1

Modular Forms (W. Stein, Math 252, 10/22/03)

1.1 Modular Forms of Level 1

In this section, we view modular forms of level 1 both as holomorphic functions on the upper half plane and functions on lattices. We then define Hecke operators on modular forms, and derive explicit formulas for the action of Hecke operators on q-expansions. An excellent reference for the theory of modular forms of level 1 is Serre [10, Ch. 7].

1.1.1 The Definition

Let k be an integer. The space $S_k = S_k(1)$ of cusp forms of level 1 and weight k consists of all functions f that are holomorphic on the upper half plane $\mathfrak{h}$ and such that for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ one has

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau),$$

and f vanishes at infinity, in a sense which we will now make precise. The matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is in $\mathrm{SL}_2(\mathbf{Z})$, so $f(\tau+1) = f(\tau)$. Thus f passes to a well-defined function of $q(\tau) = e^{2\pi i\tau}$. Since for $\tau \in \mathfrak{h}$ we have $|q(\tau)| < 1$, we may view $f = f(q)$ is a function of q on the punctured open unit disc $\{q : 0 < |q| < 1\}$. The condition that $f(\tau)$ vanishes at infinity means that $f(q)$ extends to a holomorphic function on the open disc $\{z : |z| < 1\}$ so that $f(0) = 0$. Because holomorphic functions are represented by power series, there is a neighborhood of 0 such that

$$f(q) = \sum_{n=1}^{\infty} a_n q^n,$$

so for all $\tau \in \mathfrak{h}$ with sufficiently large imaginary part, $f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i\tau}$.

It will also be useful to consider the slightly large space $M_k(1)$ of holomorphic functions on $\mathfrak{h}$ that transform as above and are merely required to be holomorphic at infinity.

Remark 1.1.1. In fact, the series $\sum_{n=1}^{\infty} a_n e^{2\pi i\tau}$ converges for all $\tau \in \mathfrak{h}$. This is because the Fourier coefficients a_n are $O(n^{k/2})$ (see [7, Cor. 2.1.6, pg. 43]).

Remark 1.1.2. In [10, Ch. 7], the weight is defined in the same way, but in the notation our k is twice his k.

1.1.2 Some Examples and Conjectures

The space $S_k(1)$ of cusp forms is a finite-dimensional complex vector space. For k even we have $\dim S_k(1) = \lfloor k/12 \rfloor$ if $k \not\equiv 2 \pmod{12}$ and $\lfloor k/12 \rfloor - 1$ if $k \equiv 2 \pmod{12}$, except when $k = 2$ in which case the dimension is 0. For even k, the space $M_k(1)$ has dimension 1 more than the dimension of $S_k(1)$, except when $k = 2$ when both have dimension 0. (For proofs, see, e.g., [10, Ch. 7, §3].)

By the dimension formula mentioned above, the first interesting example is the space $S_{12}(1)$, which is a 1-dimensional space spanned by

$$\begin{aligned}\Delta(q) &= q \prod_{n=1}^{\infty} (1 - q^n)^{24} \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 \\ &\quad - 113643q^9 - 115920q^{10} + 534612q^{11} - 370944q^{12} - 577738q^{13} + \cdots\end{aligned}$$

That Δ lies in $S_{12}(1)$ is proved in [10, Ch. 7, §4.4] by expressing Δ in terms of elements of M_4 and M_6, and computing the q-expansion of the resulting expression.

The Ramanujan τ function $\tau(n)$ assigns to n the nth coefficient of $\Delta(q)$.

Conjecture 1.1.3 (Lehmer). *$\tau(n) \neq 0$ for all $n \geq 1$.*

This conjecture has been verified for $n \leq 22689242781695999$ (see Jordan and Kelly, 1999).

Conjecture 1.1.4 (Edixhoven). *Let p be a prime. There a polynomial time algorithm to compute $\tau(p)$, polynomial in the number of digits of p.*

Edixhoven has proposed an approach to find such an algorithm. His idea is to use ℓ-adic cohomology to find an analogue of the Schoof-Elkies-Atkin algorithm (which counts the number N_q of points on an elliptic curves over a finite field $\mathbf{F}_q$ by computing $N_q \mod \ell$ for many primes ℓ). Here's what Edixhoven has to say about the status of his conjecture (email, October 22, 2003):

> I have made a lot of progress on proving that my method runs in polynomial time, but it is not yet complete. I expect that all should be completed in 2004. For higher weights [...] you need to compute on varying curves such as $X_1(\ell)$ for ℓ up to $\log(p)$ say.
>
> An important by-product of my method is the computation of the mod ℓ Galois representations associated to Δ in time polynomial in ℓ. So, it should be seen as an attempt to make the Langlands correspondence for GL_2 over $\mathbf{Q}$ available computationally.

If $f \in M_k(1)$ and $g \in M_{k'}(1)$, then it is easy to see from the definitions that $fg \in M_{k+k'}(1)$. Moreover, $\oplus_{k\geq 0} M_k(1)$ is a commutative graded ring generated freely by $E_4 = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n)q^n$ and $E_6 = 1 - 504\sum_{n=1}^{\infty} \sigma_5(n)q^n$, where $\sigma_d(n)$ is the sum of the dth powers of the positive divisors of n (see [10, Ch.7, §3.2]).

Example 1.1.5. Because E_4 and E_6 generate, it is straightforward to write down a basis for any space $M_k(1)$. For example, the space $M_{36}(1)$ has basis

$$\begin{aligned}
f_1 &= 1 + 6218175600q^4 + 15281788354560q^5 + \cdots \\
f_2 &= q + 57093088q^4 + 37927345230q^5 + \cdots \\
f_3 &= q^2 + 194184q^4 + 7442432q^5 + \cdots \\
f_4 &= q^3 - 72q^4 + 2484q^5 + \cdots
\end{aligned}$$

1.1.3 Modular Forms as Functions on Lattices

In order to define Hecke operators, it will be useful to view modular forms as functions on lattices in $\mathbf{C}$.

A *lattice* $L \subset \mathbf{C}$ is a subring $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ for which $\omega_1, \omega_2 \in \mathbf{C}$ are linearly independent over $\mathbf{R}$. We may assume that $\omega_1/\omega_2 \in \mathfrak{h} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$. Let $\mathcal{R}$ be the set of all lattices in $\mathbf{C}$.

Proposition 1.1.6. *The elements of $\mathcal{R}$ are in bijection with pairs (E, ω), where E is an elliptic curve over $\mathbf{C}$ and $\omega \in \Omega^1_E$ is a nonzero holomorphic differential 1-form on E.*

Proof. Given $L \in \mathcal{R}$, by Weierstrass theory the quotient $\mathbf{C}/L$ is an elliptic curve, which is equipped with the distinguished differential ω induced by the differential $\mathrm{d}z$ on $\mathbf{C}$.

Conversely, if E is an elliptic curve over $\mathbf{C}$ and $\omega \in \Omega^1_E$ is a nonzero differential, we obtain a lattice L in $\mathbf{C}$ by integrating all homology classes:

$$L = \left\{ \int_\gamma \omega : \gamma \in \mathrm{H}_1(E(\mathbf{C}), \mathbf{Z}) \right\}.$$

Note that the differential induced by $\mathrm{d}z$ on $\mathbf{C}/L$ corresponds to the differential ω on E, since for $\alpha \in L = \mathrm{H}_1(\mathbf{C}/L, \mathbf{Z})$, we have

$$\int_0^\alpha \mathrm{d}z = [z]_0^\alpha = \alpha - 0 = \alpha,$$

and a differential is determined by the map it induces on homology. $\square$

Let

$$\mathcal{B} = \{(\omega_1, \omega_2) : \omega_1, \omega_2 \in \mathbf{C}, \quad \omega_1/\omega_2 \in \mathfrak{h}\},$$

be the set of ordered basis of lattices in $\mathbf{C}$, ordered so that $\omega_1/\omega_2 \in \mathfrak{h}$. There is a left action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathcal{B}$ given by

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(\omega_1, \omega_2) \mapsto (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$$

and $\mathrm{SL}_2(\mathbf{Z})\backslash\mathcal{B} \cong \mathcal{R}$. (The action is just the left action of matrices on column vectors, except we write (ω_1, ω_2) as a row vector since it takes less space.)

Given $f : \mathfrak{h} \to \mathbf{C}$, associate to f define function $F : \mathcal{R} \to \mathbf{C}$ as follows. On lattices of the special form $\mathbf{Z}\tau + \mathbf{Z}$, for $\tau \in \mathfrak{h}$, let $F(\mathbf{Z}\tau + \mathbf{Z}) = f(\tau)$. In order to extend F uniquely to a function on all lattices, suppose further that F satisfies the homogeneity condition $F(\lambda L) = \lambda^{-k} F(L)$, for any $\lambda \in \mathbf{C}$ and $L \in \mathcal{R}$. Then

$$F(\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) = \omega_2^{-k} F(\mathbf{Z}\omega_1/\omega_2 + \mathbf{Z}) = \omega_2^{-k} f(\omega_1/\omega_2).$$

Since $f(\tau) = F(\mathbf{Z}\tau + \mathbf{Z})$, the map $f \mapsto F$ is injective.

If $F : \mathcal{R} \to \mathbf{C}$ is any function that satisfies the homogeneity condition $F(\lambda L) = \lambda^{-k} F(L)$ then the function $f : \mathfrak{h} \to \mathbf{C}$ defined by $f(\tau) = F(\mathbf{Z}\tau + \mathbf{Z})$ transforms like a modular form, as the following computation shows: For any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ and $\tau \in \mathfrak{h}$, we have

$$\begin{aligned} f\left(\frac{a\tau + b}{c\tau + d}\right) &= F\left(\mathbf{Z}\frac{a\tau + b}{c\tau + d} + \mathbf{Z}\right) \\ &= F((c\tau + d)^{-1}\left(\mathbf{Z}(a\tau + b) + \mathbf{Z}(c\tau + d)\right)) \\ &= (c\tau + d)^k F\left(\mathbf{Z}(a\tau + b) + \mathbf{Z}(c\tau + d)\right) \\ &= (c\tau + d)^k F(\mathbf{Z}\tau + \mathbf{Z}) \\ &= (c\tau + d)^k f(\tau). \end{aligned}$$

Thus the elements of $M_k(1)$ are in bijection with functions $F : \mathcal{R} \to \mathbf{C}$ the are homogeneous of degree $-k$ and satisfy an appropriate holomorphy condition.

1.1.4 Hecke Operators

Define a map T_n from the free abelian group generated by all $\mathbf{C}$-lattices into itself by

$$T_n(L) = \sum_{(L:L')=n} L',$$

where the sum is over all sublattices $L' \subset L$ of index n. For any function $F : \mathcal{R} \to \mathbf{C}$ on lattices, define $T_n(F) : \mathcal{R} \to \mathbf{C}$ by

$$(T_n(F))(L) = n^{k-1} \sum_{(L:L')=n} F(L').$$

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR 91i:14034

[2] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[3] B. Edixhoven, *Néron models and tame ramification*, Compositio Math. **81** (1992), no. 3, 291–306. MR 93a:14041

[4] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[5] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[6] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

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

[8] D. Mumford, *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay, 1970, Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

[9] M. Rosen, *Abelian varieties over* **C**, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 79–101.

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