**18.786 Number Theory II** **Spring 2024**
**Problem Set #5** **Due: 4/19/2024**

## Description

Your solutions should be written up in latex and submitted as a pdf-file on Gradescope before midnight on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators or the name of your group on pset partners, and any references you consulted. If there are none write "**Sources consulted: none**" at the top of your solution.

## Problem 1. Modular symbols for $S_2(\Gamma_0(N))$ (100 points)

Modular symbols are one of the main techniques used to explicitly compute modular forms (both Sage and Magma rely on them), and they also have several theoretical applications. Let us first fix some notation. Let $\mathbf{H} := \{\tau \in \mathbb{C} : \operatorname{Im}\tau > 0\}$ denote the extended upper half plane, let $\mathbb{P}^1(\mathbb{Q}) := \mathbb{Q} \cup \{\infty\}$, and let

$$\mathbf{H}^* := \mathbf{H} \cup \mathbb{P}^1(\mathbb{Q})$$

denote the extended upper half plane. Recall that the cusps of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ constitute a single orbit $\mathbb{P}^1(\mathbb{Q})$. For any distinct pair $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$ there is a unique geodesic with endpoints $\alpha$ and $\beta$. We use $[\alpha, \beta]$ to denote the oriented geodesic that starts at $\alpha$ and ends at $\beta$; it corresponds to a directed loop on the Riemann surface $X(1) = \mathbf{H}^*/\Gamma(1)$.

Let $\mathbb{M}_2$ be the $\mathbb{Z}$-module generated by the formal symbols $\{[\alpha, \beta] : \alpha, \beta \in \mathbb{P}^1(\mathbb{Q})\}$ modulo the relations[1]

$$[\alpha, \beta] + [\beta, \gamma] + [\gamma, \alpha] = 0,$$

and modulo torsion (so $[\alpha, \alpha] = 0$, since $[\alpha, \alpha] + [\alpha, \alpha] + [\alpha, \alpha] = 0$, and $[\alpha, \beta] = -[\beta, \alpha]$, since $[\alpha, \beta] + [\beta, \alpha] + [\alpha, \alpha] = 0$). We equip $\mathbb{M}_2$ with a left $\mathrm{GL}_2(\mathbb{Q})$-action by defining

$$g[\alpha, \beta] := [g\alpha, g\beta].$$

We also define $\mathbb{B}_2 := \mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]$ as the free $\mathbb{Z}$-module with basis $\mathbb{P}^1(\mathbb{Q})$, on which $\mathrm{GL}_2(\mathbb{Q})$ acts on the left via linear fractional transformations: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(x : y) := (ax + by : cx + dy)$. Let us fix notation for the following elements of $\mathrm{SL}_2(Z)$:

$$\sigma := S := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \qquad T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \qquad \tau := T\sigma = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right).$$

Recall that $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T\rangle = \langle \sigma, \tau\rangle$, and that the map from $\mathrm{SL}_2(\mathbb{Z})$ to the finitely presented group $\langle s, t | s^2 = t^3 = 1\rangle$ defined by $\sigma \mapsto s, \tau \mapsto t$ is surjective with kernel $\pm 1$.

**(a)** Show that the map $\mathbb{M}_2 \to \mathbb{B}_2$ defined by $[\alpha, \beta] \mapsto \alpha - \beta$ is an injective homomorphism of left $\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})]$-modules with image $\mathbb{B}_2^0 := \{\sum n_P P \in \mathbb{B}_2 : \sum n_P = 0\}$.

**(b)** Show that the map $\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})] \to \mathbb{B}_2$ defined by $\gamma \mapsto \gamma(1\!:\!0) - \gamma(0\!:\!1)$ is a homomorphism of left $\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})]$-modules with kernel $\langle 1+\sigma, 1+\tau+\tau^2\rangle$ (a left $\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})]$-ideal) and image $\mathbb{B}_2^0$. Conclude that the map $\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})] \to \mathbb{M}_2$ defined by $\gamma \mapsto \gamma[0, \infty]$ is surjective with kernel $\langle 1 + \sigma, 1 + \tau + \tau^2\rangle$.

[1] The notation $\{\alpha, \beta\}$ (rather than $[\alpha, \beta]$) is standard, but we shall avoid this notation (which incorrectly suggests that the order of $\alpha$ and $\beta$ is not important).

For any subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ we can view $\mathbb{M}_2$ and $\mathbb{B}_2$ as $\mathbb{Z}[\Gamma]$-modules (one could formally write $\mathrm{Res}_\Gamma^{\mathrm{SL}_2(\mathbb{Z})}\mathbb{M}_2$ and $\mathrm{Res}_\Gamma^{\mathrm{GL}_2(\mathbb{Z})}\mathbb{B}_2$, but we will avoid this clutter when it is clear from context that we are working with $\mathbb{Z}[\Gamma]$-modules). Henceforth we shall assume that $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a finite index subgroup (you may assume $\Gamma = \Gamma_0(N)$ if you wish). We define the $\mathbb{Z}[\Gamma]$-modules of coinvariants:

$$\mathbb{M}_2(\Gamma) := (\mathbb{M}_2)_\Gamma = \mathbb{M}_2/I_\Gamma\mathbb{M}_2,$$
$$\mathbb{B}_2(\Gamma) := (\mathbb{B}_2)_\Gamma = \mathbb{B}_2/I_\Gamma\mathbb{B}_2,$$

where $I_\Gamma := \ker(\sum n_\gamma \gamma \mapsto \sum n_\gamma) = \langle \gamma - 1 : \gamma \in \Gamma\rangle \subseteq \mathbb{Z}[\Gamma]$ is the augmentation ideal. We call $\mathbb{M}_2(\Gamma)$ the space of modular symbols for $\Gamma$ (of weight 2), and $\mathbb{B}_2(\Gamma)$ is the boundary space for $\Gamma$. To simplify the presentation in what follows, let us replace $\mathbb{M}_2(\Gamma)$ and $\mathbb{B}_2(\Gamma)$ by their torsion-free quotients (as in [2]).

**(c)** Show that for all $m, n \in \mathbb{Z}$ and $N \in \mathbb{Z}_{\geq 1}$ we have $[m, n] = 0$ in $\mathbb{M}_2(\Gamma_0(N))$ (in particular, the $\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})]$-modules $\mathbb{M}_2$ and $\mathbb{M}_2(\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})])$ are not the same).

**(d)** Let $\mathrm{SL}_2(\mathbb{Z}) = \Gamma\gamma_1 \sqcup \cdots \sqcup \Gamma\gamma_n$ be a right coset decomposition for $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. Show that $\{\gamma_1[0, \infty], \cdots, \gamma_n[0, \infty]\}$ generates $\mathbb{M}_2(\Gamma)$ as a $\mathbb{Z}$-module; thus $\mathbb{M}_2(\Gamma)$ is a finitely generated abelian group.

**(e)** Let $\mathbb{Z}[\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})]$ be the free abelian group on right cosets $\{\Gamma\alpha : \alpha \in \mathrm{SL}_2(\mathbb{Z})\}$ equipped with the right $\mathrm{SL}_2(\mathbb{Z})$-action $(\Gamma\alpha)\beta = \Gamma\alpha\beta$. Let $\mathbb{M}_2'(\Gamma)$ be the quotient of $\mathbb{Z}[\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})]$ modulo its image under the right $\mathbb{Z}[\mathrm{SL}_2(\mathbb{Z})]$-ideal

$$\langle 1 + \sigma, 1 + \tau + \tau^2\rangle,$$

and modulo any torsion. Show that the map $\Gamma\gamma \mapsto \gamma[0, \infty]$ defines an isomorphism of $\mathbb{Z}$-modules $\mathbb{M}_2'(\Gamma) \simeq \mathbb{M}_2(\Gamma)$.

**(f)** Let $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) := \{(a : b) : a, b \in \mathbb{Z}/N\mathbb{Z} \text{ with } \gcd(a, b, N) = 1\}$ where we define $(a : b) = (a' : b')$ if $a' = ua$ and $b' = ub$ for some $u \in (\mathbb{Z}/N\mathbb{Z})^\times$. Show that the map $\Gamma_0(N)\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \mapsto (c : d)$ defines a bijection $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

Let $X_\Gamma := \Gamma\backslash\mathbf{H}^*$. There is a natural homomorphism

$$\varphi\colon \mathbb{M}_2(\Gamma) \to H_1(X_\Gamma, \{\text{cusps}\}, \mathbb{Z})$$

that sends $\mathbb{Z}$-linear combinations of geodesic paths in $\mathbf{H}^*$ to their images in $X_\Gamma = \Gamma\backslash\mathbf{H}^*$. Here we are taking homology relative to the cusps; this means that in addition to loops, we include homology classes of paths that start and end at cusps (cusps of $X_\Gamma$ are $\Gamma$-orbits of cusps $\mathbb{P}^1(\mathbb{Q}) \subseteq \mathbf{H}^*$). If $X_\Gamma$ has only one cusp (as when $\Gamma = \mathrm{SL}_2(\mathbb{Z})$), this is just usual homology. We now define the boundary map

$$\delta\colon \mathbb{M}_2(\Gamma) \to \mathbb{B}_2(\Gamma)$$
$$[\alpha, \beta] \mapsto \beta - \alpha.$$

The kernel of this map is the subspace $\mathbb{S}_2(\Gamma)$ of cuspidal modular symbols.

**(g)** Prove that the restriction of $\varphi$ to the subspace of cuspidal modular symbols defines an isomorphism of free $\mathbb{Z}$-modules $\mathbb{S}_2(\Gamma) \xrightarrow{\sim} H_1(X_\Gamma, \mathbb{Z})$. There are several approaches to this: (a) follow Manin's topological proof in [1], (b) use group cohomology as in [3], (c) view $H_1(X_\Gamma, \mathbb{Z})$ as a lattice in $S_2(\Gamma)^\vee$ via the integration pairing. Feel free to assume $\Gamma = \Gamma_0(p)$ with $p$ prime if you wish (there are then exactly 2 cusps).

**(h)** Let $(s_1 : t_1), (s_2 : t_2) \in \mathbb{P}^1(\mathbb{Q})$ be cusps with $\gcd(s_1, t_1) = \gcd(s_2, t_2) = 1$. Show that $(s_1 : t_1) - (s_2 : t_2) = 0 \in \mathbb{B}_2(\Gamma_0(N))$ if and only if there exists $a_1, a_2 \in \mathbb{Z}$ such that $a_1 t_2 \equiv a_2 t_1 \bmod \gcd(t_1 t_2, N)$ and $a_i s_i \equiv 1 \bmod t_i$ for $i = 1, 2$.

We now specialize to $\Gamma = \Gamma_0(N)$. We want to define the action of the Hecke algebra $\mathbb{T}(N) := \mathbb{T}(\Gamma_0(N), \Delta_0(N), \mathbb{Z})$ on the space of modular symbols $\mathbb{M}_2(N) := \mathbb{M}_2(\Gamma_0(N))$ and the isomorphic space of Manin symbols $\mathbb{M}_2'(N) := \mathbb{M}_2'(\Gamma_0(N))$, where

$$\Delta_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{Z}^{2\times 2} : c \equiv 0 \bmod N, a \perp N, ad - bc > 0 \right\}$$

as usual. If $\Gamma_0(N)\alpha\Gamma_0(N)$ is a Hecke operator, with $\alpha \in \Delta_0(N)$, and

$$\Gamma_0(N)\alpha\Gamma_0(N) = \Gamma_0(N)\gamma_1 \sqcup \cdots \sqcup \Gamma_0(N)\gamma_n$$

is a right coset decomposition, then for $[\alpha, \beta] \in \mathbb{M}_2(N)$ we define

$$\Gamma_0(N)\alpha\Gamma_0(N)[\alpha, \beta] := \sum_{1 \le i \le n} \gamma_i[\alpha, \beta].$$

For example, for the Hecke operator $T_p := \Gamma_0(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_0(N)$ with $p \nmid N$ prime we have

$$T_p([\alpha, \beta]) := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)[\alpha, \beta] + \sum_{0 \le r < p} \left(\begin{smallmatrix} 1 & r \\ 0 & p \end{smallmatrix}\right)[\alpha, \beta].$$

To define the action of $T_p$ on $\mathbb{M}_2'(N)$ we will use the bijection $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ from part **(e)** to represent elements of $\mathbb{M}_2'(N)$ as elements of $\mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})]$. We now define

$$T_p((c : d)) := \sum_{M \in R_p} (c : d)M,$$

where $M$ acts by matrix multiplication on the right of the row vector $(c : d)$ and $R_p$ is the set of Heilbronn matrices. The isomorphism $\mathbb{M}_2'(N) \xrightarrow{\sim} \mathbb{M}_2(N)$ is given by

$$(c : d) = \Gamma_0(N)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)[0, \infty] = [\tfrac{b}{d}, \tfrac{a}{c}].$$

Thus the Heilbronn matrices $R_p$ must satisfy

$$T_p((c : d)) = \sum_{M \in R_p} (c : d)M \mapsto \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)[\tfrac{b}{d}, \tfrac{a}{c}] + \sum_{0 \le r < p} \left(\begin{smallmatrix} 1 & r \\ 0 & p \end{smallmatrix}\right)[\tfrac{b}{d}, \tfrac{a}{c}] \tag{1}$$

Recall that every rational number $s/t$ has a continued fraction expansion with successive convergents in lowest terms:

$$\frac{s_{-2}}{t_{-2}} = \frac{0}{1}, \ \frac{s_{-1}}{t_{-1}} = \frac{1}{0}, \ \frac{s_0}{t_0} = \frac{s_0}{1}, \ \ldots, \ \frac{s_{n-1}}{t_{n-1}}, \ \frac{s_n}{t_n} = \frac{s}{t}$$

with $s_n t_{n-1} - s_{n-1} t_n = (-1)^{n+1}$ so that

$$\begin{pmatrix} s_n & (-1)^{n+1} s_{n-1} \\ t_n & (-1)^{n+1} t_{n-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

**(i)** Show that we can match the first term on the RHS of (1) by taking $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \in R_p$. Then show that, given $(c : d)$, for each $0 \le r < p$ one can choose $a, b \in \mathbb{Z}$ so that $ad - bc = 1$ and $A := \left(\begin{smallmatrix} 1 & r \\ 0 & p \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & r \\ 0 & p \end{smallmatrix}\right)^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, and a sequence of matrices $A_0, \ldots, A_n$ such that

$$\sum_{0 \le i \le n} AA_iS[0, \infty] = A[\tfrac{r}{p}, \infty] = \left(\begin{smallmatrix} 1 & r \\ 0 & p \end{smallmatrix}\right)[\tfrac{b}{d}, \tfrac{a}{c}].$$

Now show that if define $M_i := \left(\begin{smallmatrix} p & -r \\ 0 & 1 \end{smallmatrix}\right)A_iS$ for $0 \le i \le n$ then we will have

$$\sum_{0 \le i \le n} (c : d)M_i \mapsto \left(\begin{smallmatrix} 1 & r \\ 0 & p \end{smallmatrix}\right)[\tfrac{b}{d}, \tfrac{a}{c}]$$

under the isomorphism $\mathbb{M}_2'(N) \xrightarrow{\sim} \mathbb{M}_2(N)$. Conclude that a suitable set of Heilbronn matrices $R_p$ exists (to compute them in Sage use `list(HelbronnCremona(p))`).

**(j)** Describe an algorithm that given a positive integer $N$ computes a basis for $S_2(\Gamma_0(N))$ consisting of cuspidal forms with integer Fourier coefficients $a_n$ (not necessarily newforms), with $a_n$ computed for sufficiently many $n$ to distinguish your basis elements. Illustrate your algorithm for $N = 23$ and $N = 26$ (feel free to use Sage to perform the computations, the point is to explain what your algorithm is doing).

**(k)** Give an algorithm for computing the matrix of any Hecke operator $T_p$ for $p \nmid N$ acting on this basis using the tools you developed above. Illustrate your algorithm for $N = 23$ and $N = 26$ with $p = 2$ and $p = 3$.

**(l)** Using big-$O$ notation, estimate the running time of your algorithm in **(j)** as a function of $N$, and the running time of your algorithm in **(k)** as a function of $N$ and $p$, assuming that you can multiply two $n$-bit integers in time $O(n \log n)$.

## Problem 2. Survey

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

| | Interest | Difficulty | Time Spent |
|---|---|---|---|
| Problem 1 | | | |

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

| Date | Lecture Topic | Material | Presentation | Pace | Novelty |
|---|---|---|---|---|---|
| 4/3 | Riemann zeta function | | | | |
| 4/5 | Modular form $L$-functions | | | | |
| 4/10 | Newforms and twists | | | | |
| 4/17 | Hecke eigenvalues | | | | |

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.

## References


[1] J. Manin, *Parabolic points and zeta-functions of modular curves*, Math. USSR Izv **6** (1972).

[2] W. Stein, *Modular forms: a computational approach*, AMS, 2007.

[3] G. Wiese, *Modular forms of weight one over finite fields*, Ph.D. thesis, Universiteit Leiden, 2005.