The Mathematica® Journal

Manipulating Subgroups of the Modular Group

Daniel Schultz

We describe efficient algorithms for working with subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. Operations discussed include join and meet, congruence testing, congruence closure, subgroup testing, cusp enumeration, supergroup lattice, generators and coset enumeration, and constructing a group from a list of generators.

Introduction

The set of linear fractional transformations of the form

$$f(z) = \frac{a\,z + b}{c\,z + d}, \text{ where } a, b, c, d \in \mathbb{R}, \tag{1}$$

known as Möbius transformations, has several interesting properties. First, the composition of functions of this form is still of the same form, as

$$\frac{a_1 \frac{a_2 z + b_2}{c_2 z + d_2} + b_1}{c_1 \frac{a_2 z + b_2}{c_2 z + d_2} + d_1} = \frac{(a_1 a_2 + b_1 c_2) z + a_1 b_2 + b_1 d_2}{(a_2 c_1 + c_2 d_1) z + b_2 c_1 + d_1 d_2}.$$

Since the coefficients appearing in the composition are exactly those of the product of the two matrices $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$, it is most convenient to represent transformations of the form (1) by the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. A matrix and any nonzero scalar multiple of itself represent the same Möbius transformation, so we can consider only matrices with determinant 1 without loss of generality. Since the product of two matrices with determinant 1 also has determinant 1, such a set of matrices (or Möbius transformations) forms a group, where the group operation is matrix multiplication (or composition). If we further restrict the coefficients a, b, c, and d in (1) to be integers, the resulting group is known as $\mathrm{SL}_2(\mathbb{Z})$. Now, if the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $\mathrm{SL}_2(\mathbb{Z})$, then $-\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is also in $\mathrm{SL}_2(\mathbb{Z})$ and represents the same Möbius transformation. For this reason, we consider $\mathrm{PSL}_2(\mathbb{Z})$, known as the modular group, which is $\mathrm{SL}_2(\mathbb{Z})$ with each matrix identified with its negative. That is,

$$\mathrm{PSL}_2(\mathbb{Z}) = \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z},\ a\,d - b\,c = 1 \right\}.$$

It is possible to show that every transformation in the modular group can be obtained as a combination of the two fundamental transformations

$$S(z) = -\frac{1}{z} \text{ and } T(z) = z + 1,$$

with corresponding matrices $S = \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Another way of stating this fact is that $\mathrm{PSL}_2(\mathbb{Z})$ is generated by S and T.

For example, the matrix $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ may be obtained as the product $T\,S\,T\,T\,S\,T$.

```
With[{S = {{0, -1}, {1, 0}}, T = {{1, 1}, {0, 1}}},
 MatrixForm[T.S.T.T.S.T]]
```

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

The modular group is important because of the existence of modular functions, which are functions that have simple transformation laws under the action of the modular group. A prototypical modular function is the modular discriminant function, which may be defined for $\mathrm{Im}\, z > 0$ by

$$\Delta(z) = e^{2\pi i z} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n z}\right)^{24}.$$

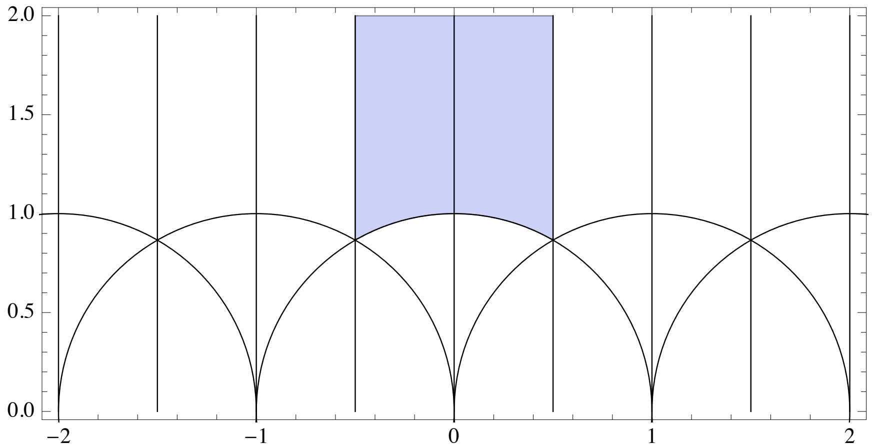
Since this product has zeros at every rational number, the real axis becomes a natural boundary of the domain $\mathbb{H}$ of $\Delta(z)$. Using the methods of analysis, it is possible to show that

$$\Delta\left(\frac{a\,z + b}{c\,z + d}\right) = (c\,z + d)^{12}\,\Delta(z) \tag{2}$$

for every matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in the modular group. Two observations are in order concerning the transformation formula (2). First, as

$$\mathrm{Im}\left(\frac{a\,z + b}{c\,z + d}\right) = \frac{(a\,d - b\,c)\,\mathrm{Im}(z)}{|\,c\,z + d\,|^2} = \frac{\mathrm{Im}(z)}{|\,c\,z + d\,|^2},$$

we see that the transformed value of z still has a positive imaginary part, so it still lies in the domain of $\Delta(z)$. Second, the values of $\Delta(z)$ where z ranges over the whole upper half-plane $\mathbb{H}$ are related to the values of $\Delta\,(z)$ where z is restricted to the region shaded blue here.



This region is known as the fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$. This is because the transformations S and T can be used to bring any point in $\mathbb{H}$ into this region, and no two points inside it differ by a Möbius transformation in $\mathrm{PSL}_2(\mathbb{Z})$. The transformation T pairs the left edge with the right edge, while the transformation S pairs the arc from i to $e^{2\pi i/6}$ with the arc from i to $e^{2\pi i/3}$.

Subgroups of the Modular Group

In the theory of modular functions one often wants to know what transformations leave a given function unchanged. For example,

$$f(z) = \frac{\Delta(5\,z)}{\Delta(z)}$$

will not be unchanged by all the transformations in $\mathrm{PSL}_2(\mathbb{Z})$, since the numerator $\Delta(5\,z)$ does not have a transformation formula under all elements of $\mathrm{PSL}_2(\mathbb{Z})$. However, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $\mathrm{PSL}_2(\mathbb{Z})$ and c is divisible by 5, then

$$\frac{\Delta\left(5\,\frac{a\,z+b}{c\,z+d}\right)}{\Delta\left(\frac{a\,z+b}{c\,z+d}\right)} = \frac{\Delta\left(\frac{a\,(5\,z)+5\,b}{(c/5)\,(5\,z)+d}\right)}{\Delta\left(\frac{a\,z+b}{c\,z+d}\right)} = \frac{((c\,/\,5)\,(5\,z)+d)^{12}\,\Delta(5\,z)}{(c\,z+d)^{12}\,\Delta(z)} = \frac{\Delta(5\,z)}{\Delta(z)}.$$

Thus, we are naturally led to the subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ given by

$$\Gamma_0(5) = \left\{\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle|\, a, b, c, d \in \mathbb{Z},\ a\,d - b\,c = 1,\ c \equiv 0 \ (\mathrm{mod}\ 5)\right\}.$$

The package ModularSubgroups.m addresses the computational problem of working with such subgroups of the modular group. However, only certain subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ can be identified by congruence conditions on their entries, as is the case with $\Gamma_0(5)$. Such subgroups are called congruence subgroups and are discussed more later. For this reason, we need a better way to represent subgroups. The key to this lies in the matrices S and $O = T\,S$. Since S and T generate $\mathrm{PSL}_2(\mathbb{Z})$, S and O are also generators. However, it can be

shown that $\mathrm{PSL}_2(\mathbb{Z})$ is the free product of $\{I, S\}$ and $\{I, O, O\,O\}$; that is, every matrix in $\mathrm{PSL}_2(\mathbb{Z})$ can be written uniquely as a word in S and O as long as no two consecutive S's appear and no three consecutive O's appear in the word. This last condition is necessary because of the relations $S^2 = O^3 = \pm I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (the identity matrix) should be thought of as the empty word.

A subgroup Γ of the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is said to have finite index (in $\mathrm{PSL}_2(\mathbb{Z})$) if $\mathrm{PSL}_2(\mathbb{Z})$ can be written as a disjoint union

$$\mathrm{PSL}_2(\mathbb{Z}) = g_1\,\Gamma \bigcup g_2\,\Gamma \bigcup \cdots \bigcup g_\mu\,\Gamma$$

of left cosets $g_i\,\Gamma$, where the left coset $g\,\Gamma$ is defined as $g_i\,\Gamma = \{g_i\,h \mid h \in \Gamma\}$. In this way, the group $\mathrm{PSL}_2(\mathbb{Z})$ is partitioned into several "copies" of Γ, and the number of copies of Γ that fit inside $\mathrm{PSL}_2(\mathbb{Z})$ is called the index μ. If Γ is a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ with index μ and left cosets $g_1\,\Gamma, \ldots, g_\mu\,\Gamma$ (with a distinguished coset $g_1\,\Gamma = \Gamma$), the matrices S and O permute the left cosets when acting by multiplication on the left; that is, we have equations

$$S\,g_i\,\Gamma = g_{S(i)}\,\Gamma$$
$$O\,g_i\,\Gamma = g_{O(i)}\,\Gamma$$

where S and O should be viewed as some permutations of the set $\{1, 2, \ldots, \mu\}$, that is, elements of the symmetric group Sym_μ.

This identification of the matrices S and O as permutations gives rise to the permutation representation of Γ, which we use to represent any subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ with finite index. Specifically, a subgroup Γ is identified by: (1) its index μ; (2) the permutation $S \in \mathrm{Sym}_\mu$; and (3) the permutation $O \in \mathrm{Sym}_\mu$. The permutations S and O are not arbitrary. The following two conditions are necessary and sufficient for a given $S, O \in \mathrm{Sym}_\mu$ to appear as the representation of some group Γ.

(1) $S^2 = O^3 = \mathrm{id}$ in Sym_μ, where id is the identity in Sym_μ. This condition arises from the fact that as matrices, we have $S^2 = O^3 = \pm I$.

(2) S and O generate a transitive subgroup of Sym_μ, or equivalently, the Schreier cosets graph discussed later is connected. This condition arises because the matrix $g_j\,g_i^{-1} \in \mathrm{PSL}_2(\mathbb{Z})$ sends the coset $g_i\,\Gamma$ to the coset $g_j\,\Gamma$, hence the action of $\mathrm{PSL}_2(\mathbb{Z})$ on the left cosets "connects" all of the cosets together.

If these two conditions are satisfied, the group Γ may be identified as $\Gamma = \{\text{words } w \text{ in } S \text{ and } O \mid w(1) = 1\}$, where the condition $w(1) = 1$ needs to be evaluated after thinking of w as a permutation by converting S and O into their corresponding permutations.

Since our representation of Γ by two permutations S and O involves an arbitrary ordering of the nontrivial cosets $g_2\,\Gamma, \ldots, g_\mu\,\Gamma$, two different representations (μ, S_1, O_1) and (μ, S_2, O_2) represent the same group precisely when there is a relabeling of the indices $2, \ldots, \mu$ in the permutations of Sym_μ that simultaneously converts S_1 into S_2 and O_1 into O_2. For, example the two representations

$$\Gamma_1 = (4, S = \{1 \to 2, 2 \to 1, 3 \to 3, 4 \to 4\}, O = \{1 \to 1, 2 \to 3, 3 \to 4, 4 \to 2\})$$
$$\Gamma_2 = (4, S = \{1 \to 2, 2 \to 1, 3 \to 3, 4 \to 4\}, O = \{1 \to 1, 2 \to 4, 4 \to 3, 3 \to 2\})$$

represent the same group, as the relabeling $\{2 \to 2, 3 \to 4, 4 \to 3\}$ converts Γ_1 to Γ_2.

Another important combinatorial object attached to a subgroup Γ of finite index is the Farey symbol for Γ, as described in [1]. This symbol directly encodes a fundamental domain for Γ as well as the edge-pairing matrices for this fundamental domain. Equivalently, it encodes independent generators for Γ. However, since the equivalence of two representations of Γ by two different Farey symbols is not as straightforward to detect, the permutation representation as described was chosen for the underlying representation for Γ.

Congruence Subgroups

A subgroup Γ of $\mathrm{PSL}_2(\mathbb{Z})$ is called a congruence subgroup if it contains the principal congruence subgroup of level N,

$$\Gamma(N) = \left\{ M \in \mathrm{PSL}_2(\mathbb{Z}) \,\middle|\, M \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\, N) \right\},$$

for some natural number N. If this is the case, we can describe Γ as those matrices whose entries satisfy certain congruences modulo N. For example, two families of congruence subgroups are $\Gamma_0(N)$ and $\Gamma_1(N)$, which are defined as

$$\Gamma_1(N) = \left\{ M \in \mathrm{PSL}_2(\mathbb{Z}) \,\middle|\, M \equiv \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\, N) \right\},$$
$$\Gamma_0(N) = \left\{ M \in \mathrm{PSL}_2(\mathbb{Z}) \,\middle|\, M \equiv \pm \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mathrm{mod}\, N) \right\}.$$

Recently in [2], Hsu gave a simple test for determining if a given subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is a congruence subgroup, based on a presentation for $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. This algorithm is implemented here and generalized to compute the congruence closure of a subgroup Γ, which is the smallest congruence subgroup that contains Γ.

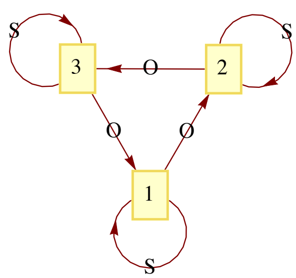
Schreier Cosets Graphs

The Schreier cosets graph of Γ is of fundamental importance to several of the algorithms in the package. Given a subgroup Γ with index μ and permutations S and O, the Schreier coset graph is the connected graph with μ vertices $1, \ldots, \mu$ and 2μ labeled edges

$$1 \xrightarrow{S} S(1), \ldots, \mu \xrightarrow{S} S(\mu), 1 \xrightarrow{O} O(1), \ldots, \mu \xrightarrow{O} O(\mu).$$

Such a graph has the property of being folded. A graph is said to be folded if every vertex has at most one edge of a given orientation and label incident with it. If there is a vertex with two or more edges of the same label and orientation, then the graph is said to be unfolded. One property of the Schreier cosets graph is that the subgroup Γ of the modular group consists of all words w in S and O such that, when starting at vertex 1, the path that follows word w must terminate at vertex 1. For example, take the subgroup Γ with the following Schreier cosets graph.

```
GraphPlot[{{1 → 2, "O"}, {2 → 3, "O"}, {3 → 1, "O"},
  {1 → 1, "S"}, {2 → 2, "S"}, {3 → 3, "S"}},
 DirectedEdges → True, VertexLabeling → True]
```



The word $w = O\,S\,O\,O$, which corresponds to the matrix

$$O\,S\,O\,O = \pm\begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix},$$

is in Γ as the path traced out by w is given by $1 \xrightarrow{O} 2 \xrightarrow{O} 3 \xrightarrow{S} 3 \xrightarrow{O} 1$ (w must be read right to left since we are dealing with left cosets). Since the graph is folded, the process of tracing a path given by a word in S and O is deterministic. The group Γ corresponding to this Schreier cosets graph turns out to be a congruence subgroup, and its defining congruences are given in Example 1.

Examples

All of these examples were tested in Mathematica 10.

Set the directory to be able to load the package and then evaluate the `Needs`.

```
Needs["ModularSubgroups`"]
```

Subgroups of the modular group are maintained in the container `mGroup[μ, S, O]`, and the names of the functions that operate on these groups start with a lower case “m” in order to avoid possible conflicts with built-in symbols. The matrices `mS`, `mO`, `mT`, `mR` of the package are set as follows.

```
MatrixForm /@ {mS, mO, mT, mR}
```

$$\left\{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\}$$

Example 1: Describing Congruence Subgroups

Here is the group Γ from the section on Schreier cosets graphs. The permutations are listed so that $S(i) = S[\![i]\!]$ and $O(i) = O[\![i]\!]$, where S and O are the last two arguments of the `mGroup` container.

```
Γ = mGroup[3, {1, 2, 3}, {2, 3, 1}];
```

This group turns out to be a congruence subgroup of level 3, and it consists of those matrices that are congruent modulo 3 to one of the following matrices.

```
{mLevel[Γ], MatrixForm /@ mCongruenceImage[Γ]}
```

$$\left\{3, \left\{\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}\right\}\right\}$$

So, for example, the group Γ has the description

$$\Gamma = \left\{\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a\,d - b\,c = 1,\; a\,b + c\,d \equiv 0 \pmod 3\right\}.$$

Example 2: Congruence Subgroups from Generating Sets

The group generated by T^n and S is of finite index only for $n = \pm 1, \pm 2$. Similarly, the group generated by T^n and O is of finite index only for $n = \pm 1, \pm 2, \pm 3$.

```
{{"n", "〈 T^n , S 〉", "〈 T^n , O 〉"}}~Join~Table[{n,
    mFromGenerators[{MatrixPower[mT, n], mS}],
    mFromGenerators[{MatrixPower[mT, n], mO}]
   }, {n, -6, 6}] // TableForm
```

```
n     〈 T^n , S 〉                    〈 T^n , O 〉
-6    $InfiniteIndex                  $InfiniteIndex
-5    $InfiniteIndex                  $InfiniteIndex
-4    $InfiniteIndex                  $InfiniteIndex
-3    $InfiniteIndex                  mGroup[4, {2, 1, 4, 3}, ·
-2    mGroup[3, {1, 3, 2}, {2, 3, 1}]  mGroup[2, {2, 1}, {1, 2}
-1    mGroup[1, {1}, {1}]             mGroup[1, {1}, {1}]
0     $InfiniteIndex                  $InfiniteIndex
1     mGroup[1, {1}, {1}]             mGroup[1, {1}, {1}]
2     mGroup[3, {1, 3, 2}, {2, 3, 1}]  mGroup[2, {2, 1}, {1, 2}
3     $InfiniteIndex                  mGroup[4, {2, 1, 4, 3}, ·
4     $InfiniteIndex                  $InfiniteIndex
5     $InfiniteIndex                  $InfiniteIndex
6     $InfiniteIndex                  $InfiniteIndex
```

Example 3: Subgroups of Index 7

There are two conjugacy classes of congruence subgroups of index 7, which we define here by their generators.

In the printed form of the group Γ:

1. μ is the index of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.
2. g is the genus of the compact surface $(\mathbb{H} \bigcup \mathbb{Q}_\infty) / \Gamma$.
3. ϵ_∞ is the number of cusps of Γ, namely, the size of $\mathbb{Q}_\infty / \Gamma$.
4. ϵ_2 is the number of fixed points of order 2 of Γ in $\mathbb{H} / \Gamma$.
5. ϵ_3 is the number of fixed points of order 3 of Γ in $\mathbb{H} / \Gamma$.

These numbers are related by $12\,g = 12 + \mu - 3\,\epsilon_2 - 4\,\epsilon_3 - 6\,\epsilon_\infty$.

```
g1 = mFromGenerators[{mS,
    MatrixPower[mT, 4].mS.MatrixPower[mT, -4],
    MatrixPower[mT, 5].mS.MatrixPower[mT, -5],
    MatrixPower[mT, 2].mS.MatrixPower[mT, -1]}];
g2 = mFromGenerators[{mS,
    MatrixPower[mT, 2].mS.MatrixPower[mT, -2],
    MatrixPower[mT, 3].mS.MatrixPower[mT, -3],
    MatrixPower[mT, 6].mS.MatrixPower[mT, -5]}];
{Most /@ mPrint[g1], Most /@ mPrint[g2]}
```

```
 μ: 7  g: 0  ∈∞: 1  ∈2: 3  ∈3: 1
{S: (1) (2.5) (3.4) (6) (7)
 O: (1.2.3) (4) (5.6.7)                ,
 T: (1.2.6.7.5.3.4)
 μ: 7  g: 0  ∈∞: 1  ∈2: 3  ∈3: 1
 S: (1) (2.7) (3.4) (5) (6)
 O: (1.2.3) (4.5.6) (7)                }
 T: (1.2.7.3.5.6.4)
```

They are indeed not conjugate.

```
mConjugateQ[g1, g2]
```

```
False
```

The intersection of these two groups turns out to have index 28, while the group generated by these two groups turns out to be the full modular group.

```
mMeet[g1, g2]
```

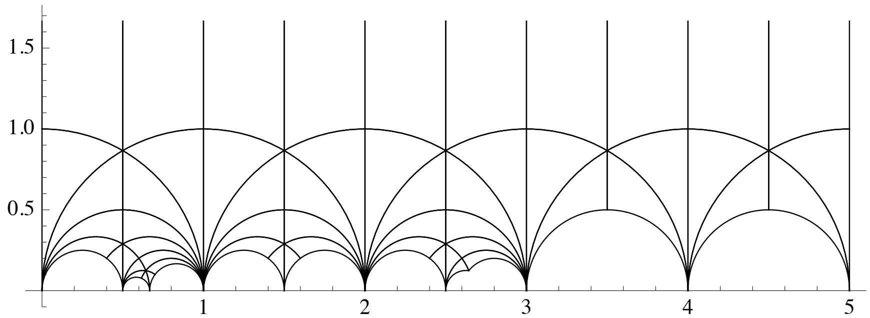
```
mGroup[28, {1, 3, 2, 4, 17, 20, 18, 19, 16, 13, 14, 15, 10,
   11, 12, 9, 5, 7, 8, 6, 21, 24, 23, 22, 28, 27, 26, 25},
  {6, 5, 8, 7, 9, 10, 11, 12, 2, 1, 4, 3, 14, 15, 13,
   16, 22, 21, 23, 24, 25, 26, 27, 28, 18, 17, 19, 20}]
```

```
mJoin[g1, g2]
```

```
mGroup[1, {1}, {1}]
```

A fundamental domain may be obtained with `mDomain`.

```
Graphics[mDomain[mMeet[g1, g2]], Axes → True]
```



The edge pairings for this fundamental domain are given in the Farey symbol. Edges $\frac{a}{b} \underset{n}{-} \frac{c}{d}$ between two rational numbers with the same integer label n are paired together, while edges with the label ● or ○ are paired with themselves.

```
mMeet[g1, g2] // mFareySymbol // mPrint
```

$$\infty \underset{\circ}{-} \frac{0}{1} \underset{2}{-} \frac{1}{2} \underset{3}{-} \frac{2}{3} \underset{\circ}{-} \frac{1}{1} \underset{\circ}{-} \frac{3}{2} \underset{3}{-} \frac{2}{1} \underset{1}{-} \frac{5}{2} \underset{\bullet}{-} \frac{3}{1} \underset{\circ}{-} \frac{4}{1} \underset{1}{-} \frac{5}{1} \underset{2}{-} \infty$$

The matrices returned by `mGenerators` are the matrices responsible for pairing the edges in this way.

```
Map[MatrixForm, mMeet[g1, g2] // mGenerators]
```

$$\left\{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 7 & -10 \\ 5 & -7 \end{pmatrix}, \begin{pmatrix} 7 & -25 \\ 2 & -7 \end{pmatrix}, \begin{pmatrix} -19 & 49 \\ -7 & 18 \end{pmatrix}, \begin{pmatrix} -7 & 33 \\ -3 & 14 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 7 \end{pmatrix}, \begin{pmatrix} 12 & -7 \\ 7 & -4 \end{pmatrix}, \begin{pmatrix} 7 & -5 \\ 10 & -7 \end{pmatrix}\right\}$$

▫ Example 4: Congruence Subgroups

The congruence closure of a subgroup Γ is the smallest congruence subgroup that contains Γ. We first start with the congruence subgroup of index 7 from the previous example and a non-congruence subgroup of index 9.

```
g = mFromGenerators[{mS,
   MatrixPower[mT, 4].mS.MatrixPower[mT, -4],
   MatrixPower[mT, 5].mS.MatrixPower[mT, -5],
   MatrixPower[mT, 2].mS.MatrixPower[mT, -1]}]
```

```
mGroup[7, {1, 5, 4, 3, 2, 6, 7}, {2, 3, 1, 4, 6, 7, 5}]
```

```
h = mGroupsOfIndex[9]〚5〛
```

```
mGroup[9, {1, 9, 4, 3, 8, 7, 6, 5, 2},
 {2, 3, 1, 5, 6, 4, 8, 9, 7}]
```

```
mCongruenceQ[h]
```

```
False
```

Its congruence closure is the theta subgroup.

```
hc = mCongruenceClosure[h]
```

```
mGroup[3, {1, 3, 2}, {2, 3, 1}]
```

One can also compute the congruence closure of a group by joining it with the principal congruence subgroup of the same level, but the package uses a much more efficient method. Membership in the groups $\Gamma(N)$, $\Gamma_1(N)$, and $\Gamma_0(N)$ can be tested with `mΓ[N]`, `mΓ1[N]`, and `mΓ0[N]`, respectively. The function `mFromMember` constructs the internal representation of the group given the group's membership function.

```
mSameQ[hc, mJoin[h, mFromMember[mΓ[mLevel[h]]]]]
```

```
True
```

We also have the following property, since `g` itself is congruence.

```
mSameQ[mCongruenceClosure[mMeet[h, g]], mMeet[hc, g]]
```

```
True
```

Next, we compute the congruence closure for the group given in Example 1.1 of [2]. It turns out to be the full modular group.

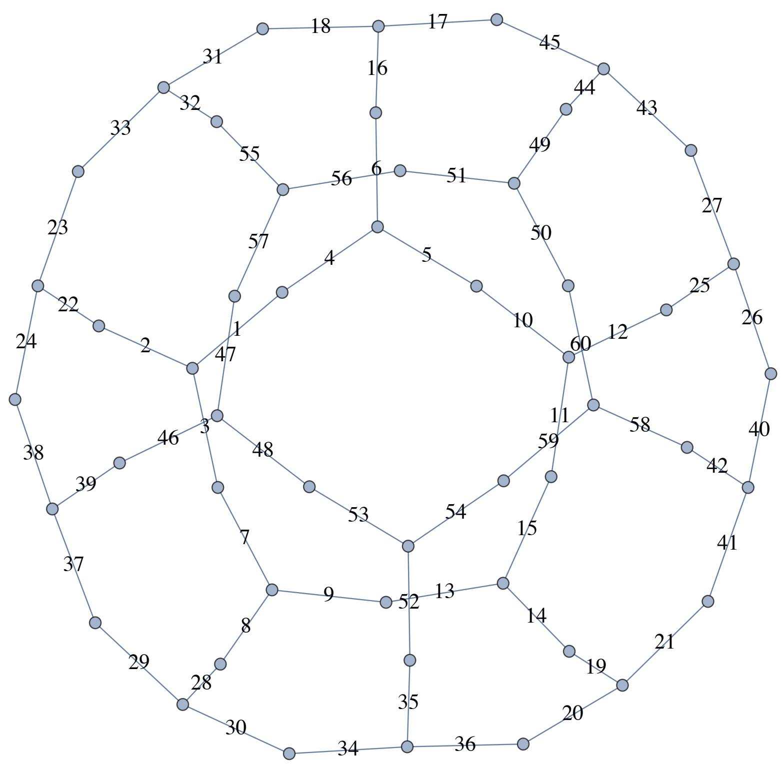
```
g = mGroup[10, {2, 1, 4, 3, 6, 5, 8, 7, 10, 9},
   {3, 7, 5, 2, 1, 8, 4, 9, 6, 10}];
mCongruenceClosure[g]
```

```
mGroup[1, {1}, {1}]
```

▫ Example 5: Generators for $\Gamma(5)$

First get the principal congruence subgroup of level 5, which has index 60.

```
g = mFromMember[mΓ[5]];
mPrint[g]⟦1, -1⟧
```



Generators may be computed quickly from this permutation representation, and we can also efficiently reconstruct the group from a list of generators.

```
Map[MatrixForm, gens = mGenerators[g]]
```

$$\left\{\begin{pmatrix}-1 & 5\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 5 & -1\end{pmatrix}, \begin{pmatrix}6 & -5\\ 5 & -4\end{pmatrix}, \begin{pmatrix}-6 & -5\\ 5 & 4\end{pmatrix}, \begin{pmatrix}11 & -20\\ 5 & -9\end{pmatrix}, \begin{pmatrix}-14 & -25\\ -5 & -9\end{pmatrix}, \begin{pmatrix}9 & -5\\ 20 & -11\end{pmatrix}, \begin{pmatrix}-9 & -5\\ -25 & -14\end{pmatrix}, \begin{pmatrix}-16 & 25\\ -25 & 39\end{pmatrix}, \begin{pmatrix}-49 & -80\\ -30 & -49\end{pmatrix}, \begin{pmatrix}16 & 25\\ -25 & -39\end{pmatrix}\right\}$$

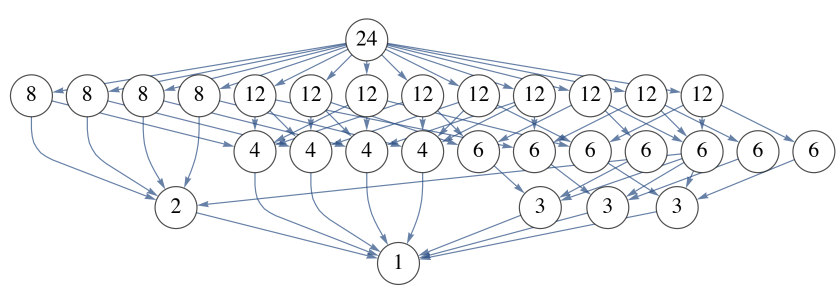
```
mSameQ[g, mFromGenerators[gens]]
```

```
True
```

Example 6: Supergroup Lattice

We will graph the supergroup lattice for the principal congruence subgroup of level 4. The `mSupergroups` function is used to make the supergroup lattice. The index of each group (in $\mathrm{PSL}_2(\mathbb{Z})$) is displayed in the lattice, and the actual group is displayed as a tooltip. Every subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ whose matrices can be described by congruence conditions modulo 4 appears somewhere on this lattice.

```
g = mFromMember[mΓ[4]];
sg = mSupergroups[g];
m = DirectedEdge @@@ Position[Outer[mLessQ, sg, sg], True];
edges = Cases[m, i_ ↔ j_ /; Not[MatchQ[m,
       {___, k_ ↔ j, ___, i ↔ k_, ___}]]];
Graph[Table[
   Tooltip[Labeled[i, Placed[sg⟦i, 1⟧, Center]], sg⟦i⟧],
   {i, 1, Length[sg]}],
  edges, VertexSize → 0.75, VertexStyle → White]
```



Example 7: Cusps for a Subgroup

If Γ is a subgroup of the modular group, then every matrix in Γ acts on $\mathbb{Q}_\infty$ (the set of rational numbers with ∞ included) and partitions $\mathbb{Q}_\infty$ into equivalence classes. We say that two rational numbers x_1 and x_2 are equivalent under Γ if there is an element of Γ that sends x_1 to x_2. The set of equivalence classes of $\mathbb{Q}_\infty$ under the action of Γ is known as the cusps for Γ, and there are finitely many cusps if Γ has finite index in the modular group. The width of a cusp x with respect to Γ is defined to be the index of the Γ stabilizer of x inside the $\mathrm{PSL}_2(\mathbb{Z})$ stabilizer of x.

Let g and h be the subgroups

$$g = \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a\,b \equiv 0 \pmod 2,\ c\,d \equiv 0 \pmod 2 \right\},$$

$$h = \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, c \equiv 0 \pmod 5,\ d \equiv 1 \pmod 5,\ b + c \equiv 0 \pmod 2 \right\}.$$

```
gmem[{{a_, b_}, {c_, d_}}] := And[EvenQ[a b], EvenQ[c d]];
hmem[{{a_, b_}, {c_, d_}}] :=
  And[Mod[c, 5] == 0, Mod[d, 5] == 1, EvenQ[b + c]];
g = mFromMember[gmem];
h = mFromMember[hmem];
```

Here is a list of inequivalent cusps of h and their widths.

```
mCusps[h]
```

$$\left\{\{\infty, 2\}, \{0, 10\}, \left\{\frac{1}{2}, 10\right\}, \left\{\frac{2}{5}, 2\right\}\right\}$$

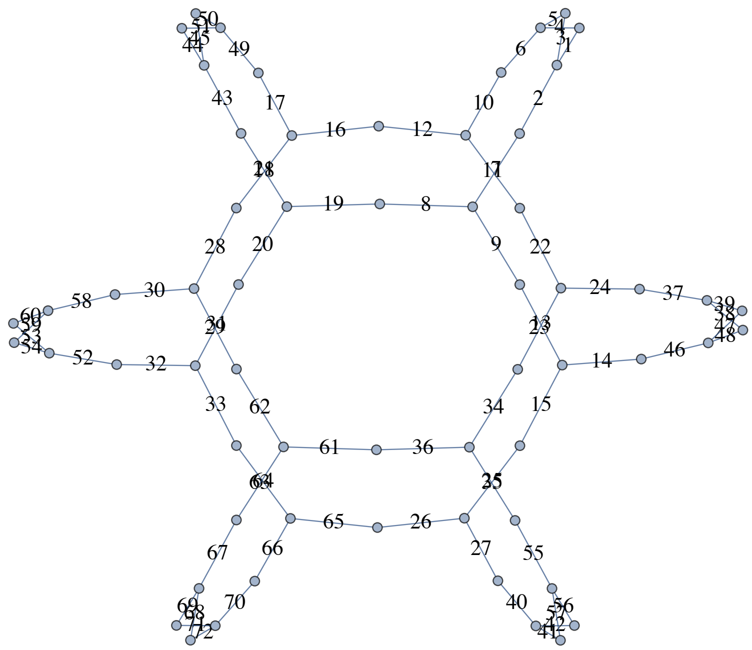
Here we reduce a list of random cusps to one of these four. The frequency of each cusp in the list should be proportional to its width.

```
mCuspReduce[h, RandomInteger[{1, 20}, 20] /
  RandomInteger[{1, 20}, 20]]
```

$$\left\{\infty, \infty, 0, 0, \frac{1}{2}, \frac{1}{2}, 0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{2}{5}, \frac{2}{5}, 0, 0, \frac{1}{2}, 0, \frac{2}{5}, 0, 0, 0\right\}$$

The intersection of `g` and `h` may be computed.

```
mPrint[
   gh = mFromMember[(mMemberQ[g, #] && mMemberQ[h, #]) &]] //
  First // Last
```



Of course, the implementation in the package is more efficient.

```
mSameQ[gh, mMeet[g, h]]
```

```
True
```

◻ Example 8: Non-congruence Subgroups from Caranica

If a_n denotes the total number of subgroups of the modular group of index n, then with $x\, f'(x) / f(x) = \sum a_n\, x^n = x + x^2 + 4\, x^3 + 8\, x^4 + \ldots$ so that $f(x) = 1 + x + 5\, x^2 / 2 + \ldots$ it is possible to show that

$$x^7 \left(x^3 - 1\right) f''(x) + \left(4\, x^9 + 2\, x^7 - 4\, x^6 - 2\, x^4 - 4\, x^3 + 1\right) f'(x) + \\ \left(2\, x^8 + 2\, x^6 - 4\, x^5 + x^4 - 4\, x^3 - 4\, x^2 - x - 1\right) f(x) = 0,$$

and that

$$a_n \sim \left(12\, \pi\, e^{1/2}\right)^{-1/2} \exp\!\left(\frac{1}{6}\, n \log(n) - \frac{1}{6}\, n + n^{1/2} + n^{1/3} + \frac{1}{2} \log(n)\right).$$

Since the radius of convergence of the power series $\sum a_n x^n$ is zero, this differential equation must be treated formally as a recurrence relation for the coefficients of $f(x)$. See Section 1 of [3] for details.

Caranica [4, Table 3.1] has computed the conjugacy classes of non-congruence subgroups of index 9. However, this table incorrectly claims that there are 11 conjugacy classes. In fact, there are 108 non-congruence subgroups of index 9 and 12 conjugacy classes. Vidal [5] has given a formula for the generating function of the total number of conjugacy classes of subgroups (congruence or not) of a given index.

```
Length[
 cclass = Select[mConjugacyClassesOfIndex[9],
   Not[mCongruenceQ[#]] &]]
```

```
12
```

Fortunately, the Farey symbols for the claimed groups are provided by Caranica, so we can recover the source of the error. First we verify that there are indeed 11 conjugacy classes of non-congruence subgroups in the table.

```
fl = mFromFarey /@ {
    mFarey[∞, -2, 0, -3, 1 / 2, -3, 1, -3, ∞],
    mFarey[∞, -2, 0, -3, 1, -3, 2, -3, ∞],
    mFarey[∞, -2, 0, 1, 1 / 2, 2, 2 / 3, 1, 1, 2, ∞],
    mFarey[∞, -2, 0, 1, 1, 1, 2, -2, 3, -2, ∞],
    mFarey[∞, 1, 0, -2, 1 / 3, -2, 1 / 2, 1, 1, -2, ∞],
    mFarey[∞, -2, 0, 1, 1, 1, 2, 2, 3, 2, ∞],
    mFarey[∞, 1, 0, 2, 1 / 3, 2, 1 / 2, 1, 1, -2, ∞],
    mFarey[∞, -2, 0, -2, 1, -2, 2, 1, 3, 1, ∞],
    mFarey[∞, 1, 0, 1, 1, -2, 2, 2, 3, 2, ∞],
    mFarey[∞, 1, 0, 1, 1, -2, 2, -2, 3, -2, ∞],
    mFarey[∞, -2, 0, 1, 1 / 2, 1, 2 / 3, 2, 1, 2, ∞]};
{
 Length[DeleteDuplicates[fl, mConjugateQ]],
 Length[Select[fl, Not[mCongruenceQ[#]] &]]
}
```

```
{11, 11}
```

This is the group that is missing from the table.

```
Fold[Function[{c, f}, Select[c, Not[mConjugateQ[#1, f]] &]],
 cclass, fl]
```

```
{mGroup[9, {4, 7, 3, 1, 9, 6, 2, 8, 5},
  {2, 3, 1, 5, 6, 4, 8, 9, 7}]}
```

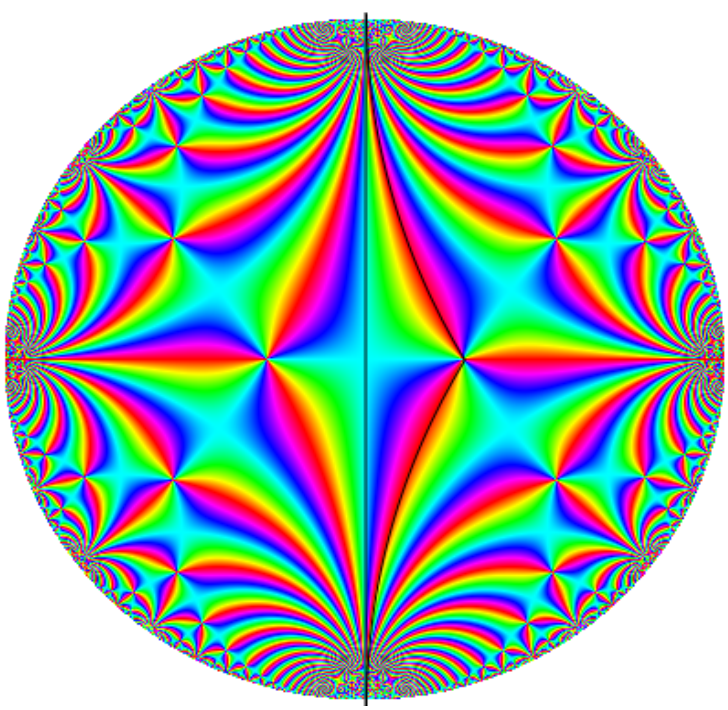
Example 9: Fundamental Domains and Univalent Functions

The Mathematica built-in function `KleinInvariantJ` is invariant under $PSL_2(\mathbb{Z})$ and takes each complex value exactly once inside a fundamental domain for $PSL_2(\mathbb{Z})$. A plot of this function and an outline of its fundamental domain are shown.

The upper half-plane, which is parameterized by z, has been mapped into the unit disk, which is parameterized by $w = x + i\,y$, by the relation $w = i\,(z - i)\,/\,(z + i)$.

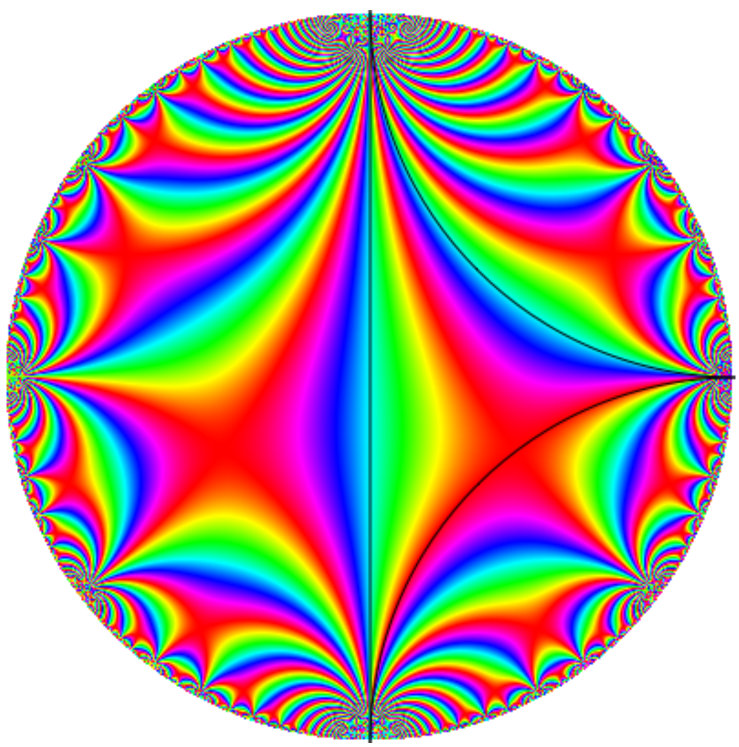
The hue of the color plotted at a point in the w disk is the argument of the complex number $f(z)$, where z is the point in the upper half-plane corresponding to w.

```
f[z_] := 1728 KleinInvariantJ[z];
im = ColorConvert[
   Image[Table[If[x^2 + y^2 > 0.97, {0, 0, 1},
      {1/2 + 1/(2 π) Arg[N[f[(1 - i x + y)/(-i + x + i y)]]], 1, 1}],
     {y, 1, -1, -1/200}, {x, -1, 1, 1/200}],
    ColorSpace → "HSB"], "RGB"];
ImageMultiply[im, Image[Graphics[{
     Line[{{0, -1}, {0, 1}}],
     Circle[{2, -1}, 2, {5 π/6, π}],
     Circle[{2, 1}, 2, {π, 7 π/6}]},
    PlotRange → {{-1, 1}, {-1, 1}}],
   ImageSize → ImageDimensions[im]]]
```



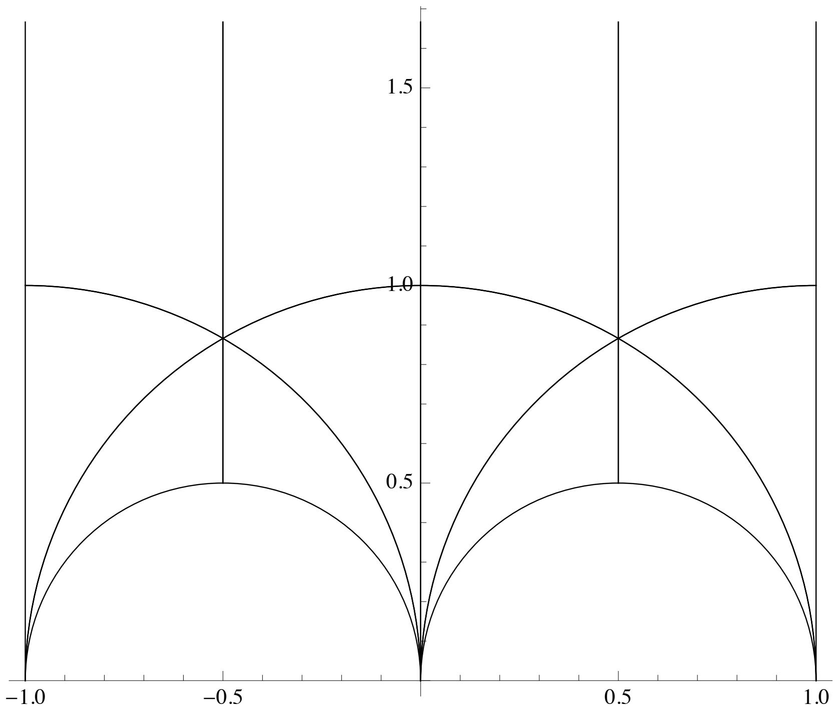
Similarly, the built-in function `DedekindEta` can be used to construct such a function $f(z)$ for $\Gamma_0(2)$, which is a congruence subgroup of $PSL_2(\mathbb{Z})$ of index 3. A plot of this function and a fundamental domain for $\Gamma_0(2)$ are shown next.

```
f[z_] := DedekindEta[z]^24 / DedekindEta[2 z]^24;
im = ColorConvert[
   Image[Table[If[x^2 + y^2 > 0.99, {0, 0, 1},
      {1/2 + 1/(2 π) Arg[N[f[(1 - ⅈ x + y)/(-ⅈ + x + ⅈ y)]]], 1, 1}],
     {y, 1, -1, -1/200}, {x, -1, 1, 1/200}],
    ColorSpace → "HSB"], "RGB"];
ImageMultiply[im, Image[Graphics[{
     Line[{{0, -1}, {0, 1}}],
     Circle[{1, 1}, 1, {π, 3 π/2}],
     Circle[{1, -1}, 1, {π/2, π}]},
    PlotRange → {{-1, 1}, {-1, 1}}],
   ImageSize → ImageDimensions[im]]]
```



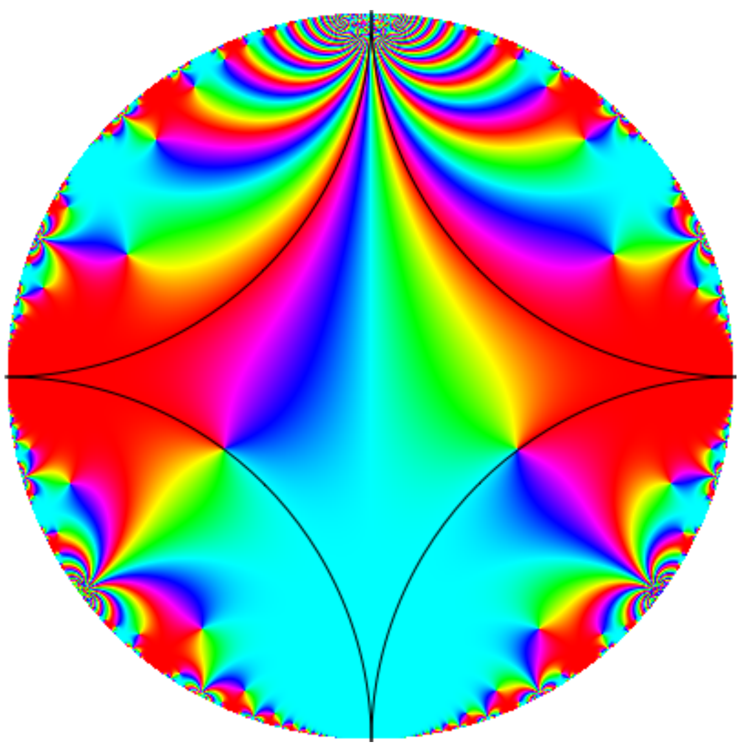
Here is a similar construction for $\Gamma(2)$. This plots the fundamental domain for $\Gamma(2)$ in the z half-plane.

```
Graphics[mDomain[mFromMember[mΓ[2]]], Axes → True]
```



In the w disk, such a region becomes a diamond shape. A univalent function on $\mathbb{H}/\Gamma(2)$ must be invariant under the generators of $\Gamma(2)$; that is, $f(z) = f(z+2) = f\left(\frac{1}{2z+1}\right)$, and such a function is provided by the built-in function `ModularLambda`.

```
f[z_] := 16 / ModularLambda[z] - 8;
im = ColorConvert[
   Image[Table[If[x^2 + y^2 > 0.99, {0, 0, 1},
      {1/2 + 1/(2 π) Arg[N[f[(1 - ⅈ x + y)/(-ⅈ + x + ⅈ y)]]], 1, 1}],
     {y, 1, -1, -1 / 200}, {x, -1, 1, 1 / 200}],
    ColorSpace → "HSB"], "RGB"];
ImageMultiply[im, Image[Graphics[{
     Circle[{-1, 1}, 1, {3 π / 2, 2 π}],
     Circle[{-1, -1}, 1, {0, π / 2}],
     Circle[{1, 1}, 1, {π, 3 π / 2}],
     Circle[{1, -1}, 1, {π / 2, π}]},
    PlotRange → {{-1, 1}, {-1, 1}}],
   ImageSize → ImageDimensions[im]]]
```

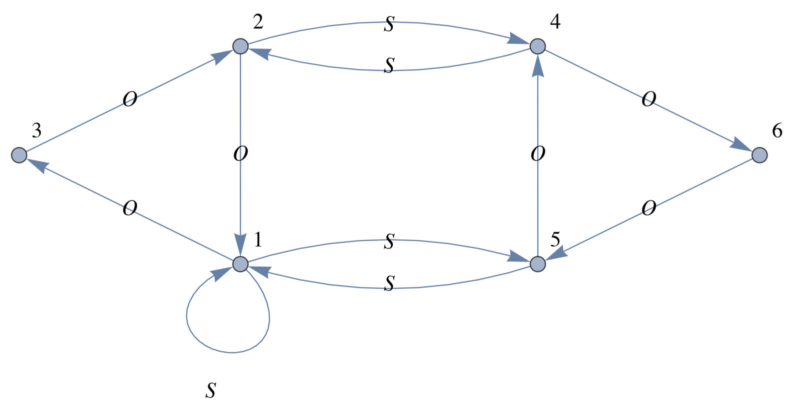


In this case, the zero of $f(z)$ occurs on this diamond where the colors coalesce. In the previous example, the zeros of $f(z)$ are not visible in this way because they occur on the boundary of the w disk.

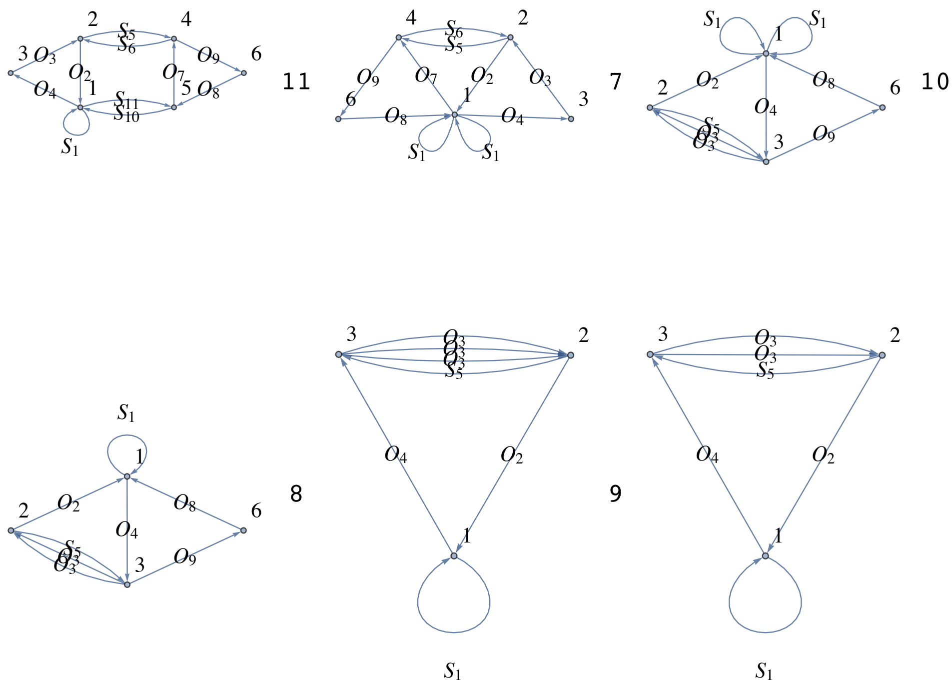
■ A Description of the Algorithms

Many operations on subgroups of the modular group depend on operations on graphs. Several of the algorithms used here encounter unfolded graphs, and we use the efficient folding algorithm described in [6] to implement Stallings's folding process, which converts any graph to a folded graph.

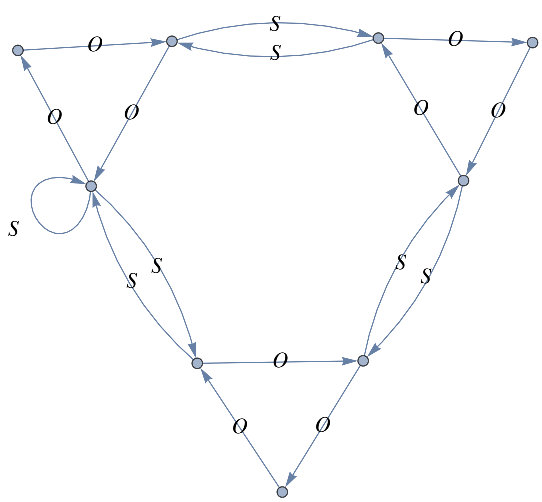
As described in the introduction, it is straightforward to convert a group Γ described by the permutations S and O to the Schreier cosets graph. In order to reverse this procedure, it is necessary that each edge labeled O either have the same initial and terminal vertex or be part of a three-cycle. Similarly, each edge labeled S needs to occur in either a loop or a two-cycle. All of the graphs used here have this property. However, when building a group from a list of a generators, we may encounter a folded graph in which some vertex does not have valence four. Such graphs do not correspond to subgroups of Γ of finite index. Let us illustrate the folding procedure on the following graph.



Such a graph represents the subgroup Γ that is generated by the two words S and $O\,S\,O\,S$, since, except for the trivial cycles induced by the relations $S^2 = O^3 = 1$, these are the only cycles in the graph. Whenever there are two edges $v \multimap u$ and $v \multimap w$ incident at the same vertex with the same orientation and label, causing the graph to be unfolded, the edge $v \multimap w$ may be deleted and the vertex w may be merged with u without changing the subgroup represented by the graph. The progression of the graph folding procedure shown is left to right, top to bottom, with the edges to be deleted shown between graphs.



The subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ represented by the final folded graph has index three and is determined by the permutations $S = (1)(23)$ and $O = (132)$. This is also known as the theta subgroup. The reader is urged to work through the folding process for the group generated by S and $O\,S\,O\,S\,O\,S$ to see that it does not have finite index in $\mathrm{PSL}_2(\mathbb{Z})$. The starting graph is shown here.



It is useful to have a notion of a standard representation (in terms of the permutations S and O) of a group Γ whereby two groups are the same if and only if their permutations S and O are identical. This can be accomplished by visiting the coset Γ first (denoted by the index 1 in the permutations). Once we have visited a coset $g_i\,\Gamma$, we then recursively visit the coset $O\,g_i\,\Gamma$ (assuming this has not been visited yet), and once this trip has returned to the coset $g_i\,\Gamma$, we visit the coset $S\,g_i\,\Gamma$ (also assuming this coset has not been visited yet). The standard labels for the indices $2, \ldots, \mu$ for the nontrivial cosets may then be determined by the order in which that coset was visited.

In the case of testing a matrix m for membership in a group Γ, write m^{-1} as a word in S and O, then set $r = 1$ and check if $m^{-1}(r) = 1$. Specifically, for a given matrix $m \in \mathrm{PSL}_2(\mathbb{Z})$ whose entries in the left column are non-negative, multiply m on the left by the matrices

$$S\,O\,O = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \text{or}\, S\,O = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

until the left column contains a zero. The variable r holds the current coset, so every time m is multiplied by $S\,O\,O$, for example, r needs to be updated to $S(O(O(r)))$.

Given the membership function on matrices for a group, we construct the group coset by coset. Assume that Γ has index at least three in $\mathrm{PSL}_2(\mathbb{Z})$. If $O \in \Gamma$, start with the four cosets $L = \{\Gamma,\ S\,\Gamma,\ O\,S\,\Gamma,\ O\,O\,S\,\Gamma\}$; otherwise, start with the three cosets $L = \{\Gamma,\ O\,\Gamma,\ O\,O\,\Gamma\}$. Proceed by adding either one or three cosets to L at a time. If $g_i\,\Gamma \in L$ is such that:

1. $S\,g_i\,\Gamma \neq m\,\Gamma$ and $O\,S\,g_i\,\Gamma = S\,g_i\,\Gamma$, then add the coset $S\,g_i\,\Gamma$ to L.
2. $S\,g_i\,\Gamma \notin L$ and $O\,S\,g_i\,\Gamma \neq S\,g_i\,\Gamma$, then add the cosets $S\,g_i\,\Gamma, O\,S\,g_i\,\Gamma, O\,O\,S\,g_i\,\Gamma$ to L.

Where there is no such coset $g_i\,\Gamma$ satisfying either of these conditions, we have found all of the cosets of Γ. A naive implementation of this procedure would have worst-case running time $\mathrm{O}(\mu^3)$, where μ is the index of the resulting group. The worst-case running time may be reduced to $\mathrm{O}(\mu^2)$ by keeping track of which cosets actually need to be checked.

We may compute coset representatives, generators, and a Farey symbol in $\mathrm{O}(\mu)$ operations for a subgroup Γ of index μ. This works as follows. Let G be the graph corresponding to a subgroup of index μ. First, the graph is cut into a tree so that the coset labeled i is given by the resulting unique path from the vertex 1 to the vertex i. Any time a cut is made or a fixed point is encountered, the corresponding matrix is added to the list of generators. Finally, after the cosets and generators are computed and the cuts have been recorded, the Farey symbol is computed by a clockwise traversal of the tree.

The cusps of a given subgroup Γ are also important. The action of $\mathrm{PSL}_2(\mathbb{Z})$ on the upper half-plane is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) :\ z \longmapsto \frac{a\,z + b}{c\,z + d},$$

and this action extends to $\mathbb{Q}_\infty = \mathbb{Q} \bigcup \{\infty\}$. The equivalence classes of $\mathbb{Q}_\infty$ under the action of Γ, namely $\mathbb{Q}_\infty / \Gamma$, are finite, and we may choose a representative for each one as follows.

The stabilizer of ∞ in $\mathrm{PSL}_2(\mathbb{Z})$ is generated by $O\,S$ (or T). Therefore, any two cusps (say $m_1^{-1}(\infty)$ and $m_2^{-1}(\infty)$ for $m_1, m_2 \in \mathrm{PSL}_2(\mathbb{Z})$) are equivalent under Γ whenever there is an integer n such that $(O\,S)^n\, m_1\,\Gamma = m_2\,\Gamma$; that is, $m_1\,\Gamma$ and $m_2\,\Gamma$ belong to the same cycle of the permutation $O\,S$. The width of a cusp $m_1^{-1}(\infty)$ can then be defined as the length of the cycle (of $O\,S$) that contains the coset $m_1\,\Gamma$.

Joining and intersecting two groups is surprisingly simple. To compute the group that is generated by Γ_1 and Γ_2, we can form the graph G for Γ_1. Then, for each generator g of Γ_2, merge the vertices in G corresponding to the cosets Γ_1 and $g\,\Gamma_1$. This will in general result in a unfolded graph, which we can then fold and convert back to a permutation representation. In order to compute the permutation representations for the intersection of Γ_1 and Γ_2, first find the orbit of $\Gamma_1 \bigcap \Gamma_2$ under the action of S and O in terms of cosets of the form $m_1\,\Gamma_1 \bigcap m_2\,\Gamma_2$. A permutation representation of $\Gamma_1 \bigcap \Gamma_2$ may then be obtained by the action of S and O on the cosets in this orbit of $\Gamma_1 \bigcap \Gamma_2$.

It is also straightforward to check if two groups are the same or conjugate, or if one group is contained in another. To test if two groups Γ_1 and Γ_2 are the same, we employ a strategy similar to the process for standardizing the representation. The cosets of Γ_1 and Γ_2 are visited simultaneously, starting with the pair (Γ_1, Γ_2). If we are currently visiting the pair $(m_1\,\Gamma_1, m_2\,\Gamma_2)$, then we visit the pairs $(O\,m_1\,\Gamma_1, O\,m_2\,\Gamma_2)$ and $(S\,m_1\,\Gamma_1, S\,m_2\,\Gamma_2)$ as described in the standardization process. If the two paths ever become out of sync, that is, if cosets are visited in a different order, then we know the groups are not the same; otherwise the two paths will return back to (Γ_1, Γ_2) and we know that Γ_1 and Γ_2 are the same. Checking if Γ_1 and Γ_2 are conjugate can be accomplished by the same procedure. We need to check if the path stays in sync when starting at some pair $(g\,\Gamma_1, \Gamma_2)$ for $g \in \mathrm{PSL}_2(\mathbb{Z}) / \Gamma_1$.

The congruence functions use the list of relations of Hsu [2]. Recall that the congruence closure Γ^c of a group Γ is the smallest congruence subgroup that contains Γ. We compute the congruence closure of Γ as follows. Hsu gives a list of relations $x = y$ that are satisfied if and only if Γ is a congruence subgroup. Let L be the list of the permutations $x\,y^{-1}$ where $x = y$ is a relation in Hsu's list. If L contains a non-identity permutation p, this represents an obstacle to Γ being a congruence subgroup. Let N denote the level of Γ, which is defined as the order of the permutation $O\,S$. As it is known that Γ^c contains $\Gamma(N)$, the set of relations for Γ is also satisfied by Γ^c. Let p be any permutation in L and i an index of any coset in Γ. Since p must act trivially on the cosets of Γ^c and Γ is a subgroup of Γ^c, the group obtained from Γ by merging cosets i and $p(i)$ must also be contained in Γ^c. Therefore, merging the cosets i and $p(i)$ of Γ for all p and i must give Γ^c.

Conclusion

We have described an efficient package for manipulating and constructing subgroups of the modular group. It is hoped that this will further interest in these groups and facilitate research dealing with these subgroups.

Acknowledgments

The author would like to thank Junxian Li of the University of Illinois at Urbana-Champaign for many helpful discussions on improvements and corrections to initial implementations of the algorithms.

References

[1] C. A. Kurth and L. Long, "Computations with Finite Index Subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ Using Farey Symbols." arxiv.org/abs/0710.1835.

[2] T. Hsu, "Identifying Congruence Subgroups of the Modular Group," *Proceedings of the American Mathematical Society*, **124**(5), 1996 pp. 1351–1359. www.ams.org/journals/proc/1996-124-05/S0002-9939-96-03496-X/S0002-9939-96-03496-X.pdf.

[3] A. Lubotzky, "Counting Finite Index Subgroups," *London Mathematical Society Lecture Note Series 212: Groups '93 Galway/St Andrews, Vol. 2* (C. M. Campbell, E. F. Robertson, T. C. Hurley, S. J. Tobin, and J. J. Ward, eds.), Cambridge: Cambridge University Press, 1995 pp. 368–404.

[4] C. C. Caranica, "Algorithms Related to Subgroups of the Modular Group," Ph.D. thesis, Louisiana State University, 2009.
etd.lsu.edu/docs/available/etd-07092009-200839/unrestricted/Caranica_diss.pdf.

[5] S. A. Vidal, "Sur la classification et le dénombrement des sous-groupes du groupe modulaire et de leurs classes de conjugaison," *Publications IRMA*, **66**(II), 2006 pp. 1–35.
Preprint: arxiv.org/abs/math.CO/0702223.

[6] N. W. M. Touikant, "A Fast Algorithm for Stallings' Folding Process," *International Journal of Algebra and Computation*, **16**(6), 2006 pp. 1031–1045. doi:10.1142/S0218196706003396.

D. Schultz, "Manipulating Subgroups of the Modular Group," *The Mathematica Journal*, 2016.
dx.doi.org/doi:10.3888/tmj.18-4.

About the Author

Daniel Schultz is a postdoctoral researcher at Pennsylvania State University who is interested in modular functions and automorphic forms in general.

Daniel Schultz
Pennsylvania State University Department of Mathematics
University Park
State College, PA 16802
dps23@psu.edu