Finding subgroups of $\mathrm{SL}_2(\mathbb{Z})$ with Arbitrary Genus

Cooper Young

January 8, 2019

Abstract

Given suitable information about a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, one can easily compute its genus. The reverse question is less straightforward; given an arbitrary genus, what can we say about the non-congruence and congruence subgroups which have that genus? Using techniques presented in Kulkarni's paper [9], one can show that there are infinitely many non-congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that have any given genus. Rademacher conjectured that there are only finitely many genus zero congruence subgroups, and indeed Dennin proved a more general result [2] that there are at most finitely many congruence subgroups of any given genus. However, it still remains an open question as to whether or not every genus can be obtained by some congruence subgroup. In this paper, we present an exposition of some results and possible ways to approach the open question.

Contents

1 Introduction

In this paper, we are interested in subgroups of $\mathrm{SL}_2(\mathbb{Z})$, the special linear group consisting of 2-by-2 integer matrices with determinant 1. Recall that the **principal congruence subgroup of level** N in $\mathrm{SL}_2(\mathbb{Z})$ is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

A finite index subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup of level** N if $\Gamma(N) \leq \Gamma$ and N is the smallest integer such that this is true. Otherwise, we call Γ a **non-congruence subgroup**.

Recall that subgroups of $\mathrm{SL}_2(\mathbb{Z})$ act on the complex upper half-plane $\mathfrak{H}$ by the linear fractional transformation $\gamma\tau \mapsto \frac{a\tau+b}{c\tau+d}$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Furthermore, we can extend this action to the space $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \infty$. Let $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ be a finite index subgroup, then we define a **fundamental domain** D_Γ for Γ to be a hyperbolic polygon in $\mathfrak{H}^*$ such that for every $\tau \in \mathfrak{H}^*$, the interior of D_Γ contains exactly one point from the Γ-orbit of τ. A complex structure can be put on the quotient space $\Gamma\backslash\mathfrak{H}$ to obtain a noncompact Riemann surface which we will denote as $Y(\Gamma)$. We can compactify this space by adding finitely many points corresponding to the cusps of Γ. This space, defined by $\Gamma\backslash\mathfrak{H}^*$, is denoted as $X(\Gamma)$ and is called a **modular curve**. For any finite index subgroup $\Gamma < \Gamma$, we define the **genus** of Γ to be the genus of the space $X(\Gamma)$, and we denote it as $g(\Gamma)$.

There are known formulas for computing the genus of various congruence subgroups, such as $\Gamma(N)$, $\Gamma_0(N)$, and $\Gamma_1(N)$ (see for example [5]). The genus increase with N at different rates for these classes of subgroups, and it increases the slowest for $\Gamma_0(N)$ for small N. One might wonder if the subgroups $\Gamma_0(N)$ attain every genus, but it can be checked using Sage that this is not true; the first few genera that are never attained by subgroups of the form $\Gamma_0(N)$ are $150, 180, 210, 286, 304, 312, 336$. In fact, it was proved in [1] that the set $\{g(\Gamma_0(N))\}_{n\in\mathbb{Z}}$ is a density zero subset of the integers. Now, it is natural to ask what genera do congruence and non-congruence subgroups attain. In the first part of this paper, we will prove that infinitely many non-congruence subgroups attain any given genus. In the second part of this paper, we will explain some approaches towards constructing congruence subgroups of an arbitrary genus.

Given some finite index subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$, we can determine its genus as follows; first, if we pick coset representatives $\{\gamma_i\}_{1\leq i\leq \mu}$ for $\mathrm{SL}_2(\mathbb{Z})/\Gamma$ and let $\mathcal{F}$ be the classical fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$, then

$$D_\Gamma = \bigcup_{i=1}^{\mu} \gamma_i \mathcal{F}$$

is a fundamental domain for Γ. Fundamental polygons are simply hyperbolic polygons on $\mathfrak{H}^*$ with identifications on certain edges, so we can view it as a fundamental polygon for $Y(\Gamma)$. Then we can obtain $X(\Gamma)$ by adding the vertices of this polygon, which correspond directly to the cusps of Γ. Finally, given a fundamental polygon, we can use tools from topology to compute its genus, thereby finding $g(\Gamma)$.

We now have three main objects of interest: the group Γ, the fundamental domains, and the space $X(\Gamma)$. As we explained above, it is easy to get from Γ to the Riemann surface, however, it is harder to work backwards from the space to the group. This is because there are infinitely many fundamental domains for a given finite index subgroup of Γ, and it is difficult to construct a subgroup given only its coset representatives. In the next section, we will introduce a special fundamental domain associated to each Γ which will help us bridge the gap between group and space.

2 Constructing Finite Index Subgroups of Arbitrary Genus

The material here follows the work of Ravi Kulkarni, as in [9].

2.1 Special Polygon

First we will prove the following lemma:

Lemma 2.1: Let $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ be a finite index subgroup and P a hyperbolic polygon such that

(1) If $\tau \in \mathfrak{H}^*$ is in the interior of P and $\gamma \in \Gamma$, then $\gamma\tau \in P$ implies that $\gamma = I$.

(2) For each side e of P, there is a $\gamma \in \Gamma$ that maps e to another side of P in an orientation reversing manner.

Then P is a fundamental domain for Γ.

Proof: Condition (1) implies that to prove P is a fundamental domain, all we have to show is that for every $\tau \in \mathfrak{H}^*$, there is a $\gamma \in \Gamma$ such that $\gamma\tau \in P$. This is equivalent to saying that

$$\mathfrak{H}^* \subseteq \bigcup_{\gamma \in \Gamma'} \gamma P$$

For each $\gamma \in \Gamma$, we will call γP a P-tile, and condition (1) means that these tiles don't overlap, except perhaps on the boundary. Now seeking a contradiction, suppose that there is some subset of $\mathfrak{H}^*$ which is not included in this tiling. Then there is an $\eta \in \Gamma$ such that ηP has an edge e without a P-tile on the other side.

Note that $\eta^{-1}e$ is a side of P, so condition (2) implies that there is another side e' of P and a matrix $\gamma \in \Gamma$ such that γP is adjacent to P and the tiles intersect at the side $\gamma e' = \eta^{-1}e$. This means that $\eta\gamma P$ is a P-tile which is adjacent to ηP and lies across the side e. However, this is a contradiction, so we conclude our claim.

□

To help keep track of all the definitions introduced in this section, we will use the Dedekind Tessellation, which first appeared in print in [7]. The tessellation is formed by taking the standard tessellation formed by the action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathfrak{H}$ and including the identification $\tau \sim -(\bar{\tau})$. Visually, each region in the standard tessellation (coming from the action of $\mathrm{SL}_2(\mathbb{Z})$) is divided into two halves, one white and one black [see Figure 1].

We define an **even vertex** to be a point where two black and two white regions meet (such as i), and we define an **odd vertex** to be a point where three black and three white regions meet (such as $\rho = e^{\pi i/3}$). Given any two points $x, y \in \mathfrak{H}^*$, there is a unique circle passing through both points and has a center on $\mathbb{Q}$. The arc of this circle contained in $\mathfrak{H}^*$ which connects x and y is called a **hyperbolic arc**.

We define an **even edge** as a hyperbolic arc connecting a cusp to an even vertex (equivalently these are the $\mathrm{PSL}_2(\mathbb{Z})$ orbits of the hyperbolic arc joining i and ∞). We define an **odd edge** as a hyperbolic arc connecting a cusp to an odd vertex (equivalently, the $\mathrm{PSL}_2(\mathbb{Z})$ orbits of the hyperbolic arc joining ρ and ∞). We define an **f-edge** as a line segment connecting an odd vertex to an even vertex (equivalently, the $\mathrm{PSL}_2(\mathbb{Z})$ orbits of the hyperbolic arc joining ρ and i).

Notice that for an odd edge, there is a unique odd edge which meets its odd vertex at an initial angle of $\frac{2\pi}{3}$. We call this pair of odd edges an **odd side**. Also notice that for each even edge, there is a unique even edge with which it forms a hyperbolic arc between elements of the cusps. We call this pair of even edges an **even side** or a **free side** depending on the side-pairing identification given to it (which will be explained immediately bellow).

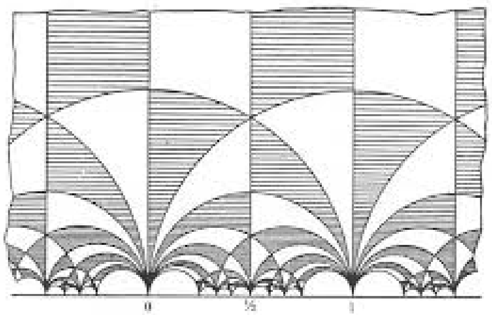

Figure 1: Dedekind Tessellation

We are now ready to define a key object of our study. A **special polygon** P is a hyperbolic polygon made of odd sides, even sides, and free sides, with certain side-pairing identifications:

(1) Each pair of odd edges which form an odd side are identified to each other in an orientation-reversing manner.

(2) For each pair free edges, we either:

- Identify the two free edges together in an orientation-reversing manner, and we call it an even pairing
- Don't identify identify the two free edges, call it a free pairing, and identify the pair to another free pairing in an orientation-reversing manner.

Note that the last condition implies that we must have an even number of free pairs. Furthermore, we require that 0 and ∞ are among the vertices of P.

Consider the example shown below in Figure 2, where the boundary of a special polygon P' is drawn in bold and the sides are identified (with orientation) by the number and direction of the arrows. The far left-hand side shows an example of a free pairing formed by the even edge from 0 to i and the even edge from i to ∞. This free pairing is identified with the free pairing formed by the even edge from ∞ to $i+2$ and the even edge from $i+2$ to 2. In the bottom left of the special polygon is an example of an odd side. Finally, the arc from $\frac{2}{3}$ to 1 is an example of an even pairing, because unlike the other pairs of even edges, we have chosen to identify the two edges together.

Given two pairings on the boundary of a special polygon P which are identified, there is a unique $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ that maps one to the other in an orientation-reversing manner. We call γ the **side pairing transformation** associated to this pairing and denote Γ_P the group generated by all the side pairings transformations of P. Because of Lemma 2.1, it seems likely that if we pick the right finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, that special polygons are actually fundamental domains for that subgroup. In fact, we have the following two theorems due to Kulkarni:

Theorem 2.1 ([9] 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. That is, the only relations on the γ_i's are $\gamma_i^2 = 1$ or $\gamma_i^3 = 1$ for the finite-order γ_i's.

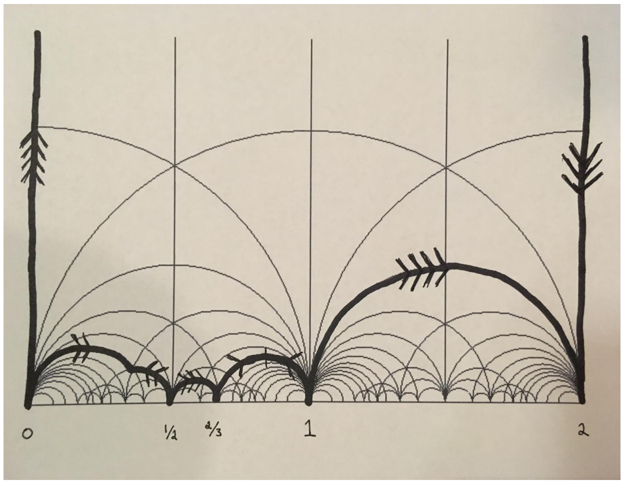

Figure 2: Example of Special Polygon, P'

Theorem 2.2 ([9] Theorem 3.3): For every $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ of finite index, there is a special polygon P such that $\Gamma = \Gamma_P$.

Note that for any fundamental domain of a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, the subgroup is generated by the transformations that map identified sides on the fundamental domain together. However, special polygons have the interesting characteristic that these generators form an independent set.

Let's return to our example above. By Theorem 2.1, we get that that P' is the fundamental domain for the finite index subgroup $\Gamma_{P'}$. If we take this fundamental domain and add one point corresponding to the cusp of $\Gamma_{P'}$ we get the fundamental polygon in Figure 3, which represents $X(\Gamma_{P'})$.

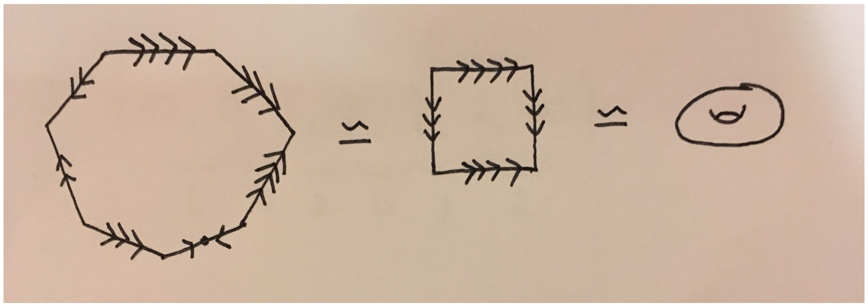

Figure 3: Fundamental Polygon for $X(\Gamma_{P'})$

From this, we see that the genus of $\Gamma_{P'}$ is equal to 1.

We have now seen the usefulness of special polygons, so it makes sense for us to get a better understanding of their components and what information they hold. To do so, we will introduce the notion of a farey symbol.

2.2 Farey Symbols

Recall that a Farey sequence (of order n) is a sequence of reduced fractions between 0 and 1 whose denominators are less than or equal to n, arranged in order of increasing size. One fundamental fact of Farey sequences is that if $\frac{a}{b}$ and $\frac{c}{d}$ are next to each other in a sequence, then $bc - ad = 1$.

With this condition in mind, we define a **generalized Farey sequence** to be a finite sequence $\left\{\frac{-1}{0}, x_0, \ldots, x_n, \frac{1}{0}\right\}$ where each $x_i = \frac{a_i}{b_i}$ is a reduced fraction with $b_i > 0$, and if we set $x_{-1} = \frac{-1}{0}$ and $x_{n+1} = \frac{1}{0}$, then

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

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

Lemma 2.2 ([9] Proposition 2.2): Two cusps $\frac{x}{y}$ and $\frac{n}{m}$ are connected by an even side or free side if and only if $|xm - ny| = 1$.

We now define a **Farey symbol** as a generalized Farey sequence which contains additional information related to side-pairing identification; between each adjacent numbers x_i, and x_{i+1}, we assign the symbol "$\circ$" for an even pairing, or the symbol "$\bullet$" for an odd pairing, or a positive integer p_i for a free pairing. Furthermore, each integer that appears as a free pairing appears exactly twice in the Farey symbol.

If P is a special polygon, let $x_0, \ldots, x_n$ be its vertices lying in $\mathbb{Q}$ listed in ascending order. By Lemma 2.2, we know that $a_{i+1}b_i - a_i b_{i+1} = 1$, which makes $\left\{\frac{-1}{0}, x_0, \ldots, x_n, \frac{1}{0}\right\}$ a generalized Farey sequence. Finally, we can include the side-pairing information to represent our special polygon as a Farey symbol.

On the other hand, if F is a Farey symbol, we can construct a unique special polygon for F. First, let the entries of F be the vertices of our special polygon. If two adjacent entries, x_i and x_{i+1}, form a free pairing or an even pairing, we let P have as a side the hyperbolic arc joining the two cusps. If the entries form an odd pairing, then let $\gamma \in \overline{\Gamma}$ be the unique element such that $\gamma(0) = x_i$ and $\gamma(\infty) = x_{i+1}$. Then if $H_{0,\rho}$ is the hyperbolic arc from 0 to ρ, and $H_{\rho,\infty}$ is the hyperbolic arc from ρ to ∞, then we let P have as a side the union of $\rho(H_{0,\rho})$ and $\rho(H_{\rho,\infty})$.

From this, it is evident that we have a bijection between Farey symbols and special polygons. Furthermore, the map from special polygons to the finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which they represent is surjective and finite-to-one, which induces the same map from Farey symbols to subgroups.

To solidify our understanding of Farey symbols, let's return to our running example. If we look at Figure 2, we see that Lemma 2.2 holds true for the vertices of our special polygon P'. Therefore, we have the generalized Farey sequence $\{\infty, 0, \frac{1}{2}, \frac{2}{3}, 1, 2, \infty\}$ which we can turn into a Farey symbol by adding the side pairing identification shown in Figure 4.

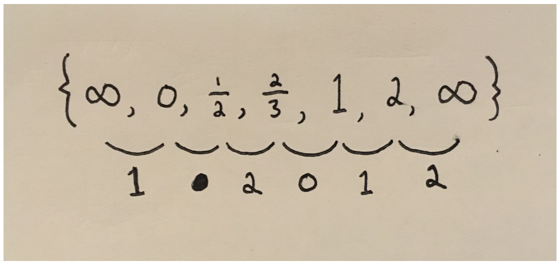

Figure 4: Farey symbol for P'

2.3 Constructing Explicit Subgroups

There are a number of properties and group invariants that can be obtained from analyzing special polygons and their corresponding Farey symbol. For one thing, it was proved by Kulkarni that

Theorem 2.3 ([9] Theorem 6.1): Suppose $\frac{a_i}{b_i}, \frac{a_{i+1}}{b_{i+1}}$ are two adjacent entries in a Farey symbol. If they form an even pairing, let

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

If they form an odd pairing, let

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

and if they form a free pairing and are identified with the side between $\frac{a_k}{b_k}$ and $\frac{a_{k+1}}{b_{k+1}}$, let

$$G_{i+1} = \begin{pmatrix} a_{k+1}b_{i+1} + a_kb_i & -a_ka_i - a_{k+1}a_{i+1} \\ b_kb_i + b_{k+1}b_{i+1} & -a_{i+1}b_{k+1} - a_ib_k \end{pmatrix}$$

Then G_{i+1} is the side transformation corresponding to the pairing of $\frac{a_i}{b_i}$ and $\frac{a_{i+1}}{b_{i+1}}$.

Using this theorem, we can compute G_{i+1} for $-1 \leq i \leq n$ and get a complete set of independent generators for the finite index subgroup which our Farey symbol represents.

Suppose we know the Farey symbol and special polygon for some finite index subgroup Γ. Then the number of order-2 elliptic points, e_2, is the number of even pairings, and the number of order-3 points, e_3, is the number of odd pairings. Also, looking at the orientation of the identified sides, we can easily compute the genus g as well as the number of cusps, t. If we let $[SL_2(\mathbb{Z}) : \Gamma] = \mu$, then we can use Proposition 1.40 in [15] to conclude that

$$\mu = 3e_2 + 4e_3 + 12g + 6t - 12$$

which means we can find the index of a subgroup given its special polygon. These are all attainable pieces of information since there are effective algorithms for computing the special polygon and Farey symbol for a given finite index subgroup (see [8] Section 5).

Proposition 2.1: There are infinitely many finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that have any given genus.

Proof: First note that we can find infinitely many generalized Farey sequences that end with an integer or a half integer and are longer than n terms, for any $n \in \mathbb{Z}$ (take for instance the classical Farey sequences). Now fix some genus g, and consider an infinite list of generalized Farey sequences that each have more than $4g$ terms. For each Farey sequence, we can turn it into a Farey symbol by including $2g$ free pairings and N even pairings (where N is the in length of the Farey sequence minus $4g$) with the orientations given in Figure 5. This results in the special polygon in Figure 5, where the orientations are given by arrows and side-pairing identifications are given by letters.

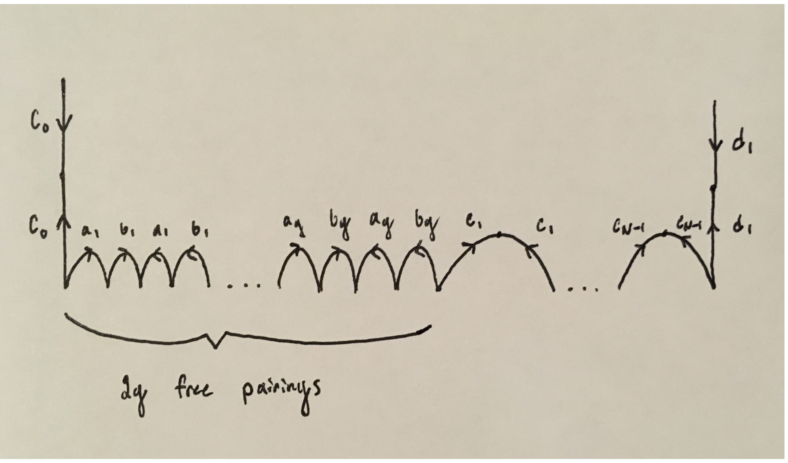

Figure 5: Special Polygon for a finite index subgroup with genus g

As it can be seen, this special polygon represents a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with genus g. Furthermore, it has either N even pairings and 1 odd pairing or $N+1$ even pairings, depending on if the Farey sequence ends in an integer or half integer. In this "proof by picture," we could have replaced the even pairings with odd pairings if we deemed fit. What's important to note is that we can keep adding 2-torsion or 3-torsion elements to create infinitely many finite index subgroups with genus g.

□

Theorem 2.4: There are infinitely many non-congruence subgroups of Γ that have any given genus.

Proof: This follows directly from Proposition 2.1 and the result proved in [2] that there are only finitely many congruence subgroups of Γ that have some fixed genus.

□

Proposition 2.1 and Theorem 2.4 are not novel results, but they were originally proved using different techniques than those introduced in Kulkarni's paper. Now that we have these results, we are left with the open question; given any genus, can we always find a *congruence* subgroup with that genus?

3 The Case of Congruence Subgroups

Suppose we wanted to use the method from Section 2 to construct congruence subgroups with arbitrary genus. A possible technique could come from finding a connection between subgourps $\Gamma' < \Gamma < \mathrm{SL}_2(\mathbb{Z})$ and the corresponding special polygons. That is, there is likely some relation between the special polygon for Γ' and the special polygon for Γ (relating the independent generators of the groups). If this connection is a strong enough, there may be a way to tell if a finite index subgroup is a congruence subgroup by comparing its special polygon to the special polygons for $\Gamma(N)$ as N ranges.

Another approach would be to use the explicit formulas in Theorem 2.3 to get a set of generators for a finite index subgroup Γ (which are independent by Theorem 2.1). Then we may write the group presentation for Γ in terms of the matrices $L = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $R = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, since these elements generate $\mathrm{SL}_2(\mathbb{Z})$. Finally, we can represent the subgroup as a transitive permutation group (see for example [4] or [8] section 4) and apply Theorem 2.4 in [4] to check if it is a congruence subgroup or not.

Yet another approach is to use the genus equation

$$g = \frac{\mu}{12} - \frac{e_2}{4} - \frac{e_3}{3} - \frac{t}{2} + 1 \tag{1}$$

for finite index subgroups $\Gamma < \mathrm{SL}_2(\mathbb{Z})$. Instead of computing the genus directly, we can focus on finding subgroups whose group-theoretic properties we can control. This is still difficult since $\mathrm{SL}_2(\mathbb{Z})$ is a group of infinite order, so we will turn our attention towards the corresponding finite groups, $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Recall that we have the following short exact sequence

$$0 \longrightarrow \Gamma(N) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 0$$

and that $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z})/\Gamma(N)$. If we consider some congruence subgroup $\Gamma(N) < \Gamma < \mathrm{SL}_2(\mathbb{Z})$ of level N, then by the third isomorphism theorem, we know that $\Gamma/\Gamma(N) \leq \mathrm{SL}_2(\mathbb{Z})/\Gamma(N)$, and furthermore every subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is of the form $\Gamma/\Gamma(N)$ for some congruence subgroup G of level N.

Also by the third isomorphism theorem, we have that

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = [\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) : \Gamma/\Gamma(N)] = [\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \Gamma/\Gamma(N)]$$

Therefore, we have a one-to-one correspondence between congruence subgroups of level N and the subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. This correspondence is particularly nice because it preserves the index of the subgroups.

In this approach, our game is two-fold; first we want to determine how the properties used in the genus equation (1) of a congruence subgroup Γ relate to group-theoretic properties of the corresponding subgroup $\Gamma/\Gamma(N)$. Second, we want to utilize the subgroup structure of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ to control these group properties and show that we can attain every genus (or determine if there are some genera that are never obtained). No substantial progress has been made using this approach, but for the rest of the paper, we will detail some work and obstacles that arise when trying to tackle the open question in this manner.

3.1 Possible Indices for Subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$

As we showed above, the simplest connection between group properties of congruence subgroups and their corresponding subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is the index. Again, this is because for every $G < \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, there is a congruence subgroup of level N with index equal to $[\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$. Now we can use this connection to try and answer the question, what are the possible indices that congruence subgroups can obtain?

By the Chinese Remainder theorem, if $N = p_1^{n_1} \dots p_s^{n_s}$ is the prime factorization of N, then we have the isomorphism

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{SL}_2\left(\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{n_s}\mathbb{Z}\right) \cong \prod_{i=1}^{s} \mathrm{SL}_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$$

Note that if we find subgroups $G_i < \mathrm{SL}_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$ for each i, then we have

$$\left[\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \prod_{i=1}^{s} G_i\right] = \prod_{i=1}^{s} [\mathrm{SL}_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z}) : G_i] \tag{2}$$

Therefore, we will restrict our attention to finding subgroups of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for primes p. What we would like to be able to do is find a subgroup in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ of index p and then use equation (2) to find construct subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with arbitrary index, thereby proving that congruence subgroups can obtain every index. Unfortunately, we will show that this approach does not work (Theorem 3.1). To see why this is, we will need some propositions to work with.

Let's define $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})/\{\pm I\}$ (where I is the identity matrix), and note that for every $0 < r < n$, there is a homomorphism

$$f_r^n : \mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/p^r\mathbb{Z})$$

defined by reduction modulo p^r, which is known to be surjective. We will define $K_r^n := \ker(f_r^n)$, which is a normal subgroup of $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$, and is known to have order $|K_r^n| = p^{3(n-r)}$. We have the following Proposition due to McQuillan:

Proposition 3.1 ([13] Proposition 4): The set $\{K_r^n\}_{r=1}^{n-1}$ gives all proper normal subgroups of $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ when $p > 3$.

Proof: See [13] for a proof.

□

Now let G be an arbitrary group, and let G^p be the group generated by the pth powers of all elements in G. That is, consider the subgroup $G^p := \langle g^p \,|\, g \in G \rangle < G$. Note that for any $g \in G$ and $h^p \in G^p$, we have $gh^pg^{-1} = \underbrace{(ghg^{-1})\dots(ghg^{-1})}_{p \text{ times}} = (ghg^{-1})^p \in G^p$. This implies that for all $g \in G$, we get $gG^pg^{-1} \subseteq G^p$, which means that $G^p \triangleleft G$ is a normal subgroup.

Proposition 3.2 ([14] Theorem 10): For a finite group G, the groups G and G/G^p have the same number of subgroups with index p.

Proof: The proof can be found in [14], but it is short enough to write here. Suppose that $H < G$ is a subgroup with index p. This means that $|G/H| = p$, so for any $g \in G$, Lagrange's Theorem implies that $g^pH = (gH)^p = H$. In particular, we have the chain of subgroups $G^p < H < G$.

The third isomorphism theorem then states that $H/G^p < G/G^p$ and that $[G/G^p : H/G^p] = [G : H] = p$. Furthermore, every subgroup of G/G^p with index p must be of the form H/G^p, for some subgroup H of G with index p.

What we've shown so far is that the map from $H \mapsto H/G^p$ sends index p subgroups to index p subgroups and is surjective. To show that it is injective, suppose that $H/G^p = K/G^p$ and consider any $h \in H$. As cosets, we have $hG^p = kG^p$ for some $k \in K$, which implies that $h = kg$ for some $g \in G^p < K$. However, this implies that $h \in K$, and so $H \subset K$. Similarly, we can go the other way and conclude that $H = K$.

□

We will now use Proposition 3.2 to prove a statement that will be used throughout the rest of this paper.

Proposition 3.3 ([14] Proposition 20): A finite group G has a subgroup of index p if and only if $G \neq G^p$.

Proof: The proof can be found in [14], but it is short enough to write here. Going one way, we will prove the contrapositive; if $G = G^p$, then G/G^p is the trivial group, which has no subgroups of index p. Therefore by Proposition 1.2, we know that G cannot have a subgroup of index p.

Going the other way, suppose that $G \neq G^p$, which implies that G/G^p is not the trivial group. If we pick any nonidentity element $xG^p \in G/G^p$, then we know that $(xG^p)^p = x^pG^p = G^p$. Therefore, every nonidentity element in G/G^p has order p, so we must have $|G/G^p| = p^k$ for some integer k. Since G/G^p is a p-group, it must have a subgroup $H < G/G^p$ such that $|H| = p^{k-1}$. This means that $[G/G^p : H] = p$, so by Proposition 1.2, the group G must have a subgroup of index p.

□

Now we are ready to show why we cannot take the naive approach of constructing subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with arbitrary index.

Theorem 3.1: For any prime $p > 3$ and any positive integer n, there is no subgroup of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ which has prime index $q > 3$.

Proof: First we will show that the we can work with the group $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ instead of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$; seeking a contradiction, suppose there is a subgroup $G < \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ with index q, which means the order is equal to $|G| = \frac{p^{3n-2}}{q}(p+1)(p-1)$. Suppose that $-I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \notin G$; then since $\{\pm I\} \triangleleft \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is a normal subgroup, the product $G\{\pm I\} := \big\{ g\alpha \,|\, g \in G,\ \alpha \in \{\pm I\} \big\}$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Furthermore, it is known that

$$|G\{\pm I\}| = \frac{|G| \times |\{\pm I\}|}{|G \cap \{\pm I\}|} = 2\frac{p^{3n-2}}{q}(p+1)(p-1)$$

We know that $|\,\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})| = p^{3n-2}(p+1)(p-1)$, so Lagrange's theorem implies that $2|q$, which is impossible since $q > 3$ is prime.

From what we've shown above, we must have $-I \in G$, so there is an inclusion of subgroups $\{\pm I\} < G < \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Note that $\{\pm I\} \triangleleft \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is a normal subgroup, so we can evoke the third isomorphism theorem. Thus, we get $G/\{\pm I\} < \mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and

$$q = [\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) : G] = [\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})/\{\pm I\} : G/\{\pm I\}] = [\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z}) : G/\{\pm I\}]$$

Furthermore, the third isomorphism theorem states that any subgroup of $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ must be of the form $G/\{\pm I\}$, so there is a subgroup of index q in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ if and only if there is a subgroup of index q in $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

For convenience sake, let's denote $\mathrm{PSL}(2, p^n) = \mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$. We will now proceed on induction by n; first we will prove the result for the case when $n = 1$. Since $\mathrm{PSL}(2, p)$ is a simple group for $p > 3$, $\mathrm{PSL}(2, p)^q$ being a normal subgroup implies that the subgroup is either trivial or equal to all of $\mathrm{PSL}(2, p)$. To show that the subgroup is not just the trivial group, note that if $p \neq q$, then

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \neq I$$

and if $p = q$, then by Fermat's little theorem

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}^q = \begin{pmatrix} a^p & 0 \\ 0 & (a^{-1})^p \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \neq I$$

for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ not equivalent to ± 1. Either way, we must have $\mathrm{PSL}(2, p)^q = \mathrm{PSL}(2, p)$, which by Proposition 3.3 implies that $\mathrm{PSL}(2, p)$ has no subgroup of index q.

Now for our inductive hypothesis, suppose that our result holds for $\mathrm{PSL}(2, p^k)$ for all $k < n$.

Seeking a contradiction, suppose that there exists a subgroup $G < \mathrm{PSL}(2, p^n)$ with index q. Using Proposition 3.1 and Proposition 3.3, we get that $\mathrm{PSL}(2, p)^q$ is isomorphic to K_l^n for some $1 \leq l \leq n-1$. Let's write $\mathrm{PSL}(2, p^n)^q = K_l^n$, then Proposition 1.2 implies that

$$\mathrm{PSL}(2, p^n)/\,\mathrm{PSL}(2, p^n)^q \cong \mathrm{PSL}(2, p^n)/K_l^n \cong \mathrm{PSL}(2, p^l)$$

has a subgroup of index q. However, this contradicts our inductive hypothesis, so we can conclude our claim.

□

Setting $q = p$ in Theorem 3.1 shows that we can't take the approach of using equation (2) and the Chinese remainder theorem, as we discussed in the beginning of this section. The theorem above does not imply that congruence subgroups cannot attain every index, it just means that we have to modify the way we are constructing them.

3.2 Elliptic Points of Subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$

Given some congruence subgroup $\Gamma(N) < \Gamma < \mathrm{SL}_2(\mathbb{Z})$, the goal of this section is to relate $e_2(\Gamma)$, the number of elliptic points of order 2 in Γ, to some group-property of the corresponding group $\Gamma/\Gamma(N) < \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. At this point it is easier to work with $\mathrm{PSL}_2(\mathbb{Z})$, so we will consider congruence subgroups that contain $\{\pm I\}$ so we can analyze their corresponding subgroups in $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. Recall that in the classical theory, we have a few ways to compute $e_2(\Gamma)$, some geometric and some algebraic (see for example, [3]).

In the geometric sense, e_2 is the number of points on $\mathfrak{H}$ (unique up to the Γ-action) which have an isotropy group of order 2. Alternatively, $e_2(\Gamma)$ is the number of points in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of i which lie the fundamental domain of Γ. On the more algebraic side, it can be shown that e_2 is the number of conjugacy classes of order 2 elements in $\Gamma/\{\pm I\}$. It is known that there is only one conjugacy class of order two elements in $\mathrm{PSL}_2(\mathbb{Z})$, namely the one corresponding to $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, so it therefore suffices to know how this conjugacy class splits in congruence subgroups.

To search for an analagous result with $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we will first take the algebraic approach. Namely, given some $G < \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ corresponding to a congruence subgroup $\Gamma < \mathrm{PSL}_2(\mathbb{Z})$, we conjecture that $e_2(\Gamma)$ is equal to the number of conjugacy classes of order 2 elements in G. If this is true, then there should be just one conjugacy class of order 2 elements in all of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$, corresponding to the similar fact above for $\mathrm{PSL}_2(\mathbb{Z})$.

For the remainder of this section, we will work towards showing that $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ does indeed have one conjugacy class of order 2 elements in most cases. To start, we will prove a lemma which will be of use later.

Lemma 3.1: For any prime $p > 3$ and positive integer n, there is no subgroup of $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ which has index 2.

Proof: For convenience sake, let $G = \mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and G' be the derived group of G. With this notation, we have the chain of subgroups $G' < G^2 \triangleleft G$, since we can write $[x, y] = xyx^{-1}y^{-1} =$

$x^2(x^{-1}y)^2y^{-2}$. Note that G' is also a normal subgroup of G, and that G/G' is abelian.

We can now use the third isomorphism theorem, which shows that

$$(G/G')/(G^2/G') \cong G/G^2$$

is abelian, since the quotient of an abelian group is abelian. However, since $G^2 \triangleleft G$ is a normal subgroup, Proposition 1 tells us that $G^2 = G$ or $G^2 = K_l^n$ for some $1 \leq l \leq n-1$. If $G^2 = K_l^n$, then by definition we get $G/G^2 = \mathrm{PSL}_2(\mathbb{Z}/p^l\mathbb{Z})$, which is not abelian. Therefore the only way to not reach a contradiction is if $G^2 = G$, and therefore Proposition 3.3 implies that G has no subgroup of index 2.

□

We will need one more working proposition before we can start showing a string of promising results. Suppose we fix some Sylow p-subgroup $K < G$ and consider any $g \in G$ with order p. The element g generates a group of order p and therefore is contained in some Sylow p-subgroup of G, and since the Sylow p-subgroups are conjugate, we know that g is conjugate (under conjugation in G) to some element of order p in K. The following proposition slightly generalizes this result in a way that we will soon exploit.

Propostion 3.4: Let G be a finite group with order $|G| = 2^k m$, where m is odd and $k \geq 1$. Let K be a Sylow 2-subgroup, and $H < K$ a subgroup with order 2^{k-1}. If G doesn't contain a subgroup of index 2, then every element of order 2 is conjugate (under conjugation in G) to an element in H.

Proof: Note that we have an action of G on the cosets $\{gH \,|\, g \in G\}$, given by $g_1(g_2H) = (g_1g_2)H$. With this, we can show that a non-identity element $g \in G$ is conjugate to an element in H if and only if g has a fixed point in this action. To see this going one way, suppose we have the fixed point

$$g(g_1H) = (gg_1)H = g_1H$$

then we get $g_1^{-1}gg_1 \in H$. Going the other way, if we started with $g_1^{-1}gg_1 \in H$ then we get that g_1H is a fixed point of g.

Recall that $[G : H] = [G : K][K : H] = 2m = 2n + 2$ for some odd integer n, since m is odd. If we consider any element $g \in G$ of order 2, then its action on the cosets above will be the product of transpositions. Seeking a contradiction, suppose that g is not conjugate to an element in H. Then what we showed above implies that g has no fixed points, and therefore its action is the product of exactly $\frac{1}{2}[G : H] = 2n + 1$ transpositions. This means that under the action above, g is an odd permutation, and it follows that exactly half of the elements in G yield even permutations. However, this means that G has a subgroup of index 2, which contradicts our assumption. Therefore, we can conclude that every element of order 2 must be conjugate to an element in H.

□

Note that Proposition 3.4 holds for the group $G = \mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ by Lemma 3.1, since we have $|G| = \frac{1}{2}p^{3n-2}(p-1)(p+1) = 2^k m$, where $k \geq 2$ and m is some odd integer. Now we can apply the proposition above to a special case:

Theorem 3.2: For any positive integer n and prime $p > 3$ such that $p \equiv 3, 5 \pmod 8$, there is only one conjugacy class of order 2 elements in $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Proof: Let's write $|\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})| = 2^k m$, where m is some odd integer. If $p \equiv 3, 5 \pmod 8$, then we get that $k = 2$. In this case, the 2-subgroup $\{I, S\}$ must lie inside of some Sylow 2-subgroup $K < \mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ that has four elements. From Proposition 3.4, we get that every order 2 element in $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ must be conjugate to an element in $\{I, S\}$, which means that the conjugacy class of S is the only conjugacy class of order 2 elements.

□

To extend the theorem above, we need to know a little bit more about the structure of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. For $p > 3$, the group structure of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ has been thoroughly studied, and it has been shown before (see the exposition [6] of work from [10]) that the subgroups of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ are:

a) Abelian groups of order p
b) Cyclic groups of order d for each $d \Big| \frac{p-1}{2}$ and for each $d \Big| \frac{p+1}{2}$
c) Dihedral groups of order $2d$ for each $d \Big| \frac{p-1}{2}$ and for each $d \Big| \frac{p+1}{2}$
d) Alternating groups A_4 when $p \equiv \pm 1$ or $\pm 3 \pmod 8$
e) Alternating groups A_5 when $p \equiv \pm 1 \pmod{10}$.
f) Symmetric groups S_4 when $p \equiv \pm 1 \pmod 8$.

Theorem 3.3: For any prime $p > 3$, there is only one conjugacy class of order 2 elements in $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$.

Proof: First note that the result can be checked directly for $p = 5$ (see for example the Groupprops Wiki for the element structure of $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$). Therefore, suppose that $p > 5$, and let's write $|\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})| = 2^k m$ for some odd integer m. Then from our list of subgroups above, we get that the Sylow p-subgroups of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ must be dihedral groups of order 2^k, where 2^{k-1} is the highest power of 2 which divides $\frac{p \pm 1}{2}$.

It's known that the subgroups of the dihedral group D_{2d} are either dihedral groups $D_{2d/r}$, (where $r|2d$), or cyclic groups $\mathbb{Z}/(d/r)\mathbb{Z}$, (where $r|d$). Therefore, we can consider the following chain of subgroups

$$\mathbb{Z}/(2^{k-1})\mathbb{Z} < D_{2(2^{k-1})} < \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$$

From Proposition 3.4 and Lemma 3.1, we get that every element in $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ with order two is conjugate to an element in the cyclic group $\mathbb{Z}/(2^{k-1})\mathbb{Z}$. However, there is only one element of order 2 in $\mathbb{Z}/(2^{k-1})\mathbb{Z}$. Therefore, every order two element in $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ must be conjugate, and we can conclude that the conjugacy class of S is the only conjugacy class of order 2 elements.

□

Using Theorem 3.3, we would like to generalize the result to $\mathrm{PSL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for any prime $p > 3$ and positive integer n. If this were true, then the result would hold for $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ for any integer N, which can be seen by using the Chinese reminder theorem and the fact that (g_1, h_1) and (g_2, h_2) are conjugate in the direct product of groups $G \times H$ if and only if g_1 and g_2 are conjugate in G and h_1 and h_2 are conjugate in H. However, as of when this paper was written, I haven't been able to do so.

I believe that the meaning of e_3 in the corresponding subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ will be analogous to the meaning of e_2. However, I'm not sure how the number of cusps of a congruence subgroup corresponds to a group theoretic property of the corresponding finite group. As Section 3 shows, finding how the varibales in the genus equation relate to properties of subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is a tedious manner, and controlling these quantities is another difficulty. Therefore, it might be better to approach this unsolved problem in a different way.

References

[1] Csirik, Janos, et al. *On the Genera of* $X_0(N)$. Preprint, 2000.

[2] Dennin Jr., Joseph B. *The genus of subfields of* $K(n)$, Proc. Amer. Math. Soc. 51 (1975), 282288.

[3] Diamond, Fred and Jerry Shurman. *A First Course in Modular Forms.* Springer, New York, 2005.

[4] Hsu, Tim. *Identifying Congruence Subgroups of the Modular Group.* Proceedings of the American Mathematical Society 124 (1996), no. 5, 13511359.

[5] Hui Hui, Yap. *Genus of Congruence Subgroups of the Modular Group.* Thesis submitted to the department of mathematics, National University of Singapore, 2003.

[6] King, Oliver. *The subgroup structure of finite classical groups in terms of geometric configurations.* Expository paper, 2015.

[7] Klein, Felix. *Uber die Transformation der elliptischen Funktionen und die Auflosung der Gleichungen funften Grades (On the transformation of elliptic functions and ...).* Math. Annalen, 14: 1375 (in Oeuvres, Tome 3), 1878.

[8] Kruth, Chris, and Ling Long. *Computations with Finite Index Subgroups of* $\mathrm{PSL}_2(\mathbb{Z})$ *Using Farey Symbols.* Preprint, 2007.

[9] Kulkarni, Ravi S. *An Arithmetic-Geometric Method in the Study of the Subgroups of the Modular Group.* American Journal of Mathematics, Vol. 113, No. 6. (Dec., 1991), pp. 1053-1133.

[10] L.E. Dickson, Linear groups, with an Exposition of the Galois Field Theory, Teubner, Leipzig, 1901.

[11] Long, Ling. *Finite Index Subgroups of the Modular Group and their Modular Forms.* Survey, 2007.

[12] MacPherson, Robert and Mark McConnell. *Classical Projective Geometry and Modular Varieties.* Algebraic Analysis, Geometry, and Number Theory, ed. J.-I. Igusa, Johns Hopkins U. Press, 1989.

[13] McQuillan, Donald. *Some results on the linear fractional group.* Illinois Journal of Mathematics, Volume 10, Issue 1, 1966.

[14] Pineda, Matthew. *Characterizing the Number of Subgroups of Prime Index.* Thesis submitted to California State Polytechnic University, Pomona, 2014.

[15] Shimura, Goro. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, Princeton, 1971.