# Mod $p$ Modular Forms

Andrew Mendelsohn

2018/19

CID: 01540461
Supervisor: Dr David Helm

# Abstract

# Contents

# 1 Preliminaries

## 1.1 Algebraic Number Theory

This subsection relies on the results and proofs of [**cox**], [**lang1**], and [**sutherland**].

Let $K$ be a number field and $\mathcal{O}_K$ denote its ring of integers. A Dedekind domain is an integrally closed, noetherian domain in which every (non-zero) prime ideal is maximal. In addition, in a Dedekind domain every fractional ideal has a unique factorization into prime ideals. Recall that $\mathcal{O}_K$ is a Dedekind domain.

**Definition 1.** Let $A \subset B$ be an inclusion of rings and $\mathfrak{p}$ a prime ideal in $A$. If $\mathfrak{q}$ is a prime ideal of $B$, we say $\mathfrak{q}$ lies above $\mathfrak{p}$ if $\mathfrak{q} \cap A = \mathfrak{p}$.

Let $L$ be a finite extension of $K$ and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, which is a Dedekind domain, so $\mathfrak{p}\mathcal{O}_L$ has a unique factorization into prime ideals of $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \prod_i \mathfrak{q}_i^{e_i} = \mathfrak{q}_1^{e_1}...\mathfrak{q}_g^{e_g}, \tag{1}$$

for $\mathfrak{q}_i$ prime in $\mathcal{O}_L$ all lying above $\mathfrak{p}$.
We call $e_i$ the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$. We call $f_i = \left[\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}\right]$ the *inertial degree* of $\mathfrak{p}$ in $\mathfrak{q}_i$. Note that since both $\mathcal{O}_L/\mathfrak{q}_i$ and $\mathcal{O}_K/\mathfrak{p}$ are finite fields, $\mathcal{O}_L/\mathfrak{q}_i$ is a separable and normal extension of $\mathcal{O}_K/\mathfrak{p}$.

For the following results, the picture is as follows: we take a number field $K$ and its ring of integers $\mathcal{O}_K$, together with $L$, a finite, Galois extension of $K$, and its ring of integers $\mathcal{O}_L$ (which is the integral closure of $\mathcal{O}_K$ in $L$) to obtain:

$$\begin{array}{ccc} K & \subset & L \\ \cup & & \cup \\ \mathcal{O}_K & \subset & \mathcal{O}_L \end{array}$$

**Lemma 1.** *Let $L$ be a finite, Galois extension of $K$ and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_k$. If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$, there exists an element $\sigma \in Gal(L/K)$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$.*

*Proof.* Suppose that $\mathfrak{q}_1 \neq \sigma(\mathfrak{q}_2)$ for all $\sigma \in Gal(L/K)$. In a Dedekind domain, non-zero prime ideals are maximal, and in general distinct maximal ideals are coprime. Thus $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are coprime, and we can apply the Chinese Remainder Theorem to find $x \in \mathcal{O}_L$ such that

$$x \equiv 0 \bmod \mathfrak{q}_1 \text{ and } x \equiv 1 \bmod \sigma(\mathfrak{q}_2)$$

for all $\sigma \in Gal(L/K)$. Denote $Gal(L/K)$ by $G$. The norm $N_{L/K}(x) = \prod_{\sigma\in G}\sigma(x)$ maps $L$ to $K$ and $\mathcal{O}_L$ to $\mathcal{O}_k$, so $N_{L/K}(x) \in K \cap \mathcal{O}_K = \mathcal{O}_K$. Moreover, since $x \equiv 0 \bmod \mathfrak{q}_1$, $N_{L/K}(x) \in \mathfrak{q}_1 \cap \mathcal{O}_K = \mathfrak{p}$. However, since $x \notin \sigma(\mathfrak{q}_2)$ for all $\sigma \in G$, we must have $\sigma^{-1}(x) \notin \mathfrak{q}_2$ for all $\sigma \in G$, which is equivalent to $\sigma(x) \notin \mathfrak{q}_2$ for all $\sigma \in G$. This is a contradiction, as $N_{L/K}(x) = \prod\limits_{\sigma\in G}\sigma(x) \in \mathfrak{p} \subset \mathfrak{q}_2$, as $\mathfrak{q}_2$ lies above $\mathfrak{p}$. □

Note: this is equivalent to saying $G$ acts transitively on the set of primes lying above $\mathfrak{p}$.

**Corollary 1.** *If $L$ and $K$ are as above, and $\mathfrak{q}_1, ..., \mathfrak{q}_g$ are the prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p} \subset \mathcal{O}_K$, then*

(i) *The $\mathfrak{q}_i$ have the same ramification index, $e$, for all $i$.*

(ii) *The inertial degrees $f_i$ of $\mathfrak{p}$ in $\mathfrak{q}_i$ are equal, for all $i$.*

*Proof.* (i) Let $\sigma \in G = Gal(L/K)$. Then $\sigma$ fixes $K$, thereby fixing $\mathfrak{p}$. In addition, $\sigma$ fixes $\mathcal{O}_L$: if $\alpha \in \mathcal{O}_L$, there exists a monic polynomial $f$ with coefficients in $\mathcal{O}_K$ such that $f(\alpha) = 0$. Then $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$, since $\sigma$ fixes elements of $K$; so $\sigma(\alpha)$ lies in $L$ and is integral over $\mathcal{O}_K$, so must be an element of $\mathcal{O}_L$. This means that $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$. The same argument holds for $\sigma^{-1}$, i.e. $\sigma^{-1}(\mathcal{O}_L) \subseteq \mathcal{O}_L$, which implies that $\mathcal{O}_L \subseteq \sigma(\mathcal{O}_L)$. Combining both inclusions, we must have that $\sigma$ fixes $\mathcal{O}_L$ setwise.

We have found that $\sigma$ fixes both $\mathfrak{p}$ and $\mathcal{O}_L$, so it follows that $\sigma$ fixes $\mathfrak{p}\mathcal{O}_L$. Define $\nu_i : \mathfrak{p}\mathcal{O}_L \mapsto e_i$ to be the function that gives the ramification index of $\mathfrak{q}_i$. Then

$$\begin{aligned} e_j = \nu_j\big(\mathfrak{p}\mathcal{O}_L\big) = \nu_j\big(\sigma\big(\mathfrak{p}\mathcal{O}_L\big)\big) &= \nu_j\big(\sigma\big(\prod_i \mathfrak{q}_i^{e_i}\big)\big) \\ &= \nu_j\big(\prod_i \sigma(\mathfrak{q}_i)^{e_i}\big) \\ &= \nu_j\big(\prod_i \mathfrak{q}_{\pi(i)}^{e_i}\big) \\ &= \nu_j\big(\prod_i \mathfrak{q}_i^{e_{\pi^{-1}(i)}}\big) = e_{\pi^{-1}(j)}, \end{aligned}$$

where $\pi$ is the induced permutation on the set $\{1, .., g\}$ of indices of the $\mathfrak{q}_i$. Since $G$ acts transitively on primes lying above $\mathfrak{p}$, the induced permutation is also transitive, and so the $e_i$ are equal for all $i$.

(ii) As shown in (i), $\sigma$ fixes $\mathcal{O}_L$, so we obtain an isomorphism $\mathcal{O}_L/\mathfrak{q}_i \tilde{\to} \mathcal{O}_L/\sigma(\mathfrak{q}_i)$. Thus

$$f_i = \big[\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}\big] = \big[\mathcal{O}_L/\sigma(\mathfrak{q}_i) : \mathcal{O}_K/\mathfrak{p}\big] = f_{\pi(i)},$$

and again by the transitivity of $G$ on primes lying above $\mathfrak{p}$, we are done.

□

**Definition 2.** In the above situation, we say an ideal $\mathfrak{p} \subset \mathcal{O}_K$ *ramifies* if $e > 1$, and is *unramified* if $e = 1$. Alternatively, we say that $L/K$ is unramified at $\mathfrak{p}$. If $e = 1$ and $f = 1$, we say $\mathfrak{p}$ *splits completely.*

**Definition 3.** Let $L$ be a finite, Galois extension of $K$ and $\mathfrak{q}$ a prime ideal of $L$. Define the *Decomposition Group* of $\mathfrak{q}$ to be the stabilizer of $\mathfrak{q}$ in $G$,

$$D_{\mathfrak{q}} = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}, \tag{2}$$

and the *Inertia Group* of $\mathfrak{q}$ to be

$$I_{\mathfrak{q}} = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{q}, \text{ for all } \alpha \in \mathcal{O}_L\} \tag{3}$$

Let $\sigma \in D_{\mathfrak{q}}$. Since any element of $D_{\mathfrak{q}}$ fixes $\mathfrak{q}$, and any element of $G$ fixes $\mathcal{O}_L$, $\sigma$ induces an automorphism on $\mathcal{O}_L/\mathfrak{q}$. Denote this automorphism by $\bar{\sigma}$. Since $\sigma \in G$, $\sigma$ fixes $\mathcal{O}_k$ and so $\bar{\sigma}$ fixes $\mathcal{O}_K/\mathfrak{p}$. So $\bar{\sigma} \in Gal(\mathcal{O}_L/\mathfrak{q}\big/\mathcal{O}_K/\mathfrak{p}) = \bar{G}$. We then obtain a homomorphism $D_{\mathfrak{q}} \to \bar{G}$, given by mapping $\sigma$ to $\bar{\sigma}$. Finally note that an element in the kernel of this map maps to the identity on $\mathcal{O}_L/\mathfrak{q}\big/\mathcal{O}_K/\mathfrak{p}$, so is the identity on $\mathcal{O}_L/\mathfrak{q}$, and thus is an element of $I_{\mathfrak{q}}$. We have obtained an isomorphism $D_{\mathfrak{q}}\big/I_{\mathfrak{q}} \tilde{\to} \bar{G}$.

**Proposition 1.** (i) $|D_\mathfrak{q}| = ef$.

(ii) $|I_\mathfrak{q}| = e$.

*Proof.* A full proof can be found in [**marcus**]; here we will sketch the proof. One proves that $[L : K] = \sum_i e_i f_i$. If $L/K$ is Galois, the ramification indices and inertial degrees are the same, so we obtain $\left[L : K\right] = efg$. Now, $\left[\mathrm{G} : D_\mathfrak{q}\right]$ $= g$ (by the orbit-stabiliser lemma), where $g$ is the number of primes lying above $\mathfrak{p}$. Hence $|D_q| = |G|\big/\left[G : D_\mathfrak{q}\right] = \left[L : K\right]\big/\left[G : D_\mathfrak{q}\right] = efg/g = ef$. Finally, $|I_\mathfrak{q}| = |D_\mathfrak{q}|\big/|\bar{G}| = ef/f = e$. □

### 1.1.1 Frobenius Elements

**Definition 4.** Let $K$ be a field of characteristic $p$. The *Frobenius map* on $K$ is the map

$$F : K \to K,\ a \mapsto a^p \tag{4}$$

If $q = p^r$ for some $r$, consider the Frobenius map $F$ on $\mathbb{F}_q$. Since $a^p \equiv a$ mod $p$ by Fermat Euler, $F$ fixes $\mathbb{F}_p$. Moreover, it is straightforward to prove that F defines a field homomorphism on $\mathbb{F}_q$ (one uses the binomial theorem to prove additivity), so F is an automorphism on $\mathbb{F}_q$ that fixes $\mathbb{F}_p$, thus is an element of $Gal(\mathbb{F}_q/\mathbb{F}_p)$. Finally, F has order $r$, since if it had order $s < r$, we would have $x^{p^s} = x$, for all $x \in \mathbb{F}_q$. Obviously we also have $x^q = x$, for all $x \in \mathbb{F}_q$. But then $X^{p^s} - X$ would have $q > p^s$ roots. So F has order $r = \left[\mathbb{F}_q : \mathbb{F}_p\right] = |Gal(\mathbb{F}_q/\mathbb{F}_p)|$. We have shown the following:

**Proposition 2.** *Let* $q = p^r$ *and* $F : \mathbb{F}_q \to \mathbb{F}_q, a \mapsto a^p$. *Then* $F$ *is an automorphism and generates* $Gal(\mathbb{F}_q/\mathbb{F}_p)$.

We can extend this notion to the case when the ground field has order a prime power. If $|K|$ has order $p^r$ and $L$ is a finite extension of $K$ of order $p^s$, where $r|s$, then the automorphism on $L$ given by

$$a \mapsto a^{p^r}$$

fixes the field $K$, and has order $s/r$. Since $Gal(\mathbb{F}_{p^s}/\mathbb{F}_{p^r})$ has order $s/r$ and is cyclic (since it is a subgroup of $Gal(\mathbb{F}_{p^s}/\mathbb{F}_p)$), the Frobenius automorphism of $L/K$ in this case again generates the Galois group.
We now begin to explore the nature of Frobenius automorphisms with regard to $Gal(\mathcal{O}_L/\mathfrak{q}\big/\mathcal{O}_K/\mathfrak{p})$: set $Nm(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$. Since $\mathcal{O}_K/\mathfrak{p}$ is finite, its order

is a power of $p$, where $p$ is the unique prime lying in $\mathbb{Z} \cap \mathfrak{p}$. Then there exists a unique automorphism on $\mathcal{O}_L/\mathfrak{q}$ given by

$$a \mapsto a^{Nm(\mathfrak{p})}$$

that fixes $\mathcal{O}_K/\mathfrak{p}$ and generates $Gal(\mathcal{O}_L/\mathfrak{q} \big/ \mathcal{O}_K/\mathfrak{p})$. Using the notation we developed above, there exists $\bar{\sigma} \in \bar{G} : \langle \bar{\sigma} \rangle = \bar{G}$. Then, using the isomorphism $D_{\mathfrak{q}} \big/ I_{\mathfrak{q}} \xrightarrow{\sim} \bar{G}$, there exists a coset of elements, $\sigma I_{\mathfrak{q}}$, that map to $\bar{\sigma}$, for some $\sigma \in D_{\mathfrak{q}}$. We can now reformulate the automorphism as

$$\sigma(a) \equiv a^{Nm(\mathfrak{p})} \bmod \mathfrak{q}, \text{ for } a \in \mathcal{O}_L. \tag{5}$$

A representative of this coset is called a *Frobenius element* of $G$, and denoted $Frob_{\mathfrak{q}}$. If $\mathfrak{p}$ is unramified, $e = 1$, and so the inertia group is trivial; then the coset of Frobenius elements consists of one unique element. In the unramified case, let $\big((L/K), \mathfrak{q}\big)$ denote the unique element in $G$ satisfying (5). Then $\big((L/K), \mathfrak{q}\big)$ is called the *Artin symbol.*

**Proposition 3.** *Let $\sigma \in G$ and $\mathfrak{p}$ be unramified. Then $Frob_{\sigma(\mathfrak{q})} = \sigma Frob_{\mathfrak{q}} \sigma^{-1}$.*

*Proof.*

$$\begin{aligned} Frob_{\mathfrak{q}}(a) &\equiv a^{Nm(\mathfrak{p})} \bmod \mathfrak{q} \Leftrightarrow \\ \sigma Frob_{\mathfrak{q}}(a) &\equiv \sigma(a)^{Nm(\mathfrak{p})} \bmod \sigma(\mathfrak{q}) \Leftrightarrow \\ \sigma Frob_{\mathfrak{q}}(\sigma^{-1}(a)) &\equiv \sigma(\sigma^{-1}(a))^{Nm(\mathfrak{p})} \bmod \sigma(\mathfrak{q}) \Leftrightarrow \\ \sigma Frob_{\mathfrak{q}} \sigma^{-1}(a) &\equiv a^{Nm(\mathfrak{p})} \bmod \sigma(\mathfrak{q}) \end{aligned}$$

By definition, we also have $Frob_{\sigma(\mathfrak{q})}(a) \equiv a^{Nm(\mathfrak{p})} \bmod \sigma(\mathfrak{q})$. Since $\mathfrak{p}$ is unramified, $D_{\mathfrak{q}} \cong \bar{G}$ and the Frobenius element is unique; so we must have $Frob_{\sigma(\mathfrak{q})} = \sigma Frob_{\mathfrak{q}} \sigma^{-1}$. □

Thus for unramified primes, the Frobenius elements are all conjugate to one another. If $G$ is abelian, the conjugacy class has size 1 and consists of a single element. We will denote this element $Frob_{\mathfrak{p}}$. In the general case, note that if $\mathfrak{p}$ is unramified, and $\mathfrak{q}_i$ are the primes lying above $\mathfrak{p}$ indexed by $i$, then the Artin symbols $\big((L/K), \mathfrak{q}_{\mathrm{i}}\big)$ form a conjugacy class in $G$. We will denote this class by $\big((L/K), \mathfrak{p}\big)$.

### 1.1.2 Cebotarev's Density Theorem

We will need Cebotarev's Density Theorem in order to better understand the conjugacy class of Frobenius elements; in particular, their density in the Galois group follows from Cebotarev's result. To begin working towards stating the result, we will let $K$ be a number field, and $\mathcal{P}_K$ the set of finite primes of $\mathcal{O}_K$. Set $\mathcal{S}$ to be a subset of $\mathcal{P}_K$. Then we define the *Dirichlet density* of $\mathcal{S}$ as

$$\delta(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} Nm(\mathfrak{p})^{-s}}{-log(s-1)}.$$

The most relevant property of Dirichlet density for us is that a finite set has zero density; thus, if a set has positive density, it must be infinite in size. We will now state Cebotarev's result:

**Theorem 1.** *Let $L/K$ be Galois and $C_\sigma$ denote the conjugacy class of $\sigma \in G$. Consider the set $\mathcal{S} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p}$ is unramified in $L$ and $\big((L/K), \mathfrak{p}\big) = C_\sigma\}$. Then $\delta(\mathcal{S}) = |C_\sigma|\big/|G| = |C_\sigma|\big/[L : K]$*

*Proof.* See [**janusz**]. □

## 1.2 Modular Forms

This section relies on [**kurinczuk**].

Let $SL_2(\mathbb{Z})$ act on the upper half of the complex plane, $\mathbb{H}$, as linear fractional transformations, i.e. for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $z \in \mathbb{H}$, $\gamma \cdot z = \frac{az+b}{cz+d}$.

**Definition 5.** A modular form of weight $k$ and level 1 is a function

$$f : \mathbb{H} \to \mathbb{C}$$

that is holomorphic on $\mathbb{H} \cup \{\infty\}$ and satisfies the modular transformation law:

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

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

**Definition 6.** Set $f|_{k,\gamma}(z) = det(\gamma)^{\frac{k}{2}}(cz+d)^{-k}f(\gamma \cdot z)$. Define

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

. This is a subgroup of $SL_2(\mathbb{Z})$ and contains

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

with finite index; thus it is a *congruence subgroup*. We say a holomorphic function $f$ is a modular form of weight $k$ on $\Gamma_0(N)$ if $f|_{k,\gamma}(z) = f$ for all $\gamma \in \Gamma_0(N)$, and it is holomorphic at the cusps of $\Gamma_0(N)$, i.e. at the orbits of $\Gamma_0(N)$ on $\mathbb{Q} \cup \infty$.

Note that by plugging in $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ one can deduce that there are no modular forms of odd weight, negative weight, or weight equal to 2. We define the Eisenstein series of weight $k$ to be

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

and the normalised Eisenstein series of weight k to be

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

where $B_k$ denotes the $k$th Bernoulli number, defined by the following expression:

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

In particular, we have

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

and

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

Any modular form of weight $k$ can be written as a homogeneous polynomial in $E_4$ and $E_6$, where for any given term ${E_4}^a {E_6}^b$ we have $4a + 6b = k$. We will denote $E_4$ and $E_6$ by $Q$ and $R$, respectively.
If $E_2$ does not quite satisfy the modular transformation rule, instead obeying

$$E_2(\frac{-1}{z}) = z^2 E_2(z) + \frac{12z}{2i\pi} \tag{6}$$

We will later see that its behaviour changes modulo $p$, and we will denote $E_2$ by $P$.

# 2 Modular Forms Reduced Mod $p$

This section follows the results of [**serre**] and [**swinnerton-dyer**], with a little help from [**lang2**].

**Definition 7.** A modular form

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

is $p$-integral if the $p$-adic valuation $v_p$ is greater than or equal to zero when evaluated at the coefficients $a_n$ for all n $\geq$ 0, i.e. $v_p(a_n) \geq 0$ for all n $\geq$ 0.

**Note**: This is equivalent to saying that the denominators of the coefficients are not divisible by $p$. Thus we can think of $p$-integral modular forms as being modular forms with coefficients in the ring of rational numbers with denominators coprime to $p$. Denote this ring by $\sigma$.

**Definition 8.** Let $f(z)$ be a $p$-integral modular form of weight $k$. Write

$$\tilde{f}(z) = \sum_{n=0}^{\infty} \tilde{a}_n q^n$$

for the reduction of $f(z)$ modulo $p$. Denote by $M_k$ the $\sigma$-module of $p$-integral modular forms of weight $k$, and by $\tilde{M_k}$ the vector space over $\mathbb{F}_p$ of $\tilde{f}$, for $f$ in $M_k$. The $\mathbb{F}_p$-algebra of modular forms mod $p$ is denoted $\tilde{M}$, and is the direct sum of the $\tilde{M_k}$.

## 2.1 Derivation on the Space of Modular Forms

**Definition 9.** If

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

is a $p$-integral modular form of weight $k$, let

$$\theta f = q\frac{df}{dq} = \sum_{n=0}^{\infty} n a_n q^n$$

Set $\partial f = 12\theta f - kPf$.

**Theorem 2.** (i) *Let $g$ and $h$ be modular forms of weights $m$ and $n$, respectively. Then $\partial$ satisfies $\partial(g \cdot h) = h \cdot \partial g + g \cdot \partial h$.*

(ii) *If $f$ is a $p$-integral modular form of weight $k$, $\partial f$ is a modular form of weight $k+2$.*

*Proof.* (i) $\theta(g \cdot h) = q \cdot \frac{d}{dq}(g \cdot h) = q \cdot (g \cdot \frac{d}{dq}h + h \cdot \frac{d}{dq}g) = g \cdot \theta h + h \cdot \theta g$. Then

$$\begin{aligned} \partial(g \cdot h) &= 12\theta(g \cdot h) - (m+n)P(g \cdot h) \\ &= 12g \cdot \theta(h) + 12h \cdot \theta(g) - mPgh - nPgh \\ &= g \cdot (12\theta(h) - nPh) + h \cdot (12\theta(g) - mPg) \\ &= g \cdot \partial h + h \cdot \partial g, \end{aligned}$$

as required.

(ii) Recall $P$ satisfies $P(\frac{-1}{z}) = z^2 P(z) + \frac{12z}{2i\pi}$. We will use this together with

$$f(\frac{-1}{z}) = z^k f(z) \tag{7}$$

to prove the result. Differentiating the left hand side of (7) with respect to z, we get $\frac{d}{dz} f(\frac{-1}{z}) = \frac{1}{z^2} f'(\frac{-1}{z})$. Differentiating the right hand side, we obtain $\frac{1}{z^2} f'(\frac{-1}{z}) = kz^{k-1} f(z) + z^k f'(z)$, and so $f'(\frac{-1}{z}) =$

$kz^{k+1}f(z) + z^{k+2}f'(z)$. Thus

$$\begin{aligned}\partial f(\frac{-1}{z}) &= 12\theta f(\frac{-1}{z}) - kP(\frac{-1}{z})f(\frac{-1}{z}) = \frac{12}{2i\pi}\frac{d}{dz}f(\frac{-1}{z}) - kP(\frac{-1}{z})f(\frac{-1}{z})\\ &= \frac{12}{2i\pi}(kz^{k+1}f(z) + z^{k+2}f'(z)) - k(z^2P(z) + \frac{12z}{2i\pi})z^kf(z)\\ &= \frac{12}{2i\pi}z^{k+2}f'(z)) - kz^{k+2}P(z)f(z)\\ &= z^{k+2}(12\theta f(z) - kP(z)f(z))\\ &= z^{k+2}\partial f(z).\end{aligned}$$

□

**Corollary 2.** *We have*

$$\partial Q = -4R, \tag{8}$$

$$\partial R = -6Q^2, \tag{9}$$

$$\partial\Delta = 0. \tag{10}$$

Before we prove this, we need a lemma:

**Lemma 2.** *We have*

$$\theta P = \frac{1}{12}(P^2 - Q) \tag{11}$$

$$\theta Q = \frac{1}{3}(PQ - R) \tag{12}$$

$$\theta R = \frac{1}{2}(PR - Q^2) \tag{13}$$

*Proof.* We show $\theta P - \frac{1}{12}P^2$ is a modular form of weight 4, and we then compare constant terms. Recall $P$ satisfies (6). Differentiating both sides of this, we obtain

$$P'(\frac{-1}{z}) = 2z^3P(z) + z^4P'(z) + \frac{12z^2}{2i\pi}$$

Using this, we find

$$\begin{aligned}\theta P(\frac{-1}{z}) - \frac{1}{12}P^2(\frac{-1}{z}) &= \frac{1}{2i\pi}\frac{d}{dz}P(\frac{-1}{z}) - \frac{1}{12}(z^2P(z) + \frac{12z}{2i\pi})^2 \\ &= \frac{2z^3}{2i\pi}P(z) + \frac{z^4}{2i\pi}P'(z) - \frac{12z^2}{4\pi^2} - \frac{z^4}{12}P^2(z) \\ &\quad - \frac{2z^3}{2i\pi}P(z) + \frac{12z^2}{4\pi^2} \\ &= z^4\big(\theta P(z) - \frac{1}{12}P^2(z)\big),\end{aligned}$$

so is modular of weight 4. The space of modular forms of weight 4 is one dimensional and spanned by Q, so $\theta P - \frac{1}{12}P^2$ is a scalar multiple of Q, with the scalar determined by the constant terms. $\theta P$ is a cusp form and so has zero constant term, and the constant terms of $P^2$ and Q are both 1, and the result follows.
We know that $\partial Q$ is a modular form of weight 6 and that $\partial Q = 12\theta Q - 4PQ$, so in order to prove (12) we show that the constant terms of $12\theta Q - 4PQ$ and $-4R$ are identical. The constant term of $R$ is 1. $\theta Q$ is a cusp form and so has zero constant term, and the constant term of $PQ$ is 1. As the space of modular forms of weight 6 is spanned by $R$, we obtain the result.

Similarly, to show (13) note that $\partial R = 12\theta R - 6PR$ has weight 8. Observe that $\theta R$ is a cusp form, $PR$ has constant term 1, and that $Q^2$ has constant term 1. Thus $12\theta R - 6PR$ and $Q^2$ are both modular forms of weight 8 with identical constant terms, so the result follows. □

*Proof of Corollary 2.* (8) and (9) follow directly from (12) and (13), and the definition of $\partial f$.

$\theta\Delta$ is a modular form of weight 14 with constant term 0. As $\Delta$ is a cusp form, $P\Delta$ is also a cusp form (of weight 14) and hence also has zero constant term. Hence $\theta\Delta = P\Delta$. Finally, $\partial\Delta = 12\theta\Delta - 12P\Delta = 12(\theta\Delta - P\Delta) = 0$, as required. □

Grade the space of modular forms by weight. Recall there is an isomorphism of graded rings from the space of modular forms to the space of homogeneous polynomials $\mathbb{C}[X, Y]$, where Q maps to X and R maps to Y. The corresponding homogeneous polynomial to $f \in M_k$ will be denoted by $\Phi(X, Y) \in \sigma[X, Y]$. Then $\tilde{\Phi}(X, Y)$ is the polynomial in $\mathbb{F}_p[X, Y]$ obtained by reducing the coefficients of $\Phi$ modulo $p$, and the corresponding polynomial to $\tilde{f} \in \tilde{M}_k$ is $\tilde{\Phi}(\tilde{X}, \tilde{Y}) \in \mathbb{F}_p[[q]]$. In the context of these polynomials, we will use X and Y interchangeably with Q and R, respectively.

Thus in order to determine the structure of $\tilde{\boldsymbol{M}}$, we must determine the kernel of the map

$$\mathbb{F}_p[Q, R] \to \tilde{M}$$

.

We will denote this kernel by **a**.

The following result will prove highly useful; a proof can be found on pages 384-386 of [**borevich**]:

**Lemma 3.** *(Von Staudt) Let $B_n$ denote the Bernoulli numbers, and p > 3. Then:*

(i) *If $p - 1 | 2\nu$, then $pB_{2\nu} \equiv -1$ mod p.*

(ii) *If $p - 1 \nmid 2\nu$, $\frac{B_{2\nu}}{2\nu}$ is p-integral, and $\frac{B_{2\nu}}{2\nu} \equiv \frac{B_{2\nu \ mod \ p-1}}{2\nu \ mod \ p-1}$ mod p.*

Until stated otherwise, the following results are all valid for $p > 3$.

Let $A$ and $B$ be the homogeneous polynomials such that

$$A(Q, R) = E_{p-1} \text{ and } B(Q, R) = E_{p+1}$$

**Lemma 4.** *A and B are polynomials in $\sigma[Q, R]$.*

*Proof.* Recall

$$E_{p-1}(z) = 1 - \frac{2p-2}{B_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-2}(n)\, q^n,$$

With $2\nu = p - 1$, we can apply Lemma 3 (i) to deduce that $p$ divides only the denominator of $B_{p-1}$; thus $\frac{2p-2}{B_{p-1}}$ is well defined modulo $p$, and $E_{p-1} \in \sigma[Q, R]$.

Using Lemma 3 (ii), we obtain $\frac{B_{p+1}}{p+1} \equiv \frac{B_2}{2}$ mod $p$. $B_2 = \frac{1}{6}$, so $\frac{B_{p+1}}{p+1} \equiv \frac{1}{12}$ mod $p$. As $p \neq 2$ or 3, $\frac{2p+2}{B_{p+1}}$ is well defined modulo $p$, and so $E_{p+1} \in \sigma[Q, R]$. □

**Lemma 5.** (i) *$\tilde{A}(\tilde{Q}, \tilde{R}) = 1$ and $\tilde{B}(\tilde{Q}, \tilde{R}) = \tilde{P}$.*

(ii) *$\partial\tilde{A} = \tilde{B}$ and $\partial\tilde{B} = -Q\tilde{A}$.*

(iii) *$\tilde{A}$ has no repeated factors and is coprime to $\tilde{B}$.*

*Proof.* (i) Note that

$$\begin{aligned} E_{p-1}(z) &= 1 - \frac{2p-2}{B_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-2}(n)\ q^n \\ &\equiv 1 \bmod p, \end{aligned}$$

since $p$ divides the denominator of $B_{p-1}$ (by Lemma 3). Thus $\tilde{A}(\tilde{Q}, \tilde{R}) = \tilde{E}_{p-1} \equiv 1 \bmod p$. For the second result, note that Fermat-Euler implies that

$$\sigma_p(n) = \sum_{d|n} d^p \equiv \sum_{d|n} d \bmod p,$$

i.e. $\sigma_p(n) \equiv \sigma_1(n) \bmod p$. Recall also (from the proof of Lemma 3) that $\frac{B_{p+1}}{p+1} \equiv \frac{1}{12} \bmod p$. Thus

$$\begin{aligned} E_{p+1} &= 1 - 2\ \frac{p+1}{B_{p+1}} \sum_{n=1}^{\infty} \sigma_p(n)\ q^n \\ &\equiv 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n)\ q^n \bmod p \\ &\equiv P \bmod p, \end{aligned}$$

and so $\tilde{B}(\tilde{Q}, \tilde{R}) \equiv \tilde{E}_{p+1} \equiv \tilde{P}$.

(ii) By (i), $\theta \tilde{A}(\tilde{Q}, \tilde{R}) = 0$, so we obtain

$$\begin{aligned} \partial \tilde{A}(\tilde{Q}, \tilde{R}) &= 12\theta \tilde{A}(\tilde{Q}, \tilde{R}) - (p-1)\tilde{P}\tilde{A}(\tilde{Q}, \tilde{R}) \\ &= \tilde{P}\tilde{A}(\tilde{Q}, \tilde{R}) \\ &= \tilde{P} \\ &= \tilde{B}(\tilde{Q}, \tilde{R}) \end{aligned}$$

This means the $q$-expansion of $\partial A - B$ has coefficients divisible by $p$. Of course, $\partial A - B$ is a modular form of weight $p+1$, and so $\partial A - B \in$ p$\sigma[Q, R]$ and $\partial \tilde{A} = \tilde{B}$.

For the second result, observe

$$\begin{aligned}
\partial \tilde{B}(\tilde{Q}, \tilde{R}) &= 12\theta \tilde{B}(\tilde{Q}, \tilde{R}) - (p+1)\tilde{P}\tilde{B}(\tilde{Q}, \tilde{R}) \\
&= 12\theta \tilde{B}(\tilde{Q}, \tilde{R}) - \tilde{P}\tilde{B}(\tilde{Q}, \tilde{R}) \\
&= 12\theta \tilde{P} - \tilde{P}^2 \\
&= -\tilde{Q},
\end{aligned}$$

by (11). Similarly to before, this means that $p$ divides the coefficients of the $q$-expansion of $\partial B + QA$, which is a modular form (of weight $p+3$) and so has coefficients in $p\sigma[Q, R]$. Thus $\partial \tilde{B} = -Q\tilde{A}$.

(iii)

□

Note: (i) means that $P$ becomes a modular form of weight $p+1$ modulo $p$.

**Theorem 3.** *The ideal* $\mathbf{a}$ *is equal to the principal ideal generated by* $\tilde{A} - 1$.

*Proof.* Recall $\mathbf{a}$ is the kernel of

$$\mathbb{F}_p[Q, R] \to \tilde{M},$$

so can also be thought of as the kernel of

$$\mathbb{F}_p[Q, R] \to \mathbb{F}_p[[q]],$$

given by replacing Q and R with $\tilde{Q}$ and $\tilde{R}$ respectively, since any modular form has a power series expansion in $q$. As in Lemma 4, $\tilde{A}(\tilde{Q}, \tilde{R}) = 1$, hence $\tilde{A} - 1 \in \mathbf{a}$. Note $\mathbf{a}$ is prime since $\mathbb{F}_p[[q]]$ is an integral domain. Let $\mathfrak{m}$ be a maximal ideal containing $\mathbf{a}$. We now have the chain of ideals

$$0 \subseteq (\tilde{A} - 1) \subseteq \mathbf{a} \subseteq \mathfrak{m} \tag{14}$$

If $(\tilde{A}-1)$ is a prime ideal, we have obtained a chain of prime ideals of length three. They cannot all be prime, as this contradicts the Krull dimension of $\mathbb{F}_p[X, Y]$, which is two. Furthermore, $\mathbf{a}$ is not maximal, since the image is $\mathbb{F}_p[\tilde{Q}, \tilde{R}]$, which is not a field. To complete the proof, we prove that $(\tilde{A} - 1)$ is prime (equivalent to $\tilde{A}-1$ being irreducible) which will imply $(\tilde{A}-1) = \mathbf{a}$.
□

## 2.2 Filtration

Let $\tilde{f}$ be a graded element in $\tilde{M}$, i.e. a linear combination of elements of various $\tilde{M}_k$ where the $k$ are all congruent modulo $p-1$ (c.f. Corollary 3). We can multiply the summands by appropriate powers of $\tilde{A}$ in order to get every summand in the same $\tilde{M}_k$, so that $\tilde{f}$ belongs to a single $\tilde{M}_k$.

**Definition 10.** Let $f$ be a graded element of $\tilde{M}$. Define the filtration of $\tilde{f}$ to be the lowest $k$ such that $\tilde{f} \in \tilde{M}_k$. We denote the filtration by $w(\tilde{f})$.

Note: We can equivalently say that the filtration of a $p$-integral modular form $f$ is the lowest weight $k$ such that there exists a modular form $g$ for which we have $f \equiv g \bmod p$.

**Lemma 6.**

(i) *If $f$ is a $p$-integral modular form of weight $k$, with $f = \phi(Q, R)$ for $\phi \in \sigma[Q, R]$ and $f \not\equiv 0$ mod $p$, the $w(\tilde{f}) < k \iff \tilde{A}|\tilde{\phi}$.*

(ii) *If $\tilde{f}$ is graded in $\tilde{M}$, we have $w(\theta \tilde{f}) \leq w(\tilde{f}) + p + 1$, with equality if and only if $w(\tilde{f}) \not\equiv 0$ mod $p$.*

*Proof.* (i) Clearly if $\tilde{A} \nmid \tilde{\phi}$, then $w(\tilde{f})$ cannot be less than $k$, since in order to obtain the isobaric polynomial of degree $k$, $\phi$, we have multiplied various summands by $\tilde{A}$ to get every summand into the same $\tilde{M}_k$. Thus, if there exists a summand not divisible by $\tilde{A}$, the filtration of $\tilde{f}$ cannot be less than the degree of that summand, which is at least $k$.
Conversely, let $\tilde{A}|\tilde{\phi}$, and suppose $w(\tilde{f}) = k$. Then we must have $\tilde{\phi} = \tilde{A}\tilde{\psi}$, for some isobaric polynomial $\psi$ corresponding to some modular form $g$ of weight less than $k$. This implies

$$\tilde{f} = \tilde{\phi}(\tilde{Q}, \tilde{R}) = \tilde{A}(\tilde{Q}, \tilde{R})\tilde{\psi}(\tilde{Q}, \tilde{R}) = \tilde{\psi}(\tilde{Q}, \tilde{R}) = \tilde{g},$$

which contradicts $w(\tilde{f}) = k$.

(ii) Let $w(f) = k$ and $f$ be as in (i). We have $\partial\tilde{\phi}(\tilde{Q}, \tilde{R}) = 12\theta\tilde{f} - k\tilde{P}\tilde{f}$, which is equivalent to

$$12\theta\tilde{f} = \tilde{A}(\tilde{Q}, \tilde{R})\partial\tilde{\phi}(\tilde{Q}, \tilde{R}) + k\tilde{B}(\tilde{Q}, \tilde{R})\tilde{f},$$

using the facts that $\tilde{A}(\tilde{Q}, \tilde{R}) = 1$ and $\tilde{B}(\tilde{Q}, \tilde{R}) = \tilde{P}$. Hence $12\theta\tilde{f}$ is the image of $\tilde{A}\partial\tilde{\phi} + k\tilde{B}\tilde{\phi}$ in $\tilde{M}$. Observe that both summands have filtration less than or equal to $w(\tilde{f}) + p + 1$: $\tilde{A}$ has filtration $p-1$ and $\partial\tilde{\phi}$ filtration $w(\tilde{f}) + 2$, and $\tilde{B}$ filtration $p+1$ and $f$ filtration $w(\tilde{f})$. Since $w(\tilde{f}) = k$, we have by (i) that $\tilde{A} \nmid \tilde{\phi}$. Furthermore, Lemma 5 implies that $\tilde{A} \nmid \tilde{B}$. Combining these two results, we find that $w(\theta\tilde{f}) = w(\tilde{f}) + p + 1$ if and only if $\tilde{A} \nmid (\tilde{A}\partial\tilde{\phi} + k\tilde{B}\tilde{\phi})$ if and only if $p \nmid k$, i.e. if and only if $w(\tilde{f}) \not\equiv 0 \bmod p$.

□

**Corollary 3.** *(Kummer's Congruence) Let $f$ and $g$ be $p$-integral modular forms of weights $k$ and $l$, respectively. If $f \equiv g \bmod p$ and $f \not\equiv 0 \bmod p$, then $k \equiv l \bmod (p-1)$.*

*Proof.* Suppose $k' < k$ and $\phi$ and $\psi$ are the isobaric polynomials corresponding to $f$ and $g$ respectively. Then $w(\tilde{f}) < k$, so by the above lemma $\tilde{A} \mid \tilde{\phi}$. If $w(\tilde{f}) = k'$, then comparing degrees we get $k = k' + m(p-1)$, and the result is clear. If $w(f) < k'$, say $w(f) = k''$, then $\tilde{A} \mid \tilde{\psi}$ also and $k = k'' + m_1(p-1) + m_2(p-1)$, and again we are done, where $m, m_1,$ and $m_2$ are integers. □

This result allows us to define $\tilde{M}^\alpha = \bigoplus_{k\in[\alpha]} \tilde{M}_k$, where $[\alpha]$ is the class of $\alpha$ mod $p-1$; since $\tilde{M}_k \subset \tilde{M}_{k+p-1} \subset \tilde{M}_{k+2(p-1)} \subset ...$, all elements of $\tilde{M}^\alpha$ have weights congruent to $\alpha$ mod $p-1$. We now deal with the cases of $p = 2$ and $p = 3$.

**Theorem 4.** *If $p = 2$ or $p = 3$, we have*

(i) $\tilde{P} = \tilde{Q} = \tilde{R} = 1$.

(ii) $\tilde{M} = \mathbb{F}_p[\tilde{\Delta}]$.

(iii) $\partial\tilde{M} = 0$.

*Proof.* (i) 24, 240, and 504 are all divisible by both 2 and 3, and the $q$-expansions of $P$, $Q$, and $R$ all begin with 1, and the result follows.

(ii) $\Delta$ can be written

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

and using the binomial theorem we can see that $\tilde{\Delta} = q$.

(iii) As in the proof of Corollary 2, $\partial\Delta = 0$. Part (ii) of this theorem implies the result.

□

## 2.3 Values of the Zeta Function

We say a field extension $K$ of $\mathbb{Q}$ is *totally real* if every embedding of $K$ into $\mathbb{C}$ is real. In the following, $K$ will be an algebraic, totally real number field of degree $r$. Recall the Dedekind zeta-function, $\zeta_K(s) = \sum_{I\subset\mathcal{O}_K}\frac{1}{(Nm(I))^s}$, where $s\in\mathbb{C}$ and $Re(s) > 1$. $\zeta_k(1-2m)$ is always a rational number, for $m$ an even positive integer - a proof of this can be found in [**zagier**]. In the following, we explore congruences involving $\zeta_k(1-2m)$, for $p > 3$.
Let $\mathbf{d}$ be the different ideal of $K$ and $Tr$ the trace map, and consider the series

$$f_m = 2^{-r}\zeta_K(1-m) + \sum_{\mathbf{a}}\sum_{\nu\in\mathbf{d}^{-1}\mathbf{a}} Nm(\mathbf{a})^{m-1}q^{Tr(\nu)},$$

where $\sigma(\nu) > 0$ for all embeddings $\sigma$ of $K$ into $\mathbb{R}$. Siegel proved in [**siegel**] that $f_m$ is a modular form of weight $k = rm$. Write $f_m$ in the form $f_m = a_m(0) + \sum_{n=1}^{\infty} a_m(n)q^n$. Clearly $2^r a_m(0) = \zeta_K(1-m)$ and the $a_m(n)$ are integers for $n \geq 1$. In addition, if $m \equiv m'$ mod $p$, we must have $a_m(n) \equiv a_{m'}(n)$ mod $p$. The key results of this section follow from the above three facts and the following three propositions:

**Proposition (i).** If $k$ is divisible by $p-1$, the formal series in $\mathbb{F}_p[q]$ given by $\varphi = \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$ is not a modular form of weight $k$.
**Note**: this is equivalent to saying $\varphi \notin \tilde{M}_k$.

*Proof.* By Fermat-Euler, we obtain $\sigma_{k-1}(n) \equiv \sigma_{p-2}(n)$ mod $p$. From this we get the congruence $\sigma_{p-2}(n) - \sigma_{p-2}(\frac{n}{p}) \equiv n^{p-2}\sigma_1(n)$ mod $p$ (where $\sigma_{p-2}(\frac{n}{p})$ is set to 0 if $p \nmid n$). This is equivalent to $\varphi - \varphi^p \equiv \theta^{p-2}\big(\sum_{n=1}^{\infty}\sigma_1(n)q^n\big)$ mod $p$. It is clear that this implies $\varphi - \varphi^p = \frac{-1}{24}\theta^{p-2}\tilde{P} = \frac{-1}{24}\theta^{p-2}\tilde{E}_{p+1}$. Suppose $\varphi$ is modular of weight divisible by $p-1$ and of filtration $h$. We can write $\varphi$ as an homogeneous polynomial of degree $h$, $\Phi(\tilde{Q},\tilde{R})$, where $A \nmid \Phi$. Since $A$ has only linear factors, the filtrations of $\varphi^p$ and $\varphi - \varphi^p$ must be $ph$. In addition, the filtration of $\theta^{p-2}\tilde{E}_{p+1}$ is $p+1+(p-2)(p+1) = p^2-1$. This is a contradiction, since we cannot have $ph = p^2-1$. □

**Proposition (ii).** Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$ be a modular form of weight $k$ with $p$-integral coefficients for $n > 0$. Then

(a) If $k \not\equiv 0 \bmod p-1, a_0$ is $p$-integral.

(b) If $k \equiv 0 \bmod p-1$, then $v_p(a_0) \geq -v_p(k) - 1$.

*Proof.* For (a), suppose that $a_0$ is not $p$-integral with $v_p(a_0) = -s$, for some positive integer $s$. Then $p^s f$ has $p$-integral coefficients. Reducing modulo $p$, we find that the constant term is non-zero, so the reduction of $p^s f$ is a constant function, and has weight 0. Since $f$ has weight $k$, we must have (by Kummer) that $k \equiv 0 \bmod p-1$ - but this is a contradiction. For (b), suppose that $s > s' = v_p(k) + 1$, and write $G_k = c + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$. By Lemma (3), $v_p(c) = -1 - v_p(2k) = -s'$. Thus $v_p(\frac{c}{a_0}) \geq 1$. Setting $g = G_k - \frac{c}{a_0} f$, we find that $g$ is a cusp form with p-integral coefficients, with

$$g \equiv \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \bmod p.$$

By Proposition (i), this is not a modular form of weight $k$. □

**Proposition (iii).** Let

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \text{ and } f'(z) = \sum_{n=0}^{\infty} a'_n q^n$$

both be modular forms of weights $k$ and $k'$ respectively, with $p$-integral coefficients for $n \geq 0$. Let $k \equiv k' \bmod p-1$ with neither weight divisible by $p-1$, and $a_n \equiv a'_n \bmod p$ for $n \geq 1$. Then $a_0 \equiv a'_0 \bmod p$.

*Proof.* Suppose that $k = k'$, and set $g = (f - f')/p$. For $n \geq 1$, the coefficients of $g$ are p-integral. By Proposition (ii), we must have $(a_0 - a'_0)/p$ $p$-integral, so $a_0 \equiv a'_0 \bmod p$. For the general case, suppose that $k' = k + s(p-1)$ for some $s \geq 0$, and set $f'' = f \cdot E_{p-1}^s$. We have $f'' \equiv f \bmod p$, and $f'$ and $f''$ have the same weight - so we have returned to the first case. □

We can now prove two theorems concerning the zeta function:

**Theorem 5.**

(i) *If $rm \not\equiv 0$ mod $p-1$, then $\zeta_K(1-m)$ is $p$-integral.*

(ii) *If $rm \equiv 0$ mod $p-1$, then $v_p(\zeta_k(1-m)) \geq -1 - v_p(rm)$.*

*Proof.* This follows directly from Proposition (ii). □

**Theorem 6.** *If $m \equiv m'$ mod $p-1$ and $rm \not\equiv 0$ mod $p-1$, we have $\zeta_k(1-m) \equiv \zeta_k(1-m')$ mod $p$.*

*Proof.* This follows from Proposition (iii), and the stated facts that the coefficients are integers and $m \equiv m'$ mod $p$ implies $a_m(n) \equiv a_{m'}(n)$ mod $p$. □

# 3 P-adic Modular Forms

In this section we will develop a theory of modular forms modulo higher powers of $p$; these objects will be known as $p$-adic modular forms, and will culminate in the construction of the p-adic zeta function. The results will heavily rely on [**serre2**].

## 3.1 Defining p-adic Modular Forms

Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$ have coefficients in $\mathbb{Q}_p$ and define $v_p(f) = \inf\{v_p(a_n)\}$ for $n \geq 0$. Clearly $v_p(f) \geq 0$ implies $f \in \mathbb{Z}_p[[q]]$. If $v_p(f) \geq m$, $f \equiv 0 \bmod p^m$. If $(f_i)$ is a sequence of modular forms in $\mathbb{Q}_p[[q]]$, we will say $f_i$ converges to $f$ if the coefficients of $f_i$ uniformly converge to the corresponding coefficients of $f$, that is $v_p(f - f_i) \to \infty$. For the sake of space, we will focus on results for $p > 2$; know, however, that all of the following results have analogous statements for the $p = 2$ case.

**Definition 11.** A p-adic modular form is a series $f(z) = \sum_{n=0}^{\infty} a_n q^n$ with the $a_n \in \mathbb{Q}_p$, such that there exists a sequence $(f_i)$ of modular forms with rational coefficients, each of weight $k_i$, such that $\lim_{i \to \infty} f_i = f$.

We have defined how a sequence of modular forms can converge to a p-adic modular form, but it remains to be seen what the behaviour of the weights of the $f_i$ is like. In the following, we will see that the $k_i$ converge as expected as $i \to \infty$, but we first need to develop the appropriate framework. Let $m \in \mathbb{Z}_{\geq 1}$ and set $X_m = \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z} = \mathbb{Z}/p^{m-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$. The inverse limit of of this is

$$X = \varprojlim X_m = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \tag{15}$$

**Lemma 7.** *Let $m \in \mathbb{Z}_{\geq 1}$ and $f, f'$ be rational modular forms of weights $k, k'$ respectively. If $f \neq f'$ and $v_p(f - f') \geq v_p(f) + m$, then $k' \equiv k \mod (p-1)p^{m-1}$.*

*Proof.* We begin with the case $m = 1$. Up to multiplying $f$ by a scalar, we can assume that $v_p(f) = 0$, so the assumption of the lemma is equivalent to $v_p(f - f') \geq m$, i.e. $f' \equiv f \mod p^m$. The coefficients of $f$ and $f'$ are p-integral and so $\tilde{f} = \tilde{f}'$. Thus $k \equiv k' \mod p - 1$, as required.
Let $m \geq 2$. Set $h = k' - k$, and note that up to replacing $f'$ by $f' E_{(p-1)p^n}$ for some $n$, we can suppose that $h \geq 4$ (noting that $E_{(p-1)p^n} \equiv 1 \mod p^{n+1}$). Since $p - 1$ divides $h$, $E_h \equiv 1 \mod p$. Set $r = v_p(h) + 1$; we need to show that $r \geq m$. Let $r < m$. Observe $f \cdot E_h - f' = f - f' + f(E_h - 1)$. Now, from the above one can see that $f \cdot E_h - f' \equiv 0 \mod p^r$, and that $p^{-r}(f \cdot E_h - f') \equiv p^{-r} f \cdot (E_h - 1) \mod p$. By Lemma 3, $p^{-r}\frac{2k}{B_k}$ is $p$-integral, so we can write $p^{-r}(E_h - 1) = \lambda\Phi$, with $\Phi = \sum_{n=1}^{\infty} \sigma_{h-1}(n) q^n$ and $\lambda$ a $p$-adic unit. Then the above congruence becomes $f\Phi \equiv g \mod p$, setting $g = \lambda^{-1} p^{-r}(f \cdot E_h - f')$, which is modular of weight $k'$. Recalling that $\tilde{f} \neq 0$ and that $k' \equiv k \mod p$, one can see that $\tilde{\Phi} = \tilde{g}/\tilde{f}$ is an element of the fraction field of $\tilde{M}_0$. As in Proposition (i) we obtain $\Phi - \Phi^p \equiv \Psi$, where $\tilde{\Psi} \in \tilde{M}_0$ and $\Psi \equiv \theta^{h-1}\big(\sum_{n=1}^{\infty} \sigma_1(n) q^n\big)$. When $p \geq 5$, $\tilde{\Psi} = \frac{-1}{24}\theta^{h-1}\tilde{P} = \frac{-1}{24}\theta^{p-2}\tilde{E}_{p+1}$. Since $\tilde{\Phi} - \tilde{\Phi}^p = \tilde{\Psi}$, $\tilde{\Phi}$ is integral over $\tilde{M}_0$, and since $\tilde{M}_0$ is integrally closed, we have $\tilde{\Phi} \in \tilde{M}_0$; but this contradicts Proposition (i), and we are done. □

**Theorem 7.** *Let there be a sequence of rational modular forms $(f_i)$ of weights $(k_i)$: $(f_i) \to f$, $i \to \infty$. Then the $k_i$ have limit $k \in X$, which depends on $f$ but not on the choice of $(f_i)$.*

*Proof.* We have $v_p(f_i - f_j) \to \infty$, and for very large $i$, we have $v_p(f_i) = v_p(f)$. By the above theorem, we must have that for all $m \geq 1$, the image of the $k_i$ in $X_m$ constant; this implies that $(k_i)$ has a limit $k$ in $X$, and the limit is independent of the choice of sequence. □

We call this limit $k$ the weight of $f$, and it is even (i.e. in $2X$). Using this notion of the weight of a p-adic modular form, the previous lemma can be rewritten as follows: if $m \in \mathbb{Z}_{\geq 1}$, and $f, f'$ are two p-adic modular forms of weights $k, k' \in X$, and if $v_p(f - f') \geq v_p(f) + m$, then $k$ and $k'$ have the same image in $X_m$.

**Corollary 4.** *Let $f^{(i)} = \sum_{n \geq 0} a_n^{(i)} q^n$ be a sequence of p-adic modular forms of weight $k^{(i)}$, and suppose that $a_n^{(i)} \to a_n$uniformly in $\mathbb{Q}_p$ for $n \geq 1$, and* *that $k^{(i)} \to k$ in $X \setminus 0$. Then $a^{(0)} \to a_0 \in \mathbb{Q}_p$, and $f = a_0 + a_1 q + a_2 q^2 ...$ is a p-adic modular form of weight $k$.*

*Proof.* Since $k^{(i)} \neq 0$ there exists an $m \in \mathbb{Z}$ such that the $k^{(i)}$ all have the same (non-zero) image in $X_m$. In addition, the condition on the coefficients implies that there exists $t \in \mathbb{Z}$ such that $v_p(a_n^{(i)}) \geq t$ for all $n \geq 1$ and for all $i$. We must have $v_p(a_0^{(i)}) > t - m$ for all $i$: taking $a_0^{(i)}$ as a modular form of weight 0, $v_p(f^{(i)} - a_0^{(i)}) = \inf_{n \geq 1} v_p(a_n^{(i)})$. Since $f^{(i)}$ and $a_0^{(i)}$ have different images in $X_{m+1}$, Theorem 7 implies that $v_p(f^{(i)}) + m + 1 > v_p(f^{(i)} - a_0^{(i)})$, and since $v_p(a_0^{(i)}) \geq v_p(f^{(i)})$, the result is shown. Then $|a_0^{(i)}| \leq p^{-t+m}$ and the closure of the set $\{a_0^{(i)}\}$ is closed and bounded, so the $a_0^{(i)}$ form a relatively compact subset of $\mathbb{Q}_p$. Select a convergent subsequence $(i_j)$ such that $a^{(i_j)} \to a_0 \in \mathbb{Q}_p$. The series $f = \lim f^{(i_j)} = a_0 + a_1 q + a_2 q^2 ...$ is a p-adic modular form of weight $k$. Finally, if $(i'_j)$ is a subsequence such that $a^{(i'_j)} \to a'_0$, we would obtain p-adic modular form $f' = a'_0 + a_1 q + a_2 q^2 + ...$ of weight $k$, and taking the difference $f - f' = a_0 - a'_0$ would be another p-adic modular form of weight $k$; but $a_0 - a'_0$ has weight 0, which is only possible if $a_0 = a'_0$. □

## 3.2 The $p$-adic Eisenstein Series

An important example of a p-adic modular form is the p-adic Eisenstein series:
Let $k \in X$ and $n \in \mathbb{Z}_{\geq 1}$. Define the function

$$\sigma^*_{k-1}(n) = \sum_{d|n,\ (d,p)=1} d^{k-1}.$$

If $k$ is even, choose a sequence of even integers $k_i \geq 4$ which diverges (in the typical sense) to infinity but which converge to $k$ in $X$. Then in $\mathbb{Z}_p$ we have

$$\lim_{i \to \infty} \sigma_{k_i - 1}(n) = \sigma^*_{k-1}(n),$$

because if $p \mid d$, $d^{k_i - 1} \to 0$, since $|k_i| \to \infty$. This convergence is uniform with respect to $n$. We now define the series

$$G_{k_i} = \frac{-B_{k_i}}{2k_i} + \sum_{n=1}^{\infty} \sigma_{k_i - 1}(n) q^n.$$

Since $\frac{-B_{k_i}}{2k_i} = \frac{1}{2}\zeta(1-k_i)$, using Corollary 4 we find, for $k \neq 0$, the limit of the $G_{k_i}$:

$$G_k^* = \frac{1}{2}\lim_{i\to\infty}\zeta(1-k_i) + \sum_{n\geq 1}\sigma_{k-1}^*(n)q^n.$$

Label this constant term $\frac{1}{2}\zeta^*(1-k)$. $G_k^*$ is the *p-adic Eisenstein series of weight $k$*. As in the classical case, we define the *normalized p-adic Eisenstein series of weight $k$* to be

$$E_k^* = 1 + \frac{2}{\zeta^*(1-k)}\sum_{n\geq 1}\sigma_{k-1}^*(n)q^n.$$

We will prove an important theorem, linking $\zeta^*$ with the p-adic zeta function, but first we need to develop the theory of L-functions.

## 3.3 Dirichlet L-functions

This section significantly relies on [**iwasawa1**].

**Definition 12.** A *Dirichlet character to the modulus $n$* is a multiplicative homomorphism $\chi : \mathbb{Z} \to \mathbb{C}$ such that $\chi(a)$ is determined modulo $n$, and for $(a,n) = 1$, we have $\chi(a) \neq 0$.

There is a bijection between such Dirichlet characters and the characters $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$.

**Definition 13.** Let $m$ divide $n$ and $\chi'$ be a Dirichlet character of modulus $m$. Define $\chi$ by

$$\chi(a) = \begin{cases} \chi'(a), & if(a,n) = 1 \\ 0, & if(a,n) > 1 \end{cases}$$

So $\chi$ is a Dirichlet character to the modulus $n$ induced by $\chi'$. If $\chi$ is a Dirichlet character *not* induced by by any character to a lower modulus, $\chi$ is primitive. The conductor of a Dirichlet character to the modulus $n$ is the smallest divisor of $n$ for which there is a Dirichlet character that induces $\chi$. Thus a Dirichlet character is primitive if and only if its modulus equals its conductor; from now on, all characters will be primitive. We denote the trivial character by $\chi^0$; it is the only character of conductor 1.

**Definition 14.** The Dirichlet L-function for $\chi$ is defined

$$L(s,\chi)=\sum_{n\geq 1}\chi(n)n^{-s}.$$

The series converges and is holomorphic when $Re(s)>1$. It has an associated Euler product

$$L(s,\chi)=\prod_{p}(1-\chi(p)p^{-s})^{-1}.$$

When $\chi=\chi^{0}$, $L(s,\chi^{0})=\zeta(s)$, which satisifes the functional equation

$$\Gamma\left(\frac{s}{2}\right)\zeta(s)\pi^{-\frac{s}{2}}=\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)\pi^{-\frac{1-s}{2}}.$$

There is a more general functional equation for Dirichlet L-series, but we will not make use of it.

We next define generalized Bernoulli numbers:

**Definition 15.** Let $\chi$ be a Dirichlet character with conductor $c_{\chi}$ and consider the functions

$$F_{\chi}(t)=\sum_{a=1}^{c_{\chi}}\frac{\chi(a)te^{at}}{e^{c_{\chi}t}-1},\ \text{and}\ F(x,t)=\frac{te^{xt}}{e^{t}-1}.$$

In a similar way to the standard Bernoulli numbers, we can expand these as a power series, to obtain:

$$F_{\chi}(t)=\sum_{n\geq 0}B_{n,\chi}\frac{t^{n}}{n!},\ \text{and}\ F(x,t)=\sum_{n\geq 0}B_{n}(x)\frac{t^{n}}{n!}$$

Then the $B_{n,\chi}$ are the *generalized Bernoulli numbers*, which lie in $\mathbb{Q}(\chi)$, obtained by adding the values $\chi(a)$, where $a\in\mathbb{Z}$, to $\mathbb{Q}$. The $B_{n}(x)$ are called the *Bernoulli polynomials*. To see the link between these and the classical Bernoulli numbers, observe the following, noted in [**arakawa**]:

$$\begin{aligned}\sum_{n\geq 0}B_{n,\chi}\frac{t^{n}}{n!}=\sum_{a=1}^{c_{\chi}}\frac{\chi(a)te^{at}}{e^{c_{\chi}t}-1}&=\sum_{a=1}^{c_{\chi}}\chi(a)\frac{1}{c_{\chi}}\sum_{n\geq 0}B_{n}(a/c_{\chi})\frac{(c_{\chi}t)^{n}}{n!}\\&=\sum_{n\geq 0}\sum_{a=1}^{c_{\chi}}\chi(a)B_{n}(a/c_{\chi})\frac{c_{\chi}^{n-1}t^{n}}{n!}.\end{aligned}$$

We then find that $B_{n,\chi}=\sum_{a=1}^{c_{\chi}}\chi(a)B_{n}(a/c_{\chi})c_{\chi}^{n-1}$; taking the trivial character, which has conductor 1, we see that $B_{n,\chi^{0}}=B_{n}(1)=B_{n}$, for $n>1$.

**Lemma 8.** *Let $n \in \mathbb{Z}_{\geq 1}$. Then $L(1-n, \chi) = \frac{-B_{n,\chi}}{n}$.*

*Proof.* The appendix of [**iwasawa1**] proves that the residue of $z^{-n-1}F_\chi(z)$ at $z = 0$ is $\frac{-L(1-n,\chi)}{\Gamma(n)}$, for all $n \geq 1$. Since $\Gamma(n) = (n-1)!$, the result follows immediately. □

Let $\Omega_p$ be an algebraic closure of $\mathbb{Q}$. Set $D$ to be the subgroup of $\mathbb{Z}_p^\times$ comprising elements of the form $1 + p\mathbb{Z}_p$, and $V$ to be the group of $p - 1th$ roots of unity in $\mathbb{Q}_p$. Then $\mathbb{Z}_p^\times \cong V \times D$ (this follows from the Weierstrass preparation theorem; for more detail see [**koblitz**]). Hence if $a \in \mathbb{Z}_p^\times$, we can write $a = \omega(a) < a >$, where $\omega, < \quad >$ denote projections onto $V$, $D$ respectively. This map $\omega$ satisfies $\omega(a) = \lim_{n\to\infty} a^{p^n}$, and we set $\omega(a) = 0$ if $(a, p) > 1$. Finally, the map $a \mapsto \omega(a)$ defines a Dirichlet character of conductor $p$, known as the *Teichmuller character*.
We are now ready to state a theorem of Kubota and Leopoldt, defining the p-adic zeta function:

**Theorem 8.** *Set $\chi_n = \chi\omega^{-n}$. There exists a p-adic meromorphic function $L_p(s, \chi)$ such that $L_p(s,\chi) = \frac{a_{-1}}{s-1} + \sum_{n=0}^{\infty} a_n(s-1)^n$, where $a_n \in \mathbb{Q}_p(\chi)$ and* $a_{-1} = \begin{cases} 1 - \frac{1}{p}, & if \chi = \chi^0 \\ 0, & if \chi \neq \chi^0. \end{cases}$
*Moreover, for $n \in \mathbb{N}_{\geq 1}$, we have $L_p(1-n, \chi) = -(1 - \chi_n(p)p^{n-1})\frac{B_{n,\chi_n}}{n} = (1 - \chi_n(p)p^{n-1})L(1-n, \chi_n)$.*

*Proof.* See [**iwasawa1**]. □

The following theorem establishes the link between p-adic modular forms and p-adic zeta functions:

**Theorem 9.** *Let $(s, u) \in X$ be odd and not equal to the identity. Then $\zeta^*(s, u) = L_p(s, \omega^{1-u})$.*

*Proof.* Denote by $\zeta'$ the function $(s, u) \mapsto L_p(s, \omega^{1-u})$. Let $\omega_{u,n}$ denote the twisted character $\omega^{1-u}\omega^{-n}$. If $k \in 2\mathbb{Z}_{\geq 2}$, write $1 - k = (s, u)$ and we have $\zeta'(1-k) = L_p(1-k, \omega^{1-u}) = -(1 - \omega_{u,k}(p)p^{k-1})\frac{B_{k,\omega_{u,k}}}{k} = -(1 - \omega^{1-u}\omega^{-k}(p)p^{k-1})\frac{B_{k,\omega_{u,k}}}{k} = -(1 - \omega^0(p)p^{k-1})\frac{B_{k,\omega_{u,k}}}{k}$. Now, since $\omega_{u,n}$ is trivial for $n = k$, we have $B_{k,\omega_{u,k}} = B_k(1) = B_k$, so $-(1 - p^{k-1})\frac{B_{k,\omega_{u,k}}}{k} = -(1 - p^{k-1})\frac{B_k}{k} = (1 - p^{k-1})\zeta(1-k)$. If $(k_i)$ is a sequence that converges to such a $k \in X$, but diverges in the usual sense, then $\zeta'(1-k) =$

$\lim_{i\to\infty}\zeta'(1-k_i) = \lim_{i\to\infty}(1-p^{k_i-1})\zeta(1-k_i)$; but since $|k_i| \to \infty$, $\zeta'(1-k) = \lim_{i\to\infty}\zeta(1-k_i) = \zeta^*(1-k)$, so $\zeta' = \zeta^*$. □

## 3.4 Hecke Operators

If $f = \sum_{n=0}^{\infty} a_n q^n$ is a p-adic modular form, define the operator $U$ by $Uf = \sum_{n=0}^{\infty} a_{pn} q^n$, and the Hecke operator $T_l$ by $f|T_l, k = \sum_{n=0}^{\infty} a_{ln} q^n + l^{k-1}\sum_{n=0}^{\infty} a_n q^{ln}$, for $k \in X$ and $l \neq p$. If the value of $k$ is clear, we will write $T_l f$ for $f|T_l, k$. It is a basic fact that for classical modular forms, the Hecke operators produce new modular forms. We will see how both operators behave in the p-adic case:

**Proposition 4.** *If $f = \sum_{n=0}^{\infty} a_n q^n$ is a p-adic modular form,, then $T_l f$ and $Uf$ are also p-adic modular forms.*

*Proof.* Let $(f_i)$ be a sequence of rational modular forms of the form $f_i = \sum a_{n,i} q^n$, converging to $f$. We can suppose the sequence $(k_i)$ of weights of the $f_i$ diverges. Then, since we know $T_l f_i = \sum_{n=0}^{\infty} a_{ln,i} q^n + l^{k_i-1}\sum_{n=0}^{\infty} a_{n,i} q^{ln}$ is a modular form of weight $k_i$, we have the two following cases: If $p \neq l$, then $\lim_{i\to\infty} l^{k_i-1} = l^{k-1}$, and $T_l f_i \to T_l f$. On the other hand, if $l = p$, $\lim_{i\to\infty} l^{k_i-1} = 0$, so $T_l f_i \to Uf$. □

We will see that we can use these two operators to calculate the constant terms of p-adic modular forms; for this we need the following preliminary results.

**Lemma 9.** *Let $w(f)$ denote the filtration of $f$. We have $w(Uf) \leq p + \frac{w(f)-1}{p}$, and when $w(f) = p-1$, we have $w(Uf) = p-1$.*

*Proof.* Consider the $q$-expansion of $f$ in $\mathbb{F}_p[[q]]$. Then $(Uf)^p = f - \theta^{p-1} f$. Clearly $w((Uf)^p) = pw(Uf)$. Set $k = w(f)$. Then $w(\theta^{p-1}f) \leq k + (p-1)(p+1) = k + p^2 - 1$. Thus $pw(Uf) \leq \mathrm{Max}(k, k+p^2-1) = k + p^2 - 1$. For the second claim, note that $12^2\theta^2 f = kP12\theta f + kf12\theta P - 12\theta\partial f = Qf + \partial^2 f$ in $\mathbb{F}_p[[q]]$, so $\theta^2 f \in \tilde{M}_{p+3}$. It must have filtration either $-\infty$, 4, or $p+3$. If $w(\theta^2 f) = -\infty$, $\theta^2 f = 0$ so $\theta^{p-1} f = 0$, and thus we would have $f = (Uf)^p$; but $p \nmid w(f)$, so this is not possible. If $w(\theta^2 f) = 4$, $\theta^2 f$ would be a multiple of $Q$; but $\theta^2 f$ is cusp form. So we must have $w(\theta^2 f) = p+3$, and that $w((Uf)^p) = w(\theta^{p-1} f) = w(\theta^{p-3}\theta^2 f) = p+3+(p-3)(p+1) = p(p-1)$, so $w(Uf) = p-1$. □

**Theorem 10.** *Let $p > 5$. If $k > p+1$, $U$ maps $\tilde{M}_k$ into $\tilde{M}_{k'}$, for some $k' < k$. Moreover, $U$ restricted to $\tilde{M}_{p-1}$ is bijective.*

*Proof.* When $k > p+1$, $p + \frac{k-1}{p} < p+1 < k$, so $w(Uf) < k$. For the second claim, let $f$ be a non-zero element of $\tilde{M}_{p-1}$. If $w(f) = 0$, $f$ is constant and $Uf = f$. If $f \in \tilde{M}_{p-1}$, $w(Uf) = p-1$ by the above lemma, so $Uf \neq 0$; this proves $U$ is injective. As $\tilde{M}_{p-1}$ is finite dimensional, we have bijectivity. □

This result implies the following decomposition: Let $p > 5$. Then $\tilde{M}^\alpha = \tilde{S}^\alpha \oplus \tilde{N}^\alpha$, with $U$ bijective on $\tilde{S}^\alpha$ and locally nilpotent on $\tilde{N}^\alpha$. If $j \in [\alpha]$ such that $4 \leq j \leq p+1$, then $\tilde{S}^\alpha \subset \tilde{M}_j$ (recall that $[\alpha]$ denotes the class of $\alpha$ modulo $p-1$). Note $\tilde{S}^0 \subset \tilde{M}_{p-1}$; in fact, one can show that $\tilde{S}^0 = \tilde{M}_{p-1}$.

**Corollary 5.** *Let $f$ be a cusp form of weight $k$ and $p \leq 7$. Then $\lim_{n\to\infty} U^n f = 0$.*

*Proof.* Up to multiplying $f$ by a scalar, we can suppose $v_p(f) = 0$. In addition, let $k \equiv \alpha \bmod p-1$. Then $\tilde{f} \in \tilde{M}^\alpha$. Since $p \leq 7$, with regards to the above decomposition of $\tilde{M}^\alpha$, we have $j \leq 8$, and $S^\alpha$ comprises multiples of $\tilde{E}_k$, since $\tilde{M}_j$ is one dimensional. Thus $\tilde{N}^\alpha$ contains the cusp forms of $\tilde{M}^\alpha$, and in particular contains $f$. By the nilpotency property of U on $\tilde{N}^\alpha$, there exists $m \in \mathbb{Z}_{\geq 1}$ such that $U^m \tilde{f} = 0$; this implies $v_p(U^m f) \geq 1$. We can then iterate the above procedure on the cusp form $\frac{1}{p}U^m f$ to deduce that there exists $m' \in \mathbb{Z}_{\geq 1}$ such that $v_p(U^{m+m'}f) \geq 2$. Hence as $n \to \infty$, $U^n f \to 0$ p-adically. □

We can state the first of two theorems on the constant terms of p-adic modular forms:

**Theorem 11.** *Let $f$ be a p-adic modular form of non-zero weight $k$, and let $p = 2, 3, 5$, or $7$. Then*

$$a_0(f) = \frac{1}{2}\zeta^*(1-k) \lim_{n\to\infty} a_{p^n}(f).$$

*Proof.* Since $p$ does not divide the numerator of $B_m$ for $m \leq p-3$, $\zeta^*(1-k)$ is non-zero and $G_k^*$ has non-zero constant term. Using the above decomposition, we can write $f$ as the sum of a cusp form and a multiple of $G_k^*$, reducing the proof to the examination of each of these cases.
For $f = G_k^*$, we have $a_0(f) = \frac{1}{2}\zeta^*(1-k)$ and $a_{p^n} = \sigma_{k-1}^*(p^n) = \lim_{i\to\infty} \sigma_{k_i-1}(p^n) =$

$\lim_{i\to\infty}\sum_{d|p^n} d^{k_i-1} = 1$, p-adically, as required.
If $f$ is a cusp form, we need to show that $a_{p^n}(f) \to 0$. Note that $a_{p^n}(f) = a_1(U^n f)$, so if $\lim_{n\to\infty} U^n f = 0$, we will be done - and this is exactly what the preceeding corollary shows. □

Before we can state the second theorem on constant terms of p-adic modular forms, we need a lemma:

**Lemma 10.** *There exists a polynomial with integer coefficients in $U$ and $T_l$, denoted $H$, such that for all $k \in X$ such that $p-1$ divides $k$, we have*

1. $HE_k^* = c(k)E_k^*$, *with $c(k)$ a p-adic unit.*
2. $\lim_{n\to\infty} H^n f = 0$, *for $f$ a p-adic cusp form of weight $k$.*

*Proof.* For $p$ =2, 3, 5, or 7, we can take $H = U$; the theorem above and Corollary 5 show the required properties. So suppose $p \geq 11$. We need to build a polynomial $\tilde{H}$ in $U$ and the $T_l$ with coefficients in $\mathbb{F}_p$ such that $\tilde{H}1 = c$, where $c \in \mathbb{F}_p \setminus \{0\}$, and $\tilde{H}$ is locally nilpotent on cusp forms in $\tilde{M}^0$. Once we have such an $\tilde{H}$, let $H$ be a polynomial with coefficients congruent to those of $\tilde{H}$ mod $p$. Then since $UE_k^* = E_k^*$ and $T_lE_k^* = (1+l^{k-1})E_k^*$, we get $HE_k^* = c(k)E_k^*$ with $c(k) \in \mathbb{Z}_p$; the fact that $c(k) \equiv c \in \mathbb{F}_p$ under reduction mod $p$ implies $c(k)$ is invertible in $\mathbb{Z}_p$. The condition on cusp forms implies a similar result to Corollary 5, as required. All that remains is to establish the existence of such an $\tilde{H}$.
It is an application of an elementary result that given an n-tuple of operators, say $(Y_i)_{i\in I}$, with each $Y_i$ as $U$ or $T_l$ for some $l$, there exists a polynomial $F \in \mathbb{F}_p[X_1, ..., X_n]$ for some $n$ such that $F((Y_i)_{i\in I}) = 0$ and $F((\lambda_i)_{i\in I}) \neq 0$. Note that there is no element of □

**Theorem 12.** *For all p-adic modular forms $f$ of non-zero weight $k$ divisible by $p-1$, we have*

$$a_0(f) = \frac{1}{2}\zeta^*(1-k)\lim_{n\to\infty} c(k)^{-n}a_1(H^n f).$$

*Proof.* It suffices to check the formula for $f = E_k^*$ and $f$ a cusp form. When $f = E_k^*$, $a_0(E_k^*) = 1$; the formula gives us $a_0(E_k^*) = \frac{1}{2}\zeta^*(1-k)\lim_{n\to\infty} c(k)^{-n}a_1(H^nE_k^*) = \frac{1}{2}\zeta^*(1-k)\lim_{n\to\infty} c(k)^{-n}c(k)^n a_1(E_k^*) = \frac{1}{2}\zeta^*(1-k)a_1(E_k^*) = 1$, as expected. When $f$ is a cusp form, we expect $a_0(f) = 0$; the formula provides the same, by the nilpotency of $H$. □

## 3.5 Modular forms on $\Gamma_0(p)$

We will prove that every modular form on $\Gamma_0(p)$ is a p-adic modular form on $SL_2(\mathbb{Z})$. It is simple to prove that $\Gamma_0(p)$ has index $p+1$ in $SL_2(\mathbb{Z})$. We will need the following operator: if $f = \sum_{n=0}^{\infty} a_n q^n$, define $V$ by $Vf = \sum_{n=0}^{\infty} a_n q^{pn}$.

**Lemma 11.** *Let $a$ be an even integer greater than 4, divisible by $p-1$, and set $W = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$. Set $g = E_a - p^{\frac{a}{2}} E_a|_{a,W}$. Then $g \equiv 1$ mod $p$ and $g|_{a,W} \equiv 0$ mod $p^{1+\frac{a}{2}}$.*

*Proof.* For the first claim, $g \equiv 1$ mod $p$, since by Lemma 3 we have $E_a \equiv 1$ mod $p$. For the second claim, note that $(f|_{a,W})|_{a,W} = f$, so we have $g|_{a,W} = E_a|_{a,W} - p^{\frac{a}{2}} E_a$. Observing that $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$, we find that $E_a|_{k,W}(z) = p^{\frac{a}{2}} E_a(pz) = p^{\frac{a}{2}} VE_a$. Since $V$ doesnt alter the coefficients, $VE_a \equiv 1$ mod $p$, and so the difference of $VE_a$ and $E_a$ is dvisible by $p$. The result follows. □

We now define a function we will call the *trace* of $f$ : Let $f$ be a modular form of weight $k$ on $\Gamma_0(p)$. Pick coset representatives $\gamma_j$ of $SL_2(\mathbb{Z})/\Gamma_0(p)$, and define $\mathrm{Tr}(f) = \sum_{j=1}^{p+1} f|_{k,\gamma_j}$. This is a modular form of weight $k$ and is independent of the choice of coset representative.

**Lemma 12.** *Let $f = \sum_{n=0}^{\infty} a_n q^n$ and $f|_{k,W} = \sum_{n=0}^{\infty} b_n q^n$. Then*

$$Tr(f) = \sum_{n=0}^{\infty} a_n q^n + p^{1-\frac{k}{2}} \sum_{n=0}^{\infty} b_{pn} q^n = f + p^{1-\frac{k}{2}} U(f|_{k,W}).$$

*Proof.* We can choose representatives such that $\gamma_j = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$ for $1 \leq j \leq p$, and $\gamma_{p+1} = 1$. Clearly $f|_{k,\gamma_{p+1}} = f$. Now, set $h = f|_{k,W}$ and for $1 \leq j \leq p$ write $\gamma_j = W \cdot \beta_j$, where $\beta_j = \begin{pmatrix} \frac{1}{p} & \frac{j}{p} \\ 0 & 1 \end{pmatrix}$. We then have

$$\sum_{1 \leq j \leq p} f|_{k,\gamma_j} = \sum_{1 \leq j \leq p} f|_{k,W\beta_j} = \sum_{1 \leq j \leq p} g|_{k,\beta_j} = p^{\frac{-k}{2}} \sum_{1 \leq j \leq p} g(\frac{z+j}{p}).$$

Using $\sum_{j=1}^{p} e^{\frac{2\pi i n j}{p}} = p$ if $p \mid n$ and is 0 otherwise, we find that $p^{\frac{-k}{2}} \sum_{1 \leq j \leq p} g(\frac{z+j}{p}) = p^{1-\frac{k}{2}} \sum_{n \geq 0} b_{pn} q^n = p^{1-\frac{k}{2}} U(f|_{k,W})$. □

Set $f_m = \mathrm{Tr}(f \cdot g^{p^m})$, for some $m \in \mathbb{Z}_{\geq 0}$. Note that $f \cdot g^{p^m}$ has weight $k_m = k + ap^m$.

**Lemma 13.** *We have $v_p(f_m - f) \geq Inf\,\{m+1+v_p(f), p^m+1+v_p(f|_{k,W}) - \frac{k}{2}\}$.*

*Proof.* Write $f_m - f = (f_m - f \cdot g^{p^m}) + f \cdot (g^{p^m} - 1)$. Since $g \equiv 1 \bmod p$, the binomial theorem implies that $g^{p^m} \equiv 1 \bmod p^{m+1}$, so that $v_p(f \cdot (g^{p^m} - 1)) \geq m + 1 + v_p(f)$. We can apply the previous lemma for $f_m - f \cdot g^{p^m} = p^{1-\frac{k_m}{2}} U(f \cdot g^{p^m}|_{k_m,W})$; thus $v_p(f_m - f \cdot g^{p^m}) \geq 1 - \frac{k_m}{2} + v_p(f|_{k,W}) + p^m v_p(g|_{a,W})$. Then $g|_{a,W} \equiv 0 \bmod p^{1+\frac{a}{2}}$ gives $v_p(f_m - f \cdot g^{p^m}) \geq 1 - \frac{k}{2} + v_p(f|_{k,W}) + p^m$. Finally, taking valutaions on the equality at the start of this proof, we obtain the result. □

**Theorem 13.** *Let $f = \sum_{n\geq 0} a_n q^n$ be a modular form of weight $k$ on $\Gamma_0(p)$, with $a_n \in \mathbb{Q}$. Then $f$ is a p-adic modular form of weight $k$.*

*Proof.* Let $g$ and $a$ be as in Lemma 11. Both $g$ and $f \cdot g^{p^m}$ are modular forms on $\Gamma_0(p)$ of weights $a$, $k_m$ respectively. Moreover, by Lemma 12, $f_m = \mathrm{Tr}(f \cdot g^{p^m})$ is a modular form of weight $k_m$ on $SL_2(\mathbb{Z})$, with rational coefficients. Clearly $k_m \to k$ p-adically, so it remains to show that $\lim_{i\to\infty} f_m = f$. This is an implication of Lemma 13. □

## 3.6 The Iwasawa Algebra

We follow the approach of [**serre2**] and [**lang3**]
Let $U_n = \{u \in \mathbb{Z}_p^* : u \equiv 1 \bmod p^n\}$. Then we have the map $U_1 \hookrightarrow \mathbb{Z}_p^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$, which has kernel $U_n$ and image comprising elements congruent to 1 mod $p$. So $U_1/U_n = \{u \in (\mathbb{Z}/p^n\mathbb{Z})^* : u \equiv 1 \bmod p\}$, and taking the inverse limit we obtain $\lim_{\leftarrow}(U_1/U_n) = \{u \in \mathbb{Z}_p^* : u \equiv 1 \bmod p\} = U_1$. Moreover, $\{u \in (\mathbb{Z}/p^n\mathbb{Z})^* : u \equiv 1 \bmod p\}$ is cyclic of order $(p^n - p^{n-1})/(p-1) = p^{n-1}$; taking the inverse limit again shows that $\lim_{\leftarrow}(U_1/U_n) \cong \mathbb{Z}_p$. Thus $U_1 \cong \mathbb{Z}_p$.

**Definition 16.** Denote by $F$ the algebra of functions $f : \mathbb{Z}_p \to \mathbb{Z}_p$. Let $u \in U_1$ and $s \in \mathbb{Z}_p$. Define $u^s = (1 + pt)^s = \sum_{n\geq 0} \binom{s}{n} t^n p^n$ and consider the functions $f_u : s \mapsto u^s$; these $f_u$ generate a sub-$\mathbb{Z}_p$-module in $F$, which we will call $L$. A general element of $L$ has the form $s \mapsto f(s) = \sum_{u\in U_1} \lambda_u u^s$, where the coefficients are almost all 0. Define $\bar{L}$ to be the closure of $L$ in $F$, under the topology induced the metric $d(f,g) = sup_{x\in\mathbb{Z}_p}|f(x) - g(x)|$. In addition, define $\Lambda = \mathbb{Z}_p[[U_1]] = \lim_{\leftarrow} \mathbb{Z}_p[U_1/U_n]$.

We say a group $G$ with a topology is a *topological group* if it forms a topological space and the binary operation and inverse maps are continuous. An element of a topological group is a topological generator if it is an element of a subset of elements of $G$, say $S$, such that the group generated by elements of $S$ is dense in $G$.

**Proposition 5.** *Let $T$ be an indeterminate. Then we have the isomorphism $\mathbb{Z}_p[[U_1]] \cong \mathbb{Z}_p[[T]]$.*

*Proof.* Take $u = 1 + \pi \in U_1$, where $v_p(\pi) = 1$; a proof that this is a topological generator of $U_1$ may be found in [**kconrad**]. In addition, take $1 + T \in \mathbb{Z}_p[[T]]$; since $\langle 1+T\rangle = \mathbb{Z}[1+T] = \mathbb{Z}[T]$, $1+T$ is a topological generator of $\mathbb{Z}_p[[T]]$. Mapping $f_u = f_{1+\pi}$ to $1 + T$ establishes the isomorphism. □

The following fact will be useful: $\mathbb{Z}_p$, and so $U_1$, is compact with the p-adic topology, hence $\Lambda$, equipped with the product topology of the p-adic topology, is also compact.

**Proposition 6.** $\Lambda \cong \bar{L}$.

*Proof.* Using the previous proposition, we can write an element of $\Lambda$ as $f = \sum a_n T^n$ and using the above identification of $f_u - 1 = T$, define a homomorphism $\epsilon(f)$ by $s \mapsto f(u^s - 1) = \sum a_n(u^s - 1)^n$. This is a continuous homomorphism and as $u^s - 1 = (1+\pi)^s - 1 \equiv 0 \bmod p$, the series converges p-adically. Since $\epsilon(f_u)(s) = \epsilon(T+1)(s) = (u^s - 1) + (u^s - 1)^0 = u^s = f_u(s)$, $\epsilon$ is trivial on $L$. Then by continuity, taking the closure implies $\epsilon(\Lambda) = \bar{L}$. This clearly has trivial kernel, so is injective. We have obtained a bijective continuous map between compact spaces with metric topologies; therefore the map is a homeomorphism, and we have the isomorphism. □

Define the integers $c_{in}$ by the following identity:

$$\sum_{i=1}^{n} c_{in} Y^n = n! \binom{Y}{n} = Y(Y-1)(Y_2)...(Y-n+1).$$

**Theorem 14.** *Let $f \in F$. For $f$ to be in $\Lambda$, it is sufficient for there to exist p-adic integers $b_n$ such that $f(s) = \sum_{n\geq 0} b_n p^n s^n / n!$ for all $s \in \mathbb{Z}_p$ and $v_p(\sum_{i=1}^{n} c_{in} b_i) \geq v_p(n!)$ for $n \geq 1$.*

*Proof.* Set $v = \log(u)$. Using the fact that exp and log are mutually inverse functions, by the series expansion of exp we can write $T = u^s - 1 = vs + ... + v^n s^n/n! + ...$, which shows that $T$ and all powers of $T$ have the required form, and thus elements of $\Lambda$, which are power series in $T$, can all be written as such series. For $f \in \Lambda$, the map $f \mapsto (b_n(f))$ is a group isomorphism; as the coefficients $b_n$ depend continuously on $f$ and $\Lambda$ is compact, the image is bounded, so we have an isomorphism from $\Lambda$ to $S_\Lambda$, a closed submodule of $\mathbb{Z}_p$-module $(\mathbb{Z}_p)^N$, of sequences $(b_n)_{n\geq 0}$. We need to show that $S_\Lambda$ is the same as $S_b$, the submodule of $(\mathbb{Z}_p)^N$ defined by sequences of elements such that $v_p(\sum_{i=1}^n c_{in}b_i) \geq v_p(n!)$.
Note that using the series expansion of exp, every element of $U_1$ can be written $\exp(py)$ for some $y \in \mathbb{Z}_p$. We then have $u^s = \exp(pys) = \sum_{n\geq 0} y^n p^n s^n/n!$ Then $b_n(f_u) = y^n$, and the sequence $(y^n)$ is in $S_b$. In addition, by the above identity $n!$ divides $\sum_{i=1}^n c_{in} y^n$, so it satisfies the appropriate congruence relation. By linearity and passing to the limit, we obtain sequences corresponding to all elements in $\Lambda$, so one can see that $S_\Lambda \subset S_b$. We complete the proof by showing that sequences $(y^n)$ generate a dense submodule in $S_b$.
Let $m \in \mathbb{Z}_{\geq 0}$, and $b_0, ..., b_m \in \mathbb{Z}_p$ satisfying the desired congruence relation for $n \leq m$. If we prove that there exists $f \in \Lambda : b_i(f) = b_i$ for $0 \leq i \leq m$, we will be done. If $m = 0$, there is nothing to prove. By induction, we can find $g \in \Lambda$ such that $b_i(g) = b_i$ for $i \leq m-1$. If we proceed to find $h \in \Lambda$ such that $b_i(h) = 0$ for $i < m$ and $b_m(h) = b_m - b_m(g)$, then $h + g$ will be the required function. It suffices to prove the result for $b_i = 0$ for $i < m$. Granted this, $v_p(\sum_{i=1}^n c_{in}b_i) \geq v_p(n!)$ shows that $b_m$ has the form $m!z$, for $z \in \mathbb{Z}_p$. We can take $zp^m v^{-m} T^m$ for $f$; writing this polynomial in the form $\sum_{n\geq 0} b_n p^n s^n/n!$ gives such a $b_m(f)$. Since the $f_u$ are dense in $\Lambda$, and we have shown that the sequences in $S_b$ can be approximated to arbitrary accuracy by the $b_i(f)$ for $f \in \Lambda$, we are done. □

An important example once again is the p-adic Eisenstein series:

**Proposition 7.** *Recall* $G_k^* = \frac{1}{2}\lim_{i\to\infty} \zeta(1-k_i) + \sum_{n\geq 1} \sigma_{k-1}^*(n) q^n$. *Then*

(i) *For fixed* $u$ *and fixed* $n \geq 1$, *the map* $s \mapsto a_n(G_{s,u}^*)$ *is an element of* $\Lambda$.

(ii) *If* $u$ *is even in* $\mathbb{Z}/(p-1)\mathbb{Z} \setminus \{0\}$, *the function* $s \mapsto a_0(G_{s,u}^*) = \frac{1}{2}\zeta^*(1-s, 1-u)$ *is in* $\Lambda$.

(iii) *If* $u = 0$, *the function* $s \mapsto a_0(G_{s,u}^*) = \frac{1}{2}\zeta^*(1-s, 1)$ *has the form* $T^{-1}g(T)$, *where* $g \in \Lambda$ *is invertible.*

*Proof.* For (i) note that if $n \geq 1$, we have $a_n(G^*_{s,u}) = \sigma^*_{k-1}(n) = \sum_{d|n,(d,p)=1} d^{k-1}$. Therefore $d$ is a p-adic unit, and we can decompose it as $\omega(d)\langle d\rangle$, where $\omega(d)$ is a $(p-1)th$ root of unity in $\mathbb{Z}_p$ and $\langle d\rangle$ is in $1 + p\mathbb{Z}_p$. Thus $a_n(G^*_{s,u}) = \sum d^{-1}\omega(d)^k\langle d\rangle^k = \sum d^{-1}\omega(d)^u\langle d\rangle^s$, which has the required form to be an element of $L$, and so is necessarily an element of $\Lambda$.
Finally, (ii) and (iii) are restatements of the results of [**iwasawa2**]. □

We can apply this to the normalized p-adic Eisenstein series, so we find that the coefficients $a_n(E^*_{s,0})$ are in $\Lambda$, and are divisible by $T$ for $n \geq 1$.

**Theorem 15.** *If the function $s \mapsto a_n(f_s)$ is in $\Lambda$ for $n \geq 1$, then so is $s \mapsto a_0(f_s)$, where $f_s$ is a p-adic modular form of even weight $k(s)$ and depends upon $s \in \mathbb{Z}_p$.*

We will need the following lemma before we prove the theorem:

**Lemma 14.** *If $k$ is even in $X$ and not divisible by $p-1$, there exists a sequence of elements $(\lambda_{m,n})_{m,n\geq 1}$ in $\mathbb{Z}_p$ such that*

(i) *For all $n$, $\lambda_{m,n} = 0$ for large $m$.*

(ii) *If $u_n(f) = \sum_{m\geq 1}\lambda_{m,n}a_m(f)$, then $a_0(f) = \lim_{n\to\infty} u_n(f)$, where $f$ is a p-adic modular form of weight $k$.*

*Proof.* Let $M(k)$ denote the $\mathbb{Q}_p$ vector space of p-adic modular forms of weight $k$. We begin by proving that for a finite-dimensional subspace $Y$ of $M(k)$, we can find a sequence $(\lambda_m)_{m\geq 1}$ such that $a_0(f) = \sum_{m\geq 1}\lambda_m a_m(f)$, for all $f \in Y$. Indeed, take $Y_0 \subset Y$ of elements with $v_p(f) \geq 0$; this is a free $\mathbb{Z}_p$-module of rank $r$, for some $r \in \mathbb{Z}$. If $f_1, ..., f_r$ form a basis of $Y_0$ we can find $m_1, ..., m_r \geq 1$ such that $det(A) \not\equiv 0$ mod $p$, where $A$ is the matrix with $i, j$ entry $a_{m_i}(f_j)$. Otherwise, there exists $c_j \in \mathbb{Z}_p$, not all divisible by $p$, with $a_m(\sum_{j=1}^r c_j f_j) \equiv 0$ mod $p$ for all $m \geq 1$. If we set $f = \sum_{j=1}^r c_j f_j$, the restatement of Theorem 7 implies $v_p(a_0(f)) \geq 1$, and hence $v_p(f) \geq 1$, contradicting that $p \nmid c_j$ for all $j$. We can then consider the $a_{m_i}$ as the dual basis of the dual to $Y_0$, since they map $Y_0$ to $\mathbb{Z}_p$, and they can be taken so that $a_{m_i}$ maps $f_i$ to a p-adic unit. Then we can write $a_0 = \sum_{i=1}^r \lambda_i a_{m_i}$, for some $\lambda_i \in \mathbb{Z}_p$.
Now, denote by $M(k)_0$ the set of $f \in M(k)$ with $v_p(f) \geq 0$ and let $k \equiv \alpha$ mod $p-1$. Clearly $M(k)_0/pM(k)_0 \cong \tilde{M}^\alpha$. Now, if $M_k(\mathbb{Z})$ is the set of classical modular forms with interger coefficients, we know $M_k(\mathbb{Z})$ is a

$\mathbb{Z}$-module with a finite basis, $f_1, ..., f_{r_k}$ for some $r_k$. Then $\cup_{k\in\mathbb{Z}}\{f_1, ... f_{r_k}\}$ is countable and an element of $\tilde{M}_k$ is congruent to a finite $\mathbb{Z}$-linear combination of modular forms; thus $\tilde{M}_k$ and $\tilde{M}^\alpha$ are countable, and so $M(k)_0/pM(k)_0$ is countable. Denote the elements of $M(k)_0/pM(k)_0$ by $\bar{f_1}, \bar{f_2}, ...$ and select $f_i \in M(k)_0$ that reduces to $\bar{f_i}$ in $M(k)_0/pM(k)_0$. Denote by $V_i$ the $\mathbb{Q}_p$-span of $\{f_1, f_2, ..., f_i\}$. We claim the union of the $V_i$ is dense in $M(k)$. Pick $g \in M(k)$. Up to replacing $g$ by $p^m g$ for some $m$, we can say $g \in M(k)_0 \setminus pM(k)_0$. Then $\bar{g} = \bar{f_{i_1}}$ for some $i_1$. Set $g_1 = f_{i_1}$. Clearly we have $g - g_1 \in pM(k)_0$ and there exists $m_1$: $\frac{g-g_1}{p^{m_1}} \in M(k)_0 \setminus pM(k)_0$. Now pick $i_2$: $\overline{\frac{g-g_1}{p^{m_1}}} = \bar{f_{i_2}}$ and set $g_2 = g_1 + p^{m_1} f_{i_2}$ and we have $g - g_2 \in p^{m_1+1}M(k)_0$. Iterating this, we obtain the result.
The above shows that for each $V_n$, there exists a $\mathbb{Z}_p$-linear combination of $a_m$, denoted by $u_n$, such that $a_0(f) = u_n(f)$ for all $f \in V_n$. □

*Proof of Theorem 15.* Write $k(s) = (rs, u)$, with $r \in \mathbb{Z}$ and $u \neq 0$. Write

$$E^*_{-rs} = 1 + \frac{2}{\zeta^*(1-k)} \sum_{n\geq 1} \sigma^*_{k-1}(n) q^n = \sum_{n=0}^{\infty} e_n(s) q^n.$$

Then the p-adic modular form $f'_s = f_s E^*_{-rs}$ has weight $(0, u)$, with coefficients $a_m(f'_s) = e_m(s)a_0(f_s) + \sum_{i=1}^m e_{m-i}(s)a_i(f_s)$. Apply the above lemma to $k = (0, u)$ for $a_0(f'_s) = \lim_{n\to\infty} \sum_m \lambda_{m,n} a_m(f'_s)$ satisfying the relevant conditions. The constant terms of $f_s$ and $f'_s$ are identical, allowing us to write

$$a_0(f_s) = \lim_{n\to\infty} \big( \sum_{m\geq 1} \lambda_{m,n} e_m(s) a_0(f_s) + \sum_{m,i\geq 1} \lambda_{m,n} e_{m-i}(s) a_i(f_s) \big).$$

Set $g_n(s) = \sum_m \lambda_{m,n} e_m(s)$; since the coefficients of $E^*_{-rs}$ are in $\Lambda$, $g_n$ is in $\Lambda$, which is compact, so up to replacing $g_n$ by a subsequence, we have that $g_n \to g \in \Lambda$. Rearranging the above and setting $b_n(s) = \sum_{m,i\geq 1} \lambda_{m,n} e_{m-i}(s) a_i(f_s)$, we obtain $(1 - g(s))a_0(f_s) = \lim_{n\to\infty} b_n(s)$. The assumption on the $a_n(f_s)$ implies that the $b_n$ are all in $\Lambda$, and their limit is in $\Lambda$. Note $g(0) = 0$ since $g_n(0) = 0$ for all $n$, which implies that $g$ is in the maximal ideal of $\Lambda$, so $1 - g$ is invertible in $\Lambda$, and we are done. □

**Lemma 15.** *If $R$ is a polynomial in $U$ and the $T_l$, where $l \neq p$ is prime, with coefficients in $\mathbb{Z}_p$, there exist functions $k \mapsto c_{ij}(R, k)_{i,j\geq 0}$ contained in $L$ such that for $i \geq 0$ we have*

(i) *$c_{ij}(R,k) = 0$ for $j >> 0$; $c_{ij}(R,k) = 0$ for $j = 0$ if $i \geq 1$; and $c_{ij}(R,k) = 0$ for $j \geq 1$ if $i = 0$, and*

(ii) *$a_i(Rf) = \sum_j c_{ij}(R,k)a_j(f)$, where $k \in 2\mathbb{Z}_p$ and $f$ is a p-adic modular form.*

*Proof.* If $R = U$ or $T_l$, we are done by the formulas for $Uf$ and $T_l f$. Suppose that the result holds for two polynomials, $R_1$ and $R_2$. Then property (i) certainly holds for $R_1 + R_2$ and $R_1 R_2$, and it is also clear that property (ii) holds for $R_1 + R_2$, since $c_{ij}(R_1 + R_2, k) = c_{ij}(R_1, k) + c_{ij}(R_2, k)$. Using the formula for the product of two polynomials, one also deduces that (ii) holds for $R_1 R_2$ as well. Finally, taking $U$ and $T_l$ in the place of $R_1$ and $R_2$, we get the result for polynomials in $U$ and $T_l$. □

**Theorem 16.** *Let $f_s$ have weight $k(s) = (rs, 0)$, where $r \in \mathbb{Z} \setminus \{0\}$, and $n \geq 1$. If the function $s \mapsto a_n(f_s)$ is an element of $\Lambda$, so is the function $s \mapsto 2\zeta^*(1 - rs, 1)^{-1} a_0(f_s)$.*

*Proof.* Pick a polynomial $H$ as in Lemma 10, with integer coefficients. Then Theorem 12 implies $2\zeta^*(1 - rs, 1)^{-1} a_0(f_s) = \lim_{n \to \infty} c(rs)^{-n} a_1(f_s | H^n, rs)$. So we show that $c(rs)^{-n}$ and $a_1(f_s | H^n, rs)$ are in $\Lambda$. By the lemma we have $a_1(f_s | H^n, rs) = \sum_{j \geq 1} c_{1j}(H^n, rs) a_j(f_s)$; since we assumed the $a_n(f_s)$ are in $\Lambda$, this proves $a_1(f_s | H^n, rs)$ is in $\Lambda$. Now, $c(k) = a_0(HE_k^*) = \sum_j c_{0j}(H, k) a_j(E_k^*) = c_{00}(H, k)$, so by the lemma $c(k)$ is in $L$ - and so must be $c(rs)$, which is a p-adic unit. Writing $c(rs)$ as an element of $\mathbb{Z}_p[[T]]$, the constant term must be a unit in $\mathbb{Z}_p$, so $s \mapsto c(rs)^{-n}$ makes sense and is in $\Lambda$ for all $n$. □

**Corollary 6.** *The function $s \mapsto a_0(f_s)$ is an element of Frac$(\Lambda)$, and we can write it in the form $c(T)/((1 + T)^r - 1)$, with $c \in \Lambda$.*

*Proof.* By Lemma 7 we can write $s \mapsto \frac{1}{2}\zeta^*(1 - s, 1)$ in the form $T^{-1} g(T)$, where $g \in \Lambda$ is invertible; hence we can write $s \mapsto 2\zeta^*(1 - s, 1)^{-1}$ in the form $Th(T)$, where $h \in \Lambda$ is invertible. Sending $s \mapsto rs$ corresponds to sending $1 + T \mapsto (1 + T)^r$, whence $s \mapsto 2\zeta^*(1 - rs, 1)^{-1}$ can be written $((1 + T)^r - 1)e(T)$, where $e \in \Lambda$ is invertible. Now, let $q$ be the largest power of $p$ that divides $r$. We can write $(1 + T)^r - 1$ in the form $u(T)((1 + T)^q - 1)$, where $u \in \Lambda$ is invertible. Using this we can write $s \mapsto a_0(f_s)$ in the form $d(T)/((1 + T)^q - 1)$, with $d \in \Lambda$. □

### 3.7 The p-adic Zeta Function

Let $K$ be a totally real number field of degree $r$ over $\mathbb{Q}$. We will define modular forms attached to $K$ and recall the definition of the zeta function of $K$, $\zeta_K(s)$; as Kubota and Leopoldt extended the L-function $L(s,\chi)$ to a p-adic meromorphic function $L_p(s,\chi)$, we will extend $\zeta_K(s)$ to a p-adic analogue.
Let $k \in \mathbb{Z}_{\geq 2}$. Recall that $\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{(Nm(I))^s}$, and that $g_k = 2^{-r}\zeta_K(1-k) + \sum_{\mathbf{a}} \sum_{\nu \in \mathbf{d}^{-1}\mathbf{a}} Nm(\mathbf{a})^{k-1} q^{Tr(\nu)}$, where $\sigma(\nu) > 0$ for all embeddings $\sigma : K \hookrightarrow \mathbb{R}$, is modular of weight $rk$, when $r > 1$. As before, write $g_k = a_0(g_k) + \sum_{n=1}^{\infty} a_n(g_k) q^n$. Note that $Tr(\nu) = n$.
Let $k \in X$ be even and $rk \neq 0$. Choose a sequence $(k_i)$ such that $k_i \geq 4$, $|k_i| \to \infty$, and $k_i \to k \in X$. Let $u \in \mathbb{Z}_p$. Similarly to when we defined the p-adic Eisenstein series, we find that the $a_n(g_{k_i})$ converge; $\lim_{i\to\infty} a_n(g_{k_i}) = \lim_{i\to\infty} \sum_{\mathbf{a}} \sum_{\nu \in \mathbf{d}^{-1}\mathbf{a}} Nm(\mathbf{a})^{k_i - 1} = \sum_{\mathbf{a}} \sum_{\nu \in \mathbf{d}^{-1}\mathbf{a}} Nm(\mathbf{a})^{k-1}$, where $\mathbf{a} \subset \mathcal{O}_K$ is prime to $p$; else, if $p \in \mathbf{a}$, then $Nm(\mathbf{a})$ is a power of $p$ and $Nm(\mathbf{a})^{k_i-1}$ tends to 0. This convergence is uniform in $n$, so by Corollary 4 the $g_{k_i}$ have a limit, $g_k^*$, which has weight $rk$ and is defined by the coefficients

$$a_0(g_k^*) = 2^{-r}\zeta_K^*(1-k) = 2^{-r} \lim_{i\to\infty} \zeta_K(1-k_i)$$

and

$$a_n(g_k^*) = \sum_{(\mathbf{a},p)=1} \sum_{\nu \in \mathbf{d}^{-1}\mathbf{a}} Nm(\mathbf{a})^{k-1},$$

with $Tr(\nu) = n$ and $\sigma(\nu) > 0$ for all embeddings $\sigma : K \hookrightarrow \mathbb{R}$. This function is the *p-adic zeta function of K.*

**Definition 17.** Let $S$ denote the set of prime ideals of $\mathcal{O}_K$ which divide $p$. Define $\zeta_{K,S}(s) = \zeta_K(s)\prod_{\mathfrak{p}\in S}(1 - Nm(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}\notin S}(1 - Nm(\mathfrak{p})^{-s}) = \sum_{(\mathbf{a},p)=1} Nm(\mathbf{a})^{-s}$. Furthermore, define a modified version of $g_k$, $g_k' = 2^{-r}\zeta_{K,S}(1-k) + \sum_{(\mathbf{a},p)=1} \sum_{\nu\in\mathbf{d}^{-1}\mathbf{a}} Nm(\mathbf{a})^{k-1} q^{Tr(\nu)}$.

**Theorem 17.** *The $g_k'$ are modular forms on $\Gamma_0(p)$ of weight $rk$.*

*Proof.* See the appendix of [**serre2**]. □

The following theorem shows that $\zeta_K^*$ is continuous on the set of negative integers:

**Theorem 18.** *Let $k \in \mathbb{Z}_{\geq 2}$. Then $\zeta_K^*(1-k) = \zeta_{K,S}(1-k) = \zeta_K(1-k)\prod_{\mathfrak{p}\in S}(1 - Nm(\mathfrak{p})^{k-1})$.*

*Proof.* Since $g'_k$ is modular on $\Gamma_0(p)$, by Theorem 13 $g'_k$ is a p-adic modular form. Clearly $a_n(g'_k) = a_n(g^*_k)$ for $n \geq 1$, so by Corollary 4, we have $a_0(g'_k) = a_0(g^*_k)$, and we are done. □

Note that we must have $rk \neq 0$ in the above. When we take $k \in X$, this is equivalent to saying $k = (s,u)$ where $s \neq 0$ or $ru \not\equiv 0$.

**Theorem 19.** *Let $k = (s,u) \in X$ where $u$ is even. Let $p > 2$.*

1. *If $ru \neq 0$, the function $s \mapsto \zeta_K^*(1-s, 1-u)$ is an element of $\Lambda = \mathbb{Z}_p[[T]]$.*

2. *If $ru = 0$, $s \mapsto \zeta_K^*(1-s, 1-u)$ has the form $h(T)/((1+T)^r - 1)$, where $h \in \Lambda$.*

*Proof.* Set $k = (s,u)$ and let $n \geq 1$. The function $s \mapsto a_n(g^*_k)$ can be considered a sum of functions $s \mapsto Nm(\mathbf{a})$, where $\mathbf{a}$ is prime to $p$, so $Nm(\mathbf{a})$ is a p-adic unit. Then we can use the decomposition $Nm(\mathbf{a})^{k-1} = Nm(\mathbf{a})^{-1}\omega(Nm(\mathbf{a}))^u\langle Nm(\mathbf{a})\rangle^s$ - which has the form of an element of $L$. The result follows from direct application of Theorem 15 and Corollary 6. □

**Corollary 7.** (i) *If $ru \neq 0$, the function $s \mapsto \zeta_K^*(1-s, 1-u)$ is holomorphic on a disc larger than the unit disc of $\mathbb{Z}_p$.*

(ii) *If $ru = 0$, $s \mapsto \zeta_K^*(1-s, 1-u)$ is meromorphic on a disc larger than the unit disc; in this case, it has a unique, simple pole at $s = 0$.*

*Proof.* The above theorem combined with Theorem 14 shows that, in the first case, $s \mapsto \zeta_K^*(1-s, 1-u)$ has a Taylor expansion; as $v_p(b_n p^n/n!) \geq n - v_p(n!) \geq n\frac{p-2}{p-1}$, it converges as stated. In the second case, $(1+T)^r - 1$ can be expressed $u^{rs} - 1$; □

# 4 Galois Representations Attached to Modular Forms

## 4.1 Introducing $\rho_l$

In this section, we will take the existence of a Galois representation attached to the coefficients of a modular form as given. We will first explore the possible images of the representation, and then go on to use our theory of mod p modular forms to examine which primes are 'exceptional' for a given modular form. Before we proceed, we need to develop some notation. We will let $l$ be a prime number, and let $K_l$ be the maximal algebraic extension of $\mathbb{Q}$ ramified only at $l$. Further, we will take $K_l^{ab}$ to be the maximal subfield of $K_l$ which is abelian over $\mathbb{Q}$. $Frob_p$ will denote the conjugacy class of Frobenius elements in Gal($K_l/\mathbb{Q}$).

**Lemma 16.** *There exists an isomorphism $Gal(K_l^{ab}/\mathbb{Q}) \cong \mathbb{Z}_l^*$, where $\mathbb{Z}_l^*$ is the group of l-adic units. This in turn induces a character*

$$\chi_l : Gal(K_l/\mathbb{Q}) \to Gal(K_l^{ab}/\mathbb{Q}) \tilde{\to} \mathbb{Z}_l^*,$$

*such that*

$$\chi(Frob_p) = p, \tag{16}$$

*for all p$\neq l$.*

**Theorem 20.** *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a normalized cusp form of weight k with integer coefficients, and Dirichlet series*

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_{i=1}^{\infty} (1 - a_p p^{-s} + p^{k-1-2s})^{-1}$$

*Then there exists a continuous homomorphism*

$$\rho_l : Gal(K_l/\mathbb{Q}) \to GL_2(\mathbb{Z}_l),$$

*that depends on $f$ such that $\rho_l(Frob_p)$ has characteristic polynomial*

$$x^2 - a_p x + p^{k-1} \tag{17}$$

*for each p $\neq l$.*

*Proof.* See [**deligne**]. □

Note that (17) implies that the trace of $\rho_l(Frob_p)$ is $a_p$, and that the norm of $\rho_l(Frob_p)$ is $p^{k-1}$. More generally than this, we have

$$det \circ \rho_l = \chi_l^{k-1}$$

Since $\chi_l$ maps into $\mathbb{Z}_l^*$, the image of $det \circ \rho_l$ is $(k-1)$th powers in $\mathbb{Z}_l^*$. Denote by $\tilde{\rho}_l$ the map

$$\tilde{\rho}_l : Gal\big(K_l/\mathbb{Q}\big) \to GL_2\big(\mathbb{Z}_l\big) \to GL_2\big(\mathbb{F}_l\big), \tag{18}$$

induced by reducing $\rho_l$ mod $l$. More generally, we will use a tilde to denote reduction mod $l$.

**Lemma 17.** *The set of matrices*

$$H_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2\big(\mathbb{Z}/l^2\mathbb{Z}\big) \middle| \begin{matrix} a \equiv d \equiv 1 \ mod \ l \\ b \equiv c \equiv 0 \ mod \ l \end{matrix} \right\}$$

*is generated by $I + lu$, for $u \in U := \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \right\}$.*

*Proof.* Label the three matrices in $U$ as $u_1, u_2,$ and $u_3$ respectively. Note that each $I + lu_i$ is an element of $H_2$: all three $I + lu_i$ reduce to the identity mod $l$, and $I + lu_1$ and $I + lu_2$ clearly have determinant 1. To see this for $I + lu_3$, observe that

$$\left| \begin{pmatrix} 1+l & -l \\ l & 1-l \end{pmatrix} \right| = (1+l)(1-l) + l^2 = 1 - l^2 + l^2 = 1.$$

The claim is that

$$H_2 = \langle I + lu_1, I + lu_2, I + lu_3 \rangle = \left\langle \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ l & 1 \end{pmatrix}, \begin{pmatrix} 1+l & -l \\ l & 1-l \end{pmatrix} \right\rangle$$

Since each $I + lu_i$ is in $H_2$, we have $\langle I + lu_1, I + lu_2, I + lu_3 \rangle \subseteq H_2$. To conclude the proof, we show that $H_2$ and $\langle I + lu_1, I + lu_2, I + lu_3 \rangle$ have the same cardinality.
We can think of $H_2$ as the kernel of $SL_2\big(\mathbb{Z}/l^2\mathbb{Z}\big) \to SL_2\big(\mathbb{Z}/l\mathbb{Z}\big)$, and so obtain

$$\Big[SL_2\big(\mathbb{Z}/l^2\mathbb{Z}\big) : SL_2\big(\mathbb{Z}/l\mathbb{Z}\big)\Big] = |H_2|$$

Using the formula $|\mathrm{SL}_2\left(\mathbb{Z}/l^e\mathbb{Z}\right)| = l^{3e}\left(1 - \frac{1}{l^2}\right)$, we find that $|SL_2\big(\mathbb{Z}/l^2\mathbb{Z}\big)| = l^6(1 - 1/l^2) = l^4(l^2 - 1)$ and $|SL_2\big(\mathbb{Z}/l\mathbb{Z}\big)| = l^3(1 - 1/l^2) = l(l^2 - 1)$, so that

$$|H_2| = \Big[SL_2\big(\mathbb{Z}/l^2\mathbb{Z}\big) : SL_2\big(\mathbb{Z}/l\mathbb{Z}\big)\Big] = l^4(l^2 - 1)/l(l^2 - 1) = l^3$$

It is clear that $I + lu_1$ and $I + lu_2$ both have order $l$; it remains to check that $I + lu_3$ has order $l$, and we will be done. To this end, observe that

$$\begin{pmatrix} 1+l & -l \\ l & 1-l \end{pmatrix}^n = \begin{pmatrix} 1+nl & -ln \\ ln & 1-nl \end{pmatrix}$$

so $I + lu_3$ has order $l$ in $SL_2(\mathbb{Z}/l^2\mathbb{Z})$. □

**Theorem 21.** *Let $l > 3$ and $G$ be a subgroup $GL_2(\mathbb{Z}_l)$ closed in the $l$-adic topology. If $\tilde{G}$ contains $SL_2(\mathbb{F}_l)$, then $G$ contains $SL_2(\mathbb{Z}_l)$.*

*Proof.* Let $G_n$ denote the image of $G$ in $GL_2(\mathbb{Z}/l^n\mathbb{Z})$. We need to prove that $SL_2(\mathbb{Z}/l^n\mathbb{Z}) \subset G_n$ for all $n > 0$. We will rely on two inductive arguments: firstly, we will show that $G_n$ contains the kernel of the map

$$\varphi : SL_2(\mathbb{Z}/l^n\mathbb{Z}) \to SL_2(\mathbb{Z}/l^{n-1}\mathbb{Z}),$$

for $n \geq 2$. After this, we will use this result and induction to prove the theorem.
Denote the kernel of $\varphi$ by $H_n$ and let $n = 2$, so

$$\begin{aligned} H_2 &= \ker\Big(SL_2(\mathbb{Z}/l^2\mathbb{Z}) \to SL_2(\mathbb{Z}/l\mathbb{Z})\Big) \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/l^2\mathbb{Z}) \middle| \begin{matrix} a \equiv d \equiv 1 \bmod l \\ b \equiv c \equiv 0 \bmod l \end{matrix} \right\}, \end{aligned}$$

which by Lemma 17 is equal to $\langle I + lu_1, I + lu_2, I + lu_3 \rangle$, with $u_i$ as in the lemma. We will show that $G_2$ contains the images of each $I + lu_i$. Since $I + u_i$ is in $SL_2(\mathbb{Z})$ and $\tilde{G}$ contains $SL_2(\mathbb{F}_l)$, there exists a matrix $b \in G$ such that $b \equiv I + u_i \bmod l$. Alternatively, we can write $b = I + u_i + lv$, for some matrix $v$ with entries in $\mathbb{Z}_l$. We can then see that

$$\begin{aligned} b^l = (I + u_i + lv)^l &= I + l(u_i + lv) + ... + (u_i + lv)^l \\ &\equiv I + lu_i \bmod l^2, \end{aligned}$$

since each term (except for $I + lu_i$) has either a factor of $l^2$ or $u_i^2$, and $u_i^2 = 0$ for each $i$. Then $H_2 \subset G_2$.
Now assume $H_{n-1} \subset G_{n-1}$. Take an element of $H_n$, say $I + l^{n-1}w$, where $w$ has entries in $\mathbb{Z}_l$; then $I + l^{n-2}w \bmod l^{n-1}$ is in $H_{n-1}$. By induction we have

$I + l^{n-2}w \bmod l^{n-1} \in G_{n-1}$. Similarly to before, there exists an element $c \in G$ such that $c = I + l^{n-2}w + l^{n-1}x$, where $x$ has entries in $\mathbb{Z}_l$. Again we have

$$\begin{aligned} c^l &= (I + l^{n-2}w + l^{n-1}x)^l = I + l(l^{n-2}w + l^{n-1}x) + \ldots + (l^{n-2}w + l^{n-1}x)^l \\ &= I + l^{n-1}w + l^n x + \ldots + (l^{n-2}w + l^{n-1}x)^l \\ &\equiv I + l^{n-1}w \bmod l^n. \end{aligned}$$

So $H_n \subset G_n$, as required.
To finish the proof, we proceed by induction, noting that we have assumed in the statement of the theorem that $G_1$ contains $SL_2(\mathbb{F}_l)$, so the $l = 1$ case holds. Fix n and suppose that $SL_2(\mathbb{Z}/l^{n-1}\mathbb{Z}) \subset G_{n-1}$. Set $K$ to be the kernel of $G_n \to G_{n-1}$. We obtain the following diagram:

$$\begin{tikzcd} H_n \arrow[r, hook, "\varphi_1"] \arrow[d, hook, "\phi_1"] & SL_2(\mathbb{Z}/l^n\mathbb{Z}) \arrow[r, two heads, "\varphi_2"] \arrow[d, "f"] & SL_2(\mathbb{Z}/l^{n-1}\mathbb{Z}) \arrow[d, hook, "\phi_2"] \\ \mathrm{K} \arrow[r, hook, "\psi_1"] & G_n \arrow[r, two heads, "\psi_2"] & G_{n-1}, \end{tikzcd}$$

which commutes. We need to show that the middle vertical map, $f$, is injective. Let $a$ be an element in the kernel of $f$. Then $f(a) = I$. As the diagram commutes, we have

$$I = \psi_2(f(a)) = \phi_2(\varphi_2(a)),$$

and by the injectivity of $\phi_2$, we must have $\varphi_2(a) = I$. So $a$ is in the kernel of $\varphi_2$, which is precisely $H_n$. Using the commutativity of the diagram again, we have

$$\psi_1(\phi_1(a)) = f(\varphi_1(a)) = I,$$

and since both $\psi_1$ and $\phi_1$ are injective, we find that $a = I$ and $f$ is injective, proving the theorem. □

Note: this theorem implies that in order to determine

**Definition 18.** A prime number $l$ is an *exceptional* prime for the cusp form $f$ if the image of $\rho_l$ does not contain $SL_2(\mathbb{Z}_l)$.

Note: In light of this definition, we can rewrite Theorem 21 as the following: If $l > 3$, $l$ is exceptional for $f$ if and only if the image of $\tilde{\rho}_l$ does not contain $SL_2(\mathbb{F}_l)$.

Recall that $\rho_l : Gal\big(K_l/\mathbb{Q}\big) \to GL_2\big(\mathbb{Z}_l\big)$, and that $det \circ \rho_l = \chi_l^{k-1}$. Thus if $l$ is *not* exceptional for $f$, the image of $\rho_l$ is the preimage of $(\mathbb{Z}_l^*)^{k-1}$ in $GL_2\big(\mathbb{Z}_l\big)$, under the determinant map. The theorem tells us that it suffices to look at the image of $\tilde{\rho}_l$ instead of $\rho_l$. We will hunt for exceptional primes; we start by finding some subgroups of $GL_2\big(\mathbb{F}_l\big)$ which do not contain $SL_2\big(\mathbb{F}_l\big)$.

## 4.2 The Images of $\tilde{\rho}_l$

Let $V$ be a 2 dimensional vector space over $\mathbb{F}_l$. We begin by defining two important subgroups of $GL_2\big(\mathbb{F}_l\big)$:

**Definition 19.** A *Borel* subgroup is any subgroup of $GL_2\big(\mathbb{F}_l\big)$ conjugate to the subgroup of non-singular (i.e. determinant non-zero) upper triangular matrices.

Remark: there is a bijection between Borel subgroups and one-dimensional subspaces of V, where for each one-dimensional subspace there exists a unique Borel subgroup, made up of matrices with the subspace as an eigenspace.

**Definition 20.**

(i) A *split* Cartan subgroup is a subgroup conjugate to the group of non-singular diagonal matrices. Thus there is a bijection between split Cartan subgroups and unordered pairs of distinct one-dimensional subspaces of V, where a pair of subspaces corresponds to the set of matrices with those both subspaces as eigenspaces.

(ii) A *non-split* Cartan subgroup, is defined as follows: let $V$ be a one-dimensional $\mathbb{F}_{l^2}$ vector space. Let $\{e_1, e_2\}$ be an $\mathbb{F}_l$ basis for $V$, and note that $\alpha \in \mathbb{F}_{l^2}^*$ acts on $V$ $\mathbb{F}_l$-linearly. Denote by $M_\alpha$ the matrix associated to multiplication by $\alpha$ with respect to the basis $\{e_1, e_2\}$. If $\alpha$ and $\beta$ are in $\mathbb{F}_{l^2}^*$, then $\alpha\beta$ has corresponding matrix $M_{\alpha\beta}$; but multiplication by $\alpha\beta$ is of course the same as multiplication by $\beta$, then $\alpha$, so we obtain $M_{\alpha\beta} = M_\alpha M_\beta$. Hence we obtain an injective homomorphism $\mathbb{F}_{l^2}^* \hookrightarrow GL_2(\mathbb{F}_l)$. The non-split Cartan subgroup is the image of this homomorphism.

We make two remarks on the definitions:
1. A split Cartan subgroup is isomorphic to $\mathbb{Z}/(l-1)\mathbb{Z} \times \mathbb{Z}/(l-1)\mathbb{Z}$. This is because its elements are non-zero, diagonal, and two-dimensional, so it is characterised by two independent non-zero elements in $\mathbb{F}_l$.

2. As conjugation by an element of the normalizer of a Cartan subgroup fixes the Cartan subgroup, it can have only two effects on subgroup's eigenspaces: it either fixes the eigenspaces, or swaps them. If it fixes the eigenspaces, it must already be in the Cartan subgroup. From this it follows (?) that a Cartan subgroup has index two in its normaliser.

**Proposition 8.** *A Cartan subgroup is semi-simple, commutative, and maximal. Moreover, any semi-simple, commutative, maximal subgroup is a Cartan subgroup.*

*Proof.* Commutativity is clear. We only need to prove semi-simplicity in the non-split case. We show that after extending $GL_2(\mathbb{F}_l)$ to $GL_2(\bar{\mathbb{F}}_l)$, a non-split Cartan subgroup becomes diagonalizable. Let $P_\alpha$ be the minimal polynomial of $\alpha$ over $\mathbb{F}_l$. If $\alpha \in \mathbb{F}_l^*$, we have $M_\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$, and so $P_\alpha = x - \alpha$. If $\alpha \in \mathbb{F}_{l^2}^* \setminus \mathbb{F}_l^*$, $P_\alpha$ is irreducible and has degree 2. Note that the characteristic polynomial, $\chi$, has degree 2 and that $P_\alpha$ divides $\chi$ - so $P_\alpha = \chi$. Since the minimal polynomial has distinct roots in $\bar{\mathbb{F}}_l$, so must the characteristic polynomial, and so $M_\alpha$ must be diagonalizable. For maximality, we first deal with the split case. Suppose the subgroup of diagonal matrices, $D$, were not maximal. Then any proper commutative subgroup containing $D$ must contain a non-diagonal element, say $c$. By writing down the condition for commutativity of $c$ with a diagonal matrix, one can see that the reverse diagonals of $c$ must vanish - but then we had $c \in D$ all along.
The non-split case requires more work. Let $A$ be the image of $\mathbb{F}_{l^2}^*$ in $GL_2(\mathbb{F}_l)$. Suppose we have subgroups $A \leq B \leq GL_2(\mathbb{F}_l)$, where $B$ is commutative, and $\alpha \in \mathbb{F}_{l^2}^* \setminus \mathbb{F}_l^*$. We have $M_\alpha \in A$, which is diagonal over $GL_2(\mathbb{F}_{l^2})$ but not $GL_2(\mathbb{F}_l)$. Thus there exist lines $w_1, w_2$ defined over $\mathbb{F}_{l^2}$ such that $M_\alpha w_1 = \alpha w_1$ and $M_\alpha w_2 = \alpha^l w_2$. Recall that commuting linear operators preserve eigenspaces; so that for an arbitrary choice of $b \in B$, $b$ preserves $w_1$ and $w_2$, i.e. $bw_1 = x_1 w_1$ and $bw_2 = x_2 w_2$, for some $x_1$, $x_2 \in \mathbb{F}_{l^2}^*$. Applying the $l$-th power map (denoted by $^*$) and noting that it interchanges the eigenspaces, we obtain $b^* w_2 = x_1^* w_2$ and $b^* w_1 = x_2^* w_1$. Since $b \in GL_2(\mathbb{F}_l)$, $b^* = b$, and hence $x_1^l = x_2$ and $x_2^l = x_1$. So $b$ is a multiple of $M_\alpha$, and $b \in A$.
We have left to show the converse. Let $A$ be a semi-simple, commutative, maximal subgroup. We first show that $A$ contains a non-scalar matrix. Indeed, if not, let $a$ be a non-scalar semi-simple matrix in $GL_2(\mathbb{F}_l)$ and consider the group generated by $A$ and $a$, $\langle A, a \rangle$. It is clearly semi-simple and com-

mutative, and it properly contains $A$ - but $A$ is maximal, so it must contain a non-scalar matrix. To conclude the proof, there are two cases to consider: either such a non-scalar element of $A$ is diagonalizable over $\mathbb{F}_l$, or it is only diagonalizable over $\mathbb{F}_{l^2}$. In the first instance, the characteristic polynomial of $a$ has two distinct roots. Let $e_1, e_2$ be bases for the two eigenspaces. Since $A$ is commutative, $e_1, e_2$ are eigenvectors for all elements of $A$, so with respect to the basis $\{e_1, e_2\}$, all elements of $A$ have the form $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$.

In the second case, □

**Proposition 9.** *$SL_2(\mathbb{F}_l)$ is generated by the matrices $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}$.*

*Proof.* $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}$ are clearly elements of $SL_2(\mathbb{F}_l)$. Multiplying a matrix by $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}$ on the right or the left is equivalent to performing elementary row and column operations on the matrix. It is known that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generate $SL_2(\mathbb{Z})$. So we show elementary row and column operations transform $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ into $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and we will be done. But this is clear, since subtracting the left column of $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ from its right column yields the result. □

**Lemma 18.** *Let $G$ be a subgroup of $GL_2(\mathbb{F}_l)$ and $H$ be the image of $G$ in $PGL_2(\mathbb{F}_l)$. If $l$ divides $|G|$, then $G$ is contained in a Borel subgroup of $GL_2(\mathbb{F}_l)$, or $SL_2(\mathbb{F}_l) \subset G$. If $l \nmid |G|$, one of the following holds:*

(i) *$H$ is cyclic and $G$ is contained in a Cartan subgroup,*

(ii) *$H$ is dihedral, $G$ is contained in the normaliser of a Cartan subgroup, but not in the Cartan subgroup, and $l$ is odd, or*

(iii) *$H \cong A_4, S_4,$ or $A_5$.*

*Proof.* Let $l$ divide $|G|$. Pick an element of order $l$ in $G$, say $a$. If $a$ had two linearly independent eigenvectors, it is diagonalizable, and a diagonal matrix over $\mathbb{F}_l$ does not have order $l$. So there is a unique one-dimensional subspace of V, say $W$, which is an eigenspace for $a$. If every element of $G$ has $W$ as an eigenspace, $G$ is contained within the same Borel subgroup as $a$. Suppose there exists an element of $G$ which does not fix $W$, i.e. maps $W$ to some other one-dimensional subspace $W'$. Call this element $b$. Observe that $bab^{-1}$ is an element of $G$ of order $l$. Moreover, since $b^{-1}$ maps $W'$ to $W$ and $a$ fixes $W$, $W'$ is an eigenspace for $bab^{-1}$, and so is the unique eigenspace for $bab^{-1}$ (for order reasons). If $W$ and $W'$ are generated by vectors $u$ and $v$, respectively, fix $u$ and $v$ as a basis for V. We can then write

$$a = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix},\ bab^{-1} = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix},$$

for some c and d in $\mathbb{F}_l \setminus \{0\}$. By Proposition 9, these matrices generate $SL_2(\mathbb{F}_l)$, and so $G$ contains $SL_2(\mathbb{F}_l)$.
Now suppose that $l \nmid |G|$, so that $l \nmid |H|$. This implies that every element of $H$ is semi-simple, and so every (non-identity) element has two eigenvectors over the algebraic closure of $\mathbb{F}_l$(?). If two elements of $H$ share an eigenvector, they have both eigenvectors in common: otherwise, suppose $a$ and $b$ are elements of $H$ with only one eigenvector in common. We can find a basis in which $a$ and $b$ have the form

$$a = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix},\ b = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix},$$

where $c, d, \alpha, \beta,$ and $\delta$ are non-zero. Then the commutator

$$[a,b] = a^{-1}b^{-1}ab = \begin{pmatrix} 1 & \alpha^{-1}\beta(1 - c^{-1}d) \\ 0 & 1 \end{pmatrix}$$

is non-identity since $c \neq d$, and so has order $l$, contradicting our assumption on the order of $H$. H fixes its set of eigenvectors(?), so let $\xi_1, ..., \xi_\nu$ be representatives for the orbits of $H$ on its set of eigenvectors, and for each $\xi_i$ set $\mu_i$ to be the size of the stabilizer of $\xi_i$ in $H$. Let $|H| = h$. By the Orbit-Stabilizer Lemma, we have $|O(\xi_i)| = |H|/|Stab_H(\xi_i)| = h/\mu_i$. Each non-identity element of $H$ has two eigenvectors, so we obtain $2(|H|-1) = 2|H|-2$ pairs of a non-trivial element of $H$ with one of its eigenvectors. We can also calculate this as follows: pick an orbit representative, $\xi_i$. Pair this representative up with the non-trivial elements fixing it - there are $\mu_i - 1$ of these. Then, since the orbits partition the group, picking a representative of each orbit and summing the (?) gives us the following formula:

$$2h - 2 = h(\mu_1 - 1)/\mu_1 + ... + h(\mu_\nu - 1)/\mu_\nu,$$

which can be rewritten as

$$2(1-h^{-1}) = (1-\mu_i^{-1}) + ... + (1-\mu_\nu^{-1}).$$

Suppose $\nu = 4$. Then since $\mu_i > 1, \sum_{n=1}^{4} \mu_i^{-1} \leq 2$. But $h^{-1} \neq 0$, so we must have $\nu \leq 3$. If we only have two orbits of eigenvectors, $\nu = 2$ and so we must have $h = \mu_1 = \mu_2$. Let $\nu = 3$. If $h$ is odd, then $\mu_i$ is also odd, since $\mu_i | h$. Then $\sum_{n=1}^{3} \mu_i^{-1} \leq 1$, which implies $h^{-1} \leq 0$, so $h$ must be even. Now let $h$ be even. Then clearly the solutions have the form $\mu_1 = \mu_2 = 2, \mu_3 = \frac{h}{2}$. We also get the following three cases:

(i) $h = 12,\ \mu_1 = 2,\ \mu_2 = \mu_3 = 3,$

(ii) $h = 24,\ \mu_1 = 2,\ \mu_2 = 3,\ \mu_3 = 4,$

(iii) $h = 60,\ \mu_1 = 2,\ \mu_2 = 3,\ \mu_3 = 5.$

We now associate each of the cases to a subgroup of $PGL_2(\mathbb{F}_l)$.
When $\nu = 2$, there are only two orbits of eigenvectors; since every element of $H$ has two eigenvectors, in this case every element has the same eigenvectors, which means that the matrices form a cyclic group. By the correspondence between Cartan subgroups and eigenvectors, every element of $G$ must lie in the same Cartan subgroup of $GL_2(\mathbb{F}_l)$.
Let $\nu = 3$ and assume we are in the general case of $H$ even. If $H > 4$, the Orbit-Stabiliser Lemma implies that the orbit of $\xi_3$ has size 2. Thus $H$ has a cyclic subgroup, say $H_0$, of index 2, so $H_0$ is normal. The preimage of $H_0$ in $GL_2(\mathbb{F}_l)$ must be contained in a Cartan subgroup, since its elements are semi-simple and commute. The remaining elements of $G$ must interchange the two eigenvectors of the orbit of $\xi_3$, since otherwise they would map to $H_0$. One can then see that conjugation of $H_0$ by one of these elements fixes $H_0$; so G is contained in the normaliser of a Cartan subgroup, but not in the Cartan subgroup itself. [pretty sure this works for h=4; sd says need a 'similar argument']
In case (i) above, $H$ permutes the $|O(\xi_3)| = 12/3 = 4$ elements of the orbit of $\xi_3$. This action is faithful, since each non-identity element has only two eigenvectors, so cannot fix all elements of $O(\xi_3)$. This means $H$ injects into $S_4$ and has order 12, so must be isomorphic to $A_4$.
In case (ii), no element of order three can be in the stabiliser of a representative of the orbits of $\xi_1$ or $\xi_3$, since their orders are powers of two. So all elements of order three must have their eigenvectors in the orbit of $\xi_2$.

$\mu_2 = 3$, so two non-identity elements fix each element of $O(\xi_2)$, and since two elements sharing an eigenvector implies they share both eigenvectors, we can pair up each element of $O(\xi_2)$ with the other eigenvector fixed by the elements that fix that eigenvector, resulting in four pairs. If a non-trivial element of $H$, say $\alpha$, fixed all four pairs, it would have order two because(?). Then since the $O(\xi_2)$ is the collection of eigenvectors of elements of $H$ of order 3, no element of $O(\xi_2)$ is an eigenvector of $\alpha$, so it must interchange the elements of each pair. Then it would commute with the elements in the stabiliser of $\xi_2$, which have order 3. Call one of these stabilising elements $a$.Then $a\alpha \in H$ would have order 6 - but $H$ has no elements of order 6, so no such $\alpha$ exists. We have found that $H$ acting as permutations on the four pairs has trivial kernel, and so $H \cong S_4$.
In case (iii), each stabiliser has prime order, so each element of $H$ has prime order. Since two eigenvectors associated to elements of the same order are equivalent under $H$(?), we must have that any two cyclic subgroups of the same order are conjugate. Thus any proper normal subgroup contains all the elements of a given order. By applying the Sylow theorems, we deduce that there are 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2. Since the order of a subgroup divides the order of a group, counting the possible orders of normal subgroups yields only the trivial subgroup. Thus $H$ is simple, and must be isomorphic to $A_5$, which is the only simple group of order 60. □

**Corollary 8.** *Let $\rho_l$ be a continuous homomorphism $Gal(K_l/\mathbb{Q}) \to GL_2(\mathbb{Z}_l)$ such that $det \circ \rho_l = \chi_l^{k-1}$ for some even $k$. Let $G \subset GL_2(\mathbb{F}_l)$ be the image of $\tilde{\rho}_l$ and let $H$ be the image of $G$ in $PGL_2(\mathbb{F}_l)$. If $G$ does not contain $SL_2(\mathbb{F}_l)$, then either*

(i) *$G$ is contained in a Borel subgroup of $GL_2(\mathbb{F}_l)$, or*

(ii) *$G$ is contained in the normalizer of a Cartan subgroup, but not in the Cartan subgroup itself, or*

(iii) *$H \cong S_4$.*

*Proof.* A subgroup of a split Cartan subgroup with eigenspaces $W_1$ and $W_2$, say, is a subgroup of the Borel subgroups corresponding to either $W_1$ or $W_2$. If we deal with the case of a non-split Cartan subgroup, and show that $H \ncong A_4$ or $A_5$, then by the above lemma we will be done. Let $C$ be a non-split Cartan subgroup, so $C \cong \mathbb{Z}/(l^2-1)\mathbb{Z}$. Since $C$ is commutative, the homomorphism

$Gal\left(K_l/\mathbb{Q}\right) \to C$ must factor through $Gal\left(K_l^{ab}/\mathbb{Q}\right)$. Recall from Lemma 16 that $Gal\left(K_l^{ab}/\mathbb{Q}\right) \cong \mathbb{Z}_l^*$, which has order prime to $l$. Combining this with $C \cong \mathbb{Z}/(l^2-1)\mathbb{Z}$, we find that the order of $\mathbb{Z}_l^*$ must divide $l-1$, and so its image must lie in the set of scalar matrices, and hence in a Borel subgroup. Thus the non-split case is covered by (i).
Now let $l > 2$. We obtain the following commutative diagram

$$\begin{tikzcd}
Gal\left(K_l/\mathbb{Q}\right) \arrow[r] & G \arrow[r, "det"] \arrow[d] & \mathbb{F}_l^* \arrow[d] \\
 & H \arrow[r] & \mathbb{F}_l^*/\left(\mathbb{F}_l^*\right)^2
\end{tikzcd}$$

We assumed that the image of $G$ is $(k-1)$th powers in $\mathbb{F}_l^*$ and that $k$ is even. Then $H$ surjects onto $\mathbb{F}_l^*/\left(\mathbb{F}_l^*\right)^2$, since the image of $H$ maps to elements of $\mathbb{F}_l^*$ that are not even powers. Since there are $\frac{l-1}{2}$ quadratic residues mod $l$, we have $\mathbb{F}_l^*/\left(\mathbb{F}_l^*\right)^2 \cong \mathbb{Z}/2\mathbb{Z}$, which implies $H$ has a subgroup of order 2 - but neither $A_4$ nor $A_5$ have such a subgroup. □

**Corollary 9.** *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight $k$ with $a_1 = 1$ and integer coefficients, with a Dirichlet series that has an Euler product, as in Theorem 20. Also, let $\rho_l$ be as in the theorem. If the image of $\tilde{\rho}_l$ does not contain $SL_2\left(\mathbb{F}_l\right)$ (so $l$ is an exceptional prime for $f$), then we have the following congruences for the coefficients of $f$:*

(i) *$\exists m \in \mathbb{Z}$ such that*

$$a_n = n^m \sigma_{k-1-2m}(n) \ mod\ l,$$

*for all n prime to l,*

(ii) *$a_n \equiv 0$ mod l, whenever n is a quadratic non-residue mod l, and*

(iii) *$p^{1-k} a_p^2 \equiv$ 0, 1, 2, or 4 mod l for all primes $p \neq l$.*

*Each case follows from the corresponding section of the preceding corollary.*

*Proof.* (i) Without loss of generality, assume that the Borel subgroup involved consists of the non-singular upper triangular matrices, so that for a general element $\sigma$ of $Gal\left(K_l/\mathbb{Q}\right)$ we have

$$\tilde{\rho}_l(\sigma) = \begin{pmatrix} \alpha(\sigma) & \beta(\sigma) \\ 0 & \delta(\sigma) \end{pmatrix}$$

$\alpha$ is a continuous homomorphism $Gal\big(K_l/\mathbb{Q}\big) \to \mathbb{F}_l^*$, so we must have $\alpha = \tilde{\chi}_l^m$ for some $m \in \mathbb{Z}$. Furthermore, note that

$$\alpha\delta = det \circ \tilde{\rho}_l(\sigma) = \tilde{\chi}_l^{k-1}$$

by Theorem 20, which implies that $\delta = \tilde{\chi}_l^{k-1-m}$. Plugging in $Frob_p$ for $\sigma$ and using (16) and (17), we see that

$$\begin{aligned}\tilde{a}_p &= tr(\tilde{\rho}_l(Frob_p)) = \alpha(Frob_p) + \delta(Frob_p)\\ &= \tilde{\chi}_l^m(Frob_p) + \tilde{\chi}_l^{k-1-m}(Frob_p)\\ &= p^m + p^{k-1-m}, \qquad (19)\end{aligned}$$

i.e. $a_p \equiv p^m + p^{k-1-m} \bmod l$ for $p \neq l$. The result follows from the relation between the Dirichlet series and the Euler product.

(ii) Since every element of $GL_2(\mathbb{F}_2)$ is contained in a Borel or Cartan subgroup, assume $l > 2$. Denote by $C$ a Cartan subgroup and by $N$ its normaliser. We have a homomorphism

$$Gal\big(K_l/\mathbb{Q}\big) \to N \to N/C,$$

and by our third remark on Cartan subgroups, we have $N/C \cong \mathbb{Z}/2\mathbb{Z}$. Since $G$ is contained in the normalizer of a Cartan subgroup, but not in the Cartan subgroup itself, the above homomorphism is surjective. $Gal\big(K_l/\mathbb{Q}\big)$ must factor through $Gal\big(K_l^{ab}/\mathbb{Q}\big)$ since $\mathbb{Z}/2\mathbb{Z}$ is commutative. Recall that $Gal\big(K_l^{ab}/\mathbb{Q}\big) \cong \mathbb{Z}_l^*$, and that the only continuous homomorphism from $\mathbb{Z}_l^*$ onto $\mathbb{Z}/2\mathbb{Z}$ has kernel consisting of the squares. Thus we obtain that $\tilde{\rho}_l(Frob_p) \in C \Leftrightarrow$ p is a quadratic residue mod $l$. If $\alpha \in N \setminus C$, so p is a quadratic non-residue, it swaps the associated eigenspaces of $C$, so can be put in the form $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$, which has zero trace. The result follows by (17).

(iii) In this case $H \cong S_4$, so every element has order 1, 2, 3, or 4. We can then write the eigenvalues of an element of $H$ as $\mu, \mu^{-1}$, where $\mu$ is a 2nd, 4th, 6th, or 8th root of unity respectively(?why not as 1st, 2nd, 3rd, 4th ro1? doesnt his way give a sign ambiguity? i suppose it doesnt matter much). Then an element of $G$ has eigenvalues $\lambda\mu, \lambda\mu^{-1}$. We now check the various cases:

(a) Let $\mu^2 = 1$. Then the characteristic polynomial, $f(x)$, has repeated root $-\lambda$, so $f(x) = x^2 + 2\lambda x + \lambda^2$. From this and (17) we obtain the congruences $p^{k-1} \equiv \lambda^2 \bmod l$ and $a_p \equiv -2\lambda \bmod l$. Thus $a_p^2 \equiv 4\lambda^2 \bmod l$, and so $a_p^2 p^{1-k} \equiv 4 \bmod l$.

(b) Let $\mu^4 = 1$. If $\mu^2 = 1$, we are back at case (a), so let $\mu^2 = -1$. Then $f(x)$ has roots $\lambda\mu, -\lambda\mu$ and we have $f(x) = x^2 + \lambda^2$. Similarly as in (a), we get $p^{k-1} \equiv \lambda^2 \bmod l$ and $a_p \equiv 0 \bmod l$. Thus $a_p^2 p^{1-k} \equiv 0 \bmod l$.

(c) Let $\mu^6 = 1$; either $\mu^3 = 1$ or $\mu^3 = -1$. If $\mu^3 = 1$, we end up with roots $\lambda\mu, \lambda\mu^2$ and $f(x) = x^2 + \lambda x + \lambda^2$. The congruences $p^{k-1} \equiv \lambda^2 \bmod l$ and $a_p \equiv -\lambda \bmod l$ result. Thus $a_p^2 \equiv \lambda^2 \bmod l$, and so $a_p^2 p^{1-k} \equiv 1 \bmod l$.
If $\mu^3 = -1$, $f(x)$ has roots $\lambda\mu, -\lambda\mu^2$, and we have $f(x) = x^2 - \lambda x + \lambda^2$. This time, our congruences are $p^{k-1} \equiv \lambda^2 \bmod l$ and $a_p \equiv \lambda \bmod l$. Thus $a_p^2 \equiv \lambda^2 \bmod l$, and again we find $a_p^2 p^{1-k} \equiv 1 \bmod l$.

(d) Let $\mu^8 = 1$. If $\mu^4 = 1$ we are back in case (b), so let $\mu^4 = -1$. Then $\mu^2 = i$ or $-i$. We obtain $f(x) = x^2 - \lambda x(\mu + \mu^7) + \lambda^2$. The congruences are $p^{k-1} \equiv \lambda^2 \bmod l$ and $a_p \equiv \lambda(\mu + \mu^7) \bmod l$. Thus $a_p^2 \equiv \lambda^2(\mu^2 + \mu^6 + 2) \equiv \lambda^2(\mu^2 + \mu^{-2} + 2) \equiv 2\lambda^2 \bmod l$, and so we find $a_p^2 p^{1-k} \equiv 2 \bmod l$.

□

## 4.3 The Exceptional Primes

Corollary 9 shows us that for exceptional primes there exist congruences on the coefficients of modular forms; but are there similar congruences for non-exceptional primes?

**Lemma 19.** *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight $k$ with $a_1 = 1$ and integer coefficients, with a Dirichlet series that has an Euler product. If $l$ is not exceptional for $f$, and $N, N^*$ are non-empty open sets in $\mathbb{Z}_l, \mathbb{Z}_l^*$ respectively, then $\{p \text{ prime} \mid p \in N^* \text{ and } a_p \in N\}$ has positive density.*

*Proof.* Consider the map

$$(\rho_l, \chi_l) : Gal(K_l/\mathbb{Q}) \to GL_2(\mathbb{Z}_l) \times \mathbb{Z}_l^*$$

The projection onto $GL_2(\mathbb{Z}_l)$ contains $SL_2(\mathbb{Z}_l)$ since $l$ is not exceptional. Then the projection onto $GL_2(\mathbb{Z}_l)$ of the commutator subgroup contains the commutator subgroup of $SL_2(\mathbb{Z}_l)$. Let $l > 3$. The commutator subgroup of $SL_2(\mathbb{F}_l)$ is normal in $SL_2(\mathbb{F}_l)$, which is simple, so the commutator subgroup is the whole of $SL_2(\mathbb{F}_l)$. Then by Theorem 21, the commutator subgroup of $SL_2(\mathbb{Z}_l)$ contains $SL_2(\mathbb{Z}_l)$, and so is the whole of $SL_2(\mathbb{Z}_l)$. If $l = 2$ or 3, let $\sigma \in Gal(K_l/\mathbb{Q})$ such that $\rho_l(\sigma) \in SL_2(\mathbb{Z}_l)$. We then have $\chi_l^{k-1}(\sigma) = det \circ \rho_l(\sigma) = 1$. Since $k$ is even, $\chi_l(\sigma) = 1$ as $\mathbb{Z}_l$ contains no non-trivial roots of unity of odd order. Thus $SL_2(\mathbb{Z}_l) \times 1$ is contained in the image of $(\rho_l, \chi_l)$. □

From now on we assume $f$ and $\rho_l$ are as in Theorem 20, and that $l$ is exceptional for $f$. We use the following lemma to restrict the number of primes for which each part of Corollary 9 can occur:

**Lemma 20.** *Congruences as in* (i) *can only occur if either* $2m < l < k$ or $m = 0$ *and* $l$ *divides the numerator of* $B_k$, *and* (ii) *can only occur if* $l < 2k$. *In the case of* (iii), *we cannot find the specific primes themselves, but we can find a finite set of primes guaranteed to contain all exceptional primes.*

*Proof.* Let $l > 3$. Recall (i) was the statement that $\exists m \in \mathbb{Z}$ such that

$$a_n = n^m \sigma_{k-1-2m}(n) \bmod l, \tag{20}$$

for all $n$ prime to $l$. It suffices to consider $a_p \equiv p^m + p^{k-1-m} \bmod l$ for $p \neq l$. Here the exponents depend on their value mod $l-1$, so reducing them (and possibly switching them) we obtain

$$a_p \equiv p^m + p^{m'} \bmod l,$$

with $0 \leq m < m' < l-1$ and $m + m' \equiv k-1 \bmod l$. Since $k-1$ is odd, $m + m'$ is odd and hence $m \neq m'$. Applying this to (20) we find that $a_n \equiv n^m \sigma_{m'-m}(n) \bmod l$, if $n$ is coprime to $l$. Thus we can write

$$\theta \tilde{f} = \theta^{m+1} \tilde{G}_{m'-m+1}, \tag{21}$$

noting that the terms involving powers of $n$, where $l|n$, disappear. This formula breaks down in the instance of $m = 0, m' = l-2$, since the constant term of $G_{l-1}$ is not reducible by $l$. Note, however, that by Lemma (3) the constant term of $G_{l-1}$ multiplied by $l$ *is* reducible mod l. Using $a_p \equiv$

$p^m + p^{k-1-m} \bmod l$, we obtain $pa_p \equiv 1 + p \bmod l$, and the congruence $na_n \equiv \sigma_1(n) \bmod l$ follows, where $l$ and $n$ are coprime. We can then write

$$\theta \tilde{f} = \theta^{l-1}\tilde{G}_2 = \theta^{l-1}\tilde{G}_{l+1}. \tag{22}$$

Recall $w(\theta \tilde{f}) \leq w(\tilde{f}) + l + 1$. If $3 < k < l-1$, we must have $w(\tilde{G}_k) = k$, so for $m' - m > 1$ we have

$$w(\theta^{m+1}\tilde{G}_{m'-m+1}) = m' - m + 1 + (m+1)(l+1)$$

Comparing this with the left, we find

$$m' - m + 1 + (m+1)(l+1) \leq k + l + 1, i.e.$$
$$m' + ml + 1 \leq k$$

if $1 < m' - m < l - 2$. If we have $k < l$, we must have $k - 1 \leq m + m'$. Combining this with our discussion of the filtration, we get $k-1 \leq m+m' \leq ml + m' \leq k-1$, and so must have $m = 0$, $m' = k-1$, and $w(\tilde{f}) = k$. Plugging these into (21) we obtain $\theta(\tilde{f} - \tilde{G}_k) = 0$. Then $\tilde{f} - \tilde{G}_k = 0$ or has filtration $k > 0$. If it has filtration $k$, we obtain (is the filtration of 0 0 or -inf?) $0 = w(\theta(\tilde{f} - \tilde{G}_k)) = w(\tilde{f} - \tilde{G}_k) + l + 1 = k + l + 1$, which is a contradiction as $k$ and $l$ are non-zero. So $l$ divides the constant term of $f - G_k$, and since $f$ is a cusp form, $l$ must divide the numerator of $B_k$.
There are two exceptions left to consider: those of $m' - m = 1$, and $m = 0, m' = l - 2$. Since there are no modular forms of weight two, in the first of these cases we must have $w(\tilde{G}_{m'-m+1}) = w(\tilde{G}_2) = l + 1$. Similarly to before, taking the filtration of either side of (21) we find $(m+1)(l+1) \leq k$, if $m' - m = 1$. For the second case, from (22) we find that $l^2 - 1 \leq k$, if $m = 0, m' = l - 2$. In either instance, we must have $l < k$.
For the second case, that of $a_n \equiv 0$ for $n$ a quadratic non-residue mod $l$, observe that $n^{\frac{l-1}{2}} \equiv 1 \bmod l$ if and only if $n$ is a quadratic residue mod $l$. We can then express this case in terms of the theta operator as follows:

$$\theta \tilde{f} = \theta^{\frac{l+1}{2}} \tilde{f}$$

If $l > 2k$, we must have $w(\tilde{f}) = k(why?)$. Then the left hand side of the above equation has filtration $k + l + 1$, while the right hand side has filtration $k + \frac{1}{2}(l+1)^2$. These are not equal for any primes, so we have obtained a contradiction. Finally, $l \neq 2k$, since $k$ is even and $l$ is odd.

Case (iii) stipulates that $p^{1-k}a_p^2 \equiv 0, 1, 2,$ or 4 mod $l$ for all primes $p \neq l$. Pick $p > 2$ such that $a_p \neq 0$. If $l$ is such an exceptional prime, we must have $l = p$ or one that of the following is divisible by $l$: $a_p^2, a_p^2 - p^{k-1}, a_p^2 - 2p^{k-1}$, or $a_p^2 - 4p^{k-1}$. Since $k$ is even, these are all non-zero and finite, so there is a finite number of divisors and hence one obtains a finite list which contains all exceptional primes. □

We are finally able to classify the exceptional primes of each type, for cusp forms satisfying the constraints of Theorem 20. There are six (known) such forms: $\Delta, Q\Delta, R\Delta, Q^2\Delta, QR\Delta$, and $Q^2R\Delta$, which have weights 12, 16, 18, 20, 22, and 26 respectively.
For type (i) exceptional primes, the results can be expressed in a table, which lists the value of $m$ for a given modular form and fixed choice of $l$:

| Form | k | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | Other |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\Delta$ | 12 | 0 | 0 | 1 | 1 | - | | | | | 691 |
| $Q\Delta$ | 16 | 0 | 0 | 1 | 1 | 1 | - | | | | 3617 |
| $R\Delta$ | 18 | 0 | 0 | 2 | 1 | 1 | 1 | - | | | 43867 |
| $Q^2\Delta$ | 20 | 0 | 0 | 1 | 2 | 1 | 1 | - | - | | 283,617 |
| QRΔ | 22 | 0 | 0 | 2 | 1 | - | 1 | 1 | - | | 131,593 |
| $Q^2R\Delta$ | 26 | 0 | 0 | 2 | 2 | 1 | - | 1 | 1 | - | 657,931 |

The $k = 2$ column follows as the coefficients $a_p$ (where $p$ is prime) of $\Delta$ are even. When $l = 3$, we make use of the property of the tau function noted in [**lehmer**], that if $n$ and 3 are coprime, then $\tau(n) \equiv \sigma(n)$ mod 3. Plugging in $p \neq 3$, we see that $a_p = \tau(p) \equiv 1 + p$ mod 3, and so must have $m = 0$. Theorem (4) implies this for the rest of the column. For the remaining cases where $l < k$, one proceeds as follows: take, for example, the form $\Delta$ and $l = 5$, and consider $p = 2$. We have $a_2 = -24$, and so (19) implies

$$-24 \equiv 2^m + 2^{12-1-m} \text{ mod } 5,$$

which simplifies to

$$1 \equiv 2^m + 2^{3-m} \text{ mod } 5.$$

Following the constraints applied in Lemma (20) (i), plug in values of $m$ satisfying $0 \leq m < m' \leq 3$, and after possibly adjusting the congruence to have the required form, one finds that 1 is the only value of m satisfying the congruence. This method works similarly for $l < k$ with small primes $p$, and also shows whether there are no such values $m$. It remains to check that these values do indeed hold for the stated cusp forms. This is done by using (21) as follows: let us continue the example of $\delta$. (here sd says to check the equation in thetas for values in the table - why? have we not just found the values of m?).

There are only two type (ii) primes: $\Delta$ has exceptional prime $l = 23$, and $Q\Delta$ has exceptional prime $l = 31$. The previous lemma indicates $l < 2k$, so we need to check $l < 2k$ such that $l$ isn't type (i), and also $l = 2k - 3$ and $l = 2k - 1$.