Lecture 1

Introduction

This lecture series is concerned with modular groups and modular curves. Our focus will be in particular on certain congruence subgroups of the modular group $\mathrm{SL}_2(\mathbb{Z})$. An action on $\mathrm{SL}_2(\mathbb{Z})$ on the complex upper half-plane $\mathcal{H}$ gives rise to the curve $Y(1)$, a curve whose points correspond to isomorphism classes of elliptic curves over $\mathbb{C}$. Moreover, certain finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ give rise to other curves – including $Y(N), Y_1(N)$, and $Y_0(N)$ – which parameterize isomorphism classes of elliptic curves with extra torsion data (more on that later). The curves $Y(N), Y_1(N)$, and $Y_0(N)$, and their respective compactifications $X(N), X_1(N)$, and $X_0(N)$, will be our primary focus.

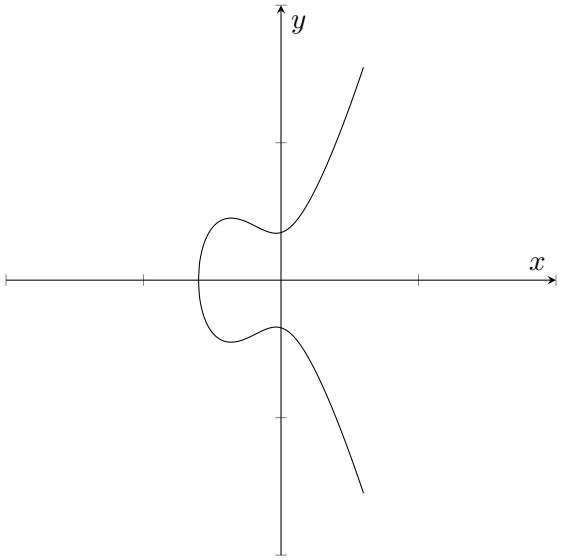
In this first lecture, we will first give an example of the group law on an elliptic curve in action. Then we will discuss the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half-plane.

An elliptic curve over $\mathbb{R}$

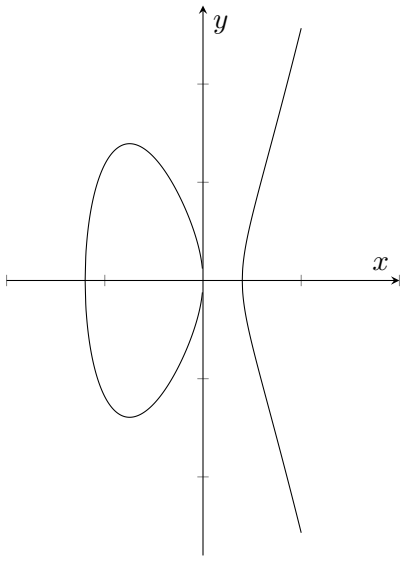
Over a field K of characteristic not equal to 2 or 3 (for example $\mathbb{C}$ or a subfield of $\mathbb{C}$ like $\mathbb{R}$ or $\mathbb{Q}$), an elliptic curve can be described by an equation

$$E : y^2 = x^3 + AX + B,$$

where $A, B \in K$ and $\Delta = -16(4A^3 + 27B^2) \neq 0$. The condition $\Delta = -16(4A^3 + 27B^2) \neq 0$ is equivalent to $x^3 + Ax + B$ having distinct roots. Over $\mathbb{R}$, an elliptic curve given by such an equation will look like one of the following two graphs



(When $x^3 + Ax + B$ has one real root.)



(When $x^3 + Ax + B$ has three real roots.)

When E is given by an equation $y^2 = x^3 + Ax + B$, there is one point at infinity, which we will denote $\mathcal{O}$. It will serve as the identity for the group law. (See the supplemental notes for an illustrated example of the group law.) The group law for an elliptic curve can be expressed using formulas so that the group law is in algebraic terms.

A brief discussion about points of order N

Since we will be interested in what modular curves can help us understand about torsion, we will touch on the notion here. A torsion point P on an elliptic curve is a point for which there is a positive integer N such that

$$\underbrace{P + P + \cdots + P}_{N \text{ times}} = \mathcal{O}$$

. If N is the smallest positive integer for which this occurs, we say that P is a point of order N.

The action of $\mathsf{SL}_2(\mathbb{Z})$ on $\mathcal{H}$

$\mathrm{SL}_2(\mathbb{Z})$ acts on the complex upper-half plane in such a way that the resulting quotient space parameterizes elliptic curves over $\mathbb{C}$ up to isomorphism (meaning each point in the space corresponds to an isomorphism class of elliptic curves). The compactification of the quotient space is, in fact, a compact Riemann surface. This is especially nice since such objects can be understood using methods from both analytic and algebraic geometry.

Definition 1 *The complex upper half-plane is*

$$\mathcal{H} \coloneqq \{\tau \in \mathbb{C} : Im(\tau) > 0\}.$$

Remark 2 *In Lecture 3, we will later see that we can relate elements of $\mathcal{H}$ to elliptic curves over $\mathbb{C}$.*

Definition 3 *The modular group is*

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = 1 \right\}.$$

It is a group under matrix multiplication and has identity $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

There has been mention of an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ several times, but we have not yet said what that action is. $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ by linear fractional transformations: for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$, we define the action as follows:

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

Claim 4 *This is a left group action of $SL_2(\mathbb{Z})$ on $\mathcal{H}$. To prove this claim, you should show that the following three things hold:*

(i) $\gamma\tau \in \mathcal{H}$ for all $\gamma \in SL_2(\mathbb{Z})$ and for all $\tau \in \mathcal{H}$.

(ii) $I_2\tau = \tau$ for all $\tau \in \mathcal{H}$.

(iii) $(\gamma_1\gamma_2)\tau = \gamma_1(\gamma_2\tau)$ for all $\gamma_1, \gamma_2 \in SL_2(\mathbb{Z})$ and for all $\tau \in \mathcal{H}$.

Part (i) of the claim above is a consequence of the following claim:

Claim 5 *For $a, b, c, d \in \mathbb{R}$ with $ad - bc \neq 0$ and for $\tau \in \mathbb{C}$ with $\tau \notin \mathbb{R}$,*

$$Im\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{(ad - bc)Im(\tau)}{|c\tau + d|^2}$$

In the introduction, it is stated that the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ gives rise to a curve $Y(1)$. This curve is the space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. We will be interested in the topology of the space as we move on, but to give a sense of what the elements of this space are, we will review some important sets that result from group actions: orbits.

For $\tau \in \mathcal{H}$, if we think of $\mathrm{SL}_2(\mathbb{Z})$ moving τ around to other points in $\mathcal{H}$, then the orbit is the set of points that τ can be moved to by some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Stated more precisely, the orbit of τ under the action is the set $\mathrm{SL}_2(\mathbb{Z})\tau = \{\tau' \in \mathcal{H} : \tau' = \gamma\tau \text{ for some } \gamma \in \mathrm{SL}_2(\mathbb{Z})\}$.

More generally, if G is a group acting (on the left) on a set X, the orbit of $x \in X$ will be denoted by $Gx = \{y \in X : y = gx \text{ for some } g \in G\}$.The set of orbits of elements of X under the action of G form a partition of X, meaning every element $x \in X$ is contained in exactly one orbit. The quotient $G\backslash X$ is the set of orbits of X under the action of G. In our case, with $G = \mathrm{SL}_2(\mathbb{Z})$ and $X = \mathcal{H}$, $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} = \{\mathrm{SL}_2(\mathbb{Z})\tau : \tau \in \mathcal{H}\}$.

Since (**claim:**) the action of γ and $-\gamma$ is the same (**end of claim**), $\mathrm{PSL}_2(\mathbb{Z}) \coloneqq \mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$ gives essentially the same action on $\mathcal{H}$ and so yields the same quotient space. You will sometimes see $\mathrm{PSL}_2(\mathbb{Z})$ referred to as the modular group, but in this series, by "the modular group," we will mean $\mathrm{SL}_2(\mathbb{Z})$.

A brief diversion into quotient spaces

Though we can talk about a quotient of a set X under a (left or right) action by a group G, when we use the term "quotient space," we are in fact referring to a topological notion. Our particular group, $\mathrm{SL}_2(\mathbb{Z})$ has a topology (the discrete topology), and $\mathcal{H}$ inherits a topology from $\mathbb{C}$. The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ therefore gives us a space that we can justifiably call a quotient space. We will discuss quotient spaces in subsequent lectures, but you have likely seen at least one quotient space before: the unit circle. The group $\mathbb{Z}$ acts on $\mathbb{R}$ (we will say on the right) by addition with the action being defined by (and I apologize for the notation) $x \cdot n = x + n$ for $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. What are the orbits of this group action (which will be the points of the quotient space)? Well, by definition, they are $\mathbb{Z}x = \{y \in \mathbb{R} : y = x + n \text{ for some } n \in \mathbb{Z}\}$, but we can actually identify each of these orbits with a point in the interval $[0, 1)$. Why? Given any real number x, we can find some integer n such that $x+n = y \in [0, 1)$, and this y will be unique in $[0, 1)$. So we can use each number in the interval $[0, 1)$ to (uniquely) represent each distinct orbit $\mathbb{Z}x$. In other words, as a set, the quotient space $\mathbb{R}/\mathbb{Z}$ is in one-to-one correspondence with the interval $[0, 1)$. The topology we get on $[0, 1)$ is not the subspace topology it inherits from $\mathbb{R}$ in this case, but it is still something we recognize. If you are comfortable with the idea of taking the closed interval $[0, 1]$ and identifying 0 and 1, you can see that we get a circle. If that's not quite convincing, then you can instead think of the map $[0, 1) \to \mathbb{C}$, $x \mapsto e^{2\pi i x}$. This gives a homeomorphism from $[0, 1)$ to the unit circle in $\mathbb{C}$. Now, this argument is not complete (one has to show that with the quotient topology $\mathbb{R}/\mathbb{Z}$ is homeomorphic to $[0, 1)$, and hence homeomorphic to the unit circle), but this does give one some hope that quotient spaces need not be mysterious.

On the other hand, we don't get for free that a quotient space is pleasant, even if the space originally acted on is. As an example, $\mathbb{Q}$ can act on $\mathbb{R}$ by addition as well, with $x \cdot r := x + r$ for any $x \in \mathbb{R}$ and any $r \in \mathbb{Q}$. In this case, the quotient space $\mathbb{R}/\mathbb{Q}$ has a very different topology from $\mathbb{R}/\mathbb{Z}$. It has the indiscrete topology, so unlike $\mathbb{R}$ and $\mathbb{R}/\mathbb{Z}$, we cannot separate two distinct points of $\mathbb{R}/\mathbb{Q}$ by open sets. Luckily for us, the quotient space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ will have a much finer topology than the indiscrete topology.

The matrices S and T

In order to understand the quotient space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, it will be helpful to identify a fundamental domain for the action. Before doing so, we introduce to matrices that will help us show that the set we will identify below is a fundamental domain. The two matrices we will use are

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

If $\tau \in \mathcal{H}$, then

$$S\tau = \frac{0\tau - 1}{\tau + 0} = -\frac{1}{\tau},$$

and

$$T\tau = \frac{\tau + 1}{0\tau + 1} = \tau + 1.$$

Claim 6 *(i)* $S^2 = -I_2$ *and* S *has order 4.*

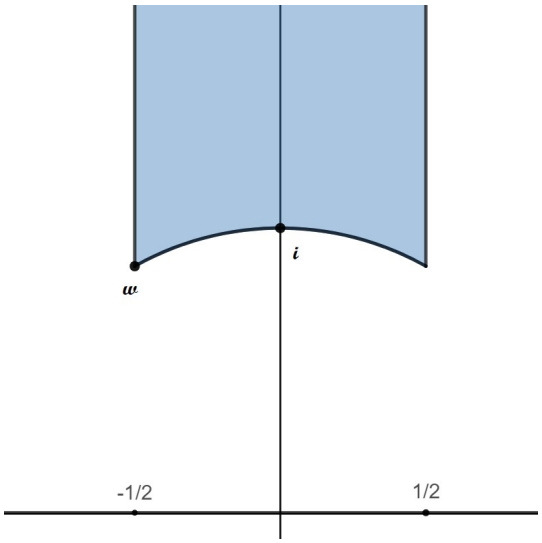
(ii) $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ *for all* $n \in \mathbb{Z}$ *(as a consequence,* T *has infinite order).*

A fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$

We will now identify one fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$, but this set is by no means the only one.

Remark 7 *Note that the set we identify below as a fundamental domain does not satisfy everyone's definition of a fundamental domain. If you require fundamental domains to be open and to have at most one representative of each orbit, then the interior of the set below is a fundamental domain.*

Let $\mathcal{F} :- \{\tau \in \mathcal{H} : |\tau| \geq 1 \text{ and } |\mathrm{Re}(\tau)| \leq 1/2\}$. The set $\mathcal{F}$ is pictured below.



Remark 8 *In the image above,* $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

We now show that $\mathcal{F}$ is a fundamental domain for the $\mathrm{SL}_2(\mathbb{Z})$ action on $\mathcal{H}$.

Proposition 9 *(A) Let* $\tau \in \mathcal{H}$. *Then there is some* $\gamma \in SL_2(\mathbb{Z})$ *such that* $\gamma\tau \in \mathcal{F}$.
(B) If $\tau, \gamma\tau \in \mathcal{F}$ *for some* $\gamma \in SL_2(\mathbb{Z})$ *with* $\tau \neq \gamma\tau$, *then one of the following is true:*
(i) $Re(\tau) = \pm\frac{1}{2}$ *and* $\gamma\tau = \tau + 1$
(ii) $|\tau| = 1$ *and* $\gamma\tau = -\frac{1}{\tau}$.

Proof: (A) Let G be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by S and T, and fix $\tau \in \mathcal{H}$. We will show that there is some $\gamma \in G$ such that $\gamma\tau \in \mathcal{F}$. First, recall that if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then $\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}$. Since τ is fixed and $\mathrm{Im}(\tau) > 0$, there are only finitely many pairs $c, d \in \mathbb{Z}$ such that

$$|c\tau + d| \leq M$$

for any given $M \in \mathbb{Z}^+$. Thus, there is some $\left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & d_0 \end{smallmatrix}\right) = \gamma_0 \in G$ such that $|c_0\tau + d_0|$ is minimal and $\mathrm{Im}(\gamma_0\tau)$ is maximal. For some $n \in \mathbb{Z}$, $\tau' \coloneqq T^n(\gamma_0\tau)$ has $-1/2 \leq \mathrm{Re}(\tau') \leq 1/2$. We claim that $|\tau'| \geq 1$. If not, then $|\tau'| < 1$ gives

$$\mathrm{Im}(S\tau') = \frac{\mathrm{Im}(\tau')}{|\tau'|^2} > \mathrm{Im}(\tau') = \mathrm{Im}(T^n\gamma_0\tau) = \mathrm{Im}(\gamma_0\tau),$$

contradicting our choice of γ_0. Thus $\tau' = (T^n\gamma_0)\tau \in \mathcal{F}$ (and $T^n\gamma_0 \in G$).
(B) Suppose there is some $\gamma \neq \pm I_2$ and some $\tau \in \mathcal{F}$ such that $\gamma\tau \in \mathcal{F}$ also. Without loss of generality, we may assume that $\mathrm{Im}(\gamma\tau) \geq \mathrm{Im}(\tau)$. Writing $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, our assumption that $\mathrm{Im}(\gamma\tau) \geq \mathrm{Im}(\tau)$ implies

$$\mathrm{Im}(\tau) \leq \mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2},$$

so that $|c\tau + d|^2 \leq 1$. Since $\frac{\sqrt{3}}{2} = \mathrm{Im}(\omega) \leq \mathrm{Im}(\tau)$, we must have $|c| \leq \frac{2}{\sqrt{3}}$; as $c \in \mathbb{Z}$, this implies $|c| \leq 1$. We now proceed by cases.

If $c = 0$, then $ad - bc = ad = 1$, so $a = d = \pm 1$ and $\gamma = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$. Then $\gamma\tau = \tau + b$ or $\gamma\tau = \tau - b$. Since both τ and $\gamma\tau$ are in $\mathcal{F}$, we must have $|\mathrm{Re}(\tau) = 1/2$, and since by assumption $b \neq 0$, we must have $b = \pm 1$.

If $c = 1$, let $x = \mathrm{Re}(\tau)$ and $y = \mathrm{Im}(\tau)$. Then $(x+d)^2+y^2 = x^2+2xd+d^2+y^2 = xd+d^2+|\tau|^2 \leq 1$, we have $|d| \leq 1$, and we consider three subcases.

Case $c = 1, d = 0$**:** if $d = 0$, then $|\tau| \geq 1$ and $|c\tau + d|^2 = |\tau| \leq 1$ implies $|\tau| = 1$. Additionally, since $d = 0$ and $ad - bc = -bc = 1$, $b = -1$. Therefore, $\gamma\tau = \frac{a\tau - 1}{\tau} = a - \frac{1}{\tau}$. If $a = 0$, then we are in case (B)(ii), otherwise, $a = \pm 1$ (if $|a| > 1$, then we cannot have both $a - \frac{1}{\tau} \in \mathcal{F}$ and $\left|-\frac{1}{\tau}\right| = 1$). If $a = -1$, then $\tau = \omega$, and $\gamma = (ST)^2 = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, γ fixes ω. If $a = 1$, then $\tau = -\bar{\omega}$ and $\gamma = TS = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and γ fixes $-\bar{\omega}$.

Case $c = 1, d = 1$**:** Again letting $x = \mathrm{Re}(\tau)$ and $y = \mathrm{Im}(\tau)$, note that on the one hand $1 \geq |c\tau + d|^2 = |\tau + 1|^2 = (x+1)^2 + y^2 = x^2 + 2x + 1 + y^2 = (x^2 + y^2) + 2x + 1 = |\tau|^2 + 2x + 1 \geq |\tau|^2$, where in the last inequality, we use $x \geq -1/2$. Since by definition of $\tau \in \mathcal{F}$, we know that $|\tau| \geq 1$, we conclude $|\tau| = 1$. On the other hand, $|\tau|^2 \geq 1 \geq |c\tau+d| = |\tau+1|^2$. Then $x^2+y^2 \geq (x+1)^2+y^2 = x^2 + 2x + 1 + y^2$ holds only if $0 \geq 2x + 1$ or equivalently $-1/2 \geq x$. Thus $x = -1/2$. Since $\tau \in \mathcal{H}$, $|\tau| = 1$ and $\mathrm{Re}(\tau) = -1/2$, $\tau = \omega$. Then since $c = d = 1$, $\gamma = \left(\begin{smallmatrix} a & b \\ 1 & 1 \end{smallmatrix}\right)$, in which case $b = a - 1$, and $\gamma\tau = a - \frac{1}{\omega+1} = a + \omega$. Since $a + \omega \in \mathcal{F}$, we conclude that either $a = 0$, in which case $\gamma = ST$ and γ fixes ω, or $a = 1$ and $\gamma\tau = \omega + 1$.

Case $c = 1, d = -1$**:** Then $1 \geq |\tau - 1|^2 = |\tau|^2 - 2x + 1$ (where $x = \mathrm{Re}(\tau)$ as before). Then since $1/2 \geq x$, we have $1 \geq 2x \geq |\tau|^2 \geq 1$, so $|\tau| = 1$. Similar to above, $|\tau - 1|^2 \leq |\tau|^2$ gives $|\tau|^2 - 2x + 1 \leq |\tau|^2$ so that $x \leq 1/2$, and we conclude $x = 1/2$ and $\tau = -\bar{\omega}$. Since $c = 1$, $d = -1$, we have $\gamma = \left(\begin{smallmatrix} a & b \\ 1 & -1 \end{smallmatrix}\right)$, so $b = -a - 1$. Thefore, $\gamma\tau = a - \frac{1}{-\bar{\omega}-1} = a - \frac{1}{\omega} = a + \omega$. This requires either $a = 0$ so that $\gamma = (TS)^2$ and γ fixes $-\bar{\omega}$, or $a = -1$ and $\gamma\tau = \omega - 1$.

The case for $c = -1$ is similar to the case $c = 1$. □

To end this first lecture, we give a corollary to the above proposition:

Corollary 10 *The matrices S and T generate $SL_2(\mathbb{Z})$.*

Proof: Let G be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by S and T, let τ be any element in the interior of $\mathcal{F}$, and let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. By the proof of part (A) of the proposition, there is some $\gamma' \in G$ such

that $\gamma'(\gamma\tau) \in \mathcal{F}$. By part (B), since both $\gamma'(\gamma\tau) = (\gamma'\gamma)\tau$ and τ are in the interior of $\mathcal{F}$ rather than the boundary, they must be equal. Therefore we must have $\gamma'\gamma = \pm I_2$ so that $\gamma = \pm(\gamma')^{-1}$. Since $S^2 = -I_2 \in G$, we conclude that $\gamma \in G$. $\square$