AWS 2021: Modular Groups
Problem Set 2

Lecturer: Lori Watson
Written by: Tyler Genao, Hyun Jong Kim, Zonia Menendez and Sam Mundy (Assistants)

Last updated: February 4, 2021

1 Definitions and Notations

1. Let N be a positive integer. The special linear group $\mathrm{SL}_2(\mathbb{Z})$ has subgroups $\Gamma(N), \Gamma_0(N)$, and $\Gamma_1(N)$ defined as

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$$
$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\}$$
$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

The subgroup $\Gamma(N)$ is called the *principal congruence modular subgroup* of level N and the subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$ are called *modular groups of Hecke type*.

2. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is a congruence subgroup of *level* N.

2 Introductory Problems

Problem 1. Show that any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ has finite index.

Problem 2. Show that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$.

Problem 3. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ reduce to a matrix of the form $\begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix}$ modulo N, where α, δ are relatively prime to N. Show that $\Gamma(N), \Gamma_0(N)$, and $\Gamma_1(N)$ are each closed under conjugation by γ.

Problem 4. Show that $\Gamma_1(N^2) \subset \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma(N) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$.

Problem 5. Show that the map $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \pmod{N}$$

is a group homomorphism.

3 Intermediate Problems

Problem 6 (Lifting an element of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$; Diamond & Shurman, Exercise 1.2.2)**.** Given an integer $N > 1$, we defined the *principal congruence subgroup mod* N as a kernel of reduction,

$$\Gamma(N) := \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})).$$

The goal of this problem is to show that this reduction map is also surjective. Note this would imply that the index

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

Let $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be a matrix. Writing it as $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we know that $ad - bc \equiv 1 \pmod N$. We wish to lift this to a matrix $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, thereby showing that the reduction of γ' modulo N is γ.

a. First, we suppose that $c \neq 0$. Show that $\gcd(c, d, N) = 1$, and that there exist $c', d' \in \mathbb{Z}$ with $c' \equiv c \pmod N$, $d' \equiv d \pmod N$ and $\gcd(c', d') = 1$. (*Hint:* use the Chinese remainder theorem to construct $x \in \mathbb{Z}$ with $x \equiv 1 \pmod p$ for $p \mid \gcd(c, d)$, and $x \equiv 0 \pmod p$ for $p \mid c$ but $p \nmid d$.)

b. Show that there exist $a', b' \in \mathbb{Z}$ with $a' \equiv a \pmod N$, $b' \equiv b \pmod N$ and $a'd' - b'c' = 1$. Use this to construct a lift of γ in $\mathrm{SL}_2(\mathbb{Z})$. (*Hint:* start with computing $a'd' - b'c' = 1$ for arbitrary $a' = a + uN$ and $b' = b + vN$ with $u, v \in \mathbb{Z}$, and then determine which u, v would work, utilizing that $ad' - bc' \equiv 1$ mod N and $\gcd(c, d) = 1$.)

c. Assuming $c = 0$, construct a lift of γ in $\mathrm{SL}_2(\mathbb{Z})$.

Problem 7 (Diamond & Shurman, Exercise 1.2.3)**.**

1. Show that the map $\Gamma_1(N) \longrightarrow \mathbb{Z}/N\mathbb{Z}$ given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto b \pmod N$ surjects and has kernel $\Gamma(N)$.

2. Show that the map $\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \pmod N$ surjects and has kernel $\Gamma_1(N)$.

Problem 8 (Also Diamond & Shurman, Exercise 1.2.3)**.**

1. Show that $[\Gamma_0(N) : \Gamma_1(N)] = \phi(N)$, where $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is Euler's totient function.[1]

2. Using equation (1) from Problem 13, show that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p \mid N} (1 + 1/p)$.

Problem 9 (Computing the size of $\mathrm{GL}_2(\mathbb{F}_q)$)**.** For a prime power $q \in \mathbb{Z}^+$, let us use $\mathbb{F}_q$ to denote the finite field of size q.

For a prime power $q \in \mathbb{Z}^+$ and integer $n \in \mathbb{Z}^+$, show that the cardinality

$$\# \mathrm{GL}_n(\mathbb{F}_q) = \prod_{k=1}^{n} (q^n - q^{k-1}).$$

(*Hint:* A matrix $\gamma \in M_{n \times n}(\mathbb{F}_q)$ is invertible iff its rows are linearly independent over $\mathbb{F}_q$.)

Problem 10 (Automorphism group over a finite product of rings)**.** Recall that any ring R has its *group of automorphisms*

$$\mathrm{Aut}(R) := \{\text{isomorphisms } \varphi : R \xrightarrow{\sim} R\}.$$

a. Suppose $R_1, \ldots, R_n$ are commutative rings with coprime positive characteristic.[2] Show that the automorphism group of their product is the product of their automorphism groups,

$$\mathrm{Aut}(R_1 \times \ldots \times R_n) \cong \mathrm{Aut}(R_1) \times \ldots \times \mathrm{Aut}(R_n).$$

[1] Euler's totient function is usually defined via the following: $\phi(N)$ counts the number of integers between 1 and N which are coprime to N. It is a multiplicative function – meaning $\phi(ab) = \phi(a)\phi(b)$ if $\gcd(a, b) = 1$ – and is such that $\phi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times$.

[2] Recall that the *characteristic* of a ring R is the least integer $p \in \mathbb{Z}^+$ for which $pr = 0$ for all $r \in R$. If no such p exists, we set $p = 0$ and say that R has characteristic zero.

b. Show that for a commutative ring R and an integer $n \in \mathbb{Z}^+$, one has

$$\mathrm{Aut}(R^n) \cong \mathrm{GL}_n(R).$$

c. Find an example of rings R and S for which

$$\mathrm{Aut}(R \times S) \ncong \mathrm{Aut}(R) \times \mathrm{Aut}(S)$$

(*Hint:* The ring homomorphisms we are considering must take multiplicative identities to multiplicative identities).

Problem 11.

a. For any integer $N > 1$, show that the matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

generate $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

b. Let $M \geq 1$ be another integer, and assume M is not divisible by 2 or 3. Show that there are no nontrivial homomorphisms

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/M\mathbb{Z}.$$

If M is divisible by 2 or 3, then there are such homomorphisms, and they all factor through $\mathrm{SL}_2(\mathbb{Z}/N_0\mathbb{Z})$ for some $N_0 \in \{2, 3, 4, 6, 12\}$. Can you find all such homomorphisms $\mathrm{SL}_2(\mathbb{Z}/N_0\mathbb{Z}) \to \mathbb{Z}/M\mathbb{Z}$ for these N_0's? (*Hint:* Where would a matrix

$$\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}^{-1}$$

be sent under such a homomorphism?)

Problem 12. Let p be a prime number. Let $M_2(\mathbb{Z}/p\mathbb{Z})$ be the additive group of 2 by 2 matrices with coefficients in $\mathbb{Z}/p\mathbb{Z}$. If $n > 0$ is an integer, show that $\Gamma(p^n)/\Gamma(p^{n+1})$ is isomorphic to the subgroup of matrices in $M_2(\mathbb{Z}/p\mathbb{Z})$ of trace zero. [*Hint:* Build a map in the opposite direction as follows: Describe $\Gamma(p^n)/\Gamma(p^{n+1})$ as a subgroup of $\mathrm{SL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Then send a trace zero matrix M in $M_2(\mathbb{Z}/p\mathbb{Z})$ to $1 + p^n M$.]

4 Advanced Problems

Problem 13 (Computing the size of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$)**.** This exercise will determine the cardinality of the group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for any integer $N \geq 1$,

$$\#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right). \tag{1}$$

a. Show that the determinant map $\det : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ gives a short exact sequence[3]

$$1 \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/N\mathbb{Z})^\times \to 1.$$

Deduce that the size

$$\#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}{\phi(N)}$$

where $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is Euler's totient function.

[3] In a short exact sequence of groups, each arrow is a group homomorphism, and at each group the image of the preceding map is the kernel of the proceeding map.

b. Using Problem 10 and the Chinese remainder theorem, show that for any integer $N \in \mathbb{Z}^+$, if its factorization into distinct prime powers is

$$N = p_1^{e_1} \cdots p_n^{e_n}$$

then one has

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \ldots \times \mathrm{GL}_2(\mathbb{Z}/p^{e_n}\mathbb{Z}).$$

c. Combining the two previous parts, to compute $\# \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ it suffices to compute both $\phi(p^e)$ and $\# \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ for each prime power $p^e > 1$ that divides N.

Show there exists a short exact sequence of groups

$$1 \to K \to \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1,$$

and determine K explicitly.

d. Compute $\#K$, and then use Problem 9 to determine what $\# \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is.

e. Deduce that for a prime power $p^e \in \mathbb{Z}^+$, one has

$$\# \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}) = p^{3e-2}(p^2 - 1).$$

Show that for any integer $N \in \mathbb{Z}^+$, equation (1) holds.

f. Using Problem 6, compute the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ explicitly.

Problem 14. In the previous problem set we showed that the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

is freely generated by those elements. Let us call this group F. Show that F is a congruence subgroup. (In fact, it contains $\Gamma(4)$.)

Problem 15. Continuing with the notation of Problem 14, let $M > 0$ be an integer and let $\phi : F \to \mathbb{Z}/M\mathbb{Z}$ be any surjective homomorphism. For example, we can define such a homomorphism on generators by declaring

$$\phi\left(\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\right) = 1 \bmod M, \quad \phi\left(\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}\right) = 0 \bmod M.$$

If M is not divisible by 2 or 3 and sufficiently large, show then that the kernel K of ϕ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which is of finite index and not congruence. (*Hints:* Argue by contradiction; if K contains $\Gamma(N)$ for some N, consider the map ϕ induces on $\Gamma(4)/\Gamma(N)$. Use the Chinese remainder theorem to decompose this group based on the prime factorization of N, similarly to Problem 13 b. Then appeal to Problems 11 and 12, using the latter when $p = 2$.)