The modular group and some relatives

Master Course, Spring term 2025

Fernando Chamizo https://matematicas.uam.es/~fernando.chamizo/

Contents. The modular group and its generators. Congruence subgroups. The theta group and its generators. Some connections with elementary number theory.

1.1 The full modular group

Let us start anticipating that modular forms are complex functions having a large group of symmetries related to the humble matrix group (under multiplication)

$$\mathrm{SL}_2(\mathbb{Z})=\big\{\gamma\in\mathcal{M}_{2\times 2}(\mathbb{Z})\,:\,\det(\gamma)=1\big\}$$

that, consequently, is called the *modular group*. The "S" and "L" stand for "special" and "linear". In general, the *special linear group* $\mathrm{SL}_n(R)$ with R a unitary commutative ring is the group of $n\times n$ matrices of determinant 1 with entries in R.

Most authors consider that, instead of $\mathrm{SL}_2(\mathbb{Z})$, the group $\mathrm{PSL}_2(\mathbb{Z})=\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$, where "P" stands for "projective", deserves the name of modular group because it is closer to the symmetries of the classical modular forms. We will only apply this name to $\mathrm{SL}_2(\mathbb{Z})$. In the classic book [6] it is said that $\mathrm{SL}_2(\mathbb{Z})$ is the *homogeneous* modular group and $\mathrm{PSL}_2(\mathbb{Z})$ is the *inhomogeneous* one. The homogeneity is associated to maps mentioned in another section.

We highlight two elements in the modular group

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

Later we will assign a geometric meaning to them. Note that

$$S^2=-I\qquad\text{and}\qquad T^n=\begin{pmatrix}1&n\\0&1\end{pmatrix}\quad\text{for}\quad n\in\mathbb{Z}. \tag{1}$$

In particular, S has order 4 and T has infinite order. We also have the relation $(ST)^3=S^2$. They are two simple elements generating the full group.

Theorem 1.1. *For S and T as before,* $\mathrm{SL}_2(\mathbb{Z})=\langle S,T\rangle$.

Proof. Consider the map $H:\mathrm{SL}_2(\mathbb{Z})\longrightarrow\mathbb{Z}_{\geq 0}$ given by $H(\gamma)=\min\big(|\gamma_{11}|,|\gamma_{21}|\big)$. Assume $\mathrm{SL}_2(\mathbb{Z})\neq\langle S,T\rangle$ and let $\delta\in\mathrm{SL}_2(\mathbb{Z})-\langle S,T\rangle$ with $H(\delta)$ minimal. If $\delta_{21}=0$ it is easy to get

with (1) simple products of powers of S and T giving δ (exercise). Hence $\delta_{21} \neq 0$. Note the relations

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

By the first one, perhaps changing δ into $S\delta$ we can assume $|\delta_{11}| \geq |\delta_{21}| > 0$. In this situation the second relation implies $H(T^n\delta) < H(\delta)$ with n the nearest integer to $-\delta_{11}/\delta_{21}$, contradicting the choice of δ. □

The direct version, without reductio ad absurdum, of the previous proof gives an actual algorithm to express γ in terms of S and T (Exercise 2).

The relation mentioned before between S and T is the only relevant and we have the presentation

$$\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \,:\, S^4 = I,\ (TS)^3 = S^2 \rangle.$$

We do not include a proof here (it can be deduced from [6, Th. 1.2.5] or [8, Th. I.11]). Note that in $\mathrm{PSL}_2(\mathbb{Z})$ we have also $S^2 = I$ and it becomes isomorphic to the free product $C_2 * C_3$ with C_k denotes the cyclic group of order k.

1.2 Congruence subgroups

Arguably, the most important subgroup of $\mathrm{SL}_2(\mathbb{Z})$ in the context of modular forms is the *Hecke congruence subgroup* of level N (here $N \in \mathbb{Z}^+$), defined as

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

To build the theory it is also important the *principal congruence subgroup* of level N given by

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

Any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ is said to be a *congruence group* and its level is the minimum of the values of N with this property. For instance, $\Gamma_0(N)$ is a congruence group and it is pretty easy to check that actually its level is N. A congruence subgroup that appears naturally in the proof of Proposition 1.2 and in some parts of modular form theory consists in dropping the condition $N \mid b$ in the definition of $\Gamma(N)$.

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

Trivially, $\Gamma_0(1) = \Gamma(1) = \Gamma_1(1) = \mathrm{SL}_2(\mathbb{Z})$. Our next target is to compute the index of $\Gamma(N)$ and $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ for $N > 1$.

Proposition 1.2. *If $N > 1$ then $\Gamma(N)$ is a proper normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $\Gamma_0(N)$ is a proper not normal subgroup. Their indexes are*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - p^{-2}\right) \qquad \text{and} \qquad [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + p^{-1}\right)$$

where p runs over the prime numbers.

An immediate consequence is that any congruence subgroup has finite index in $\mathrm{SL}_2(\mathbb{Z})$. The converse is false [1, §6.2.3], [2, §5].

The proof of Proposition 1.2 depends on the following three surjectivity results. All of them are elementary, the first is harder.

Lemma 1.3. *The map $\phi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ given by the reduction modulo N is an* epimorphism *(a surjective homomorphism).*

In general, $\mathrm{SL}_m(\mathbb{Z}) \longrightarrow \mathrm{SL}_m(\mathbb{Z}/N\mathbb{Z})$ is an epimorphism for any m [9, Lemma 1.38].

Proof. It is a homomorphism because matrix product only involves sums and products which are preserved modulo N.

For each element in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ consider an integer matrix γ such that is reduction modulo N is the chosen element. This means

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}) \qquad \text{with} \quad ad - bc = 1 \pmod N.$$

The surjectivity follows if we find $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma' \equiv \gamma \pmod N$. Clearly, $\gcd(a, N) = 1$ or $\gcd(c, N) = 1$. Assume the first possibility, the other is completely similar exchanging the role of a and c. Let M such that $MN \equiv 1 \pmod a$ and take

$$\gamma' = \begin{pmatrix} a & b + Ny \\ c - (c-1)MN & d + Nx \end{pmatrix} \quad \text{with} \quad ax - \big(c - (c-1)MN\big)y = \frac{1 - ad + bc}{N} + (1-c)Mb.$$

The coefficients of x and y in the latter equation are coprime because a divides the coefficient of y minus 1. Then it has integer solutions. Choosing x and y as one of them, we have $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, by the equation, and $\gamma' \equiv \gamma \pmod N$. □

Lemma 1.4. *For $N > 1$, the map $\psi : \Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^*$ assigning to each γ the congruence class of γ_{11} is an epimorphism.*

Proof. Working modulo N the homomorphism condition reduces to note that

$$\delta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \quad \text{has } aa' \text{ as its } \delta_{11} \text{ entry.}$$

The surjectivity is proved choosing γ_{11} in an arbitrary class of $(\mathbb{Z}/N\mathbb{Z})^*$, $\gamma_{12} = 1$, γ_{22} satisfying $\gamma_{11}\gamma_{22} \equiv 1 \pmod N$ and $\gamma_{21} = \gamma_{11}\gamma_{22} - 1$. □

Lemma 1.5. *For $N > 1$, the map $\lambda : \Gamma_1(N) \longrightarrow \mathbb{Z}/N\mathbb{Z}$ assigning to each γ the congruence class of γ_{12} is an epimorphism.*

Proof. As before, working modulo N the homomorphism condition reduces to

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix}.$$

The surjectivity is obvious taking $\gamma_{11} = \gamma_{22} = 1$, $\gamma_{21} = 0$ and γ_{12} arbitrary. □

Proof of Proposition 1.2. Clearly $\Gamma(N) = \mathrm{Ker}(\phi)$ with ϕ as in Lemma 1.3. By the isomorphism theorem, $\Gamma(N) \triangleleft \mathrm{SL}_2(\mathbb{Z})$ and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = \left|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right|$. An argument involving the Chinese remainder theorem shows that this cardinality is given by the claimed formula (Exercise 3).

On the other hand, $\Gamma_1(N) = \mathrm{Ker}(\psi)$ with ψ as in Lemma 1.4 and the isomorphism theorem gives this time $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$ with φ Euler's totient function [7] which equals $N\prod_{p|N}\left(1-p^{-1}\right)$. In the same way, using Lemma 1.5, $\Gamma(N) = \mathrm{Ker}(\lambda)$ and $[\Gamma_1(N) : \Gamma(N)] = N$.

If we substitute these indexes in the relation

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)][\Gamma_0(N) : \Gamma_1(N)][\Gamma_1(N) : \Gamma(N)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)],$$

we can eliminate $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ to get the expected formula. It is an exercise to check $\Gamma_0(N) \not\triangleleft \mathrm{SL}_2(\mathbb{Z})$ for $N > 1$. □

1.3 The theta group

Consider $\overline{S} \in \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ given by the reduction modulo 2 of S. With the notation of Lemma 1.3, the *theta group* is defined as $\Gamma_\theta = \phi^{-1}\left(\langle\overline{S}\rangle\right)$. More explicit equivalent definitions are

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,:\, 2 \mid a+d,\ 2 \mid b+c \right\} \quad \text{and} \quad \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,:\, 2 \mid ac,\ 2 \mid bd \right\}.$$

Before going further, it is important to note that some authors define the theta group as $\Gamma_0(4)$, keeping the notation Γ_θ. Note that this is different from our Γ_θ. The reason for this duplicity is that there are two normalizations of a modular form called θ and both give rise to different groups of symmetries.

The first result about Γ_θ shows that it is just $\Gamma_0(2)$ under a "change of variables". Its proof is a simple exercise.

Lemma 1.6. *The groups Γ_θ and $\Gamma_0(2)$ are conjugate. Namely, $\Gamma_\theta = (ST)^{-1}\Gamma_0(2)ST$.*

The relation to $\mathrm{SL}_2(\mathbb{Z})$ is summarized by

Proposition 1.7. *The theta group is a congruence group of level 2 leading to the right coset decomposition $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_\theta \sqcup \Gamma_\theta T \sqcup \Gamma_\theta TS$. In particular, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_\theta] = 3$.*

Proof. With any of the definitions it is obvious that $\Gamma(2) \subset \Gamma_\theta \neq \mathrm{SL}_2(\mathbb{Z})$ then it is a congruence group of level 2.

By Lemma 1.6 and Proposition 1.2 with $N = 2$, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_\theta] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2)] = 3$. Then the right coset decomposition follows noting that the three cosets are distinct and it is equivalent to check $T, TS, TST^{-1} \notin \Gamma_\theta$. □

The analog of Theorem 1.1 for Γ_θ is

Theorem 1.8. *We have* $\Gamma_\theta = \langle S, T^2 \rangle$.

This raises the question of whether there exists an algorithmic method to find generators of $\Gamma_0(N)$ or, in general, of a congruence group. There is an approach based on the so-called *Farey symbols*. Unfortunately the original reference [4], which introduces them, is quite long and it does not invite to a quick reading. An excerpt is [5]. The Farey symbols are related to the geometric interpretation of the congruence groups that will be covered in a later section. Nowadays we can benefit from the software packages that use them to provide generators of $\Gamma_0(N)$ and $\Gamma(N)$. For instance, the sagemath command `Gamma0(2).generators()` gives generators of $\Gamma_0(2)$ and it allows to obtain a short computer assisted proof of the previous result.

Proof of Theorem 1.8 (computer assisted). Since Lemma 1.6, this sagemath code gives generators of Γ_θ:

```
S = matrix(2,2,[0,-1,1,0])
T = matrix(2,2,[1,1,0,1])
c = S*T
for item in Gamma0(2).generators():
        print()
        print (c.inverse()*item*c)
```

The output is

$$\gamma_1 = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{and} \qquad \gamma_2 = \begin{pmatrix} -2 & -5 \\ 1 & 2 \end{pmatrix}.$$

A calculation shows $\gamma_1 = T^{-2}S^{-1}$ and $\gamma_2 = T^{-2}ST^2$, hence $\Gamma_\theta \subset \langle S, T^2 \rangle$. The reversed inclusion is obvious. □

Here it is another proof appealing only to the covered material.

Proof of Theorem 1.8 (perhaps more complicated than needed). By Theorem 1.1 and recalling that S has finite order, for each $\gamma \in \Gamma_\theta$ there exists a finite integer sequence $\{a_n\}_{n=1}^N$ such that $\gamma = T^{a_N} S T^{a_{N-1}} S \cdots S T^{a_1} S$. If $\Gamma_\theta \neq \langle S, T^2 \rangle$ then some of the a_j are odd. Let us choose in that case an expression of this kind such that $k = \max\{\ell : a_\ell \text{ is odd}\}$ is minimal.

If $k = 1$ we have a contradiction with Proposition 1.7 because $\gamma \in \langle S, T^2 \rangle TS \subset \Gamma_\theta TS$. If $k > 1$, consider U given by the transpose of T. Using the relations $T^{-1}S = SU$, $UTU^{-1} = (T^2S)^{-1}$ and $US = ST^{-1}$ we have

$$T^{a_k} S T^{a_{k-1}} S = T^{1+a_k} S (UTU^{-1})^{a_{k-1}} US = T^{1+a_k} S (T^2 S)^{-a_{k-1}} S T^{-1}.$$

It reduces the value of k (at the expense of increasing N), contradicting its minimality. □

1.4 The modular group and elementary number theory

One of the cornerstones in elementary and very basic number theory is *Euclid's algorithm* and its relation to *Bézout's identity* (by the way, according to [3] this is not a good name).

Given a and c with $c \in \mathbb{Z}^+$, Euclid's algorithm for them consists in iterating

$$r_{n-1} = c_{n-1} r_n + r_{n+1} \qquad \text{with} \quad r_0 = a,\ r_1 = b$$

where c_{n-1} is the quotient and r_{n+1} the remainder when r_{n-1} is divided by r_n. Let us say that r_N is the last nonzero remainder. So, $r_{N+1} = 0$ and the process ends. It turns out that c_n are the *partial quotients* in the *continued fraction* of a/c. In modern notation [7], the *convergents* of a/c are $p_n/q_n = [c_0, c_1, \ldots, c_n]$ for $0 \le n < N$ and $a/c = p_{N-1}/q_{N-1}$.

There is a very easy way of getting the convergents from the partial quotients that can be written in a less easy matrix form as

$$C_n = \begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{where} \quad C_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \quad \text{for} \quad 0 \le 0 < n < N$$

and we use the rather standard convention that $p_{-1} = 1$, $q_{-1} = 0$ to match the case $n = 0$.

If a and c are coprime, then $a/c = p_{N-1}/q_{N-1}$ implies $a = p_{N-1}$ and $c = q_{N-1}$. Taking determinants, $\det(C_{N-1}) = (-1)^N$ and we conclude that

$$(x_0, y_0) = (-1)^N (q_{N-2}, p_{N-2}) \quad \text{ is an integer solution of } \quad ax - cy = 1.$$

We know that all the integer solutions are $(x, y) = (x_0 + mc, y_0 + am)$ with $m \in \mathbb{Z}$.

The equation $ax - cy = 1$ can be rephrased saying that fixing a first column (a, c) of an element of $\mathrm{SL}_2(\mathbb{Z})$, where $c \in \mathbb{Z}^+$ is assumed, the possibilities for the second column are given by (y, x). This allows to "parametrize" or "construct" the modular group via Euclid's algorithm. As this is a little off-topic, we only state a result of this kind without proof. As usual, $\lfloor x \rfloor$ is the *floor function* giving the integral part.

Theorem 1.9. *With the previous notation, given a and $c \in \mathbb{Z}^+$ coprime the product*

$$S^{2\lfloor N/2 \rfloor} T^{c_0} S T^{-c_1} S T^{c_2} S T^{-c_3} S \cdots T^{(-1)^{N-1} c_{N-1}} S$$

gives an element of $\mathrm{SL}_2(\mathbb{Z})$ having (a, c) as its first column and all the matrices with this property are obtained postmultiplying by T^m with $m \in \mathbb{Z}$.

Note that this gives a constructive proof of Theorem 1.1 based on Euclid's algorithm (the cases with $c = 0$ are easy and $c < 0$ is covered multiplying by $S^2 = -I$). Just for illustration, let us apply it to express

$$\gamma = \begin{pmatrix} 18 & -31 \\ 7 & -12 \end{pmatrix}$$

in terms of S and T. Here, $18/7 = [2, 1, 1, 3]$, in particular $N = 4$. The last but one convergent is $p_2/q_2 = [2, 1, 1] = 5/2$, hence

$$T^2 S T^{-1} S T S T^{-3} S = \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix}.$$

To adjust the last column we postmultiply by T^{-2} getting $\gamma = T^2 S T^{-1} S T S T^{-3} S T^{-2}$.

Exercises of lecture 1

Exercise 1. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma_{21} = 0$ show that $\gamma \in \langle T, S\rangle$, as claimed in the proof of Theorem 1.1.

Exercise 2. Using the reduction of H in the proof of Theorem 1.1, for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ one finds $\gamma' \in \langle T, S\rangle$ such that $\gamma'\gamma \in \langle T, S\rangle$ because its 21-entry vanishes. Implement this idea in a sagemath code that for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ outputs a list $n_1, m_1, \ldots, m_k, n_k$ such that $\gamma = T^{n_1}S^{m_1}\cdots T^{n_k}S^{m_k}$.

Exercise 3. Prove that if p is prime and $\alpha \in \mathbb{Z}^+$ then $\left|\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z})\right| = p^{3\alpha} - p^{3\alpha-2}$. Use the Chinese remainder theorem to conclude $\left|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right| = N^3\prod_{p|N}\left(1-p^{-2}\right)$ for $N > 1$.

Exercise 4. Prove $\Gamma_0(N) \not\lhd \mathrm{SL}_2(\mathbb{Z})$ except for $N = 1$.

Exercise 5. Show that the tree definitions of Γ_θ are indeed equivalent.

Exercise 6. Prove Lemma 1.6.

References

[1] H. Cohen and F. Strömberg. *Modular forms*, volume 179 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. A classical approach.

[2] K. Conrad. $\mathrm{SL}_2(\mathbb{Z})$. `https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf`, 2023. Expository papers.

[3] A. Granville. It is not "Bézout's identity". arXiv:2406.15642 [math.HO], 2024.

[4] R. S. Kulkarni. An arithmetic-geometric method in the study of the subgroups of the modular group. *Amer. J. Math.*, 113(6):1053–1133, 1991.

[5] C. A. Kurth and L. Long. Computations with finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ using Farey symbols. In *Advances in algebra and combinatorics*, pages 225–242. World Sci. Publ., Hackensack, NJ, 2008.

[6] R. A. Rankin. *Modular forms and functions*. Cambridge University Press, Cambridge-New York-Melbourne, 1977.

[7] H. E. Rose. *A course in number theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, second edition, 1994.

[8] B. Schoeneberg. *Elliptic modular functions: an introduction*. Die Grundlehren der mathematischen Wissenschaften, Band 203. Springer-Verlag, New York-Heidelberg, 1974. Translated from the German by J. R. Smart and E. A. Schwandt.

[9] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Kanô Memorial Lectures, No. 1. Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971. Publications of the Mathematical Society of Japan, No. 11.