Modular forms modulo 2

Paul Dubois

February 21, 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 Modulo Two

1.1 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 $\overline{T_n}$.

1.2 Integral Basis

1.2.1 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 mod2 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.

1.2.2 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 $\{G_2^a G_3^b | 2a + 3b = k\}$ is a basis for modular forms of weight $2k$ over the complex (see **??**). As $E_2 = \lambda G_2$, $\lambda \in \mathbb{C}$ and $E_3 = \mu G_3$, $\mu \in \mathbb{C}$, we have that $\{E_2^a E_3^b | 2a + 3b = k\}$ 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 1. *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

$$2a + 3b \leq 7 \ \& \ 2a + 3b \cong k \bmod 6$$

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

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 1.2.2) 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 $f_1 = g_1 + 552g_2$, 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, $f_0 = g_0 - 1920g_1 - 1630080g_2$, so:

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

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}:

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

1.3 Basis Modulo Two

1.3.1 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:

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

1.3.2 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.

1.4 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.

By abuse of notation, we denote the reduction of Δ modulo 2 (written $\overline{\Delta}$ until here) also by Δ, that is,

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

1.4.1 Weights of Modular Forms Modulo Two

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

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 no dependence on k.

1.4.2 Powers of the Modular Discriminant Δ

Set of Powers of the Modular Discriminant Δ As we just saw, the Gaussian elimination of powers Δ^k up to $\dim(\overline{M_k})$ form the Miller basis of $\overline{M_k}$ (modular forms of weight $2k$ reduced 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 1.3.1 we had:

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

Therefore, we define

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

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.

1.4.3 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 1.4.1. The observations modulo 8 that we have done in 1.4.2 yields that it will be useful to denote:

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

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

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

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

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.]):

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

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

1.4.4 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.

1.5 Hecke Operators Modulo Two

1.5.1 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. The fact that T_p and $\overline{T_p}$ have exactly the same action on the q-expansions of modular forms is only true when p is an odd prime. This is why we will concentrate on this case.

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

Modularity Remains From definition **??**, 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:

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

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 **??**, 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 $f \in \mathcal{F}_i$ [1], using 1.4.2, 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 (1.5.1), we have:

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

$c(np)$: 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 1.4.2, $p^2 \equiv 1 \bmod 8$, 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 1.4.2 again, we deduce that $\overline{T_p}|f \in \mathcal{F}_j$ with $j \equiv pi \bmod 8$.

Overall, we have the following:

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

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

This property follows the idea developed in [Ono, 2004, p.33].

Property 1.1. *If $f \in \mathcal{F}$, and $\overline{T_p}|f = 0$ 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 $q = e^{2\pi i z}$). With p an odd prime, we similarly define $\overline{T_p}|f(z) = \sum_{n=0}^{\infty} \gamma(n) q^n$ 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 $\overline{T_p}|f \neq 0$. Thus, for any $k > 1$, we get that there is a prime p such that $\overline{T_p}|\Delta^k \neq 0$. This means that $\overline{T_p}$ is never the null operator (so reduction modulo two doesn't become trivial).

[1] By abuse of notation, denote by f a modular forms modulo (instead of $\overline{f}$).

1.5.3 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 **??**, 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). Note that there is a modular form f that corresponds to $\overline{f}$ when reduced modulo two. Now we want to know the maximum degree (again in terms of Δ) of $\overline{T_p}|\overline{f}$. Let n be the smallest integer such that $\overline{f} \in \overline{M_{12n}}$.

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

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

Order of Δ decrease Since T_p and $\overline{T_p}$ have exactly the same action on q-expansions of modular forms, we can interchange them as we want. By abuse of notation (again), we denote the reduction of T_p modulo 2 (usually denoted $\overline{T_p}$) by T_p as well.

Now that we have proved that

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

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 $\{\Delta, \Delta^3, \cdots, \Delta^k\}$. We may 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 1.5.2), 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 eigenvalues of the matrix A_p, i.e. eigenvalues of the Hecke operator T_p. Some knowledge about eigenvalues of Hecke operators has been proved already (see Hatada [1979]), 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.

1.5.4 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 1.5.2) 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 $k \equiv i \bmod 8$)

1.5.5 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 1.5.1), 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 (1.3.1), 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:

$$\begin{array}{rlll} p \equiv 7 \bmod 8: & T_p|\Delta^5 = \Delta^3 \text{ or } 0 & \text{if } 3 \equiv 5p \bmod 8 & \text{i.e. } p \equiv 7 \bmod 8 \\ p \equiv 5 \bmod 8: & T_p|\Delta^5 = \Delta \text{ or } 0 & \text{if } 1 \equiv 5p \bmod 8 & \text{i.e. } p \equiv 5 \bmod 8 \\ p \equiv 1 \text{ or } 3 \bmod 8: & T_p|\Delta^5 = 0 & \text{else} & \end{array}$$

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 1.5.1), 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 (1.3.1), 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

1.5.6 Table of Hecke Operators

Here is a table of Hecke operators for primes up to 50, and powers of Δ up to 20:

	Δ^1	Δ^3	Δ^5	Δ^7	Δ^9	Δ^{11}	Δ^{13}	Δ^{15}	Δ^{17}	Δ^{19}
T_3	0	Δ	0	Δ^5	Δ^3	Δ^9	Δ^7	$\Delta^5+\Delta^{13}$	0	$\Delta^9+\Delta^{17}$
T_5	0	0	Δ	Δ^3	0	0	Δ^9	$\Delta^3+\Delta^{11}$	Δ^5	Δ^7
T_7	0	0	0	Δ	0	0	Δ^3	Δ^9	0	Δ^5
T_{11}	0	Δ	0	Δ^5	Δ^3	$\Delta+\Delta^9$	Δ^7	Δ^{13}	0	$\Delta^9+\Delta^{17}$
T_{13}	0	0	Δ	Δ^3	0	0	$\Delta+\Delta^9$	Δ^{11}	Δ^5	Δ^7
T_{17}	0	0	0	0	Δ	Δ^3	Δ^5	Δ^7	Δ	0
T_{19}	0	Δ	0	Δ^5	Δ^3	$\Delta+\Delta^9$	Δ^7	Δ^{13}	0	$\Delta+\Delta^9+\Delta^{17}$
T_{23}	0	0	0	Δ	0	0	Δ^3	$\Delta+\Delta^9$	0	Δ^5
T_{29}	0	0	Δ	Δ^3	0	0	Δ^9	$\Delta^3+\Delta^{11}$	Δ^5	Δ^7
T_{31}	0	0	0	0	0	0	0	Δ	0	0
T_{37}	0	0	Δ	Δ^3	0	0	$\Delta+\Delta^9$	Δ^{11}	Δ^5	Δ^7
T_{41}	0	0	0	0	0	0	0	0	Δ	Δ^3
T_{43}	0	Δ	0	Δ^5	Δ^3	Δ^9	Δ^7	$\Delta^5+\Delta^{13}$	0	$\Delta^9+\Delta^{17}$
T_{47}	0	0	0	0	0	0	0	Δ	0	0

It seems quite random, which makes sense since the Hecke operators depend on prime, and primes appear at random. However, it is interesting to try to find patterns and rules for this table.

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?]

1.5.7 Nil-potency 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

Maximum Order All Hecke operators lower by at least two the maximum degree of Δ in the Δ-expansion of a modular form modulo 2 1.5.3. We deduce that $g(f) \leq g(T_p|f) + 1$. Applied to Δ^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.

Minimum Order If the degree of f is strictly greater than 1 (i.e. $f \neq 0, \Delta$), then $g(f) \geq 2$.

We deduce this from the fact that Hecke operators are not null operators in general (1.5.2): Remember that one consequence of non nullity is that if $f \neq 0, \Delta$, then there exists an odd prime p such that $T_p|f \neq 0$. This directly implies that $g(f) > 1$.

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 1.5.3
- $g(\Delta^3) = 2$:
  $T_p|\Delta^3 = \Delta$ 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}... [To do]

2 Hecke Algebra

This section follows from Nicolas and Serre [2012b].

We recall $\mathcal{F} = \big\langle \Delta^k \mid k \text{ odd} \big\rangle$, i.e. $\mathcal{F} = \big\langle \Delta, \Delta^3, \Delta^5, \Delta^7, \Delta^9, \dots \big\rangle$

2.1 Definition

We redefine $\mathcal{F}(n) = \big\langle \Delta, \Delta^3, \Delta^5, \dots, \Delta^{2n-1} \big\rangle$ so that $\dim(\mathcal{F}(n)) = n$

We define $A(n)$ as the $\mathbb{F}_2$-subalgebra of $\mathrm{End}(\mathcal{F}(n))$ given by $\mathbb{F}_2$ and T_p. That is, if $\mathfrak{m}(n) = \{T_{p_1} \cdot T_{p_2} \cdots T_{p_k} | p_1, p_2, \dots, p_k \in \mathbb{P}, k \geq 1\}$ is a sub-vector-space of $\mathcal{F}$, we get $A(n) = \mathbb{F}_2 \oplus \mathfrak{m}(n)$.

Property 2.1. *$\mathfrak{m}(n)$ is the only maximum ideal of $A(n)$.*

Proof. Firstly, we note that ${}^{A(n)}/_{\mathfrak{m}} \cong \mathbb{F}_2$. Since $\mathbb{F}_2$ is a field, $\mathfrak{m}$ must be a maximum ideal.

Now, suppose I is an other (i.e. $I \neq \mathfrak{m}$) maximum ideal of $A(n)$. Then there is an operator $u \in \mathfrak{m}$ such that $(1 + u) \in I$. Since Hecke operators are nilpotent 1.5.3, there exists $n \in \mathbb{N}$ such that $u^n = 0$. By induction, $(1 + u^n) \in I$ for all $n \geq 1$. □

Note that as Hecke operators are all nilpotent 1.5.3, the ideal $\mathfrak{m}(n)$ is itself nilpotent. In fact, from the minimum 1.5.7 and maximum 1.5.7 nil-potency order property extend to the ideal $\mathfrak{m}$.

Let the dual of $\mathbb{F}(n)$ be $\mathcal{F}(n)^* = \{F : \mathcal{F} \to \mathbb{F}_2\}$. Then $\mathbb{F}(n)^*$ is an $A(n)$-module with operation $(u \cdot F)(f) = F(u|f)$ for $u \in A(n)$ and $F \in \mathcal{F}(n)$.

We define e_n to be the element of $\mathcal{F}(n)$ such that $e_n(\Delta) = 1$ and $e_n(\Delta^{2j+1}) = 0$ for all $1 \leq j < n$ (i.e. characteristic of Δ).

Denote the q-coefficients of a modular form f by $a_m(f)$, so $f = \sum_{m>0} a_m(f) q^m$. Then $e_n(f) = a_1(f)$. For an odd prime p, have $a_1(T_p|f) = a_p(f)$, so $T_p \cdot e_n(f) = a_p(f)$. By induction, this gives for odd primes $p_1, p_2, \dots, p_k$:

$$T_{p_1} T_{p_2} \cdots T_{p_k} \cdot e_n(f) = a_{p_1 p_2 \cdots p_k}(f)$$

2.2 Basic Properties

Property 2.2. *Note that for a non zero modular forms $f \in \mathcal{F}(n)$, there exists an operator $u \in A(n)$ such that $e_n(u|f) = 1$.*

Proof. We can write $f = q^m + \mathcal{O}(q^{m+1})$ for some m odd (as $\mathcal{F}(n)$ is generated by odd powers of Δ). Now, as m is odd, $m = p_1 p_2 \cdots p_k$ with p_i odd primes for all $1 \leq i \leq k$. Then, by the above, $T_{p_1} T_{p_2} \cdots T_{p_k} \cdot e_n(f) = a_m(f) = 1$. Letting $u = T_{p_1} T_{p_2} \cdots T_{p_k}$, we have $e_n(u|f) = u \cdot e_n(f) = 1$. □

Property 2.3. *$\mathcal{F}(n)^*$ is free as an $A(n)$-module, with basis e_n; i.e., $\mathcal{F}(n)^* = A(n) \cdot e_n$.*

Proof. By contradiction, suppose (e_n) (the $A(n)$-module generated by e_n) isn't $\mathcal{F}(n)^*$. The there must be a non-zero modular form $f \in \mathcal{F}(n)$ such that $u \cdot e_n(f) = 0$ for all $u \in A(n)$. This would contradict the last property. Therefore, we have $\mathcal{F}(n)^* = A(n) \cdot e_n$. □

Corollary 2.1. *From last property, we deduce:*

- *The map $\phi : A(n) \to \mathcal{F}(n)^*$ such that $\phi(u) = u \cdot e_n$ is a bijection.*
- *The dimension of $A(n)$ is n.*
- *There is a bijection $\phi : A(n) \to \mathcal{F}(n)^*$.*

Proof. We prove separately:

- This follows directly from the fact that $\mathcal{F}(n)^* = A(n) \cdot e_n$.
- We have $\dim(A(n)) = \dim(\mathcal{F}(n)^*)$ by the above, and $\dim(\mathcal{F}(n)^*) = \dim(\mathcal{F}(n))$ by duality.
- Since $\mathcal{F}(n)^* \leftrightarrow A(n)$ [2], $\mathcal{F}(n)^{**} \leftrightarrow A(n)^*$. And as $\mathcal{F}(n)^{**} \cong \mathcal{F}(n)$, we have $\mathcal{F}(n) \leftrightarrow A(n)^*$.

$\square$

2.3 Generated by T_3 and T_5

[2] $A \leftrightarrow B$ means there exists a bijection from A to B

3 Frobenian Elements

3.1 Context

Let R be a commutative ring, M and P ideals in R. We can then prove the followings:

Theorem 2. • *M is maximal $\iff$ R/M is a field*

• *P is prime $\iff$ R/P is an integral domain*

Property 3.1. *Maximal ideals are prime.*

Proof.

$$\begin{aligned} M \text{ maximal ideal} &\iff R/M \text{ field} \\ &\implies \text{R/M Integral Domain} \iff M \text{ prime ideal} \end{aligned}$$

□

If L/K is a Galois extension, then we will denote it's Galois group by $\mathrm{Gal}(L/K)$.

———–

Let K be a number field, and $\mathcal{O}_K$ be the corresponding ring of integers. Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$. Let L/K be a finite extension and again, $\mathcal{O}_L$ be the ring of integers in L.

Then we know that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L

We have $\mathfrak{p}\mathcal{O}_L$ an ideal in $\mathcal{O}_L$. It is not a prime ideal in general, but as L/K is finite, there exists a factorization as the following:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

Where the integers e_i are called the ramification indexes. We also have $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$, and we say that the ideals $\mathfrak{P}_i$ in L extend the ideal $\mathfrak{p}$ in K.

Then, there are three possibilities for an ideal: it may split, ramify of be inert.

Definition 3.1 (Ideal Ramifies)**.** *We say that an ideal $\mathfrak{p}$ ramifies in L/K if a ramification index e_i is greater then one, i.e. if $e_i > 1$ for some $1 \leq i \leq r$.*

Definition 3.2 (Ideal Splits)**.** *We say that $\mathfrak{p}$ splits in L/K if none of the ramification indexes e_i is greater then one, and r is a least two; i.e. if $e_i = 1 \quad \forall 1 \leq i \leq r$ and $r \geq 2$.*

Definition 3.3 (Ideal Inert)**.** *We say that $\mathfrak{p}$ is inert in L/K if there is only one ramification index e_1 and it is equal to one; i.e. if $e_1 = 1$ and $r = 1$.*

We know that the extension L/K is ramified in the primes that divide the discriminant. Therefore, the extension is unramified in all but finitely many prime ideals.

3.2 Residue Fields Extensions

The ideal $\mathfrak{p}$ defines the residue field $F = \mathcal{O}_K/\mathfrak{p}$. The ideals $\mathfrak{P}_i$ define the residue fields $F_i = \mathcal{O}_L/\mathfrak{P}_i$. The field F then naturally embeds to F_i (so each $\mathfrak{P}_i$ defines a field extension). The inertia degree of $\mathfrak{P}_i$ is the degree $f_i = [F_i : F] = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ of this extension.

We then observe that $[L : K] = \sum_{i=1}^{r} e_i f_i$

We can then specify when an ideal splits or ramifies completely.

Definition 3.4 (Ideal Splits Completely). *We say that $\mathfrak{p}$ splits completely in L/K if all ramification indexes e_i and inertia degrees f_i are one. i.e. if $e_i = f_i = 1 \quad \forall 1 \le i \le r$.*
In this case, $r = [L : K]$.

Definition 3.5 (Ideal Ramifies Completely). *We say that $\mathfrak{p}$ ramifies completely in L/K if the inertia degrees f_1 is one, and r is one. i.e. if $r = 1$ and $f_1 = 1$.*
In this case, $e_1 = [L : K]$.

3.3 Norms of Ideals

We define the norm of an ideal I in $\mathcal{O}_K$ as $N(I) = |\mathcal{O}_K/I|$.

If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal, then we can put $(p) = \mathfrak{p} \cap \mathbb{Z}$. It follows that $p\mathcal{O}_K \subset \mathfrak{p}$. $\mathcal{O}_K$ is a free $\mathbb{Z} - module$ of rank $[K : \mathbb{Q}] = q$, i.e. $\exists \alpha_1, \dots, \alpha_q$ s.t. $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_q$. Thus, $|\mathcal{O}_K/\mathfrak{p}| \le |\mathcal{O}_K/(p)| \le p^q$.

We have $\mathrm{Norm}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = p^m$ and $\mathrm{Norm}_{L/\mathbb{Q}}(\mathfrak{P}_i) = \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})^{f_i}$. This implies $\mathrm{Norm}(\mathfrak{P}_i) = |\mathcal{O}_L/\mathfrak{P}_i| = p^{mf_i}$.
We also have: $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{\mathrm{Norm}(\mathfrak{p})}$ and $\mathcal{O}_L/\mathfrak{P}_i \cong \mathbb{F}_{\mathrm{Norm}(\mathfrak{P}_i)}$

3.4 Galois Extensions Simplifications

When the extension L/K is Galois, the ramification indexes e_i are all the same ($e_i = e$), as well as the inertia degrees $f_i = f$. We then have

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^e \text{ and } [L : K] = ref.$$

The Galois group $\mathrm{Gal}(L/K)$ is often denoted G.

We define the decomposition group $G_{\mathfrak{P}}$ of the ideal $\mathfrak{P}$ to be $\{\sigma \in G | \sigma(\mathfrak{P}) = \mathfrak{P}\}$. It turns out that $G_{\mathfrak{P}} \cong \mathrm{Gal}({}^{\mathcal{O}_L/\mathfrak{P}}/{}_{\mathcal{O}_K/\mathfrak{p}}) \cong \mathrm{Gal}(\mathbb{F}_{p^{mf}}/\mathbb{F}_{p^f})$. Moreover, it is a cyclic group, so $G_{\mathfrak{P}} =< \tilde{\sigma} >$.

3.5 Unramified Prime Simplifications

When the ideal $\mathfrak{p}$ is unramified, $e = 1$, so we get:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P} \text{ and } [L : K] = rf$$

3.6 The Frobenius Element

3.6.1 Definition

[is it ok as a subsection title? (perhaps too generic?) alternatives: well definiteness, introduction]

We can construct the *Frobenius element* (sometimes also called the Artin symbol, or the Frobenius map) that depend on the extension L/K and ideal $\mathfrak{P}$ in $\mathcal{O}_L$. It is denoted $\mathrm{Frob}_{L/K}(\mathfrak{P})$, and is *the* element $\sigma \in G$ such that:

$$\sigma\mathfrak{P} = \mathfrak{P} \quad \text{and} \quad \sigma(\alpha) \equiv \alpha^{\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})} \bmod \mathfrak{P} \quad \forall \alpha \in \mathcal{O}_L.$$

The second condition is the interesting one; while the first is only useful to make the Frobenius element unique. The second condition defines a unique element only up to conjugacy class. Most of the time, we will consider abelian extensions, so the conjugacy classes will only have one element, and the first condition will be dropped.

We define the Frobenius element for $\mathfrak{p}$ (denoted $\mathrm{Frob}_{L/K}(\mathfrak{p})$) in a meaning full manner, to be the set $\{\mathrm{Frob}_{L/K}(\mathfrak{P}) | \mathfrak{P} \text{ extending } \mathfrak{p}\} \subset G$.

[is this construction / definition ok? or maybe I should rephrase it? (it look weird to me)]

Property 3.2. *If $\tau \in G$, then $Frob_{L/K}(\tau\mathfrak{P}) = \tau Frob_{L/K}(\mathfrak{P})\tau^{-1}$.*

Proof. For all $x \in \mathcal{O}_L$, we have:

$$\mathrm{Frob}_{L/K}(\mathfrak{P})x = x^{\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})} \mod \mathfrak{P}$$

But all such x may be written as $\tau^{-1}(x)$, so we have:

$$\mathrm{Frob}_{L/K}(\mathfrak{P})\tau^{-1}(x) = (\tau^{-1}x)^{\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})} \mod \mathfrak{P}$$

Which gives:

$$\tau\mathrm{Frob}_{L/K}(\mathfrak{P})\tau^{-1}(x) = x^{\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})} \mod \mathfrak{P}$$

□

Property 3.3. *If $\mathfrak{P}_1$ and $\mathfrak{P}_2$ extend $\mathfrak{p}$, then $Frob_{L/K}(\mathfrak{P}_1)$ and $Frob_{L/K}(\mathfrak{P}_2)$ are conjugates.*

Proof. We have the following scheme:

$$\begin{tikzcd}
L \arrow[d, dash] & \supseteq & \mathfrak{P}_1 \arrow[dr, dash] & & \mathfrak{P}_2 \arrow[dl, dash] \\
K & \supseteq & & \mathfrak{p} &
\end{tikzcd}$$

There is an element $\tau \in G$ such that $\tau(\mathfrak{P}_1) = \mathfrak{P}_2$. Then using last property, we deduce that $\mathrm{Frob}_{L/K}(\mathfrak{P}_1)$ and $\mathrm{Frob}_{L/K}(\mathfrak{P}_2)$ are conjugates. □

Never the less, is important to notice at this point that if G is abelian, then all conjugacy classes are made up of only one element. Therefore, the Frobenius element is well defined in this case. Moreover, it will only depend on the prime $\mathfrak{p}$ that is extended. [should this comment be before or after the property?]

3.6.2 Examples

$\mathbb{Q}[\sqrt{7}]/\mathbb{Q}$ (quadratic field extension) We have minimum polynomial $m(x) = x^2 - 7$, the discriminant is $\Delta = 4.7 = 28$.
We write

$$G = \mathrm{Gal}(\mathbb{Q}[\sqrt{7}] : \mathbb{Q}) = <\sigma \mid \sigma^2 = 1_G > \cong C_2.$$

As C_2 is abelian, we will have no problem defining Frobenius elements.

The prime ideal (3) As $m(x) = (x+1)(x-1) \mod 3$, we have $(3) = (3, \sqrt{7}+1)(3, \sqrt{7}-1)$. As well, $\mathrm{Norm}_{\mathbb{Q}[\sqrt{7}]/\mathbb{Q}}((3)) = 3$ and $\mathrm{Norm}_{\mathbb{Q}[\sqrt{7}]/\mathbb{Q}}((3, \sqrt{7}+1)) = \mathrm{Norm}_{\mathbb{Q}[\sqrt{7}]/\mathbb{Q}}((3, \sqrt{7}-1)) = 3$, but $\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((3)) = 3$. So we have:

$$\begin{aligned}\mathrm{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((3, \sqrt{7}+1)) : \alpha &\to \alpha^{\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((3))} \mod (3, \sqrt{7}+1) \\ \sqrt{7} &\to \left(\sqrt{7}\right)^3 \equiv \sqrt{7} \mod (3, \sqrt{7}+1)\end{aligned}$$

Thus, $\mathrm{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((3, \sqrt{7}+1)) = 1_G \in G$. Similarly, $\mathrm{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((3, \sqrt{7}-1)) = 1_G \in G$.

The prime ideal (5) As $m(x)$ has no root mod2. So $m(x)$ is irreducible mod5 and (5) is inert in $\mathbb{Q}[\sqrt{7}]$ As well, $\mathrm{Norm}_{\mathbb{Q}[\sqrt{7}]/\mathbb{Q}}((5)) = 5^2 = 25$ but $\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((5)) = 5$. So we have:

$$\begin{aligned}\mathrm{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((5)) : \alpha &\to \alpha^{\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((5))} \bmod (5)\\ \sqrt{7} &\to \left(\sqrt{7}\right)^5 \equiv -\sqrt{7} \bmod (5)\end{aligned}$$

Thus, $\mathrm{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((5)) = \sigma \in G$.

$\mathbb{Q}[\zeta_n]/\mathbb{Q}$ **(n^{th} Cyclotomic Field Extensions)** We have minimum polynomial:

$$\Phi(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - e^{2i\pi \frac{k}{n}}\right)$$

(so degree of the extension is $\varphi(n)$, where φ is Euler totient function).

Discriminant of the extension is:

$$\Delta = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}$$

see [Washington, 1997, Proposition 2.7].

The Galois group G consist of σ_k such that $\sigma_k(\zeta_n^i) = \zeta_n^{ik}$, with $\gcd(k,n) = 1$.) Note as well that G is abelian, so it is simple to calculate the Frobenius element. It is straightforward that G is naturally isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. Note that $\sigma \in G$ is determined by $\sigma(\zeta_n)$. Note as well that this group is abelian.

With $p \in \mathbb{P}$, a prime that is unramified in $\mathbb{Q}[\zeta_n]/\mathbb{Q}$, let P be an ideal lying above (p). We want to look at $\mathrm{Frob}_{\mathbb{Q}[\zeta_n]/\mathbb{Q}}(P)$:

We have:

$$\begin{aligned}\mathrm{Frob}_{\mathbb{Q}[\zeta_n]/\mathbb{Q}}(P) : \alpha &\to \alpha^{\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((p))} \bmod P\\ \zeta_n &\to \zeta_n^p \bmod P\end{aligned}$$

Case $\mathbb{Q}[\zeta_{10}]/\mathbb{Q}$ **(10^{th} cyclotomic field extension)** We denote by $\zeta_{10} = e^{\pi i/5}$ the 10^{th} root of unity. We have minimum polynomial $m(x) = x^4 - x^3 + x^2 - x + 1$ (so degree of the extension is 4), the discriminant is $\Delta = 5^3$.

We write $G = \mathrm{Gal}(\mathbb{Q}[\zeta_{10}] : \mathbb{Q}) =< \sigma : \zeta_{10} \to \zeta_{10}^3 \mid \sigma^4 = Id >\cong C_4$.

The prime ideal (3) As $m(x)$ has no root mod3, so (3) is inert. We have:

$$\begin{aligned}\mathrm{Frob}_{\mathbb{Q}[\zeta_{10}]/\mathbb{Q}}((3)) : \alpha &\to \alpha^{\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((3))} \bmod (3)\\ \zeta_{10} &\to (\zeta_{10})^3 \bmod (3)\end{aligned}$$

Thus, $\mathrm{Frob}_{\mathbb{Q}[\zeta_{10}]:\mathbb{Q}}((3)) = \sigma \in G$.

The prime ideal (7) As $m(x)$ has no root mod7, so (7) is inert. We have:

$$\begin{aligned}\mathrm{Frob}_{\mathbb{Q}[\zeta_{10}]/\mathbb{Q}}((7)) : \alpha &\to \alpha^{\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((7))} \bmod (7)\\ \zeta_{10} &\to (\zeta_{10})^7 \bmod (7)\end{aligned}$$

Thus, $\mathrm{Frob}_{\mathbb{Q}[\zeta_{10}]:\mathbb{Q}}((7)) = \sigma^3 \in G$.

The prime ideal (11) As $m(x) = (x-2)(x+3)(x+4)(x+4) \bmod 11$, so (11) splits. We have:

$$\begin{aligned} \mathrm{Frob}_{\mathbb{Q}[\zeta_{10}]/\mathbb{Q}}((11)) : \alpha &\to \alpha^{\mathrm{Norm}_{\mathbb{Q}/\mathbb{Q}}((11))} \bmod (11) \\ \zeta_{10} &\to (\zeta_{10})^{11} = \zeta_{10} \bmod (11) \end{aligned}$$

Thus, $\mathrm{Frob}_{\mathbb{Q}[\zeta_{10}]:\mathbb{Q}}((11)) = \sigma^4 = Id \in G$.

3.6.3 Behaviour in Chained Extensions

We will consider the following scheme:

$$\begin{array}{ccc} \mathcal{O}_M \subset M & \supseteq & \mathfrak{P} \\ | & & | \\ \mathcal{O}_L \subset L & \supseteq & \mathfrak{p} \\ | & & | \\ \mathcal{O}_K \subset K & \supseteq & p \end{array}$$

In such a situation, we can define (for M/K Galois) $\mathrm{Frob}_{M/K}(\mathfrak{P})$, $\mathrm{Frob}_{M/K}(p)$, $\mathrm{Frob}_{M/L}(\mathfrak{P})$, $\mathrm{Frob}_{M/L}(\mathfrak{p})$. If, in addition, L/K is normal: $\mathrm{Frob}_{L/K}(\mathfrak{p})$, and $\mathrm{Frob}_{L/K}(p)$. [Janusz, 1996, p.99]

We will look at properties of these Frobenius elements (relation between each others).

Property 3.4.

$$Frob_{M/K}(\mathfrak{P})^{f(\mathfrak{P}/\mathfrak{p})} = Frob_{M/L}(\mathfrak{P})$$

[what is this $f(\mathfrak{P}/\mathfrak{p})$? is it the fields of $\mathfrak{P}$ over $\mathfrak{p}$?]

to write... [Janusz, 1996, p.99] □

Property 3.5.

$$Frob_{L/K}(\mathfrak{p}) = Frob_{M/K}(\mathfrak{P})\big|_L$$

Proof. Let $\sigma = \mathrm{Frob}_{M/K}(\mathfrak{P}) \in \mathrm{Gal}(M/K)$ so $\sigma : M \to M$ s.t. $\sigma|_K = Id$ and σ is an autotomorphism. Similarly, let $\tau = \mathrm{Frob}_{L/K}(\mathfrak{p}) \in \mathrm{Gal}(L/K)$ so $\tau : L \to L$ s.t. $\tau|_K = Id$ and τ is an autotomorphism.

As M extends L, σ being an automorphism of M makes it an automorphism of L as well. The restriction condition stays the same. □

Property 3.6.

$$Gal(L/K) \cong {}^{Gal(M/K)}/_{Gal(M/L)}$$

Proof. Let $\sigma \in \mathrm{Gal}(M/K)$, i.e. $\sigma : M \to M$ s.t. $\sigma|_K = Id$ and σ is an autotomorphism.

Let $\phi : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ be such that: $\phi(\sigma) = \sigma|_L$. This is well defined as an automorphism of M restricts to an automorphism of L when M extends L.

It is trivial to check that ϕ is a homomorphism.

The kernel of ϕ is clearly $\mathrm{Gal}(M/L)$.

The image of ϕ is $\mathrm{Gal}(L/K)$ as every element of $\mathrm{Gal}(L/K)$ may be extended to $\mathrm{Gal}(M/K)$.

Therefore, the property follows via the 1^{st} isomorphism theorem. □

Property 3.7. *We have:*

$$\mathfrak{p} \textit{ splits complitely in } L \iff Frob_{L/K}(\mathfrak{P}) = 1$$

[Janusz, 1996, p.100]

We will consider the following scheme:

$$\begin{tikzcd}
& L_1L_2 \supseteq \mathfrak{P} \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \supseteq \mathfrak{p}_1 \arrow[dr, dash] & & L_2 \supseteq \mathfrak{p}_2 \arrow[dl, dash] \\
& K \supseteq \mathfrak{p} &
\end{tikzcd}$$

Property 3.8. *We have:*

$$Frob_{L_1L_2/K}(\mathfrak{P}) = Frob_{L_1/K}(\mathfrak{p}_1) \times Frob_{L_2/K}(\mathfrak{p}_2)$$

[Janusz, 1996, p.100]

Property 3.9. *We have:*

$$\mathfrak{p} \text{ splits complitely in } L_1L_2 \iff \mathfrak{p} \text{ splits complitely in } L_1 \text{ and } L_2$$

Proof. Combine the last two proposition. [Janusz, 1996, p.100] □

3.7 The Chebotarev's Density Theorem

3.7.1 Motivations

If we look at the distribution of primes numbers modulo a number (15 in the next example), we get a table as follows:

Table mod 15:

mod15	primes (up to 500)
0	
1	31, 61, 151, 181, 211, 241, 271, 331, 421,
2	2, 17, 47, 107, 137, 167, 197, 227, 257, 317, 347, 467,
3	3,
4	19, 79, 109, 139, 199, 229, 349, 379, 409, 439, 499,
5	5,
6	
7	7, 37, 67, 97, 127, 157, 277, 307, 337, 367, 397, 457, 487,
8	23, 53, 83, 113, 173, 233, 263, 293, 353, 383, 443,
9	
10	
11	11, 41, 71, 101, 131, 191, 251, 281, 311, 401, 431, 461, 491,
12	
13	13, 43, 73, 103, 163, 193, 223, 283, 313, 373, 433, 463,
14	29, 59, 89, 149, 179, 239, 269, 359, 389, 419, 449, 479,

It looks like there are classes of primes. We would like to characterize this repartition: that is, decide if classes are finite or infinite, and quantify the repartitions.

3.7.2 Notions of Density

As discussed previously, we are interested in subsets of $\mathbb{P}$ (the set of primes numbers). Euler proved that there are infinitely many primes. Therefore, there are two types of subsets of $\mathbb{P}$: the ones that are infinite, and the finites ones. For finite sets, we can characterise the size by just counting elements. In fact, we will mainly be interested in sets that have infinitely many primes, and again, we would like a notion of size.

A suitable way would be to compare the subset with the set of all primes, and, say look at the proportions of primes included in the subset.

We call this the density, there are two rigorous ways to define it:

Definition 3.6 (Natural density). *We say that $S \subseteq \mathbb{P}$ has natural density δ when:*

$$\lim_{x \to +\infty} \frac{\#\{p \in \mathbb{P} | p \in S\}}{\#\{p \in \mathbb{P} | p \in \mathbb{P}\}} = \delta$$

Definition 3.7 (Analytic density or Dirichlet density). *We say that $S \subseteq \mathbb{P}$ has analytical (or Dirichlet) density δ when:*

$$\lim_{s \to 1^+} \left(\sum_{p \in S} \frac{1}{p^s} \right) \left(\sum_{p \in \mathbb{P}} \frac{1}{p} \right)^{-1} = \delta$$

Note that the natural density may not exist. However, when both exist, the two densities are the same.

3.7.3 Statement

One of the most important results that use Frobenian maps is probably the Chebotarev density theorem.

Theorem 3 (Chebotarev Density Theorem). *With L/K an extension of Galois group $G = Gal(L/K)$. Let C be a conjugacy class in G.*

Then, the proportion of unramified primes ideals $\mathfrak{p}$ in K that have Frobenius element $Frob_{L/K}(\mathfrak{p}) = C$ [3] is $|C|/|G|$.

We see that Frobenius elements are in the heart of this theorem. It was proved by Nikolai Chebotarev in his thesis (Tschebotareff [1926]).

3.7.4 Example

[extension of order 3?]

3.7.5 Special Case

Here, we want to apply Chebotarev theorem in the case of a quadratic field extension. We are looking at the field extension $L/K = \mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ for $d \in \mathbb{Z}$ a square-free integer. Denote by $G = \mathrm{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q}) \cong C_2$ the Galois group of this extension. This group is abelian (so all conjugacy classes are made of a single element), and for any conjugacy class C, $|C|/|G| = 1/2$.

Now, for a prime p unramified, we want to calculate the Frobenius element. If p is unramified, either $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = R_1 R_2$ or $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = R$.

[3] When depending on a prime in the "lower" field, the Frobenius element is a conjugacy class to be well defined.

In the first case, we have $\left(\frac{d}{p}\right) = 1$ (i.e. $\sqrt{d} \in \mathbb{F}_p$, so d is a square modulo p). In this case, $\sqrt{d}^p \equiv \sqrt{d} \bmod p$ so $\text{Frob}_{\mathbb{Q}[\sqrt{d}]}(p) = \left\{Id : \sqrt{d} \to \sqrt{d}\right\} \in G$.

In the second case, $\left(\frac{d}{p}\right) = -1$ (i.e. $\sqrt{d} \notin \mathbb{F}_p$, so d is not a square modulo p). In this case, $\sqrt{d}^p \not\equiv \sqrt{d} \bmod p$ as there is no other choice, $\text{Frob}_{\mathbb{Q}[\sqrt{d}]}(p) = \left\{\sigma : \sqrt{d} \to -\sqrt{d}\right\} \in G$.

Then by Chebotarev's density theorem, we have that the density of primes p such that $\left(\frac{d}{p}\right) = \pm 1$ is $1/2$ in both cases.

Therefore, we have the following summary:

Primes $p \in \mathbb{P}$ such that:	Density:
$\left(\frac{d}{p}\right) = +1$	$1/2$
$\left(\frac{d}{p}\right) = 0$	0
$\left(\frac{d}{p}\right) = -1$	$1/2$

Thus, for a square free d, $\left(\frac{d}{p}\right)$ is as often $+1$ as -1 (for a prime p), and $\left(\frac{d}{p}\right) = 0$ happens only finitely many times.

3.8 The Dirichlet's Density Theorem

3.8.1 Statement

The most common application of Chebotarev density theorem is probably the Dirichlet's density theorem.

Theorem 4 (Dirichlet's Density Theorem)**.** *Let* $n \in \mathbb{N}^*$*,* $a \in \mathbb{N}$ *such that* $\gcd(a, n) = 1$*. If* $S = \{p \in \mathbb{P} \mid p \equiv a \mod n\}$*, then* S *has density* $1/\varphi(n)$*.*

3.8.2 Link with Chebotarev

This is a direct application of Chebotarev's density theorem for the field extension $\mathbb{Q}[\zeta] : \mathbb{Q}$ where ζ is the n^{th} root of unity (this is the cyclotomic field).

The Galois group is abelian (it is precisely $G = \mathbb{Z}_n^\times$ and has order $\varphi(n)$). The abelian property implies that all conjugacy classes are made of a single element. Thus, for any conjugacy class C, the fraction $|C|/|G|$ is just $1/\varphi(n)$. Primes ideals in $\mathbb{Q}$ are just primes numbers. Therefore, Chebotarev gives Dirichlet's density theorem in the particular case of cyclotomic extensions.

3.8.3 Example

Here, look at the example of Dirichlet theorem in the case $n = 15$ from the motivation subsection above (see 3.7.1).

We apply the last theorem in the case of $n = 15$: $\varphi(15) = 8$. We define $S_k = \{p \in \mathbb{P} \mid p \equiv k \bmod 15\}$. By Dirichlet density theorem, the density of S_k is $1/8$ if k and 15 are co-prime (i.e. if $k = 1, 2, 4, 7, 8, 11, 13, 14$), otherwise (if $k = 0, 3, 5, 6, 9, 10, 12$) it is 0. This is what we could conjecture from the observations.

4 Frobenian Maps

Class functions Let G be a group, Ω a set, and $f : G \to \Omega$. We say that f is a *class function* (of G) if f is constant on conjugacy classes of G. That is, if f remains unchanged under conjugation map of G.

Frobenian Property for Maps Let K be a number field. Let P be the set of primes ideals in K A map $f : P \to \Omega$ is said to be *Frobenian* if there exists a field extension M/K and a class function $\phi : \mathrm{Gal}(M/K) \to \Omega$ such that for all $\mathfrak{p} \in P$ (prime ideal of K) unramified in M/K, we have $f(\mathfrak{p}) = \phi(\mathrm{Frob}_{M/K}(\mathfrak{p}))$ [4].

In the case of $K = \mathbb{Q}$, the set of primes ideals becomes just the set of primes $\mathbb{P}$. And a map $f : \mathbb{P} \to \Omega$ is said to be *Frobenian* if there exists a field extension $M/\mathbb{Q}$ and a class function $\phi : \mathrm{Gal}(M/\mathbb{Q}) \to \Omega$ such that for all $p \in \mathbb{P}$ (prime) unramified in $M/\mathbb{Q}$, we have $f(p) = \phi(\mathrm{Frob}_{M/\mathbb{Q}}(p))$.

$a_{ij}(p)$ **Frobenian** We recall that for all p odd prime,

$$T_p = \sum_{i,j \geq 0} a_{ij}(p) T_3^i T_5^j \qquad \text{with } a_{ij}(p) \in \mathbb{F}_2.$$

Theorem 5. *The map $p \to a_{ij}(p)$ is Frobenian (for all $i, j \geq 0$).*
That is, for all $i, j \geq 0$, there exists an extension $M_{ij}/\mathbb{Q}$ and a class function $\phi_{ij} : Gal(M_{ij}/\mathbb{Q}) \to \mathbb{F}_2$ such that $a_{ij}(p) = \phi_{ij}(Frob_{M_{ij}/\mathbb{Q}}(p))$ for all $p \in \mathbb{P}$ unramified in $M_{ij}/\mathbb{Q}$.

In such a configuration, M_{ij} are called *governing fields.*

[4]Note that $\phi(\mathrm{Frob}_{M/K}(\mathfrak{p}))$ is well defined since ϕ is a class function, and $\mathrm{Frob}_{M/K}(\mathfrak{p})$ is a conjugacy class of $\mathrm{Gal}(M/K)$.

References

Keith Conrad. $SL_2(\mathbb{Z})$. [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.

Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. ISBN 0-8218-3368-5.

Kazuyuki Hatada. Eigenvalues of Hecke operators on SL(2, **Z**). *Math. Ann.*, 239(1):75–96, 1979. ISSN 0025-5831. doi: 10.1007/BF01420494. URL https://doi.org/10.1007/BF01420494.

Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997. ISBN 0-387-94762-0. doi: 10.1007/978-1-4612-1934-7. URL https://doi.org/10.1007/978-1-4612-1934-7.

Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996. ISBN 0-8218-0429-4.

N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.*, 95(1):191–228, 1926. ISSN 0025-5831. doi: 10.1007/BF01206606. URL https://doi.org/10.1007/BF01206606.