Ribet’s construction of a suitable cusp eigenform

Anupam Saikia

Department of Mathematics, IIT Guwahati,
Guwahati 781039.
Email: a.saikia@iitg.ernet.in

Abstract: The aim of this article to give a self-contained exposition on Ribet’s construction of a cusp eigenform of weight 2 with certain congruence properties for its eigenvalues.

Acknowledgement: I am very grateful to Kevin Buzzard for pointing out errors in an earlier version.

1 Preliminaries

We begin by recalling some of the rudiments of modular forms. Other basic ingredients are included in the Appendix.

1.1 Modular forms

Let \( p \) be an odd prime. Let \( \mathfrak{h} \) denote the upper half complex plane, i.e.,

\[ \mathfrak{h} = \{ z \in \mathbb{C} \mid \text{Im}(z) > 0 \}. \]

Let \( SL_2(\mathbb{Z}) \), \( \Gamma_0(p) \) and \( \Gamma_1(p) \) respectively denote the following groups:

\[
SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}, \ ad - bc = 1 \right\}
\]

\[
\Gamma_0(p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \text{ modulo } p \right\},
\]

\[
\Gamma_1(p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(p) \mid a \equiv 1 \text{ modulo } p, \ d \equiv 1 \text{ modulo } p \right\},
\]

Let \( GL_2(\mathbb{Q}) \) (\( GL_2(\mathbb{R}) \)) denote the 2×2 invertible matrices with rational (real) coefficients. It is easy to note all these matrix groups act on \( \mathfrak{h} \) by sending \( z \) to \( \frac{az + b}{cz + d} \). For a function \( f : \mathfrak{h} \to \mathbb{C} \) and any fixed integer \( k \geq 0 \), we can define a function \( f[\gamma]_k \) as

\[
f[\gamma]_k(z) = (cz + d)^{-k} f(\gamma(z)) \quad \forall \ \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Q}).
\]
A function \( f : \mathfrak{h} \rightarrow \mathbb{C} \) is called \textit{weakly modular} of weight \( k \) with respect to \( \Gamma \) if \( f[\gamma]_k = f \) for all \( \gamma \in \Gamma \) where \( \Gamma \) can mean anyone of \( SL_2(\mathbb{Z}) \), \( \Gamma_0(p) \) or \( \Gamma_1(p) \). It is clear that \( \left[ \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right] \in \Gamma \) and hence we must have \( f(z + 1) = f(z) \) for a weakly modular function. If \( f \) is holomorphic on \( \mathfrak{h} \), we can look at the Fourier expansion of \( f \) in terms of \( q = e^{2\pi iz} \), i.e., \( \sum_{n=-\infty}^{+\infty} a_n q^n \). We say \( f \) is holomorphic at \( \infty \) if its \( q \)-expansion does not involve negative powers of \( q \), i.e., \( a_n = 0 \) for \( n < 0 \). If \( a_n = 0 \) for \( n \leq 0 \), then we say that \( f \) vanishes at \( \infty \). Note that \( q = e^{2\pi iz} \rightarrow 0 \) as \( \text{Im}(z) \rightarrow \infty \), justifying the terminology.

We say that \( f \) is a modular form of weight \( k \) with respect to \( \Gamma \) if

(i) \( f \) is weakly modular of weight \( k \) with respect to \( \Gamma \).

(ii) \( f \) is holomorphic on \( \mathfrak{h} \).

(iii) \( f[\gamma]_k \) is holomorphic at \( \infty \) for all \( \gamma \in SL_2(\mathbb{Z}) \).

(iv) If, in addition, the \( q \)-expansion of \( f[\gamma]_k \) has \( a(0) = 0 \) for all \( \gamma \in \Gamma \), then \( f \) is said to be a cusp form.

Note that it is enough to check the last two conditions for a finite number of coset representatives \( \{\alpha_i\} \) of \( \Gamma \) in \( SL_2(\mathbb{Z}) \). The set \( \{\alpha_i(\infty)\} \) is known as the \textit{cusps} of \( \Gamma \). Let us denote the space of all modular forms (cusp forms) of weight \( k \) for \( \Gamma \) by \( M_k(\Gamma) \) (\( S_k(\Gamma) \) respectively). These turn out to be finite dimensional vector spaces. The quotient vector space of \( M_k(\Gamma) \) by \( S_k(\Gamma) \) is known as the Eisenstein space, denoted by \( E_k(\Gamma) \). It can be identified as the orthogonal complement of \( S_k(\Gamma) \) under Petersson inner product, and hence can be thought of as a subspace of \( M_k(\Gamma) \) (see section 6.6 of Appendix).

### 1.2 Semi-cusp forms

**Definition 1.1** A \textit{semi-cusp form} \( f \) is a modular form whose leading Fourier coefficient is 0, though \( f[\gamma]_k \) need not have its leading Fourier coefficient 0 for all \( \gamma \in SL_2(\mathbb{Z}) \). In other words, a semi-cusp form vanishes at \( \infty \), but it need not vanish at the other ‘cusps’. We shall denote the space of semi-cusp forms of \( \Gamma \) by \( S'_k(\Gamma) \).

Consider the map

\[
\beta : \Gamma_0(p) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times, \quad \gamma = \left[ \begin{array}{cc} a & b \\ c & d \end{array} \right] \mapsto d \mod p.
\]

(Note that \( (d, p) = 1 \) for \( \gamma \in \Gamma_0(p) \) as \( ad - bc = 1 \) and \( p|c \)). Clearly, \( \Gamma_1(p) \) is the kernel of \( \beta \), and the quotient is \( (\mathbb{Z}/p\mathbb{Z})^\times \). For a character \( \epsilon \) of \( (\mathbb{Z}/p\mathbb{Z})^\times \), we can define a subspace \( M_k(\Gamma_1(p), \epsilon) \) of \( M_k(\Gamma_1(p)) \), which consists of modular forms \( f \) such that \( f[\gamma]_k = \epsilon(d)f \).
for any \( \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(p) \). We can define \( S_k'((\Gamma_1(p), \epsilon)) \) and \( S_k((\Gamma_1(p), \epsilon)) \) analogously. Note that any character of \( \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \) is of the form \( w^i, i = 0, 1, \ldots, (p-2) \) where \( w \) is the Teichmüller character (see section 6.5 Appendix).

### 1.3 Examples of modular forms

For a non-trivial even character \( \epsilon \) of \( \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \), we have the following Eisenstein series of weight 2 and type \( \epsilon \) (cf chapter 4 of [Di-S]):

\[
G_{2,\epsilon} = \frac{L(-1, \epsilon)}{2} + \sum_{n \geq 1} \sum_{d|n} \epsilon(d) dq^n, \quad (1)
\]

\[
s_{2,\epsilon} = \sum_{n \geq 1} \sum_{d|n} \epsilon\left(\frac{n}{d}\right) dq^n. \quad (2)
\]

These two form a basis for the Eisenstein space \( E_2((\Gamma_1(p), \epsilon)) \) (cf theorem 4.6.2 [Di-S]). Note that \( s_{2,\epsilon} \) is a semi-cusp form. Moreover, both of these are eigenvectors for all Hecke operators \( T_l \) with \( (l, p) = 1 \) (cf proposition 5.2.3 [Di-S]):

\[ T_l s_{2,\epsilon} = (l + \epsilon(l)) s_{2,\epsilon}, \quad T_l G_{2,\epsilon} = (1 + \epsilon(l)l) G_{2,\epsilon}. \]

(See section 6.7 of the Appendix for Hecke operators.)

If \( \epsilon \) is an odd character of \( \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \), we have an Eisenstein series of weight 1 and type \( \epsilon \) given by (cf section 4.8 in [Di-S])

\[ G_{1,\epsilon} = \frac{L(0, \epsilon)}{2} + \sum_{n \geq 1} \sum_{d|n} \epsilon(d) q^n. \]

The above three forms have coefficients defined over \( \mathbb{Q}(\mu_{p-1}) \), where \( \mu_{p-1} \) denotes the \((p-1)^{th}\) roots of 1. Let \( \wp \) denote any of the unramified primes of \( \mathbb{Q}(\mu_{p-1}) \) lying above \( p \). Clearly, all the Eisenstein forms given above have \( \wp \) integral coefficients (except possibly for the constant terms, but see lemma 3.1 later).

For the trivial character \( \epsilon = 1 \), we have the following Eisenstein series (cf Theorem 4.6.2 in [Di-S]) in \( M_k(\Gamma_0(p)) = M_k(\Gamma_1(p), 1) \):

\[
G_k = -\frac{B_k}{2k} + \sum_{n \geq 1} \sum_{d|n} d^{k-1} q^n \quad \text{for } k \geq 4, \quad (3)
\]

\[
G_2 = E_2(z) - p E_2(pz), \quad \text{where } E_2(z) = -\frac{B_2}{4} + \sum_{n \geq 1} \sum_{d|n} dq^n, \quad (4)
\]
2 Key steps in the construction of the unramified \( p \)-extension

For Ribet’s construction of an unramified extension of \( \mathbb{Q}(\mu_p) \), one requires a Galois representation on which the Frobenius elements act in a suitable way (see [D]). We can use the representation associated with a cusp eigenform (cf chapter 9 of [Di-S]). But we need to show that there indeed exists a cusp eigenform whose eigenvalues have certain congruence properties.

The Eisenstein series \( G_{2,\epsilon} \) is a simultaneous eigenform for the Hecke operators \( T_l \) where \( l \) is a prime other than \( p \), with corresponding eigenvalues \( 1 + \epsilon(l)l \equiv 1 + l^{k-1} \) modulo \( \varphi \). Here, \( \varphi \) denotes a prime of \( \mathbb{Q}(\mu_{p-1}) \) lying above \( p \). It turns out that we need precisely these congruence properties for the Hecke eigenvalues of a cusp form. Ribet’s idea is to subtract off the constant term of the Eisenstein series \( G_{2,\epsilon} \) in a way that preserves the congruence properties of the coefficients and leaves us with a semi-cusp form \( f \) which is an eigenvector modulo \( \varphi \) for all Hecke operators \( T_l \) with \( (l, p) = 1 \). Then one can invoke a result of Deligne and Serre and obtain a semi-cusp form \( f' \) which is also an eigenvector for the \( T_l \)’s with eigenvalues congruent to those of \( f \) modulo \( \varphi \). The congruence properties of \( f' \) then ensures that \( f' \) is actually a cusp form. Any cusp form in \( S_2(\Gamma_1(p)) \) is bound to be a newform. Thus, one can invoke the theory of newforms to conclude that \( f' \) is in fact a cusp eigenform, that is, an eigenvector for all Hecke operators including \( T_n \)'s with \( p|n \).

To remove the constant term of the Eisenstein series \( G_{2,\epsilon} \) without affecting the congruence properties of its coefficients modulo \( \varphi \), it suffices to produce another Eisenstein series whose constant term is a \( \varphi \)-unit. This will be done in the next section.

3 Construction of an Eisenstein series with \( \varphi \)-unit constant term

As before, we will denote by \( \varphi \) a prime of \( \mathbb{Q}(\mu_{p-1}) \) lying above \( p \). Note that \( \varphi \) is unramified. We continue to denote the Teichmuller character by \( w \).

Lemma 3.1 Let \( k \) be even and \( 2 \leq k \leq p - 3 \). Then the \( q \)-expansions of the modular forms \( G_{2,w^{k-2}} \) and \( G_{1,w^{k-1}} \) have \( \varphi \)-integral coefficients in \( \mathbb{Q}(\mu_{p-1}) \) and are congruent modulo \( \varphi \) to the \( q \)-expansion

\[
-\frac{B_k}{2k} + \sum_{n \geq 1} \sum_{d|n} d^{k-1} q^n.
\]
Proof: Since \( w(d) \equiv d \mod \varphi, \) \( w^{k-2}(d)d \equiv d^{k-1} \mod \varphi \) and \( w^{k-1}(d) \equiv d^{k-1} \mod p. \) Hence it suffices to investigate the constant terms only. We know that (see (6) and (7) of Appendix)

\[
L(0, \epsilon) = \frac{-1}{p} \sum_{n=1}^{p-1} \epsilon(n) \left( n - \frac{p}{2} \right),
\]

\[
L(-1, \epsilon) = \frac{-1}{2p} \sum_{n=1}^{p-1} \epsilon(n) \left( n^2 - pn - \frac{p^2}{6} \right).
\]

Since we know that \( w(n) \equiv n^p \mod (\varphi^2) \) (cf section 6.5 of Appendix), we find that

\[
pL(0, wk^1) \equiv -\sum_{n=1}^{p-1} n^{1+p(k-1)} \mod \varphi^2,
\]

\[
pL(-1, w^{k-2}) \equiv -\frac{1}{2} \sum_{n=1}^{p-1} n^{2+p(k-2)} \mod \varphi^2.
\]

Note that \( \sum_{n=1}^{p-1} \epsilon(n)n \equiv 0 \mod \varphi \) when \( \epsilon \) is an even character. Moreover, we know that (see proposition 6.6 of Appendix)

\[
pB_t \equiv \sum_{n=1}^{p-1} n^t \mod p^2.
\]

Therefore, we have

\[
L(0, w^{k-1}) \equiv -\frac{1}{2} B_{1+p(k-1)} \equiv -\frac{1}{2} (1 + p(k - 1)) \frac{B_k}{k} \equiv -\frac{B_k}{k} \mod \varphi,
\]

\[
L(-1, w^{k-2}) \equiv -\frac{1}{2} B_{2+p(k-2)} \equiv -\frac{1}{2} (2 + p(k - 2)) \frac{B_k}{k} \equiv -\frac{B_k}{k} \mod \varphi.
\]

For the second equivalence of each statement above, we use Kummer congruence as explained in proposition 6.4 in the Appendix. Note that

\[
1 + p(k - 1) = k + (p - 1)(k - 1) \equiv k \mod (p - 1),
\]

\[
2 + p(k - 2) = k + (p - 1)(k - 2) \equiv k \mod (p - 1). \quad \square
\]

The following corollary is now obvious.

**Corollary 3.2** Let \( k \) be even and \( 2 \leq k \leq p - 3. \) Let \( n, m \) be even integers such that \( n + m \equiv k \mod (p - 1) \) and \( 2 \leq n, m \leq p - 3. \) The product \( G_{1,w^{n-1}}G_{1,w^{m-1}} \) is a modular form of weight 2 and type \( w^{k-2} \) whose \( q \)-expansion coefficients are \( \varphi \)-integral in \( \mathbb{Q} \left( \mu_{p-1} \right) \). Its constant term is a \( \varphi \)-adic unit if neither \( B_n \) nor \( B_m \) is divisible by \( p. \)
The next theorem guarantees the existence of the Eisenstein series we are looking for.

**Theorem 3.3** Let $k$ be an even integer $2 \leq k \leq p - 3$. Then there exists a modular form $g$ of weight 2 and type $w^{k-2}$ whose $q$-expansion coefficients are $\varphi$-integers in $\mathbb{Q}(\mu_{p-1})$ and whose constant term is a $\varphi$-unit.

**Proof:**

Case (i) If $p \nmid B_k$, we can take $G_{2,w^{k-2}}$ by lemma 3.1.

Case (ii) If we have a pair of even integers $m, n$ such that $n + m \equiv k \pmod{(p - 1)}$, $2 \leq n, m \leq p - 3$ and $p \nmid B_mB_n$, then we can take $G_{1,w^{n-1}}G_{1,w^{m-1}}$ by corollary 3.2.

Case (iii) Suppose neither of the above two cases are true. W e will show that consequently too many Bernoulli numbers will be $p$-divisible, which will lead to violation of an upper bound for the $p$-part $h_p^\ast$ of the relative class number of $\mathbb{Q}(\mu_p)$. Let $t$ be the number of even integers $n$, $2 \leq n \leq p - 3$ such that $p$ divides $B_n$. It is easy to see that $t \geq \frac{p-1}{4}$ if the cases (i) and (ii) do not arise. But then, $p^t$ must divide $h_p^\ast$ (see section 6.2 of Appendix). However, that contradicts a result of Carlitz, which says that $h_p^\ast < p^{\left(\frac{p-1}{4}\right)}$. Hence we must be in either in case (i) or case (ii). \(\square\)

### 4 Existence of a semi-cusp form with suitable eigenvalues

In this section, we will first construct a semi-cusp form $f$ which is a simultaneous eigenvector modulo $\varphi$ for all Hecke operators $T_l$ with $(p, l) = 1$. Then we will lift $f$ to a semi-cusp form $f'$ which is an eigenvector for all such $T_l$'s.

Fix an even integer $k$, $2 \leq k \leq p - 3$ and assume that $p|B_k$. Consider $\epsilon = w^{k-2}$. Since $B_2 = \frac{1}{6}$, $k$ is at least 4, and hence $\epsilon$ is a non-trivial even character. We will only be interested in modular forms of weight 2 and type $\epsilon$.

**Proposition 4.1** There exists a semi-cusp form $f = \sum_{n \geq 1} a_n q^n$ such that $a_n$ are $\varphi$-integers in $\mathbb{Q}(\mu_{p-1})$ and such that $f \equiv G_{2,\epsilon} \equiv G_k \mod \varphi$.

**Proof:** Consider $f = G_{2,\epsilon} - c.g$, where $c$ is the constant term of $G_{2,\epsilon}$. Then $f$ is a semi-cusp form. Now, $c \in \varphi$ as $p|B_k$. Hence, $f \equiv G_{2,\epsilon} \equiv G_k \mod \varphi$. \(\square\)

Observe further that $f$ is a mod $\varphi$-eigenform for all Hecke operators $T_l$ with $(l, p) = 1$, as the Eisenstein series $G_{2,\epsilon}$ is an eigenform for all such $T_l$ with eigenvalue $(1 + \epsilon(l))$. Therefore,

$$T_l(f) \equiv T_l(G_{2,\epsilon}) \equiv (1 + \epsilon(l))G_{2,\epsilon} \equiv (1 + \epsilon(l))f \mod \varphi. \quad (5)$$
4.1 Deligne-Serre lifting lemma

The following result of Deligne and Serre [D-S] ensures that there exists a semi-cusp form \( f' \) which is an eigenvector for the \( T_i \)'s ((\( l, p \) = 1) with eigenvalues congruent modulo \( \varphi \) to those of the mod-\( \varphi \) eigenvector \( f \) obtained previously.

**Lemma 4.2** Let \( M \) be a free module of finite rank over a discrete valuation ring \( R \) with residue field \( k \), fraction field \( K \) and maximal ideal \( m \). Let \( S \) be a (possibly infinite) set of commuting \( R \)-endomorphisms of \( M \). Let \( 0 \neq f \in M \) be an eigenvector modulo \( mm \) for all operators in \( S \), i.e., \( Tf = a_T f \mod mm \forall T \in S \) (\( a_T \in R \)). Then there exists a DVR \( R' \) containing \( R \) with maximal ideal \( m' \) containing \( m \), whose field of fractions \( K' \) is a finite extension of \( K \) and a non-zero vector \( f' \in R' \otimes_R M \) such that \( Tf' = a'_T f' \) for all \( T \in S \) with eigenvalues \( a'_T \) satisfying \( a'_T \equiv a_T \mod m' \).

Proof: Let \( \mathbb{T} \) be the algebra generated by \( S \) over \( R \). Clearly \( \mathbb{T} \in \text{End}_R(M) \). As \( M \) is a free \( R \)-module of finite rank, so is \( \text{End}_R(M) \). Therefore, \( \mathbb{T} \) is also free module of finite rank over \( R \), generated by \( T_1, \ldots, T_r \in S \). Let \( h_i \) denote the minimal polynomial of \( T_i \) acting on \( K \otimes_R M \). If we adjoin the roots of all such minimal polynomials to \( K \), we get a finite extension \( K' \) of \( K \). The integral closure of \( R \) in \( K' \) gives us a DVR \( R' \) with maximal ideal \( m' \) lying over \( m \), and with residue field \( k' \) containing \( k \). By replacing \( M \) with \( R' \otimes M \) and \( \mathbb{T} \) with \( R' \otimes_R \mathbb{T} \), we will continue to write \( R, m, k, K \) in stead of \( R', m', k' \) etc.

Consider the ring homomorphism \( \lambda : \mathbb{T} \to k \) given by \( T \mapsto a_T \mod m \) for all \( T \) in \( S \). Clearly, ker(\( \lambda \)) is a maximal ideal of \( \mathbb{T} \). Choose a minimal prime \( \varphi \) in ker(\( \lambda \)). Then, \( \varphi \) is contained in the set of zero-divisors of \( \mathbb{T} \) (see proposition 6.9 of Appendix). As \( \mathbb{T} \) is a free \( R \)-module, \( R \) contains no zero-divisors of \( \mathbb{T} \) and hence, \( p \cap R = \{0\} \). Thus, \( \mathbb{T}/p \) is a finite integral extension of \( R \). Let \( L \) denote the field of fractions of the integral domain \( \mathbb{T}/p \). Let \( R_L \) be the integral closure of \( R \) in \( L \), then \( R_L \) is a DVR with maximal ideal \( m_L \) containing \( m \) and residue field \( l \) containing \( k \).

Consider the map \( \lambda' : \mathbb{T} \to \mathbb{T}/p(\to R_L) \) given by reduction modulo \( p \). Let \( \lambda'(T) = a'_T \) for all \( T \in S \). Clearly, \( \lambda' \) maps the maximal ideal ker(\( \lambda \)) of \( \mathbb{T} \) into the maximal ideal \( m_L \) of \( R_L \). But \( (T - a_T) \in \text{ker}(\lambda) \), hence \( \lambda'(T - a_T) \in m_L \) i.e., \( a'_T \equiv a_T \mod m_L \).

Now consider the ring \( K \otimes_R \mathbb{T} \). It is an Artinian ring, hence it has finitely many maximal ideals with residue fields all isomorphic to \( K \). Let \( P \) be the prime ideal in \( K \otimes \mathbb{T} \) generated by \( p \). It will suffice to show that \( P \) is an associated prime of \( K \otimes M \). Note that \( \varphi \subseteq \text{ker}(\lambda) \) implies \( \varphi \) annihilates \( f \) in \( M/m \). Now let \( x \in \text{Ann}_{\mathbb{T}/m}(f) \), say \( x = g(T_1, \ldots, T_n) \). Then, \( x = \bar{g}(a'_T, \ldots, a'_T) \mod (T_1 - a'_T, \ldots, T_n - a'_T) \). Thus,
Construction of cusp eigenform coefficients in L. Then, we will finally show that the cusp form Kₘ by applying the lifting lemma 4.2, we can conclude that there is a finite extension and (5) that there exists f semi-cusp forms generated by B Kₘ of the ring of integers of K coefficients are defined over a finite extension ℘ integral where B Proof: There is a basis that all its coefficients are defined over a finite extension of L. Theorem 4.3 There is a semi-cusp form associated prime of M/ₘ for all Hecke operators (i) Now, it follows that Annₘ(M/ₘ) ⊂ φ. (ii) Now, it follows that Annₘ(M/ₘ) ⊂ φ. hence P ∈ Suppₘ(K ⊗ M) and therefore P is in Assocₘ(K ⊗ M).

Now, P is the annihilator of some 0 ≠ f'' ∈ K ⊗ M, hence P annihilates some f' ∈ M. As T - aₖ' ∈ p, we have T - aₖ' ∈ P and (T - aₖ')(f') = 0. Thus, Tf' = aₖ'f' where aₖ' ≡ aₖ modulo mₗ, which concludes our proof. □

4.2 Lifting the semi-cusp form to an eigenvector for Tₙ for (n, p) = 1

The following theorem ensures that we have a semi-cusp form which is an eigenvector for all Hecke operators Tₙ with p ∤ n.

Theorem 4.3 There is a semi-cusp form f' = ∑ₘ₌₁ᵃₙqⁿ of weight 2 and type ε such that all its coefficients are defined over a finite extension of L of Q(µ₋₁) and are φₗ-integral where φₗ is a prime above p. Further, Tᵢf' ≡ (1 + ε(l)l)f' modulo φₗ.

Proof: There is a basis B of S₂ₘ(Γₙ(p), ε) consisting of semi-cusp forms all of whose coefficients are defined over a finite extension K of Q(µ₋₁). Let R be the localization of the ring of integers of K at a prime φₖ above φ. Let M be the free R-module of semi-cusp forms generated by B. Let S = {Tₙ(p, n) = 1}. We know by proposition 4.1 and [5] that there exists f ∈ M such that

Tᵢ(f) ≡ (1 + ε(l)l)f modulo φ.

By applying the lifting lemma 4.2, we can conclude that there is a finite extension L of K with a prime φₗ over φₖ such that there exists a semi-cusp form f', with φₗ-integral coefficients in L such that Tᵢ(f') = cᵢf' and cᵢ ≡ 1 + ε(l)l modulo φₗ. □

5 Construction of cusp eigenform

We will first show that the semi-cusp form f' obtained in the previous section is in fact a cusp form. Then, we will finally show that the cusp form f' must be an eigenvector
for all Hecke operators $T_n$ including those $n$ which are not co-prime to $p$.

5.1 Existence of a suitable cusp form

**Proposition 5.1** There exists a non-zero cusp form $f'$ of type $\epsilon$, which is an eigenform for all Hecke operators $T_n$ with $(n,p) = 1$, and which has the property that for any prime $l \neq p$, the eigenvalue $\lambda_l$ of $T_l$ acting on $f'$ satisfies

$$\lambda_l \equiv 1 + l^{k-1} \equiv 1 + \epsilon(l)l \mod \wp_L,$$

where $\wp_L$ is a certain prime (independent of $l$) lying over $\wp$ in the field $L = \mathbb{Q}(\mu_{p-1}, \lambda_n)$ generated by the eigenvalues over $\mathbb{Q}(\mu_{p-1})$.

**Proof:** We already established the existence of a semi-cusp form $f'$ which is an eigenform for all Hecke operators $T_n$ with $(n,p) = 1$ whose eigenvalues have the required congruence properties. It suffices to assert that $f'$ is in fact a cusp form. As $M_2(\Gamma_0(p), \epsilon)$ is spanned by the cusp forms, the semi-cusp form $S_2,\epsilon$ and the Eisenstein series $G_2,\epsilon$, we must have

$$S'_2(\Gamma_1(p), \epsilon) = S_2(\Gamma_1(p), \epsilon) \oplus \mathbb{C}s_2,\epsilon,$$

where orthogonality of the Eisenstein space and the space of cusp forms under Petersson inner product $\langle , \rangle$ is the reason behind the above sum being a direct one (see section 6.6 of Appendix). Suppose $f' = h + as_{2,\epsilon}$ ($a \neq 0$). Then, $f' - as_{2,\epsilon} \in S_2(\Gamma_1(p), \epsilon)$. But, $f' - as_{2,\epsilon} \in E_2(\Gamma_1(p), \epsilon)$ as well, where $E_2(\Gamma_1(p), \epsilon)$ denotes the subspace consisting of Eisenstein series in $M_2(\Gamma_1(p), \epsilon)$. As the orthogonal subspaces $E_2(\Gamma_1(p), \epsilon)$ and $S_2(\Gamma_1(p), \epsilon)$ have trivial intersection, $f' - as_{2,\epsilon} = 0$, i.e., $f' = as_{2,\epsilon}$. Applying $T_l$ to both sides, ($l \neq p$), we see that we must have $1 + \epsilon(l)l \equiv 1 + \epsilon(l) \mod \wp_L$, which forces $\epsilon(l) = 1$.

But $\epsilon$ is a non-trivial character and $l \neq p$ is arbitrary, hence $f'$ must be a cusp form. □

5.2 Operators $T_n$ for $(n,p) \neq 1$

So far, we know that we have a cusp form $f$ for $\Gamma_1(p)$ of weight 2 and type $\epsilon$ which is an eigenform for all Hecke operators $T_l$ ($l,p) = 1$. In this section we will assert that $f$ is in fact a common eigenform for all Hecke operators, including $T_n$ $(n,p) \neq 1$.

**Proposition 5.2** Any form $f'$ as above is an eigenform for all Hecke operators (including those for which $p|n$). Hence, after replacing $f'$ by a suitable multiple of $f'$, we have

$$f' = \sum_{n=1}^{\infty} \lambda_n q^n,$$

where $T_n(f') = \lambda_n f'$. 

9
Proof: $f'$ must be a newform. For, if it were an old form it will have to originate from a non-zero modular form in $M_2(SL_2(\mathbb{Z}))$, but that space is trivial. Now for a new form $f'$, if it is an eigenform for $T_n \ (\gcd(n, p) = 1)$ it has to be an eigenform for all $T_n$ by the theory of newforms (see Theorem 5.8.2 of [Di-S]). Now we can take a suitable multiple of $f'$ to get a normalized cusp eigenform as prescribed in the theorem. □

Remark: The cusp eigenform obtained above can be associated to a Galois representation which finally gives an unramified $p$-extension of $\mathbb{Q}(\mu_p)$, where $\mu_p$ denotes the $p$-power roots of unity for an odd prime $p$. This exposition can be found in [D].

6 Appendix

Here we provide a brief discussion of the various ingredients used in the previous sections.

6.1 Dirichlet $L$-functions

A Dirichlet character is a homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$, where $N$ is any positive integer, and $A^\times$ denote the multiplicative group of units in a ring $A$. $N$ is called the conductor of $\chi$ if $\chi$ does not factor through $(\mathbb{Z}/M\mathbb{Z})^\times$ for any $M < N$. We denote the conductor of $\chi$ by $f_\chi$. We can easily extend the definition of $\chi$ to $\mathbb{Z}$ by setting $\chi(n) = \chi(n \mod N)$ if $(n, N) = 1$ and $\chi(n) = 0$ otherwise. The Dirichlet $L$-series of $\chi$ is defined as

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

where $s$ is a complex number with $\text{Re}(s) > 1$. It is well-known that $L(s, \chi)$ can be analytically continued to the whole complex plane except a simple pole of residue 1 at $s = 1$ when $\chi$ is the trivial character (in which case the function is just the Riemann-zeta function). Further, $L(s, \chi)$ satisfies a functional equation relating its values at $s = 1$ to values $1 - s$. It also has a Euler product, i.e.,

$$L(s, \chi) = \prod_{l}(1 - \chi(l)l^{-s})^{-1}, \quad \text{Re}(s) > 1$$

where $l$ runs over the rational primes. The Dirichlet $L$-functions are related to the Dedekind zeta function of an abelian number field, as explained below.

Recall that for a number field $K$, the Dedekind zeta function is defined as

$$\zeta_K(s) = \sum_a (Na)^{-s}, \quad \text{Re}(s) > 1,$$
where $\alpha$ runs over the ideals of the ring $\mathcal{O}_K$ of integers in $K$. It is well-known that $\zeta_K(s)$ can be analytically continued to the whole complex plane except for a simple pole at $s = 1$. Further, $\zeta_K(s)$ satisfies a functional equation, relating the values at $s$ to values at $1 - s$.

We can view $\chi$ as a Galois character

$$
\chi : \text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times,
$$

and this gives a correspondence $\chi \rightarrow$ fixed subfield of $\ker(\chi)$ in $\mathbb{Q}(\mu_N)$, which is an abelian extension of $\mathbb{Q}$. This leads to a one-to-one correspondence between groups of Dirichlet characters and abelian extensions of $\mathbb{Q}$. If $K$ is an abelian extension of $\mathbb{Q}$, it is contained in some $\mathbb{Q}(\mu_N)$ and there will be a corresponding group $X$ of Dirichlet characters of conductor dividing $N$.

If $K$ is an abelian number field and $X$ is the corresponding group of Dirichlet characters, then one can show that (see theorem 4.3 in [Wa])

$$
\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).
$$

### 6.2 The relative class number and Dirichlet $L$-values

The analytic class number formula is given by

$$
\lim_{s \to 1} \zeta_K(s) = \frac{2^r (2\pi)^t h_K R_K}{w_K \sqrt{|d_K|}},
$$

where $r_K$ and $t_K$ denote respectively the number of real and complex pairs of embedding of $K$, $w_K$ the number of roots of unity in $K$, $R_K$ the regulator of $K$, $d_K$ the discriminant of $K$ and $h_K$ the class number of $K$.

Now consider $K = \mathbb{Q}(\zeta_p)$, then $r_K = 0$, $t_K = \frac{p-1}{2}$. Let $K^+$ be the maximal real subfield of $K$, for which $r_{K^+} = \frac{p-1}{2}$ and $t_{K^+} = 0$. It is easy to establish that $h_{K^+}$ divides $h_K$. The relative class number of $K$ is defined as $h_K^- = \frac{h_K}{h_{K^+}}$. The purpose of this section is to investigate the $p$-part $h_K^-$, and relate it to the values of Dirichlet $L$-functions.

**Proposition 6.1**

$$
h_K^- = \alpha p \prod_{i=0}^{p-2} L(0, w^i),
$$

where $\alpha$ is a certain power of $2$.
Proof: Dividing the analytic class number formulas for \(K\) and \(K^+\), and then shifting the limit to \(s \to 0\) via the functional equations, one can cancel out the extraneous factors and deduce that (see [Gr])

\[
h_K = \frac{w_K}{2^e w_K^+} \lim_{s \to 0} \frac{\zeta_K(s)}{\zeta_{K^+}(s)},
\]

where \(\frac{R_K}{R_{K^+}} = 2^e\). But

\[
\zeta_K(s) = \prod_{i=0}^{\frac{p-2}{2}} L(0, w^i), \quad \zeta_{K^+}(s) = \prod_{i \text{ even}}^{\frac{p-2}{2}} L(0, w^i).
\]

Now observing that \(w_K = 2p\) and \(w_K^+ = 2\), we obtain the desired result. \(\square\)

### 6.3 Dirichlet L-values and Bernoulli numbers

Recall that Bernoulli numbers \(B_n\) are given by

\[
\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.
\]

Eg, \(B_0 = 1\), \(B_1 = -\frac{1}{2}\), \(B_2 = \frac{1}{6}\) etc.

The \(n\)-th Bernoulli polynomial \(B_n(X)\) is defined by

\[
\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X) \frac{t^n}{n!}.
\]

It is easy to see that

\[
B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}.
\]

Eg, \(B_1(X) = X - \frac{1}{2}\), \(B_2(X) = X^2 - X + \frac{1}{6}\), etc.

Now, for a Dirichlet character \(\chi\) of conductor \(f\), we define the generalized Bernoulli numbers \(B_{n,\chi}\) by

\[
\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.
\]

The following well-known proposition allows us to express generalized Bernoulli numbers in terms of Bernoulli polynomials (cf [Wa]).

**Proposition 6.2** If \(g\) is any multiple of \(f\), then

\[
B_{n,\chi} = g^{n-1} \sum_{a=1}^{g} \chi(a) B_{n,\chi} \frac{a}{g}.
\]

12
Proof:
\[\sum_{n=0}^{\infty} g^{n-1} \sum_{a=1}^{g} \chi(a) B_n \left(\frac{a}{g}\right) \frac{t^n}{n!} = \sum_{a=1}^{g} \chi(a) \frac{1}{g} \frac{(gt)^{(a/g)t}}{e^{gt} - 1} \]
\[= \sum_{b=1}^{f} \sum_{c=0}^{h-1} \chi(b + cf) \frac{t e^{(b+cf)t}}{e^{hf t} - 1} \text{ where } g = hf, \ a = b + cf \]
\[= \sum_{b=1}^{f} \chi(b) t e^{ht} \frac{1}{e^{ht} - 1} \]
\[= \sum_{n=0}^{\infty} B_n \chi \frac{t^n}{n!}. \quad \square \]

For example,
\[B_{1,\chi} = \sum_{a=1}^{f} \chi(a) \left(\frac{a}{f} - \frac{1}{2}\right) = \frac{1}{f} \sum_{a=1}^{f} \chi(a) \left(a - \frac{1}{2} f\right). \]
\[B_{2,\chi} = f \sum_{a=1}^{f} \chi(a) \left(\frac{a}{f}^2 - \frac{1}{2} \frac{a}{f} + \frac{1}{6}\right) = \frac{1}{f} \sum_{a=1}^{f} \chi(a) \left(a^2 - fa + \frac{f^2}{6}\right). \]

The generalized Bernoulli numbers can be relate to the values of Dirichlet \(L\)-values as follows:

**Proposition 6.3** \(L(1-n, \chi) = -\frac{B_{n,\chi}}{n}, \ n \geq 1.\)

For example, if \(\chi\) is a Dirichlet character modulo \(p\), we have
\[L(0, \chi) = -B_{1,\chi} = -\frac{1}{p} \sum_{n=1}^{p} \chi(n) \left(n - \frac{1}{2} p\right). \quad (6)\]
\[L(-1, \chi) = -B_{2,\chi} = -\frac{1}{2p} \sum_{n=1}^{p} \chi(a) \left(n^2 - pn + \frac{p^2}{6}\right). \quad (7)\]

### 6.4 Some congruences involving Bernoulli numbers

We require the following congruences involving Bernoulli numbers.

**Proposition 6.4** *(Kummer Congruence)* \(\frac{B_{m,\chi}}{m} \equiv \frac{B_m}{m} \text{ if } m \equiv n \not\equiv 0 \mod (p - 1).\)

Kummer’s congruence can be proved in the following manner (cf [B-S]):

let \(g\) be a primitive root mod \(p\). Consider
\[F(t) = \frac{gt}{e^{gt} - 1} - \frac{t}{e^{t} - 1} = \sum_{m=1}^{\infty} (g^m - 1) B_m \frac{t^m}{m!}. \quad (8)\]
Letting $e^t - 1 = u$, we can write

$$F(t) = \frac{gt}{(1+u)^g - 1} - \frac{t}{u} = tG(u), \text{ where } G(u) = \frac{g}{(1+u)^g - 1} - \frac{1}{u} = \sum_{k=1}^{\infty} c_k u^k, \ c_k \in \mathbb{Z}.$$

Now,

$$G(u) = G(e^t - 1) = \sum_{k=0}^{\infty} c_k (e^t - 1)^k = \sum_{m=1}^{\infty} \frac{A_m t^m}{m!}. \quad (9)$$

But $A_m$ are $p$-integral as they are integral linear combinations of $c_k$'s. Further, they have period $(p-1)$ modulo $p$, as the coefficients $r^n$ of $\frac{t^n}{n!}$ in $e^t$ ($r \geq 0$) have that periodicity by Fermat’s little theorem $r^{n+p-1} \equiv r^n \mod p$. Comparing coefficients in (8) and (9), we obtain

$$\frac{g^m - 1}{m!} B_m = \frac{A_{m-1}}{(m-1)!} \Rightarrow \frac{B_m}{m} (g^m - 1) = A_{m-1}.$$

If $p-1 \nmid m$, then $g^m - 1 \not\equiv 0 \mod p$ as $g$ is a primitive root mod $p$. Clearly, $g^m - 1$ has period $p-1 \mod p$. Therefore, $\frac{B_m}{m}$ also has period $p-1 \mod p$ and is $p$-integral. \qed

**Proposition 6.5** $pB_m$ is $p$-integral, and $B_m$ is $p$-integral if $(p-1) \nmid m$.

**Proposition 6.6** For an even integer $m$, $pB_m \equiv \sum_{a=1}^{p-1} a^m \mod p^2$ if $p \geq 5$.

We can easily prove the above two propositions using the following lemma.

**Lemma 6.7** $(m+1)S_m(n) = \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}$, where $S_m(n) = 1^n + 2^n + \ldots + m^n$.

Proof:

$$\sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!} = \sum_{a=0}^{n-1} e^a t - 1 = e^a e^t - 1 = \sum_{l=1}^{\infty} t^{l-1} \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

$$\Rightarrow S_m(n) \frac{t^m}{m!} = \sum_{k=0}^{m+1} \frac{B_k}{(m+1-k)!} n^{m+1-k}$$

$$\Rightarrow (m+1)! S_m(n) \frac{t^m}{m!} = \sum_{k=0}^{m+1} \binom{m+1}{k} B_k n^{m+1-k} \quad \Box$$

In order to prove proposition 6.5, it is enough to show that $pB_m \equiv S_m(p)$ modulo $p$. It is clear that $S_m(p) \equiv 0 \mod p$ if $(p-1) \nmid m$ and $S_m(p) \equiv p - 1 \mod p$ if $(p-1)|m$. By our lemma, we have

$$S_m(p) = pB_m + \binom{m}{1} B_{m-1} \frac{p^2}{2} + \binom{m}{2} B_{m-2} \frac{p^3}{3} + \ldots + \binom{m}{m} B_0 \frac{p^{k+1}}{k+1}, \quad (10)$$
To prove proposition 6.6, it suffices to establish that \( \text{ord}_p \text{prime} f \) is \( p \)-integral for \( k \geq 2 \), and \( \frac{p^{k+1}}{k+1} \) is \( p \)-integral even for \( k = 1 \). Applying induction, let \( pB_j \) be \( p \)-integral for \( j < m \). Then, \( pB_m \) is \( p \)-integral as well, and we also obtain \( S_m(n) \equiv pB_m \mod p \) from (10). Note that though we need the result only for odd prime \( p \), not that the above proof works for \( p = 2 \) as well, as \( B_n \) vanishes for odd \( n \geq 3 \). □

To prove proposition 6.6, it suffices to establish that \( \text{ord}_p (\binom{m}{k}) B_{m-k} p^{k+1} \geq 2 \) in view of (10). Since \( pB_{m-k} \) is \( p \)-integral, we need only \( k - \text{ord}_p (k+1) \geq 2 \). For \( p \geq 5 \) and \( k \geq 2 \), it is obvious. For \( k = 1 \), note that \( B_{m-1} = 0 \) unless \( m = 2 \), which again follows trivially. □

### 6.5 A refined congruence for the Teichmuller character

Let \( w : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1} \) be the character given by \( w(n) \equiv n \mod \varphi \) where \( \varphi \) is any prime ideal above \( p \) in \( Q(\mu_{p-1}) \). The character \( w \) is known as the Teichmuller character. We have used the following congruence for the Teichmuller character.

**Proposition 6.8** For \( (n, p) = 1 \), we have \( w(n) \equiv n^p \mod \varphi^2 \) where \( \varphi \) is a fixed prime above \( p \) in \( K = Q(\mu_{p-1}) \).

**Proof:** Let us recall Hensel’s lemma:

Let \( R \) be a ring which is complete with respect to an ideal \( I \) and let \( f(x) \in R[x] \). If \( f(a) \equiv 0 \mod (f'(a)^2 I) \) then there exists \( b \in R \) with \( b \equiv a \mod (f'(a)I) \) such that \( f(b) = 0 \). Further, \( b \) is unique if \( f'(a) \) is a non-zero divisor in \( R \).

Now, let \( K_p \) be the completion of \( K \) at \( \varphi \). Let \( R = \mathcal{O}_p \) be the completion of the ring of integers \( \mathcal{O} \) of \( K \) with respect to \( \varphi \). Let \( I = \varphi^2 \), then we can also think of \( R \) as the completion of \( \mathcal{O} \) with respect to \( I \). Consider \( f(x) = x^{p-1} - 1 \) and let \( a = n^p \), where \( (n, p) = 1 \). Then,

\[
f(a) = (n^p)^{p-1} - 1 \equiv 0 \mod \varphi^2, \quad \text{as } \# \left( \frac{\mathcal{O}_p}{\varphi^2} \right)^\times = \# \left( \frac{\mathcal{O}}{\varphi^2} \right)^\times = N \varphi^2 - N \varphi = p(p - 1).
\]

Moreover \( f'(a) = (p - 1)ap^{p-2} \) is not a zero-divisor in \( R \). Therefore by Hensel’s lemma there exists a unique \( b_n \) in \( R \) such that \( b_n^{p-1} - 1 = 0 \) and \( b_n \equiv n^p \mod \varphi^2 \). Now, if we define \( w(n) = b_n \), we obtain the Teichmuller character \( w : \left( \frac{\mathbb{Z}}{p\mathbb{Z}} \right)^\times \to \mu_{p-1} \) with the more refined congruence \( w(n) \equiv n^p \mod \varphi^2 \). □

### 6.6 Petersson inner product

There is a measure on the upper half complex plane \( \mathfrak{h} \) given by \( d\mu(\tau) = \frac{dx\,dy}{y^2} \) where \( \tau = x + iy \in \mathfrak{h} \). It is easy to show that \( d\mu(\tau) \) is invariant under \( GL_2(\mathbb{R})^+ \subset \text{Aut}(\mathfrak{h}) \),
i.e., \( d\mu(\alpha \tau) = d\mu(\tau) \). In particular, the measure is \( SL_2(\mathbb{Z}) \)-invariant. As \( \mathbb{Q} \cup \{ \infty \} \) is a countable set of measure 0, \( d\mu \) suffices for integration over the extended upper half plane \( \mathfrak{h}^* = \mathfrak{h} \cup \mathbb{Q} \cup \{ \infty \} \). Let \( D^* \) be the fundamental domain for \( SL_2(\mathbb{Z}) \), i.e.,

\[
D^* = \mathfrak{h}^*/SL_2(\mathbb{Z}) = \{ \tau \in \mathfrak{h} \mid \text{Re}(\tau) \leq \frac{1}{2}, |\tau| \geq 1 \} \cup \{ \infty \}.
\]

For a congruence subgroup \( \Gamma \) of \( SL_2(\mathbb{Z}) \), we have \( (\pm I)\Gamma SL_2(\mathbb{Z}) = \bigcup_j (\pm 1)\alpha_j \) where \( j \) runs over a finite set. Then, the fundamental domain for \( \Gamma \) is given by

\[
X(\Gamma) = \mathfrak{h}^*/\Gamma = \bigcup \alpha_j(D^*).
\]

This allows us to integrate function of \( \mathfrak{h}^* \) invariant under \( \Gamma \) by setting

\[
\int_{X(\Gamma)} \phi(\tau)d\mu(\tau) = \int_{\bigcup \alpha_j(D^*)} \phi(\tau)d\mu(\tau) = \sum_j \int_{D^*} \phi(\alpha_j(\tau))d\mu(\tau).
\]

By letting \( V_\Gamma = \int_{X(\Gamma)} d\mu(\tau) \), we can define an inner product

\[
<, >_{\Gamma} : S_k(\Gamma) \times M_k(\Gamma) \rightarrow \mathbb{C}.
\]

given by

\[
< f, g >_{\Gamma} = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau) \overline{g(\tau)(Im(\tau))^k}d\mu(\tau).
\]

Note that the integrand is invariant under \( \Gamma \). For the integral to converge, we need one of \( f \) or \( g \) to be a cusp form (see section 5.4 in [Di-S]). Clearly this inner product is Hermitian and positive definite. When we take a modular form \( f \in M_k(\Gamma) - S_k(\Gamma) \), we can show that \( f \) is orthogonal under \( <, >_{\Gamma} \) to all of \( S_k(\Gamma) \). Thus, we can think of the quotient space \( \mathcal{E}_k(\Gamma) = M_k(\Gamma)/S_k(\Gamma) \) as the complementary subspace linearly disjoint from \( S_k(\Gamma) \). This allows us to write

\[
S_k(\Gamma) = S_k(\Gamma) \oplus \mathcal{E}_k(\Gamma).
\]

### 6.7 Hecke operators

For any \( \alpha \in GL_2(\mathbb{Q}) \), one can write the double coset \( \Gamma\alpha\Gamma = \bigcup_i \Gamma\alpha_i \) where \( \alpha_i \) runs over a finite set. We can define an action of the double coset on \( M_k(\Gamma) \) by setting

\[
f|\Gamma\alpha\Gamma = \sum f|[^i]\alpha_i.
\]

It is easy to verify that these operators preserve \( M_k(\Gamma), S_k(\Gamma) \) and \( \mathcal{E}_k(\Gamma) \).
We need to consider only the case $\Gamma = \Gamma_1(p)$. For any integer $d$ such that $(d, p) = 1$, we can define an operator $< d >$ as follows: we have $ad - bp = 1$ for some $a, b \in \mathbb{Z}$.

Taking $\alpha = \begin{bmatrix} a & b \\ p & d \end{bmatrix} \in \Gamma_0(p)$, we obtain

$$< d > : M_k(\Gamma_1(p)) \rightarrow M_k(\Gamma_1(p)),$$

$$< d > f := f|_{\Gamma_1(p)\alpha\Gamma_1(p)} = f|_{[\alpha]},$$

noting that $\Gamma_1(p)\alpha\Gamma_1(p) = \Gamma_1(p)\alpha$ as $\Gamma_1(p)$ is a normal subgroup of $\Gamma_0(p)$. The operators $< d >$ are called diamond operators.

By taking $\alpha_l = \begin{bmatrix} 1 & 0 \\ 0 & l \end{bmatrix}$ for any prime $l$, we get an operator $T_l = f|_{\Gamma\alpha_l\Gamma}$ for any prime $l$. We extend the definition of Hecke operators to all natural numbers inductively by setting

$$T_{l^{r+1}} = T_lT_{l^r} - l^{k-1} < l > T_l^{r-1} \text{ for } r \geq 1,$$

$$T_{mn} = T_mT_n \text{ when } gcd(m, n) = 1.$$

All these Hecke operators defined above are self adjoint with respect to the Petersson inner product. For more details, see chapter 5 of [Di-S]. A modular form is called an eigenform if it is a simultaneous eigenform for all Hecke operators $T_n$ and $< d >$, $(d, p) = 1$.

### 6.8 Ingredients from commutative algebra

The results proved below are required for the lifting lemma of Deligne and Serre in section 4.1.

#### 6.8.1 Minimal primes

Let $A$ be a commutative ring with 1. A prime ideal $\mathfrak{p}$ of $A$ is called a minimal prime if it the smallest prime ideal (containing 0) in $A$. Such a prime exists by Zorn’s lemma on the (non-empty as 1 $\in A$) set $S$ of primes ideals of $A$ with the partial order $I \leq J$ when $J \subset I$, noting that any descending chain in $S$ has its intersection as an upper bound in $S$.

**Proposition 6.9** A minimal prime $\mathfrak{p}$ of $A$ is contained in the set $Z$ of zero-divisors of $A$.  

17
Proof: Note that \( x, y \in D = A - Z \Rightarrow xy \in D \). Thus \( D \) is a multiplicative set. On the other hand, \( S = A - \wp \) is a maximal multiplicative closed set (as \( \wp \) is a minimal prime). If \( D \not\subseteq S \), then \( SD \) would be a multiplicative set strictly larger than \( S \). Therefore, \( D \subseteq S \) and \( \wp \subseteq Z \). \( \square \)

### 6.8.2 Associated primes and support primes

Let \( A \) be a commutative ring and \( M \) be an \( A \)-module. The annihilator of a submodule \( N \) of \( M \) is defined as

\[
\text{Ann}_A(N) = \{ a \in A | an = 0 \ \forall n \in N \}.
\]

Clearly, \( \text{Ann}_A(N) \) is an ideal of \( A \). For an element \( m \in M \), we can define its annihilator as \( \text{Ann}_A(m) = \{ a \in A | am = 0 \} \).

**Definition 6.10** A prime ideal \( \wp \) of \( A \) is called an **associated prime** if \( \wp \) is the annihilator of some element of \( M \). The set of associated primes of \( M \) in \( A \) is denoted by \( \text{Assoc}_A(M) \).

**Proposition 6.11** If \( M \) is non-zero and \( A \) is Noetherian, then \( \text{Assoc}_A(M) \) is non-empty.

Proof: Consider the set \( S \) of ideals \( (\neq A) \) of \( A \) which are annihilators of some element of \( M \). As \( A \) is Noetherian, \( S \) has a maximal element, say \( \wp \), which is necessarily the annihilator of some element \( m \) in \( M \). Let \( x, y \in A \) such that \( xy \in \wp \) but \( y \not\in \wp \). Then \( ym \neq 0 \), but \( \wp \subseteq (\wp, x) \subseteq \text{Ann}_A(ym) \in S \). It follows that \( \text{Ann}_A(ym) = (\wp, x) = \wp \) by maximality of \( \wp \). Therefore \( x \in \wp \), and hence \( \wp \) is an associated prime. \( \square \)

**Definition 6.12** A prime ideal \( \wp \) of \( A \) is called a **support prime** of \( M \) if \( M_\wp \neq 0 \).

The set of support primes of \( M \) in \( A \) is denoted by \( \text{Supp}_A(M) \).

**Proposition 6.13** Let \( A \) be Noetherian and \( M \) be a finitely generated \( A \)-module. Then \( \wp \in \text{Supp}_A(M) \Leftrightarrow \text{Ann}_A(M) \subseteq \wp \)

Proof: Let \( \text{Ann}_A(M) \not\subseteq \wp \). Then there exists \( s \in A - \wp \) such that \( sM = 0 \), hence \( M_\wp = 0 \). Contra-positively, \( \wp \in \text{Supp}_A(M) \) implies \( \text{Ann}_A(M) \subseteq \wp \).

For the converse, let \( m_1, \ldots, m_r \) generate \( M \) as an \( A \)-module. If \( M_\wp = 0 \), then we can find \( s_i \in A - \wp \) such that \( s_im_i = 0 \). Now \( s = s_1 \ldots s_r \in A - \wp \) annihilates \( M \), hence \( \text{Ann}_A(M) \not\subseteq \wp \). \( \square \)
Proposition 6.14 \( \text{Assoc}_A(M) \subset \text{Supp}_A(M) \).

Proof: Let \( \wp \) be an associated prime of \( M \), say \( \wp = \text{Ann}_A(m) \) for some \( m \in M \). If \( M_\wp = 0 \) then there exists \( s \in A - \wp \) such that \( sm = 0 \). But it would mean \( s \in \text{Ann}_A(m) = \wp \), which is a contradiction. Thus, \( M_\wp \neq 0 \) and \( \wp \) must be a support prime of \( M \). \( \square \)

Proposition 6.15 \( A \) be a Noetherian ring and \( \wp \) be a support prime. Then \( \wp \) contains an associated prime \( q \) of \( M \).

Proof: If \( \wp \) is a support prime, \( M_\wp \neq 0 \). Then there must exist some \( x \in M \) such that \( (Ax)_\wp \neq 0 \). Thus, there exists an associated prime \( q \) of the \( A \)-module \( (Ax)_\wp \). Hence there is an element \( 0 \neq \frac{y}{s} \) of \( (Ax)_\wp \) with \( y \in Ax \) and \( s \notin \wp \) such that \( q \) is the annihilator of \( \frac{y}{s} \).
Now, if there exists \( b \in q - \wp \), then \( b \frac{y}{s} = 0 \) would imply \( \frac{y}{s} = 0 \), which is a contradiction.

Now we still have to show that \( q \) is an associated prime of \( M \) as well. Let \( b_1, \ldots, b_n \) be a set of generators of \( q \). Then, there exists \( t_i \in A - \wp \) such that \( b_it_\wp y = 0 \). Let \( t = t_1 \ldots t_n \). Then, \( q \) is the annihilator of \( ty \in M \). \( \square \)

Corollary 6.16 If \( \wp \) is a minimal prime in the support of \( M \), then \( \wp \) is also an associated prime when \( A \) is Noetherian.

Proof: As \( \wp \) must contain an associated prime, we get our result by minimality of \( \wp \). \( \square \)

References

[BS] Borevich, Z. I., Shafarevich, I. R.; Number Theory, Academic Press, 1966.

[C] Carlitz, L.; A generalization of Maillet’s determinant and a bound for the first factor of the class number, Proc. A.M.S. 12, 256–261, 1961.

[C-O] Carlitz, L. Olson F.R.; Maillet’s determinant, Proc. A.M.S. 6, 265–269, 1955.

[D] Dalawat, C.S.; Ribet’s modular construction of unramified \( p \)-extensions of \( \mathbb{Q}(\mu_p) \) (to appear)

[D-S] Deligne P., Serre, J-P.; Formes modulaires de poids 1, Ann. Scient. Ec. Norm. Sup., 4\textsuperscript{e} serie, 7, 507–530, 1974.

[Di-S] Diamond, F., Shurman S.; A First Course on Modular Forms, Springer, 2005.

[Gr] Greenberg, R.; A generalization of Kummer’s criterion, Inventiones Math. 21, 247–254, 1973.
[La] Lang, S.; Algebra, Springer-Verlag, 2002.

[R] Ribet, K.; A modular construction of unramified $p$-extensions of $\mathbb{Q}(\mu_p)$, Inventiones Math. 34, 151–162, 1976.

[Wa] Washington, L.; Introduction to Cyclotomic Fields, Springer-Verlag, 1997.