# MODULAR FORMS LECTURE 5: ELLIPTIC CURVES

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> It is possible to write endlessly on elliptic curves. (This is not a threat.)
>
> Serge Lang

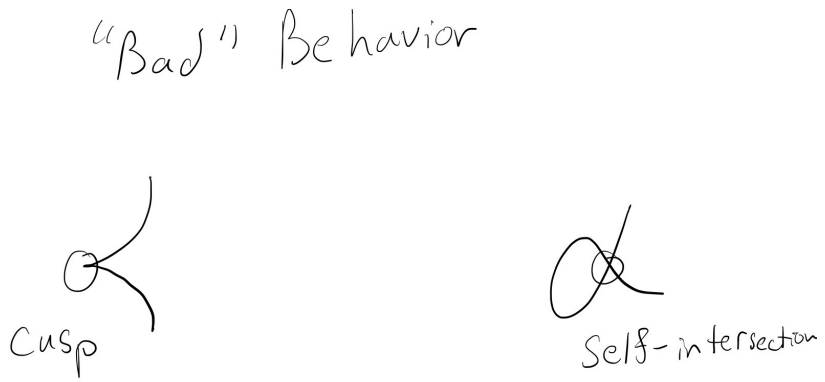
**Definitions.** An **elliptic curve** is a given by an equation of the special shape

$$E\colon y^2 = x^3 + ax + b,$$

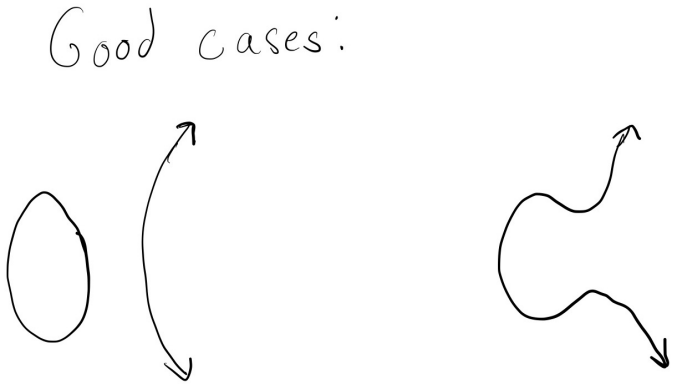
where $a$ and $b$ are fixed. Here, $x, y$ may range over different fields, for example, $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. The set of $K$**-points** over a field $K$ is denoted $E(K)$.

Not all such cubic curves are elliptic curves. In order for it to be called an elliptic curve, we must choose $a, b$ such that the following two conditions hold.

(1) The curve is **non-singular**. There are two types of "bad behavior we want to avoid (examples here sketched over $\mathbb{R}$):




Non-singular curves over $\mathbb{R}$ look like one of the following (as some people like to say, there may or may not be an "egg piece"):




(2) The other condition we require is that the set of points on the curve is **non-empty**.

**N.B.: All of this is secretly avoiding fields of characteristic $2, 3$. This is more technical, so we will avoid it for now.**

**Question.** *How can we tell if, for given $a$ and $b$, a curve is non-singular?*

Let's set $F(x, y) := y^2 - x^3 - ax - b$. Thus, $E(K) = \{(x, y) \in K^2 : F(x, y) = 0\}$. What we want is that there are no points where

$$\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = 0.$$

The partial derivative with respect to $y$ is just $2y$, so the second vanishing implies that $y = 0$. Thus, if the curve has any singular points, they are on the $x$-axis. Further, we have

$$\frac{\partial F}{\partial x} = -3x^2 - a = 0 \implies a = -3x^2.$$

Since $y = 0$, we have

$$x^3 + ax + b = 0 \implies x^3 - 3x^3 + b = -2x^3 + b = 0 \implies x^3 = b/2.$$

Combining, we find that

$$x^6 = \left(\frac{b}{2}\right)^2 = \left(\frac{-a}{3}\right)^3 \implies 27b^2 + 4a^3 = 0.$$

Thus,

$$E\colon y^2 = x^3 + ax + b \text{ is non-singular} \iff \Delta := -16(4a^3 + 27b^2) \neq 0.$$

The constant $\Delta$ is the **discriminant** of the curve. It will also give us an important modular form.

**What's special about elliptic curves?** At first glance, the defining cubic equation seems "random". Although we will be most interested in studying these curves over $\mathbb{Q}$, the simplest field to look over is $\mathbb{C}$. One of the amazing things about algebraic geometry is that in number theory we are often interested in curves over $\mathbb{Q}$ and it would seem that the complex points wouldn't reveal much about the $\mathbb{Q}$-structure, but the situation there is nicer and it does tell you a lot about the curve over smaller fields.

Suppose we study an algebraic plane curve of the form $f(x, y) = 0$ which is non-singular. These can be classified over $\mathbb{C}$ by something called the **genus**. To describe this, we have to talk about **projective space**:

$$\mathbb{P}^2 := \{(x, y, z) \in \mathbb{C}^3 : x, y, z \text{ not all } 0\}/\sim,$$

where $(x, y, z) \sim \lambda(x, y, z)\ \forall \lambda \in \mathbb{C}^\times$. These are called **homogenous coordinates**. If $z \neq 0$, then we can rescale and WLOG look at a point of the form $(x, y, 1)$. The set of such points thus looks like $\mathbb{C}^2$.

If $z = 0$, then we think of such a coordinate as a "point at infinity".

Given an equation $f(x, y) = 0$ over $\mathbb{C}^2$, we can **projectivize** to make it compatible with $\mathbb{P}^2$ homogenous coordinates. For instance, if we have the equation

$$y^2 = x^3 + ax + b,$$

in order to be well-defined over $\mathbb{P}^2$, we need a homogenous polynomial, and we insert the minimal powers of $z$ to make it so:

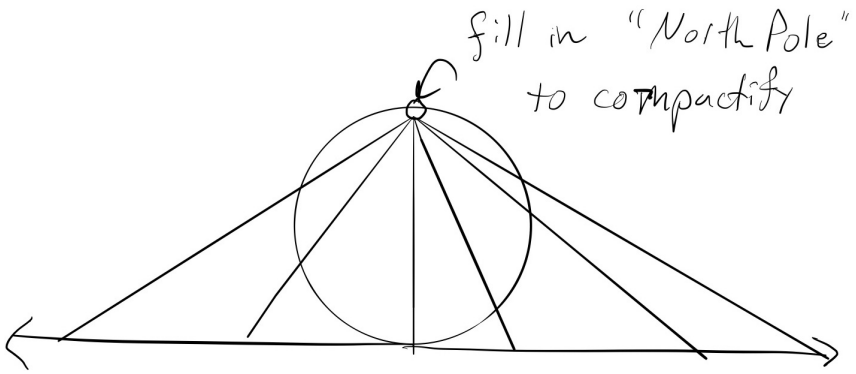
$$y^2 z = x^3 + axz^2 + bz^3.$$

This is the equation of the corresponding cubic curve in $\mathbb{P}^2$.

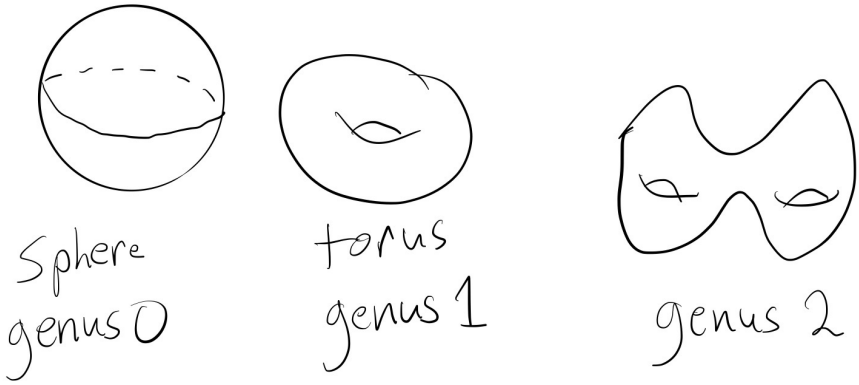
Why would we want to do this? So that the curve becomes **compactified**. For example, think of the pictures of the elliptic curves over $\mathbb{R}$ above. One of them had an egg piece, but both had a piece which shot off to $\pm\infty$ as you move to the right. However, if you add a single point at $\infty$, it becomes compact.

**Exercise 1.** *Check that there is just one point at infinity for any elliptic curve (that is, that the projectivized equation has exactly one point where $z = 0$).*

Here is an analogous pictures of compactification of a line by adding a single point using stereographic projection:




Once we perform this procedure, our elliptic curve is a **compact Riemann surface**. These can be classified by the "number of holes" they have, also known as their genus:




Next time, we'll use this classification to give an explanation for why elliptic curves are so interesting, and what is special about the equation $y^2 = x^3 + ax + b$.