Modular forms modulo 2

Paul Dubois

February 15, 2020

Abstract

We are interested in Modular forms modulo 2, and computing thing about it. [temporary abstract]

Key words that should appear: Modular forms; Mod 2; Duality of definitions; Governing fields; Frobenian map?; Exact computations;

Contents

1 Modular forms

1.1 Modular forms of level 1

Let $\mathbb{H}$ denote the *upper-half plane*, that is, $\mathbb{H} = \{z = x + yi \in \mathbb{C} | \; y > 0\}$.

We say that a function $f : \mathbb{H} \to \mathbb{C}$ is *weakly modular* of *weight* $2k$ if f is meromorphic and

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

The group $\mathrm{SL}_2(\mathbb{Z})$ of invertible $(2x2)$ matrices over $\mathbb{Z}$ with is generated by

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

see [Conrad, 2020, p.1-2].

From this property, we can derive an alternative definition of weakly modular functions: f is weakly modular of weight $2k$ if f is meromorphic and

$$f(z+1) = f(z) \quad \text{and} \quad f(-1/z) = z^k f(z)$$

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

Moreover, we define a function $f : \mathbb{H} \to \mathbb{C}$ to be *modular* of weight $2k$ if f is holomorphic and weakly modular. Lastly, we say that a function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form* of weight $2k$ if it modular and holomorphic at ∞, that is, $f(1/z)$ is holomorphic at $z = 0$.

It is straightforward to check, using the above definition, that the set of modular forms of weight $2k$ is closed under addition and multiplication by complex scalars. More precisely:

- If f_1 and f_2 are modular forms of weight $2k$, then $f_1 + f_2 : z \to f_1(z) + f_2(z)$ is modular of weight $2k$ as well.

- Similarly, if $\lambda \in \mathbb{C}$ and f is a modular form of weight $2k$, then so is $\lambda \cdot f : z \to \lambda f(z)$.

Therefore, modular forms of weight $2k$ over $\mathbb{C}$ form a space. We denote it M_k.

It is also possible to multiply modular forms, in which case the weights are additive: If f_1 and f_2 are modular forms of respective weights $2k_1$ and $2k_2$, then $f_1 f_2 : a \to f_1(z) f_2(z)$ is modular of weight $2k_1 + 2k_2$.

We deduce that we can take powers of modular forms, and the weight is then multiplied by the exponent: if $f(z)$ is modular of weight $2k$, then $f^n(z)$ is modular of weight $2k \cdot n$ (with $n \in \mathbb{N}$ [1]).

1.2 Typical Modular Forms

1.2.1 Eisenstein series G_k

The most famous class of modular forms is probably the *Eisenstein series*, usually denoted G_k. We define them as follows [Stein, 2007, Examples of Modular Forms]:

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

for $k \geq 2$.

[1] The set of naturals $\mathbb{N}$ is taken to start from 0 in this paper.

It is easy to check that G_k are modular of weight $2k$ [Stein, 2007, Proposition 2.1], as:

$$G_k(z+1) = G_k(z)$$

(using $(m, n+m) \to (m, n)$, an invertible map)

$$G_k(-1/z) = z^k G_k(z)$$

(using $(m, -n) \to (m, n)$, an invertible map).

It is pleasant to remark that [Stein, 2007, Proposition 2.2]

$$G_k(\infty) = \sum_{n \in \mathbb{Z}^*} \frac{1}{n^{2k}} = 2\zeta(2k)$$

. Where $\zeta(k)$ is Riemann zeta function. The values of this function are well-known on positive even numbers, and we deduce [Lennart Rade, 2013, p.194] that:

$$G_k(\infty) = 2\zeta(2k) = \frac{(2\pi)^{2k}}{(2k)!} B_k$$

where $B_k = (-1)^{k+1} b_{2k}$ and b_k are Bernoulli numbers.

1.2.2 The Modular Discriminant Δ

We will be interested in one main modular form in the rest of this article: the *modular discriminant* Δ. We define Δ in terms of G_k as follows [Serre, 1973, p.84]:

$$\Delta = \left(\frac{1}{(2\pi)^{12}}\right)(g_2^3 - 27g_3^2) \in M_6^0 \qquad \text{with } g_2 = 40G_2 \text{ and } g_3 = 140G_3$$

As g_2^3 is modular of weight $4 \cdot 3 = 12$ and g_3^2 of weight $6 \cdot 2 = 12$, Δ is modular of weight 12. Multiplying by the scalar $({}^1\!/_{(2\pi)^{12}})$ doesn't change the weight of the modular form, and it will we useful later for normalization purposes.

Now, using $G_2(\infty) = 2\zeta(4) = \frac{\pi^4}{45}$ and $G_3(\infty) = 2\zeta(6) = \frac{2\pi^4}{945}$, we get

$$\Delta(\infty) = \left(\frac{1}{(2\pi)^{12}}\right)\left[\left(\frac{4\pi^4}{3}\right)^3 - \left(\frac{8\pi^4}{27}\right)^2\right] = 0$$

so Δ has a zero at infinity.

1.3 Cusp Forms

A function $f : \mathbb{H} \to \mathbb{C}$ that is a modular form may in addition be a *cusp form*, if $f(\infty) = 0$. We will denote the *space of modular cusp forms* of weight $2k$ over $\mathbb{C}$ by M_k^0.

It is useful to note $G_k(\infty) = \sum_{n \in \mathbb{N}^*} \frac{2}{n^{2k}} > 2$ and in particular, $G_k(\infty) \neq 0$, so G_k are *not* cusp forms for any k. As we have shown it before, $\Delta(\infty) = 0$, so Δ is a modular cusp form of weight 12, so $\Delta \in M_6^0$. Using tools from complex analysis, we can prove that Δ has only one zero (at infinity), which has order one [Serre, 1973, p.88].

We have the following relation:

Theorem 1. $M_k \cong M_k^0 \oplus \mathbb{C} \cdot G_k$ *for all* $k \geq 2$ *[Serre, 1973, p.88]*

Proof. We let $\Phi : M_k \to \mathbb{C}$ such that if $f \in M_k$, $\Phi(f) = f(\infty)$.

Now, we have $\mathrm{Ker}(\Phi) = M_k^0$, therefore, by the 1st Isomorphism Theorem, ${M_k}/{M_k^0} \cong \mathrm{Im}(\Phi) \subseteq \mathbb{C}$.

Note that $G_k \in M_k$, and $G_k(\infty) = \sum_{n\in\mathbb{Z}^*} \frac{1}{n^{2k}} \neq 0$, so $G_k \notin M_k^0$. As $G_k \neq 0$, $\dim({M_k}/{M_k^0}) \geq 1$ and $\mathrm{Im}(\Phi) = \mathbb{C}$. Thus, $G_k \in M_k$
M_k^0

Finally, we have $M_k \cong M_k^0 \oplus \mathbb{C}.G_k$ if $k \geq 2$. (The above argument fails for $k < 2$ as G_k is not well defined any more.) $\square$

Therefore, the dimensions of M_k and M_k^0 are closely linked.

1.4 Dimensions of Spaces of Modular Forms

The fact that multiplying two modular forms gives a function that remains modular yields that we may map a set of modular forms to an other.

Theorem 2. $M_{k-6} \cong M_k^0$. *[Serre, 1973, p.88]*

Proof. We let $\Phi : M_{k-6} \to M_k^0$ such that if $f \in M_k$, $\Phi(f)(z) = \Delta(z)f(z)$.

This is well defined as if f has weight $2(k-6)$, $\Delta.f$ has weight $2k$ since Δ has weight 12. As Δ is a cusp from, $\Delta.f$ will also be a cusp form.

From definition, Φ is clearly homomorphic.

Now, if $g \in M_k^0$, we may define $\Psi : M_k^0 \to M_{k-6}$ such that $\Psi(g)(z) = {g(z)}/{\Delta(z)}$

This is well defined as if g has weight $2k$, $\Delta.f$ has weight $2k$ since Δ has weight 12. As Δ is a cusp from, $\Delta.f$ will also be a cusp form.

This is well defined as Δ has only one zero, at infinity, where g also has a zero (as g is a cusp form). The weights agree again as well.

It is then easy to remark that $\Psi = \Phi^{-1}$. So Φ is bijective, and thus isomorphic.

Finally, we have $M_{k-6} \cong M_k^0$. $\square$

This theorem, combined with the previous one is very powerful: it shows that there must be a pattern (of 6) in the sequence of dimensions $\dim(M_k)$ and $\dim(M_k^0)$ for $k \geq 2$. We have $M_k \cong M_k^0 \oplus \mathbb{C}.G_k \cong M_{k-6} \oplus \mathbb{C}.G_k$, so $\dim(M_k) = \dim(M_{k-6}) + 1$ when $k \geq 2$. Thus, if we compute the dimensions of M_0, M_1, M_2, M_3, M_4, M_5, we can extrapolate dimensions of M_k and M_k^0 for all k.

Using complex analysis techniques again, we have:

- $\dim(M_k) = 0 \quad k < 0$
- $\dim(M_1) = 0$
- $\dim(M_0) = \dim(M_2) = \dim(M_3) = \dim(M_4) = \dim(M_5) = 1$

In the case $k = 0$, $\dim(M_0) = 1$. As $f(z) = 1$ is clearly a modular from of weight 0, $\{1\}$ is a basis for M_0. We deduce $\dim(M_k^0) = 0$ as 1 is clearly not a cusp form. In the case $k = 1$, $\dim(M_1) = 0$, which makes $\dim(M_1^0) = 0$ automatically. (Cases $k < 0$ are similar to $k = 1$.)

Other cases may be derived directly from the relations (using induction to get general formulas), and we obtain:

Space	$k < 0$	$k \geq 0,\ k \equiv 1 \bmod 6$	$k \geq 0,\ k \not\equiv 1 \bmod 6$
$\dim(M_k)$	0	$\lfloor {k}/{6} \rfloor$	$\lfloor {k}/{6} \rfloor + 1$
$\dim(M_k^0)$	0	$\max\{0, \lfloor {k}/{6} \rfloor - 1\}$	$\lfloor {k}/{6} \rfloor$

Note that the max is taken only to avoid negative dimensions.

1.5 Fourier Expansion

1.5.1 Definition

To study such function, we use Fourier Expansion. In the case of f being a modular form of weight $2k$, a *Fourier Expansion* is a representation of f as a power series of $e^{2\pi inz}$ i.e.

$$f(z) = \sum_{n\in\mathbb{Z}} a_n(f)e^{2\pi inz}.$$

We usually denote $q = e^{2\pi iz}$ so that $q^n = e^{2\pi inz}$ and the Fourier expansion of f become

$$f(q) = \sum_{n\in\mathbb{Z}} a_n(f)q^n.$$

When in this form, we may as well call it the *q-expansion*.

1.5.2 Typical Modular Forms Fourier Expansion

Fourier Expansions of G_k The modular forms G_k have the following q-expansion [Serre, 1973, p.92]:

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

where σ_d is the generalized divisor function such that:

$$\sigma_d(n) = \sum_{m|n} m^d.$$

Fourier Expansion of Δ We also have [Serre, 1973, p.95]:

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

1.6 A Basis for Modular Forms

The set of modular forms that are weight $2k$ in fact form a vector space (we can add modular forms together, and multiply them with a constant) over the complex numbers. One may ask then a basis for this vector space.

We would like to find a basis for each set M_k. It turns out that the modular forms G_2 and G_3 introduced before in fact generate a basis for all M_k. It is not obvious and may in fact seems wrong at a first stage: G_2 and G_3 are modular forms of weight 4 and 6, whereas M_k in general have modular forms of weight $2k$. However, by taking combinations of G_2 and G_3, we may obtain modular forms of any weight $2k$. It is important to remember that when multiplied, the weight of modular forms add up.

Theorem 3. *The set $S = \{G_2^a G_3^b | a, b \in \mathbb{N}, 2a+3b = k\}$ is a basis for M_k. [Stein, 2007, Theorem 2.17]*

Proof. Of course, the cases when $\dim(M_k) = 0$ (for $k < 0$ and $k = 1$) are trivial, as the basis is empty, and $2a + 3b = k$ has no solution for $a, b \in \mathbb{N}$.

To show S is a basis, we need it to span M_k and to be linearly independent.

We start with spanning, and we proceed by induction on k, with step 6.

As $\dim(M_k) = 1$ for $k = 0, 2, 3, 4, 5, 7$, and the equation $2a + 3b = k$ has exactly one solution for $a, b \in \mathbb{N}$ (namely $(a, b) = (0,0), (1,0), (0,1), (2,0), (1,1), (2,1)$), S has only one element, which must be the basis.

Now, for $k > 7$, take some $a, b \in \mathbb{N}$ such that $2a + 3b = k$. Let $f \in M_k$, and $g = G_2^a G_3^b \in M_k$. $g(\infty) \neq 0$ as none of G_2 or G_3 is a cusp form. So there must be a complex λ such that $f - \lambda g$ is a cusp form. Then $f - \lambda g \in M_k \cong M_{k-6}^0$ and we can find a $h \in M_{k-6}^*$ such that $h.\Delta = f - \lambda g$.

By induction, h must be a polynomial of G_2 and G_3; by definition, Δ is one as well (note that yet, we don't put any restriction on powers of G_2 and G_3, other then being positive integers). Therefore, $f = \Delta.h + \lambda g$ is a polynomial of G_2 and G_3. From the fact that $f \in M_k$ (i.e. f has weight $2k$), terms of f as a polynomial of G_2 and G_3 have the from $G_2^a G_3^b$ with $2a + 3b = k$.

We now want to show linear independence, we proceed by contradiction.

Suppose there is a non-trivial linear relation of terms $G_2^a G_3^b$. We can multiply it by suitable G_2 and G_3 so that all terms have the form $2a+3b = k \equiv 0 \bmod 12$. Then, we can divide all terms by G_3^2, witch gives us that there is a polynomial for which ${G_2^3}/{G_3^2}$ is a root. In particular, this polynomial is constant when ${G_2^3}/{G_3^2}$ is plugged. This contradicts the fact that q-expansion of ${G_2^3}/{G_3^2}$ is not constant. $\square$

This set of makes to be a basis, and one may even find it pleasant: given the two modular forms G_2 and G_3, this set generates all the modular forms of weight $2k$ that we could think of, if we only knew these two modular forms.

1.7 Hecke Operators

We define the *Hecke operators* for a modular form f as follows [Serre, 1973, p.100]:

$$T_n f(z) = n^{2k-1} \sum_{a \geq 1,\, ad=n,\, 0 \leq b < d} d^{-2k} f\left(\frac{az+b}{d}\right)$$

with $n \in \mathbb{N}$.

We can check that $T_n f$ is modular if f is (as the sum of modular forms).

We may as well write $T_n f$ as a Fourier Expansion of $q = e^{2\pi i z}$ as follows [Serre, 1973, p.100]:

$$T_n f(z) = \sum_{m \in \mathbb{Z}} \gamma(m) q^m \quad \text{with} \quad \gamma(z) = \sum_{a|(n,m),\, a \geq 1} a^{2k-1} c\left(\frac{mn}{a^2}\right)$$

$$\text{For modular forms } f \text{ s.t. } f(z) = \sum_{n \in \mathbb{Z}} \alpha(n) q^n$$

2 Modular Forms Modulo Two

2.1 Strategy to Reduce Modulo Two

It is not trivial, at this point, why and how we can reduce modulo 2 modular forms, objects that have coefficients in $\mathbb{C}$. In general, reduction modulo a number is only possible with whole numbers (integers). We would like to reduce modulo 2 coefficients of the Fourier series for modular forms. But at the moment, they lie in $\mathbb{C}$.

In fact, we will introduce a new basis for the modular forms: the so called Miller Basis. The coefficients of all the forms in this basis are integers. It is then possible to consider the space of modular forms over $\mathbb{Z}$ instead of $\mathbb{C}$. Once this is done, we will reduce all the newly integral coefficients modulo 2.

In this section, we will denote all objects reduced modulo 2 with an $\overline{\text{over-line}}$:

- The modular form f once reduced will be denoted $\overline{f}$.
- The coefficients of the q-expansion c will reduce to $\bar{c}$
- The Hecke operators T_n reduced will be denoted $\overline{T_n}$.

2.2 Integral Basis

2.2.1 Normalisation of Typical Modular Forms

Normalisation of Eisenstein series G_k We first recall the formula for q extension of G_k and the one for $\zeta(2k)$:

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

and

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

so overall:

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

We would like to normalize this series, so that the coefficients become integers, so that we can ultimately reduce them modulo 2. Right now, coefficients are rational.

As we want to keep the series modular with same weight, the only tool we have to normalize the series is multiplication by a constant. The normalization is a crucial point: If we multiply by 2 all coefficients of a modular form that already lie in $\mathbb{Z}$, the reduction $\bmod 2$ will always give zero.

First, let's normalize the series to have particular values on some coefficients of interest. There are two justified ways to do so: normalize to have constant coefficient set to one, and to have q coefficient is set to one. We will introduce both: Let E_k be such that:

$$E_k.2\zeta(2k) = G_k$$

so that

$$E_k = 1 + (-1)^k\frac{4k}{B_k}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

E_k then has constant coefficient set to one.

Let F_k be such that:

$$F_k.\left(2\frac{(2\pi i)^{2k}}{(2k-1)!}\right) = G_k$$

so that

$$F_k = (-1)^k\frac{B_k}{4k} + \sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

F_k then has q coefficient set to one (as $\sigma_{2k-1}(1) = 1$).

Clearly, the coefficients of this expansion remain in $\mathbb{Q}$ at least, and we will show that for some specific k, the coefficients lie in fact in $\mathbb{Z}$. Both F_k and E_k are interesting, but for our purpose (reducing modulo 2), we will use E_k. Note that E_k are normalized versions of Eisenstein series G_k, but in literature, both are called Eisenstein series see [Shrivastava, 2017, p.6] for example.

The Modular Discriminant Δ Normalized Again, we recall the formula for q extension of Δ:

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

Clearly, the coefficients in expansion of Δ are integers (which we can reduce modulo 2). This is the reason why we defined Δ with the $\frac{1}{(2\pi)^{12}}$ factor in front.

2.2.2 Miller Basis

Basis with Integral Coefficients (in Fourier Series) Applying normalization $G_k \to E_k$ above for $k = 2, 3$, we get:

$$\begin{aligned} E_2 &= 1 + \frac{8}{B_2}\sum_{n=1}^{\infty}\sigma_3(n)q^n \qquad B_2 = \frac{1}{30} \\ &= 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \end{aligned}$$

and

$$\begin{aligned} E_3 &= 1 - \frac{12}{B_3}\sum_{n=1}^{\infty}\sigma_5(n)q^n \qquad B_3 = \frac{1}{42} \\ &= 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n \end{aligned}$$

Now, we have shown that $\{G_2^aG_3^b | 2a+3b = k\}$ is a basis for modular forms of weight $2k$ over the complex (see 1.6). As $E_2 = \lambda G_2,\ \lambda \in \mathbb{C}$ and $E_3 = \mu G_3,\ \mu \in \mathbb{C}$, we have that $\{E_2^aE_3^b | 2a+3b = k\}$ remains a basis for M_k over $\mathbb{C}$.

It is clear, from the series, that coefficients of the q-expansion of both E_2 and E_3 are all integers. Thus, so are coefficients of combinations of E_2 and E_3. Therefore, we have found a basis for M_k such that all elements in the basis have only integral coefficients in their q-expansion.

Miller Basis for M_k^0 This is a nice result, but we can in fact do better, by forcing the first coefficients to chosen values.

Theorem 4. *For the space of modular cusp forms M_k^0, there exists a basis $\{f_1, \cdots, f_r\}$ such that:*

- $f_i \in Z[q]$

- $a_i^j = \delta_i j = \begin{cases} 1 & \textit{if } i = j \\ 0 & \textit{if } i \neq j \end{cases} \quad \forall 1 \leq i, j \leq r$
  where a_i^j is the coefficient of q^j in expansion of f_i.

This is commonly called the Miller basis for M_k^0, as it was first introduced by Victor Saul Miller Miller [1975].

Proof.
- For $k < 6$, $k = 7$, we have $\dim(M_k^0) = 0$. Thus, $\emptyset$ is a basis which satisfies the Miller basis properties.
- For $k = 6$, we have $\dim(M_k^0) = 1$. Thus, $\{\Delta\}$ is a basis which satisfies the Miller basis properties.
- For $k \geq 7$, we let $r = \dim(M_k^0) \geq 1$. We then consider the set

$$\{g_j | 1 \leq j \leq r\}$$

where

$$g_j = \Delta^j E_3^{2(d-j)+b} E_2^a$$

with

$$2a + 3b \leq 7 \text{ \& } 2a + 3b \cong k \bmod 6$$
$$\text{\& } \; d = \frac{k - (2a + 3b)}{6} \quad \in \mathbb{N} \text{ as } k \geq 7$$

Note that a and b are unique unless $k \cong 0 \bmod 6$. In witch case, we use by convention $a = 0$, $b = 0$.

As all E_2, E_3, and Δ have integral coefficients, g_j will as well.

We then look at the q series:

$$\Delta(q) = q + O(k^2) \implies \Delta^j(q) = q^j + O(k^{j+1})$$

As we normalized so,

$$E_2(q) = 1 + O(q) \implies E_2^\alpha(q) = 1 + O(q)$$
$$E_3(q) = 1 + O(q) \implies E_3^\alpha(q) = 1 + O(q)$$

This gives:

$$g_j(q) = q^j + O(q^{j+1}) \quad \forall 1 \leq j \leq r.$$

Therefore, $\{g_j, | 1 \leq j \leq r\}$ is clearly a linearly independent set. By dimension argument, it also spans M_k^0. Therefore, it forms a basis. Moreover, in this basis: $a_i^j = \delta_{ij} \quad i \leq j$.

Finally, we can use Gaussian elimination on $\{g_j\}$ to obtain a basis $\{f_j | 1 \leq j \leq r\}$ such that: $a_i^j = \delta_{ij} \quad \forall 1 \leq i, j \leq r$. The coefficients will remain in $\mathbb{Z}$ after Gaussian elimination.

□

Extension to all M_k We already have a basis for M_k^0, as $\dim(M_k) = \dim(M_k^0) + 1$ (over $\mathbb{C}$), we just need to adjoint one element of $M_k \setminus M_k^0$ to our basis.

It was shown before that $\{E_2^a E_3^b | 2a + 3b = k\}$ is a basis for M_k with integral coefficients (see 2.2.2) One may see from the q-expansion that $E_2^a E_3^b = 1 + O(q)$ so $E_2^a E_3^b \in M_k \setminus M_k^0$.

Therefore, we can just add one element of $\{E_2^a E_3^b | 2a + 3b = k\}$ to the Miller basis, and use Gaussian elimination again. We get a basis foe M_k of the form $\{f_j | 0 \leq j \leq r\}$ such that in this basis: $a_i^j = \delta_{ij} \quad \forall 0 \leq i, j \leq r$ (with $r = dim(M_k^0)$ i.e. $r + 1 = dim(M_k)$).

Miller Basis Examples

Miller basis for $k = 16$ We can calculate the Miller basis for $k = 16$: $k \cong 4 \bmod 12$ so $a = 2$ and $b = 0$; $d = 2$. We put $g_1 = \Delta^1 E_3^2 E_2^2$, so:

$$\begin{aligned} g_1(q) &= \Delta(q) E_2^2(q) E_3^2(q) \\ &= \left[q - 24q^2 + 252q^3 + O(q^4)\right] \\ &\qquad \cdot \left[1 + 240q + 2160q^2 + 6720q^3 + O(q^4)\right]^2 \\ &\qquad\qquad \cdot \left[1 - 504q - 16632q^2 + 122976q^3 + O(q^4)\right]^2 \\ &= q - 552q^2 - 188244q^3 + O(q^4) \end{aligned}$$

and $g_2 = \Delta^2 E_3^0 E_2^2$, so:

$$\begin{aligned} g_2(q) &= \Delta^2(q) E_2^2(q) \\ &= \left[q - 24q^2 + 252q^3 + O(q^4)\right]^2 \\ &\qquad \cdot \left[1 + 240q + 2160q^2 + 6720q^3 + O(q^4)\right]^2 \\ &= q^2 + 432q^3 + O(q^4) \end{aligned}$$

Then, $f_2 = g_2$ and $f_1 = g_1 + 552 g_2$, so:

$$\begin{aligned} f_1(q) &= q - 552q^2 - 188244q^3 + O(q^4) \;+\; 552 \cdot \left[q^2 + 432q^3 + O(q^4)\right] \\ &= q + 50220q^3 + O(q^4) \\ f_2(q) &= q^2 + 432q^3 + O(q^4) \end{aligned}$$

Therefore, up to $O(q^4)$, $\{f_1, f_2\} = \{q + 50220q^3 + O(q^4), q^2 + 432q^3 + O(q^4)\}$ is a basis for M_{16}^0.

To extend this base to M_k, we adjoint a term of the form $g_0 = E_2^a E_3^b$ where $2a + 3b = 16$. We pick $g_0 = E_2^8$, so:

$$\begin{aligned} g_0(q) &= E_2^8(q) \\ &= \left[1 + 240q + 2160q^2 + 6720q^3 + O(q^4)\right]^8 \\ &= 1 + 1920q + 1630080q^2 + 803228160q^3 + O(q^4) \end{aligned}$$

Then, $f_0 = g_0 - 1920 g_1 - 1630080 g_2$, so:

$$\begin{aligned} f_0(q) &= g_0(q) - 1920 g_1(q) - 1630080 g_2(q) \\ &= \left[1 + 1920q + 1630080q^2 + 803228160q^3 + O(q^4)\right] \\ &\qquad - 1920 \left[q + 50220q^3 + O(q^4)\right] \\ &\qquad\qquad - 1630080 \left[q^2 + 432q^3 + O(q^4)\right] \\ &= 1 + 2611200q^3 + O(q^4) \end{aligned}$$

Therefore, up to $O(q^4)$, $\{f_0, f_1, f_2\} = \{1 + 2611200q^3 + O(q^4), q + 50220q^3 + O(q^4), q^2 + 432q^3 + O(q^4)\}$ is a basis for M_{16}.

Miller basis for $k = 92$ The calculation of this basis may be interesting by hand once; However, it is possible to automate it. The procedure that calculates such coefficients is a standard in SageMath Contributors [2020]. Here is, up to $O(q^{10})$, the Miller basis for M_{92}:

$$\begin{aligned}
f_0 &= 1 + 3034192667130000q^8 + 137290127714549760000q^9 + O(q^{10})\\
f_1 &= q + 91578443563200q^8 + 2651503140376278561q^9 + O(q^{10})\\
f_2 &= q^2 + 2380310529376q^8 + 42238207588515840q^9 + O(q^{10})\\
f_3 &= q^3 + 51682260816q^8 + 530253459731160q^9 + O(q^{10})\\
f_4 &= q^4 + 896013480q^8 + 4882999541760q^9 + O(q^{10})\\
f_5 &= q^5 + 11516000q^8 + 28971735750q^9 + O(q^{10})\\
f_6 &= q^6 + 94680q^8 + 80990208q^9 + O(q^{10})\\
f_7 &= q^7 + 312q^8 - 4860q^9 + O(q^{10})
\end{aligned}$$

2.3 Basis Modulo Two

2.3.1 Reduced Modular Forms

Now that we have a basis with integral coefficients, it makes sense to reduce forms modulo 2. For a modular form f, we denote its reduced modulo 2 from $\overline{f}$. It is defined as follows:

If

$$f(q) = \sum_{n\in\mathbb{N}} c(n)q^n$$

then

$$\overline{f}(q) = \sum_{n\in\mathbb{N}} \overline{c}(n)q^n \qquad \text{with } \ \overline{c}(n) = c(n) \bmod 2.$$

We want to reduce Miller basis modulo 2. The reason is that as we know that some coefficients are ones, the reduction will not be trivial. We will reduce separately E_2, E_3 and Δ (witch together generate the Miller basis).

E_2 reduced We have:

$$E_2(q) = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n)q^n \equiv 1 \bmod 2$$

Therefore, the reduction modulo 2 of E_2 is just 1. We write $\overline{E_2} = 1$, so $\overline{E_2^a} = 1$, for all $a \geq 0$.

E_3 reduced We have:

$$E_3(q) = 1 - 504\sum_{n=1}^{\infty} \sigma_5(n)q^n \equiv 1 \bmod 2$$

Therefore, the reduction modulo 2 of E_3 is 1 as well. We write $\overline{E_3} = 1$, so $\overline{E_3^b} = 1$, for all $b \geq 0$.

Δ reduced We defined before Δ, and we would now like to know its q extension in the standard way. That is, an infinite sum of q^n, instead of an infinite product as we have at the moment.

We define the coefficients $\tau(n)$ to match in the equation:

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

When this holds, τ is called the Ramanujan function.

We would like an explicit formula for $\tau(n)$. More precisely, we are interested in a formula for $\tau(n)$ mod 2.

We will calculate separately the coefficients $\tau(n)$ mod 2 for n even and odd.

Case n odd Remember $\sigma_s(n)$ as the sum of s^{th} powers of (positive) divisors of n. It is known from classical theory [Kolberg, 1962, p.8] that:

$$\tau(8n+l) \equiv a_l \sigma_{11}(8n+l) \pmod{2^{b_l}}$$

where $gcd(l,8)=1$, $a_1=1$, $a_3=1217$, $a_5=1537$, $a_7=705$, $b_1=11$, $b_3=13$, $b_5=12$, $b_7=14$

We are interested in congruence class (mod 2) of the Ramanujan function $\tau(n)$. For n odd, we deduce the following:

$$\tau(n) \equiv \sigma_{11}(n) \equiv \sum_{d|n} d^{11} \equiv \sum_{d|n} 1 \equiv \begin{cases} 1 \bmod 2 & \text{if } n \text{ is a square} \\ 0 \bmod 2 & \text{else} \end{cases}$$

Case n even It is easy to calculate that $\tau(2) = -24 \equiv 0 \bmod 2$.
Using $\tau(p^{n+1}) = \tau(p^n)\tau(p) - p^{11}\tau(p^{n-1}) \quad p \in \mathbb{P}$ [Serre, 1973, p.97] with $p=2$, it follows by induction that $\tau(2^k) \equiv 0 \bmod 2 \quad \forall k \in \mathbb{N}$.
Using $\tau(nm) = \tau(n)\tau(m) \quad$ if $gcd(n,m) = 1$ [Serre, 1973, p.97], it follows that for all n even, $\tau(n) \equiv 0 \bmod 2$.

Explicit series of the discriminant Therefore, the only non-zero coefficients (modulo 2) appears on odd squares, i.e.:

$$\tau(n) \equiv \begin{cases} 1 \bmod 2 & \text{if } n = (2m+1)^2 \quad \text{for } m \in \mathbb{N} \\ 0 \bmod 2 & \text{else} \end{cases}$$

Thus, we can write the power series of Δ as:

$$\Delta(q) \equiv \overline{\Delta}(q) = \sum_{m=0}^{\infty} q^{(2m+1)^2} \bmod 2$$

2.3.2 Reduced Basis

The Miller basis for M_k was obtained via the Gauss elimination of the set $\{\Delta^j E_3^{2(d-j)+b} E_2^a | 1 \leq j \leq \dim(M_k)\}$ (with some conditions on a,b,d).

But $\overline{E_2^a} = \overline{E_2}^a = 1^a = 1 \bmod 2$ and similarly, $\overline{E_3^{2(d-j)+b}} = 1 \bmod 2$. So once the above set is reduced modulo 2, we are left with $\{\overline{\Delta}^j | 1 \leq j \leq \dim(M_k)\}$. So the Miller basis just becomes the Gauss elimination of $\overline{\Delta}$ powers.

This is what motivates the next section.

2.4 Space of Modular Forms Modulo Two

We would like to have a definition for this space in a similar way as M_k was used for modular forms (of weight $2k$) before reduction.

2.4.1 Weights of Modular Forms Modulo Two

We just saw that the Miller basis for $\overline{M_k}$ is (the Gaussian elimination of) $\{\overline{\Delta}^j | 1 \leq j \leq \dim(M_k)\}$.

Now, if we look at this set not reduced modulo 2, we have: $\{\Delta^j | 1 \leq j \leq \dim(M_k)\}$. This is a set of modular forms that have different weights. However, we started with a modular forms in M_k, i.e. all modular forms having weight $2k$.

We understand now that modulo 2, the weight of modular form doesn't make sense any more. This is one of the consequences of reducing modulo 2: we lose some informations about the modular forms, such as the weight.

From this observation, we should study all modular forms together, modulo 2 (instead of separating by weights). This is why the space of modular forms modulo 2 will be denoted $\mathcal{F}$, with mo dependence on k.

2.4.2 Powers of the Modular Discriminant Δ

Set of Powers of the Modular Discriminant Δ As we just saw, the Gaussian elimination of powers $\overline{\Delta}^k$ up to $\dim(\overline{M_k})$ form the Miller basis of $\overline{M_k}$ (modular forms of weight $2k$ reduced modulo 2).

To lighten the notation, we will now write Δ instead of $\overline{\Delta}$, and consider everything modulo 2. For simplicity again, we will just take the powers of Δ to be our basis for modular forms modulo 2 (i.e. drop the Gaussian elimination process).

We define the space $\mathbb{F}_2[\Delta]$ in the usual way:

$$\mathbb{F}_2[\Delta] = \left\{ \sum_{k=1}^{n} a_k \Delta^k | n \in \mathbb{N},\ a_k \in \mathbb{F}_2 \right\}$$

From 2.3.1 we had:

$$\Delta(q) = \sum_{n=0}^{\infty} \tau(n) q^n = \sum_{m=0}^{\infty} q^{(2m+1)^2}$$

Therefore, we define

$$\Delta^k(q) = \sum_{n=0}^{\infty} \tau_k(n) q^n = \left(\sum_{m=0}^{\infty} q^{(2m+1)^2} \right)^k \bmod 2$$

Thus, we have $\tau(n) = \tau_1(n)$.

Proportion of zeros In fact, most of the coefficients $\tau_k(n)$ are 0 modulo 2.

When $k = 1$, there is already few coefficients that are ones: only the odd squares. When raising to the k^{th} power, there are even "less".

Conditions on non-zero coefficients We can find conditions on coefficients that may not be zero.

We observe: We remark that odd squares are all 1 mod 8, and even squares are all 0 mod 8.

$a =$	0	1	2	3	4	5	6	7	mod8
$a^2 =$	0	1	4	1	0	1	4	1	mod8

Table 1: Squares modulo 8

We know from previous calculations that $\Delta(q)$ only has odd powers of q. Thus, raising to the k^{th} power give terms of power n such that:

$$\begin{aligned} n &= m_1^2 + m_2^2 + m_3^2 + \cdots + m_k^2 \\ &\equiv \ 1 \ + \ 1 \ + \ 1 + \cdots + \ 1 \bmod 8 \\ &\equiv k \bmod 8 \end{aligned}$$

Therefore: $\tau_k(n) \equiv 1 \mod 2 \implies n \equiv k \mod 8$
Equivalently: $n \not\equiv k \mod 8 \implies \tau_k(n) \equiv 0 \mod 2$ (by taking the contra-positive)

This means, that Δ^k may only have terms q^n such that $n \equiv k \bmod 8$, i.e. Δ^k may only have terms of power congruent to $k \bmod 8$. When $k = 1$, this is that Δ may only have terms of power $1 \bmod 8$, this matches with table 1: all odd squares are $1 \bmod 8$.

Even powers of Δ We compare $\Delta^{2k}(q)$ and $\Delta^k(q^2)$:

$$\begin{aligned} \Delta^{2k}(q) &= \left(\sum_{m=0}^{\infty} q^{(2m+1)^2}\right)^{2k} \\ &= \sum_{n=0}^{\infty} \#[(2m_1+1)^2 + (2m_2+1)^2 + ... + (2m_{2k}+1)^2 = n \mid m_0, m_1, ..., m_{2k} \in \mathbb{N}] \ q^n \\ &= \sum_{n \ even}^{\infty} \#[(2m_1+1)^2 + (2m_2+1)^2 + ... + (2m_k+1)^2 = n/2 \mid m_0, m_1, ..., m_k \in \mathbb{N}] \ q^n \\ &= \left(\sum_{m=0}^{\infty} q^{((2m+1)^2)\cdot 2}\right)^{k} \\ &= \left(\sum_{m=0}^{\infty} (q^2)^{(2m+1)^2}\right)^{k} = \Delta^k(q^2) \end{aligned}$$

Thus, $\Delta^{2k}(q) = \Delta^k(q^2)$. Therefore, we can write any modular form modulo 2 f as the following:

$$f = \sum_{s \geq 0} f_s^{2^s} \quad \text{with } f_s \text{ having only odd powers of } \Delta$$

[Nicolas and Serre, 2012a, (3)] So it is sufficient to study only the odd powers of Δ.

2.4.3 The Space $\mathcal{F}$

We define the space of modular forms modulo 2 denoted $\mathcal{F}$ to be [Nicolas and Serre, 2012a, 2.1]:

$$\mathcal{F} = \left\langle \Delta^k | k \text{ odd} \right\rangle = \langle \Delta, \Delta^3, \Delta^5, \Delta^7, \dots \rangle$$

That is, all finite polynomials of Δ over $\mathbb{F}_2$, having only odd powers. We remark that the weight of modular forms do not appear, as it was discussed before in 2.4.1. The observations modulo 8 that we have done in 2.4.2 yields that it will be useful to denote:

$$\mathcal{F}_1 = \left\langle \Delta^k \mid k = 1 \bmod 8 \right\rangle = \langle \Delta, \Delta^9, \Delta^{17}, \Delta^{25}, \cdots \rangle$$

$$\mathcal{F}_3 = \left\langle \Delta^k \mid k = 3 \bmod 8 \right\rangle = \langle \Delta^3, \Delta^{11}, \Delta^{19}, \Delta^{27}, \cdots \rangle$$

$$\mathcal{F}_5 = \left\langle \Delta^k \mid k = 5 \bmod 8 \right\rangle = \langle \Delta^5, \Delta^{13}, \Delta^{21}, \Delta^{29}, \cdots \rangle$$

$$\mathcal{F}_7 = \left\langle \Delta^k \mid k = 7 \bmod 8 \right\rangle = \left\langle \Delta^7, \Delta^{15}, \Delta^{23}, \Delta^{31}, \cdots \right\rangle$$

Of course, we have:

$$\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_3 \oplus \mathcal{F}_5 \oplus \mathcal{F}_7$$

We will also introduce (as in [Nicolas and Serre, 2012b, 2.]):

$$\mathcal{F}(n) = \left\langle \Delta^k \mid k \text{ odd and } k \leq 2n-1 \right\rangle = \left\langle \Delta, \Delta^3, \Delta^5, \ldots, \Delta^n \right\rangle$$

This matches specifically $\overline{M_{12\cdot n}} = \mathcal{F}(n)$.

2.4.4 Duality between Δ and q

As we defined $\mathcal{F}$ above, a modular form modulo 2 is an expression of powers Δ^k. But we had from before that $\Delta = \sum_{m=0}^{\infty} q^{(2m+1)^2} \bmod 2$. Therefore, we can translate a modular form given as a finite polynomial of Δ into an infinite polynomial of q. Thus, there are two ways to write a modular form modulo 2.

This duality between the two definitions is what makes the study of modular forms modulo 2 so interesting: we go back and forth between an infinite series and a finite polynomial. One is easy to express, the other easy to compute. This will lead to new reasoning. In particular, there is a new technique of computation ("exact computations") that uses equivalence between the two ways of writing a modular form.

2.5 Hecke Operators Modulo Two

2.5.1 Reduction Modulo Two

Definition Now that we have reduced modular forms modulo 2, we would like to study the Hecke operators on these reduced modular forms. We define Hecke operators modulo 2 as follows:

With f a modular form modulo 2 with q definition

$$f(q) = \sum_{n \in \mathbb{N}} c(n) q^n$$

we define

$$\overline{T_p}|f(q) = \sum_{n \in \mathbb{N}} \gamma(n) q^n$$

where

$$\gamma(n) = \begin{cases} c(np) & \text{if } p \nmid n \\ c(np) + c(n/p) & \text{if } p \mid n \end{cases} \qquad \& \ p \text{ an odd prime}$$

Well-definiteness We want to check that all the definitions make sense. When we look at $T_p|f$, there is a number of ways to to reduce it modulo 2: $\overline{T_p|f}$, $\overline{T_p|\overline{f}}$, $\overline{\overline{T_p}|f}$, $\overline{T_p}|\overline{f}$.

Let's compare coefficients:

$\overline{T_p|f}$:

$$\gamma(n) = \sum_{a|(n,p),\, a \geq 1} a^{2k-1} c\left(\frac{np}{a^2}\right) = \begin{cases} \bar{c}(np) & \text{if } p \nmid n \\ \bar{c}(np) + \bar{c}(n/p) & \text{if } p \mid n \end{cases}$$

Divisors of (n, p) are $\{1\}$ or $\{1, p\}$ since p is prime, so the sum split in two cases, with one or two terms. We see now that looking at Hecke operators modulo 2 only for primes simplifies the sum to a computable formula.

As both 1 and p are odd, the term a^{2k-1} reduces to 1 modulo 2. We understand why Hecke operators modulo 2 isn't defined for even numbers: many terms in the summation would become zero. It would not make sense to call it a Hecke operator any more.

It also makes sense why we look at modular forms modulo 2 and not say three or five: the coefficient a^{2k-1} collapse nicely modulo 2, which won't be the case modulo an other number then 2.

$\overline{T_p|\overline{f}}$: This is (very) similar to the case before.

$\overline{T_p}|\overline{f}$:

$$\gamma(n) = \begin{cases} \overline{c}(np) & \text{if } p \nmid n \\ \overline{c}(np) + \overline{c}(n/p) & \text{if } p \mid n \end{cases}$$

$\overline{\overline{T_n}|f}$: Again, this is (very) similar to the case before.

All reductions give in fact the same result, so it makes sense to reduce modular forms modulo 2, and still study the Hecke operators (but now only for odd primes). As this all makes sense, we will now write only consider modular forms modulo 2, and we will drop the over lines for simplicity.

2.5.2 Basic Properties

When reduced modulo 2, Hecke operators $\overline{T_p}$ for primes p have more properties then the general T_p. The extra properties make the study modulo two interesting.

Inherited properties From the fact that $\overline{T_p}|f(q) = \overline{T_p|f(q)}$, we get that the Hecke operators modulo 2 keep the properties they had before being reduced.

Modularity Remains From definition 1.7, a Hecke operators transform a modular form to an other. This is because from definition, $T_n f$ is a sum of modular forms (which remain modular). Therefore, Hecke operators modulo 2 will as well transform a modular form to an other. This was not clear from the definition modulo 2 that we had (which was in terms of q series).

Commutativity As in general [Serre, 1973, p.101]:

$$T_n T_m = T_{mn} \quad \text{if } \gcd(m, n) = 1$$

We get that:

$$T_p T_q = T_q T_p \quad \forall p, q \in \mathbb{P}$$

Therefore, the Hecke operators modulo 2 commute. This, as well, was not clear form definition. It will be very convenient for future calculations.

Linearity From definition 1.7, we have that the Hecke operators are immediately linear. That is:

$$T_p|(f+g) = T_p|f + T_p|g$$

(this follows directly from definition).

This property will also remain modulo 2.

Behaviour of $\mathcal{F}_i$ Suppose $f \in \mathcal{F}_i$, using 2.4.2, we have:

$$f = \sum_{m \equiv i \bmod 8} \mu_m \Delta^m = \sum_{n \equiv i \bmod 8} c(n) q^n$$

From the definition of Hecke operator modulo 2 (2.5.1), we have:

$$T_p|f = \sum_{n\in\mathbb{N}} \gamma(n)q^n \quad \text{with } \gamma(n) = \begin{cases} c(np) & \text{if } p \nmid n \\ c(np) + c(n/p) & \text{if } p \mid n \end{cases}$$

$c(np)$: We have $np \not\equiv i \bmod 8 \implies c(np) = 0$.

$c(n/p)$: As p is an odd prime, it is an odd number, so from 2.4.2, $p^2 \equiv 1 \bmod 8$, so $p^{-2} \equiv 1 \bmod 8$ as well (with p^{-2} seen mod8).

Therefore, $np \not\equiv i \bmod 8 \implies n/p \equiv {}^{np}/_{p^2} \equiv np \not\equiv i \bmod 8$.

$\gamma(n)$: We conclude that $n \equiv np^2 \not\equiv pi \bmod 8 \implies \gamma(n) = 0$

Using 2.4.2 again, we deduce that $T_p|f \in \mathcal{F}_j$ with $j \equiv pi \bmod 8$.

Overall, we have the following:

$$f \in \mathcal{F}_i \implies T_p|f \in \mathcal{F}_j \text{ with } j \equiv pj \bmod 8$$

Non-Nullity of Hecke Opereator We will prove a property that directly implies the non nullity of Hecke Operators.

Property 2.1. *If $f \in \mathcal{F}$, and $T_p|f = 0$ for all odd primes p, then either $f = 0$ or $f = \Delta$. That is, only Δ and 0 give zero after applying any Hecke operator.*

Proof. Let's denote by $a(n)$ the coefficients of the q-expansion of f in the usual way ($f(z) = \sum_{n=0}^{\infty} a(n)q^n$, with $q = e^{2\pi iz}$). With p an odd prime, we similarly define $T_p|f(z) = \sum_{n=0}^{\infty} \gamma(n)q^n$ with $\gamma(n) = c(np) + c(n/p)$.

1. if r simple odd:
   $p \nmid n$ gives $0 = \gamma(n) = a(np)$, so $a(r) = 0$

2. If r odd of power 3 or more:
   Putting $n = mp^2$, we get: $0 = \gamma(mp^2) = a(mp^3) + a(mp) = a(mp^3)$.
   Thus, $a(r) = 0$

Thus, $a(r) \neq 0$ implies r is an odd square. Note that $0 = \gamma(np) = a(np^2) + a(n)$, so $a(1) = 1$ will implies $a(r) = 1$ for all odd squares r. In this case, $f = \Delta$.

Similarly, $a(1) = 0$ makes $a(n) = 0$ for all n. Therefore, f may only be Δ or 0. □

An immediate consequence (by taking the contra-positive) of this property is that if $f \neq 0, \Delta$, then there exists a p such that $T_p|f \neq 0$. Thus, for any $k > 1$, we get that there is a prime p such that $T_p|\Delta^k \neq 0$. This means that T_p is never the null operator.

2.5.3 Nil-potency

The properties of Hecke operators is that, given a modular form f, if we apply a Hecke operators enough times, the form will become zero (i.e. they are nilpotent). The strategy to show this is to prove that for any k (odd), and any prime p, we have:

$$\overline{T_p}|\Delta^k = \sum_{j<k} \mu_j \Delta^j$$

The proof of this property will be divided in two main steps:

Order of Δ doesn't increase We first want to show that:

$$\overline{T_p}|\Delta^k = \sum_{j\leq k} \mu_j \Delta^j$$

From definition 1.7, a Hecke operators takes a modular form of weight $2k$ to an other modular form of weight $2k$. Take a modular form modulo 2 $\overline{f}$ with degree k (in terms of Δ). Now we want to know the maximum degree (again in terms of Δ) of $T_p|\overline{f}$. Let n be the smallest integer such that $\overline{f} \in \overline{M_{12(2n-1)}}$.

We know $T_p|\overline{f} = \overline{T(p)f}$ and $\overline{f} \in \mathcal{F}(n) = \overline{M_{12(2n-1)}}$ so $f \in M_{12(2n-1)}$. This implies that $T(p)f \in M_{12(2n-1)}$ so $T_p|\overline{f} = \overline{T(p)f} \in \overline{M_{12(2n-1)}} = \mathcal{F}(n)$.

Therefore, the maximum degree (in terms of Δ) of $T_p|\overline{f}$ is k as well. Thus, the degree of $\overline{f}$ doesn't increase after applying a Hecke operator.

Order of Δ decrease Now that we have proved that

$$\overline{T_p}|\Delta^k = \sum_{j\leq k} \mu_j \Delta^j$$

we need to show that $\mu_k = 0$, so that the maximum order of Δ in fact effectively decrease.

Let's look at $\mathcal{F}(k)$ as a vector space over $\mathbb{F}_2$ with basis $\{\Delta, \Delta^3, \ddots, \Delta^k\}$. We may the represent a modular form modulo 2 by a k-vector over $\mathbb{F}_2$ (note that even powers of Δ will always be zero, but we keep track of them to lighten notation). Then, as T_p are linear (see 2.5.2), we can represent each operator T_p with a matrix. Let A_p be the $(k \times k)$-matrix (over $\mathbb{F}_2$) representing the action of T_p on $\mathcal{F}(k)$. Since the order of Δ doesn't increase when applying a Hecke operator, the matrix A_p should be upper-triangular, i.e.:

$$A_p = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,k} \\ 0 & a_{2,2} & a_{2,3} & \cdots & a_{2,k} \\ 0 & 0 & a_{3,3} & \cdots & a_{3,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{k,k} \end{pmatrix}$$

We need to show that the coefficients $a_{i,i}$ are zero.

We will do this by induction. Suppose we know T_p decrease the degree of Δ^j for all $j \leq k-1$. Translating this information to the matrix, it means that $a_{j,j} = 0$ for all $j \leq k-1$. Then, we only need to show that $a_{k,k} = 0$.

Now that we have all this information on the diagonal, it makes sense to study the trace: $\mathrm{Tr}(A_p) = a_{k,k}$. A nice interpretation of the Trace should give us an equation for $a_{k,k}$.

We can interpret the trace as the sum of eigenvaues of the matrix A_p, i.e. eigenvalues of the Hecke oprator T_p. Some knoledge about eigenvalues of Hecke operators has been proved already (by Hatada, see Hatada), we have: For p an odd prime, if λ_p is an eigenvalue of T_p, we have the congruence: $\lambda_p \equiv 1 + p \bmod 8$ Since p is an odd (prime) number, we get: $\lambda_p \equiv 0 \bmod 2$. As this is true for all eigenvalues of T_p, we have that the sum of eigenvalues (which corresponds to the trace of the matrix) is zero over $\mathbb{F}_2$. Thus: $a_{k,k} = \mathrm{Tr}(A_p) \equiv 0 \bmod 2$

Now, this is a proof by induction, but the first case really is $k = 0$, in which case, all modular forms are just 0, so all Hecke operators are obviously zero so nilpotent in this case.

Therefore, we proved the nilpotence modulo 2 of Hecke operators T_p for all p odd primes.

2.5.4 Expression as a Sum of Powers of Δ

As the degree of a modular form doesn't increase after applying a Hecke operator, we can apply this the modular form Δ^k to get:

$$T_p|\Delta^k = \sum_{\substack{j\leq k \\ j \text{ odd}}} \mu_j \Delta^j$$

As we know, moreover, that the degree of a modular form will in fact decrease, we deduce that in fact:

$$T_p|\Delta^k = \sum_{\substack{j\leq k-2 \\ j \text{ odd}}} \mu_j \Delta^j \tag{*}$$

The observation on $\mathcal{F}_i$ (in 2.5.2) leads us to the formula:

$$T_p|\Delta^k = \sum_{\substack{j\leq k-2 \\ j\equiv pk \bmod 8}} \mu_j \Delta^j \tag{**}$$

(since $\Delta^k \in \mathcal{F}_i$ with $k \equiv i \bmod 8$)

2.5.5 Examples (for Small Powers of Δ)

We will describe the behaviour of Hecke operators when applied to Δ^k with k odd, $k \leq 7$.

Δ Clearly, from (*), we have $T_p|\Delta = 0$, since the sum is empty (for any p odd prime).

Δ^3 From (*), we have $T_p|\Delta^3 = \Delta$ or 0.
Moreover, (**) gives $T_p|\Delta^3 = 0$ if $1 \not\equiv 3p \bmod 8$ i.e. if $p \not\equiv 3 \bmod 8$.

Now, if $p \equiv 3 \bmod 8$, we may only look at the coefficient q^1 of $T_p|\Delta^3$ (if it is 1, $T_p|\Delta^3 = \Delta$ and if it is 0, $T_p|\Delta^3 = 0$, as there is no other possibilities).

From definition (in 2.5.1), we have that the coefficient of q^1 is $\gamma(1) = c(p)$ (since $p \nmid 1$) with c the q coefficients of Δ^3.

From (2.3.1), the none zero coefficients of Δ are odd squares.

Now, $c(p)$ is th p^{th} coefficient of Δ^3. We have:

$$(\Delta(q))^3 = \left(\sum_{m=0}^{\infty} q^{(2m+1)^2}\right)^3 = \sum_{n=0}^{\infty} \#\{m_1, m_2, m_3 \text{ odds } | m_1^2 + m_2^2 + m_3^2 = n\} q^n$$

So $c(p) = \#\{m_1, m_2, m_3 \text{ odds } | m_1^2 + m_2^2 + m_3^2 = p\} \bmod 2$ corresponds $(\bmod 2)$ to the number of ways to write p as sum of three odd squares.

Need in fact $m_1 = m_2 \neq m_3$, but then?? [I am stuck]

Δ^5 From (*), we have $T_p|\Delta^5 = \Delta^3$ or Δ or 0.
Moreover, (**) gives:

$p \equiv 7 \bmod 8:$	$T_p\|\Delta^5 = \Delta^3$ or 0	if $3 \equiv 5p \bmod 8$	i.e. $p \equiv 7 \bmod 8$
$p \equiv 5 \bmod 8:$	$T_p\|\Delta^5 = \Delta$ or 0	if $1 \equiv 5p \bmod 8$	i.e. $p \equiv 5 \bmod 8$
$p \equiv 1$ or $3 \bmod 8:$	$T_p\|\Delta^5 = 0$	else	

Now, if $p \equiv 7 \bmod 8$, we may only look at the coefficient q^3 of $T_p|\Delta^5$ (if it is 1, $T_p|\Delta^5 = \Delta^3$ and if it is 0, $T_p|\Delta^3 = 0$, as there is no other possibilities).

From definition (in 2.5.1), we have that the coefficient of q^3 is $\gamma(3) = c(3p)$ (since $p \nmid 3$) with c the q coefficients of Δ^5.

From (2.3.1), the none zero coefficients of Δ are odd squares. Now, $c(3p)$ is th p^{th} coefficient of Δ^5. We have:

$$(\Delta(q))^5 = \left(\sum_{m=0}^{\infty} q^{(2m+1)^2}\right)^5 = \sum_{n=0}^{\infty} \#\{m_1, m_2, m_3, m_4, m_5 \text{ odds } | m_1^2 + m_2^2 + m_3^2 + m_4^2 + m_5^2 = n\} q^n$$

So $c(3p) = \#\{m_1, m_2, m_3, m_4, m_5 \text{ odds } | m_1^2 + m_2^2 + m_3^2 + m_4^2 + m_5^2 = 3p\} \bmod 2$ corresponds (mod2) to the number of ways to write $3p$ as sum of five odd squares.

When looked mod8, $m_1^2 + m_2^2 + m_3^2 + m_4^2 + m_5^2 \equiv 5 \bmod 8$. We can check, $p \equiv 7 \bmod 8$ so $3p \equiv 5 \bmod 8$.

Need in fact $m_1 = m_2 \neq m_3$, but then?? [I am stuck]

Δ^7

2.5.6 Table of Hecke Operators

Here is a table of Hecke operators that was computed with a computer:

	T_3	T_5	T_7	T_{11}	T_{13}	T_{17}	T_{19}	T_{23}	T_{29}	T_{31}	T_{37}	T_{41}	T_{43}	T_{47}
Δ	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Δ^3	Δ	0	0	Δ	0	0	Δ	0	0	0	0	0	Δ	0
Δ^5	0	Δ	0	0	Δ	0	0	0	Δ	0	Δ	0	0	0
Δ^7														
Δ^9														
Δ^{11}														
Δ^{13}														
Δ^{15}														
Δ^{17}														
Δ^{19}														

It seems quite random, which makes sense since the Hecke operators depend on prime, and primes appear at random. In line one (Δ^3), we get $1/4^{\text{th}}$ of the primes giving Δ, this is a consequence of Dirichlet Density Theorem, that will be discussed later in this paper. [Is this remark pertinent?]

2.5.7 Nilpotent Order

As we know that the Hecke operators are nilpotent, we may want to study the order of nil potentness.

Definition For a modular from modulo 2 $f \in \mathcal{F}$, we define the *nil potentness order* to be the smallest integer $g(f)$ such that we have

$$T_{p_1} T_{p_2} \cdots T_{p_{g(f)}} | f = 0$$

for any set of primes numbers $p_1, p_2, \ldots, p_{g(f)} \in \mathbb{P}$. The primes p_i involved do not need to be distinct. Note as well that from commutativity of the Hecke operators, the order of the primes p_i doesn't matter.

By convention, we write $g(0) = -\infty$. With a slight abuse of notation, we will write $g(k)$ for $g(\Delta^k)$.

Properties

Well-definiteness All Hecke operators lower by at least two the maximum degree of Δ in the Δ-expansion of a modular form modulo 2 2.5.3. We deduce that $g(f) \leq g(T_p|f) + 1$. Applied to $Delta^k$, we get: $g(k) \leq g(k-2) + 1$. Therefore, by induction, we have $g(k) \leq \lfloor \frac{k+1}{2} \rfloor$. This implies by the same occasion, the well definiteness of the order of nil potentness for all modular form modulo two.

conjecture Let $f_1, f_2 \in \mathcal{F}$ be modular form modulo 2, such that $f_1 = \Delta^k + \sum_{j<k} \mu_j \Delta^k$ and $f_2 = \Delta^k + \sum_{j<k} \nu_j \Delta^k$ (i.e. both having maximum power Δ^k).

Then $g(f_1) = g(f_2)$.

proof attempt By induction?

Case $k = 1$: This is trivial.

Case $k = 3$: This is rather straightforward as well: $g(\Delta^3) = 1$ and $g(\Delta^3 + \Delta) = 1$.

Now, suppose this is true for all $k^* < k$. Want to show it is true for k.

Need

$$T_p|\Delta^k = \Delta^l + O(\Delta^{l-2}) \implies \exists q \in \mathbb{P} \text{ such that } T_q|\Delta^{k+2} = \Delta^m + O(\Delta^{l-2}) \text{ with } m \geq l$$

—— or ——

$$MaxOrder(T_p|\Delta^k) \geq MaxOrder(T_p|\Delta^k + \Delta^l) \quad \forall l < k$$

Is any of the two reasonable to prove?

Note that if it is not provable, I should do a numerical analysis, and mension it as a [rather strong, depending on the analysis] conjecture. Note that it might be wrong, and maybe that numerical analysis will find it out. In such a case, it is nice to mention.

Examples

By hand We can compute a few nil potentness by hand:

- $g(0) = -\infty$
- $g(\Delta) = 1$:
  $T_p(\Delta) = 0$ as order of Δ decrease, see 2.5.3
- $g(\Delta^3) = 2$:
  $T_p|\Delta^3 = \Delta$ or 0
  thus: $g(\Delta^3) = 1 + \max(g(\Delta), g(0)) = 2$
- $g(\Delta^3 + \Delta) = 2$
  similarly
- $g(\Delta^5) = 2$:
  $T_p|\Delta^5 = \Delta$ or 0
  thus: $g(\Delta^5) = 1 + \max(g(\Delta), g(0)) = 2$
- $g(\Delta^5 + \Delta^3 + \Delta) = g(\Delta^5 + \Delta^3) = g(\Delta^5 + \Delta) = 2$
  similarly
- $g(\Delta^7) = 3$:
  $T_p(\Delta^7) = \Delta^5$ or Δ^3 or Δ or 0
  thus: $g(\Delta^7) = 1 + \max(g(\Delta^5), g(\Delta^3), g(\Delta), g(0)) = 3$

Computer calculated We will look at Δ^{95}...

References

Keith Conrad. $\mathrm{SL}_2(\mathbb{Z})$. [Online], 2020. URL `https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf`. Available from `https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf`.

William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. ISBN 978-0-8218-3960-7; 0-8218-3960-8. doi: 10.1090/gsm/079. URL `https://doi.org/10.1090/gsm/079`. With an appendix by Paul E. Gunnells.

Bertil Westergren Lennart Rade. *Mathematics Handbook for Science and Engineering*. Springer Science and Business Media, 2013, 2013. 5th edition, illustrated.

J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

Sagar Shrivastava. Introduction to modular forms, 2017.

Victor Saul Miller. DIOPHANTINE AND P-ADIC ANALYSIS OF ELLIPTIC CURVES AND MODULAR FORMS, 1975. URL `http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:0295447`. Thesis (Ph.D.)–Harvard University.

SageMath Contributors. Sagemath. Software tool, 2020. URL `https://www.sagemath.org/`.

O. Kolberg. Congruences for Ramanujan's function $\tau(n)$. *Arbok Univ. Bergen Mat.-Natur. Ser.*, 1962 (11), 1962. ISSN 0522-9189.

Jean-Louis Nicolas and Jean-Pierre Serre. Formes modulaires modulo 2: l'ordre de nilpotence des opérateurs de Hecke. *C. R. Math. Acad. Sci. Paris*, 350(7-8):343–348, 2012a. ISSN 1631-073X. doi: 10.1016/j.crma.2012.03.013. URL `https://doi.org/10.1016/j.crma.2012.03.013`.

Jean-Louis Nicolas and Jean-Pierre Serre. Formes modulaires modulo 2: structure de l'algèbre de Hecke. *C. R. Math. Acad. Sci. Paris*, 350(9-10):449–454, 2012b. ISSN 1631-073X. doi: 10.1016/j.crma.2012.03.019. URL `https://doi.org/10.1016/j.crma.2012.03.019`.

Hatada. Eigenvaluesofheckeoperatorsons.