Congruence and non-congruence subgroups of $SL_2(\mathbb{Z})$

Marco Forte

School of Mathematics and Statistics

University College Dublin

Undergraduate research project
Supervisor: Dr. Kevin Hutchinson

May 2016

Abstract

The theory of linear groups goes back to the foundation of group theory. Évariste Galois constructed the groups $PSL(2,p)$ were constructed by Évariste Galois in the 1830s, he also constructed the general linear group over a prime field, $GL(n,p)$, in studying the Galois group of the general equation of degree p^n. The existence of non-congruence subgroups was known to Felix Klein who made extensive contribution in the related field of modular forms. This project give's an undergraduate accessible exposition of the theory of congruence and non-congruence subgroups. A goal of the project was to give a more detailed report sized overview of the theory.

Acknowledgements: I would like to thank Dr. Kevin Hutchinson for his excellent mentoring and support over the months of the module. I believe his guidance has enabled to do far more than I thought I was capable of and helped me become a much better mathematics student. I would also like to mention Dr. Keith Conrad for his superb collection of expository papers, especially the one on $SL_2(\mathbb{Z})$ [Conrad] which served as the initial motivation for beginning this project.
I would also like to thank University College Dublin and University of California: Santa Cruz for high quality mathematics education I have been given.

Contents

Chapter 1

Preliminary group theory

The level of this project is aimed at final year undergraduate mathematics students. Knowledge of basic group theory, number theory, complex numbers is assumed. We us some more specialised theory that readers may be unaware of or might need a quick refresh. So this prelimanary chapter contains definitions and results of this kind.

1.1 Group Actions

Definition 1.1.1. A group action of a group G on a set A is the map from $G \times A$ to A (written as $g \cdot a$, for for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot s$ for all $g_1, g_2 \in G, a \in A$,
2. $1 \cdot a = a$, for all $a \in A$

The set A is called a G-set.

We often refer to this as G is a group acting on a set A. The expression $g \cdot a$ will usually be written simply as ga or $g(a)$.

Definition 1.1.2. Let A be a G-set. The *stabilizer* of $a \in A$ is the set,

$$G_a = \{g \in G \,|\, g \cdot a = a\}$$

Proposition 1.1.3. *Let A be a G-set. The relation on A defined by a b if and only if $b = g \cdot a$ for some $g \in G$ is an equivalence relation on A.*

Definition 1.1.4. The equivalence class of $a \in A$ is called the orbit of a.

We using equivalence and orbit we often refer to the group explicitly, we say the points a, b are G-equivalent and a, b in the same G-orbit.

1.2 Isomorphism Theorems

Theorem 1.2.1. *First Isomorphism Theorem Let $\theta : G \to H$ be a group homomorphism. Then*

$$G/ker\theta \cong Im\theta$$

Theorem 1.2.2. *Third Isomorphism / Factor of a factor Theorem Let M, N be normal subgroups of the group G with M contained in N. Then,*

1. *N/M is a normal subgroup of G/M and*
2. *$(G/M)/(N/M) \cong G/N$*

Theorem 1.2.3. *Fourth Isomorphism / Correspondence theorem Let N be a normal subgroup of G, let H be a subgroup of G. The mapping $H \mapsto H/N$ defines a bijection between the set of subgroups of G containing N and the set of subgroups of G/N. Furthermore this correspondence preserves normality.*

1.3 Jordan-Holder Theorem

Definition 1.3.1. Internal / external direct product

A group G is an (internal) direct product $H_1 \times \cdots \times H_n$ of subgroups $H_1, \ldots, H_n$ if

1. $H_i \trianglelefteq G$ for $i = 1, \ldots, n$ and
2. every element $g \in G$ can be uniquely written in the form

   $$g = h_1 \cdots h_n$$

   with $h_i \in H_i$.

The external direct product is defined as the n-tuples $(h_1, \ldots, h_n)$ with $h_i \in H_i$, with multiplication

$$(g_1, \ldots, g_n)(h_1, \ldots h_n) = (g_1h_1, \ldots, g_nh_n)$$

Definition 1.3.2. A **normal series** for a group G is a chain

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$$

of normal subgroups of G.

Definition 1.3.3. A **subnormal series** for a group G is a chain

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$$

of subgroups of G with $G_i \trianglelefteq G_{i+1}$.

Definition 1.3.4. Let

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$$

and

$$H = H_0 \geq H_1 \geq \cdots \geq H_s = \{1\}$$

be two normal (or subnormal series) for G.

(a) Then the second series is a **refinement** of the first if each group which appears in the first series also appears in the second.

(b) The two series are **isomorphic** if there exists a bijection from

$$\{G_0/G_1, G_1/G_2, \ldots, G_{r-1}/G_r\} \to \{H_0/H_1, \ldots, H_{s-1}/H_s\}$$

such that the quotient groups that correspond under the bijection are isomorphic.

Definition 1.3.5. A normal series for a group G with no repeated terms which cannot be refined except by repeating terms is called a **chief** series for G.

Definition 1.3.6. A subnormal series for a group G with no repeated terms which cannot be refined except by repeating terms is called a **composition** series for G.

Theorem 1.3.7. *(Jordan-Holder Theorem). If a group has a chief (or composition) series then any two chief (or composition) series are isomorphic.*

1.4 Free groups

The following exposition on free groups is taken directly from section 6.3 of the book Abstract Algebra [Dummit and Foote, 2004]. Only the relevant informal discussion is included here, there is much more detailed discussion available in the book.

The basic idea of a free group $F(S)$ generated by a set S is that there are no relations satisfied by any of the elements in S (S is "free" of relations). For example, if S is the set $\{a, b\}$ then the elements of the free group on the two generators a and b are of the form $a, aa, ab, abab, bab$, etc., called words in a and b, together with the inverses of these elements, and all these elements are considered distinct. If we group like terms together, then we obtain elements of the familiar form a, b^-3, aba^-1b^2 etc. Such elements are multiplied by concatenating their words (for example, the product of aba and b^-1a^3b would simply be $abab^-1a^3b$). It is natural at the outset (even before we know S is contained in some group) to simply define $F(S)$ to be the set of all words in S, where two such expressions are multiplied in $F(S)$ by concatenating them.

One important property reflecting the fact that there are no relations that must be satisfied by the generators in S is that any map from the set S to a group G can be uniquely extended to a homomorphism from the group $F(S)$ to G (basically since we have specified where the generators must go and the images of all the other elements are uniquely determined by the homomorphism property - the fact that there are no relations to worry about means that we can specify the images of the generators arbitrarily). This is frequently referred to as the universal property of the free group and in fact characterizes the group $F(S)$.

Definition 1.4.1. The group $F(S)$ is called the free group on the set S. A group F is a free group if there is some set S such that $F = F(S)$ - in this case we call S a set of free generators (or a free basis) of F. The cardinality of S is called the rank of the free group.

Definition 1.4.2. Let S be a subset of a group G such that $G = \langle S \rangle$.
A presentation for G is a pair (S, R), where R is a set of words in $F(S)$ such that the normal closure of $\langle R \rangle$ in $F(S)$ (the smallest normal subgroup containing $\langle R \rangle$) equals the kernel of the homomorphism $\pi : F(S) \to G$ (where π extends the identity map from S to S). The elements of S are called generators and those of R are called relations of G.
We say G is **finitely generated** if there is a presentation (S, R) such that S is a finite set, and we say G is finitely presented if there is a presentation (S, R) with both S and R finite sets.

The following comes from Chapter 11 of the book An introduction to the theory of groups [Rotman, 2012].

Definition 1.4.3. The free product $G \star H$ of groups G and H is the set of elements of the form

$$g_1h_1g_2h_2 \cdots g_rh_r,$$

where g_i in G and h_i in H, with g_1 and h_r possibly equal to e, the identity element of G and H.

Definition 1.4.4. Let S be a subset of the group G. A **word** on S is a sequence $w = (s_1, s_2, \ldots)$, where $s_i \in S \cup S^{-1} \cup \{1\}$ for all i, such that all $i = 1$ from some point on. The **length** of $w = s_1^{a_1} \cdots s_n a_n$ is defined to be n.
Since words contain only a finite number of letter before they become constant, we use the more suggestive notation for non-identity words,

$$w = s_1^{a_1} s_2^{a_2} \cdots s_n a_n$$

where $s_i \in S$, $a_i = \pm 1$ or 0, and $a_n = \pm 1$.

Definition 1.4.5. If $w = s_1^{a_1} \cdots s_n a_n$ is a word, then it's **inverse** is the word $w^{-1} = s_1^{-a_1} \cdots s_n - a_n$.

Definition 1.4.6. A word w on S is **reduced** if either w is the identity, or $w = s_1^{a_1} s_2^{a_2} \cdots s_n a_n$, where all $s_i \in S$, all $a_i = \pm 1$, and x and x^{-1} are never adjacent.

Chapter 2

The special linear group $SL_2(\mathbb{Z})$

2.1 Introduction

Definition 2.1.1. The special linear group of degree two over the ring of integers is

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}\, ad - bc = 1 \right\}$$

The set $SL_2(\mathbb{Z})$ forms a group under matrix multiplication since, matrix multiplication is associative, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, it is closed under multiplication since $\det(AB) = \det(A)\det(B) = 1$ for $A, B \in SL_2(\mathbb{Z})$.

The two most important matrices for $SL_2(\mathbb{Z})$ are $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The matrix S has order 4 and $S^2 = -I_2$. For T we have $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for $n \in \mathbb{Z}$, so the matrix T has infinite order. In words, left multiplication by S swaps the rows of a matrix and changes the sign of the new top row. Left multiplication by T adds the bottom row to the top row and leaves the bottom row unchanged.

$$S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \quad T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + cn & b + dn \\ c & d \end{pmatrix}.$$

Theorem 2.1.2. *The group $SL_2(\mathbb{Z})$ is generated by S and T.*

This theorem is central to the study of $SL_2(\mathbb{Z})$, most of the results in this report make use of it. There are two common methods to prove this, one geometric and the other algebraic given in subsection 2.3.1.

2.2 Möbius transformations

In this section we discuss a geometric approach to $SL_2(\mathbb{Z})$, we give a version of the classic geometric proof of Theorem 2.1.2. Some of the exposition on Möbius transformations was derived from University of Manchester hyperbolic geometry course notes [Walkden, 2016]

Definition 2.2.1. The upper half-plane is the set of complex numbers with positive imaginary part:

$$\mathcal{H} := \{z = x + iy \in \mathbb{C} \,:\, y > 0\}$$

Definition 2.2.2. Let $a, b, c, d \in \mathbb{R}$ such that $ad - bc > 0 \in \mathbb{R}$, and define the map

$$\gamma \,:\, \mathcal{H} \to \mathcal{H}$$
$$\gamma(z) = \frac{az + b}{cz + d}$$

The map γ is called a Möbius transformation of $\mathcal{H}$. The set of these Möbius transformations is denoted Möb$(\mathcal{H})$

Remark 2.2.3. Let $\gamma = \frac{az+b}{cz+d} \in$ Möb$(\mathcal{H})$ and let $z \in \mathcal{H}$. Expanding out $\gamma(z)$ we get,

$$\begin{aligned}\gamma z = \frac{az + b}{cz + d} = \frac{ax + aiy + b}{cx + ciy + d} &= \frac{(ax + aiy + b)(cx + d - ciy}{(cx + d)^2 + (cy)^2} \\ = \frac{ac(x^2 + y^2) + x(ad + bc) + bd}{|cz + d|^2} &+ i\frac{y(ad - bc)}{|cz + d|^2}\end{aligned} \tag{2.1}$$

Focusing on the imaginary part in equation 2.1 we see that the image of a Möbius transformation of $\mathcal{H}$ does indeed lie in $\mathcal{H}$,

$$Im(\gamma z) = \frac{Im(z)(ad - bc)}{|cz + d|^2} > 0 \tag{2.2}$$

We can actually go further to say that $\gamma \in$ Möb$(\mathcal{H})$ is a bijective map from $\mathcal{H}$ to itself, we can show this by finding the inverse of γ in Möb$(\mathcal{H})$. Let $g = \frac{dz-b}{-cz+a}$, first we note $da - (-b)(-c) = ad - bc > 0$ so $g \in$ Möb$(\mathcal{H})$. We can show g is a left inverse directly,

$$\begin{aligned}\gamma^{-1}\gamma(z) = \gamma^{-1}(\frac{az + b}{cz + d}) &= \frac{d\frac{az+b}{cz+d} - b}{-c\frac{az+b}{cz+d} + a} \\ &= \frac{\frac{d(az+b)-b(cz+d)}{cz+d}}{\frac{-c(az+b)+a(cz+d)}{cz+d}} = \frac{daz + db - bcz - bd}{-caz - cb + acz + ad} \\ &= \frac{(da - bc)z}{-cb + ad} \\ &= z\end{aligned}$$

By a similar computation we can show g is a right inverse, so we have γ is invertible and,

$$\gamma^{-1}(z) = \frac{dz - b}{-cz + a}. \tag{2.3}$$

For two $\gamma_1, \gamma_2 \in \text{Möb}(\mathcal{H})$ we often use $\gamma_1\gamma_2$ to denote the function composition $\gamma_1 \circ \gamma_2$.

Proposition 2.2.4. *The set Möb($\mathcal{H}$) forms a group under composition.*

Proof. Let $\gamma_1 = \frac{a_1z+b_1}{c_1z+d_1}, \gamma_2 = \frac{a_2z+b_2}{c_2z+d_2} \in \text{Möb}(\mathcal{H})$. The composition $\gamma_1 \circ \gamma_2$ is of the form,

$$\begin{aligned} \gamma_1\gamma_2(z) = \gamma_1(\frac{a_2z+b_2}{c_2z+d_2}) &= \frac{a_1\frac{a_2z+b_2}{c_2z+b_2} + b_1}{c_1\frac{a_2z+b_2}{c_2z+d_2} + d_1} \\ &= \frac{(a_2a_1 + b_1c_2)z + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2)z + (c_1b_2 + d_2d_1)} \end{aligned} \tag{2.4}$$

For this we must compute $(a_2a_1+b_1c_2)(c_1b_2+d_2d_1)-(a_1b_2+b_1d_2)(c_1a_2+d_1c_2)$ and check that it's positive. It factors to $(a_1d_1-b_1d_1)(a_2d_2-b_2c_2)$ and both terms are positive, so $\gamma_1\gamma_2 \in \text{Möb}(\mathcal{H})$.

The operation on Möb($\mathcal{H}$) is associative since function composition is associative.

The identity transformation $Id(z) = z$ is a Möbius transformation, we can write it in explicit form as $Id(z) = \frac{1\cdot z+0}{0\cdot 0+1}$.

In remark 2.2.3 we found an inverse Möbius transformation γ^{-1} for each $\gamma \in \text{Möb}(\mathcal{H})$. □

Example 2.2.5. Examples of Möbius transformation of $\mathcal{H}$ include dilations $z \mapsto kz = \frac{kz+0}{0\cdot z+1}$ for $k > 0$, translations $z \mapsto z + b = \frac{1\cdot z+b}{0\cdot z+1}$ for $b \in \mathbb{R}$, and inversion $z \mapsto -1/z = \frac{0\cdot z-1}{1\cdot z+0}$. Where the values for $ad - bc$ are $k, 1$ and 1 respectively.

Proposition 2.2.6. *Let H be either (i) a semi-circle orthogonal to the real axis, or (ii) a vertical straight line.*
Let γ be a Möbius transformation of $\mathcal{H}$. Then $\gamma(H)$ is either a semi-circle orthogonal to the real axis or a vertical straight line.

Proof. A proof of this can be found in [Walkden, 2016] p.20. □

2.2.1 Group action of $SL_2(\mathbb{Z})$ on the upper half plane

Remark 2.2.7. Notice that if

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

is a Möbius transformation of $\mathcal{H}$, then

$$z \mapsto \frac{\lambda az + \lambda b}{\lambda cz + \lambda d}$$

gives the same Möbius transformation of $\mathcal{H}$ (for $\lambda \neq 0$). Where $(\lambda a)(\lambda d) - (\lambda b)(\lambda c) = \lambda^2(ad - bc)$, thus if we take $\lambda = 1/\sqrt{ad - bc}$ we can always assume that $ad - bc = 1$.

Definition 2.2.8. The Möbius transformation $\gamma(z) = (az + b)/(cz + d)$ of $\mathcal{H}$ is said to be in normalised form if $ad - bc = 1$.

This brings us to the relation between Möbius transformation of $\mathcal{H}$ and the group $SL_2(\mathbb{R})$. If we have $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ then we can associate a normalised Möbius transformation $\gamma_A = \frac{az+b}{cz+d} \in \text{Möb}(\mathcal{H})$.
In particular we can define a map from $SL_2(\mathbb{Z})$ to Möb($\mathcal{H}$),

$$h : SL_2(\mathbb{Z}) \to \text{Möb}(\mathcal{H})$$
$$h(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \frac{az + b}{cz + d}, \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

In particular the image of h is $\{\frac{az+b}{cz+d} \,|\, ad - bc = 1 \text{ where } a, b, c, d \in \mathbb{Z}\}$.
The map h is a homomorphism, let $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in SL_2(\mathbb{Z})$,

$$\begin{aligned} h(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}) &= h(\begin{pmatrix} a_2a_1 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_2d_1 \end{pmatrix}) \\ &= \frac{(a_2a_1 + b_1c_2)z + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2)z + (c_1b_2 + d_2d_1)} \\ &= h(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix})h(\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}) \text{ Using Equation 2.4} \end{aligned}$$

The homomorphism h is certainly not surjective since for example it won't map to any normalised Möbius transformation with non-integer coefficients.
The homomorphism is also not injective, since for example $h(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}) = \frac{-z}{-1} = z = h(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$.
We can show however that $\pm I_2$ are the only matrices in $SL_2(\mathbb{Z})$ that get mapped to the identity, i.e $\ker(h) = \{I_2, -I_2\}$: Suppose we have $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, such that $h(A) = \frac{az+b}{cz+d} = z$.
Then $cz^2 + z(d - a) - b = 0$ for all z. Letting $Z = 0$ we get $c \cdot 0^2 + 0 \cdot (b - a) - b = \implies b = 0$, letting $z = 1$ we get $c \cdot 1^2 + 1 \cdot (d - a) = c + (d - a) = 0 \implies c = a - d$, finally let $z = -1$ and $c \cdot (-1)^2 + (-1) \cdot (d - a) = c + a - d = 0 \implies c = d - a$. Putting this together we have $b = 0$

and $c = a - d = d - a$, therefore $c = b = 0$ and $d = a$. Thus A is of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. The condition on $\det(A) = 1$ implies $a = \pm 1$.

This leads us to the following remark,

Remark 2.2.9. Claim: Let $A, B \in SL_2(\mathbb{Z})$, then $h(A) = h(B) \iff A = B$ or $A = -B$.
Suppose $h(A) = h(B)$ then since h is a homomorphism we get $h(AB^{-1}) = Id$ and so by the above we get $A = \pm B$. For the reverse implication note that for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $h(-A) = \frac{-az-b}{-cz-d} = \frac{az+b}{cz+d} = h(A)$.
In fact it is really the first isomorphism theorem that gives

$$SL_2(\mathbb{Z})/\{\pm I_2\} \cong PSL_2(\mathbb{Z}) \cong Image(h) = \{\frac{az+b}{cz+d} \,|\, ad - bc = 1 \text{ where } a, b, c, d \in \mathbb{Z}\}$$

Remark 2.2.10. The identification of $A, -A \in \Gamma$ as the same transformation also means that orders of transformations may be lower than the order of their corresponding matrix.
Denote the order of x in a group G as $o(x)$, then if $o(A)$ is finite,

$$o(A) = o(h(A)) \text{or} o(A) = 2 \cdot o(h(A)) \text{ also.}$$

Proof of claim, let n be the order of A, let t be order $o(h(A))$.
We have $h(A^n) = h(I_2) = I_2$ and so $h(A)^n = I_2$ hence $t \mid n$. Conversely suppose $h(A)^t = id$, this implies $h(A^t) = Id$, and then $A^t = \pm I_2$ since $\ker(h) = \{\pm I_2\}$. Therefore $n \mid t$ if $A^t = I_2$ or $n \mid 2t$, $n \nmid t$ if $A^t = -I_2$.
So $t \mid n \implies n = kt$ for some t, we also have $n \mid 2t$, so $k = 1$ or $k = 2$. □

A matrix A has infinite order if and only if it's Möbius transformation $h(A)$ also has infinite order. This follows by contradiction from proof above, suppose A had finite order n then $o(h(A)) < n < \infty$. Now suppose $h(A)$ has order t, then $o(A) < 2t < \infty$.
For example, recall the matrices we defined at the beginning of this chapter, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The corresponding Möbius transformation of S is $h(S) = \frac{-1}{z}$ which is the transformation that invert's points through the unit circle in $\mathcal{H}$. The transformation $-1/z$ has order 2 and the matrix S has order 4.
The corresponding Möbius transformation of T is $h(T) = t + 1$. We can observe that $h(T) \circ h(T) = (z + 1) + 1 = z + 2$, and in general $(h(T))^n = z + n$. So the transformation $h(T)$ has infinite order since $z + n \neq z$ for $z > 0$, we've also already seen that the matrix T has infinite order.

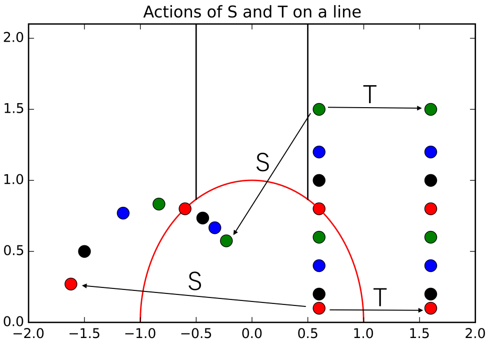
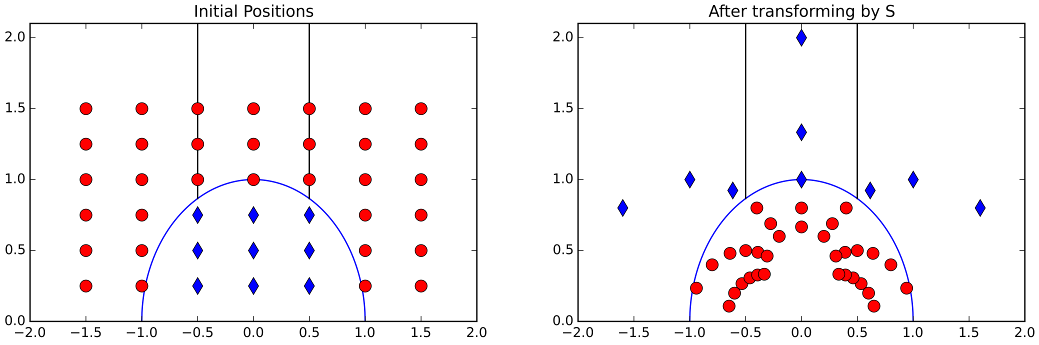


Figure 2.1: Example: action of S and T



(a) Before

(b) After action by S

Figure 2.2: Example: Action on grid of points

We can define a group action of $SL_2(\mathbb{Z})$ on the upper half plane $\mathcal{H}$ through Möbius transformations.
Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and let $z \in \mathcal{H}$, we define the group action $A \cdot z = h(A)(z) = \frac{az+b}{cz+d}$. We can check this satisfies the definition of group action given in 1.1.1. This group action satisfies associativity: if we have $A, B \in SL_2(\mathbb{Z})$, then for $z \in \mathcal{H}$,

$$\begin{aligned} A \cdot (b \cdot z) = A \cdot (h(B)(z)) &= h(A)(h(B)(z)) \\ &= (h(A)h \circ (B))(z) \\ (h \text{ is a homomorphism}) \qquad &= h(AB)(z) = (AB) \cdot z \end{aligned}$$

The second condition of being a group action is also satisfied, $I_2 \cdot (z) = z$ for all $z \in \mathcal{H}$.

From now on we often refer to $SL_2(\mathbb{Z})$ as Γ.

Definition 2.2.11. Let Γ' be a subgroup of Γ. Two points z_1, z_2 in $\mathcal{H}$ are said to be Γ' equivalent if they are in the same Γ'-orbit. That is to say there exists a $\gamma \in \Gamma'$ such that $\gamma z_1 = z_2$.

Note: Recall the notation γz for $\gamma \in \Gamma$ and $z \in \mathcal{H}$ means the group action of γ on z, i.e $h(\gamma)(z)$.

Definition 2.2.12. A fundamental domain $\mathcal{F}$ for a subgroup Γ' of Γ is a closed subset of $\mathcal{H}$ such that

1. $\cup_\gamma \Gamma' \gamma(\mathcal{F}) = \mathcal{H}$,
2. the images $\gamma(\text{int}(\mathcal{F}))$ are pairwise disjoint; that is $\gamma_1(\text{int}(\mathcal{F})) \cap \gamma_2(\text{int}(\mathcal{F})) = \emptyset$ if $\gamma_1, \gamma_2 \in \Gamma', \gamma_1 \neq \gamma_2$.
   (Here $\text{int}(\mathcal{F})$ denotes the *interior* of F, the largest open set contained inside $\mathcal{F}$).

Restating the above definition gives, a closed subset of $\mathcal{H}$, $\mathcal{F}$, is a fundamental domain for Γ' if

1. The orbit of every $z \in \mathcal{H}$ contains some point in $\mathcal{F}$
2. No two distinct points in the interior of $\mathcal{F}$ are contained in the same orbit.

We say that the images of $\mathcal{F}$ under Γ' *tessellate* $\mathcal{H}$.

Example 2.2.13. Consider the subgroup $\langle T \rangle$ of Γ, which has corresponding subgroup $\{\gamma_n \mid \gamma_n(z) = z + n, n \in \mathbb{Z}\}$ in Möb($\mathcal{H}$) under the image $h : \Gamma \to$ Möb($\mathcal{H}$). The set $\mathcal{F} = \{z \in \mathcal{H} | 0 \leq Re(z) \leq 1\}$ is closed. Let $z \in \mathcal{H}$, then $\leq nRe(z) < n + 1$ for some $n \in \mathbb{N}$. We consider $Re(\gamma_{-n}(z)) = Re(z - n) = Re(z) - n$, which lies in the interval $0 \leq Re(\gamma_{-n} z) < 1$, so

$\gamma_{-n}(z) \in \mathcal{F}$.
Next suppose we have $z_1, z_2 \in \mathrm{int}(\mathcal{F})$, in particular $0 \leq Re(z_1) < Re(z_2) \leq 1$, and suppose $\gamma_n z_1 = z_2$ for some n. The bounds on z_1 and z_2 mean that the maximum distance is 1 and so $\gamma_n = \gamma_1 = z+1$. The only two points distance 1 in the interval $[0, 1]$ are 0 and 1, so $Re(z_1) = 0$ and $Re(z_2) = 1$. So they do not lie in the interior of $\mathcal{F}$.
Hence $\mathcal{F}$ is a fundamental domain for $\langle T\rangle$.

Example 2.2.14. The set $\mathcal{F} = \{z \in \mathcal{H} \,|\, |c| \leq 1\}$ is a fundamental domain for the group $\Gamma' = \langle S\rangle$. The subgroup of Möb($\mathcal{H}$) corresponding to Γ' is $\{z, -1/z\}$.
Let z be a point in $\mathcal{H}$ that is not in $\mathcal{F}$, then $-1/z$ is in the fundamental domain.
If z_1, z_1 are two distinct Γ' equivalent points then we must have $-1/z_1 = z_2$, this occurs only when $|z_1| = |z_2| = 1$, i.e only on the boundary of $\mathcal{F}$.

2.2.2 Geometric proof that S, T generate $SL_2(\mathbb{Z})$

The geometric proof of Theorem 2.1.2 is done in two main steps. First we construct a fundamental domain for Γ using the action of $G := \langle S, T\rangle \subset \Gamma$, next we use it to show $G \supset \Gamma$ and so $G = \Gamma$.
The actions of S, T, along with the fundamental domains of $\langle T\rangle$ and $\langle S\rangle$ give an idea of one possible fundamental domain for Γ.

Lemma 2.2.15. *Every element $z \in \mathcal{H}$ has an element of it's G-orbit in $\mathcal{F} = \{z \in \mathcal{H} \,|\, -1/2 \leq z \leq 1/2 \, |z| \geq 1\}$.*

(Note: This implies every element of $Z \in \mathcal{H}$ has an element of it's Γ-orbit in $\mathcal{F}$, since $G \subset \Gamma$).

Proof. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, let $z \in \mathcal{H}$. Then as we've observed in 2.2,

$$Im(gz) = \frac{Im(z)}{|cz+d|^2}.$$

Geometrically since c, d are integers the points $cz + d$ lie on the lattice generated by 1 and z. This means that there is no infinite decreasing sequence

$$|c_1 z + d_1| > |c_2 z + d_2| > |c_3 z + d_3| > \cdots \text{ for integers } c_i, d_i.$$

This is since for any $\lambda \in \mathbb{R}, c \in \mathbb{Z}$ we could find d sufficiently large such that $|cz + d| > \lambda$ and $|cz - d| > \lambda$. So given $c \in \mathbb{Z}$ there are finitely many $d_i \in \mathbb{Z}$ such that $|cz + d_i| < |c_1 z + d_1|$. For each such d_i there are finitely many c_i that satisfy $|cz + d_i| < |c_1 z + d_1|$. Thus the sequence is finite and must terminate.
It implies there is no infinite increasing sequence

$$Im(g_1 z) < Im(g_2 z) < \cdots \text{ for } g_i \in G$$

This means that the following procedure will eventually move every element z in $\mathcal{H}$ in to the fundamental domain $\mathcal{F}$.
Let $z = z_0$.

(i) Translate z_0 to z_1 by T^n such that $|Re(T^n z)| \leq 1/2$ for some $n \in \mathbb{N}$. (We showed this was possible, for a translated domain, in Example 2.2.13).

(ii) If z_1 lies in the fundamental domain we are done. If not then it must lie inside the unit circle with $|z_1| < 1$, so we invert by S to get $z_2 = S(z_1)$. Observe that

$$Im(z_2) = Im(Sz_1) = \frac{Im(z_1)}{|z_1|^2} > Im(z_1) \text{ since } |z_1| < 1.$$

(iii) If z_2 is in the fundamental domain we are done, otherwise let $z_0 = z_2$ and return to the first step.

From this procedure we get a sequence

$$Im(z) < Im(ST^{n_1}z) < Im(ST^{n_2}ST^{n_1}z) < \cdots ,$$

we noted already that such a sequence must be finite, so eventually the process will terminate. □

An example of this procedure applied to multiple points is given in Figure 2.3.

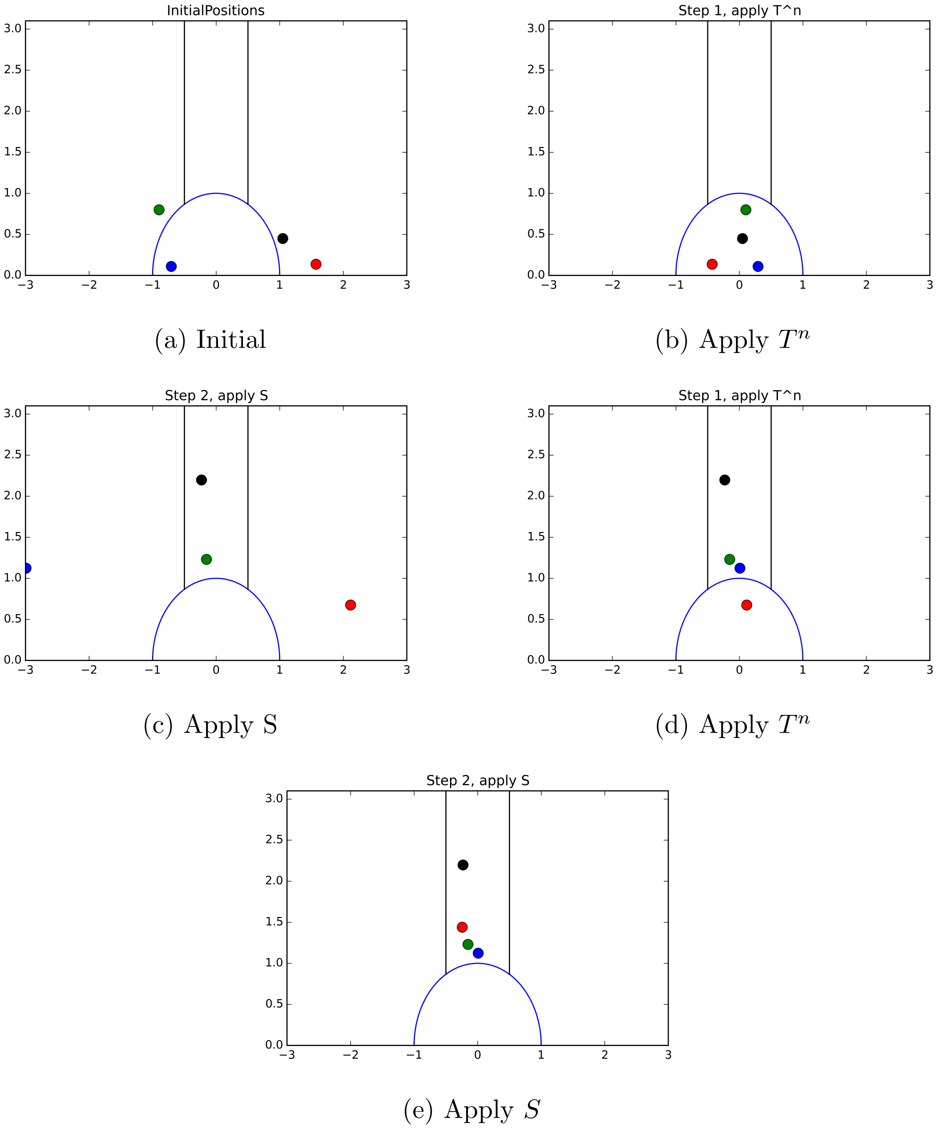
Lemma 2.2.16. *No two distinct points in the interior of $\mathcal{F}$ are Γ-equivalent*

Proof. Suppose we have two distinct points $z_1, z_2 \in \mathcal{F}$ and there exists a $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ such that $\gamma z_1 = z_2$. I.e $-1/2 \leq Re(z_1), Re(z_2) \leq 1/2$ and $|z_1|, |z_2| \geq 1$. We will show that both the points must lie on the boundary of $\mathcal{F}$.
Assume without loss of generality that $Im(z_1) \leq Im(z_2) (\star)$.
Writing out $Im(z_2)$ explicitly using 2.2,

$$\begin{aligned} Im(z_2) = Im(\gamma z_1) = \frac{Im(z_1)}{|cz_1 + d|^2} &\overset{(\star)}{\geq} Im(z_1) \\ \implies |cz_1 + d| &\leq 1 \end{aligned} \tag{2.5}$$

We will now investigate the possible values for c, d based on the bound $|cz_1 + d| \leq 1$. The values we find for c, d along with the condition on the determinant $ad - bc = 1$ will allow us to determine all the possible matrices γ.

If $|c| \geq 2$ then $Im(cz_1) \geq 2Im(z_1) \overset{Im(z_1) \geq 1}{\geq} \sqrt{3}$ and so $Im(cz_1 + d) > 1$. The imaginary part of $cz_1 + d$ thus lies outside the unit circle, it follows that the point $cz_1 + d$ lies outside the



(a) Initial

(b) Apply T^n

(c) Apply S

(d) Apply T^n

(e) Apply S

Figure 2.3: Example of procedure given in Lemma 2.2.15 .

unit circle and so $|cz_1 + d| > 1$, which is a contradiction to 2.5.

The simplifies the possible c, d pairs greatly since we must have $c \in \{-1, 0, 1\}$.

We consider the following cases separately,

(i) $c = 0$:

Here the condition on the determinant means $ad = 1$ and so $a = d = \pm 1$. Thus $\gamma = \pm \begin{pmatrix} 1 & \pm b \\ 0 & 1 \end{pmatrix}$, and so $\gamma = \pm T^{\pm b}$.

If $b = 0$ then $\gamma \pm I_2$ and so $\gamma z_1 = z_1$, which is a contradiction.

If $b \neq 0$, then $|Re(\gamma z_1)| = |Re(z_1) \pm b| \geq |Re(z_1) \pm 1| \geq 1/2$. So γz_1 is only in $\mathcal{F}$ if $|Re(\gamma z_1)| = 1/2$, i.e only if $b = \pm 1$ and $\gamma = \pm T^{\pm 1}$. So $z_2 = z_1 \pm 1$, therefore they both lie on the boundary.

(ii) $c = \pm 1$, $d = 0$:

The condition on the determinant gives $-bc = 1$ and so $c = -b = \pm 1$. Then $\gamma = \pm \begin{pmatrix} \pm a & -1 \\ 1 & 0 \end{pmatrix}$ thus it is of the form $\gamma = \pm T^{\pm a} S$.

The inequality 2.5 gives $| \pm z_1| = |z_1| \leq 1$, so z_1 since $z_1 \in \mathcal{F}$ we have $|z_1| = 1$. So $|Sz_1| = |-1/z_1| = 1$. We are thus in the situation of (i) where we consider $-1/z_1$ instead of z_1, and a in place of b. It follows that if $a = 0$, that $-1/z_1 = z_1$ and so $z_1^2 = -1$, the only solution in $\mathcal{H}$ is $z_1 = i$ and so $z_1 = z_2$ and lies on the boundary of $\mathcal{H}$.

If $a \neq 0$ it follows from (i) that the only solution is $a = \pm 1$, and $-1/z_1 \pm 1 = z_1$. So the two possibilities are $z_1 = z_2 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ where $\gamma = \pm TS$ or $z_1 = z_2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ where $\gamma = \pm T^{-1}S$. These are the two points that lie both on the unit circle and one of the lines $Re(z) = \pm 1/2$.

(iii) $c = \pm 1$, $d \neq 0$:

The inequality 2.5 gives the condition $| \pm z_1 + d| \leq 1$. But since $\mathcal{F}$ is symmetric this is equivalent to $|z_1 + d| \leq 1$. We can write it out fully as $|z_1 + d| = \sqrt{(x+d)^2 + y^2}$ where $z = x + iy$, firstly it's clear $|z_1 + d| \geq \sqrt{(x+d)^2} = |(x+d)|$, since $y^2 > 0$. Suppose $|d| \geq 2$, then use $-1/2 \leq x \leq 1/2$ to get $|x + d| \geq -1/2 + d$. Therefore $| \pm z_1 + d| \geq 3/2 > 1$ for $|d| \geq 2$, which is a contradiction.

So the only other possibility is $d = \pm 1$, We can repeat the above but include that the minimum value for y is $\frac{\sqrt{3}}{2}$ and use the fact that $(x \pm 1)^2 \geq 1/4$, so $|z_1 \pm 1| = \sqrt{(x \pm 1)^2 + y^2} \geq \sqrt{1/4 + 3/4} = 1$. Thus we must have

$$| \pm z_1 \pm 1| = 1.$$

From this we go through all the possibilities:

Let $\omega^+ = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \omega^- = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

- Case, $c = d = 1$:

Then $|z_1+1| = 1 \implies z_1 = \omega^-$. The determinant of γ is $a - b = 1 \implies a = b+1$. This means $\gamma = \begin{pmatrix} b+1 & b \\ 1 & 1 \end{pmatrix} = T^{b+1}ST$, note $ST(z_1) = z_1$.

If $b = 0$, then $\gamma = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = TST$ and $\gamma z_1 = \omega^+$.

If $b = -1$ then $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = ST$, $\gamma z_1 = z_1$.

For any other value of b then γz_1 will not lie in the fundamental domain.

- Case, $c = -d = 1$:

  Then $|z_1 - 1| = 1 \implies z_1 = \omega^+$. The determinant of γ is $-a-b = 1 \implies a = 1-b$. This means $\gamma = \begin{pmatrix} 1-b & b \\ 1 & -1 \end{pmatrix} = T^{-b}STS$, note $STS(z_1) = \omega^-$.

  If $b = 0$, then $\gamma = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} = STS$ and $\gamma z_1 = \omega^-$.

  If $b = -1$, then $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = (TS)^2$, and $\gamma z_1 = z_1$.

  For any other value of b then γz_1 will not lie in the fundamental domain.

- Case, $c = d = -1$:

  Then $|-z_1 - 1| = |z_1 + 1| = 1 \implies z_1 = \omega^-$. The determinant of γ is $-a+b = 1 \implies a = b-1$. This means $\gamma = \begin{pmatrix} b-1 & b \\ -1 & -1 \end{pmatrix} = -T^{-b}TST$, note $TST(z_1) = \omega^+$.

  If $b = 0$, then $\gamma = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} = -TST$, and $\gamma z_1 = \omega^+$.

  If $b = 1$, the n $\gamma = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = -ST$, and $\gamma z_1 = z_1$.

- Case, $c = -d = -1$:

  Then $|-z_1 + 1| = 1 \implies z_1 = \omega^+$. The determinant of γ is $a+b = 1 \implies a = 1-b$. This means $\gamma = \begin{pmatrix} 1-b & b \\ -1 & 1 \end{pmatrix} = -T^bSTS$, note $STS(z_1) = \omega^-$.

  If $b = 0$, then $\gamma = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = STS$, and $\gamma z_1 = \omega^-$.

  If $b = 1$, then $\gamma = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = (TS)^2$, and $\gamma z_1 = z_1$

□

Proposition 2.2.17. $\mathcal{F} = \{z \in \mathcal{H} \mid -1/2 \leq z \leq 1/2\, |z| \geq 1\}$ *is a fundamental domain for* Γ.

Proof. By applying Lemmas 2.2.15 and 2.2.16 we see that $\mathcal{F}$ satisfies both parts of the definition for a fundamental domain. □

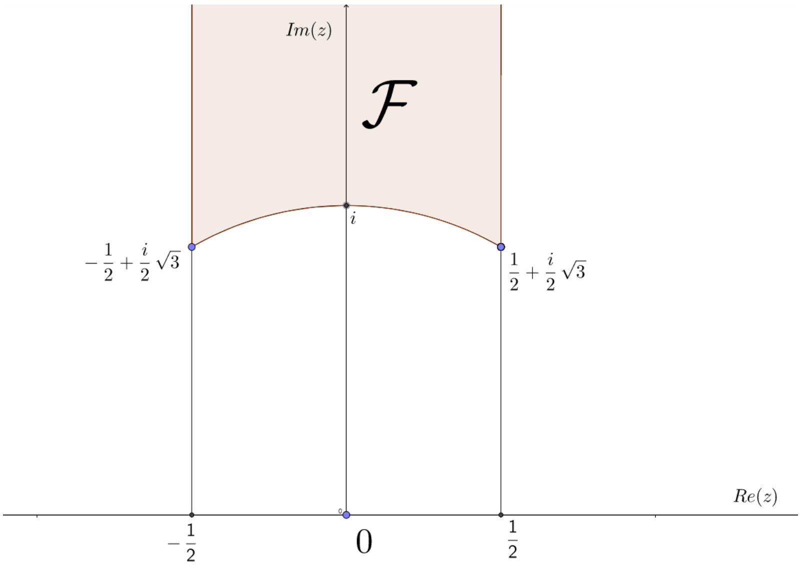

$Im(z)$
$\mathcal{F}$
i
$-\frac{1}{2}+\frac{i}{2}\sqrt{3}$
$\frac{1}{2}+\frac{i}{2}\sqrt{3}$
$Re(z)$
$-\frac{1}{2}$
0
$\frac{1}{2}$

Figure 2.4: A fundamental domain $\mathcal{F}$ of Γ

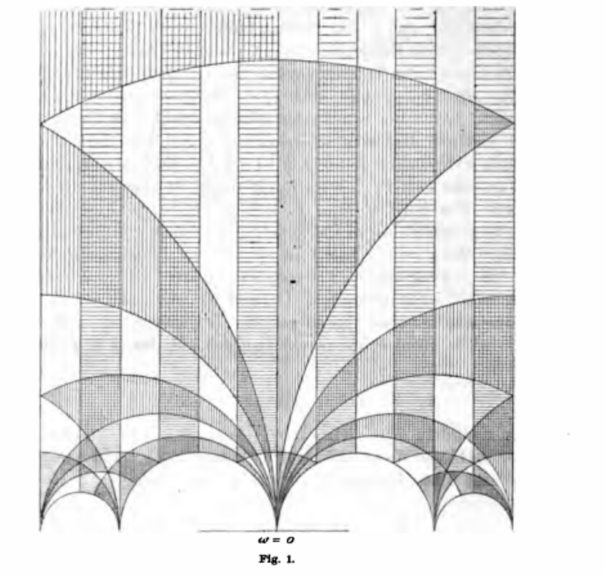


Figure 2.5: Tessellation of $\mathcal{H}$

See 2.5 for a tessellation of $\mathcal{H}$ by Klein [Klein, 1890].

In the course of proving Lemma 2.2.16 we proved following two facts.

Proposition 2.2.18. *Two distinct points z_1, z_2 on the boundary of $\mathcal{F}$ are Γ-equivalent only if $Re(z_1) = \pm 1/2$ and $z_2 = z_1 \mp 1$ or $|z_1| = 1$ and $z_2 = -1/z_1$*

Proposition 2.2.19. *If $z \in \mathcal{F}$ then the stabilizer of z in Γ, Γ_z, is $\{I, -I\}$, except in the following cases:*
(i) $\Gamma_z = \pm\{I, S\}$ if $z = i$
(ii) $\Gamma_z = \pm\{I, ST, (ST)^2\}$ if $z = -1/2 + \frac{\sqrt{-3}}{2}$
(iii) $\Gamma_z = \pm\{I, TS, (TS)^2\}$ if $z = 1/2 + \frac{\sqrt{-3}}{2}$

Theorem 2.2.20. *The matrices S, T generate Γ, i.e $\langle S, T\rangle = SL_2(\mathbb{Z})$.*

Proof. Let γ be an element of Γ, and let z be a point in the interior of $\mathcal{F}$. Then consider the point $\gamma z \in \mathcal{H}$. In lemma 2.2.15 we showed that there exists a $g \in \langle S, T\rangle$ such that $g\gamma z \in \mathcal{F}$. So the points z and $g\gamma z$ are Γ equivalent. But since z is in the interior of $\mathcal{F}$ it follows from Propositions 2.2.17 and 2.2.19 that $g\gamma = \pm I_2$ and so $\gamma = g^{-1} \in \langle S, T\rangle$. □

The proof of Theorem 2.2.20 can be used to write an element $\gamma \in \Gamma$ as a word in S, T. Take a point in int($\mathcal{F}$), like $2i$, then consider the point $\gamma 2i$. We use the algorithm described the proof of Lemma 2.2.15 to find $g \in \langle S, T\rangle$ such that $g\gamma 2i = 2i$ then $\gamma = g^{-1} \in \langle S, T\rangle$.

Example 2.2.21. Consider the matrix $\gamma = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \in SL_2(\mathbb{Z})$ and let $z = 2i \in \mathcal{F}$.
Then $\gamma z = \frac{2i+1}{2i+2} = \frac{3}{4} + i\frac{1}{4}$.
This lies outside the interval so we translate, $T^{-1}\gamma z = \frac{-1}{4} + i\frac{1}{4}$. However this is inside the unit circle so we invert to get $ST^{-1}\gamma z = 2 + 2i$. Again we do not lie in the interval so we need to translate. The translation by T^2 gives,

$$T^{-2}ST^{-1}\gamma(2i) = 2i \text{ and so } \gamma = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = (T^{-2}ST^{-1})^{-1} = TST^2$$

2.3 Algebraic approach to $SL_2(\mathbb{Z})$

2.3.1 Algebraic proof that S, T generate $SL_2(\mathbb{Z})$

It is possible to prove that S, T generate $SL_2(\mathbb{Z})$ in a more direct way. We take a matrix in $SL_2(\mathbb{Z})$, and reduce it via the action of S, T to the identity. Recall their action,

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \quad T^n\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \pm a + cn & b + dn \\ c & d \end{pmatrix}.$$

Note also for any $n \in \mathbb{Z}$ that we can construct a matrix in $SL_2(\mathbb{Z})$ with lower left entry n, ex $A = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$.

Proof. (Algebraic)
Let A be a matrix in $SL_2(\mathbb{Z})$.
If A has lower left entry 0, then it is of the form $\begin{pmatrix} \pm 1 & m \\ 0 & \pm 1 \end{pmatrix} = \pm T^m$ where $m \in \mathbb{Z}$. We know that $S^2 = -I_2$ so $A \in \langle S, T \rangle$.
We proceed by induction on the size of the lower left entry.
The base case lower left entry equals 0 has been covered above.
Let us assume that all matrices in $SL_2(\mathbb{Z})$ with lower left entry less in absolute value than $n+1$ are also in $\langle S, T \rangle$:
Now suppose we have a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $|c| = n+1$.
Case (i) : If $|a| < |c|$, then $SA = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$ has lower left entry a, with $|a| < n+1$ so by induction hypothesis $SA \in \langle S, T \rangle$ which implies $A \in \langle S, T \rangle$.
Case (ii) : If $|a| \geq |c|$, then use the division algorithm to write $a = cq + r$ where $0 \leq r < |c|$. Then

$$T^{-q}A = T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \pm a - cq & b - dq \\ c & d \end{pmatrix} = T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \pm r & b - dq \\ c & d \end{pmatrix}$$

. $T^{-q}A$ has upper left entry r where $|r| < |c|$, so we can use case (i) to conclude $T^{-q}A \in \langle S, T \rangle$ and so $A \in \langle S, T \rangle$. □

Example 2.3.1. We can carry out an example of the algebraic proof by hand. Let $A = \begin{pmatrix} 13 & 37 \\ 7 & 20 \end{pmatrix}$. First observe $13 = 7 \cdot 1 + 6$, so subtract the bottom row from the top, multiplying by T^{-1},

$$T^{-1}A = \begin{pmatrix} 6 & 17 \\ 7 & 20 \end{pmatrix}.$$

Now $6 > 7$ so we interchange rows, multiplying by S,

$$ST^{-1}A = \begin{pmatrix} 7 & 20 \\ -6 & -17 \end{pmatrix}.$$

And now we can write $7 = -6 \cdot -1 + 1$, so we add the second row to the first, with T

$$TST^{-1}A = \begin{pmatrix} 1 & 3 \\ -6 & -17 \end{pmatrix}.$$

We see that $|-6| > |1|$ so we invert with S,

$$STST^{-1}A = \begin{pmatrix} -6 & -17 \\ -1 & -3 \end{pmatrix}.$$

We can at last reduce the upper left entry to 0, write $-6 = -1 \cdot 6 + 0$, multiply by T^{-6},

$$T^{-6}STST^{-1}A = \begin{pmatrix} 0 & 1 \\ -1 & -3 \end{pmatrix}.$$

And to switch this into correct from, swap rows using S and get,

$$ST^{-6}STST^{-1}A = \begin{pmatrix} -1 & -3 \\ 0 & -1 \end{pmatrix} = -T^3.$$

Rearrange this to get

$$A = \begin{pmatrix} 13 & 37 \\ 7 & 20 \end{pmatrix} = -TST^{-1}ST^6ST^3$$

While working through this example or reexamining the proof one might notice that this algorithm is not the only way to get a decomposition of A in terms of S, T. For example in the first step we could multiply A by T^{-2} instead, and get,

$$T^{-2}A = \begin{pmatrix} -1 & -3 \\ 7 & 20 \end{pmatrix}$$

An advantage being we arrive at upper left entry with absolute value 1 in less steps, and so lower left entry 0 in less steps. Continuing the algorithm as normal from here we get the decomposition,

$$A = \begin{pmatrix} 13 & 37 \\ 7 & 20 \end{pmatrix} = T^2ST^7ST^3$$

Corollary 2.3.2. *The group $SL_2(\mathbb{Z})$ is generated by two matrices of finite order. In particular $SL_2(\mathbb{Z}) = \langle S, ST\rangle$*

Proof. We have $SL_2(\mathbb{Z}) = \langle S, T\rangle$. So $\langle S, ST\rangle \subset SL_2(\mathbb{Z})$. But also $S \in \langle S, ST\rangle$ and $T = S^3(ST) \in \langle S, ST\rangle$. So $SL_2(\mathbb{Z}) = \langle S, T\rangle = \langle S, ST\rangle$. The matrix $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4 and $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ has order 4. □

Corollary 2.3.3. *The group $SL_2(\mathbb{Z})$ is generated by two matrices of infinite order. In particular $SL_2(\mathbb{Z}) = \langle T, U\rangle$, where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.*

Proof. Both T and U are in $SL_2(\mathbb{Z})$, so $\langle T, U\rangle \subset SL_2(\mathbb{Z})$. Conversely, since $S = T^{-1}UT^{-1}$, $\langle T, U\rangle \supset \langle S, T\rangle = SL_2(\mathbb{Z})$. $\square$

Chapter 3

Congruence subgroups of $SL_2(\mathbb{Z})$

3.1 The principal congruence subgroup $\Gamma(N)$

Recall the notation $SL_2(\mathbb{Z}) = \Gamma$.

Definition 3.1.1. The group denoted $\Gamma(N)$, $N \in \mathbb{N}^+$, is called the principal congruence subgroup of level N, defined to be

$$\Gamma(N) := \Big\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,\Big|\, A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \Big\}$$

We define $\Gamma(1) := \Gamma$.

This subgroup $\Gamma(N)$ is actually a normal subgroup in Γ since it is the kernel of the group homomorphism from $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing entries modulo N. Notice that $a \equiv x \mod Nt \implies a \equiv x \mod N$ so for any multiple Nt we get $\Gamma(Nt) \subset \Gamma(N)$.
We will make use of the following elementary lemma in several proofs.

Lemma 3.1.2. *Given integers $c \neq 0$, d, $N \in \mathbb{Z}$. The set $\{t \,|\, (d + tN, c) = 1\}$ is non-empty, and this set is infinite if there exists a prime dividing c but not d. (I.e $\gcd(c, d) \neq c$ or d).*

Proof. Let $d' = d + tN$. Our goal is to find appropriate values for t.
We begin by splitting the prime divisors of c into two groups,

$$\{p_1, p_2, \dots, p_s \colon\, p_i \mid c\,,\, p_i \mid d\} \text{ and } \{q_1, q_2, \dots, q_r \colon\, q_j \mid c\,,\, q_j \nmid d\}$$

If $\gcd(c, d) \neq c$ or d : then the set of q_j is non empty.
Define $k = \prod q_j = \prod_{p|c, p\nmid d} p$, and $d' = d + tN$, where $t = k^m$. Where m any positive integer.
Suppose p is a prime divisor of c and d'.
Suppose also $p \mid d$, then $p \mid (d' - d) = tN$ and $p \nmid t$. This implies $p \mid N$, which is a contradiction, since $\gcd(c, dN) = 1$.

Otherwise if $p \nmid d$, then $p \nmid (d' - d) = tN$ and $p \mid t$. These two results contradict.
So there are no common prime divisors of c, d' and so $gcd(c, d' = d + k^m) = 1$, for all $m \in \mathbb{N}$.

In the other case, if $\gcd(c, d) = c$ or d, define $d' = d + N$. Now $\gcd(c, d') = 1$ since $\gcd(c, d, N) = 1$. □

Theorem 3.1.3. *The natural map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.*

Proof. Let $\gamma = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$ be given. A lift of $A \in SL_2(\mathbb{Z}/N\mathbb{Z})$ to $M_2(\mathbb{Z})$ is an element in the inverse image of A by the reduction homomorphism. Let $\tilde{\gamma} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$, such that $\tilde{\gamma} \equiv \gamma \mod N$. We show it's possible to modify $\tilde{\gamma}$ such that it's still congruent to γ but has unit determinant.

First note that $ad - bc \equiv 1 \mod N$. So $ad - bc + Nk = 1$ for some $k \in \mathbb{Z}$, so $\gcd(c, d, N) = 1$. We suppose $c \neq 0$ for now. We can apply Lemma 3.1.2 to find a d' such that $\gcd(c, d') = 1$, and $d' \equiv d \mod N$. Define $\tilde{\gamma_1} = \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \equiv \gamma$.
We can now consider lifts of γ of form $\tilde{\gamma_2} = \begin{pmatrix} a + kN & b + lN \\ c & d' \end{pmatrix}$, $k, l \in \mathbb{Z}$. The determinant is $\det(\tilde{\gamma_2}) = (a + kN)d' - (b + lN)c = ad' - bc + N(kd' - lc)$.
From the definition of γ_1 we have $ad' - bc = 1 + qN$ for some $q \in \mathbb{Z}$. By substitution, $\det(\tilde{\gamma_2}) = 1 + N(q + kd' - lc) = 1$.
Now the fact that $\gcd(c, d') = 1$ allows us to solve $q = lc - kd'$ for $k, l \in \mathbb{Z}$. We obtain the lift,

$$\begin{pmatrix} a + kN & b + lN \\ c & d' \end{pmatrix} \in SL_2(\mathbb{Z}) \equiv \gamma \mod N$$

The case $c = 0$ is not much different. The condition $\det(\gamma) = 1$ gives that $d \neq 0$, and we proceed similarly to above. We have $\gcd(a, d, N) = 1$, and we set $d' = d + tN$ where $t = \prod_{p \mid a, p \nmid d} p$. This gives $gcd(d', a) = 1$. Then we compute q from $ad = 1 + qN$. Finally we solve $ax + yd' = -q$ for integers x, y. Our desired lift is then $\begin{pmatrix} a + yN & b \\ 0 & d' + xN \end{pmatrix}$ □

Theorem 3.1.4. *The group $\Gamma(2)$ is generated by the matrices $-I, T^2$ and U^2, where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ as before, so $T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $U^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.*

Proof. We have that $-I, T^2, U^2 \in \Gamma(2)$ so $\langle -I, T^2, U^2 \rangle \subset \Gamma(2)$. For the reverse inclusion we adapt the algebraic proof that $\langle S, T \rangle = SL_2(\mathbb{Z})$. We will use the modified division theorem, that is, given $a, b \in \mathbb{Z}$ we can write $a = bq + r$ where $|r| \leq |b|/2$.

So we pick any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$, the definition gives that a, d are odd and b, c are even. If $c = 0$, then $ad - bc = ad = 1$ implies that $a = d = \pm 1$, also b is even so can write as $b = 2k$ so $A = \begin{pmatrix} \pm 1 & 2k \\ 0 & \pm 1 \end{pmatrix} \in \Gamma(2)$. This is of the form $\pm T^{2k} = \pm T^{2^k} \in \langle -I, T^2 \rangle$.

What we wish to show is that every matrix in $\Gamma(2)$ can be reduced to a matrix with lower left entry 0 by an element of $-I, T^2, U^2$. We can proceed by induction on the size of c, the lower left entry. If $c = 0$ we are done by the above.

Suppose every matrix in $\Gamma(2)$ with lower left entry,c , such that $|c| < n$, can be reduced to a matrix with lower left entry 0 by an element of $-I, T^2, U^2$.

Now suppose we have a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ with $|c| = n$. From the definition of $\Gamma(2)$ we see that a and c have different parity, so $|a| \neq |c|$, there are two possibilities. If $|a| < |c|$, use the modified division theorem to write $c = (2a)q + r$, where $|r| \leq |2a|/2 = |a|$. Then

$$U^{-2q}A = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c - 2qa & d - 2qb \end{pmatrix} = \begin{pmatrix} a & b \\ r & d - 2qb \end{pmatrix}$$

. Now the matrix $U^{-2q}A$ has lower left entry r, and $|r| < |c|$, i.e lower left entry less in absolute value than before, so we can conclude by the induction hypothesis. If $|a| > |c|$, then use the modified division theorem to write $a = (2c)q + r$, where $|r| \leq |2c|/2 = |c|$. Then

$$T^{-2q}A = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - 2qc & b - 2qd \\ c & d \end{pmatrix} = \begin{pmatrix} r & b - 2qd \\ c & d \end{pmatrix}$$

Now the upper left entry r is less in absolute value than the lower left entry so we can apply the first case and then conclude by induction.

This shows we can find $g \in \langle -I, T^2, U^2 \rangle$, such that gA has lower left entry 0. This is of the form $gA = \pm T^{2k} \in \langle -I, T^2 \rangle \implies A = \pm g^{-1}T^{2k} \in \langle -I, T^2, U^2 \rangle$.

□

Lemma 3.1.5. *The order of $SL_2(\mathbb{Z}/p^e\mathbb{Z})$ is $p^{3e}(1 - 1/p^2)$ when p is prime and $e \in \mathbb{N}$.*

Proof. The case $e = 1$ can be computed by considering two subcases and counting the number of possible $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/p\mathbb{Z})$. The definition of $SL_2(\mathbb{Z}/p\mathbb{Z})$ gives us that $A \in SL_2(\mathbb{Z}/p\mathbb{Z})$ if and only if $det(A) = ad - bc \equiv 1 \mod p$. The number of solutions to this equation in $\mathbb{Z}/p\mathbb{Z}$ is equal to the number of possible A. A key fact we will use is that $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, so each non-zero element in $\mathbb{Z}/N\mathbb{Z}$ has a unique multiplicative inverse $(\star)$.

Case $a \equiv 0$: $A = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$, and $\det(A) = -bc \equiv 1 \mod p$. We can apply $(\star)$ to say there are $p-1$ solutions in b, c to this congruence. Also d can take any of p values in $\mathbb{Z}/N\mathbb{Z}$. The total gives $p \cdot (p-1) = p(p-1)$ solutions to $ad - bc \equiv 1 \mod p$ for $a \equiv 0, b, c, d \in \mathbb{Z}/p\mathbb{Z}$.

Case $a \not\equiv 0$: We can rearrange the equation to $ad \equiv 1 + bc \mod p$. There are $p-1$ possible values for $a \not\equiv 0$, and p possible values for each b and c. From these the value for d is determined uniquely by ($\star$). In total there are $(p-1) \cdot p \cdot p \cdot 1 = (p-1)p^2$ in solutions to $ad - bc \equiv 1 \mod p$ for $a \not\equiv 0, b, c, d \in \mathbb{Z}/p\mathbb{Z}$.
Totaling from both cases we have $p(p-1) + (p-1)p^2 = p^3 - p$ solutions to the equation for determinant. So the order of $SL_2(\mathbb{Z}/p\mathbb{Z})$ is $p^3 - p$.
The case $e > 1$ is more complex since then for $a \not\equiv 0$ the relation $ad \equiv 1 + bc \mod p^e$ is not always solvable so we would have to separately consider further subcases a invertible and not invertible $\mod p$.
We can proceed by induction on e. We have shown $SL_2(\mathbb{Z}/p^e\mathbb{Z})| = p^{3e}(1 - 1/p^2)$ for $e = 1$. Suppose that the result holds for $e = k$, i.e

$$|SL_2(\mathbb{Z}/p^k\mathbb{Z})| = p^{3k}(1 - 1/p^2).$$

Consider the reduction homomorphism

$$f : SL_2(\mathbb{Z}/p^{k+1}\mathbb{Z}) \to SL_2(\mathbb{Z}/p^k\mathbb{Z})$$

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod p^k$$

The kernel of f is,

$$\left\{ A \in SL_2(\mathbb{Z}/p^{k+1}\mathbb{Z}) \middle| A = \begin{pmatrix} 1 + a'p^k & b'p^k \\ c'p^k & 1 + d'p^k \end{pmatrix} \text{ and } 0 \leq a', b', c', d' < p \in \mathbb{Z}/p^{k+1}\mathbb{Z} \right\}$$

Again we can count the number of possible matrices by counting the number of solutions to the determinant equation.

$$\begin{aligned} A \in ker(f) &\iff \det(A) \equiv 1 \mod p^{k+1} \\ &\iff (1 + a'p^k)(1 + d'p^k) - (b'p^k)(c'p^k) \equiv 1 \mod p^{k+1} \\ &\iff 1 + a'p^k + d'p^k + a'd'p^{2k} - b'c'p^k \equiv 1 \mod p^{k+1} \\ &\iff a'p^k + d'p^k \equiv 0 \mod p^{k+1} \\ &\iff a' \equiv -d' \mod p \end{aligned}$$

So we if we let $d' = np - a'$ for some $n \in \mathbb{Z}/p\mathbb{Z}$, we can rewrite,

$$\{A \in SL_2(\mathbb{Z}/p^{k+1}\mathbb{Z})\Big| A = \begin{pmatrix} 1 + a'p^k & b'p^k \\ c'p^k & 1 + (np - a')p^k \end{pmatrix}$$
$$\text{and } 0 \leq a', b', c', (np - a') < p \,, n \in \mathbb{Z}/p^{k+1}\mathbb{Z}\Big\}$$

The restriction $0 \leq a', (np - a') < p$ means we must have $n = 1$. A matrix in $ker(f)$ is thus determined uniquely by the values $0 \leq a', b', c' < p$. The order of $ker(f)$ is thus the product of the number of possibilities for each value, ie $ker(f) = p^3$.
The reduction map f is also surjective, this is because the reduction map from $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/p^k\mathbb{Z})$ is surjective and it can be decomposed into two maps $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/p^{k+1}\mathbb{Z}) \xrightarrow{f} SL_2(\mathbb{Z}/p^k\mathbb{Z})$, so both the intermediate maps must be surjective.
We can apply the first isomorphism theorem to obtain $SL_2(\mathbb{Z}/p^{k+1}\mathbb{Z})/ker(f) \cong SL_2(\mathbb{Z}/p^k\mathbb{Z})$, and so

$$|SL_2(\mathbb{Z}/p^{k+1}\mathbb{Z})| = p^3|SL_2(\mathbb{Z}/p^k\mathbb{Z})| \overset{\text{induction}}{=} p^{3(k+1)}(1 - 1/p^2)$$

□

Proposition 3.1.6. *Let $N \in \mathbb{Z}$, then,*

$$SL_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^{k} SL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$$

Where $N = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ is the prime factorization.

Proof. If we write N as it's prime factorization $N = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$. Define the homomorphism,

$$f \,:\, SL_2(\mathbb{Z}/N\mathbb{Z}) \to \prod_{i=1}^{k} SL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \Big(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod p_1^{r_1}, \ldots, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod p_k^{r_k} \Big)$$

The function f is well-defined, let $x \in \mathbb{Z}$,

$$\begin{aligned} x \equiv x' \mod N \iff N \mid (x - x') &\iff p_1^{r_1} \ldots p_k^{r_k} \mid (x - x') \\ &\implies p_i^{r_i} \mid (x - x') \iff x \equiv x' \mod p_i^{r_i} \end{aligned}$$

To show f is surjective, suppose we have $\Big(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in SL_2(\mathbb{Z}/p_1^{r_1}\mathbb{Z}), \ldots, \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} \in SL_2(\mathbb{Z}/p_k^{r_k}\mathbb{Z}) \Big)$ then we can find a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z})$ by solving the cor-

responding system of congruences for each entry using the Chinese Remainder Theorem. For example, we take a as the solution to the system $\left(a \equiv a_1 \mod p_1^{r_1}, \ldots, a \equiv a_k \mod p_k^{r_k}\right)$. We also must check A does indeed lie in $SL_2(\mathbb{Z}/N\mathbb{Z})$, i.e $\det(A) \equiv 1 \mod N$.
For each $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in SL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$ we have $a_i d_i - b_i c_i \equiv 1 \mod p_i^{r_i}$. Then $ad - bc \equiv 1 \mod p_i^{r_i}$ by definition of a, b, c, d. From this we see $p_i^{r_i} \mid (ad - bc) - 1$ for each prime power $p_i^{r_i}$, it follows that $N = \prod_{i=1}^k p_i^{r_i} \mid (ad - bc) - 1$. So $ad - bc \equiv 1 \mod N$ and $A \in SL_2(\mathbb{Z})$.
To show injectivity suppose,

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = f(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix})$$

Then $a \equiv a' \mod p_i^{r_i}$ so by the Chinese Remainder Theorem $a \equiv a' \mod p_1^{r_1} \ldots p_k^{r_k} = N$, similarly we get $b \equiv b' \mod$, $c \equiv c' \mod N$,$d \equiv d' \mod N$. □

Corollary 3.1.7. *The order of $SL_2(\mathbb{Z}/N\mathbb{Z})$ is $N^3 \prod_{p|N}(1 - 1/p^2)$.*

Proof. From Proposition 3.1.6 we have $SL_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^k SL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$. So

$$|SL_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{p^e|N} |SL_2(\mathbb{Z}/p^e\mathbb{Z})| = \prod_{p^e|N} p^{3e}(1 - 1/p^2) = N^3 \prod_{p|N}(1 - 1/p^2)$$

□

Corollary 3.1.8. *The finite group $SL_2(\mathbb{Z}/N\mathbb{Z})$ is generated by two elements of order N.*

Proof. Every element of $SL_2(\mathbb{Z}/N\mathbb{Z})$ has a lift in $SL_2(\mathbb{Z})$. In Corollary 2.3.3 we showed $\langle T, U\rangle = SL_2(\mathbb{Z})$, where $T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. So this lift can be written as an element of $\langle T, U\rangle$. So reducing the lift modulo N we get it as a product T, U modulo N, i.e

$$SL_2(\mathbb{Z}/N\mathbb{Z}) = \langle T \mod N, U \mod N\rangle.$$

Also $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $U^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ for all $n \in \mathbb{Z}$, so both have order N. □

Corollary 3.1.9. *For any integer $N > 1$,*

$$SL_2(\mathbb{Z}/N\mathbb{Z}) \cong SL_2(\mathbb{Z})/\Gamma(N) \text{ and } [\Gamma : \Gamma(N)] = N^3 \prod_{p|N}(1 - 1/p^2)$$

Proof. We have shown in Theorem 3.1.3 that the natural reduction map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is onto and has kernel $\Gamma(N)$. The result follows from the first isomorphism theorem for groups. The index of $\Gamma(N)$ is exactly the order of $SL_2(\mathbb{Z}/N\mathbb{Z})$ which was computed Corollary 3.1.7. □

3.2 General congruence subgroups

We can define a more general notion of congruence subgroup than $\Gamma(n)$.

Definition 3.2.1. A subgroup of Γ is called a congruence subgroup of level N if it contains $\Gamma(N)$ and N is the least such integer.

The isomorphism in Corollary 3.1.9 is central to the study of congruence subgroups. It allows us to carry over properties of $SL_2(\mathbb{Z}/N\mathbb{Z})$ to $SL_2(\mathbb{Z})$ and vice versa. In particular we use the Third Isomorphism Theorem and the Correspondence Theorem in group theory to do so.

Corollary 3.2.2. *In $SL_2(\mathbb{Z})$ the subgroup $\langle S, T^2\rangle$ has index* 3.

Proof. We begin by showing that $\Gamma(2) \subset \langle S, T^2\rangle$. It is enough to show the generators $-I_2, T^2, U^2$ from theorem 3.1.4 are each in $\langle S, T^2\rangle$. We have $-I_2 = S^2, T^2 = T^2$ and $U^2 = ST^{-2}S^{-1}$. Now because $\Gamma(2)$ is a normal subgroup, when computing the index of $\langle S, T^2\rangle$ it is equivalent to work modulo $\Gamma(2)$, i.e $[SL_2(\mathbb{Z}) : \langle S, T^2\rangle] = [SL_2(\mathbb{Z})/\Gamma(2) : \langle S, T^2\rangle/\Gamma(2)]$. This follows from the correspondence theorem.
The image of $\langle S, T^2\rangle$ in $SL_2(\mathbb{Z})/\Gamma(2) \cong SL_2(\mathbb{Z}/2\mathbb{Z})$ is $\{\bar{I}, \bar{S}\}$, so $\langle S, T^2\rangle/\Gamma(2) \cong \{\bar{I}, \bar{S}\}$. So finally we get

$$[SL_2(\mathbb{Z}) : \langle S, T^2\rangle] = [SL_2(\mathbb{Z})/\Gamma(2) : \langle S, T^2\rangle/\Gamma(2)] = [SL_2(\mathbb{Z}/2\mathbb{Z})) : \{\bar{I}, \bar{S}\}] = 6/2 = 3$$

□

If we replace $\langle S, T^2\rangle$ with $\langle S, T^m\rangle$ for $m > 2$ there is no analog of corollary 3.2.2 since $\langle S, T^m\rangle$ does not have finite index in $SL_2(\mathbb{Z})$ for $m > 2$. The proof is omitted here but it sketched out in Conrad's expository paper on $SL_2(\mathbb{Z})$ [Conrad].

The meaning of the terminology *congruence* subgroup is that they can be described by a finite set of congruence conditions.

Example 3.2.3. It was shown in the proof of 3.2.2 that $\Gamma(2) \subset \langle S, T^2\rangle$ so $\langle S, T^2\rangle$ is a congruence subgroup of level 2. We also showed that $\langle S, T^2\rangle/\Gamma(2) \cong \{\bar{I}, \bar{S}\}$, and so we can represent $\langle S, T^2\rangle$ by a set of congruence relations modulo 2,

$$\langle S, T^2\rangle = \left\{A \in SL_2(\mathbb{Z}) \,\middle|\, A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mod 2\right\}$$

An equivalent definition of congruence subgroup is a subgroup that is the inverse image under reduction modulo N of some subgroup of $SL_2(\mathbb{Z}/N\mathbb{Z})$. (Can verify easily, Let $\Gamma(N) \subset G$ be a subgroup of Γ. Then the image of G is a subgroup of $SL_2(\mathbb{Z}/N\mathbb{Z})$. Conversely if G is the inverse image of some subgroup of $SL_2(\mathbb{Z}/N\mathbb{Z})$. Then G contains the inverse image of $\{\bar{I}\}$ so

$\Gamma(N) \subset G$.)
Every $\Gamma(N)$ has finite index in Γ so every congruence subgroup will have finite index also.

Remark 3.2.4. In the previous example we began with a congruence subgroup containing $\Gamma(2)$. The group was represented by a set of generators and we then found the subgroup of $SL_2(\mathbb{Z}/2\mathbb{Z})$ that it was the inverse image of.
It is natural to then ask the converse, given a subgroup $\bar{G}$ of $SL_2(\mathbb{Z}/2\mathbb{Z})$, how do we find a set of elements in $SL_2(\mathbb{Z})$ that generate the inverse image, G, of $\bar{G}$?

It is a well known fact, referred to as Schreier's lemma, that every finite index subgroup of a finitely generated group is also finitely generated. This means we can find a set of generators for all the subgroups $\Gamma(N)$ since they have finite index. Below is a method to do so for them, but more general algorithms are known [Seress, 2002]
Given $\bar{G} = \{\bar{A}_0, \bar{A}_1, \ldots, \bar{A}_k\} \leq SL_2(\mathbb{Z}/N\mathbb{Z})$. We can form a finite set $\mathcal{S} = \{A_0, A_1, \ldots, A_k\}$ with each $A_i \equiv \bar{A}_i$. Define C as the union of this set and the set of generators for $\Gamma(n)$. We claim that $\langle C \rangle$ equals the inverse image, G, of $\bar{G}$.
The group $\langle C \rangle$ contains all the generators for $\Gamma(n)$ by definition. Now by the same reasoning as in the proof of Corollary 3.2.2 we can consider the image of $\langle S \rangle$ in $SL_2(\mathbb{Z})/\Gamma(N)$, the image is $\bar{G}$. So we get $\langle C \rangle/\Gamma(N) \cong \bar{G}$, and so $G = \langle C \rangle$, since $\Gamma(N) \subset G$.
Note: The set C is not necessarily a minimal generating set. We can reduce the size of C by excluding the generators of $\Gamma(N)$ that can be generated from the $\langle \mathcal{S} \rangle$. Note also that the set of generators will not be unique.

Example 3.2.5. Consider the subgroup $\bar{G}$ of $SL_2(\mathbb{Z}/2\mathbb{Z})$, where

$$\bar{G} = \{\overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}, \overline{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}, \overline{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}\}.$$

By inspection we can find a set $\mathcal{S}$ such that,

$$\mathcal{S} = \{I_2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, ST \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, TS \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\}$$

Now from the remark above,

$$\langle I_2, ST, TS, -I_2, T^2, U^2 \rangle =$$

$$= G = \left\{ A \in SL_2(\mathbb{Z}) \,\middle|\, A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mod 2 \right\}$$

We can reduce the size of $\mathcal{S}$, without changing the group it generates, by noticing that: $I_2 = (ST)^0$, $-I_2 = (TS)(ST)(T^{-2})$, and $U^2 = (ST)T^{(}-2)(ST)^{-1}$. So we get $G = \langle ST, TS, T^2\rangle$, (or also $G = \langle -I_2, ST, TS\rangle$).

Example 3.2.6. We can repeat this procedure for each of the two other proper subgroups of $SL_2(\mathbb{Z}/2\mathbb{Z})$.
A set of generators for each congruence subgroup containing $\Gamma(2)$ is collected below:

$$\begin{aligned}
\langle -I_2, T^2, U^2\rangle = \Gamma(2) &= \Big\{A \in SL_2(\mathbb{Z}) \Big| A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 2\Big\} \\
\langle -I_2, T, U^2\rangle = \Gamma_0(2) &= \Big\{A \in SL_2(\mathbb{Z}) \Big| A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod 2\Big\} \\
\langle S, T^2\rangle &= \Big\{A \in SL_2(\mathbb{Z}) \Big| A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mod 2\Big\} \\
\langle T^{-1}ST, U^2, T^2\rangle &= \Big\{A \in SL_2(\mathbb{Z}) \Big| A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mod 2\Big\} \\
\langle ST, TS, T^2\rangle &= \Big\{A \in SL_2(\mathbb{Z}) \Big| A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ or } A \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mod 2\Big\}
\end{aligned}$$

3.2.1 The congruence subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$

Other than $\Gamma(N)$ the two other most important congruence subgroups are the inverse images of the $SL_2(\mathbb{Z}/N\mathbb{Z})$ subgroups,

$$\begin{aligned}
G_1 =& \{\begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})\Big\} \\
G_0 =& \{\begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})\Big\}
\end{aligned}$$

The star indicates no restriction on the entry, except det = 1. (It is a short exercise to check that these are indeed subgroups).
Specifically we define these congruence subgroups as follows,

Definition 3.2.7.

$$\Gamma_1(N) = \Big\{A \in SL_2(\mathbb{Z}) \Big| A \equiv \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \mod N\Big\} \tag{3.2.1}$$

$$\Gamma_0(N) = \Big\{A \in SL_2(\mathbb{Z}) \Big| A \equiv \begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix} \mod N\Big\} \tag{3.2.2}$$

These subgroups have many applications to the theory of modular functions [Koblitz, 2012]. Thus for any positive integer N we have the chain of containments

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma$$

Lemma 3.2.8. *The following maps are surjective homomorphisms,*

(a) $g_1 : \Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}\,, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \pmod N\,, \quad ker(g_1) = \Gamma(N)$

(b) $g_0 : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\star\,, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \pmod N\,, \quad ker(g_0) = \Gamma_1(N)$

Proof. (a) Let $b \in \mathbb{Z}/N\mathbb{Z}$, then $g_1(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) = b$.

The map g_1 is surjective since $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$.

Let $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \Gamma_1(N)$. Then

$$g_1(A_1A_2) = g_1(\begin{pmatrix} \star & a_1b_2 + b_1d_2 \\ \star & \star \end{pmatrix} = a_1b_2 + b_1d_2 \overset{a_1,d_2\equiv 1}{\equiv} b_1 + b_2 \pmod N$$

So g_1 is a homomorphism.

The identity of $\mathbb{Z}/N\mathbb{Z}$ is 0 so the kernel of g_1 are matrices with upper left entry congruent to 0.

If $A \in \Gamma(N) \implies b \equiv 0 \mod N \implies g_1(A) = 0$, so $\Gamma(N) \subset ker(g_1)$.

For the reverse inclusion, $ker(g_1) \subset \Gamma(N)$: let $A = \begin{pmatrix} a & b \\ d & d \end{pmatrix} \in ker(g_1)$ then by definition of $\Gamma_1(N)$ and $ker(g_1)$ we have $A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N)$.

(b) Let $d \in (\mathbb{Z}/N\mathbb{Z})^\star$, so d is invertible mod N. Let a be the solution of $ad = 1 \mod N$. Then $ad = 1 + Nk$, $k \in \mathbb{Z}$. The matrix $A = \begin{pmatrix} a & 1 \\ Nk & d \end{pmatrix})$ is thus in $\Gamma_0(N)$ and $g_0(A) = d$. So the map is surjective.

Let $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \Gamma_0(N)$. Then

$$g_0(A_1A_2) = g_1(\begin{pmatrix} \star & \star \\ \star & c_1b_2 + d_1d_2 \end{pmatrix}) = c_1b_2 + d_1d_2 \overset{c_1\equiv 0}{\equiv} d_1d_2 \pmod N$$

So g_0 is a homomorphism.

The identity of $(\mathbb{Z}/N\mathbb{Z})^\star$ is 1 so the kernel of g_0 is the set of matrices with lower right entry

congruent to 1.
If $A \in \Gamma_1(N) \implies d \equiv 1 \mod N \implies g_0(A) = 1$, so $\Gamma_1(N) \subset ker(g_0)$.
For the reverse inclusion, $ker(g_1) \subset \Gamma(N)$: let $A = \begin{pmatrix} a & b \\ d & d \end{pmatrix} \in ker(g_0)$ then by definition of $\Gamma_0(N)$ and $ker(g_0)$ we have $A \equiv \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mod N)$. So we must have $a \cdot 1 - b \cdot 0 = a \equiv 1 \mod N$. Then $A \in \Gamma_1(N)$.

□

Corollary 3.2.9. *The following isomorphisms hold,*

(a) $\Gamma(N) \lhd \Gamma_1(N)\,,\, \Gamma_1(N)/\Gamma(N) \cong \mathbb{Z}/N\mathbb{Z}$

(b) $\Gamma_1(N) \lhd \Gamma_0(N)\,,\, \Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\star$

Proof. Parts (a), (b) follow from their respective parts in Lemma 3.2.8. We use the fact that the kernel of homomorphisms is a normal subgroup. The First Isomorphism Theorem gives the isomorphisms, □

Corollary 3.2.10. *The following is a list of formulas for each index in the chain* $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma$.

$$|\Gamma \,:\, \Gamma_0(N)| = N \prod_{p|N} (1 + \frac{1}{p}) \qquad |\Gamma \,:\, \Gamma_1(N)| = N^2 \prod_{p|N} (1 - \frac{1}{p^2})$$

$$|\Gamma \,:\, \Gamma(N)| = N^3 \prod_{p|N} (1 - \frac{1}{p^2}) \qquad |\Gamma_0(N) \,:\, \Gamma_1(N)| = \varphi(N)$$

$$|\Gamma_0(N) \,:\, \Gamma(N)| = N\varphi(N) \qquad |\Gamma_1(N) \,:\, \Gamma(N)| = N$$

Proof. The indexes $[\Gamma_1(N) \,:\, \Gamma(N)] = N$ and $[\Gamma_0(N) \,:\, \Gamma_1(N)] = \varphi(N)$ can be obtained from the isomorphisms in Proposition 3.2.9 and the observation that $|\mathbb{Z}/N\mathbb{Z}| = N, |(\mathbb{Z}/N\mathbb{Z})^\star| = \phi(N)$.
The index $[\Gamma : \Gamma_(N)] = N^3 \prod_{p|N}(1 - 1/p^2)$ was determined in Corollary 3.1.9.
To compute the other index's we make use of the multiplicative property of indexes.

$$[\Gamma_0(N) \,:\, \Gamma(N)] = [\Gamma_0(N) \,:\, \Gamma_1(N)][\Gamma_1(N) \,:\, \Gamma(N)] = N\varphi(N)$$

$$\begin{aligned} [\Gamma : \Gamma(N)] = &\quad [\Gamma : \Gamma_0(N)][\Gamma_0(N) : \Gamma(N)] \\ = &\quad [\Gamma : \Gamma_0(N)]N\varphi(N) \\ \implies [\Gamma : \Gamma_0(N)] = &\quad \frac{1}{N\varphi(N)}N^3\prod_{p|N}(1-1/p^2) \end{aligned}$$

We then can then use Euler's product formula $\varphi(N) = N\prod_{p|N}(1-1/p)$ to simplify the expression,

$$[\Gamma : \Gamma_0(N)] = N\prod_{p|N}(1+\frac{1}{p})$$

For the final index we get

$$\begin{aligned} [\Gamma : \Gamma(N)] &= [\Gamma : \Gamma_1(N)][\Gamma_1(N) : \Gamma(N)] \\ \implies \frac{[\Gamma : \Gamma_(N)]}{[\Gamma_1(N) : \Gamma(N)]} &= [\Gamma : \Gamma_1(N)] \\ \implies \frac{1}{N}N^3\prod_{p|N}(1-1/p^2) &= [\Gamma : \Gamma_1(N)] \\ \implies N^2\prod_{p|N}(1-1/p^2) &= [\Gamma : \Gamma_1(N)] \end{aligned}$$

□

Proposition 3.2.11. *The subgroups* $\Gamma(N), \Gamma_0(N), \Gamma_1(N)$ *satisfy the relation*

$$\Gamma(N) \cong \Gamma_1(N) \cap \Gamma_0(N^2), \textit{ for all } N \in \mathbb{Z}$$

Proof. See Excersise III.I Q8 in [Koblitz, 2012]. □

Example 3.2.12. In particular notice $\Gamma_0(4) \subset \Gamma_1(2)$, Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$. Then we have $ad - bc = 1$ and $c \equiv 0 \mod 4$. So $c \equiv 0 \mod 2$. Also $ad \equiv 1 \mod 2 \implies a \equiv d \equiv 1 \mod 2$. Finally we get $A \equiv \begin{pmatrix} 1 & b \\ 0 & \star \end{pmatrix} \pmod 2$. So Proposition 3.2.11 we get $\Gamma(2) \cong \Gamma_1(2) \cap \Gamma_0(4) = \Gamma_0(4)$.

3.3 Fundamental domains for congruence subgroups

Recall in Proposition 2.2.17, we found a fundamental domain for $SL_2(\mathbb{Z})$, to be $\mathcal{F} = \{z \in \mathcal{H} \mid -1/2 \leq z \leq 1/2 \, |z| \geq 1\}$. We can ask the question of what the fundamental domain might be for some subgroup of $SL_2(\mathbb{Z})$. For example if we consider the subgroup generated by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, if follows from example 2.2.13 that the set $\{z \in \mathcal{H} \mid 1/2 \leq Re(z) \leq 1/2\}$ is a fundamental domain for the infinite-index subgroup $\langle T \rangle$. Example 2.2.14 showed that,

$\{z \,|\, |z| \leq 1\}$ is a fundamental domain for the infinite-index subgroup $\langle S \rangle$.

In this section we discuss how to find fundamental domains for finite index subgroups and give examples for congruence subgroups.

Remark 3.3.1. The set $\cup_{i=1}^{n} \alpha_i^{-1}\mathcal{F}$ is the union of the hyperbolic triangles $\{\alpha_2^{-1}\mathcal{F}, \dots, \alpha_n^{-1}\mathcal{F}\}$, they are images of the fundamental domain.

Proposition 3.3.2. *Suppose we have a finite index subgroup Γ' of Γ, $[\Gamma\,, \Gamma'] = n$. Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be a set of coset representatives for Γ', where $\Gamma = \coprod_{i=1}^{n} \alpha_i \Gamma'$ is the disjoint union of left cosets of Γ'.($\coprod$ denotes disjoint union.) Then,*

$$\mathcal{F}' = \cup i = 1^n \alpha_i^{-1}\mathcal{F},$$

is a fundamental domain for Γ'.

Proof. First we verify every point $z \in \mathcal{H}$ contains a point in F' in it's Γ'-orbit.
Let $z \in \mathcal{H}$, the set $\mathcal{F}$ is a fundamental domain for Γ, there exists a $\gamma \in \Gamma$ such that $\gamma(z) \in \mathcal{F}$. Recall that $\Gamma = \cup_{i=1}^{n} \alpha_i \Gamma'$, so we can find a coset representative $\alpha_i \in \Gamma$ and $\gamma' \in \Gamma'$ such that $\gamma = \alpha_i \gamma'$. By substitution we get $\gamma(z) = \alpha_i \gamma'(z) \in \mathcal{F}$, and so $\gamma'(z) \in \alpha_i^{-1}\mathcal{F} \subset \mathcal{F}'$.

(The following part of the proof was derived from Theorem 3.1.2 in [Katok, 1992])
We must also check no Γ'-orbit of any point in $\mathcal{H}$ two distinct points in the interior of $\mathcal{F}'$, (denoted $\mathring{\mathcal{F}}'$):
Suppose we have $f_1', f_2' \in \mathring{\mathcal{F}}'$ and there exists $\gamma' \in \Gamma'$ such that $\gamma'(f_1') = f_2'$.

The notation $\mathring{A}$ is used to denote the interior of a set.

We make use of the fact that f_1' is in the interior of $\mathcal{F}'$ to construct a ball of size ϵ around f_1', such that $B_\epsilon(f_1') \subset \mathring{\mathcal{F}}'$. This ball will intersect with $\alpha_i^{-1}\mathring{\mathcal{F}}$ for some i, but it could also intersect with more of α_j^{-1} images of $\mathring{\mathcal{F}}$. Let $\alpha_{t_1}^{-1}\mathring{\mathcal{F}}, \dots, \alpha_{t_k}^{-1}\mathring{\mathcal{F}}$ be exactly the k images it intersects with.

We have that $B_\epsilon(\gamma'(f_1')) = \gamma'(B_\epsilon(f_1'))$ since γ' is an isometry. This ball must intersect with some $\alpha_m^{-1}\mathring{\mathcal{F}}$, where $1 \leq m \leq n$.

It follows that $B_\epsilon(f_1')$ has a non-empty intersection with $(\gamma')^{-1}\alpha_m^{-1}\mathring{\mathcal{F}}$. Now this means $\alpha_{t_l}^{-1}\mathring{\mathcal{F}}$ intersects with $(\gamma')^{-1}\alpha_m^{-1}\mathring{\mathcal{F}}$ for some $1 \leq l \leq k$. So for some $z_1, z_2 \in \mathring{\mathcal{F}}$ we have $\alpha_{t_l}^{-1} z_1 = (\gamma')^{-1}\alpha_m^{-1} z_2$ which is equivalent to $\alpha_m(\gamma')\alpha_{t_l}^{-1} z_1 = (\gamma')^{-1} z_2$, now since $\mathcal{F}$ is a fundamental domain, we must have $\alpha_{t_l}^{-1} = (\gamma')^{-1}\alpha_m^{-1}$.

Hence,

$$\alpha_m \Gamma' \overset{\gamma' \in \Gamma'}{=} \alpha_m \gamma' \Gamma' = \alpha_{t_l} \Gamma'$$

So we must have $\alpha_m = \alpha_{t_l}$, and so $\gamma' = Id$. Hence, $f_1' = f_2'$.

□

Remark 3.3.3. In Proposition 3.3.2 we showed that we could construct a fundamental domain for a finite index subgroup of Γ given coset representatives. In particular we can use this to construct a fundamental domain for any principle congruence subgroup $\Gamma(N)$.
Recall in Corollary 3.1.9 we showed $SL_2(\mathbb{Z})/\Gamma(N) \cong SL_2(\mathbb{Z}/N\mathbb{Z})$, where the reduction map $\phi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective with kernel $\Gamma(N)$. If we take an element from the inverse image of each element in $SL_2(\mathbb{Z}/N\mathbb{Z})$ then we get a set of coset representatives.
Proof of claim:
Write $SL_2(\mathbb{Z}/N\mathbb{Z}) = \{a_1, a_2, \ldots, a_t\}$, and consider corresponding $A_1, A_2, \ldots, A_t \in SL_2(\mathbb{Z})$ such that $\phi(A_i) = a_i$. The uniqueness of the a_i's implies $\phi(A_j) \neq \phi(A_i)$ for $i \neq j$.

$$\phi(A) = \phi(B) \iff \phi(A^{-1}B) = I \iff A^{-1}B \in \Gamma(N) \iff A\Gamma(N) = B\Gamma(N)$$

So $A_j\Gamma(N) \neq A_i\Gamma(N)$. Now the isomorphism gives $|SL_2(\mathbb{Z})/\Gamma(N)| = |SL_2(\mathbb{Z}/N\mathbb{Z})|$, hence $\{A_1, A_2, \ldots, A_t\}$ is a complete list of coset representatives.

Example 3.3.4. We can use the above remark to find a fundamental domain for $\Gamma(2)$.
We have $SL_2(\mathbb{Z})/\Gamma(2) \cong SL_2(\mathbb{Z}/2\mathbb{Z})$, where

$$SL_2(\mathbb{Z}/N\mathbb{Z}) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\}$$

In Theorem 3.1.3 a method for finding lift's to $SL_2(\mathbb{Z})$ of matrices in $SL_2(\mathbb{Z}/N\mathbb{Z})$. With $SL_2(\mathbb{Z}/2\mathbb{Z})$ it is simple enough to be done by inspection or the following method. For each $a \in SL_2(\mathbb{Z}/N\mathbb{Z})$, $\det(a) \equiv \mod 2 \implies \det(a) = \pm 1$, and each entry is just one or zero, finding a lift will involve just a sign change of one entry. One natural set of lifts(by the above) is,

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

Finding the boundaries of the corresponding fundamental domain directly can be made easier by writing the coset representatives as a product of S, T. The above set can be written(in same order) as

$$\{I, T, TST, TS, S, ST\}$$

Now finding the boundaries just corresponds to repeated inversion and translation. In general it is common to choose the coset representatives such that they can be expressed in as few S, T as possible while having a symmetrical & connected fundamental domain. One such set of coset representatives is,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, T^{-1}ST = \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}$$

Applying these transformations to the boundary lines of the fundamental domain for $SL_2(\mathbb{Z})$, we obtain the fundamental domain shown in figure 3.1.

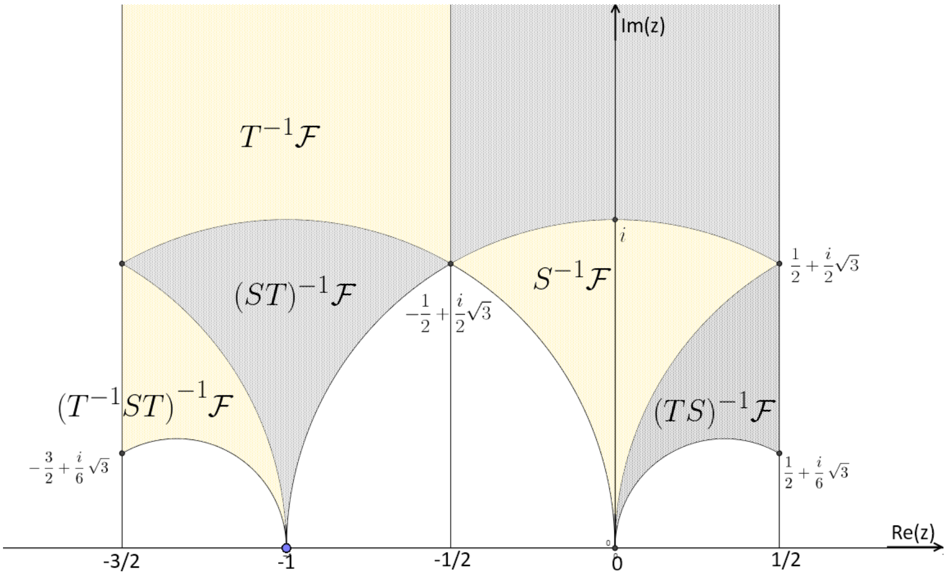

Im(z)
$T^{-1}\mathcal{F}$
i
$\frac{1}{2}+\frac{i}{2}\sqrt{3}$
$(ST)^{-1}\mathcal{F}$
$S^{-1}\mathcal{F}$
$-\frac{1}{2}+\frac{i}{2}\sqrt{3}$
$(T^{-1}ST)^{-1}\mathcal{F}$
$(TS)^{-1}\mathcal{F}$
$-\frac{3}{2}+\frac{i}{6}\sqrt{3}$
$\frac{1}{2}+\frac{i}{6}\sqrt{3}$
Re(z)
-3/2
-1
-1/2
0
1/2

Figure 3.1: Example: A Fundamental domain for $\Gamma(2)$

Remark 3.3.5. In [Verrill, 2001] an algorithm is described to construct fundamental domain's for certain congruence subgroups, like $\Gamma(N)$ and $\Gamma_0(N)$, so that the fundamental domain is connected and so that the triangles are "large" when drawn. The Java tool for drawing fundamental domains described in the paper is available at http://www.math.lsu.edu/ verrill/fundomain/index2.html.

Chapter 4

Non-congruence subgroups of $SL_2(\mathbb{Z})$

Definition 4.0.1. A non-congruence subgroup $SL_2(\mathbb{Z})$ is a finite index subgroup that does not contain $\Gamma(n)$ for any n.

Lemma 4.0.2. *Let G be a group with normal series $G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$, $G_i \trianglelefteq G$. Then the composition factors of G are precisely the union of the composition factors $G/G_1, G_1/G_2, \ldots, G_{r-1}/G_r, G_r$.*

Proof. The case $n = 0$, $G = G_0 = 1$ is trivial. We can proceed by induction on n.
Suppose we have the normal series $G = G_0 \geq G_1 \geq \cdots \geq G_{k+1} = \{1\}$ and that the lemma holds for $n = k$.
One can derive the normal series $G_0 \geq G_1 \geq ... \geq G_{k-1} \geq G_{k+1} = \{1\}$ of length k by removing the term G_k. So by induction hypothesis, the composition factors of G_{k+1} are the union of the composition factors $G/G_1, G_1/G_2, \ldots, G_{k-1}/G_{k+1}, G_{k+1}$.

We need only show the composition factors for G_{k-1} are the union of the composition factors for G_k and G_{k-1}/G_k.
Consider the refinement

$$G_{k-1} = A_0 \trianglelefteq \cdots \trianglelefteq A_q = G_k = B_0 \trianglelefteq \cdots \trianglelefteq B_t = G_{k+1},$$

where the compositions factors A_m/A_{m+1} and B_j/B_{j+1} are simple.
Then since $G_k \triangleleft G_i$ the Third isomorphism theorem gives the normal series $G_{k-1}/G_k = A_0/G_k \trianglelefteq \cdots \trianglelefteq A_q/G_k = \{e\}$, the factor of a factor part of the theorem gives us that $(A_m/H)/(A_{m+1}/H) \cong A_m/A_{m+1}$, so the factors are simple and the series is a composition series. The composition factors of G_{k-1}/H are thus equal to (upto isomorphism) the composition factors A_m/A_{m+1} of G_{k-1}/G_{k+1}

Similarly we can show the composition factors for G_k/G_{k+1} are the composition factors B_j/B_{j+1} of G_{k-1}/G_{k+1}. So the composition factors for G_{k-1}/G_{k+1} are the same as the composition factors for G_{k-1}/g_k and G_k/G_{k+1}.
We have shown the lemma to be true for $n = k+1$ if it is true for $n = k$, so we can conclude it holds for all $n \in \mathbb{N}$ by induction. □

Remark 4.0.3. If we have the internal direct product $G = H_1 \times \cdots \times H_n$, then rewriting the element $h_1 \cdots h_n$ as $(h_1, \ldots, h_n)$ we can construct the external direct product which is isomorphic to G under the map $(h_1, \ldots h_n) \mapsto h_1 \cdots h_n$.
Conversely if G is the external direct product $H_1 \times \cdots \times H_n$ we can define G_i to be the set of all n-tuples of G containing all 1s except (possibly) in ith position. Then $G_i \cong H_i$ and G is the internal direct product of $G_1, \ldots, G_n$. For these reasons many authors do not distinguish between usage of external and internal direct product.

Remark 4.0.4. Suppose we have the groups $G_1, G_2, \ldots, G_n$, and the direct product $G : G_1 \times G_2 \times \cdots \times G_n$. Then we can define the maps

$$\pi_{!G_i} : G \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$
$$\pi_{!G_i}(g_1, \ldots g_n) \mapsto (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$$

Then we can see that the maps are surjective homomorphisms, and have kernel $\{e\} \times \cdots \times \{e\} \times G_i \times \{e\} \times \cdots \times \{e\} \cong G_i$.
This shows each G_i is normal in G.
We can also define the maps

$$\pi_{G_i} : G \to G_i \quad , \quad \pi_{G_i}((g_1, \ldots, g_i, \ldots, g_n)) \mapsto g_i$$

These are also surjective homomorphisms, and have kernel $G_1 \times \cdots \times G_{i-1} \times \{e\} \times G_{i+1} \times \cdots \times G_1$.
We then get the isomorphism

$$G/(G_1 \times \cdots \times G_{i-1} \times \{e\} \times G_{i+1} \times \cdots \times G_1) \cong G_i$$

Lemma 4.0.5. *If $G_1, \ldots, G_n$ are non-trivial finite groups then the composition factors of the direct product $G = G_1 \times \cdots \times G_n$ are precisely the union of composition factors of each $G_1, \ldots, G_1$.*

Proof. We can use the above remark to get a normal series for G,

$$\{e\} \times \cdots \times \{e\} \lhd G_1 \times \{e\} \times \cdots \{e\} \lhd \cdots \lhd G_1 \times G_2 \times \cdots \times G_m$$

We can apply lemma 4.0.2 to conclude that the composition factors for G are the union of composition factors for $(G_1 \times \cdots \times G_n)/(\{G_1\} \times \cdots G_{n-1} \cdots \{e\})$, $(G_1 \times \cdots \times G_{n-1} \times \{e\})/(\{G_1\} \times \cdots G_{n-2} \cdots \{e\} \times \{e\})$, $\ldots (G_1 \times \{e\} \cdots \times \{e\})/(\{e\} \times \cdots \times \{e\})$. The above remark also gives that these are isomorphic to $G_n, G_{n-1}, \ldots, G_1$ respectively. □

□

Lemma 4.0.6. *If S is a finite simple group S, and $G_1, \ldots, G_n$ are non-trivial finite groups, such that S is not a composition factor of any G_i. Then S it is not a composition factor of $G := G_1 \times \cdots \times G_n$. In particular S is not a quotient group of $G_1 \times \cdots G_n$.*

Proof. The Jordan Holder Theorem gives that any two composition series are isomorphic, so if S was a composition factor of G it must be a composition factor of some G_i by lemma 4.0.5, which it is not by hypotheses so we get a contradiction.
If G had a quotient group isomorphic to S, then there would be a normal series $\{e\} \times \cdots \{e\} \trianglelefteq N \trianglelefteq G$ with $G/N \cong S$. This normal series could be extended to a composition series with S as the top composition factor (There are non in-between since $S \cong G/N$ is simple). This is a contradiction to the above.

□

Theorem 4.0.7. *For $n \geq 6$ the alternating group A_n is not (isomorphic to) a quotient group of $SL_2(\mathbb{Z}/N\mathbb{Z})$. for any $N \geq 2$.*

Proof. Write $N = p_1^{r_1} \cdots p_m^{r_m}$, so we can apply Proposition 3.1.6 to get

$$SL_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^{m} SL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z}).$$

So by lemma 4.0.6 it suffices to show that A_n for $n \geq 6$ is not a composition factor of $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ for any prime power p^r.
In the proof lemma 3.1.5 we showed that the reduction map $SL_2(\mathbb{Z}/p^r\mathbb{Z}) \to SL_2(\mathbb{Z}/p\mathbb{Z})$ is onto. Let K be it's kernel, so we have the normal series,

$$\{I_2 \mod p^r\} \trianglelefteq K \trianglelefteq SL_2(\mathbb{Z}/p^r\mathbb{Z})$$

Then we can apply lemma 4.0.2 to say the composition factors of $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ are the composition factors of K and those of $sltznz/K \cong SL_2(\mathbb{Z}/p\mathbb{Z})$(By first isomorphism theorem).
We begin by considering composition factors of K: We have shown in lemma 3.1.5 that the order of $SL_2(\mathbb{Z}/p^r\mathbb{Z}) = p^{3r}(1-1/p^2)$, we can use this to compute the order of K.

$$|K| = |SL_2(\mathbb{Z}/p^r\mathbb{Z})|/|SL_2(\mathbb{Z}/N\mathbb{Z})| = \frac{p^{3r}(1-1/p^2)}{p^3(1-1/p^2)} = p^{3(e-1)}$$

This tells us that K is a p-group, and so it's subgroups are p-groups and thus it's composition factors are p-groups so A_n is not a composition factor for $n \geq 6$ since it is not a p-group.
Now we can consider the composition factors of $SL_2(\mathbb{Z}/p\mathbb{Z})$: We use without proof the known fact that $PSL_2(\mathbb{Z}/p\mathbb{Z})$ is simple for $p \geq 5$. The simplicity gives us the composition series

$\{I_2\} \lhd \{\pm I_2\} \lhd SL_2(\mathbb{Z}/p\mathbb{Z})$, recall $PSL_2(\mathbb{Z}/p\mathbb{Z})/\{\pm I_2\} \cong SL_2(\mathbb{Z}/p\mathbb{Z})$. So we get the composition factors $\mathbb{Z}/2\mathbb{Z}$ and $PSL_2(\mathbb{Z}/p\mathbb{Z})$ for $p \geq 5$. In the case $p = 2$, we have $SL_2(\mathbb{Z}/2\mathbb{Z}) = GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$, and in the case $p = 3$ we have $SL_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\} \cong A_4$, the composition factors of these groups are cyclic (of order 2 or 3).
We have shown that the only case where A_n could possibly be a composition factor of $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ is if $A_n \cong PSL_2(\mathbb{Z}/p\mathbb{Z})$ and $p \geq 5$. We can show this never occurs by comparing the sizes of the two groups.
The group $PSL_2(\mathbb{Z}/p\mathbb{Z})$ has order $|SL_2(\mathbb{Z}/p\mathbb{Z})|/2 = (p^2-1)p/2$, and the group A_n has order $n!/2$, we seek

$$(p-1)p(p+1) = n!$$

If $n < p$ then $n!$ is not divisible by p and we have a contradiction. If $n = p$ when we obtain the equation $p+1 = (p-2)!$, we can check the only solution is $p = n = 5$. If $n = p+1$ then dividing both sides by $(p-1)p(p+1)$ we get $1 = (p-2)!$ so $p = 3$ or $p = 2$, but we need $p \geq 5$. The final case where $n \geq p+2$ then $n! > (p-1)p(p+1)$.
The only solution we found was $n = p = 5$(and indeed it can be shown $PSL_2(\mathbb{Z}/5\mathbb{Z}) \cong A_5$), for $n \geq 6$ the group A_n is not a quotient group of $SL_2(\mathbb{Z}/N\mathbb{Z})$ for any $N \geq 2$.

□

Theorem 4.0.8. *For $n \geq 9$, A_n is a quotient of $SL_2(\mathbb{Z})$.*

Proof. We will actually get $A_n \cong PSL_2(\mathbb{Z})/K$, but since $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I_2\}$ we can use the correspondence theorem to say $K = N/\{\pm I_2\}$ for some $N \lhd SL_2(\mathbb{Z})$. Which by the factor of a factor theorem means we get $SL_2(\mathbb{Z})/N \cong A_n$, and so A_n is a quotient of $SL_2(\mathbb{Z})$.
We use two principal facts to prove this result: A_n (for $n \geq 9$) is generated by two elements of order 2 and 3, and $PSL_2(\mathbb{Z})$ is also freely generated by two elements of order 2 and 3. In 1901, G. A Miller first constructed generating elements of order 2 and 3 for A_n [Miller, 1901].
We showed in Theorem 2.3.2 that S, ST generate $SL_2(\mathbb{Z})$ and so every element in $PSL_2(\mathbb{Z})$ can be written as a product of $x = \bar{S} = S/\{\pm I_2\}$, $y = \bar{ST} = ST\{\pm I_2\}$ and these have order 2 and 3. We can then write any product of x, y in "reduced" form,

$$y^{i_0}xy^{i_1}x\cdots y^{i_{n-1}}xy^{i_n},$$

where the exponents i_j are taken $\mathbb{Z}/3\mathbb{Z}$ and they are nonzero modulo 3 except possibly i_0 and i_n. Now since we have shown $PSL_2(\mathbb{Z})$ to be freely generated it means each such representation is unique.
Following from this, suppose we have another group $G = \langle a, b\rangle$ where a, b have order 2 and 3. A map $f : \{x, y\} \to \{a, b\}$ where $f(x) = a$, $f(y) = b$ and $f' : PSL_2(\mathbb{Z}) \to G$ extends uniquely to a homorphism $f' : PSL_2(\mathbb{Z}) \to G$. I.e there is a unique homorphism f' such that $f'(x) = a$ and $f'(y) = b$
The uniqueness is readily proven. Let $s \in PSL_2(\mathbb{Z})$, then we can write s as a word in in reduced

form x, y, $s = y^{i_0}xy^{i_1}x \cdots y^{i_{n-1}}xy^{i_n}$,

$$\begin{aligned} f'(y^{i_0}xy^{i_1}x \cdots y^{i_n-1}xy^{i_n}) & \overset{f' \text{ hom.}}{=} & f'(y)^{i_0}f'(x)f'(y)^{i_1}f'(x) \cdots f'(y)^{i_{n-1}}f'(x)f'(y)^{i_n} \\ & = & f(y)^{i_0}f(x)f(y)^{i_1}f(x) \cdots f(y)^{i_{n-1}}f(x)f(y)^{i_n} \end{aligned}$$

Since $PSL_2(\mathbb{Z})$ is freely generated by x, y the representation for s is unique and so there is no other possible value for $f'(s)$.
The homomorphism f' is also surjective, given any element $c \in G$ we can write it in "reduced" form as a word in a, b, $c = a^{j_0}ba^{j_1}b \cdots a^{j_{k-1}}ba^{j_k}$. And then $f'(y^{j_0}xy^{j_1}x \cdots y^{j_{k-1}}xy^{i_k}) = c$.
The First Isomorphism theorem gives us that $PSL_2(\mathbb{Z})/ker(f') \cong A_n$. □

Example 4.0.9. The group A_9 turns out to be generated by

$$(14)(29)(37)(56) \text{ and } (123)(456)(789),$$

so one surjective homorphism from $SL_2(\mathbb{Z})$ to A_9 is the composite map $SL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}) \to A_9$ where the first map is reduction $\mod \{\pm I_2\}$ and the second is determined by $\bar{S} \mapsto (14)(29)(37)(56)$ and $\bar{ST} \mapsto (123)(456)(789)$.
Note this is not going to be the only homomorphism, for example A_9 will also be generated by $((14)(29)(37)(56))^{-1}$ and $(23)(456)(789)$ so we can define another composite map with $\bar{S} \mapsto ((14)(29)(37)(56))^{-1}$ instead.

Corollary 4.0.10. *Let $\phi : SL_2(\mathbb{Z}) \to A_n$ be a surjective homomorphism. Then the kernel of ϕ is a non-congruence subgroup.*

Proof. Let $\phi : SL_2(\mathbb{Z}) \to A_n$ be a surjective homomorphism, with kernel K. So we have $SL_2(\mathbb{Z})/K \cong A_n$. The kernel, K will have finite index of order $|A_n| = n!/2$. Suppose we had $\Gamma(N) \subset K$. Recall kernels of homorphisms are normal subgroups so we get the normal series, $\{I_2\} \subset \Gamma(N) \subset K \subset SL_2(\mathbb{Z})$. We can apply the Factor of a Factor theorem to say $(SL_2(\mathbb{Z})/\Gamma(N))/(K/\Gamma(N)) \cong SL_2(\mathbb{Z})/K \cong A_n$. Then since $SL_2(\mathbb{Z})/\Gamma(N) \cong SL_2(\mathbb{Z}/N\mathbb{Z})$, we arrive at

$$SL_2(\mathbb{Z}/N\mathbb{Z})/(K/\Gamma(N) \cong A_n.$$

This implies A_n is a quotient group of $SL_2(\mathbb{Z}/N\mathbb{Z})$ but this raises a contradiction by Theorem 4.0.7. So the kernel K is a finite index non-congruence subgroup of $SL_2(\mathbb{Z})$. □

Remark 4.0.11. We can construct matrices in the $\ker \phi$ non-congruence subgroup and also check if matrices are in it. For $n \geq 9$ pick two elements x and y in A_n or respective orders 2 and 3 such that $A_n = \langle x, y \rangle$. To construct a matrix in the subgroup, take an element $a \in A_n$ such that it can be written as a "reduced" word in x, y in two different ways,

$$a = y^{i_0}xy^{i_1}x \cdots y^{i_{n-1}}xy^{i_n} = y^{j_0}xy^{j_1}x \cdots y^{j_{k-1}}xy^{j_k}$$

(This is possible since A_n is not freely generated). The product of the first word and the inverse of the second will be the identity.

$$I = y^{i_0}xy^{i_1}x\cdots y^{i_{n-1}}xy^{i_n}(y^{-j_k}xy^{-j_{k-1}}\cdots xy^{-j_1}xy^{-j_0})$$

Now replace each x, y by S, ST respectively and you get matrix, A, in the kernel of the map ϕ. I.e

$$A = (ST)^{i_0}S(ST)^{i_1}S\cdots(ST)^{i_{n-1}}S(ST)^{i_n}\cdot(ST)^{-j_k}S(ST)^{-j_{k-1}}\cdots S(ST)^{-j_1}S(ST)^{-j_0}$$

The matrix will not be the identity matrix since $PSL_2(\mathbb{Z})$ is freely generated.
In the reverse direction, take a matrix $A \in SL_2(\mathbb{Z})$ and write it (up to an overall sign) as a product of S and ST. Turn that word in S and ST into a word in x and y. The matrices whose corresponding word in x and y is trivial form a non-congruence subgroup of $SL_2(\mathbb{Z})$.

More general algorithms are known that could find the generators of $\ker\phi$ but are beyond the scope of this project. It would be an interesting exercise to try this in the future, perhaps with use of computer algebra systems like GAP.

Remark 4.0.12. The procedures used in the proofs of Theorems 4.0.7 & 4.0.8 in order to construct a non congruence subgroup can be generalized in order to find other non-congruence subgroups.
The steps are the same, we must find a finite simple non-abelian group that is not a quotient of $SL_2(\mathbb{Z}/N\mathbb{Z})$ but is a quotient of $SL_2(\mathbb{Z})$, then by the same steps as in 4.0.10, this group is isomorphic to $SL_2(\mathbb{Z})/N$ where N is a non-congruence subgroup.
In order to show a finite simple non-abelian group is not a quotient of $SL_2(\mathbb{Z}/N\mathbb{Z})$ we have shown it is sufficient to show it is not isomorphic to $PSL_2(\mathbb{Z}/p\mathbb{Z})$ for some prime $p \geq 5$ where $p|N$.
In order to show it is a quotient of $SL_2(\mathbb{Z})$ we have shown it to be sufficient that it is generated by a pair of elements with order 2 and 3.

The above sufficient conditions in order to find a non-congruence subgroup are actually satisfied by most non-abelian finite simple groups. The classification of finite simple groups allows us to find many groups of this form.

Remark 4.0.13. The classification of finite simple groups gave a result that all non-abelian finite simple groups have rank 2. I.e they can all be generated by two elements. We desire that the groups are so called (2,3)-generated, I.e that they can be generated by an element of order 2 and 3. The results about (2,3)-generated groups are taken from the book Groups of Lie Type and Their Geometries[Kantor and Di Martino, 1995]. We have already stated that the alternating groups A_n for $n \geq 9$ are all (2,3)-generated.

In 1989 it was shown by Woldar that the non-abelian finite simple groups belonging to the family called Sporadic groups are all (2,3) generated with the exception of the groups denoted M_{11}, M_{22}, M_{23}, McL.
In 1990 Malle showed that the Chevalley groups $G_2(q)$ and the twisted groups ${}^2G_2(q),{}^3D_4(q)$ and ${}^2F_4(q)$ are (2,3)-generated.

Due to the classification of finite simple groups it is known that none of these are isomorphic to $PSL_2(\mathbb{Z}/p\mathbb{Z})$ for any prime $p \geq 5$ so none of them are quotients of $SL_2(\mathbb{Z}/N\mathbb{Z})$ where $P|N$. So for each of the groups G above satisfying both conditions, we can construct a surjective homomorphism $\phi : SL_2(\mathbb{Z}) \to G$ and the kernel of ϕ will be a finite-index non-congruence subgroup.

The proof of the following Theorem was derived from Alperin [Alperin, 1993].

Theorem 4.0.14. *The group $PSL_2(\mathbb{Z})$ is freely generated by two elements of order two and three. I.e $PSL_2(\mathbb{Z}) \cong C_2 * C_3$.*

Proof. We consider the action of $PSL_2(\mathbb{Z})$ by linear fractional transformations on the extended complex plane, like discussed in Chapter 2. In particular it's action on the irrational numbers. Explicitly if z is an irrational number and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, we have the action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

We use irrational numbers since unlike rational numbers the denominator will never be zero, since if it was zero then would have $cz + d = 0 \implies z = -d/c\mathbb{Q}$ which is a contradiction.
The action also preserves irrationality: Suppose for some irrational z and some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ we had $\frac{az+b}{cz+d} = m/n$ with $m/n \in \mathbb{Q}$ and $\gcd(m,n) = 1$. Then we could rearrange to get $z(ay - cx) = dx - by$. Now since $(x,y) = 1$, we get $ay - cx = 0 \iff a = x, c = y$. If then must also have $d = y, b = x$, so $ad - bc = xy - xy = 0$ which is a contradiction, so $ay - cx \neq 0$. This means we could write $z = \frac{dx-by}{ay-cx} \in \mathbb{Q}$ which is a contradiction.

We have shown in Corollary 2.3.2 that S, ST are matrices of order 2 and 3 (in $PSL_2(\mathbb{Z})$) that generate $PSL_2(\mathbb{Z})$, so we also have that $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ are matrices of order 2 and 3 that generate $PSL_2(\mathbb{Z})$. Their action on the irrational numbers is,

$$\begin{aligned} S(z) &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}(z) = \frac{-1}{z} \\ TS(z) &= \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}(z) = \frac{z-1}{z} \\ (TS)^{-1}(z) &= \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}(z) = \frac{1}{1-z} \end{aligned}$$

Alternating word are of the form $S^{k_1}(TS)^{j_1}S^{k_2}(TS)^{j_1}\cdots S^{k_n}(TS)^{j_n}$, where $j_i, k_i \neq 0$. In order to prove $PSL_2(\mathbb{Z})$ is a free group we show that if we take a word in $\{S, TS, (TS)^{-1}\}$ that is alternating from S to $(TS)^{\pm 1}$ then is not the identity. This is called the alternating word characterization and is equivalent to the definition a free group. (If we could find an alternating word that is the identity then the group would not be free. Conversely if the group was not free then we could find an element that can be written as two distinct alternating words, so the inverse of the first times the second is an alternating word representation for the identity).
We make use of the following properties of the action of S and $(TS)^{\pm 1}$. Let us denote $\mathcal{P}$ as the set of positive irrationals and $\mathcal{N}$ as the set of negative irrationals. We an observe that,

$$S(z) = -1/z \implies S(\mathcal{P}) \subset \mathcal{N}$$

and,

$$(TS)(z) = 1 - \frac{1}{z} \text{ and } (TS)^{-1}(z) = \frac{1}{1-z} \implies (TS)^{\pm 1}(\mathcal{N}) \subset \mathcal{P}.$$

suppose we have a word w that is alternating from $\{S\}$ to $\{(TS)^{\pm 1}\}$. The core idea is that we can use the alternating effect to determine whether $w(\mathcal{P})$ or $w(\mathcal{N})$ are subsets of $\mathcal{P}$ or $\mathcal{N}$. For notation we use, $\alpha = S, \beta = TS$

If the word has odd length, then it either begins and ends with α or begins and ends with β^{-1}.
In the first case we can consider $w(\mathcal{P}) = \alpha(\beta^{i_0}\alpha)\cdots(\beta^{i_k}\alpha)(\mathcal{P})$. For each pair we have $(\beta^{\pm 1}\alpha)(\mathcal{P}) \subset (\beta^{\pm 1})(\mathcal{N}) \subset \mathcal{P}$. So we are left with $\alpha(\mathcal{P}) \subset \mathcal{N}$, i.e $w(\mathcal{P}) \subset \mathcal{N}$.
In the second case we can consider $w(\mathcal{N}) = \beta^{i_0}(\alpha\beta^{i_1})\cdots(\alpha\beta^{i_n})(\mathcal{N})$. For each pair we have $(\beta^{\pm 1}\alpha)(\mathcal{N}) \subset \mathcal{N}$. So we are left with $\beta^{i_0}(\mathcal{N}) \subset \mathcal{P}$, i.e $w(\mathcal{N}) \subset \mathcal{P}$.

If the word has even length, then it either begins with α and ends with $\beta^{\pm 1}$ or vice versa. If it begins with α we can take the conjugate by α so we need only consider the one case, we will reconcile this afterwords.
In the first case, $w = \beta\cdots\alpha$. We can use the same "pairing" reasoning as above to get $w(\mathcal{P}) \subset \beta(\mathcal{N})$ which by looking at the function β we can see is the set of positive irrationals

greater than one.
In the other case, $w = \beta^{-1} \cdots \alpha$, and similarly we get $W(\mathcal{P}) \subset \beta^{-1}(\mathcal{N})$, this is the set of positive irrationals less than one.

We have shown that in all cases there will exist an irrational z such that $w(z) \neq z$. (Example: if w is an even length word beginning with β and we take $z = \sqrt{2}$, we've shown $w(z) < 1$ but $\sqrt{2} > 1$ so $w(z) \neq z$).
In conclusion we have shown for any word w that is alternating from $\{S\}$ to $\{(TS)^{\pm 1}\}$ it is not the identity. (In the case of taking the conjugate, if $\alpha^{-1} w \alpha \neq I_2 \implies w \neq I_2$). So by the alternating word characterization we get $PSL_2(\mathbb{Z}) \cong C_2 * C_3$. □

4.0.1 More examples of non congruence subgroups

The following section is from Chapter 3 in the book *The congruence subgroup problem: an elementary approach aimed at applications* [Sury, 2003].

Example 4.0.15. It's possible to give a more explicit construction of a non-congruence subgroup.
It is shown in [Sury, 2003] that the group G generated by $A := T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $B := U^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ is free and has index 2 in $\Gamma(2)$.
For any word w in A, B we may define the T^2-exponent $E_A(w) : G \to \mathbb{Z}$ of w to be the sum of the exponents of A occurring in w.
We can show this defines a homomorphism from G to $\mathbb{Z}$: For any $w \in G$ there is a unique representation, excluding trivial variations in A, B, since G is a free group. The trivial variations, eg $w = ABA = A(AA^{-1})BA$ cancel out and do not affect $E_A(w)$, this makes the map well defined.
Let $w_1, w_2 \in G$, then the product $W_1 w_2$ can simply be thought of as a concatenation of the two words and as a result we get $E_A(w_1 w_2) = E_A(w_1) + E_A(w_2)$.

For any integer $l \geq 1$, let us define

$$\Gamma_l^A = \{g \in G \, : \, E_A(g) \equiv 0 \mod l\} = Ker(G \to \mathbb{Z} \to \mathbb{Z}/l\mathbb{Z})$$

We claim that Γ_l^A is a non-congruence subgroup if l is not a power of 2.
Now since $\Gamma(lt) \subset \Gamma(t)$ it suffices to show $\Gamma(tl) \not\subset \Gamma_l$ for any t. We can write $l = 2^q * k$ where $k > 1$ odd. From this we can rewrite $ln = 2^q kt = 2^m kn$ with n odd. For the sake of contradiction let us suppose $\Gamma(2^t kn) \subset \Gamma_l^A$ for some $m \geq 0$ and odd n.
The integers $2^m 5kn$ and $5kn - 4$ are comprime, 2 is not a common divisor since $5kn - 4$ is odd,

$$\begin{tikzcd}
& SL_2(\mathbb{Z}) \arrow[d, dash] & \\
& G \arrow[dl, dash] \arrow[dr, dash] & \\
\Gamma_l^A \arrow[dr, dash] & & \Gamma(2) \arrow[dl, dash] \\
& \{I_2\} &
\end{tikzcd}$$

Figure 4.1: Hasse diagram

and also if an odd prime $p|2^m 5kn \implies p|5kn$ so it will not divide $5kn-4$. There exists an integer s such that $s(5kn-4) \equiv 1 \mod 2^m 5kn$, i.e $s(5kn-4) = 1 + (2^m 5kn)h$ for some $h \in \mathbb{Z}$. If we consider this equation modulo 5, we get $s \equiv 1 \mod 5$. Let us write $s = 5r+1$.
The matrix $P = B^r ABA^{kn-1} = \begin{pmatrix} 5 & 2(5kn-4) \\ 2s & \delta \end{pmatrix} \in G$ for some δ. Note that the condition on the determinant $\det(P) = 1$ gives $\delta \equiv 1 \mod 2^m kn$, $(\star)$.
We can also consider the matrix $Q = A^{5kn-4}B^s = \begin{pmatrix} \alpha & 2(5kn-4) \\ 2s & 1 \end{pmatrix} \in G$ for some α. Again the condition on the determinant is $5\delta - 4s(5kn-4) = 1$, now consider this modulo $2^m 5kn$ and use $(\star)$, to get $5\delta \equiv 5 \mod 2^m 5kn$. This implies that $\alpha \equiv 5 \mod 2^m 5kn \implies \alpha \equiv 5 \mod 2^m kn$.

Therefore we can see by considering each entry that $P \equiv Q \mod 2^m kn$. In other words, $PQ^{-1} \in \Gamma(2^m kn)$. But, $E_A(PQ^{-1}) = 1 + (kn-1) + 4 - 5kn = -4kn + 4 \equiv 4 \not\equiv 0 \mod k$.Hence $E_A(PQ^{-1}) \not\equiv 0 \mod l$. This contradicts our assumption that $\Gamma(2^m kn) \subset \Gamma_l^A$. Hence, Γ_l^A cannot be a congruence subgroup.

We can determine the index of Γ_l^A. From figure 4.1 we have,

$$[SL_2(\mathbb{Z}) : \Gamma_l^A] = [SL_2(\mathbb{Z}) : G][G : \Gamma_l^A] = [SL_2(\mathbb{Z}) : G] \cdot |\mathbb{Z}/l\mathbb{Z}| = [SL_2(\mathbb{Z}) : G] \cdot l$$

Also,

$$[SL_2(\mathbb{Z}) : G] = \frac{[SL_2(\mathbb{Z}) : \Gamma(2)]}{[G : \Gamma(2)]} = \frac{6}{2} = 3.$$

So we have $[SL_2(\mathbb{Z}) : \Gamma_l^A] = 3l$.

4.0.2 Local versus index - a criterion

Theorem 4.0.16. *'Wohlfahrt's criterion'*
Let $G \leq SL_2(\mathbb{Z})$ be a subgroup of finite index. Suppose n is a positive integer such that $G \supset \gamma \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \gamma^{-1}$ for every $\gamma \in SL_2(\mathbb{Z})$. Then, G is a congruence subgroup if, and only if, $G \geq \Gamma(n)$. (The notation $G \geq H$ means H is a subgroup of G.)

Proof. If $G \geq \Gamma(n)$ then by definition it is a congruence subgroup.

For the reverse implication let us assume that G is a congruence subgroup, $G \geq \Gamma(m)$ for some m, and that there is a n such that $G \supset \gamma \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \gamma^{-1}$ for every $\gamma \in sltz$. (Note in particular $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in G$). We wish to show that $G \geq \Gamma(n)$.

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n)$. From the determinant we get $\det(g) = ad - bc = 1 \implies (a, c) = 1$ and also since $g \in \Gamma(n)$ we have $n|c$ so $(a, nc) = 1$. From Lemma 3.1.2 we can find $x \in \mathbb{Z}$ such that $(a + ncx, m) = 1$. Therefore, there exists y such that $y(a + ncx) \equiv 1 \mod m$ $(\star)$.

Now let g_1 be the product,

$$g_1 = \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix} g = \begin{pmatrix} a + ncx & b + ndx \\ c & d \end{pmatrix} \in \Gamma(n)$$

Moreover from the assumption about G, we have for any integer z, if we let,

$$g_2 := \begin{pmatrix} 1 + nz & -n \\ nz^2 & 1 - nz \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -z & 1 \end{pmatrix}$$

Then the matrix g_2 is in G since it is the inverse of a matrix of the form $\gamma \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \gamma^{-1}$n and $g_2 \in \Gamma(n)$.

We have $g_2 g_1 = \begin{pmatrix} (1 + nz)(a + ncx) - nc & \star \\ \star & \star \end{pmatrix}$.

If we choose $z = y(c(1 - x) + \frac{1-a}{n})$, we get

$$\begin{aligned}
(1 + nz)(a + ncx) - nc &= (1 + ny(c(1 - x) + \frac{1 - a}{n})(a + ncx) - nc \\
&= a + ncx + ny(a + ncx)(c(1 - x) + \frac{1 - a}{n} \\
\text{use } (\star) &= a + ncx + n(1 + mt)(c(1 - x) + \frac{1 - a}{n} \text{ for some } t \in \mathbb{Z} \\
&= a + ncx + nc - ncx + 1 - a + nmt(c(1 - x)) + mt(1 - a) \\
&= 1 + (1 - a)mt + nmt(c(1 - x)) \\
(a \equiv 1 \mod n) &\equiv 1 \mod mn
\end{aligned}$$

Let

$$h = \begin{pmatrix} 1 + nz & -n \\ nz^2 & 1 - nz \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -z & 1 \end{pmatrix} \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix}, \quad z = y(c(1-x)+\frac{1 - a}{n}).$$

Then by inspection we see $h \in G \cap \Gamma(N)$. Now consider $hg \in \Gamma(n)$.

The matrix hg can be written in the form $\begin{pmatrix} \star & nu \\ nv & \star \end{pmatrix}$ since $hg \in \Gamma(n)$.

From the work above we also have $hg \equiv \begin{pmatrix} 1 & \star \\ \star & \star \end{pmatrix} \mod mn$. So we combine these to get $hg \equiv \gamma = \begin{pmatrix} 1 & nu \\ nv & \star \end{pmatrix} \mod mn$.

The condition on the determinant gives $\gamma \equiv \begin{pmatrix} 1 & nu \\ nv & 1+n^2uv \end{pmatrix} \mod mn$. We may decompose this as

$$\begin{aligned} \gamma &\equiv \begin{pmatrix} 1 & 0 \\ nv & 1 \end{pmatrix} \begin{pmatrix} 1 & nu \\ 0 & 1 \end{pmatrix} \\ &\equiv \begin{pmatrix} 0 & 1 \\ v & 0 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ v & 0 \end{pmatrix}^{-1} \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

So if consider $\gamma' = \begin{pmatrix} 1 & nu \\ nv & 1+n^2uv \end{pmatrix} \equiv \gamma$ be an element in $SL_2(\mathbb{Z})$, then $\gamma' \in G$.

We use, $\gamma^{-1}hg \equiv I_2 \mod mn$, to say $\gamma'^{-1}hg \in \Gamma(mn) \leq \Gamma(m) \leq G$. Finally since $\gamma', g \in G$ we can conclude $g \in G$ and so $\Gamma(n) \leq G$. □

Example 4.0.17. We can use the above criterion to obtain another example of a non-congruence subgroup.

Let us recall the homomorphism $E_A : w(A,B) \to \mathbb{Z}$ from Example 4.0.15, and define $E_B : w(A,B) \to \mathbb{Z}$ similarly, as the sum of the exponents of B occurring in a word w. From these we can define a new homorphism, $E_{A,B} : w(A,B) \to \mathbb{Z} \times \mathbb{Z}$, where $E_{A,B}(w) = (E_A(w), E_B(w))$. For a positive integer l let us define

$$\begin{aligned} \Gamma_l^{A,B} &= \{g \in w(A,B) : E_A(g) \equiv E_B(g) \equiv 0 \mod l\} \\ \ker(w(A,B) &\to \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \end{aligned}$$

This group is a subgroup of the non-congruence subgroup, Γ_l^A from example 4.0.15.

We claim: If l is not a power of 2. then Γ_l is not a congruence subgroup.
If it were a congruence subgroup, then $\Gamma_p \geq \Gamma_l$ would also be a congruence subgroup for any odd prime divisor p of l.

Consider the matrix, $A^{2p} = \begin{pmatrix} 1 & 2p \\ 0 & 1 \end{pmatrix} \in \Gamma_p$, then for any $\gamma \in SL_2(\mathbb{Z})$ we have $E_A(\gamma A^p \gamma^{-1}) = E_A(\gamma) + E_A(A^p) + E_A(\gamma^{-1}) = E_A(\gamma) + E_A(A^p) - E_A(\gamma) = E_A(A^p) = p \equiv 0 \mod p$, and similarly $E_B(\gamma A^p \gamma^{-1}) = E_B(\gamma A^p) = 0 \equiv 0 \mod p$. So $\gamma A^p \gamma^{-1} \in \Gamma_p$ and the criterion in Theorem 4.0.16, is satisfied for $n = 2p$, thus $\Gamma_p \geq \Gamma(2p)$.

Thus the index $[SL_2(\mathbb{Z}) : \Gamma_p]$ divides $[SL_2(\mathbb{Z}) : \Gamma(2p)]$. We will see that this gives a contradiction.

We obtained an expression for index's of congruence subgroups in Corollary 3.2.10,

$$[SL_2(\mathbb{Z}) : \Gamma(2p)] = (2p)^3 \prod_{p|2p} (1 - 1/p^2) = 8p^3(1 - 1/4)(1 - 1/p^2) = 6p(p^2 - 1)$$

From the presentation of Γ_p as a kernel, we get that the index $[w(A, B) : \Gamma_p] = |\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}| = p^2$. We computed in Example 4.0.15, that $[SL_2(\mathbb{Z}) : w(A, B)] = 3$ so we can combine these two to get $[SL_2(\mathbb{Z}) : \Gamma_p] = 3p^2$.
Suppose then that $[SL_2(\mathbb{Z}) : \Gamma_p]|[SL_2(\mathbb{Z}) : \Gamma(2p)]$, then

$$3p^2 | 6p(p^2 - 1) \implies p|2(p^2 - 1) \overset{\text{p odd}}{\implies} p|(p^2 - 1)$$

This is a contradiction so Γ_l cannot be a congruence subgroup if it contains an odd prime factor.

4.1 Conclusion

For another construction of non-congruence subgroups see [Hsu, 1996], in this a method, based on permutation representations of $PSL_2(\mathbb{Z})$, of identifying congruence subgroups is detailed.
The question of determining whether or not finite-index subgroup of $SL_2(\mathbb{Z})$ that are not congruence subgroups exist, is more generally known as the Congruence Subgroup Problem. We have shown they do exist for $SL_2(\mathbb{Z})$ but it is easy to pose the problem similarly for $SL_n(\mathbb{Z})$. It was actually shown in [Bass et al., 1964] that for $n > 2$ every finite index subgroup of $SL_n(\mathbb{Z})$ are congruence subgroups.
Even further it is possible to define the notion of congruence for more general number fields K, a more general result about $SL_n(\mathcal{O}_K$ is proven in [Bass et al., 1967].

Python code written for this project is available at https://github.com/MarcoForte/UndergradThesis
The code includes, the generating of the images, and implementations of algorithms like those described geometric and algebraic proof that $\langle S, T \rangle = SL_2(\mathbb{Z})$.

References

Roger C Alperin. Psl 2 (z)= z 2* z 3. *The American Mathematical Monthly*, 100(4):385–386, 1993.

H. Bass, J. Milnor, and J. P. Serre. Solution of the congruence subgroup problem for sl(n,z)(n ¿ 2) and sp(2n,z) (n ¿ 1). *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 33(1):59–137, 1967. ISSN 1618-1913. doi: 10.1007/BF02684586. URL http://dx.doi.org/10.1007/BF02684586.

Hyman Bass, Michel Lazard, and Jean-Pierre Serre. Sous-groupes d'indice fini dans $sl\,(n, Z)$. *Bulletin of the American mathematical society*, 70(3):385–392, 1964.

Keith Conrad. Sl2 (z). *Expository Papers, http://www. math. uconn. edu/kconrad/blurbs.*

David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 1984. Wiley Hoboken, 2004.

Tim Hsu. Identifying congruence subgroups of the modular group. *Proceedings of the American Mathematical Society*, 124(5):1351–1359, 1996.

William M Kantor and Lino Di Martino. *Groups of Lie Type and Their Geometries*, volume 207. Cambridge University Press, 1995.

Svetlana Katok. *Fuchsian groups.* University of Chicago press, 1992.

Felix Klein. *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, volume 1. BG Teubner, 1890.

Neal I Koblitz. *Introduction to elliptic curves and modular forms*, volume 97. Springer Science & Business Media, 2012.

G. A. Miller. On the groups generated by two operators. *Bull. Amer. Math. Soc.*, 7(10):424–426, 07 1901. URL http://projecteuclid.org/euclid.bams/1183416688.

Joseph Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012.

Á Seress. Permutation group algorithms, cambridge u. *Press, Cambridge*, 2002.

B Sury. *The congruence subgroup problem: an elementary approach aimed at applications*, volume 24. Hindustan Book Agency, 2003.

Helena Verrill. Fundamental domain drawer. *Java program, http://www. math. lsu. edu/˜ verrill/D d ()(sage. modular. arithgroup. arithgroup_element. ArithmeticSubgroupElement method)*, 36, 2001.

Charles Walkden. Hyperbolic geometry lecture notes, January 2016.