1.5.3 The Hecke Algebra and Eigenforms

Definition 1.5.7 (Hecke Algebra). The *Hecke algebra* $\mathbf{T}$ associated to $M_k(1)$ is the subring of $\mathrm{End}(M_k(1))$ generated by the operators T_n for all n. Similarly, the *Hecke algebra* associated to $S_k(1)$ is the subring of $\mathrm{End}(S_k(1))$ generated by all Hecke operators T_n.

The Hecke algebra is commutative (e.g., when $(n, m) = 1$ we have $T_n T_m = T_{nm} = T_{mn} = T_m T_n$) of finite rank over $\mathbf{Z}$.

Definition 1.5.8 (Eigenform). An *eigenform* $f \in M_k(1)$ is a nonzero element such that f is an eigenvector for every Hecke operator T_n. If $f \in S_k(1)$ is an eigenform, then f is *normalized* if the coefficient of q in the q-expansion of f is 1. We sometimes called a normalized cuspidal eigenform a *newform*.

If $f = \sum_{n=1}^{\infty} c_n q^n$ is a normalized eigenform, then Remark 1.5.5 implies that $T_n(f) = c_n f$. Thus the coefficients of a newform are exactly the system of eigenvalues of the Hecke operators acting on the newform.

Remark 1.5.9. It follows from Victor Miller's thesis that $T_1, \ldots, T_n$ generate $\mathbf{T} \subset S_k(1)$, where $n = \dim S_k(1)$.

1.5.4 Examples

```
> M := ModularForms(1,12);
> HeckeOperator(M,2);
[  2049 196560]
[     0    -24]
> S := CuspidalSubspace(M);
> HeckeOperator(S,2);
[-24]
> Factorization(CharacteristicPolynomial(HeckeOperator(M,2)));
[
    <x - 2049, 1>,
    <x + 24, 1>
]
> M := ModularForms(1,40);
> M;
Space of modular forms on Gamma_0(1) of weight 40 and dimension 4
over Integer Ring.
> Basis(M);
[
    1 + 1250172000*q^4 + 7541401190400*q^5 + 9236514405888000*q^6
    + 3770797689077760000*q^7 + O(q^8),
    q + 19291168*q^4 + 37956369150*q^5 + 14446985236992*q^6 +
    1741415886056000*q^7 + O(q^8),
    q^2 + 156024*q^4 + 57085952*q^5 + 1914094476*q^6 -
    27480047616*q^7 + O(q^8),
    q^3 + 168*q^4 - 12636*q^5 + 392832*q^6 - 7335174*q^7 + O(q^8)
]
> HeckeOperator(M,2);
[549755813889 0 1250172000 9236514405888000]
[0 0 549775105056 14446985236992]
[0 1 156024 1914094476]
```

```
[0 0 168 392832]
> Factorization(CharacteristicPolynomial(HeckeOperator(M,2)));
[
    <x - 549755813889, 1>,
    <x^3 - 548856*x^2 - 810051757056*x + 213542160549543936, 1>
]
```

1.6 Two Conjectures about Hecke Operators on Level 1 Modular Forms

1.6.1 Maeda's Conjecture

Conjecture 1.6.1 (Maeda). *Let k be a positive integer such that $S_k(1)$ has positive dimension and let $T \subset \mathrm{End}(S_k(1))$ be the Hecke algebra. Then there is only one $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ orbit of normalized eigenforms of level 1.*

There is some numerical evidence for this conjecture. It is true for $k \leq 2000$, according to [3]. Buzzard shows in [1] that for the weights $k \leq 228$ with $k/12$ a prime, the Galois group of the characteristic polynomial of T_2 is the full symmetric group.

Possible student project: I have computed the characteristic polynomial of T_2 for all weights $k \leq 3000$:

`http://modular.fas.harvard.edu/Tables/charpoly_level1/t2/`

However, I never bothered to try to prove that these are all irreducible, which would establish Maeda's conjecture for $k \leq 3000$. The MathSciNet reviewer of [3] said "In the present paper the authors take a big step forward towards proving Maeda's conjecture in the affirmative by establishing that the Hecke polynomial $T_{p,k}(x)$ is irreducible and has full Galois group over $\mathbb{Q}$ for $k \leq 2000$ and $p < 2000, p$ prime." Thus stepping forward to $k \leq 3000$, at least for $p = 2$, might be worth doing.

1.6.2 The Gouvea-Mazur Conjecture

Fix a prime p, and let $F_{p,k} \in \mathbf{Z}[x]$ be the characteristic polynomial of T_p acting on $M_k(1)$. The *slopes* of $F_{p,k}$ are the p-adic valuations $\mathrm{ord}_p(\alpha) \in \mathbf{Q}$ of the roots $\alpha \in \overline{\mathbf{Q}}_p$ of $F_{p,k}$. They can be computed easily using Newton polygons. For example, the $p = 5$ slopes for $F_{5,12}$ are $0, 1, 1$, for $F_{5,12+4\cdot 5}$ they are $0, 1, 1, 4, 4$, and for $F_{5,12+4\cdot 5^2}$ they are $0, 1, 1, 5, 5, 5, 5, 5, 5, 10, 10, 11, 11, 14, 14, 15, 15, 16, 16$.

```
> function s(k,p)
    return NewtonSlopes(CharacteristicPolynomial(
               HeckeOperator(ModularForms(1,k),p)),p);
  end function;
> s(12,5);
[* 0, 1 *]
> s(12+4*5,5);
[* 0, 1, 4 *]
> s(12+4*5^2,5);
[* 0, 1, 5, 5, 5, 10, 11, 14, 15, 16 *]
> s(12+4*5^3,5);
```

```
[* 0, 1, 5, 5, 5, 10, 11, 14, 15, 16, 20, 21, 24, 25, 27, 30, 31,
  34, 36, 37, 40, 41, 45, 46, 47, 50, 51, 55, 55, 55, 59, 60, 63,
  64, 65, 69, 70, 73, 74, 76, 79, 80, 83 *]
```

Let $d(k, \alpha, p)$ be the multiplicity of α as a slope of $F_{p,k}$.

Conjecture 1.6.2 (Gouvea-Mazur, 1992). *Fix a prime p and a nonnegative rational number α. Suppose k_1 and k_2 are integers with $k_1, k_2 \geq 2\alpha+2$, and $k_1 \equiv k_2 \pmod{p^n(p-1)}$ for some $n \geq \alpha$. Then $d(k_1, \alpha, p) = d(k_2, \alpha, p)$.*

Notice that the above examples, with $p = 5$ and $k_1 = 12$, are consistent with this conjecture. However, the conjecture is false in general. Frank Calegari and Kevin Buzzard recently found the first counterexample, when $p = 59$, $k_1 = 16$, $\alpha = 1$, and $k_2 = 16 + 59 \cdot 58 = 3438$. We have $d(16, 0, 59) = 0d(16, 1, 59) = 1$, $d(16, \alpha, 59) = 0$ for all other α. However, initial computations strongly suggest (but do not prove!) that $d(3438, 1, 59) = 2$. (**This was incorrect in the version of the notes from Friday.**) It is a finite, but difficult, computation to decide what $d(3438, 1, 59)$ really is (see Section 1.7). **Potential student project: Show that $d(3438, 1, 59) = 2$! Also, look at higher level, where the computations are easier.** Using a trace formula, Calegari and Buzzard at least showed that either $d(3438, 1, 59) \geq 2$ or there exists $\alpha < 1$ such that $d(3438, \alpha, 59) > 0$, both of which contradict Conjecture 1.6.2.

There are many theorems about more general formulations of the Gouvea-Mazur conjecture, and a whole geometric theory "the Eigencurve" [2] that helps explain it, but discussing this further is beyond the scope of this book.

1.7 A Modular Algorithm for Computing Characteristic Polynomials of Hecke Operators

In computational investigations, it is frequently useful to compute the characteristic polynomial $T_{p,k}$ of the Hecke operator T_p acting on $S_k(1)$. This can be accomplished in several ways, each of which has advantages. The Eichler-Selberg trace formula (see Zagier's appendix to [6, Ch. III]), can be used to compute the trace of $T_{n,k}$, for $n = 1, p, p^2, \ldots, p^{d-1}$, where $d = \dim S_k(1)$, and from these traces it is straightforward to recover the characteristic polynomial of $T_{p,k}$. Using the trace formula, the time required to compute $\mathrm{Tr}(T_{n,k})$ grows "very quickly" in n (though *not* in k), so this method becomes unsuitable when the dimension is large or p is large, since p^{d-1} is huge. Another alternative is to use modular symbols of weight k, as in [7], but if one is only interested in characteristic polynomials, little is gained over more naive methods (modular symbols are most useful for investigating special values of L-functions).

In this section, we describe an algorithm to compute the characteristic polynomial of the Hecke operator $T_{p,k}$, which is adapted for the case when $p > 2$. It could be generalized to modular forms for $\Gamma_1(N)$, given a method to compute a basis of q-expansions to "low precision" for the space of modular forms of weight k and level N. By "low precision" we mean to precision $O(q^{dp+1})$, where $T_1, T_2, \ldots, T_d$ generate the Hecke algebra $\mathbf{T}$ as a ring. The algorithm described here uses nothing more than the basics of modular forms and some linear algebra; in particular, no trace formulas or modular symbols are involved.

1.7.1 Review of Basic Facts About Modular Forms

We briefly recall the background for this section. Fix an even integer k. Let $M_k(1)$ denote the space of weight k modular forms for $\mathrm{SL}_2(\mathbf{Z})$ and $S_k(1)$ the subspace of cusp forms. Thus $M_k(1)$ is a $\mathbf{C}$-vector space that is equipped with a ring

$$\mathbf{T} = \mathbf{Z}[\ldots T_{p,k} \ldots] \subset \mathrm{End}(M_k(1))$$

of Hecke operators. Moreover, there is an injective q-expansion map $M_k(1) \hookrightarrow \mathbf{C}[[q]]$. For example, when $k \geq 4$ there is an Eisenstein series E_k, which lies in $M_k(1)$. The first two Eisenstein series are

$$E_4(q) = \frac{1}{240} + \sum_{n\geq 1} \sigma_3(n)q^n \quad \text{and} \quad E_6(q) = \frac{1}{504} + \sum_{n\geq 1} \sigma_5(n)q^n,$$

where $q = e^{2\pi iz}$, $\sigma_{k-1}(n)$ is the sum of the $k-1$st power of the positive divisors. For every prime number p, the *Hecke operator* $T_{p,k}$ acts on $M_k(1)$ by

$$T_{p,k}\left(\sum_{n\geq 0} a_n q^n\right) = \sum_{n\geq 0} a_{np}q^n + p^{k-1}a_n q^{np}. \tag{1.7.1}$$

Proposition 1.7.1. *The set of modular forms $E_4^a E_6^b$ is a basis for $M_k(1)$, where a and b range through nonnegative integers such that $4a+6b=k$. Moreover, $S_k(1)$ is the subspace of $M_k(1)$ of elements whose q-expansions have constant coefficient 0.*

1.7.2 The Naive Approach

Let k be an even positive integer and p be a prime. Our goal is to compute the characteristic polynomial of the Hecke operator $T_{p,k}$ acting on $S_k(1)$. In practice, when k and p are both reasonably large, e.g., $k = 886$ and $p = 59$, then the coefficients of the characteristic polynomial are huge (the roots of the characteristic polynomial are $O(p^{k/2-1})$). A naive way to compute the characteristic polynomial of $T_{p,k}$ is to use (1.7.1) to compute the matrix $[T_{p,k}]$ of $T_{p,k}$ on the basis of Proposition 1.7.1, where E_4 and E_6 are computed to precision $p \dim M_k(1)$, and to then compute the characteristic polynomial of $[T_{p,k}]$ using, e.g., a modular algorithm (compute the characteristic polynomial modulo many primes, and use the Chinese Remainder Theorem). The difficulty with this approach is that the coefficients of the q-expansions of $E_4^a E_6^b$ to precision $p \dim M_k(1)$ quickly become enormous, so both storing them and computing with them is costly, and the components of $[T_{p,k}]$ are also huge so the characteristic polynomial is difficult to compute. See Example 1.2.3 above, where the coefficients of the q-expansions are already large.

1.7.3 The Eigenform Method

We now describe another approach to computing characteristic polynomials, which gets just the information required. Recall Maeda's conjecture from Section 1.6.1, which asserts that $S_k(1)$ is spanned by the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugates of a single eigenform $f = \sum b_n q^n$. For simplicity of exposition below, we assume this conjecture, though the algorithm can probably be modified to deal with the general case. We will refer to this eigenform f, which is well-defined up to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugacy, as *Maeda's eigenform.*

Lemma 1.7.2. *The characteristic polynomial of the pth coefficient b_p of Maeda's eigenform f, in the field $\mathbf{Q}(b_1, b_2, \ldots)$, is equal to the characteristic polynomial of $T_{p,k}$ acting on $S_k(1)$.*

Proof. The map $\mathbf{T} \otimes \mathbf{Q} \to \mathbf{Q}(b_1, b_2, \ldots)$ that sends $T_n \to b_n$ is an isomorphism of $\mathbf{Q}$-algebras. □

Victor Miller shows in his thesis that $S_k(1)$ has a unique basis $f_1, \ldots, f_d \in \mathbf{Z}[[q]]$ with $a_i(f_j) = \delta_{ij}$, i.e., the first $d \times d$ block of coefficients is the identity matrix. Again, in the general case, the requirement that there is such a basis can be avoided, but for simplicity of exposition we assume there is such a basis. We refer to the basis $f_1, \ldots, f_d$ as *Miller's basis.*

Algorithm 1.7.3. We assume in the algorithm that the characteristic polynomial of T_2 has no multiple roots (this is easy to check, and if false, you've found on interesting counterexample to the conjecture that the characteristic polynomial of T_2 has Galois group the full symmetric group).

1. Using Proposition 1.7.1 and Gauss elimination, we compute Miller's basis $f_1, \ldots, f_d$ to precision $O(q^{2d+1})$, where $d = \dim S_k(1)$. This is exactly the precision needed to compute the matrix of T_2.

2. Using (1.7.1), we compute the matrix $[T_2]$ of T_2 with respect to Miller's basis $f_1, \ldots, f_d$.

3. Using Algorithm 1.7.5 below we write down an eigenvector $\mathbf{e} = (e_1, \ldots, e_d) \in K^d$ for $[T_2]$. In practice, the components of T_2 are not very large, so the numbers involved in computing $\mathbf{e}$ are also not very large.

4. Since $e_1 f_1 + \cdots + e_d f_d$ is an eigenvector for T_2, our assumption that the characteristic polynomial of T_2 is square free (and the fact that $\mathbf{T}$ is commutative) implies that $e_1 f_1 + \cdots + e_d f_d$ is also an eigenvector for T_p. Normalizing, we see that up to Galois conjugacy,
$$b_p = \sum_{i=1}^{d} \frac{e_i}{e_1} \cdot a_p(f_i),$$
where the b_p are the coefficients of Maeda's eigenform f. For example, since the f_i are Miller's basis, if $p \leq d$ then
$$b_p = \frac{e_p}{e_1} \qquad \text{if } p \leq d,$$
since $a_p(f_i) = 0$ for all $i \neq p$ and $a_p(f_p) = 1$. Once we have computed b_p, we can compute the characteristic polynomial of T_p, because it is the minimal polynomial of b_p. We spend the rest of this section discussing how to make this step practical.

Computing b_p directly in step 4 is extremely costly because the divisions e_i/e_1 lead to massive coefficient explosion, and the same remark applies to computing the minimal polynomial of b_p. Instead we compute the reductions $\overline{b}_p$ modulo ℓ and the characteristic polynomial of $\overline{b}_p$ modulo ℓ for many primes ℓ, then recover *only* the characteristic polynomial of b_p using the Chinese Remainder Theorem. Deligne's bound on the magnitude of Fourier coefficients tells us how many primes we need to work modulo (we leave this analysis to the reader).

More precisely, the reduction modulo ℓ steps are as follows. The field K can be viewed as $\mathbf{Q}[x]/(f(x))$ where $f(x) \in \mathbf{Z}[x]$ is the characteristic polynomial of T_2. We work only modulo primes such that

1. $f(x)$ has no repeated roots modulo ℓ,
2. ℓ does not divide any denominator involved in our representation of $\mathbf{e}$, and
3. the image of e_1 in $\mathbf{F}_\ell[x]/(f(x))$ is invertible.

For each such prime, we compute the image $\overline{b}_p$ of b_p in the reduced Artin ring $\mathbf{F}_\ell[x]/(f(x))$. Then the characteristic polynomial of T_p modulo ℓ equals the characteristic polynomial of $\overline{b}_p$. This modular arithmetic is fast and requires negligible storage. Most of the time is spent doing the Chinese Remainder Theorem computations, which we do each time we do a few computations of the characteristic polynomial of T_p modulo ℓ.

Remark 1.7.4. If k is really large, so that steps 1 and 2 of the algorithm take too long or require too much memory, steps 1 and 2 can be performed modulo the prime ℓ. Since the characteristic polynomial of $T_{p,k}$ modulo ℓ does not depend on any choices, we will still be able to recover the original characteristic polynomial.

1.7.4 How to Write Down an Eigenvector over an Extension Field

The following algorithm, which was suggested to the author by H. Lenstra, produces an eigenvector defined over an extension of the base field.

Algorithm 1.7.5. Let A be an $n \times n$ matrix over an arbitrary field k and suppose that the characteristic polynomial $f(x) = x^n + \cdots + a_1 x + a_0$ of A is irreducible. Let α be a root of $f(x)$ in an algebraic closure $\overline{k}$ of k. Factor $f(x)$ over $k(\alpha)$ as $f(x) = (x - \alpha)g(x)$. Then for any element $v \in k^n$ the vector $g(A)v$ is either 0 or it is an eigenvector of A with eigenvalue α. The vector $g(A)v$ can be computed by finding Av, $A(Av)$, $A(A(Av))$, and then using that

$$g(x) = x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0,$$

where the coefficients c_i are determined by the recurrence

$$c_0 = -\frac{a_0}{\alpha}, \qquad c_i = \frac{c_{i-1} - a_i}{\alpha}.$$

We prove below that $g(A)v \neq 0$ for all vectors v not in a proper subspace of k^n. Thus with high probability, a "randomly chosen" v will have the property that $g(A)v \neq 0$. Alternatively, if $v_1, \ldots v_n$ form a basis for k^n, then $g(A)v_i$ must be nonzero for some i.

Proof. By the Cayley-Hamilton theorem [5, XIV.3] we have that $f(A) = 0$. Consequently, for any $v \in k^n$, we have $(A - \alpha)g(A)v = 0$ so that $Ag(A)v = \alpha v$. Since f is irreducible it is the polynomial of least degree satisfied by A and so $g(A) \neq 0$. Therefore $g(A)v \neq 0$ for all v not in the proper closed subspace $\ker(g(A))$. □

1.7.5 Simple Example: Weight 36, $p = 3$

We compute the characteristic polynomial of T_3 acting on $S_{36}(1)$ using the algorithm described above. A basis for $M_{36}(1)$ to precision $6 = 2\dim(S_{36}(1))$ is

$$\begin{aligned}
E_4^9 &= 1 + 2160q + 2093040q^2 + 1198601280q^3 + 449674832880q^4 \\
&\quad + 115759487504160q^5 + 20820305837344320q^6 + O(q^7) \\
E_4^6 E_6^2 &= 1 + 432q - 353808q^2 - 257501376q^3 - 19281363984q^4 \\
&\quad + 28393576094880q^5 + 11565037898063424q^6 + O(q^7) \\
E_4^3 E_6^4 &= 1 - 1296q + 185328q^2 + 292977216q^3 - 52881093648q^4 \\
&\quad - 31765004621280q^5 + 1611326503499328q^6 + O(q^7) \\
E_6^6 &= 1 - 3024q + 3710448q^2 - 2309743296q^3 + 720379829232q^4 \\
&\quad - 77533149038688q^5 - 8759475843314112q^6 + O(q^7)
\end{aligned}$$

The reduced row-echelon form (Miller) basis is:

$$\begin{aligned}
f_0 &= 1 + 6218175600q^4 + 15281788354560q^5 + 9026867482214400q^6 + O(q^7) \\
f_1 &= q + 57093088q^4 + 37927345230q^5 + 5681332472832q^6 + O(q^7) \\
f_2 &= q^2 + 194184q^4 + 7442432q^5 - 197264484q^6 + O(q^7) \\
f_3 &= q^3 - 72q^4 + 2484q^5 - 54528q^6 + O(q^7)
\end{aligned}$$

The matrix of T_2 with respect to the basis f_1, f_2, f_3 is

$$[T_2] = \begin{pmatrix} 0 & 34416831456 & 5681332472832 \\ 1 & 194184 & -197264484 \\ 0 & -72 & -54528 \end{pmatrix}$$

This matrix has (irreducible) characteristic polynomial

$$g = x^3 - 139656x^2 - 59208339456x - 1467625047588864.$$

If a is a root of this polynomial, then one finds that

$$\mathbf{e} = (2a + 108984, \quad 2a^2 + 108984a, \quad a^2 - 394723152a + 11328248114208)$$

is an eigenvector with eigenvalue a. The characteristic polynomial of T_3 is then the characteristic polynomial of e_3/e_1, which we can compute modulo ℓ for any prime ℓ such that $\overline{g} \in \mathbf{F}_\ell[x]$ is square free. For example, when $\ell = 11$,

$$\frac{e_3}{e_1} = \frac{a^2 + a + 3}{2a^2 + 7} = 9a^2 + 2a + 3,$$

which has characteristic polynomial

$$^3 + 10x^2 + 8x + 2.$$

If we repeat this process for enough primes ℓ and use the Chinese remainder theorem, we find that the characteristic polynomial of T_3 acting on $S_{36}(1)$ is

$$x^3 + 104875308x^2 - 144593891972573904x - 21175292105104984004394432.$$

References

[1] Kevin Buzzard, *On the eigenvalues of the Hecke operator T_2*, J. Number Theory **57** (1996), no. 1, 130–132. MR 96m:11033

[2] R. Coleman and B. Mazur, *The Eigencurve*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 1–113. MR 1 696 469

[3] D. W. Farmer and K. James, *The irreducibility of some level 1 Hecke polynomials*, Math. Comp. **71** (2002), no. 239, 1263–1270 (electronic). MR 2003e:11046

[4] N. M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350.

[5] S. Lang, *Algebra*, third ed., Addison-Wesley Publishing Co., Reading, Mass., 1993.

[6] ———, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original.

[7] L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations, Springer, 1994, pp. 59–94.

[8] T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda.

[9] J-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.