Computational Number Theory

Alyson Deines

2009

Abstract

My paper explains how $X_0(p)$ has complex structure for p prime, via Exercise 3.1.4 in Diamond and Shurman's **A First Course in Modular Forms**. It illustrates how to compute the orbits of the fundamental domain, the elliptic points, and the congruence classes on the boundary arcs used to "glue" these arcs together into a torus of genus g. I then demonstrate the process with $p = 13$.

1 Exercise 3.1.4 from Washington

I will begin with the proof of exercise 3.1.4 in Washington.

First the setup. As usual let p be a prime, $i = e^{i\pi/2}$, and $\mu_n = e^{i2\pi/n}$.

Take $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, $\mathcal{H}^* = \mathcal{H} \cup (\mathbb{Q} \cup \{\infty\})$, $X_0(p) = \Gamma_0(p)\backslash\mathcal{H}^*$. Let $\alpha_\infty = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ and $\alpha_j = \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix}$ for $j = 0, 1, ..., p-1$.

To identify which "sides" of the orbits are "glued" together, it is necessary to examine elliptic points and cusps.

Definition 1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. For each point $\tau \in \mathcal{H}$ let Γ_τ denote the isotropy subgroup of τ, i.e. the subgroup of Γ which fixes τ,*

$$\Gamma_\tau = \{\gamma \in \Gamma : \gamma(\tau) = \tau\}.$$

Definition 2. *A point $\tau \in \mathcal{H}$ is an elliptic point for Γ if Γ_τ is nontrival as a group of transformations.*

Definition 3. *The points $\Gamma\tau \in \Gamma \setminus (\mathbb{Q} \cup \{\infty\})$ are the cusps of $X(\Gamma)$.*

Now on to the exercises.

Theorem 4 (3.1.4(a))**.** *$SL_2(\mathbb{Z}) = \cup_j \Gamma_0(p)\alpha_j$, where $\cup_j \Gamma_0(p)\alpha_j$ is a disjoint union.*

Proof. First notice that $\cup_j \Gamma_0(p)\alpha_j \subset \mathrm{SL}_2(\mathbb{Z})$. Next I show the other inclusion. For some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, Let $\alpha_\infty = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ say $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, if $\gamma = \alpha\alpha_j$ for some $\alpha \in \Gamma_0(p)$, say $\alpha = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, then $f = b$ and $h = d$ so $e + bj = a$ and $g + dj = c$. Note that as $\alpha \in \Gamma_0(p)$, p divides g. So $dj \equiv c \pmod{p}$. As p is prime, d is invertable modulo p. As $j = 0, 1, 2, ..., p-1$, we have found

a unique $j \equiv cd^{-1} \pmod{p}$. Thus we have $e = a - bj$ and so we have found a matrix $\alpha \in \Gamma_0(p)$ so that $\gamma = \alpha\alpha_j$. So $\mathrm{SL}_2(\mathbb{Z}) \subset \cup_j \Gamma_0(p)\alpha_j$ and thus we have equality.

To show the disjoint union, notice that to prove equality the j found is uniquely defined. So no γ can be in $\Gamma_0(p)\alpha_j$ and $\Gamma_0(p)\alpha_i$ for $i \neq j$.

□

Theorem 5 (3.1.4 (b))**.** *$X_0(p)$ has exactly two cusps.*

Proof. Suppose there is only one cusp. Specifically, suppose for some $\gamma \in \Gamma_0(p)$ that $\gamma(\infty) = 0$. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $0 = \gamma(\infty) = \frac{a}{c}$. Thus $a = 0$. However $ad - bc = 1$ and p divides c. So we get $-bc = 1$ and so p divides 1. As $p > 1$ this cannot occur. Thus $X_0(p)$ has at least two cusps.

To show $X_0(p)$ has only two cusps, I will show that for any s divisible by p, there exists γ so that $\gamma(\infty) = \frac{r}{s}$ where r, s are coprime. Further if p does not divide s then there exists γ such that $\gamma(0) = \frac{r}{s}$ where r, s are coprime.

For the first, take $a = r$ and $c = s$. Then $\gamma(\infty) = \frac{a}{c} = \frac{r}{s}$.

For the second, take $b = r$ and $d = s$. If p divides d then p divides $ad - bc = 1$. So p cannot divide d thus cannot divide s. □

Theorem 6 (3.1.4 (c))**.** *$\gamma\alpha_j(i) = \alpha_j(i)$ for some $\gamma \in \Gamma_0(p)$ of order 4 if and only if $j^2 + 1 \equiv 0 \pmod{p}$. Thus the number of elliptic points of period 2 in $X_0(p)$ is 2 if $p \equiv 1 \pmod 4$, 0 if $p \equiv 3 \pmod 4$, and 1 if $p = 2$.*

Before I prove this theorem, I need a lemma:

Lemma 7. *The isotropy subgroups of i and μ_3 are*

$$SL_2(\mathbb{Z})_i = \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$$

and

$$SL_2(\mathbb{Z})_{\mu_3} = \langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle.$$

In other words, the only matrices in $\mathrm{SL}_2(\mathbb{Z})$ which fix i are those generated in a group generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and the only matrices in $\mathrm{SL}_2(\mathbb{Z})$ which fix μ_3 are those in a group generated by $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

Proof of 3.1.4.(c). First, $\gamma\alpha_j(i) = \alpha_j(i)$ if and only if $\alpha_j^{-1}\gamma\alpha_j(i) = i$. Computing the matrix $\alpha_j^{-1}\gamma\alpha_j = \begin{pmatrix} bj + a & b \\ -(bj - d)j - aj + c & -bj + d \end{pmatrix}$. However, by the previous lemma,

$$\alpha_j^{-1}\gamma\alpha_j = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Without loss of generality pick

$$\alpha_j^{-1}\gamma\alpha_j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Thus $b = -1$, $a = -d = j$, and $c = j^2 + 1$. As $\gamma \in \Gamma_0(p)$, $p|c$. Thus $j^2 + 1 \equiv 0 \pmod{p}$.

Working backwards, if $p|j^2 + 1$ we can construct a matrix $\gamma \in \Gamma_0(p)$,

$$\gamma = \begin{pmatrix} j & -1 \\ j^2+1 & -j \end{pmatrix}$$

which satisfies $\gamma\alpha_j(i) = \alpha_j(i)$. Thus the theorem holds. □

Theorem 8 (3.1.4 (d))**.** *$\gamma\alpha_j(\mu_3) = \alpha_j(\mu_3)$ for some $\gamma \in \Gamma_0(p)$ of order 6 if and only if $j^2 - j + 1 \equiv 0$ (mod p). Thus the number of elliptic points of period 3 in $X_0(p)$ is the number of solutions of $x^2 - x + 1 \equiv 0$ (mod p). This number is 2 if $p \equiv 1$ (mod 3), 0 if $p \equiv 2$ (mod 3), and 1 if $p = 3$.*

Along with 3.1.4 (c), this shows that the number of elliptic points is determined by $p \pmod{12}$. The following example of $p = 13$ is the smallest case where all four possible elliptic points exist.

Proof. First, $\gamma\alpha_j(\mu_3) = \alpha_j(\mu_3)$ if and only if $\alpha_j^{-1}\gamma\alpha_j(\mu_3) = \mu_3$. As the matrix is $\alpha_j^{-1}\gamma\alpha_j = \begin{pmatrix} bj + a & b \\ -(bj-d)j - aj + c & -bj + d \end{pmatrix}$ and by the previous lemma,

$$\alpha_j^{-1}\gamma\alpha_j = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

we have $b = -1$, $d = 1 - j$, $a = j$, and $c = j^2 - j + 1$. As $p|c$, $j^2 - j + 1 \equiv 0 \pmod{p}$.

Again, moving backwards we can take

$$\gamma = \begin{pmatrix} j & -1 \\ j^2 - j + 1 & 1 - j \end{pmatrix}.$$

Then $\gamma \in \Gamma_0(p)$ and $\gamma\alpha_j(\mu_3) = \alpha_j(\mu_3)$. □

Theorem 9 (3.1.4 (e))**.** *Let g be the genus of $X_0(p)$ and let $k = p + 1$. Show that*

$$g = \begin{cases} \lfloor \frac{k}{12} \rfloor - 1 & \text{if } k \equiv 2 (\text{mod } 12) \\ \lfloor \frac{k}{12} \rfloor & \text{otherwise.} \end{cases}$$

To prove this I need the following well known theorem:

Theorem 10. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. Let $f : X(\Gamma) \to X(1)$ be the natural projection, and let d denote its degree. Let ϵ_2 and ϵ_3 denote the number of elliptic points of period 2 and 3 in $X(\Gamma)$, and ϵ_∞ the number of cusps of $X(\Gamma)$. Then the genus of $X(\Gamma)$ is*

$$g = 1 + \frac{d}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}.$$

Proof of 3.1.4 (e). First take $p \neq 2, 3$. If $p \equiv 3, 9 \pmod{12}$ then $p \equiv 0 \pmod{p}$ so $3|p$. Thus $p \not\equiv 3, 9 \pmod{12}$. The choices left are $p \equiv 1, 5, 7, 11 \pmod{12}$. Notice that the natural projection $X_0(p) \to X(1)$ has degree $p + 1$ and that from a prevoious exercise $\epsilon_\infty = 2$. Going through by cases:

If $p \equiv 1 \pmod{12}$, $k = 2 + 12n$ for some $n \in \mathbb{N}$, $p \equiv 1 \pmod{4}$, and $p \equiv 1 \pmod{3}$. By the previous exercises $\epsilon_2 = 2$ and $\epsilon_3 = 2$, so

$$\begin{aligned} g &= 1 + \frac{p+1}{12} - \frac{2}{4} - \frac{2}{3} - \frac{2}{2} \\ &= \frac{12n-12}{12} \\ &= n-1 \\ &= \lfloor \frac{k}{12} \rfloor - 1. \end{aligned}$$

If $p \equiv 5 \pmod{12}$, $k = 6 + 12n$ for some n, $p \equiv 1 \pmod 4$, and $p \equiv 2 \pmod 3$. So

$$\begin{aligned} g &= 1 + \frac{p+1}{12} - \frac{2}{4} - \frac{0}{3} - \frac{2}{2} \\ &= \frac{12n+6-6}{12} \\ &= \lfloor \frac{k}{12} \rfloor. \end{aligned}$$

Similarly the cases $p \equiv 7, 11 \pmod{12}$ hold.
If $p = 2$, $\epsilon_2 = 1$ and $\epsilon_3 = 0$. Thus

$$\begin{aligned} g &= \frac{3}{12} - \frac{1}{4} \\ &= 0 \\ &= \lfloor \frac{3}{12} \rfloor. \end{aligned}$$

If $p = 3$, $\epsilon_2 = 0$ and $\epsilon_3 = 1$. So

$$\begin{aligned} g &= \frac{4}{12} - \frac{1}{3} \\ &= 0 \\ &= \lfloor \frac{4}{12} \rfloor. \end{aligned}$$

Thus all the cases are covered and we have for all p prime

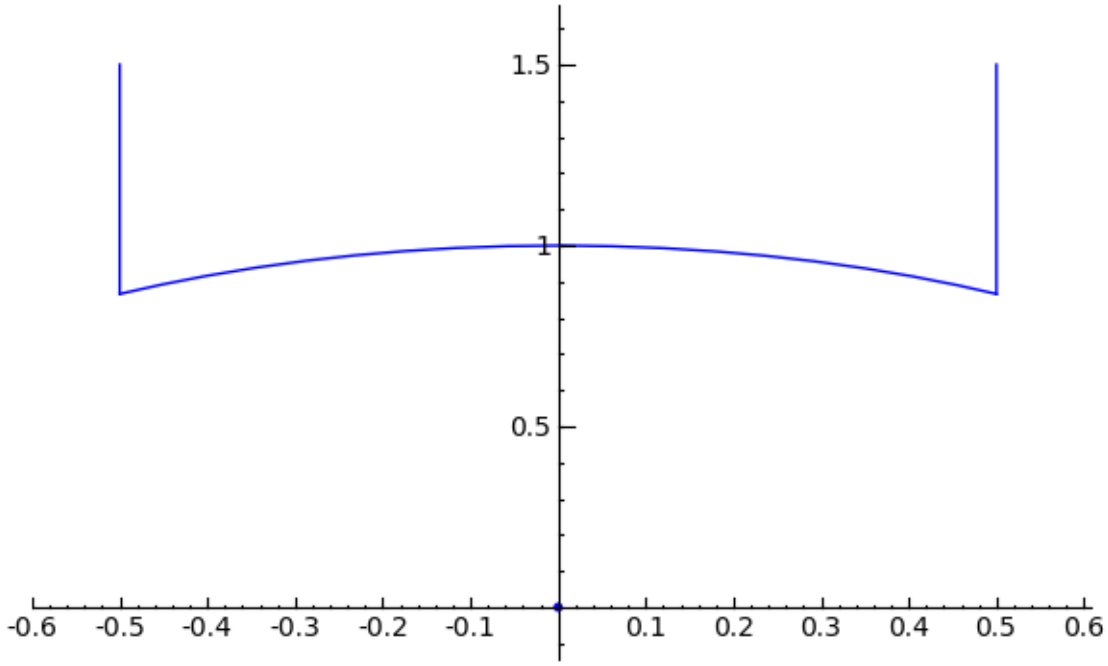
$$g = \begin{cases} \lfloor \frac{k}{12} \rfloor - 1 & \text{if } k \equiv 2 (\text{mod } 12) \\ \lfloor \frac{k}{12} \rfloor & \text{otherwise.} \end{cases}$$

□

The rest of this exercise (3.1.4 (f)) focuses on using the previous exercises to construct the orbits of $\Gamma_0(p)$ for a few primes p, and further to show how the edges glue together to create the associated tori with g holes.

2 Example $p = 13$

Take $\alpha_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\beta_j = \alpha_j\alpha_i$ for $j = -6, ..., 6$ and $\beta_\infty = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\alpha_\infty\alpha_i$. Additionally let $\mathcal{D}$ be the fundamental domain, i.e. $\mathcal{D} = \{z \in \mathbb{C} : \frac{-1}{2} \leq \mathrm{Re}(z)\frac{1}{2} \text{ and } |z| \geq 1\}$.



I will show that the coset representatives $\{\beta_j\}$ and β_∞ generate the orbits of $\Gamma_0(13)$. The code which generates these images ($\beta_j(\mathcal{D})$ for $j = -6, ..., 6$) can be found at the end of the paper.

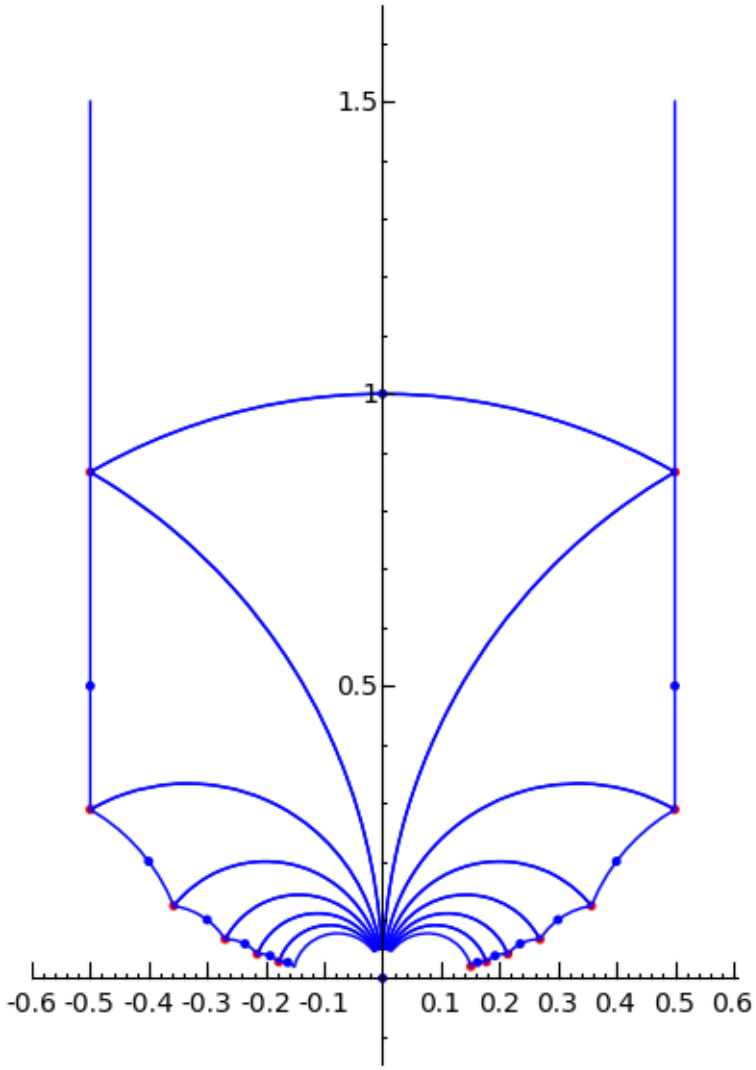
Showing the coset representatives $\{\beta_j\}$ for $j = -6, ..., 6$ generate the orbits of $\Gamma_0(13)$ amounts to finding what the region $\mathcal{D}$ is mapped to via each linear fractional transformation β_j. As each β_j is an linear fractional transformation, it maps circles to circles (where a line is just a circle through infinity) and discs to discs. So it is enough to check where each β_j sends the arcs $\{z = x + iy : x = 1/2, \sqrt{3}/2 \leq y\}$, $\{z = x + iy : x = -1/2, \sqrt{3}/2 \leq y\}$, and $\{z = e^{i\theta} : \pi/3 \leq \theta \leq 2\pi/3\}$. We have $\beta_j(z) = \frac{-1}{z-j}$, so

$$\beta_j(\pm\frac{1}{2} + iy) = \frac{(j \mp 1/2) + iy}{(j \mp 1/2)^2 + y^2}$$

for $0 \leq y \leq \infty$. The unit circle is mapped to

$$\beta_j(e^{i\theta}) = \frac{j - \cos(\theta) + i\sin(\theta)}{(\cos(\theta) - j)^2 + \sin^2\theta}.$$

By examining these for individual j's, $j = -6, ..., 6$, we can compute the end points of the curves. These are $\beta_j(\pm 1/2 + i\sqrt{3}/2)$ and $\beta_j(\infty) = 0$ (for $j = -6, ..., 6$). From this we see we get the desired orbits. Additionally, this shows the 13 points of $\mathrm{SL}_2(\mathbb{Z})(i)$ are $\beta_j(i)$ for $j = -6, ..., 6$, and the 14 points of $\mathrm{SL}_2(\mathbb{Z})(\mu_3) = \mathrm{SL}_2(\mathbb{Z})(\mu_6)$ are $\beta_j(\mu_6)$ for $j = -6, ..., 7$. In the following image, the blue points are the $\beta_j(i)$ and the red points are the $\beta_j(\mu_6)$. Attached is the sage code which graphs these orbits for given j and the points $\beta_j(i)$ and $\beta_j(\mu_6)$.



Now that we have the orbits, we will examine the elliptic points and cusps so that we can glue the orbits together.

We have seen that the map α_i fixes i, thus from 3.1.4 (c) the elliptic points of order 2 in $\Gamma_0(13)$ are $\beta_j(i)$ when $j^2 + 1 \equiv 0 \pmod{13}$, so when $j = 5, 8$. Thus the elliptic points of order 2 are $\frac{i+5}{26}$ and $\frac{i+8}{65}$.

Lemma 11. *$\gamma\beta_j(i) = \beta_{j'}(i)$ for some $\gamma \in \Gamma_0(p)$ of order 4 if and only if $jj' + 1 \equiv 0$ (mod p).*

This lemma will be used to partition the 13 points of $\mathrm{SL}_2(\mathbb{Z})(i)$ into eight equivalence classes under $\Gamma_0(13)$; five with two points each where the angle is π, giving a total of 2π; one with a point where the angle is 2π; and two with one point where the angle is π as it is at i in $\mathcal{D}$, representing the unramified points.

Proof of Lemma. Noticing that $\gamma\beta_j(i) = \beta_{j'}(i)$ if and only if $\beta_{j'}^{-1}\gamma\beta_j(i) = i$, we again have $\beta_{j'}^{-1}\gamma\beta_j = \alpha_i$. The rest of the proof follows identically to 3.1.4 (c). □

Now to partition the 13 points of $\mathrm{SL}_2(\mathbb{Z})(i)$, we see that the pairs $\{j, j'\}$ so that $jj' + 1 \equiv 0 \pmod{13}$ are $\{1, -1)\}, \{2, 6\}, \{3, 4\}, \{-2, -6\}, \{-4, -3\}, \{5\}, \{-5\}$ giving 7 equivalence classes and that leave 0 in its separate equivalence class $\{0\}$. Thus we can identify the boundary arcs pairwise, i.e. for j and j', $j \neq j'$ so that $jj' + 1 \equiv 0 \pmod{13}$, except for the two arcs that fold in on themselves $j^2 + 1 \equiv 0 \pmod{13}$.

Now moving on to elliptic points of order 3, note that $\mathrm{SL}_2(\mathbb{Z})(\mu_3) = \mathrm{SL}_2(\mathbb{Z})(\mu_6)$. Since α_i takes μ_6 to μ_3, the ellitpic points of order 3 are $\beta_j(\mu_6)$ when $j^2 - j + 1 \equiv 0 \pmod{13}$. We have $j^2 - j + 1 \equiv 0 \pmod{13}$ when $j = 4, 10$. So the elliptic points of order 3 are

$$\beta_4(\mu_6) = (1266)3i + 23266\left(\frac{1}{266}\right)\sqrt{3}i + \frac{23}{266}$$

and

$$\beta_{10}(\mu + 6) = (1266I)3 + 23266\left(\frac{1}{266}I\right)\sqrt{3} + \frac{23}{266}.$$

Lemma 12. *$\gamma\beta_j(\mu_6) = \beta_{j'}(\mu_6)$ for some $\gamma \in \Gamma_0(p)$ of order 3 or 6 if and only if $j^2 - j + 1 \equiv 0$ (mod 13) or $jj' - j' + 1 \equiv 0$ (mod p).*

Proof. This proof follows exactly as the similar proofs before. □

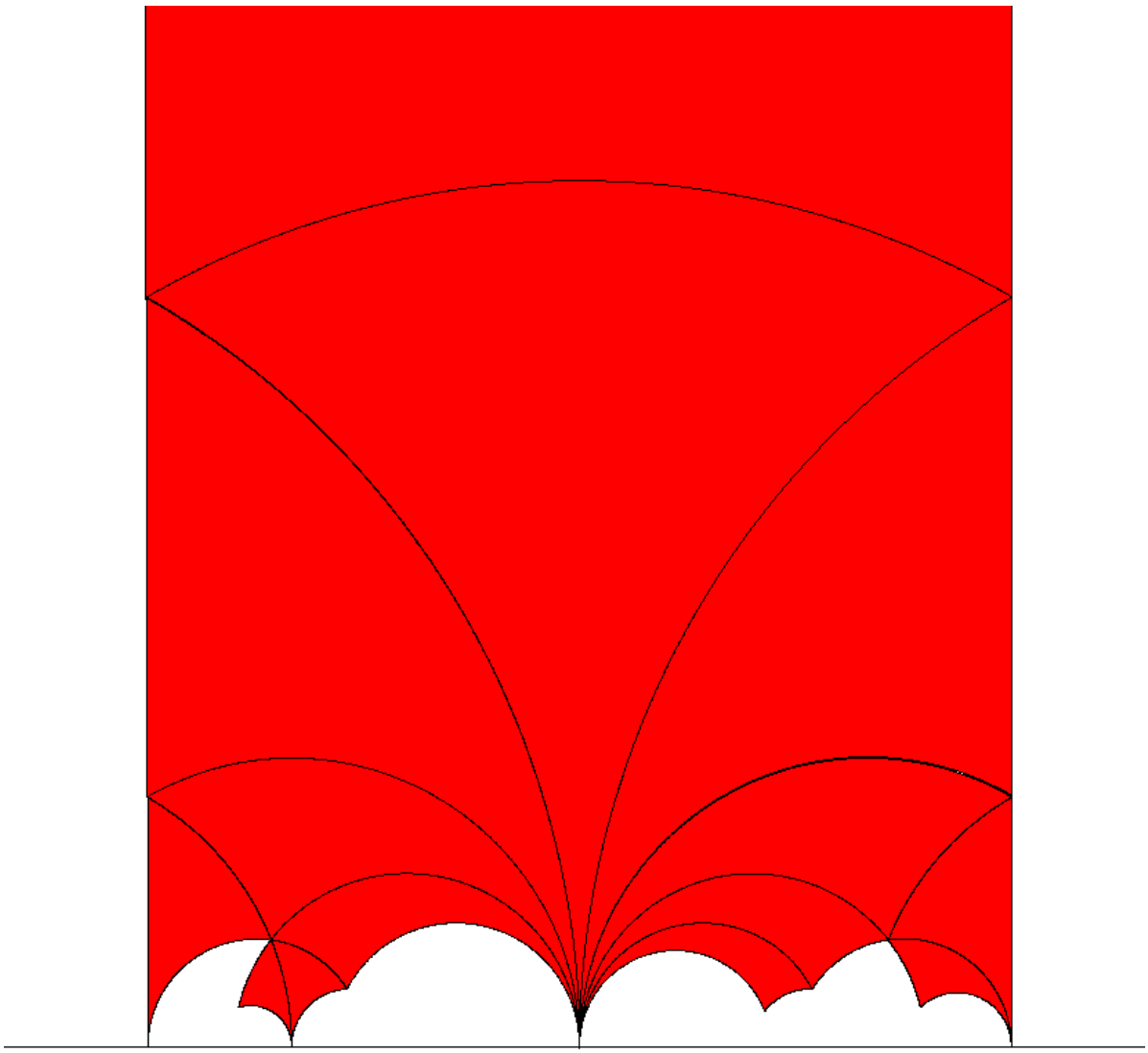
Using this to partition the 14 points of $\mathrm{SL}_2(\mathbb{Z})(\mu_3)$ in the figure into six equivalence classes under $\Gamma_0(13)$, we get one equivalence class $\{-6, -1, 2, 7\}$ with the four points where two of the angles are $2\pi/3$ and two of the angles are $\pi/3$, giving a total of 2π; two with three points where the angle is $2\pi/3$, $\{-2, -4, -5\}$ and $\{3, 5, 6\}$, again giving 2π; one with the two pints where the angle is π, $\{0, 1\}$ giving 2π; and two classes with one point each, $\{-3\}$ and $\{4\}$, where the angle is $2\pi/3$ as it is at μ_3 in $\mathcal{D}$, representing the unrammified points.

From the information we have gathered we can now determine how to glue the edges together to create a sphere (as $g = 0$ we know this will be a sphere). The boundary arcs with elliptic points of order 2 fold together at the elliptic point. Similarly the boundary arcs joined at an elliptic point of order 3 fold together at those elliptic points. This is because the elliptic points there is a $\gamma \in \Gamma_0(13)$ such that they are fixed, i.e. they get sent to themselves. This is exactly what has happened to the $\beta_j(i)$ or $\beta_j(\mu_6)$ when we see that for j so that they are in their own equivalence class (under either $jj' + 1$ or $jj' - j' + 1 \equiv 0 \pmod{13}$ respectively).

Using the other equivalence relations we find how to glue the rest of the boundary arcs. We then identify the two remaining curved boundary arcs in the left half which don't include the cusp 0 with each other and similarly we identify the equivalent boundary arcs in the right half. Via the linear fractional transformation which sends $z \mapsto z + 1$ the vertical segments of the left identify with the vertical segments of the right. The two remaining boundary arcs are thus identified with eachother as well. Via this gluing we arrive at a sphere.

This same process of finding the elliptic points of order 2 and 3, using the coset represenatatives of β_j for $j = -(p-1), ..., p-1$, and then computing the two sets of cosets, can be used to find the orbits of $\Gamma_0(p)$ for any p prime and to further find how to glue the edges to gether to get a g-holed torus. The code for the primes $p = 11$ and $p = 17$, to show $X_0(p)$ is a torus in these cases, is attached.

To see the orbits of the fundamental domain computed for general $N \in \mathbb{N}$ see H. A. Verrill's webpage: http://www.math.lsu.edu/ verrill/ One quick note on the choice of orbits, they are non-cannonical. How Verrill computes the orbits gives a different map for some of the orbits. Her aim is to compute each orbit so that is has as large an area as possible. Here is her $\Gamma_0(13)$.



References

[1] Fred Diamond, Jerry Shurman. *A First Course in Modular Forms* Graduate Texts in Mathematics **228**. Springer-Verlag 2000.

[2] H. A. Verrill. *fundomain.c*

[3] H. A. Verrill. *http://www.math.lsu.edu/ verrill/*