3.3 Hecke Operators

In this section we will only consider the modular curve $X_0(N)$ associated to the subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbf{Z})$ of matrices that are upper triangular modulo N. Much of what we say will also be true, possibly with slight modification, for $X_1(N)$, but not for arbitrary finite-index subgroups.

There is a commutative ring

$$\mathbf{T} = \mathbf{Z}[T_1, T_2, T_3, \ldots]$$

of *Hecke operators* that acts on $\mathrm{H}_1(X_0(N), \mathbf{R})$. We will frequently revisit this ring, which also acts on the Jacobian $J_0(N)$ of $X_0(N)$, and on modular forms. The ring $\mathbf{T}$ is generated by T_p, for p prime, and as a free $\mathbf{Z}$-module $\mathbf{T}$ is isomorphic to $\mathbf{Z}^g$, where g is the genus of $X_0(N)$. We will not prove these facts here (see).

Suppose

$$\{\alpha, \beta\} \in \mathrm{H}_1(X_0(N), \mathbf{R}),$$

is a modular symbol, with $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q})$. For $g \in \mathrm{M}_2(\mathbf{Z})$, write $g(\{\alpha, \beta\}) = \{g(\alpha), g(\beta)\}$. This is **not** a well-defined action of $\mathrm{M}_2(\mathbf{Z})$ on $\mathrm{H}_1(X_0(N), \mathbf{R})$, since $\{\alpha', \beta'\} = \{\alpha, \beta\} \in \mathrm{H}_1(X_0(N), \mathbf{R})$ does not imply that $\{g(\alpha'), g(\beta')\} = \{g(\alpha), g(\beta)\}$.

Example 3.3.1. Using MAGMA we see that the homology $\mathrm{H}_1(X_0(11), \mathbf{R})$ is generated by $\{-1/7, 0\}$ and $\{-1/5, 0\}$.

```
> M := ModularSymbols(11);   // Homology relative to cusps,
                             // with Q coefficients.
> S := CuspidalSubspace(M);  // Homology, with Q coefficients.
> Basis(S);
[ {-1/7, 0}, {-1/5, 0} ]
```

Also, we have $5\{0, \infty\} = \{-1/5, 0\}$.

```
> pi := ProjectionMap(S);    // The natural map M --> S.
> M.3;
{oo, 0}
> pi(M.3);
-1/5*{-1/5, 0}
```

Let $g = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $5\{g(0), g(\infty)\}$ is not equal to $\{g(-1/5), g(0)\}$, so g does not define a well-defined map on $\mathrm{H}_1(X_0(11), \mathbf{R})$.

```
> x := 5*pi(M!<1,[Cusps()|0,Infinity()]>);
> y := pi(M!<1,[-2/5,0]>);
> x;
{-1/5, 0}
> y;
-1*{-1/7, 0} + -1*{-1/5, 0}
> x eq y;
false
```

Definition 3.3.2 (Hecke operators). We define the *Hecke operator* T_p on $\mathrm{H}_1(X_0(N), \mathbf{R})$ as follows. When p is a prime with $p \nmid N$, we have

$$T_p(\{\alpha, \beta\}) = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}(\{\alpha, \beta\}) + \sum_{r=0}^{p-1} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix}(\{\alpha, \beta\}).$$

When $p \mid N$, the formula is the same, except that the first summand, which involves $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, is omitted.

Example 3.3.3. We continue with Example 3.3.1. If we apply the Hecke operator T_2 to both $5\{0,\infty\}$ and $\{-1/5,0\}$, the "non-well-definedness" cancels out.

```
> x := 5*pi(M!<1,[Cusps()|0,Infinity()]> +
     M!<1,[Cusps()|0,Infinity()]> + M!<1,[Cusps()|1/2,Infinity()]>);
> x;
-2*{-1/5, 0}
> y := pi(M!<1,[-2/5,0]>+ M!<1,[-1/10,0]> + M!<1,[2/5,1/2]>);
> y;
-2*{-1/5, 0}
```

Examples 3.3.1 shows that it is not clear that the definition of T_p given above makes sense. For example, if $\{\alpha,\beta\}$ is replaced by an equivalent modular symbol $\{\alpha',\beta'\}$, why does the formula for T_p give the same answer? We will not address this question further here, but will revisit it later when we have a more natural and intrinsic definition of Hecke operators. We only remark that T_p is induced by a "correspondence" from $X_0(N)$ to $X_0(N)$, so T_p preserve $\mathrm{H}_1(X_0(N),\mathbf{Z})$.

3.4 Modular Symbols and Rational Homology

In this section we sketch a beautiful proof, due to Manin, of a result that is crucial to our understanding of rationality properties of special values of L-functions. For example, Mazur and Swinnerton-Dyer write in [5, §6], "The modular symbol is essential for our theory of p-adic Mellin transforms," right before discussing this rationality result. Also, as we will see in the next section, this result implies that if E is an elliptic curve over $\mathbf{Q}$, then $L(E,1)/\Omega_E \in \mathbf{Q}$, which confirms a consequence of the Birch and Swinnerton-Dyer conjecture.

Theorem 3.4.1 (Manin). *For any $\alpha,\beta \in \mathbf{P}^1(\mathbf{Q})$, we have*

$$\{\alpha,\beta\} \in \mathrm{H}_1(X_0(N),\mathbf{Q}).$$

Proof (sketch). Since $\{\alpha,\beta\} = \{\alpha,\infty\} - \{\beta,\infty\}$, it suffices to show that $\{\alpha,\infty\} \in \mathrm{H}_1(X_0(N),\mathbf{Q})$ for all $\alpha \in \mathbf{Q}$. We content ourselves with proving that $\{0,\infty\} \in \mathrm{H}_1(X_0(N),\mathbf{Z})$, since the proof for general $\{0,\alpha\}$ is almost the same.

We will use that the eigenvalues of T_p on $\mathrm{H}_1(X_0(N),\mathbf{R})$ have absolute value bounded by $2\sqrt{p}$, a fact that was proved by Deligne. Let $p \nmid N$ be a prime. Then

$$T_p(\{0,\infty\}) = \{0,\infty\} + \sum_{r=0}^{p-1}\left\{\frac{r}{p},\infty\right\} = (1+p)\{0,\infty\} + \sum_{r=0}^{p-1}\left\{\frac{r}{p},0\right\},$$

so

$$(1+p-T_p)(\{0,\infty\}) = \sum_{r=0}^{p-1}\left\{0,\frac{r}{p}\right\}.$$

Since $p \nmid N$, the cusps 0 and r/p are equivalent (use the Euclidean algorithm to find a matrix in $\mathrm{SL}_2(\mathbf{Z})$ of the form $\left(\begin{smallmatrix} r & * \\ p & * \end{smallmatrix}\right)$), so the modular symbols $\{0,r/p\}$, for $r = 0,1,\ldots,p-1$ all lie in $\mathrm{H}_1(X_0(N),\mathbf{Z})$. Since the eigenvalues of T_p have absolute value at most $2\sqrt{p}$, the linear transformation $1+p-T_p$ of $\mathrm{H}_1(X_0(N),\mathbf{Z})$ is invertible. It follows that some integer multiple of $\{0,\infty\}$ lies in $\mathrm{H}_1(X_0(N),\mathbf{Z})$, as claimed. □

There are general theorems about the denominator of $\{\alpha,\beta\}$ in some cases. Example 3.3.1 above demonstrated the following theorem in the case $N=11$.

Theorem 3.4.2 (Ogg [7]). *Let N be a prime. Then the image*

$$[\{0,\infty\}] \in \mathrm{H}_1(X_0(N),\mathbf{Q})/\,\mathrm{H}_1(X_0(N),\mathbf{Z})$$

has order equal to the numerator of $(N-1)/12$.

3.5 Special Values of L-functions

This section is a preview of one of the central arithmetic results we will discuss in more generality later in this book.

The celebrated modularity theorem of Wiles et al. asserts that there is a correspondence between isogeny classes of elliptic curves E of conductor N and normalized new modular eigenforms $f=\sum a_n q^n \in S_2(\Gamma_0(N))$ with $a_n\in\mathbf{Z}$. This correspondence is characterized by the fact that for all primes $p\nmid N$, we have $a_p = p+1-\#E(\mathbf{F}_p)$.

Recall that a modular form for $\Gamma_0(N)$ of weight 2 is a holomorphic function $f:\mathfrak{h}\to\mathbf{C}$ that is "holomorphic at the cusps" and such that for all $\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in\Gamma_0(N)$,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z).$$

Suppose E is an elliptic curve that corresponds to a modular form f. If $L(E,s)$ is the L-function attached to E, then

$$L(E,s) = L(f,s) = \sum \frac{a_n}{n^s},$$

so, by a theorem of Hecke which we will prove [later], $L(f,s)$ is holomorphic on all $\mathbf{C}$. Note that $L(f,s)$ is the Mellin transform of the modular form f:

$$L(f,s) = (2\pi)^s\Gamma(s)^{-1}\int_0^{i\infty}(-iz)^s f(z)\frac{dz}{z}. \tag{3.5.1}$$

The Birch and Swinnerton-Dyer conjecture concerns the leading coefficient of the series expansion of $L(E,s)$ about $s=1$. A special case is that if $L(E,1)\neq 0$, then

$$\frac{L(E,1)}{\Omega_E} = \frac{\prod c_p\cdot\#\text{Ш}(E)}{\#E(\mathbf{Q})_{\mathrm{tor}}^2}.$$

Here $\Omega_E = |\int_{E(\mathbf{R})}\omega|$, where ω is a "Néron" differential 1-form on E, i.e., a generator for $\mathrm{H}^0(\mathcal{E},\Omega^1_{\mathcal{E}/\mathbf{Z}})$, where $\mathcal{E}$ is the Néron model of E. (The Néron model of E is the unique, up to unique isomorphism, smooth group scheme $\mathcal{E}$ over $\mathbf{Z}$, with generic fiber E, such that for all smooth schemes S over $\mathbf{Z}$, the natural map $\mathrm{Hom}_{\mathbf{Z}}(S,\mathcal{E})\to\mathrm{Hom}_{\mathbf{Q}}(S\times\mathrm{Spec}(\mathbf{Q}),E)$ is an isomorphism.) In particular, the conjecture asserts that for any elliptic curve E we have $L(E,1)/\Omega_E\in\mathbf{Q}$.

Theorem 3.5.1. *Let E be an elliptic curve over $\mathbf{Q}$. Then $L(E,1)/\Omega_E \in \mathbf{Q}$.*

Proof (sketch). By the modularity theorem of Wiles et al., E is modular, so there is a surjective morphism $\pi_E : X_0(N) \to E$, where N is the conductor of E. This implies that there is a newform f that corresponds to (the isogeny class of) E, with $L(f,s) = L(E,s)$. Also assume, without loss of generality, that E is "optimal" in its isogeny class, which means that if $X_0(N) \to E' \to E$ is a sequence of morphism whose composition is π_E and E' is an elliptic curve, then $E' = E$.

By Equation 3.5.1, we have

$$L(E,1) = 2\pi \int_0^{i\infty} -izf(z)dz/z. \tag{3.5.2}$$

If $q = e^{2\pi i z}$, then $dq = 2\pi i q dz$, so $2\pi i f(z)dz = dq/q$, and (3.5.2) becomes

$$L(E,1) = -\int_0^{i\infty} f(q)dq.$$

Recall that $\Omega_E = |\int_{E(\mathbf{R})} \omega|$, where ω is a Néron differential on E. The expression $f(q)dq$ defines a differential on the modular curve $X_0(N)$, and there is a rational number c, the *Manin constant*, such that $\pi_E^*\omega = cf(q)dq$. More is true: Edixhoven proved (as did Ofer Gabber) that $c \in \mathbf{Z}$; also Manin conjectured that $c = 1$ and Edixhoven proved (unpublished) that if $p \mid c$, then $p = 2, 3, 5, 7$.

A standard fact is that if

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

is the period lattice of E associated to ω, then $E(\mathbf{C}) \cong \mathbf{C}/\mathcal{L}$. Note that Ω_E is either the least positive real element of $\mathcal{L}$ or twice this least positive element (if $E(\mathbf{R})$ has two real components).

The next crucial observation is that by Theorem 3.4.1, there is an integer n such that $n\{0,\infty\} \in \mathrm{H}_1(X_0(N), \mathbf{Z})$. This is relevant because if

$$\mathcal{L}' = \left\{ \int_\gamma f(q)dq \, : \, \gamma \in \mathrm{H}_1(X_0(N), \mathbf{Z}) \right\} \subset \mathbf{C}.$$

then $\mathcal{L} = \frac{1}{c}\mathcal{L}' \subset \mathcal{L}'$. This assertion follows from our hypothesis that E is optimal and standard facts about complex tori and Jacobians, which we will prove later [in this course/book].

One can show that $L(E,1) \in \mathbf{R}$, for example, by writing down an explicit real convergent series that converges to $L(E,1)$. This series is used in algorithms to compute $L(E,1)$, and the derivation of the series uses properties of modular forms that we have not yet developed. Another approach is to use complex conjugation to define an involution $*$ on $\mathrm{H}_1(X_0(N), \mathbf{R})$, then observe that $\{0,\infty\}$ is fixed by $*$. (The involution $*$ is given on modular symbols by $*\{\alpha,\beta\} = \{-\alpha,-\beta\}$.)

Since $L(E,1) \in \mathbf{R}$, the integral

$$\int_{n\{0,\infty\}} f(q)dq = n\int_0^{i\infty} f(q)dq = -nL(E,1) \in \mathcal{L}'$$

lies in the subgroup $(\mathcal{L}')^+$ of elements fixed by complex conjugation. If c is the Manin constant, we have $cnL(E,1) \in \mathcal{L}^+$. Since Ω_E is the least nonzero element of $\mathcal{L}^+$ (or twice it), it follows that $2cnL(E,1)/\Omega_E \in \mathbf{Z}$, which proves the proposition. $\square$

References

[1] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[2] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133.

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

[4] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66. MR 47 #3396

[5] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61. MR 50 #7152

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

[7] A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 221–231. MR 49 #2743

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

[9] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.