8.3 Hecke Operators

Just as for modular forms, there is a *Hecke algebra* $\mathbb{T} = \mathbb{Z}[T_1, T_2, \ldots]$ of Hecke operators that act on $\mathbb{M}_k(\Gamma_0(N))$. Let

$$R_p = \left\{ \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} : r = 0, 1, \ldots, p-1 \right\} \cup \left\{ \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right\},$$

where we omit $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ if $p \mid N$. Then the *Hecke operator* T_p on $\mathbb{M}_k(\Gamma_0(N))$ is given by

$$T_p(x) = \sum_{g \in R} gx.$$

Notice when $p \nmid N$, that T_p is defined by summing over $p+1$ matrices that correspond to the $p+1$ sublattices of $\mathbb{Z} \times \mathbb{Z}$ of index p. This is exactly how we defined T_p on modular forms in Definition 2.4.1.

The ring $\mathbb{T}$ generated by all T_p acting on $\mathbb{M}_k(\Gamma_1(N), \mathbb{R})$ is commutative, and $\mathbb{M}_k(\Gamma_1(N), \mathbb{R})$ is non-canonically isomorphic as a $\mathbb{T}$-module to the space $M_k(\Gamma_1(N))$ of modular forms. Note that $\mathbb{M}_k(\Gamma_1(N), \mathbb{R})$ is a real vector space and $M_k(\Gamma_1(N))$ is a complex vector space, so this should be viewed as an isomorphism of $\mathbb{R}$-vector spaces.

8.3.1 General Definition of Hecke Operators

Let Γ be a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and suppose

$$\Delta \subset \mathrm{GL}_2(\mathbb{Q})$$

is a set such that $\Gamma\Delta = \Delta\Gamma = \Delta$ and $\Gamma\backslash\Delta$ is finite. For example, $\Delta = \Gamma$ trivially satisfies this condition. Also, if $\Gamma = \Gamma_1(N)$, then for any positive integer n, the set

$$\Delta_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \ : \ ad - bc = n, \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \pmod N \right\}$$

also satisfies this condition, as we will now prove.

Lemma 8.3.1. *We have*

$$\Gamma_1(N) \cdot \Delta_n = \Delta_n \cdot \Gamma_1(N) = \Delta_n$$

and

$$\Delta_n = \bigcup_{a,b} \Gamma_1(N) \cdot \sigma_a \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix},$$

where $\sigma_a \equiv \left(\begin{smallmatrix} 1/a & 0 \\ 0 & a \end{smallmatrix}\right) \pmod N$*, the union is disjoint and* $1 \le a \le n$ *with* $a \mid n$*,* $\gcd(a, N) = 1$*, and* $0 \le b < n/a$*. In particular, the set of cosets* $\Gamma_1(N)\backslash\Delta_n$ *is finite.*

Proof. If $\gamma \in \Gamma_1(N)$ and $\delta \in \Delta_n$, then

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \cdot \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \pmod N.$$

Thus $\Gamma_1(N)\Delta_n \subset \Delta_n$, and since $\Gamma_1(N)$ is a group $\Gamma_1(N)\Delta_n = \Delta_n$; likewise $\Delta_n\Gamma_1(N) = \Delta_n$.

For the coset decomposition, we first prove the statement for $N = 1$, i.e., for $\Gamma_1(N) = \mathrm{SL}_2(\mathbb{Z})$. If A is an arbitrary element of $M_2(\mathbb{Z})$ with determinant n, then using row operators on the left with determinant 1, i.e., left multiplication by elements of $\mathrm{SL}_2(\mathbb{Z})$, we can transform A into the form $\left(\begin{smallmatrix} a & b \\ 0 & n/a \end{smallmatrix}\right)$, with $1 \le a \le n$ and $0 \le b < n$. (Just imagine applying the Euclidean algorithm to the two entries in the first column of A. Then a is the gcd of the two entries in the first column, and the lower left entry is 0. Next subtract n/a from b until $0 \le b < n/a$.)

Next suppose N is arbitrary. Let $g_1, \ldots, g_r$ be such that

$$g_1\Gamma_1(N) \cup \cdots \cup g_r\Gamma_1(N) = \mathrm{SL}_2(\mathbb{Z})$$

is a disjoint union. If $A \in \Delta_n$ is arbitrary, then as we showed above, there is some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, so that $\gamma \cdot A = \left(\begin{smallmatrix} a & b \\ 0 & n/a \end{smallmatrix}\right)$, with $1 \le a \le n$ and $0 \le b < n/a$, and $a \mid n$. Write $\gamma = g_i \cdot \alpha$, with $\alpha \in \Gamma_1(N)$. Then

$$\alpha \cdot A = g_i^{-1} \cdot \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \pmod N.$$

It follows that

$$g_i^{-1} \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix}^{-1} \equiv \begin{pmatrix} 1/a & * \\ 0 & a \end{pmatrix} \pmod N.$$

Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$ and $\gcd(a, N) = 1$, there is $\gamma' \in \Gamma_1(N)$ such that

$$\gamma' g_i^{-1} \equiv \begin{pmatrix} 1/a & 0 \\ 0 & a \end{pmatrix} \pmod N.$$

We may then choose $\sigma_a = \gamma' g_i^{-1}$. Thus every $A \in \Delta_n$ is of the form $\gamma\sigma_a \left(\begin{smallmatrix} a & b \\ 0 & n/a \end{smallmatrix}\right)$, with $\gamma \in \Gamma_1(N)$ and a, b suitably bounded. This proves the second claim. □

Let any element $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$ act on the left on modular symbols $\mathcal{M}_k$ by

$$\delta(P\{\alpha, \beta\}) = P(dX - bY, -cX + aY)\{\delta(\alpha), \delta(\beta)\}.$$

(Until now we had only defined an action of $\mathrm{SL}_2(\mathbb{Z})$ on modular symbols.) For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, let

$$\tilde{g} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \det(g) \cdot g^{-1}. \tag{8.3.1}$$

Note that $\tilde{\tilde{g}} = g$. Also, $\delta P(X,Y) = (P \circ \tilde{g})(X,Y)$, where we set

$$\tilde{g}(X,Y) = (dX - bY, -cX + aY).$$

Suppose Γ and Δ are as above. Fix a finite set R of representatives for $\Gamma\backslash\Delta$. Let

$$T_\Delta : \mathcal{M}_k(\Gamma) \to \mathcal{M}_k(\Gamma)$$

be the linear map

$$T_\Delta(x) = \sum_{\delta \in R} \delta x,$$

This map is well defined because if $\gamma \in \Gamma$ and $x \in \mathcal{M}_k(\Gamma)$, then

$$\sum_{\delta \in R} \delta\gamma x = \sum_{\text{certain } \delta'} \gamma\delta' x = \sum_{\text{certain } \delta'} \delta' x = \sum_{\delta \in R} \delta x,$$

where we have used that $\Delta\Gamma = \Gamma\Delta$, and Γ acts trivially on $\mathcal{M}_k(\Gamma)$.

Let $\Gamma = \Gamma_1(N)$ and $\Delta = \Delta_n$. Then the nth Hecke operator T_n is T_{Δ_n}, and by Lemma 8.3.1,

$$T_n(x) = \sum_{a,b} \sigma_a \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix} \cdot x,$$

where a, b are as in Lemma 8.3.1.

Given this definition, we can compute the Hecke operators on $M_k(\Gamma_1(N))$ as follows. Write x as a modular symbol $P\{\alpha,\beta\}$, compute $T_n(x)$ as a modular symbol, then convert back to Manin symbols using (many!) continued fractions expansions. This is extremely inefficient, and fortunately Loïc Merel found a much better way, which we now describe (see also [Mer94] and also [Maz73]).

8.3.2 Hecke Operators on Manin Symbols

If S is a subset of $\mathrm{GL}_2(\mathbb{Q})$, let

$$\tilde{S} = \{\tilde{g} : g \in S\}.$$

Also, for any ring R and any subset $S \subset M_2(\mathbb{Z})$, let $R[S]$ denote the free R-module with basis the elements of S, so the elements of $R[S]$ are the finite R-linear combinations of the elements of S.

One of the main theorems of [Mer94] is that for any Γ, Δ as above, if one can find $\sum u_M M \in \mathbb{C}[M_2(\mathbb{Z})]$ and a map

$$\phi : \tilde{\Delta}\,\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z})$$

that satisfies a list of conditions (see below), then for any Manin symbol $[P,g] \in \mathcal{M}_k(\Gamma)$, we have

$$T_\Delta([P,g]) = \sum_{gM \in \tilde{\Delta}\,\mathrm{SL}_2(\mathbb{Z}) \text{ with } M \in \mathrm{SL}_2(\mathbb{Z})} u_M[\tilde{M}\cdot P,\ \phi(gM)].$$

Merel devotes substantial part of his paper to giving examples of ϕ and $\sum u_M M \in \mathbb{C}[M_2(\mathbb{Z})]$ that satisfy all his conditions.

When $\Gamma = \Gamma_1(N)$, the complicated list of conditions becomes simpler. Let $M_2(\mathbb{Z})_n$ be the set of 2×2 matrices with determinant n. An element

$$h = \sum u_M[M] \in \mathbb{C}[M_2(\mathbb{Z})_n]$$

satisfies condition C_n if for every $K \in M_2(\mathbb{Z})_n/\,\mathrm{SL}_2(\mathbb{Z})$, we have that

$$\sum_{M\in K} u_M([M\infty] - [M0]) = [\infty] - [0] \in \mathbb{C}[P^1(\mathbb{Q})]. \tag{8.3.2}$$

If h satisfies condition C_n, then for any Manin symbol $[P,g] \in M_k(\Gamma_1(N))$, Merel proves that

$$T_n([P,(u,v)]) = \sum_M u_M[P(aX+bY,\, cX+dY), (u,v)M]. \tag{8.3.3}$$

Here $(u,v) \in (\mathbb{Z}/N\mathbb{Z})^2$ corresponds to a coset of $\Gamma_1(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, as in Proposition 8.2.3, and if $(u',v') = (u,v)M \in (\mathbb{Z}/N\mathbb{Z})^2$, and $\gcd(u',v',N) \neq 1$, then we omit the corresponding summand.

For example, we will now check directly that the element

$$h_2 = \left[\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\right] + \left[\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}\right]$$

satisfies condition C_2. We have, as in the proof of Lemma 8.3.1 (but using elementary column operations), that

$$\begin{aligned} M_2(\mathbb{Z})_2/\,\mathrm{SL}_2(\mathbb{Z}) &= \left\{\begin{pmatrix} a & 0 \\ b & 2/a \end{pmatrix}\mathrm{SL}_2(\mathbb{Z}) : a = 1,2 \text{ and } 0 \le b < 2/a\right\} \\ &= \left\{\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\mathrm{SL}_2(\mathbb{Z}),\ \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}\mathrm{SL}_2(\mathbb{Z}),\ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\mathrm{SL}_2(\mathbb{Z})\right\}. \end{aligned}$$

To verify condition C_2, we consider each of the three elements of $M_2(\mathbb{Z})_2/\,\mathrm{SL}_2(\mathbb{Z})$ and check that (8.3.2) holds. We have that

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\mathrm{SL}_2(\mathbb{Z}),$$

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \in \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}\mathrm{SL}_2(\mathbb{Z}),$$

and

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\mathrm{SL}_2(\mathbb{Z}).$$

Thus if $K = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$, the left sum of (8.3.2) is $[\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)(\infty)] - [\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)(0)] = [\infty] - [0]$, as required. If $K = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 2 \end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$, then the left side of (8.3.2) is

$$[\left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)(\infty)] - [\left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)(0)] + [\left(\begin{smallmatrix} 1 & 0 \\ 1 & 2 \end{smallmatrix}\right)(\infty)] - [\left(\begin{smallmatrix} 1 & 0 \\ 1 & 2 \end{smallmatrix}\right)(0)] = [\infty] - [1] + [1] - [0] = [\infty] - [0].$$

Finally, for $K = \left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$ we also have $[\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)(\infty)] - [\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)(0)] = [\infty] - [0]$, as required. Thus by (8.3.3) we can compute T_2 on *any* Manin symbol, by summing over the action of the four matrices $\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right), \left(\begin{smallmatrix}2&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&2\end{smallmatrix}\right)$.

Proposition 8.3.2 (Merel)**.** *The element*

$$\sum_{\substack{a>b\geq 0\\ d>c\geq 0\\ ad-bc=n}} \left[\begin{pmatrix} a & b\\ c & d\end{pmatrix}\right] \in \mathbb{Z}[M_2(\mathbb{Z})_n]$$

satisfies condition C_n.

Merel's proof isn't too difficult, but takes two pages.

Remark 8.3.3. In [Cre97a, §2.4], Cremona discusses the work of Merel and Mazur on Heilbronn matrices in the special cases $\Gamma = \Gamma_0(N)$ and weight 2. He gives a fairly simple proof that the action of T_p on Manin symbols can be computed by summing the action of some set R_p of matrices of determinant p. He then describes the set R_p, and gives an efficient continued fractions algorithm for computing it (but he does not seem to prove that his description of R_p satisfies Merel's hypotheses). (Note: My experience is that Cremona's set R_p is significantly smaller than the sets appearing in Merel's paper, but when I've tried to use R_p to do certain more general higher-weight computations that are correct using Merel's sets, they do not work.)

8.3.3 Remarks on Complexity

Merel also gives another family $\mathcal{S}_n$ of matrices that satisfy condition C_n, and he proves that as $n \to \infty$,

$$\#\mathcal{S}_n \sim \frac{12\log(2)}{\pi^2}\cdot \sigma_1(n)\log(n),$$

where $\sigma_1(n)$ is the sum of the divisors of n. Thus for a fixed space $M_k(\Gamma)$ of modular symbols, one can compute the Hecke operator T_n using $O(\sigma_1(n)\log(n))$ arithmetic operations in the base field. Note that we've fixed $M_k(\Gamma)$, so we ignore the linear algebra involved in computation of a presentation; also, adding elements takes a bounded number of field operations when the space is fixed. Thus using Manin symbols the complexity of computing T_p, for p prime, is $O((p+1)\log(p))$ field operations, which is *exponential* in the number of digits of p.

8.3.4 Basmaji's Trick

There is a trick of Basmaji (see [Bas96]) for computing a matrix of T_n on $\mathbb{M}_k(\Gamma)$, when n is very large, and it is more efficient than one might naively expect. Basmaji's trick doesn't improve the big-oh complexity for a fixed space, but does improve the complexity by a constant factor of the dimension of $\mathbb{M}_k(\Gamma,\mathbb{Q})$.

Suppose we are interested in computing the matrix for T_n for some massive integer n, and that $\mathbb{M}_k(\Gamma,\mathbb{Q})$ as has fairly large dimension. The trick is as follows. Choose, a list

$$x_1 = [P_1, g_1], \ldots, x_r = [P_r, g_r] \in V = \mathbb{M}_k(\Gamma,\mathbb{Q})$$

of Manin symbols such that the map $\Psi : \mathbb{T} \to V^r$ given by

$$t \mapsto (tx_1, \ldots, tx_r)$$

is injective. In practice, it is often possible to do this with r "very small". Also, we emphasize that V^r is a $\mathbb{Q}$-vector space of dimension $r\cdot\dim(V)$.

Next find Hecke operators T_i, with i small, whose images form a basis for the image of Ψ. Now with the above data precomputed, which only required working with Hecke operators T_i for small i, we are ready to compute T_n with n huge. Compute $y_i = T_n(x_i)$, for each $i = 1, \ldots, r$, which we can compute using Heilbronn matrices since each $x_i = [P_i, g_i]$ is a Manin symbol. We thus obtain $\Psi(T_n) \in V^r$. Since we have precomputed Hecke operators T_j such that $\Psi(T_j)$ generate V^r, we can find a_j such that $\sum a_j\Psi(T_j) = \Psi(T_n)$. Then since Ψ is injective, we have $T_n = \sum a_j T_j$, which gives the full matrix of T_n on $M_k(\Gamma,\mathbb{Q})$.

8.4 Cuspidal Modular Symbols

Let $\mathbb{B}$ be the free abelian group on symbols $\{\alpha\}$, for $\alpha \in \mathbb{P}^1(\mathbb{Q})$, and set

$$\mathbb{B}_k = \mathbb{Z}_{k-2}[X,Y]\otimes\mathbb{B}.$$

Define a left action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{B}_k$ by

$$g.(P\{\alpha\}) = (gP)\{g(\alpha)\},$$

for $g \in \mathrm{SL}_2(\mathbb{Z})$. For any finite index subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, let $\mathbb{B}_k(\Gamma)$ be the quotient of $\mathbb{B}_k$ by the relations $x - g.x$ for all $g \in \Gamma$ and by any torsion. Thus $\mathbb{B}_k(\Gamma)$ is a torsion free abelian group.

The *boundary map* is the map

$$b : \mathbb{M}_k(\Gamma) \to \mathbb{B}_k(\Gamma)$$

given by extending the map

$$b(P\{\alpha,\beta\}) = P\{\beta\} - P\{\alpha\}$$

linearly. The space $\mathbb{S}_k(\Gamma)$ of *cuspidal modular symbols* is the kernel

$$\mathbb{S}_k(\Gamma) = \ker(\mathbb{M}_k(\Gamma) \to \mathbb{B}_k(\Gamma)),$$

so we have an exact sequence

$$0 \to \mathbb{S}_k(\Gamma) \to \mathbb{M}_k(\Gamma) \to \mathbb{B}_k(\Gamma).$$

One can prove that when $k > 2$ this sequence is exact on the right. Next we give a presentation of $\mathbb{B}_k(\Gamma)$ in terms of "boundary Manin symbols".

8.4.1 Boundary Manin Symbols

We give an explicit description of the boundary map in terms of Manin symbols for $\Gamma = \Gamma_1(N)$, then describe an efficient way to compute the boundary map.

Let $\mathcal{R}$ be the equivalence relation on $\Gamma\backslash\mathbb{Q}^2$ given by

$$[\Gamma \left(\begin{smallmatrix}\lambda u\\ \lambda v\end{smallmatrix}\right)] \sim \mathrm{sign}(\lambda)^k [\Gamma \left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)],$$

for any $\lambda \in \mathbb{Q}^*$. Denote by $B_k(\Gamma)$ the finite dimensional $\mathbb{Q}$-vector space with basis the equivalence classes $(\Gamma\backslash\mathbb{Q}^2)/\mathcal{R}$. The following two propositions are proved in [Mer94].

Proposition 8.4.1. *The map*

$$\mu : \mathbb{B}_k(\Gamma) \to B_k(\Gamma), \qquad P\left\{\frac{u}{v}\right\} \mapsto P(u,v)\left[\Gamma\begin{pmatrix}u\\ v\end{pmatrix}\right]$$

is well defined and injective. Here u and v are assumed coprime.

Thus the kernel of $\delta : \mathbb{S}_k(\Gamma) \to \mathbb{B}_k(\Gamma)$ is the same as the kernel of $\mu \circ \delta$.

Proposition 8.4.2. *Let $P \in V_{k-2}$ and $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We have*

$$\mu \circ \delta([P,(c,d)]) = P(1,0)[\Gamma \left(\begin{smallmatrix}a\\ c\end{smallmatrix}\right)] - P(0,1)[\Gamma \left(\begin{smallmatrix}b\\ d\end{smallmatrix}\right)].$$

We next describe how to explicitly compute $\mu \circ \delta : \mathbb{M}_k(N,\varepsilon) \to B_k(N,\varepsilon)$ by generalizing the algorithm of [Cre97a, §2.2]. To compute the image of $[P,(c,d)]$, with $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we must compute the class of $[\left(\begin{smallmatrix}a\\ c\end{smallmatrix}\right)]$ and of $[\left(\begin{smallmatrix}b\\ d\end{smallmatrix}\right)]$. Instead of finding a canonical form for cusps, we use a quick test for equivalence modulo scalars. In the following algorithm, by the ith symbol we mean the ith basis vector for a basis of $B_k(N,\varepsilon)$. This basis is constructed as the algorithm is called successively. We first give the algorithm, then prove the facts used by the algorithm in testing equivalence.

Algorithm 8.4.3 (Cusp Representation)**.** *Given a boundary Manin symbol $[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$ this algorithm outputs an integer i and a scalar α such that $[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$ is equivalent to α times the ith symbol found so far. (This algorithm is called repeatedly and maintains a running list of cusps seen so far.)*

1. Use Proposition 8.4.4 check whether or not $[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$ is equivalent, modulo scalars, to any cusp found so far. If so, return the index of the representative and the scalar. If not, record $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ in the representative list.
2. Using Proposition 8.4.7, check whether or not $[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$ is forced to equal zero by the relations. If it does not equal zero, return its position in the list and the scalar 1. If it equals zero, return the scalar 0 and the position 1; keep $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ in the list, and record that it is equivalent to zero.

In the case considered in Cremona's book [Cre97a], the relations between cusps involve only the trivial character, so they do not force any cusp classes to vanish. Cremona gives the following two criteria for equivalence.

Proposition 8.4.4 (Cremona)**.** *Consider $\left(\begin{smallmatrix}u_i\\ v_i\end{smallmatrix}\right)$, $i = 1,2$, with u_i, v_i integers such that $\gcd(u_i, v_i) = 1$ for each i.*

1. *There exists $g \in \Gamma_0(N)$ such that $g\left(\begin{smallmatrix}u_1\\ v_1\end{smallmatrix}\right) = \left(\begin{smallmatrix}u_2\\ v_2\end{smallmatrix}\right)$ if and only if*
$$s_1 v_2 \equiv s_2 v_1 \pmod{\gcd(v_1 v_2, N)}, \text{ where } s_j \text{ satisfies } u_j s_j \equiv 1 \pmod{v_j}.$$
2. *There exists $g \in \Gamma_1(N)$ such that $g\left(\begin{smallmatrix}u_1\\ v_1\end{smallmatrix}\right) = \left(\begin{smallmatrix}u_2\\ v_2\end{smallmatrix}\right)$ if and only if*
$$v_2 \equiv v_1 \pmod{N} \text{ and } u_2 \equiv u_1 \pmod{\gcd(v_1, N)}.$$

Proof. The first is [Cre97a, Prop. 2.2.3], and the second is [Cre92, Lem. 3.2]. $\square$

Algorithm 8.4.5 (Explicit Cusp Equivalence)**.** *Suppose $\left(\begin{smallmatrix}u_1\\ v_1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}u_2\\ v_2\end{smallmatrix}\right)$ are equivalent modulo $\Gamma_0(N)$. This algorithm computes a matrix $g \in \Gamma_0(N)$ such that $g\left(\begin{smallmatrix}u_1\\ v_1\end{smallmatrix}\right) = \left(\begin{smallmatrix}u_2\\ v_2\end{smallmatrix}\right)$.*

1. Let s_1, s_2, r_1, r_2 be solutions to $s_1u_1 - r_1v_1 = 1$ and $s_2u_2 - r_2v_2 = 1$.
2. Find integers x_0 and y_0 such that $x_0v_1v_2 + y_0N = 1$.
3. Let $x = -x_0(s_1v_2 - s_2v_1)/(v_1v_2, N)$ and $s_1' = s_1 + xv_1$.
4. Output $g = \left(\begin{smallmatrix}u_2 & r_2\\ v_2 & s_2\end{smallmatrix}\right) \cdot \left(\begin{smallmatrix}u_1 & r_1\\ v_1 & s_1'\end{smallmatrix}\right)^{-1}$, which sends $\left(\begin{smallmatrix}u_1\\ v_1\end{smallmatrix}\right)$ to $\left(\begin{smallmatrix}u_2\\ v_2\end{smallmatrix}\right)$.

Proof. See the proof of [Cre97a, Prop. 8.4.4]. $\square$

To see how the ε relations, for nontrivial ε, make the situation more complicated, observe that it is possible that $\varepsilon(\alpha) \neq \varepsilon(\beta)$ but

$$\varepsilon(\alpha)\left[\begin{pmatrix}u\\ v\end{pmatrix}\right] = \left[\gamma_\alpha\begin{pmatrix}u\\ v\end{pmatrix}\right] = \left[\gamma_\beta\begin{pmatrix}u\\ v\end{pmatrix}\right] = \varepsilon(\beta)\left[\begin{pmatrix}u\\ v\end{pmatrix}\right];$$

One way out of this difficulty is to construct the cusp classes for $\Gamma_1(N)$, then quotient out by the additional ε relations using Gaussian elimination. This is far too inefficient to be useful in practice because the number of $\Gamma_1(N)$ cusp classes can be unreasonably large. Instead, we give a quick test to determine whether or not a cusp vanishes modulo the ε-relations.

Lemma 8.4.6. *Suppose α and α' are integers such that $\gcd(\alpha, \alpha', N) = 1$. Then there exist integers β and β', congruent to α and α' modulo N, respectively, such that $\gcd(\beta, \beta') = 1$.*

Proof. By Exercise 8.2 the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. By the Euclidean algorithm, there exist integers x, y and z such that $x\alpha + y\alpha' + zN = 1$. Consider the matrix $\left(\begin{smallmatrix}y & -x\\ \alpha & \alpha'\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and take β, β' to be the bottom row of a lift of this matrix to $\mathrm{SL}_2(\mathbb{Z})$. $\square$

Proposition 8.4.7. *Let N be a positive integer and ε a Dirichlet character of modulus N. Suppose $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$ is a cusp with u and v coprime. Then $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$ vanishes modulo the relations*

$$[\gamma\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)] = \varepsilon(\gamma)\,[\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)], \qquad \textit{all } \gamma \in \Gamma_0(N)$$

if and only if there exists $\alpha \in (\mathbb{Z}/N\mathbb{Z})^*$, with $\varepsilon(\alpha) \neq 1$, such that

$$\begin{aligned} v &\equiv \alpha v \pmod{N},\\ u &\equiv \alpha u \pmod{\gcd(v,N)}. \end{aligned}$$

Proof. First suppose such an α exists. By Lemma 8.4.6 there exists $\beta, \beta' \in \mathbb{Z}$ lifting α, α^{-1} such that $\gcd(\beta,\beta') = 1$. The cusp $\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)$ has coprime coordinates so, by Proposition 8.4.4 and our congruence conditions on α, the cusps $\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$ are equivalent by an element of $\Gamma_1(N)$. This implies that $\left[\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)\right] = [\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)]$. Since $\left[\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)\right] = \varepsilon(\alpha)\,[\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)]$ and $\varepsilon(\alpha) \neq 1$, we have $[\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)] = 0$.

Conversely, suppose $[\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)] = 0$. Because all relations are two-term relations, and the $\Gamma_1(N)$-relations identify $\Gamma_1(N)$-orbits, there must exists α and β with

$$\left[\gamma_\alpha \begin{pmatrix}u\\v\end{pmatrix}\right] = \left[\gamma_\beta \begin{pmatrix}u\\v\end{pmatrix}\right] \qquad \text{and } \varepsilon(\alpha) \neq \varepsilon(\beta).$$

Indeed, if this did not occur, then we could mod out by the ε relations by writing each $[\gamma_\alpha\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)]$ in terms of $[\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)]$, and there would be no further relations left to kill $[\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)]$. Next observe that

$$\left[\gamma_{\beta^{-1}\alpha}\begin{pmatrix}u\\v\end{pmatrix}\right] = \left[\gamma_{\beta^{-1}}\gamma_\alpha\begin{pmatrix}u\\v\end{pmatrix}\right] = \varepsilon(\beta^{-1})\left[\gamma_\alpha\begin{pmatrix}u\\v\end{pmatrix}\right] = \varepsilon(\beta^{-1})\left[\gamma_\beta\begin{pmatrix}u\\v\end{pmatrix}\right] = \left[\begin{pmatrix}u\\v\end{pmatrix}\right].$$

Applying Proposition 8.4.4 and noting that $\varepsilon(\beta^{-1}\alpha) \neq 1$ shows that $\beta^{-1}\alpha$ satisfies the properties of the "α" in the statement of the proposition. $\square$

We enumerate the possible α appearing in Proposition 8.4.7 as follows. Let $g = (v, N)$ and list the $\alpha = v \cdot \frac{N}{g} \cdot a + 1$, for $a = 0, \ldots, g-1$, such that $\varepsilon(\alpha) \neq 0$.

8.5 The Pairing Between Modular Symbols and Modular Forms

In this section we define a pairing between modular symbols and modular forms, and prove that the Hecke operators respect this pairing. We also define an involution on modular symbols, and study its relationship with the pairing. This pairing is crucial in much that follows, because it gives rise to period maps from modular symbols to certain complex vector spaces.

Fix an integer weight $k \geq 2$ and a finite-index subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. Let $M_k(\Gamma)$ denote the space of holomorphic modular forms of weight k for Γ, and $S_k(\Gamma)$ its cuspidal subspace. Following [Mer94, §1.5], let

$$\overline{S}_k(\Gamma) = \{\overline{f} : f \in S_k(\Gamma)\}$$

denote the space of *antiholomorphic* cuspforms. Here $\overline{f}$ is the function on $\mathfrak{h}^*$ given by $\overline{f}(z) = \overline{f(z)}$.

Define a pairing

$$(S_k(\Gamma) \oplus \overline{S}_k(\Gamma)) \times \mathbb{M}_k(\Gamma) \to \mathbb{C} \tag{8.5.1}$$

by

$$\langle (f_1, f_2), P\{\alpha,\beta\}\rangle = \int_\alpha^\beta f_1(z)P(z,1)dz + \int_\alpha^\beta f_2(z)P(\overline{z},1)d\overline{z},$$

and extending linearly. Here the integral is a complex path integral along a great circle (or vertical line) from α to β (so, e.g., write $z(t) = x(t) + iy(t)$, where $(x(t), y(t))$ traces out the path, and consider two real integrals; see any introductory book on complex analysis for more details).

The integration pairing is well defined, which means that if we replace $P\{\alpha,\beta\}$ by an equivalent modular symbols (equivalent modulo the left action of Γ), then the integral is the same. This follows from the change of variables formulas for integration and the fact that $f_1 \in S_k(\Gamma)$ and $f_2 \in \overline{S}_k(\Gamma)$. For example, if $k = 2$, $g \in \Gamma$ and $f \in S_k(\Gamma)$, then

$$\begin{aligned} \langle f, g\{\alpha,\beta\}\rangle &= \langle f, \{g(\alpha), g(\beta)\}\rangle\\ &= \int_{g(\alpha)}^{g(\beta)} f(z)dz\\ &= \int_\alpha^\beta f(g(z))dg(z)\\ &= \int_\alpha^\beta f(z)dz = \langle f, \{\alpha,\beta\}\rangle, \end{aligned}$$

where in the last step we use that f is a weight 2 modular form.

Remark 8.5.1. The integration pairing is related to special values of L-functions. The L-function attached to a cusp form $f = \sum a_n q^n \in S_k(\Gamma_1(N))$ is

$$L(f,s) = (2\pi)^s\Gamma(s)^{-1}\int_0^\infty f(it)t^s\frac{dt}{t} \tag{8.5.2}$$

Note that one can show that $L(f,s) = \sum_{n=1}^\infty \frac{a_n}{n^s}$ by switching the order of summation and integration, which is justified using standard estimates on $|a_n|$ (see, e.g., [Kna92, §VIII.5]).

For each integer j with $1 \leq j \leq k-1$, we have setting $s = j$ and making the change of variables $t \mapsto -it$ in (8.5.2), that

$$L(f,j) = \frac{(-2\pi i)^j}{(j-1)!}\cdot\left\langle f,\ X^{j-1}Y^{k-2-(j-1)}\{0,\infty\}\right\rangle. \tag{8.5.3}$$

The integers j as above are called *critical integers*, and when f is an eigenform, they have deep conjectural significance. We will discuss tricks to efficiently compute $L(f, j)$ later in this book.

Theorem 8.5.2 (Shokoruv)**.** *The pairing $\langle\cdot\,,\,\cdot\rangle$ is nondegenerate when restricted to cuspidal modular symbols:*

$$\langle\cdot\,,\,\cdot\rangle : (S_k(\Gamma) \oplus \overline{S}_k(\Gamma)) \times \mathbb{S}_k(\Gamma) \to \mathbb{C}.$$

The pairing is also compatible with Hecke operators. Before proving this, we define an action of *Hecke operators* on $M_k(\Gamma_1(N))$ and on $\overline{S}_k(\Gamma_1(N))$. The definition is very similar to the one we gave in Section 2.4 for modular forms of level 1. For a positive integer n, let R_n be a set of coset representatives for $\Gamma_1(N)\backslash\Delta_n$ from Lemma 8.3.1. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$ and $f \in M_k(\Gamma_1(N))$ set

$$f|[\gamma]_k = \det(\gamma)^{k-1}(cz+d)^{-k} f(\gamma(z)).$$

Also, for $f \in \overline{S}_k(\Gamma_1(N))$, set

$$f|[\gamma]'_k = \det(\gamma)^{k-1}(c\overline{z}+d)^{-k} f(\gamma(z)).$$

Then for $f \in M_k(\Gamma_1(N))$,

$$T_n(f) = \sum_{\gamma\in R_n} f|[\gamma]_k$$

and for $f \in \overline{S}_k(\Gamma_1(N))$,

$$T_n(f) = \sum_{\gamma\in R_n} f|[\gamma]'_k.$$

This agrees with the definition from 2.4 when $N = 1$.

Remark 8.5.3. If Γ is an arbitrary finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then we can define operators T_Δ on $M_k(\Gamma)$ for any Δ with $\Delta\Gamma = \Gamma\Delta = \Delta$ and $\Gamma\backslash\Delta$ finite. For concreteness we do not do the general case here or in the theorem below, but the proof is exactly the same (see [Mer94, §1.5]).

Finally we prove the promised Hecke compatibility of the pairing. This proof should convince you that the definition of modular symbols is sensible, in that they are "natural" expressions to integrate against modular forms.

Theorem 8.5.4. *If $f = (f_1, f_2) \in S_k(\Gamma_1(N)) \oplus \overline{S}_k(\Gamma_1(N))$ and $x \in \mathbb{M}_k(\Gamma_1(N))$, then for any n,*

$$\langle T_n(f), x\rangle = \langle f, T_n(x)\rangle.$$

Proof. We exactly follow [Mer94, §2.1], and will only prove the theorem when $f = f_1 \in S_k(\Gamma_1(N))$, the proof in the general case being the same.

Let $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, $P \in \mathbb{Z}_{k-2}[X, Y]$, and for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, set $j(g, z) = (cz+d)$. Let n be any positive integer, and let R_n be a set of coset representatives for $\Gamma_1(N)\backslash\Delta_n$ from Lemma 8.3.1.

We have

$$\begin{aligned}\langle T_n(f), P\{\alpha,\beta\}\rangle &= \int_\alpha^\beta T_n(f)P(z,1)dz \\ &= \sum_{\delta\in R}\int_\alpha^\beta \det(\delta)^{k-1} f(\delta(z)) j(\delta,z)^{-k} P(z,1)dz.\end{aligned}$$

Now for each summand corresponding to the $\delta \in R$, make the change of variables $u = \delta z$. Thus we make $\#R$ change of variables. Also, recall the notation from (8.3.1), which we will use below.

$$\begin{aligned}\langle T_n(f), P\{\alpha,\beta\}\rangle &= \sum_{\delta\in R}\int_{\delta(\alpha)}^{\delta(\beta)} \det(\delta)^{k-1} f(u) j(\delta,\delta^{-1}(u))^{-k} P(\delta^{-1}(u),1) d(\delta^{-1}(u)) \\ &= \sum_{\delta\in R}\int_{\delta(\alpha)}^{\delta(\beta)} \det(\delta)^{k-1} f(u) j(\tilde\delta,u)^{k} \det(\delta)^{-k} P(\tilde\delta(u),1)\frac{\det(\delta)du}{j(\tilde\delta,u)^2} \\ &= \sum_{\delta\in R}\int_{\delta(\alpha)}^{\delta(\beta)} f(u) j(\tilde\delta,u)^{k-2} P(\tilde\delta(u),1)du \\ &= \sum_{\delta\in R}\int_{\delta(\alpha)}^{\delta(\beta)} f(u)\cdot((\delta.P)(u,1))du \\ &= \langle f, T_n(P\{\alpha,\beta\})\rangle.\end{aligned}$$

The second equality is the trickiest. First, note that $\delta^{-1}(u) = \tilde\delta(u)$, since a linear fractional transformation is unchanged by a nonzero rescaling of a matrix that induces it. Thus by the quotient rule, using that $\tilde\delta$ has determinant $\det(\delta)$, we see that

$$d(\delta^{-1}(u)) = \frac{\det(\delta)du}{j(\tilde\delta,u)^2}.$$

The other part of the second equality asserts that

$$j(\delta,\delta^{-1}(u))^{-k} P(\delta^{-1}(u),1) = j(\tilde\delta,u)^k \det(\delta)^{-k} P(\tilde\delta(u),1). \tag{8.5.4}$$

From the definitions, and again using that $\delta^{-1}(u) = \tilde\delta(u)$, we see that

$$j(\delta,\delta^{-1}(u)) = \frac{\det(\delta)}{j(\tilde\delta,u)},$$

which proves that (8.5.4) holds. In the third equality, we use that

$$(\delta.P)(u,1) = j(\tilde\delta,u)^{k-2} P(\tilde\delta(u),1).$$

To see this, note that $P(X,Y) = P(X/Y,1)\cdot Y^{k-2}$. Using this we see that

$$\begin{aligned}(\delta.P)(X,Y) &= (P\circ\tilde\delta)(X,Y) \\ &= P\left(\tilde\delta\left(\frac{X}{Y}\right),1\right)\cdot\left(-c\cdot\frac{X}{Y}+a\right)^{k-2}\cdot Y^{k-2}.\end{aligned}$$

Now substituting $(u,1)$ for $(X,1)$, we see that

$$(\delta.P)(u,1) = P(\tilde{\delta}(u),1)\cdot(-cu+a)^{k-2},$$

as required. □

Remark 8.5.5. The theorem is true more generally for any Γ and any operator T_Δ, via the same proof.

Suppose that Γ is finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that if $\eta = \left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$, then

$$\eta\Gamma\eta = \Gamma.$$

For example, $\Gamma = \Gamma_1(N)$ satisfies this condition. There is an involution ι^* on $\mathbb{M}_k(\Gamma)$ given by

$$\iota^*(P(X,Y)\{\alpha,\beta\}) = -P(X,-Y)\{-\alpha,-\beta\}, \tag{8.5.5}$$

which we call the *star involution*. On Manin symbols, ι^* it is

$$\iota^*[P,(u,v)] = -[P(-X,Y),(-u,v)].$$

Let $\mathbb{S}_k(\Gamma)^+$ be the $+1$ eigenspace for ι^* and $\mathbb{S}_k(\Gamma)^-$ the -1 eigenspace. There is also a map ι on modular forms, which is adjoint to ι^*.

Remark 8.5.6 (WARNING)**.** Notice the $-$ sign in front of $-P(X,-Y)\{-\alpha,-\beta\}$ in (8.5.5). This sign is missing in [Cre97a], which is a potential source of confusion.

We now state the final result about the pairing, which explains how modular symbols and modular forms are related.

Theorem 8.5.7. *The pairing $\langle\cdot,\cdot\rangle$ restricts to give nondegenerate Hecke compatible bilinear pairings*

$$\mathbb{S}_k(\Gamma)^+\times S_k(\Gamma)\to\mathbb{C} \qquad \textit{and} \qquad \mathbb{S}_k(\Gamma)^-\times\overline{S}_k(\Gamma)\to\mathbb{C}.$$

In light of the Peterson inner product, the above theorem implies that there is a canonical isomorphism of $\mathbb{T}'$-modules

$$\mathbb{S}_k(\Gamma,\mathbb{C})^+\cong S_k(\Gamma),$$

where $\mathbb{T}'$ is the anemic Hecke algebra, i.e., the subring of $\mathbb{T}$ generated by Hecke operators T_n with $\gcd(n,N)=1$. In fact, one can prove, e.g., using Eichler-Shimura cohomology, that there is a non-canonical isomorphism over the full Hecke algebra

$$\mathbb{M}_k(\Gamma,\mathbb{C})\cong M_k(\Gamma)\oplus\overline{S}_k(\Gamma).$$

Remark 8.5.8. We make some remarks about computing the boundary map of Section 8.4.1 when working in the ±1 quotient. Let s be a sign, either $+1$ or -1. To compute $\mathbb{S}_k(N,\varepsilon)_s$ it is necessary to replace $B_k(N,\varepsilon)$ by its quotient modulo the additional relations $[\left(\begin{smallmatrix}-u\\v\end{smallmatrix}\right)] = s\,[\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)]$ for all cusps $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$. Algorithm 8.4.3 can be modified to deal with this situation as follows. Given a cusp $x=\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$, proceed as in Algorithm 8.4.3 and check if either $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}-u\\v\end{smallmatrix}\right)$ is equivalent (modulo scalars) to any cusp seen so far. If not, use the following trick to determine whether the ε and s-relations kill the class of $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$: use the unmodified Algorithm 8.4.3 to compute the scalars α_1,α_2 and indices i_1, i_2 associated to $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}-u\\v\end{smallmatrix}\right)$, respectively. The s-relation kills the class of $\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$ if and only if $i_1=i_2$ but $\alpha_1\neq s\alpha_2$.

8.6 Explicitly Computing $\mathbb{M}_k(\Gamma_0(N)$

In this section we explicitly compute $\mathbb{M}_k(\Gamma_0(N))$ for various k and N. We represent Manin symbols for $\Gamma_0(N)$ as triples (i,u,v), where $(u,v)\in\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, and (i,u,v) corresponds to $[X^iY^{k-2-i},(u,v)]$ in the usual notation. Also, recall that (u,v) corresponds to the right coset in $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$ that contains a matrix $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ with $(u,v)\equiv(c,d)$ as elements of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, i.e., up to rescaling by an element of $(\mathbb{Z}/N\mathbb{Z})^*$.

8.6.1 Computing $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$

In this section we give an algorithm to compute a canonical representative for each element of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. This algorithm is extremely important because modular symbols implementations call it a huge number of times. A more naive approach would be to store all pairs $(u,v)\in(\mathbb{Z}/N\mathbb{Z})^2$, and a fixed reduced representative, but this wastes a huge amount of memory. For example, if $N=10^5$, we would store an array of

$$2\cdot10^5\cdot10^5 = 20\text{ billion integers.}$$

Another approach to enumerating $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ is described at the end of [Cre97a, §2.2]. We use that it is easy to test whether two pairs $(u_0,v_0),(u_1,v_1)$ define the same element of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$; they do if and only if we have equality of cross terms $u_0v_1=v_0u_1 \pmod N$ (see [Cre97a, Prop. 2.2.1]). So we consider the 0-based list of elements

$$(1,0),(1,1),\ldots,(1,N-1),(0,1)$$

concated with the list of non-equivalent elements (d,a) for $d\mid N$ and $a=1,\ldots,N-1$, checking each time we add a new element to our list (of (d,a)) whether we have already seen it.

Given a random pair (u,v) the problem is then to find the index into our list of the equivalent representative in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. We use the following algorithm, which finds a canonical representative for each element of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Given an arbitrary (u, v), we first find the canonical equivalent elements (u', v'). If $u' = 1$, then the index is v'. If $u' \neq 1$, we find the corresponding element in an explicit sorted list, e.g., using binary search.

In the following algorithm, $a \pmod N$ denotes the residue of a modulo N that satisfies $0 \leq a < N$.

Algorithm 8.6.1 (Reduction in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ to Canonical Form)**.** Given integers u and v and a positive integer N, this algorithm outputs a pair u_0, v_0 such that $(u, v) \equiv (u_0, v_0)$ as elements of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ and $s \in \mathbb{Z}$ such that $(u, v) = (su_0, sv_0) \pmod{\mathbb{Z}/n\mathbb{Z}}$. Moreover, the element (u_0, v_0) does not depend on the class of (u, v), i.e., for any s with $\gcd(N, s) = 1$ the input (su, sv) also outputs (u_0, v_0). If (u, v) is not in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, this algorithm outputs $(0, 0), 0$.

1. [Reduce] Reduce both u and v modulo N.
2. [Easy $(0, 1)$ case] If $u = 0$ check that $\gcd(v, N) = 1$. If so, return $s = 1$ and $(0, 1)$; otherwise return 0.
3. [GCD] Compute $g = \gcd(u, N)$ and $s, t \in \mathbb{Z}$ such that $g = su + tN$.
4. [Not in P^1?] We have $\gcd(u, v, N) = \gcd(g, v)$, so if $\gcd(g, v) > 1$, then $(u, v) \notin \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, and we return 0.
5. [Pseudo-Inverse] Now $g = su + tN$, so we may think of s as "pseudo-inverse" of $u \pmod N$, in the sense that su is as close as possible to being 1 modulo N. Note that since $g \mid u$, changing s modulo N/g does not change $su \pmod N$. We can adjust s modulo N/g so it is coprime to N (by adding multiples of N/g to s. (This is because $1 = su/g + tN/g$, so s is a unit mod N/g, and the map $(\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/(N/g)\mathbb{Z})^*$ is surjective, e.g., as we saw in the proof of Algorithm 4.6.1.)
6. [Multiply by s] Multiply (u, v) by s, replacing (u, v) by the equivalent element (g, sv) of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.
7. [Normalize] Compute the pair (g, v') equivalent to (g, v) that minimizes v.
   (a) [Easy case] If $g = 1$ this pair is $(1, v)$.
   (b) [Enumerate and find best] Otherwise, note that if $1 \neq t \in (\mathbb{Z}/N\mathbb{Z})^*$ and $tg \equiv g \pmod N$, then $(t-1)g \equiv 0 \pmod N$, so $t-1 = kN/g$ for some k with $1 \leq k \leq g-1$. Then for $t = 1 + kN/g$ coprime to N, we have $(gt, vt) = (g, v+kvN/g)$. So we compute all pairs $(g, v+kvN/g)$ and pick out the one that minimizes the least nonnegative residue of vt modulo N.
   (c) [Invert s and Output] The s that we have computed in the above steps multiples the input (u, v) to give the output (u_0, v_0). Thus we invert it, since the output scalar is supposed to multiply (u_0, v_0) to give (u, v).

Remark 8.6.2. Allan Steel and the author jointly came up with Algorithm 8.6.1.

Remark 8.6.3. Alternatively one could use that

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{p \mid N} \mathbb{P}^1(\mathbb{Z}/p^{\nu_p}\mathbb{Z}),$$

that that it is relatively easy to enumerate the elements of $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ for a prime power p^n.

Algorithm 8.6.4 (List $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$)**.** *Given an integer $N > 1$, this algorithm makes a sorted list of the distinct canonical representatives (c, d) of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ with $c \neq 0, 1$, as output by Algorithm 8.6.1.*

1. For each $c = 1, \ldots, N-1$ with $g = \gcd(c, N) > 1$ do the following:
   (a) Use Algorithm 8.6.1 to compute the canonical representative (u', v') equivalent to $(c, 1)$, and it include it in the list.
   (b) If $g = c$, for each $d = 2, \ldots, N-1$ with $\gcd(d, N) > 1$ and $\gcd(c, d) = 1$, append the normalized representative of (c, d) to the list.
2. Sort the list
3. Pass through the sorted list and delete any duplicates.