Chapter 4

Dirichlet Characters

In this chapter we develop a systematic theory for computing with Dirichlet characters, which are extremely important to computations with modular forms for (at least) two reasons:

- To compute the Eisenstein subspace $E_k(\Gamma_1(N))$ of $M_k(\Gamma_1(N))$ we explicitly write down Eisenstein series attached to pairs of Dirichlet characters (see Chapter 5).

- To compute $S_k(\Gamma_1(N))$, we instead compute a decomposition

$$M_k(\Gamma_1(N)) = \bigoplus M_k(\Gamma_1(N), \varepsilon)$$

  then compute each factor. Here the sum is over all Dirichlet characters ε modulo N.

Example 4.0.1. Expanding on the second point, the spaces $M_k(\Gamma_1(N), \varepsilon)$ are frequently much easier to compute with than the full $M_k(\Gamma_1(N))$. As we will see, if $\varepsilon = 1$ is the trivial character, then $M_k(\Gamma_1(N), 1) = M_k(\Gamma_0(N))$, which has much smaller dimension than $M_k(\Gamma_1(N))$. For example, $M_2(\Gamma_1(100))$ has dimension 370, whereas $M_2(\Gamma_1(100), 1)$ has dimension only 24, and $M_2(\Gamma_1(389))$ has dimension 6499, whereas $M_2(\Gamma_1(389), 1)$ has dimension only 33.

```
sage: dimension_modular_forms(Gamma1(100),2)
370
sage: dimension_modular_forms(Gamma0(100),2)
24
sage: dimension_modular_forms(Gamma1(389),2)
6499
sage: dimension_modular_forms(Gamma0(389),2)
33
```

4.1 The Definition

Fix an integral domain R and a root ζ of unity in R.

Definition 4.1.1 (Dirichlet Character)**.** A *Dirichlet character* modulo N over R is a map $\varepsilon : \mathbb{Z} \to R$ such that there is a homomorphism $f : (\mathbb{Z}/N\mathbb{Z})^* \to \langle\zeta\rangle$ for which

$$\varepsilon(a) = \begin{cases} 0 & \text{if } (a, N) > 1, \\ f(a \bmod N) & \text{if } (a, N) = 1. \end{cases}$$

We denote the group of such Dirichlet characters by $D(N, R)$. Note that elements of $D(N, R)$ are in bijection with homomorphisms $(\mathbb{Z}/N\mathbb{Z})^* \to \langle\zeta\rangle$.

One familiar example of a Dirichlet characters is the Legendre symbol $\left(\frac{a}{p}\right)$ that appears in quadratic reciprocity theory. It is a Dirichlet character modulo p that takes the value 1 on integers that are congruent to a nonzero square modulo p, the value -1 on integers that are congruent to a nonzero non-square modulo p, and 0 on integers divisible by p.

4.2 Dirichlet Characters in SAGE

To create a Dirichlet character in SAGE you first create the group $D(N, R)$ of Dirichlet characters, then obtain elements of that group. First we make $D(11, \mathbb{Q})$:

```
sage: G = DirichletGroup(11, RationalField())
sage: G
Group of Dirichlet characters of modulus 11 over Rational Field
```

A Dirichlet character prints as a matrix that gives the values of the character on canonical generators of $(\mathbb{Z}/N\mathbb{Z})^*$ (as discussed below).

```
sage: list(G)
[[1], [-1]]
sage: eps = G.0      # 0th generator for Dirichlet group
sage: eps
[-1]
```

The character takes the value -1 on the unit generator.

```
sage: G.unit_gens()
[2]
sage: eps(2)
-1
sage: eps(3)
1
```

It is 0 on any integer not coprime to 11:

```
sage: eps(22)
0
```

We can also create groups of Dirichlet characters taking values in other rings or fields. For example, we create the cyclotomic field $\mathbb{Q}(\zeta_4)$.

```
sage: R = CyclotomicField(4)
sage: CyclotomicField(4)
Cyclotomic Field of order 4 and degree 2
```

Then we define $G = D(15, \mathbb{Q}(\zeta_4)$.

```
sage: G = DirichletGroup(15, R)
sage: G
Group of Dirichlet characters of modulus 15 over Cyclotomic Field
of order 4 and degree 2
```

And we list each of its elements.

```
sage: list(G)
[[1, 1], [-1, 1], [1, zeta_4], [-1, zeta_4], [1, -1], [-1, -1],
 [1, -zeta_4], [-1, -zeta_4]]
```

Now lets evaluate the second generator of G on various integers:

```
sage: e = G.1
sage: e(4)
-1
sage: e(-1)
-1
sage: e(5)
0
```

Finally we make a list of all the values of e.

```
sage: [e(n) for n in range(15)]
[0, 1, zeta_4, 0, -1, 0, 0, zeta_4, -zeta_4,
    0, 0, 1, 0, -zeta_4, -1]
```

We can also compute with groups of Dirichlet characters with values in a finite field.

```
sage: G = DirichletGroup(15, GF(5))
sage: G
Group of Dirichlet characters of modulus 15 over Finite field of size 5
```

We list all the elements of G, again represented by matrices that give the images of each unit generator, as an element of $\mathbb{F}_5$.

```
sage: list(G)
  [[1, 1], [4, 1], [1, 2], [4, 2], [1, 4], [4, 4], [1, 3], [4, 3]]
```

We evaluate the second generator of G on several integers.

```
sage: e = G.1
sage: e(-1)
4
sage: e(2)
2
sage: e(5)
0
sage: print [e(n) for n in range(15)]
[0, 1, 2, 0, 4, 0, 0, 2, 3, 0, 0, 1, 0, 3, 4]
```

4.3 Representing Dirichlet Characters

Lemma 4.3.1. *The groups $(\mathbb{Z}/N\mathbb{Z})^*$ and $D(N, \mathbb{C})$ are non-canonically isomorphic.*

Proof. This follows from the more general fact that for any finite abelian group G, we have that $G \approx \mathrm{Hom}(G, \mathbb{C}^*)$. To prove that this latter non-canonical isomorphism exists, first reduce to the case when G is cyclic of order n, in which case the statement follows because $\mathbb{C}^*$ contains the nth root of unity $e^{2\pi i/n}$, so $\mathrm{Hom}(G, \mathbb{C}^*)$ is also cyclic of order n. $\square$

Corollary 4.3.2. *We have $\#D(N, R) \mid \varphi(N)$, with equality if and only if the order of our choice of $\zeta \in R$ is a multiple of the exponent of the group $(\mathbb{Z}/N\mathbb{Z})^*$.*

Example 4.3.3. The group $D(5, \mathbb{C})$ has elements $\{[1], [i], [-1], [-i]\}$, so is cyclic of order $\varphi(5) = 4$. In contrast, the group $D(5, \mathbb{Q})$ has only the two elements $[1]$ and $[-1]$ and order 2. In SAGE the command `DirichletGroup(N)` with no second argument create the group of Dirichlet characters with values in the cyclotomic field $\mathbb{Q}(\zeta_n)$, where n is the exponent of the group $(\mathbb{Z}/N\mathbb{Z})^*$. Every element in $D(N, \mathbb{C})$ takes values in $\mathbb{Q}(\zeta_n)$, so $D(N, \mathbb{Q}(\zeta_n)) \cong D(N, \mathbb{C})$.

```
sage: list(DirichletGroup(5))
[[1], [zeta_4], [-1], [-zeta_4]]
sage: list(DirichletGroup(5, Q))
[[1], [-1]]
```

Fix a positive integer N, and write $N = \prod_{i=0}^{n} p_i^{e_i}$ where $p_0 < p_1 < \cdots < p_n$ are the prime divisors of N. By Exercise 4.1, each factor $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ is a cyclic group $C_i = \langle g_i \rangle$, except if $p_0 = 2$ and $e_0 \geq 3$, in which case $(\mathbb{Z}/p_0^{e_0}\mathbb{Z})^*$ is a product of the cyclic subgroup $C_0 = \langle -1 \rangle$ of order 2 with the cyclic subgroup $C_1 = \langle 5 \rangle$. In all cases we have

$$(\mathbb{Z}/N\mathbb{Z})^* \cong \prod_{0 \leq i \leq n} C_i = \prod_{0 \leq i \leq n} \langle g_i \rangle.$$

For i such that $p_i > 2$, choose the generator g_i of C_i to be the element of $\{2, 3, \ldots, p_i^{e_i} - 1\}$ that is smallest and generates. Finally, use the Chinese Remainder Theorem (see [Coh93, §1.3.3])) to lift each g_i to an element in $(\mathbb{Z}/N\mathbb{Z})^*$, also denoted g_i, that is 1 modulo each $p_j^{e_j}$ for $j \neq i$.

Algorithm 4.3.4 (Minimal generator for $(\mathbb{Z}/p^r\mathbb{Z})^*$)**.** *Given an odd prime power p^r, this algorithm computes the minimal generator for $(\mathbb{Z}/p^r\mathbb{Z})^*$.*

1. [Factor Group Order] Factor $n = \phi(p^r) = p^{r-1} \cdot 2 \cdot ((p-1)/2)$ as a product $\prod p_i^{e_i}$ of primes. This is equivalent in difficulty to factoring $(p-1)/2$. (See, e.g., [Coh93, Ch.8, 10] for integer factorization algorithms.)
2. [Initialize] Set $g = 2$.
3. [Generator?] Using the binary powering algorithm (see [Coh93, §1.2]), compute $g^{n/p_i} \pmod{p^r}$, for each prime divisor p_i of n. If any of these powers are 1, set $g = g + 1$ and go to Step 2. If no powers are 1, output g and terminate.

For the proof, see Exercise 4.2.

Example 4.3.5. A minimal generator for $(\mathbb{Z}/49\mathbb{Z})^*$ is 3. We have $n = \varphi(49) = 42 = 2 \cdot 3 \cdot 7$, and

$$2^{n/2} \equiv 1, \qquad 2^{n/3} \equiv 18, \qquad 2^{n/7} \equiv 15 \pmod{49}.$$

so 2 is not a generator for $(\mathbb{Z}/49\mathbb{Z})^*$. (We see this just from $2^{n/2} \equiv 1 \pmod{49}$.) However 3 is since

$$3^{n/2} \equiv 48, \qquad 3^{n/3} \equiv 30, \qquad 3^{n/7} \equiv 43 \pmod{49}.$$

Example 4.3.6. In this example we compute minimal generators for $N = 25$, 100, and 200:

1. The minimal generator for $(\mathbb{Z}/25\mathbb{Z})^*$ is 2.
2. Minimal generators for $(\mathbb{Z}/100\mathbb{Z})^*$, lifted to numbers modulo 100, are $g_0 = 51$ and $g_1 = 77$. Notice that $g_0 \equiv -1 \pmod{4}$ and $g_0 \equiv 1 \pmod{25}$, and $g_1 \equiv 2 \pmod{25}$ is the minimal generator modulo 25.
3. Minimal generators for $(\mathbb{Z}/200\mathbb{Z})^*$, lifted to numbers modulo 200, are $g_0 = 151$, $g_1 = 101$, and $g_2 = 177$. Note that $g_0 \equiv -1 \pmod{4}$, that $g_1 \equiv 5 \pmod{8}$, and $g_2 \equiv 2 \pmod{25}$.

The command `Integers(N)` creates $\mathbb{Z}/N\mathbb{Z}$.

```
sage: R = Integers(49)
sage: R
Ring of integers modulo 49
```

The `unit_gens()` command computes the unit generators as defined above.

```
sage: R.unit_gens()
[3]
sage: Integers(25).unit_gens()
[2]
sage: Integers(100).unit_gens()
[51, 77]
sage: Integers(200).unit_gens()
[151, 101, 177]
sage: Integers(2005).unit_gens()
[402, 1206]
sage: Integers(200000000).unit_gens()
[174218751, 51562501, 187109377]
```

Fix an element ζ of finite multiplicative order in a ring R, and let $D(N, R)$ denote the group of Dirichlet characters modulo N over R, with image in $\langle\zeta\rangle \cup \{0\}$. We specify an element $\varepsilon \in D(N, R)$ by giving the list

$$[\varepsilon(g_0), \varepsilon(g_1), \ldots, \varepsilon(g_n)] \tag{4.3.1}$$

of images of the generators of $(\mathbb{Z}/N\mathbb{Z})^*$. (Note if N is even, the number of elements of the list (4.3.1) does *not* depend on whether or not $8 \mid N$—there are always two factors corresponding to 2.) This representation completely determines ε and is convenient for arithmetic operations with Dirichlet characters. It is analogous to representing a linear transformation by a matrix. See Section 4.7 for a discussion of alternative ways to represent Dirichlet characters.

4.4 Evaluation of Dirichlet Characters

This section is about how to compute $\varepsilon(n)$, where ε is a Dirichlet character and n is an integer. We begin with an example.

Example 4.4.1. If $N = 200$, then $g_0 = 151$, $g_1 = 101$ and $g_2 = 177$, as we saw in Example 4.3.6. The exponent of $(\mathbb{Z}/200\mathbb{Z})^*$ is 20, since that is the least common multiple of the exponents of $4 = \#(\mathbb{Z}/8\mathbb{Z})^*$ and $20 = \#(\mathbb{Z}/25\mathbb{Z})^*$. The orders of g_0, g_1 and g_2 are 2, 2, and 20. Let $\zeta = \zeta_{20}$ be a primitive 20th root of unity in $\mathbb{C}$. Then the following are generators for $D(200, \mathbb{C})$:

$$\varepsilon_0 = [-1, 1, 1], \qquad \varepsilon_1 = [1, -1, 1], \qquad \varepsilon_2 = [1, 1, \zeta],$$

and $\varepsilon = [1, -1, \zeta^5]$ is an example element of order 4. To evaluate $\varepsilon(3)$, we write 3 in terms of g_0, g_1, and g_2. First, reducing 3 modulo 8, we see that $3 \equiv g_0 \cdot g_1 \pmod 8$. Next reducing 3 modulo 25, and trying powers of $g_2 = 2$, we find that $e \equiv g_2^7 \pmod{25}$. Thus

$$\begin{aligned}\varepsilon(3) &= \varepsilon(g_0 \cdot g_1 \cdot g_2^7)\\ &= \varepsilon(g_0)\varepsilon(g_1)\varepsilon(g_2)^7\\ &= 1 \cdot (-1) \cdot (\zeta^5)^7\\ &= -\zeta^{35} = -\zeta^{15}.\end{aligned}$$

We next illustrate the above computation of $\varepsilon(3)$ in SAGE. First we make the group $D(200, \mathbb{Q}(\zeta_8))$, and list its generators.

```
sage: G = DirichletGroup(200)
sage: G
Group of Dirichlet characters of modulus 200 over Cyclotomic Field
      of order 20 and degree 8
sage: G.exponent()
20
sage: G.gens()
[[-1, 1, 1], [1, -1, 1], [1, 1, zeta_20]]
```

Next we construct ε.

```
sage: K = G.base_ring()
sage: zeta = K.gen()
sage: eps = G([1,-1,zeta^5])
sage: eps
[1, -1, zeta_20^5]
```

Finally, we evaluate ε at 3.

```
sage: eps(3)
zeta_20^5
sage: -zeta^15
zeta_20^5
```

Example 4.4.1 illustrates that if ε is represented using a list as described above, evaluation of ε on an arbitrary integer is inefficient without extra information; it requires solving the discrete log problem in $(\mathbb{Z}/N\mathbb{Z})^*$. In fact, for a general character ε calculation of ε will probably be at least as hard as finding discrete logarithms no matter what representation we use (quadratic characters are easier—see Algorithm 4.4.5).

Chapter 5

Eisenstein Series

We introduce generalized Bernoulli numbers attached to Dirichlet characters, and give an algorithm to enumerate the Eisenstein series in $M_k(N, \varepsilon)$. We will wait until Chapter 8 for an algorithm to compute all cusp forms in $M_k(N, \varepsilon)$.

5.1 Generalized Bernoulli Numbers

Suppose ε is a Dirichlet character modulo N over $\mathbb{C}$.

Definition 5.1.1 (Generalized Bernoulli Number)**.** Define the *generalized Bernoulli numbers $B_{k,\varepsilon}$* attached to ε by the following identity of infinite series:

$$\sum_{a=1}^{N-1} \frac{\varepsilon(a) \cdot x \cdot e^{ax}}{e^{Nx} - 1} = \sum_{k=0}^{\infty} B_{k,\varepsilon} \cdot \frac{x^k}{k!}.$$

If ε is the trivial character of modulus 1 and B_k are as in Section 2.1, then $B_{k,\varepsilon} = B_k$, except when $k = 1$, in which case $B_{1,\varepsilon} = -B_1 = 1/2$ (see Exercise 5.5).

Let $\mathbb{Q}(\varepsilon)$ denote the field generated by the values of the character ε, so $\mathbb{Q}(\varepsilon)$ is the cyclotomic extension $\mathbb{Q}(\zeta_n)$, where n is the order of ε.

Algorithm 5.1.2 (Bernoulli Numbers)**.** *Given an integer $k \geq 0$ and any Dirichlet character ε with modulus N, this algorithm computes the generalized Bernoulli numbers $B_{j,\varepsilon}$, for $j \leq k$.*

1. Compute $g = x/(e^{Nx} - 1) \in \mathbb{Q}[[x]]$ to precision $O(x^{k+1})$ by computing $e^{Nx} - 1 = \sum_{n \geq 1} N^n x^n / n!$ to precision $O(x^{k+2})$, and computing the inverse $x/(e^{Nx} - 1)$. For completeness, note that if $f = a_0 + a_1 x + a_2 x^2 + \cdots$, then we have the following recursive formula for the coefficients b_n of the expansion of $1/f$:

$$b_n = -\frac{b_0}{a_0} \cdot (b_{n-1} a_1 + b_{n-2} a_2 + \cdots + b_0 a_n).$$

2. For each $a = 1, \ldots, N$, compute $f_a = g \cdot e^{ax} \in \mathbb{Q}[[x]]$, to precision $O(x^{k+1})$. This requires computing $e^{ax} = \sum_{n \geq 0} a^n x^n / n!$ to precision $O(x^{k+1})$. (One can omit computation of e^{Nx} if $N > 1$.)

3. Then for $j \leq k$, we have

$$B_{j,\varepsilon} = j! \cdot \sum_{a=1}^{N} \varepsilon(a) \cdot c_j(f_a),$$

   where $c_j(f_a)$ is the coefficient of x^j in f_a.

Note that in Steps 1 and 2 we compute the power series doing arithmetic only in $\mathbb{Q}[[x]]$, not in $\mathbb{Q}(\varepsilon)[[x]]$, which could be much less efficient if ε has large order. One could also write down a recurrence formula for $B_{j,\varepsilon}$, but this would simply encode arithmetic in power series rings and the definitions in a formula.

Example 5.1.3. Let ε be the nontrivial character with modulus 4. Thus ε has order 2 and takes values in $\mathbb{Q}$. Then the Bernoulli numbers $B_{k,\varepsilon}$ for k even are all 0 and for k odd they are

$$\begin{aligned}
B_{1,\varepsilon} &= -1/2 \\
B_{3,\varepsilon} &= 3/2 \\
B_{5,\varepsilon} &= -25/2 \\
B_{7,\varepsilon} &= 427/2 \\
B_{9,\varepsilon} &= -12465/2 \\
B_{11,\varepsilon} &= 555731/2 \\
B_{13,\varepsilon} &= -35135945/2 \\
B_{15,\varepsilon} &= 2990414715/2 \\
B_{17,\varepsilon} &= -329655706465/2 \\
B_{19,\varepsilon} &= 45692713833379/2.
\end{aligned}$$

These Bernoulli numbers can be divisible by large primes. For example, $B_{17,\varepsilon} = 5 \cdot 17^2 \cdot 228135437/2$.

Example 5.1.4. This examples illustrates that the generalized Bernoulli numbers need not be rational numbers. Suppose ε is the mod 5 character such that

$\varepsilon(2) = i = \sqrt{-1}$. Then $B_{k,\varepsilon} = 0$ for k even and

$$\begin{aligned}
B_{1,\varepsilon} &= \frac{-i-3}{5}\\
B_{3,\varepsilon} &= \frac{6i+12}{5}\\
B_{5,\varepsilon} &= \frac{-86i-148}{5}\\
B_{7,\varepsilon} &= \frac{2366i+3892}{5}\\
B_{9,\varepsilon} &= \frac{-108846i-176868}{5}\\
B_{11,\varepsilon} &= \frac{7599526i+12309572}{5}\\
B_{13,\varepsilon} &= \frac{-751182406i-1215768788}{5}\\
B_{15,\varepsilon} &= \frac{99909993486i+161668772052}{5}\\
B_{17,\varepsilon} &= \frac{-17209733596766i-27846408467908}{5}
\end{aligned}$$

Proposition 5.1.5. *If $\varepsilon(-1) \neq (-1)^k$, then $B_{k,\varepsilon} = 0$.*

5.2 Explicit Basis for the Eisenstein Subspace

Suppose χ and ψ are primitive Dirichlet characters with conductors L and M, respectively. Let

$$E_{k,\chi,\psi}(q) = c_0 + \sum_{m\geq 1}\left(\sum_{n\mid m}\psi(n)\cdot\chi(m/n)\cdot n^{k-1}\right)q^m \in \mathbb{Q}(\chi,\psi)[[q]], \quad (5.2.1)$$

where

$$c_0 = \begin{cases} 0 & \text{if } L > 1,\\ -\dfrac{B_{k,\psi}}{2k} & \text{if } L = 1.\end{cases}$$

Note that when $\chi = \psi = 1$ and $k \geq 4$, then $E_{k,\chi,\psi} = E_k$, where E_k is from Chapter 1.

Miyake proves statements that imply the following theorems in [Miy89, Ch. 7]. We will not prove them in this book since developing the theory needed to prove them would take us far afield from our goal, which is to compute $M_k(N,\varepsilon)$.

Theorem 5.2.1. *Suppose t is a positive integer and χ, ψ are as above, and that k is a positive integer such that $\chi(-1)\psi(-1) = (-1)^k$. Except when*

$k = 2$ and $\chi = \psi = 1$, the power series $E_{k,\chi,\psi}(q^t)$ defines an element of $M_k(MLt, \chi/\psi)$. If $\chi = \psi = 1$, $k = 2$, $t > 1$, and $E_2 = E_{k,\chi,\psi}$, then $E_2(q) - tE_2(q^t)$ is a modular form in $M_2(\Gamma_0(t))$.

Theorem 5.2.2. *The Eisenstein series in $M_k(N, \varepsilon)$ coming from Theorem 5.2.1 form a basis for the Eisenstein subspace $E_k(N, \varepsilon)$.*

Theorem 5.2.3. *The Eisenstein series $E_{k,\chi,\psi}(q) \in M_k(ML)$ defined above is an eigenvector for all Hecke operators T_n. Also $E_2(q) - tE_2(q^t)$, for $t > 1$, is an eigenform.*

Since $E_{k,\chi,\psi}(q)$ is normalizes so the coefficient of q is 1, the eigenvalue of T_m is

$$\sum_{n|m} \psi(n) \cdot \chi(m/n) \cdot n^{k-1}.$$

Also for $f = E_2(q) - tE_2(q^t)$ with $t > 1$ prime, the coefficient of q is 1, and $T_m(f) = \sigma_1(m) \cdot f$ for $(m, t) = 1$, and $T_t(f) = ((t + 1) - t)f = f$.

Algorithm 5.2.4 (Enumerating Eisenstein Series)**.** *Given a weight k and a Dirichlet character ε of modulus N, this algorithm computes a basis for the Eisenstein subspace $E_k(N, \varepsilon)$ of $M_k(N, \varepsilon)$ to precision $O(q^r)$.*

1. [Weight 2 Trivial Character?] If $k = 2$ and $\varepsilon = 1$, output the Eisenstein series $E_2(q) - tE_2(q^t)$, for each divisor $t \mid N$ with $t \neq 1$, then terminate.
2. [Compute Dirichlet Group] Let $G = D(N, \mathbb{Q}(\zeta_n))$ be the group of Dirichlet characters with values in $\mathbb{Q}(\zeta_n)$, where n is the exponent fo $(\mathbb{Z}/N\mathbb{Z})^*$.
3. [Compute Conductors] Compute the conductor of every element of G (which just involves computing the orders of the local components of each character).
4. [List Characters χ] Form a list V all Dirichlet characters $\chi \in G$ such that $\mathrm{cond}(\chi) \cdot \mathrm{cond}(\chi/\varepsilon)$ divides N.
5. [Compute Eisenstein Series] For each character χ in V, let $\psi = \chi/\varepsilon$, and compute $E_{k,\chi,\psi}(q^t) \pmod{q^r}$ for each divisor t of $N/(\mathrm{cond}(\chi) \cdot \mathrm{cond}(\psi))$. We compute $E_{k,\chi,\psi}(q^t) \pmod{q^r}$ using (5.2.1) and Algorithm 5.1.2.

Remark 5.2.5. Algorithm 5.2.4 is what I currently use in my programs. It might be better to first reduce to the prime power case by writing all characters as product of local characters and combine Steps 3 and 4 into a single step that involves orders. However, this might make things more complicated and obscure.

Example 5.2.6. The following is a basis of Eisenstein series $E_{2,\chi,\psi}$ for $E_2(\Gamma_1(13))$.

```
f1 = 1/2 + q + 3*q^2 + 4*q^3 + O(q^4)

f2 = (-7/13*zeta_12^2 - 11/13) + q + (2*zeta_12^2 + 1)*q^2
                            + (-3*zeta_12^2 + 1)*q^3 + O(q^4)

f3 = q + (zeta_12^2 + 2)*q^2 + (-1*zeta_12^2 + 3)*q^3 + O(q^4)

f4 = (-1*zeta_12^2) + q + (2*zeta_12^2 - 1)*q^2
                     + (3*zeta_12^2 - 2)*q^3 + O(q^4)

f5 = q + (zeta_12^2 + 1)*q^2 + (zeta_12^2 + 2)*q^3 + O(q^4)

f6 = (-1) + q + (-1)*q^2 + 4*q^3 + O(q^4)

f7 = q + q^2 + 4*q^3 + O(q^4)

f8 = (zeta_12^2 - 1) + q + (-2*zeta_12^2 + 1)*q^2
                      + (-3*zeta_12^2 + 1)*q^3 + O(q^4)

f9 = q + (-1*zeta_12^2 + 2)*q^2 + (-1*zeta_12^2 + 3)*q^3 + O(q^4)

f10 = (7/13*zeta_12^2 - 18/13) + q + (-2*zeta_12^2 + 3)*q^2
                                 + (3*zeta_12^2 - 2)*q^3 + O(q^4)

f11 = q + (-1*zeta_12^2 + 3)*q^2 + (zeta_12^2 + 2)*q^3 + O(q^4)
```

5.3 Exercises

5.1 Suppose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and N is a positive integer. Prove that there is a positive integer h such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \gamma^{-1}\Gamma_1(N)\gamma$.

5.2 Prove that the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. (Hint: There is a proof of a more general result near the beginning of Shimura's book [Shi94].)

5.3 Prove that $M_k(N, 1) = M_k(\Gamma_0(N))$.

5.4 Suppose A and B are diagonalizable linear transformations of a finite-dimensional vector space V and that both A and B are diagonalizable. Prove there is a basis for V so that the matrices of A and B with respect to that both are simultaneously diagonal.

5.5 If ε is the trivial character of modulus 1 and B_k are as in Section 2.1, then $B_{k,\varepsilon} = B_k$, except when $k = 1$, in which case $B_{1,\varepsilon} = -B_1 = 1/2$.

5.6 Prove that if $n > 1$ is odd, then the Bernoulli number B_n is 0.