

COMPUTATIONS WITH FINITE INDEX SUBGROUPS OF $\mathrm{PSL}_2(\mathbb{Z})$ USING FAREY SYMBOLS

CHRIS A. KURTH AND LING LONG

ABSTRACT. Finite index subgroups of the modular group are of great arithmetic importance. Farey symbols, introduced by Ravi Kulkarni in 1991, are a tool for working with these groups. Given such a group Γ , a Farey symbol for Γ is a certain finite sequence of rational numbers (representing vertices of a fundamental domain of Γ) together with pairing information for the edges between the vertices. They are a compact way of encoding the information about the group and they provide a simple way to do calculations with the group. For example: calculating an independent set of generators and decomposing group elements into a word in these generators, finding coset representatives, elliptic points, and genus of the group, testing if the group is congruence, etc. In this expository article, we will discuss Farey Symbols and explicit algorithms for working with them.

1. INTRODUCTION

Modular forms are certain functions defined on the upper half plane displaying certain symmetries under the Möbius transformation action of a finite-index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. The theory of modular forms has been in the central stage of number theory for more than one century and continues to be one of its most exciting areas. Working with modular forms requires knowing information about their underlying groups. There is a vast literature about many aspects of finite index subgroups of the modular groups and their relations with other fields such as combinatorics, algebraic curves. Interested readers are referred to articles like [ASD71], [Bir94], or a recent survey article by the second author on these groups and their modular forms [Lon07].

Some finite index subgroups of the modular group can be described purely by congruence relations, and as such are called congruence subgroups of the modular group. These groups are relatively easy to work with, as they contain a certain normal subgroup $\Gamma(N)$, such that the quotient of the group by $\Gamma(N)$ is just a subgroup of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. Most computational methods for working with modular forms work only for congruence subgroups (cf. [Ste07]). Noncongruence subgroups are finite-index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ that cannot be described by congruence relations. Even though they make up the majority of finite-index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ there are few tools for working with them. One tool that works equally well with both congruence

and noncongruence groups is the method of Farey symbols introduced by Ravi Kulkarni [Kul91]. In this expository paper we will recast how to use Farey symbols and some related computational topics. We will discuss some explicit algorithms for working with Farey symbols. The first author has implemented a collection of such algorithms into a free SAGE package called “KFarey”. It should be made clear to the readers that “KFarey” is an ongoing project and we will continue to improve the current functions, implement other existing algorithms such as [Hsu97, Lan02], and investigate new algorithms to make “KFarey” useful to a wide range of audience. The second author would like to thank ICAC 2007 organizers for inviting her to attend the conference and give a talk on this topic.

2. SUBGROUPS OF $\mathrm{PSL}_2(\mathbb{Z})$

Let $\mathrm{SL}_2(\mathbb{Z})$ be the group of 2×2 matrices with integer coefficients and determinant 1, and let $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{I, -I\}$. Let \mathbb{H} be the upper half plane $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Then $\mathrm{PSL}_2(\mathbb{Z})$ acts faithfully on \mathbb{H} under the action

$$\gamma z = \frac{az + b}{cz + d}$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$. The objects of our study will be the finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. For example, the standard congruence groups, $\Gamma(N)$, $\Gamma_1(N)$, and $\Gamma_0(N)$.

If Γ is a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ then the action of Γ partitions $\mathbb{Q} \cup \{\infty\}$ into equivalence classes, where $q_1 \sim q_2$ if $q_1 = \gamma q_2$ for some $\gamma \in \Gamma$. These equivalence classes $\{q\}$ are called the **cusps** of Γ and the width of the cusp $\{q\}$ is $[\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}(q) : \mathrm{Stab}_{\Gamma}(q)]$. We say that the level of Γ is the least common multiple of the cusp widths of Γ .

Recall that a congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is a subgroup Γ that contains a principal level N congruence subgroup $\Gamma(N)$ for some N . If N is the smallest such N such that this is true, then Γ has level N .

Definition 1. *Let Γ be a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. For our purposes, a fundamental domain of Γ is a hyperbolic polygon P on $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ such that:*

- (1) *If z is in the interior of P and $\gamma \in \Gamma$, then $\gamma z \in P$ implies $\gamma = I$.*
- (2) *For every $z \in \mathbb{H}$ there is $\gamma \in \Gamma$ such that $\gamma z \in P$.*

Lemma 1. *Let Γ be a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ and P a hyperbolic polygon. Suppose P is such that:*

- (1) *If z is in the interior of P and $\gamma \in \Gamma$, then $\gamma z \in P$ implies $\gamma = I$.*
- (2) *For each side e of P , there is $\gamma \in \Gamma$ such that γ maps e to another side of P in an orientation reversing manner.*

Then P is a fundamental domain of Γ .

Proof. Let the images γP of P under elements γ of Γ be called P -tiles. By Condition 1 they cannot overlap. Also, given Condition 1, we only need to show that $\mathbb{H} \subseteq \bigcup_{\gamma \in \Gamma} \gamma P$. Suppose this is not true. Then there is $\eta \in \Gamma$

such that ηP has an edge e without a P -tile on the other side. Then $\eta^{-1}e$ is an side of P and the γ of Condition 2 maps $\eta^{-1}e$ to another side of P . Specifically, γ^{-1} maps P to a P -tile adjacent to P across the side e . Then $\eta\gamma^{-1}P$ is a P -tile adjacent to ηP across the side e . Contradiction. \square

3. FAREY SYMBOLS

3.1. Special Polygons. Farey Symbols were introduced by Ravi Kulkarni in 1991 [Kul91] as a compact and efficient way to compute with finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. The idea is to describe the group by a fundamental domain with vertices at certain rational numbers and certain hyperbolic arcs joining these rational numbers. Most of the theory here is summarized from [Kul91].

If x and y are two points on $\mathbb{H} \cup \mathbb{Q}$ then there is a unique circle passing through x and y with center on \mathbb{Q} . We say the **hyperbolic arc** joining x and y is the arc of this circle contained in $\mathbb{H} \cup \mathbb{Q}$ joining x and y . We also say the hyperbolic arc joining $x \in \mathbb{H}$ to ∞ is the vertical line segment $\{x + ti : 0 \leq t \in \mathbb{R}\} \cup \{\infty\}$. We write $H_{x,y}$ for the hyperbolic arc joining x and y . A **hyperbolic polygon** is a polygon composed of hyperbolic arcs.

Through the course of this paper, when a vertex of a hyperbolic arc is in \mathbb{Q} it will always be assumed to be in the form $\frac{a}{b}$ with $a, b \in \mathbb{Z}$, $(a, b) = 1$ and $b > 0$. If the vertex is ∞ , we will write it either $\frac{-1}{0}$ or $\frac{1}{0}$ (depending on if it is the leftmost or rightmost element of a Farey sequence).

Let $\rho = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ and let T be the hyperbolic triangle with vertices ρ , ρ^2 and ∞ . Then T is a fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$ ([Kob93] Prop. III.1). Let E_e be the edge joining i to ∞ , E_o be the edge joining ρ to ∞ , and E_f be the edge joining i to ρ . Then we call an arc A in the upper half plane an **even edge** (resp. **odd edge**, resp. **f-edge**) if $A = \gamma E_e$ (resp. $A = \gamma E_o$, resp. $A = \gamma E_f$) for some $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ (See Figure 1). E_e and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} E_e$ together form a hyperbolic arc from 0 to ∞ , and in general even edges come in pairs joining rational numbers $\frac{a}{b}$, and $\frac{a'}{b'}$ with $|a'b - ab'| = 1$ because of the following lemma:

Lemma 2. *If $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ and a_1/b_1 , a_2/b_2 , a'_1/b'_1 , and a'_2/b'_2 are rational numbers in simplest form such that*

$$\gamma(a_1/b_1) = a'_1/b'_1, \text{ and } \gamma(a_2/b_2) = a'_2/b'_2$$

then

$$a_2b_1 - a_1b_2 = a'_2b'_1 - a'_1b'_2$$

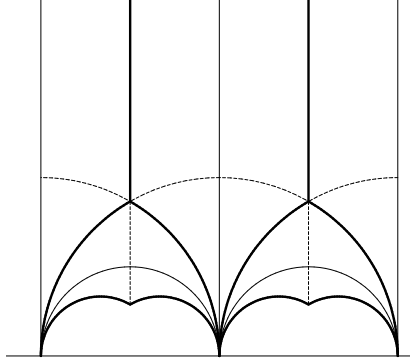


FIGURE 1. Even edges are thin, odd edges are thick, and f-edges are dashed

Proof. If $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ then

$$\gamma\left(\frac{a_1}{b_1}\right) = \frac{Aa_1 + Bb_1}{Ca_1 + Db_1} = \frac{a'_1}{b'_1} \quad \text{and} \quad \gamma\left(\frac{a_2}{b_2}\right) = \frac{Aa_2 + Bb_2}{Ca_2 + Db_2} = \frac{a'_2}{b'_2}.$$

So:

$$\begin{aligned} a'_1 b'_2 - a'_2 b'_1 &= (Aa_1 + Bb_1)(Ca_2 + Db_2) - (Aa_2 + Bb_2)(Ca_1 + Db_1) \\ &= ADa_1 b_2 + BCa_2 b_1 - ADa_2 b_1 - BCa_1 b_2 \\ &= (AD - BC)(a_1 b_2 - a_2 b_1) \\ &= (a_1 b_2 - a_2 b_1) \end{aligned}$$

□

So the quantity $a_2 b_1 - a_1 b_2$ is invariant under transformations in $\text{PSL}_2(\mathbb{Z})$. Note that even edges, odd edges and free edges only map to even edges, odd edges and free edges respectively under transformations $\gamma \in \text{PSL}_2(\mathbb{Z})$.

Definition 2. A special polygon P is a convex hyperbolic polygon together with a side pairing defined in the following way: The polygon is such that:

- (1) The boundary of P consists of even and odd edges.
- (2) The even edges of P come in pairs, each pair forming a hyperbolic arc between elements of $\mathbb{Q} \cup \{\infty\}$.
- (3) The odd edges of P come in pairs, each pair meeting a vertex with initial angle $\frac{2\pi}{3}$.

The sides of the polygon are denoted as follows:

- (1) Each odd edge is called an **odd side**.
- (2) As even edges come in pairs, either each edge of the pair is an **even side**, or the union of the two edges (a semicircle) is called a **free side**.

The side pairing on the edges is defined as follows:

- (1) *Each odd side is paired with the odd side it meets at an angle of $\frac{2\pi}{3}$. This is called an **odd pairing**.*
- (2) *Each even side is paired with the even side with which it forms a semicircular arc. This is called an **even pairing**.*
- (3) *There are an even number of free sides and they are partitioned into sets of two, each called a **free pairing**.*

We will always assume that 0 and ∞ are vertices of P .

The sides of a special polygon P have a natural orientation obtained by tracing the perimeter of the polygon in a certain direction. If $\{s, s'\}$ is a side pairing then there is a unique $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ such that γ maps s to s' in an orientation-reversing manner. We call this the **side pairing transformation** associated with the side pairing, and we let Γ_P be the group generated by all the side pairing transformations of P . Note that it doesn't matter which side we pick for s and which for s' because the two possible γ 's are inverses of each other. Also note that if s is an even side (resp. odd side) then γ is order 2 (resp. order 3).

Two theorems of Kulkarni are fundamental here:

Theorem 1 ([Kul91] Theorem 3.2). *If P is a special polygon then P is a fundamental domain for Γ_P . Moreover, the side pairing transformations $\{\gamma_i\}$ are an independent set of generators of Γ_P (i.e. the only relations on the γ_i 's are $\gamma_i^2 = 1$ or $\gamma_i^3 = 1$ for any finite-order γ_i 's).*

Theorem 2 ([Kul91] Theorem 3.3). *For every $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ of finite index, there is a special polygon P such that $\Gamma = \Gamma_P$.*

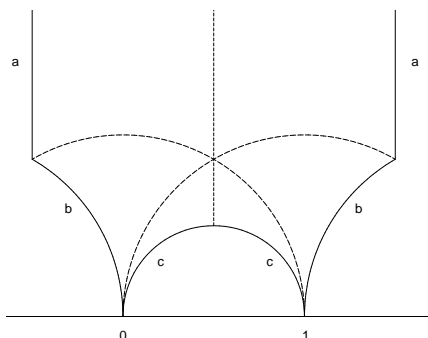
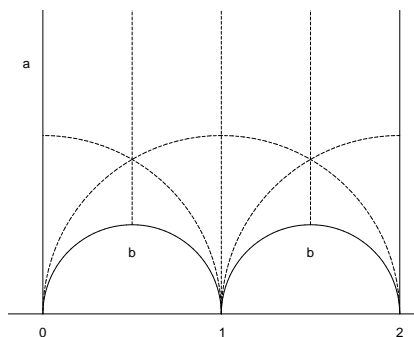
Proof. [Kul91] and also follows from the proof of the algorithm in Section 4. □

Note that although it is true that any subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ with fundamental domain F is generated by the transformations that map its edges together, the fact that the set of generators of a special polygon is an independent set of generators is something special to the special polygon. For example $\Gamma(2)$ has a fundamental domain shown in Figure 2. There are six sides, and the three side pairing transformations are $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$,

and $\begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}$. But this is not an independent list of generators because $\begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

A special polygon for $\Gamma(2)$ is shown in Figure 3. The pairing transformations from the special polygon are $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}$. These are independent generators of $\Gamma(2)$.

3.2. Farey Symbols. Recall that the classical Farey sequences F_n are constructed by taking all the rational numbers $0 \leq a/b \leq 1$ with denominator

FIGURE 2. A fundamental domain for $\Gamma(2)$ FIGURE 3. A special polygon for $\Gamma(2)$

at most n and $(a, b) = 1$ and writing them as a finite sequence in ascending order $\{a_0/b_0, \dots, a_n/b_n\}$. Then for each i we have $a_{i+1}b_i - a_i b_{i+1} = 1$. We are interested in sequences that satisfy this condition.

Definition 3. A *generalized Farey sequence* is a finite sequence:

$$\left\{ \frac{-1}{0}, x_0, \dots, x_n, \frac{1}{0} \right\}$$

such that:

- (1) Each $x_i = a_i/b_i$ is a rational number in reduced form with $b_i > 0$. Additionally, we often consider $x_{-1} = \frac{-1}{0}$ and $x_{n+1} = \frac{1}{0}$.
- (2) If we let $a_{-1} = -1$, $b_{-1} = 0$, $a_{n+1} = 1$, and $b_{n+1} = 0$ then

$$a_{i+1}b_i - a_i b_{i+1} = 1 \tag{1}$$

for $-1 \leq i \leq n$.

Note that this definition forces x_0 and x_n to be integers. We will always assume $x_i = 0$ for some i .

Definition 4. A *Farey symbol* is a generalized Farey sequence with some additional pairing information. Namely, between each adjacent entries x_{i-1} and x_i we assign a *pairing* p_i which is either a positive integer called a **free pairing** or the symbol “ \circ ” called an **even pairing** or “ \bullet ” called an **odd pairing**. Each integer that appears as a free pairing appears exactly twice in the pairing information.

So if P is a special polygon, let x_0, \dots, x_n be the vertices of P lying in \mathbb{Q} listed in ascending order. Recall these vertices satisfy $a_{i+1}b_i - a_i b_{i+1} = 1$. Then $\{\frac{-1}{0}, x_0, \dots, x_n, \frac{1}{0}\}$ is a generalized Farey sequence. We make a Farey symbol out of the generalized Farey sequence by adding the pairing information in the obvious way.

On the other hand, if F is a Farey symbol we can construct a special polygon for F . For adjacent entries of the Farey sequence x_{i-1} and x_i , if p_i is a free pairing or an even pairing we let P have as a side the hyperbolic arc joining x_{i-1} and x_i . Otherwise if it is odd we let γ be the unique element of $\mathrm{PSL}_2(\mathbb{Z})$ such that $\gamma(0) = x_{i-1}$ and $\gamma = x_i$ and join x_{i-1} and x_i by the arcs $\gamma(H_{0,\rho})$ and $\gamma(H_{\rho,\infty})$. Thus we get a hyperbolic polygon which is made into a special polygon by adding pairing information in the obvious way.

Example 1. $\Gamma(2)$ has a Farey symbol $-\infty \underset{1}{\frown} \frac{0}{1} \underset{2}{\frown} \frac{1}{1} \underset{2}{\frown} \frac{2}{1} \underset{1}{\frown} \infty$

3.3. Generators. If P is a special polygon for a group Γ then Γ is independently generated by the transformations mapping each side to its paired side. If F is a Farey symbol:

$$-\infty \underset{p_0}{\frown} a_0/b_0 \underset{p_1}{\frown} a_1/b_1 \underset{p_2}{\frown} \cdots \underset{p_{n-1}}{\frown} a_{n-1}/b_{n-1} \underset{p_n}{\frown} a_n/b_n \underset{p_{n+1}}{\frown} \infty$$

then we can explicitly give formulas for the γ corresponding to a given side pairing.

Theorem 3. Suppose $(a_i/b_i, a_{i+1}/b_{i+1})$ are two adjacent vertices of F . Then if the pairing between them p_{i+1} is an even pairing, let:

$$G_{i+1} = \begin{pmatrix} a_{i+1}b_{i+1} + a_i b_i & -a_i^2 - a_{i+1}^2 \\ b_i^2 + b_{i+1}^2 & -a_{i+1}b_{i+1} - a_i b_i \end{pmatrix}$$

If p_{i+1} is an odd pairing, let:

$$G_{i+1} = \begin{pmatrix} a_{i+1}b_{i+1} + a_i b_{i+1} + a_i b_i & -a_i^2 - a_i a_{i+1} - a_{i+1}^2 \\ b_i^2 + b_i b_{i+1} + b_{i+1}^2 & -a_{i+1}b_{i+1} - a_{i+1}b_i - a_i b_i \end{pmatrix}$$

And if p_{i+1} is a free pairing that is paired with the side between a_k/b_k and a_{k+1}/b_{k+1} , let:

$$G_{i+1} = \begin{pmatrix} a_{k+1}b_{i+1} + a_k b_i & -a_k a_i - a_{k+1} a_{i+1} \\ b_k b_i + b_{k+1} b_{i+1} & -a_{i+1} b_{k+1} - a_i b_k \end{pmatrix}$$

Then G_{i+1} is the side transformation corresponding to the pairing p_{i+1} .

Proof. [Kul91] Theorem 6.1 □

3.4. Group Invariants. Several invariants of the group Γ can be read off from the Farey symbol F . Firstly, the number of inequivalent order-2 (resp. order-3) elliptic points, e_2 (resp. e_3), is the number of even (resp. odd) pairings in F . Also, the number of free pairings in F (half the number of free edges) is equal to r , the rank of $\pi_1(\Gamma \backslash \mathbb{H})$ (the fundamental group of the uncompactified modular curve).

To discuss the cusps of Γ , note that if (x_i, x_{i+1}) is an edge with an even or odd pairing, then x_i and x_{i+1} are equivalent cusps (since $G_{i+1} \in \Gamma$ maps x_i to x_{i+1}). Likewise, if (x_i, x_{i+1}) and (x_j, x_{j+1}) are paired edges then x_i and x_{j+1} are equivalent cusps and x_j and x_{i+1} are equivalent cusps. This defines an equivalence relation on the vertices of P . The equivalence classes are easy to compute, because the defining equivalences occur in a cyclic pattern. So the number of cusps t can be counted as the number of equivalence classes.

For an edge $(\frac{a_i}{b_i}, \frac{a_{i+1}}{b_{i+1}})$ let $\gamma = \begin{pmatrix} a_i & a_{i+1} \\ b_i & b_{i+1} \end{pmatrix}$. So $\gamma^{-1}(x_i) = \infty$ and $\gamma^{-1}(x_{i+1}) = 0$. Then define the **width** of a vertex x_i to be the “width” of γP at ∞ . That is:

$$\text{width}(x_i) = \begin{cases} |a_{i-1}b_{i+1} - a_{i+1}b_{i-1}| & \text{if } x_i \text{ is adjacent to no odd edge} \\ |a_{i-1}b_{i+1} - a_{i+1}b_{i-1}| + 1/2 & \text{if } x_i \text{ is adjacent to 1 odd edge} \\ |a_{i-1}b_{i+1} - a_{i+1}b_{i-1}| + 1 & \text{if } x_i \text{ is adjacent to 2 odd edges} \end{cases}$$

The cusp width of a cusp x of Γ is then the sum of the widths of the vertices of P Γ -equivalent to x .

$\Gamma \backslash \mathbb{H}$ is a genus g orientable surface with t points missing, one for each cusp. The rank of its fundamental group is $r = 2g + t - 1$, so we can calculate the genus $g = \frac{r-t+1}{2}$. Moreover, using the Hurwitz formula ([Shi71] Prop. 1.40) we get the index of Γ in $\text{PSL}_2(\mathbb{Z})$, $\mu = 3e_2 + 4e_3 + 12g + 6t - 12$. An even simpler formula for the index comes from noting that $n + 2 = 2r + e_2 + e_3$ where $n + 1$ is as in Definition 3. This, combined with the previous formula, implies $\mu = 3n + e_3$.

4. COSET PERMUTATION REPRESENTATION OF A GROUP

Another method of representing groups that will be useful to us in determining if a group is congruence is the coset permutation representation developed by Millington [Mil69a] [Mil69b]. Let Γ be a subgroup of $\text{PSL}_2(\mathbb{Z})$ with $[\text{PSL}_2(\mathbb{Z}) : \Gamma] = \mu$ and $\text{PSL}_2(\mathbb{Z}) = \cup_{i=1}^{\mu} \alpha_i \Gamma$ a coset decomposition with $\alpha_1 = I$. Let F be the standard fundamental domain for $\text{PSL}_2(\mathbb{Z})$. Then $\cup_{i=1}^{\mu} \alpha_i^{-1} F$ is a fundamental domain for Γ . Let

$$E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

E and V generate $\text{PSL}_2(\mathbb{Z})$, as do L and R . The conversions between them are:

$$E = LR^{-1}L, \quad V = R^{-1}L \tag{2}$$

$$L = EV^{-1}, \quad R = EV^{-2} \tag{3}$$

We have $E^2 = V^3 = 1$. In fact it is well-known that $\mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to the group (cf. [Ran77]):

$$\mathrm{PSL}_2(\mathbb{Z}) \cong \langle e, v : e^2 = v^3 = 1 \rangle \quad (4)$$

For each γ in $\mathrm{PSL}_2(\mathbb{Z})$, left multiplication acts on the left cosets of Γ in $\mathrm{PSL}_2(\mathbb{Z})$ by permutation, i.e. there is a homomorphism $\phi : \mathrm{PSL}_2(\mathbb{Z}) \rightarrow S_n$, such that if $\phi(\gamma) = \sigma_\gamma$ then $\gamma\alpha_i\Gamma = \alpha_{\sigma_\gamma(i)}\Gamma$. In this way every finite-index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is associated with a pair of permutations $e = \varphi(E)$ and $v = \varphi(V)$ with $e^2 = v^3 = 1$ which generate a transitive permutation group (transitivity comes from E and V generating $\mathrm{PSL}_2(\mathbb{Z})$). We call (e, v) a **coset permutation representation** of Γ and (l, r) an **LR-representation** of Γ , where $l = \varphi(L)$ and $r = \varphi(R)$. Each form can be obtained from the other form by the equations (2). Note that $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ is in Γ if and only if $\gamma\Gamma = \Gamma$, i.e. $\sigma_\gamma(1) = 1$.

On the other hand, suppose e and v are a pair of permutations on μ letters with $e^2 = v^3 = 1$ that generate a transitive permutation group S (such a permutation we call **valid**). Define a homomorphism $\varphi : \mathrm{PSL}_2(\mathbb{Z}) \rightarrow S$ such that $\varphi(E) = e$ and $\varphi(V) = v$ (This is well-defined because of (4)). Let $\Gamma = \{\gamma \in \mathrm{PSL}_2(\mathbb{Z}) : \varphi(\gamma)(1) = 1\}$. Then Γ is an index- μ subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. Thus we have a correlation between valid pairs of permutations and finite-index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. To test if $A \in \mathrm{PSL}_2(\mathbb{Z})$ is in Γ we write A as a word in L and R (Using, essentially, the Euclidean Algorithm) and replace L and R with the permutations l and r . If the resulting permutation fixes 1 then A is in Γ .

If one of the cosets is fixed by e , say $e(i) = i$, it corresponds to an elliptic element in Γ , for $E\alpha_i\Gamma = \alpha_i\Gamma$ means $\alpha_i^{-1}E\alpha_i\Gamma = \Gamma$, meaning $\alpha_i^{-1}E\alpha_i$ (which is order 2) is in Γ . So e_2 , the number of inequivalent elliptic elements of order 2 in Γ , is equal to the number of elements fixed by e . Similarly, e_3 is the number of elements fixed by v .

The cusp width of Γ at ∞ is the smallest positive integer n such that $L^n \in \Gamma$. Thus the cusp width at infinity is the order of the cycle in $\varphi(L)$ which contains "1". Likewise, suppose i is in a cycle of length k in $\varphi(L)$, i.e. $L^k\alpha_i\Gamma = \alpha_i\Gamma$, but $L^n\alpha_i\Gamma \neq \alpha_i\Gamma$ for $0 < n < k$. Then $\alpha_i^{-1}L^k\alpha_i \in \Gamma$, but $\alpha_i^{-1}L^n\alpha_i \notin \Gamma$ for $0 < n < k$. If $q = \alpha_i^{-1}\infty$ then $\alpha_i^{-1}L^k\alpha_i q = q$ but $\alpha_i^{-1}L^n\alpha_i q \neq q$ for $0 < n < k$. Thus $\alpha_i^{-1}L^k\alpha_i$ is a generator for the stabilizer of the cusp q , and this cusp has width k .

5. ALGORITHMS

5.1. Calculating a Farey Symbol. Recall that T is the standard fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$, and let T^* be the hyperbolic triangle with vertices ρ , i and ∞ (So $T = T^* \cup (-\overline{T^*})$). $\mathcal{T} = \{\gamma T : \gamma \in \mathrm{PSL}_2(\mathbb{Z})\}$ is a tessellation of the upper half plane and any finite index subgroup Γ has a fundamental domain which is a simply connected union of \mathcal{T} -tiles. Let

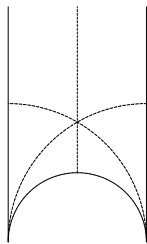


FIGURE 4. A hyperbolic triangle

$\mathcal{T}^* = \{\gamma T^* : \gamma \in \mathrm{PSL}_2(\mathbb{Z})\} \cup \{\gamma(-\overline{T^*}) : \gamma \in \mathrm{PSL}_2(\mathbb{Z})\}$. \mathcal{T}^* is also a tessellation of the upper half plane, and we will construct a fundamental domain for Γ out of \mathcal{T}^* -tiles. The starting point for our construction will be the six tiles around an odd vertex. The following lemma shows this is a reasonable starting point:

Lemma 3. *Let Γ be a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ with index ≥ 3 . Then the stabilizer of $\rho = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ or $\rho - 1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is trivial (i.e. one of these points is not elliptic in Γ).*

Proof. If the two stabilizers are not trivial then they must be $\Gamma_\rho = \{I, A, A^2\}$ and $\Gamma_{\rho-1} = \{I, B, B^2\}$ where $A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. But A and B generate an index-2 subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. So Γ is either the (unique) index-2 subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ or $\mathrm{PSL}_2(\mathbb{Z})$ itself. And if the index of Γ in $\mathrm{PSL}_2(\mathbb{Z})$ is bigger than 2, at least one of A and B cannot be in Γ . \square

So if Γ is not $\mathrm{PSL}_2(\mathbb{Z})$ or Γ_2 , the unique index 2 subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ (cf. [Ran77]), then the hyperbolic triangle with vertices either 0, 1 and ∞ , or $-1, 0$ and ∞ (cf. Figure 4) is contained in a fundamental domain of Γ . The triangle is made of 6 \mathcal{T}^* -tiles. We will make a polygon P starting with this triangle, then attach \mathcal{T}^* -tiles to P and assign partial pairing information to sides until we get a fundamental domain for Γ (at which point all the pairing information will be filled in). In the algorithm we will say a \mathcal{T}^* -tile T is **adjoinable** to P if T is adjacent to a tile of P and if $P \cup T$ is contained in some fundamental domain of Γ . Note that if T is adjacent to P with adjacency edge e and if e cannot be paired with any other edge of P then T is adjoinable.

Algorithm:

- (1) If $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ let P be the special polygon with Farey symbol

$$-\infty \underset{\circ}{\frown} 0 \underset{\bullet}{\smile} \infty$$

- or if $\Gamma = \Gamma_2$ let P be the special polygon with Farey symbol

$$-\infty \underset{\bullet}{\frown} 0 \underset{\bullet}{\smile} \infty$$

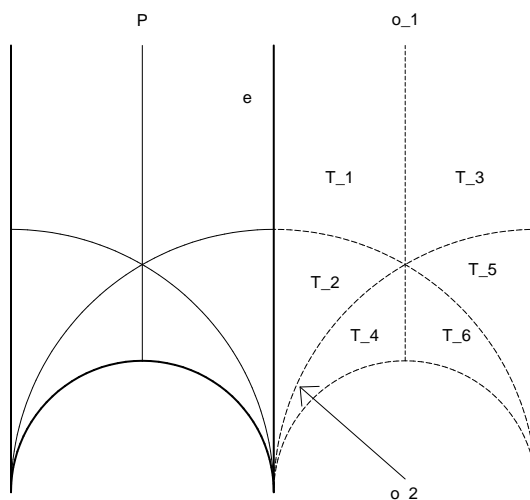


FIGURE 5

- In either case return P and terminate.
- (2) If $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ is not in Γ then let P be the hyperbolic polygon with vertices $0, 1,$ and ∞ . Otherwise let P be the hyperbolic polygon with edges $-1, 0$ and ∞ .
 - (3) If any of the three sides of P map to each other by a $\gamma \in \Gamma$, assign that pairing to the side. (Note that initially all sides are even sides).
 - (4) P is now a polygon where every side is either:
 - (a) even and already paired.
 - (b) odd and already paired.
 - (c) even and unpaired.
 - (5) Pick an unpaired even side e . Figure 5 shows the typical case (The other cases are the same as this case with everything translated by some $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$). Since e is unpaired, T_1 and T_2 must be adjoinable. If o_1 and o_2 are the new odd edges of P after adding T_1 and T_2 to P then either $\gamma o_1 = o_2$ for some $\gamma \in \Gamma$, or there is no such γ . If there is γ pair the two edges and go to Step 3.
 - (6) If o_1 doesn't pair with o_2 then it doesn't pair with any other side because the only other unpaired sides are odd. So tiles T_3 and likewise T_4 are adjoinable. Each of these tiles has a free edge and the free edges cannot pair with each other (because their common vertex would have an internal angle of $\frac{4\pi}{3}$, so the pairing transformations would make things overlap), so T_5 and T_6 are adjoinable.
 - (7) We've now added 6 \mathcal{S}^* -tiles to P (One even triangle). If either of the new even edges pair with any of the old unpaired even edges then assign that pairing.

- (8) If all the sides of P are paired then we are done. Otherwise go to Step 4.

The output of the algorithm is a special polygon P with $\Gamma_P = \Gamma$. Note that the algorithm must terminate, because a fundamental domain of Γ has hyperbolic area $\frac{\pi}{3}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma]$ and a single \mathcal{T}^* -tile has area $\frac{\pi}{6}$. So for P to be contained in a fundamental domain of Γ it can have at most $2 \cdot [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma]$ \mathcal{T}^* -tiles.

To effectively implement the algorithm we use Farey symbols. We need only a way to test for group membership. Note that if p_i/q_i and p_{i+1}/q_{i+1} are two adjacent vertices of the fundamental polygon then the hyperbolic triangle added to the edge $H_{x_i, x_{i+1}}$ in Step 6 is the triangle with vertices p_i/q_i , p_{i+1}/q_{i+1} , and $(p_i + p_{i+1})/(q_i + q_{i+1})$.

So given a finite-index subgroup Γ of $\mathrm{PSL}_2(\mathbb{Z})$, if we have a way to test for group membership we can calculate a Farey symbol by the following algorithm:

Algorithm for calculating a Farey Symbol:

- (1) If $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ are in Γ then $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$, so return

$$-\infty \underset{\circ}{\frown} 0 \underset{\bullet}{\frown} \infty$$

and terminate. If $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ are in Γ then $\Gamma = \Gamma_2$, so return

$$-\infty \underset{\bullet}{\frown} 0 \underset{\bullet}{\frown} \infty$$

and terminate.

- (2) If $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \notin \Gamma$ then let F be the (partial) Farey symbol:

$$-\infty \frown \frac{0}{1} \frown \frac{1}{1} \frown \infty$$

Otherwise let F be:

$$-\infty \frown \frac{-1}{1} \frown \frac{0}{1} \frown \infty$$

- (3) For each i with $0 \leq i \leq n+1$, if the pairing between x_{i-1} and x_i is not filled in then check if it can be paired with itself (even or odd pairing), or if it can be paired with another unpaired edge (i.e., check if the appropriate G_i is in Γ). Wherever something can be paired, assign that pairing.
- (4) If all edges are now paired, return F and terminate.
- (5) If there is still an unpaired edge, say between p_i/q_i and p_{i+1}/q_{i+1} , make a new vertex $(p_i + p_{i+1})/(q_i + q_{i+1})$ with no pairing information on the edges adjacent to it. Go to Step 3.

The output is a Farey symbol for Γ .

5.2. Group Membership. The following algorithm described in [LLT95] tests if $A \in \mathrm{PSL}_2(\mathbb{Z})$ is an element of the group corresponding to a Farey symbol F . We will need a lemma about even lines:

Lemma 4. *Let l be an even line (a semicircle on the upper half plane with rational endpoints a/b and a'/b' such that $|ab' - a'b| = 1$). Let P be a special polygon in \mathbb{H} . Then either $l \subset P$ or $l \cap P = \emptyset$.*

Proof. [LLT95] Proposition 2.1 □

Let Γ be a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ and A an element of $\mathrm{PSL}_2(\mathbb{Z})$.

$$A = \begin{pmatrix} c_0 & c'_0 \\ d_0 & d'_0 \end{pmatrix} \quad (5)$$

A maps the even line $H_{0,\infty}$ to $l = H_{c'_0/d'_0, c_0/d_0}$. By the lemma, either $l \subset P$ or it is disjoint from P (except possibly at endpoints). If it is disjoint there is an edge which it is naturally “closest” to (In a sense discussed in [LLT95]). The idea of the algorithm is to translate P across the “closest” edge until P intersects $H_{c/d, c'/d'}$, at which point A will be in Γ if and only if l is the image of $(0, \infty)$ or the an edge paired with $(0, \infty)$. In the actual algorithm we work in the other direction, translating the even line instead of the special polygon.

Algorithm: [LLT95]

Let $k = 0$ and F be a Farey symbol for Γ with 0 as one of its vertices.

Without loss of generality, we can assume $\frac{c'_k}{d'_k} < \frac{c_k}{d_k}$.

- (1) There are two possibilities: If $\frac{c'_k}{d'_k}$ and $\frac{c_k}{d_k}$ are both vertices of P then terminate. Otherwise we must have $x_i \leq \frac{c'_k}{d'_k} < \frac{c_k}{d_k} \leq x_{i+1}$ with at least one “ \leq ” a strict inequality.
- (2) Let g_{i+1} be the generator corresponding to the pairing p_{i+1} (recall this is the transformation mapping $l = H_{c'_k/d'_k, c_k/d_k}$ to its paired side). If p_{i+1} is a free or even pairing, let $\alpha_k = g_{i+1}$. If p_{i+1} is an odd pairing, let $m = \frac{a_i + a_{i+1}}{b_i + b_{i+1}}$ where $x_i = \frac{a_i}{b_i}$, $x_{i+1} = \frac{b_{i+1}}{b_{i+1}}$. Then the interval $(\frac{c'_k}{d'_k}, \frac{c_k}{d_k})$ must be between either x_i and m or between m and x_{i+1} . If $\frac{c_k}{d_k} \leq m$, let $\alpha_k = g_{i+1}$. Otherwise let $\alpha_k = g_{i+1}^{-1}$.
- (3) Let $\frac{c_{k+1}}{d_{k+1}} = \alpha_k \cdot \frac{c_k}{d_k}$, $\frac{c'_{k+1}}{d'_{k+1}} = \alpha_k \cdot \frac{c'_k}{d'_k}$. Replace k with $k + 1$ and go to Step 1.

The algorithm returns $\frac{c'_k}{d'_k}$ and $\frac{c_k}{d_k}$, which are two vertices of P , and a list of α_i 's.

Theorem 4. *The algorithm terminates, and A is in Γ if and only if one of the following is true:*

- (1) $\begin{pmatrix} c_k & c'_k \\ d_k & d'_k \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- (2) $(\frac{c'_k}{d'_k}, \frac{c_k}{d_k})$ is a free side paired with $(0, \infty)$.
- (3) $\begin{pmatrix} c_k & c'_k \\ d_k & d'_k \end{pmatrix} = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and 0 and ∞ are adjacent vertices with an even pairing between them.

Proof. [LLT95] □

In addition, if A is in Γ , A can be written as a word in the generators of Γ because $A = \alpha_0^{-1} \alpha_1^{-1} \dots \alpha_k^{-1} \begin{pmatrix} c_k & c'_k \\ d_k & d'_k \end{pmatrix}$, and each term in that product is one of the generators for F .

5.3. Coset Representatives. Let Γ be a group with special polygon P . Let T be the hyperbolic triangle with vertices i , ρ , and ∞ . By the construction of P , T is contained in P . The set of $\gamma \in \Gamma$ such that γT is in P is a set of coset representatives of Γ .

Let a_i/b_i and a_{i+1}/b_{i+1} be a vertex of the special polygon, and let $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\varphi = \begin{pmatrix} a_i & a_{i+1} \\ b_i & b_{i+1} \end{pmatrix}$. Then $\varphi^{-1}(a_i/b_i) = \infty$ and $\varphi^{-1}(a_{i+1}/b_{i+1}) = 0$. Let w_i be $|a_{i-1}b_{i+1} - a_{i+1}b_{i-1}|$ if the pairing between a_i/b_i and a_{i+1}/b_{i+1} is not an odd pairing and $|a_{i-1}b_{i+1} - a_{i+1}b_{i-1}| + 1$ if it is. Then w_i is the number of \mathcal{T}^* -tiles of the form γT in P . Thus a list of left coset representatives for Γ is $\bigcup_{i=0}^n \{T^{-j} \phi_i^{-1} : 0 \leq j < w_i\}$.

5.4. Congruence Testing. Let Γ be a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. Lang, Lim and Tan give a test purely in terms of Farey symbols to determine if Γ is a congruence group [LLT95]. Their test relies on Wohlfahrt's Theorem [Woh64] which says that if Γ has level N then Γ is a congruence group if and only if Γ contains $\Gamma(N)$. In Lang, Lim and Tan's test, if Γ has level N one computes a Farey symbol for $\Gamma(N)$, giving a complete set of generators for $\Gamma(N)$. One then checks if each of these generators is contained in Γ using the above algorithm. The difficulty with this algorithm is that the index of $\Gamma(N)$ increases very quickly with N , so if Γ has large level, the calculation of a Farey symbol for $\Gamma(N)$ can be very lengthy, even if Γ has relatively small index.

Another test for congruence was developed by Tim Hsu using Millington's coset permutation representations [Hsu96]. If we have an LR-representation of Γ there is a list of relations that are satisfied if and only if Γ is congruence.

To calculate an LR-representation from a Farey symbol, use the above algorithm to calculate a list of left coset representatives $\alpha_i \in \mathrm{PSL}_2(\mathbb{Z})$ where $\mathrm{PSL}_2(\mathbb{Z}) = \bigcup_{i=1}^{\mu} \alpha_i \Gamma$. To calculate l , for instance, recall that l is the permutation such that $L\alpha_i \Gamma = \alpha_{l(i)} \Gamma$. So l sends i to the unique j such that $\alpha_j^{-1} L\alpha_i \in \Gamma$. So we run through every $1 \leq i \leq \mu$ and calculate the permutation. r can be calculated similarly. (Actually, although we need l and r

it is easier to calculate e and v , because we know beforehand that they are order 2 and 3 respectively. Then $l = ev^{-1}$ and $r = ev^{-2}$).

Knowing l and r we can directly apply Tim Hsu's congruence algorithm [Hsu96]. Depending on the order of l , (i.e. the level of Γ) there are different lists of relations of l and r that are satisfied if and only if Γ is congruence. For example, if N is the order of l and N is odd then Γ is a congruence group if and only if $r^2l^{-\frac{1}{2}}$ is the identity permutation (where $\frac{1}{2}$ is the inverse of 2 modulo N).

6. IMPLEMENTATION

Helena Verrill has written a MAGMA package for working with Farey symbols for congruence groups. Also, for congruence or noncongruence groups, the algorithms described above have been implemented by the first author as a collection of functions for SAGE. The package and basic examples may be downloaded at:

<http://www.public.iastate.edu/~kurthc/research/index.html>

REFERENCES

- [ASD71] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., 1971, pp. 1–25.
- [Bir94] B. Birch, *Noncongruence subgroups, covers and drawings*, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, pp. 25–46.
- [Hsu96] T. Hsu, *Identifying congruence subgroups of the modular subgroup*, Proceedings of the American Mathematical Society **124** (1996), no. 5, 1351–1359.
- [Hsu97] ———, *Permutation techniques for coset representations of modular subgroups*, Geometric Galois actions, 2, London Math. Soc. Lecture Note Ser., vol. 243, Cambridge Univ. Press, Cambridge, 1997, pp. 67–77.
- [Kob93] N. Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Springer-Verlag, New York, 1993.
- [Kul91] R. S. Kulkarni, *An arithmetic geometric method in the study of the subgroups of the modular group*, American Journal of Mathematics **113** (1991), no. 6, 1053–1133.
- [LLT95] M. L. Lang, Chong-Hai Lim, and Ser-Peow Tan, *An algorithm for determining if a subgroup of the modular group is congruence*, Journal of the London Mathematical Society **51** (1995), 491–502.
- [Lan02] M. L. Lang, *Normalisers of subgroups of the modular group*, J. Algebra **248** (2002), no. 1, 202–218.
- [Lon07] L. Long, *Finite index subgroups of the modular group and their modular forms*, arXiv:0707.3315 (2007).
- [Mil69a] M. H. Millington, *On cycloidal subgroups of the modular group*, Proc. London Math. Soc. (3) **19** (1969), 164–176.
- [Mil69b] ———, *Subgroups of the classical modular group*, J. London Math. Soc. (2) **1** (1969), 351–357.
- [Ran77] R. A. Rankin, *Modular forms and functions*, Cambridge University Press, Cambridge, 1977.

- [Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.
- [Ste07] W. A. Stein, *Modular forms: A computational approach*, American Mathematical Society, 2007.
- [Woh64] K. Wohlfahrt, *An extension of f. klein's level concept*, Ill. J. Math. **8** (1964), 529–539.

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IA 50011, USA
E-mail address: `kurthc@iastate.edu`

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IA 50011, USA
E-mail address: `linglong@iastate.edu`