want to show the reverse. Let $f \in M_0$ be an arbitrary modular form of weight 0 and let $z \in \mathbb{C}$ be any element in the image of f. Then $f(z) - c \in M_0$ has a zero in $\mathcal{H}$, i.e. one of the terms in the equation in the $k - 12$ lemma is strictly positive. Since the right-hand side is 0, this can only happen if $f(z) - c$ is the zero function, i.e. f is constant.

ii) We already saw that $M_k = 0$ if k is odd. if $k = 2$ or $k < 0$ then $k/12$ is negative or $1/6$, which has no positive solutions on the left-hand side

iii) If $k \in \{4, 6, 8, 10, 14\}$, then there is only one possible way of choosing the $v_x(f)$ in the $k - 12$ lemma is:

- $k = 4 : v_\rho(f) = 1$ and all other $v_x(f) = 0$.

- $k = 6 : v_i(f) = 1$ and all other $v_x(f) = 0$.

- $k = 8 : v_\rho(f) = 2$ and all other $v_x(f) = 0$.

- $k = 10 : v_\rho(f) = v_i(f) = 1$ and all other $v_x(f) = 0$.

- $k = 14 : v_\rho(f) = 2, v_i(f) = 1$ and all other $v_x(f) = 0$.

iv) If $f \in S_k$ we have $v_\infty(f) > 0$, which is not possible by the $k - 12$ lemma for $k < 12$ or $k = 14$.

v) We know that $v_\infty(\Delta) = 1$ and by the $k - 12$ lemma this can be the only zero of Δ. Therefore for any $f \in S_k$ the function $f\Delta$ is a modular form of weight $k - 12$.

vi) If $f \in M_k$ is not a cusp form then its Fourier expansion at ∞ has a non zero constant term c. We note that $f - cE_k$ ia a modular form of weight k and has a zero constant term in its Fourier expansion, i.e. $M_k = \mathbb{C}E_2 \bigoplus S_k$

∎

Theorem 6.2 (Dimenton of $M_k(\Gamma)$ and $S_k(\Gamma)$)

Let K be an even positive integer. Then

$$\dim M_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1, & \text{if } k \not\equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor, & \text{if } k \equiv 2 \mod 12 \end{cases}$$

and

$$\dim S_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor, & \text{if } k \not\equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor - 1, & \text{if } k \equiv 2 \mod 12 \end{cases}$$

> **Proof**
>
> We will proceed by induction. We already know the formulas to be true for $k \leq 14$. Now by the 5th point of the proposision above we know that the dimention of S_k is one less than the dimension of M_k. It suffices to prove the theorem for M_k.
>
> Assume we have proved the formula for k and now we consider the dimension of M_{k+12}. From the preceding proposition we see that
>
> $$M_{k+12} = \mathbb{C}E_{k+12} \bigoplus S_{k+12} = \mathbb{C}E_{k+12} \bigoplus \Delta M_k,$$
>
> and now we use the induction hypothesis to get the result.
>
> ■

Let's now show that it can be equivalently defined as

$$\Delta = \frac{E_4^3 - E_6^2}{1728}$$

.

We know that Δ is a modular form of weight 12. Also by the graded $\mathbb{C}$ algebra structure of modular forms we have that $E_4^3, E_6^2 \in M_12$. Now the constant term of E_4^3 and E_6^2 are both equal to one and thus $E_4^3 - E_6^2 \in S_12$. But we have seen that the dimension of S_12 as a $\mathbb{C}$ vector space is equal to one. We can now see that $E_4^3 - E_6^2 = C\Delta$. Now we can write

$$E_4^3(q) = (1 + 240q + O(q^2))^3 = 1 + 720q + O(q^2)$$
$$E_6^2(q) = (1 - 504q + O(q^2))^2 = 1 - 1008q + O(q^2)$$
$$E_4^3 - E_6^2 = 1728q + O(q^2)$$
$$\Delta(q) = q + O(q^2)$$

By comparing the coefficients at q we can deduce that $C = 1728$ proving the formula.

Conclusion

Mathematics is not a spectator sport.

-George Polya.

Exercise 6.1. Proof the following relations:

$$\sigma_7(n) = \sigma_3(n) + \sum_{i=1}^{n-1} \sigma_3(i)\sigma_3(n-i)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{i=1}^{n-i} \sigma_3(i)\sigma_5(n-i)$$

$$\sigma_{13}(n) = 21\sigma_5(n) - 20\sigma_7(n) + 10080 \sum_{i=1}^{n-i} \sigma_5(i)\sigma_7(n-i)$$

$$\tau(n) \equiv \sigma_{11}(n) \quad \mod 691$$

Exercise 6.2. Let $\Delta = \frac{1}{1728}(E_4^3 - E_6^2) = \sum_{n=1}^{\infty} \tau(n)q^n$ and D be the opperator $D = \frac{1}{2\pi i}\frac{d}{d\tau} = q\frac{d}{dq}$

1. Show that the fonction $H = 4E_4 D(E_6) - 6E_6 D(E_4)$ is a modular form of weight 12.

2. Deduce that

$$\tau(n) = \frac{n}{12}(5\sigma_3(n) + 7\sigma_5(n)) + \sum_{1 \le m \le n}(2n - 5m)\sigma_3(m)\sigma_5(n - m)$$

3. Conclude that

$$\tau(n) \equiv n\sigma_5(n) \equiv \sigma_1(n) \bmod 5,$$

$$\tau(n) \equiv n\sigma_3(n) \bmod 7.$$

The reader is encouraged to look through the Bibliography for a more thorough look at the field of modular forms, in particular [5] for as an Introduction, [7] for a elegant concise view of the basics, [1] for more interesting congruences and [6] for various applications of modular forms.

References

[1] G.E. Andrews and B.C. Berndt. *Ramanujan's Lost Notebook: Part III*. ptie. 3. Springer New York, 2012. ISBN: 9781461438106. URL: https://books.google.fr/books?id=YPWrm2VWDYIC.

[2] Pierre Charlois. *Introduction aux formes modulares*. Dec. 2022.

[3] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer New York, 2006. ISBN: 9780387272269. URL: https://books.google.fr/books?id=EXZCAAAAQBAJ.

[4] I. L. W. V. Jensen and J. L. W. V. Jensen. "Forskellige Bidrag til Ligningernes Theori". In: *Nyt tidsskrift for matematik* 26 (1915), pp. 6–13. ISSN: 09093524, 24460753. URL: http://www.jstor.org/stable/24532196 (visited on 01/23/2023).

[5] L.J.P. Kilford. *Modular Forms: A Classical and Computational Introduction*. Imperial College Press, 2008. ISBN: 9781848162136. URL: https://books.google.fr/books?id=yuRpDQAAQBAJ.

[6] K. Ranestad et al. *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*. Universitext. Springer Berlin Heidelberg, 2008. ISBN: 9783540741190. URL: https://books.google.fr/books?id=tsTfnHLmgmQC.

[7] Jean-Pierre Serre. *A course in arithmetic*. Springer, 1993.