The Modular Group $\mathrm{SL}_2(\mathbb{Z})$ and Its Congruence Subgroups

[Koblitz]: III.1

Linear fractional transformation

Denote by $\mathrm{SL}_2(\mathbb{R})$ (SL stands for special linear group) the group of 2×2 real matrices of determinant 1. The linear fractional transformation of $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \longmapsto \frac{az+b}{cz+d},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty \longmapsto \frac{a}{c} = \lim_{z \to \infty} \begin{pmatrix} a & b \\ c & d \end{pmatrix} z,$$

gives a group action of $\mathrm{SL}_2(\mathbb{R})$ on $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

Recall.

- $\mathrm{PSL}_2(\mathbb{R}) := \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ acts faithfully on $\hat{\mathbb{C}}$.
- For any $g \in \mathrm{PSL}_2(\mathbb{R})$,

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}, \quad \text{where } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

  Hence, $\mathrm{PSL}_2(\mathbb{R})$ acts faithfully on $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

Notations. In this course, we will denote

- $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $\overline{\Gamma} = \mathrm{PSL}_2(\mathbb{Z})$.
- For any $G \leq \mathrm{SL}_2(\mathbb{R})$,

$$\overline{G} = \begin{cases} G/\{\pm I\}, & \text{if } -I \in G, \\ G, & \text{if } -I \notin G. \end{cases}$$

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ be a representation of a linear fractional transformations. When $\gamma \neq \pm I$, there are three possibilities, namely,

- γ has one fixed point on $\mathbb{P}^1(\mathbb{R})$,
- γ has two distinct fixed points on $\mathbb{P}^1(\mathbb{R})$,
- γ has one fixed point in $\mathbb{H}$ and the complex conjugate one in $\bar{\mathbb{H}}$.

Definition. An element $\gamma \in \mathrm{SL}_2(\mathbb{R})$ is

- parabolic if it has one fixed point,
- hyperbolic if it has two distinct fixed points on $\mathbb{P}^1(\mathbb{R})$,
- elliptic if it has a pair of conjugate complex numbers as fixed points.

Lemma. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \pm I \in SL_2(\mathbb{R})$. Then

- γ is parabolic if and only if $|a + d| = 2$,
- γ is hyperbolic if and only if $|a + d| > 2$,
- γ is elliptic if and only if $|a + d| < 2$.

Defintion. A point in $\mathbb{P}^1(\mathbb{R})$ fixed by a parabolic element is called a cusp, and a point in $\mathbb{H}$ fixed by an elliptic element is called an elliptic point.

Congruence Subgroups

Definition. Let G be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ commensurable with $\mathrm{SL}_2(\mathbb{Z})$. If G contains the subgroup

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

for some positive integer N, then Γ is a congruence subgroup. The smallest such positive integer N is the level of G. The group $\Gamma(N)$ is called the principal congruence subgroup of level N.

Facts.

- $\overline{\Gamma}(N) = \begin{cases} \Gamma(N)/\{\pm I\}, & \text{if } N \leq 2, \\ \Gamma(N), & \text{if } N > 2. \end{cases}$
- $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Congruence Subgroups

Let N be a poistive integer. The following two types of congruence subgroups

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\},$$

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

are most often encountered in number theory.

Proposition. We have $\Gamma(N) \lhd \Gamma_1(N) \lhd \Gamma_0(N) \leq SL_2(\mathbb{Z})$.

- $[\Gamma_1(N) : \Gamma(N)] = N$,
- $[\Gamma_0(N) : \Gamma_1(N)] = N \prod_{p|N} (1 - 1/p)$,
- $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p)$.

Moduli Spaces

For a fixed $\tau \in \mathbb{H}$, let L_τ be the lattice $L_\tau := \mathbb{Z}\tau + \mathbb{Z}$ and $E_\tau = \mathbb{C}/L_\tau$.

G	moduli space for G
$\Gamma(N)$	$\{[E_\tau, (\tau/N + L_\tau, 1/N + L_\tau)] : \tau \in \mathbb{H}\}$
$\Gamma_1(N)$	$\{[E_\tau, 1/N + L_\tau] : \tau \in \mathbb{H}\}$
$\Gamma_0(N)$	$\{[E_\tau, \langle 1/N + L_\tau \rangle] : \tau \in \mathbb{H}\}$
$\mathrm{SL}_2(\mathbb{Z})$	$\{[E_\tau] : \tau \in \mathbb{H}\}$

Notation. Two points $[E_\tau, *]$ and $[E_{\tau'}, *']$ are equal if and only if $G\tau = G\tau'$.

Quotient Space	Isomorphism Classes
$\Gamma(N)\backslash\mathbb{H}$	elliptic curve + a "basis" of points of order N
$\Gamma_1(N)\backslash\mathbb{H}$	elliptic curve + a point of order N
$\Gamma_0(N)\backslash\mathbb{H}$	elliptic curve + a cyclic subgroup of order N
$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$	elliptic curve

Fundamental Domain

Example

Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. The fundamental parallelogram

$$\Pi_L := \{a\omega_1 + b\omega_2 : 0 \leq a \leq 1, 0 \leq b \leq 1\}$$

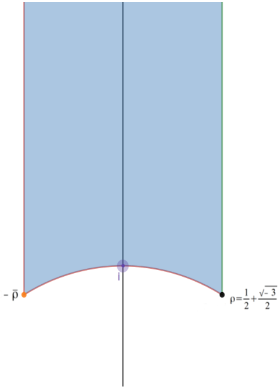
is a fundamental domain for the complex torus $\mathbb{C}/L$.

Definition. Let $G \leq \mathrm{PSL}_2(\mathbb{Z})$ be a discrete subgroup. A set $F \subset \mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ is called a fundamental domain for G if

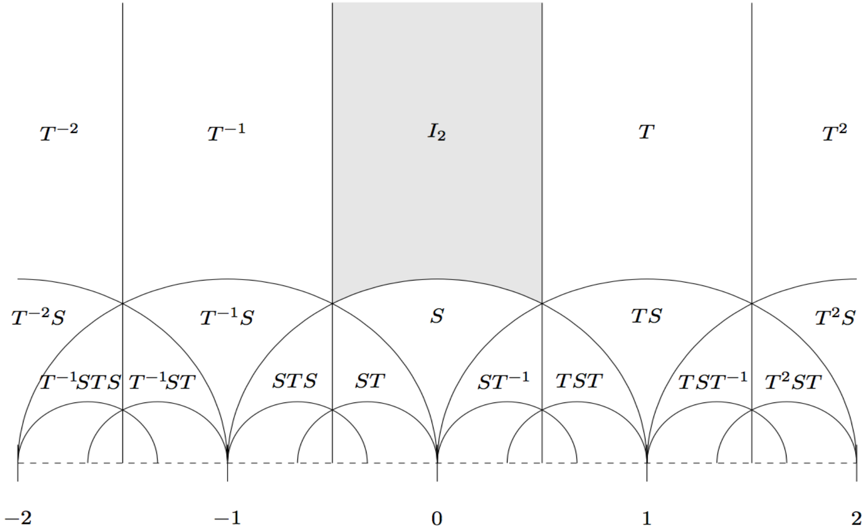
- F is a closed region,
- any points $\tau \in \mathbb{H}^*$ is G-equivalent to a point in F.
- if $\tau \neq \tau' \in F$ are G-equivalent, then τ and τ' belong to the boundary of F.

Proposition III.1.1. A fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$ is

$$F := \{x + iy \in \mathbb{H} : |x| \leq 1/2,\ x^2 + y^2 \geq 1\} \cup \{i\infty\}.$$



(Pictures by Bao Pham)


T^{-2}
T^{-1}
I_2
T
T^2
$T^{-2}S$
$T^{-1}S$
S
TS
T^2S
$T^{-1}STS$
$T^{-1}ST$
STS
ST
ST^{-1}
TST
TST^{-1}
T^2ST
-2
-1
0
1
2

$\mathrm{PSL}_2(\mathbb{Z})$

Proposition III.1.4. The modular group $\mathrm{PSL}_2(\mathbb{Z})$ is generated by

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Key idea: Induction on c + Division Algorithm. For $c > 1$, write $d = cq + r$, $0 < r < c$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} T^{-q} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -aq + b \\ c & r \end{pmatrix}$$

and

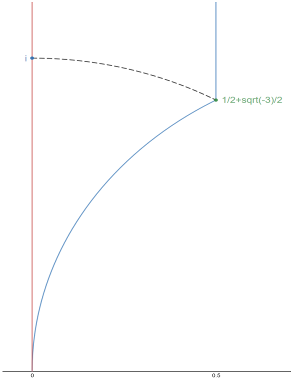
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} T^{-q} S = \begin{pmatrix} a & -aq + b \\ c & r \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -aq + b & -a \\ r & -c \end{pmatrix}.$$

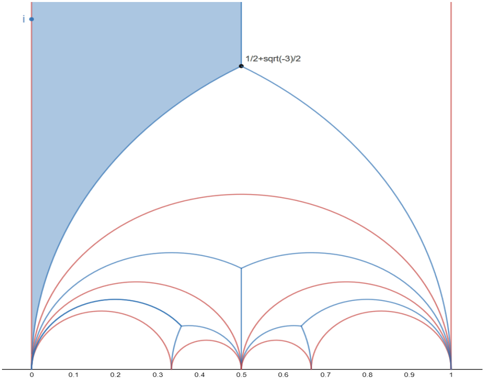
Proposition. The set of cusps of $\mathrm{PSL}_2(\mathbb{Z})$ are $\mathbb{P}^1(\mathbb{Q})$, and the cusps are all equivalent to each other under $\mathrm{PSL}_2(\mathbb{Z})$.

Theorem.

- Every elliptic element of $\mathrm{PSL}_2(\mathbb{Z})$ has order 2 or 3. An element of $\mathrm{PSL}_2(\mathbb{Z})$ has order 2 if and only if its trace is 0. An element has order 3 if and only if its trace has absolute value 1.
- Every elliptic element of order 2 is conjugate to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ in $\mathrm{PSL}_2(\mathbb{Z})$. Every elliptic element of order 3 is conjugate to either $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$.
- $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}$ has only two elliptic points. One is represented by i, which is of order 2, and the other is represented by $e^{\pi i/3}$, which is of order 3.

Here is another choice of fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$ and its related tessellation of $\mathbb{H}^*$.





Proposition. Let F be a fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$. Let G be a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index, and γ_j be its right coset representatives. Then the set

$$\bigcup_j \gamma_j F$$

is a fundamental domain for G.

Advertisement.

- Bao Pham's work: Algorithm Relating to Finite Index Subgroups of the Modular Group.
- Southern Regional Number Theory Conference (3/21-3/22): https://www.math.lsu.edu/srntc/nt2020/