MODULAR FORMS LECTURE 6: MORE ON ELLIPTIC CURVES

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

[On the Bourbaki wedding] The identity of the celebrating priest "P. Adic, of the Diophantine Order" remained unclear. The most likely suspect was Helmut Hasse, but I couldn't place him in Paris on June 3rd, 1939.

LIEVENLB: `http://www.neverendingbooks.org/hasse-le-p-adique-de-lordre-des-diophantiens`

What's special about elliptic curves? Last time, we defined elliptic curves (over some field) as plane curves of the shape $y^2 = x^3 + ax + b$ which are non-singular and have at least one point. So why this equation? Last time, we also talked about projectivizing plane curves to get compact Riemann surfaces. In turn, these are classified by the genus.

Fact. *The genus of an irreducible non-singular plane curve of degree d (this is the degree of the defining polynomial) is*

$$g = \frac{1}{2}(d-1)(d-2).$$

Roughly speaking, the higher the genus of a curve, the more difficult it is to study. As the genus grows with the degree, this matches with the intuition that curves defined by higher degree polynomials are more "complicated". For $d = 3$, as in the case of elliptic curves, the genus is $\frac{1}{2}(3-1)(3-2) = 1$.

This kind of result can show that **all** genus 1 plane projective curves are of this shape. While one could consider more general cubic polynomials, the point is that you can make linear changes of variables to get it in the shape $y^2 = x^3 + ax + b$. If we want to know what the points look like over some field, these changes of variables won't fundamentally change the situation. As an example, suppose that you have an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If the characteristic of your field is not 2, then letting $Y := y + \frac{a_1x+a_3}{2}$ completes the square:

$$Y^2 = x^3 + \frac{A}{4}x^2 + \frac{B}{2}x + \frac{C}{4},$$

where

$$A = a_1^2 + 4a_2, \quad B = a_1a_3 + 2a_4, \quad C = a_3^2 + 4a_6.$$

If the characteristic if the field is not 3, then we can go further by setting $X := x + A/12$, giving

$$Y^2 = X^3 - \frac{a}{48}X - \frac{b}{864},$$

where

$$a = A^2 - 24B, \quad b = -A^3 + 36AB - 216C.$$

When the curve is written in such a form, namely the form $y^2 = x^3 + ax + b$, we say that it is in **Weierstraß normal form**.

Thus, elliptic curves are basically just nice plane algebraic curves of genus 1. Specifically, we have the following.

Alternate Definition. *An* **elliptic curve** *over a field K is a non-singular projective algebraic curve E over K (meaning it has coefficients in K) which has genus* 1*, together with a choice of a K-rational point on E.*

Ok, but why is genus 1 **interesting?** In number theory, we often study **Diophantine problems**, which seek to understand the points of curves over $\mathbb{Z}$ or $\mathbb{Q}$, or the set of prime numbers. Many problems which don't look like they are expressible in terms of solving polynomials over integers or rationals can actually be recast in such a framework. You should think of polynomial equations over different fields as follows. Over $\mathbb{C}$, things are the nicest possible; its an algebraically closed field and the set of points has a nice geometric structure. Over $\mathbb{R}$, you have Calculus, so things are still pretty nice. In particular, you have the Intermediate Value Theorem, so solutions exist in between any pair of positive and negative values.

Over $\mathbb{Q}$, you don't have calculus, so things aren't as nice. But at least its a field. Over $\mathbb{Z}$, things are even harder, and studying solutions of polynomial equations over the set of prime numbers is usually extremely difficult.

There is a really big idea in number theory, called the **Local to Global Principle**. This states that if you're lucky, you would like to try to build up points on curves over $\mathbb{Q}$ (we call these "global points") by using points over $\mathbb{R}$ and over all of the so-called p-adic fields $\mathbb{Q}_p$ for primes p (the so-called "local points"). These fields all contain $\mathbb{Q}$, so of course a $\mathbb{Q}$ point automatically gives a point over all these fields; here we are after the converse. The p-adic fields are like alternate universes which a number theorist likes to say are as natural as $\mathbb{R}$; they can be defined in a similar way as a completion of $\mathbb{Q}$ just with a non-standard metric (and in fact these give all other possible completions of this type). The point is that like $\mathbb{R}$, the p-adic fields have well-defined theories of Calculus. In fact, things are in ways nicer than over $\mathbb{R}$. As we will discuss, studying p-adic solutions essentially boils down to knowing the points over *finite fields* like $\mathbb{F}_p$. Thus, the hope is that after trading the study of the curve over one field like $\mathbb{Q}$ for the infinite number of "easier" fields $\mathbb{R}$ and $\mathbb{Q}_p$, not too much information is lost.

The Local to Global Principle is sometimes literally true. A key example is the following.

Theorem (Hasse Principle)**.** *If $C/\mathbb{Q}$ has genus 0, then*

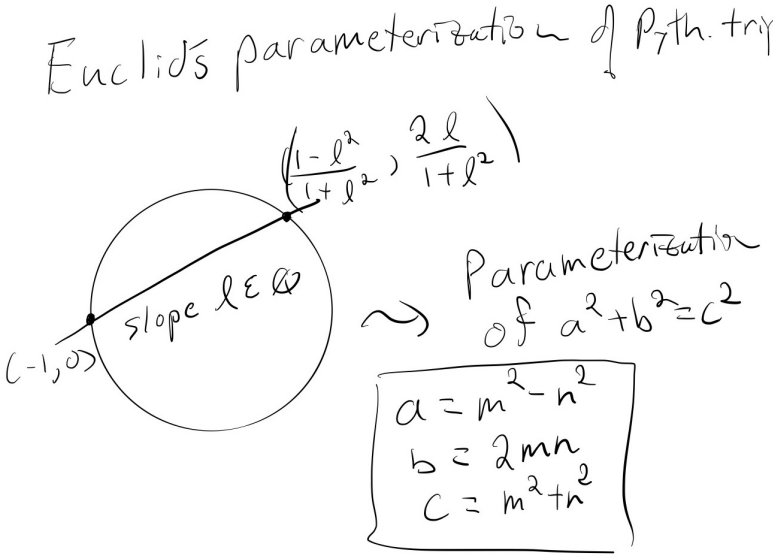
$$C(\mathbb{Q}) \neq \emptyset \iff C(\mathbb{R}) \neq \emptyset,\ C(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p.$$

The same is true if we replace "non-empty" by "has a non-trivial solution" everywhere.

As mentioned above, whether $C(\mathbb{R})$ is empty is easy to test thanks to the IVT, and thanks to **Hensel's Lemma**, the $\mathbb{Q}_p$ criterion can be reduced to a finite check (more on this later). In fact, for genus 0 curves, you can go further. Once you have a point, its easy to parameterize **all** rational points on a genus zero curve. For instance, Pythagorean triples are solutions to $a^2 + b^2 = c^2$. There is an easy bijection

$$\left\{(0,0,0) \neq (a,b,c) \in \mathbb{Z}^3 \,:\, a^2+b^2=c^2\right\} \leftrightarrow \left\{(X,Y) \in \mathbb{Q}^2 \,:\, X^2+Y^2=1\right\}$$

given by $(a,b,c) \mapsto (a/c, b/c)$. As solved in Euclid's Elements, you can parameterize all rational points on the unit circle by drawing lines of rational slope through a fixed point, usually taken to be $(-1,0)$.



Thus, the problem of determining rational points on genus 0 curves is basically solved. Elliptic curves are the first case where the Local to Global Principle **fails**.

Example 1. Selmer's cubic $3x^3 + 4y^3 + 5z^3 = 0$ has no non-zero $\mathbb{Q}$-rational points, but has a non-zero real point and non-zero points over all $\mathbb{Q}_p$. If you're curious, Keith Conrad wrote up a nice proof of this here: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf`

But it doesn't fail as badly as in higher genus cases, Curves of genus 2 are much harder. There is still a lot of structure in the genus 1 case, including a not-so-bad failure to the

Local to Global Principle. In fact, some measure of the failure of elliptic curves to satisfy it should be finite (but you'll be famous if you can prove this!), just as class numbers in algebraic number theory are finite and measure failure of unique factorization.

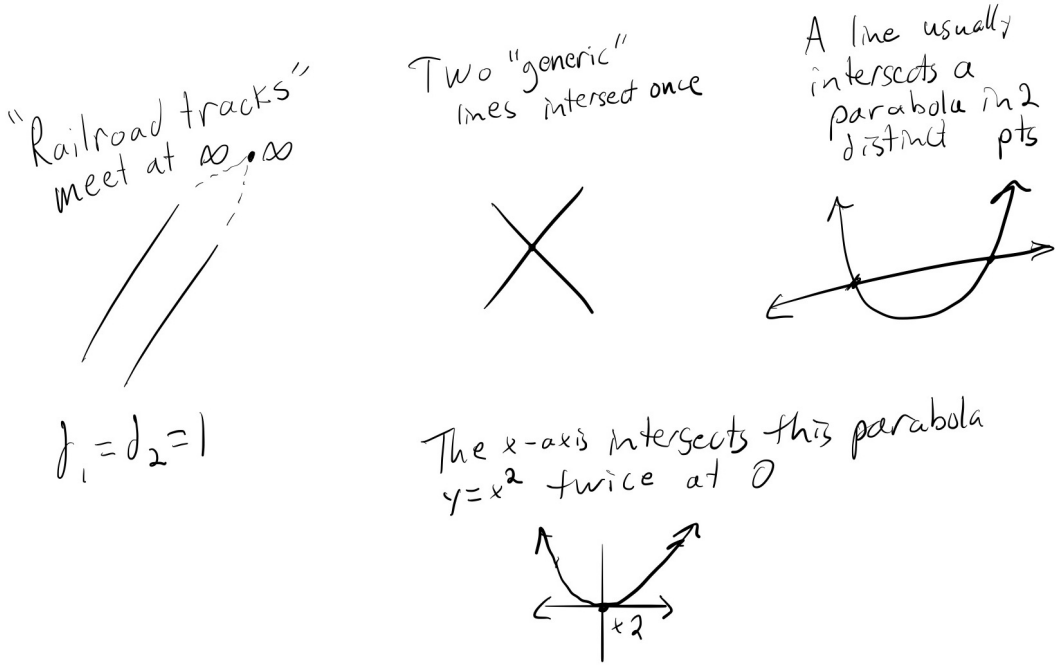
Takeaway. Genus 0 curves (think: conic sections) are relatively easy to understand using some big hammers from modern number theory. Elliptic curves are the next-easiest case, where many things are still open problems, but where there is still a lot of explicit structure to exploit.

Another explicit structure elliptic curves have is that they are **groups**.

Group structure of elliptic curves. Unlike higher genus curves, elliptic curves have a group structure. Let's illustrate this over $\mathbb{R}$, so that we can draw pictures. Recall that elliptic curves have to have a point on them. We can choose any point as the identity of our group. It is customary to pick the point at infinity. There is a key fact we will need. Basically, the number of intersection points between two algebraic curves **in projective space** should be the product of their degrees. This is not true of course, if the two curves are the same, or share some component, and one also has to count points with multiplicity (for example, a line intersects a curve with multiplicity greater than one if its **tangent** to it).

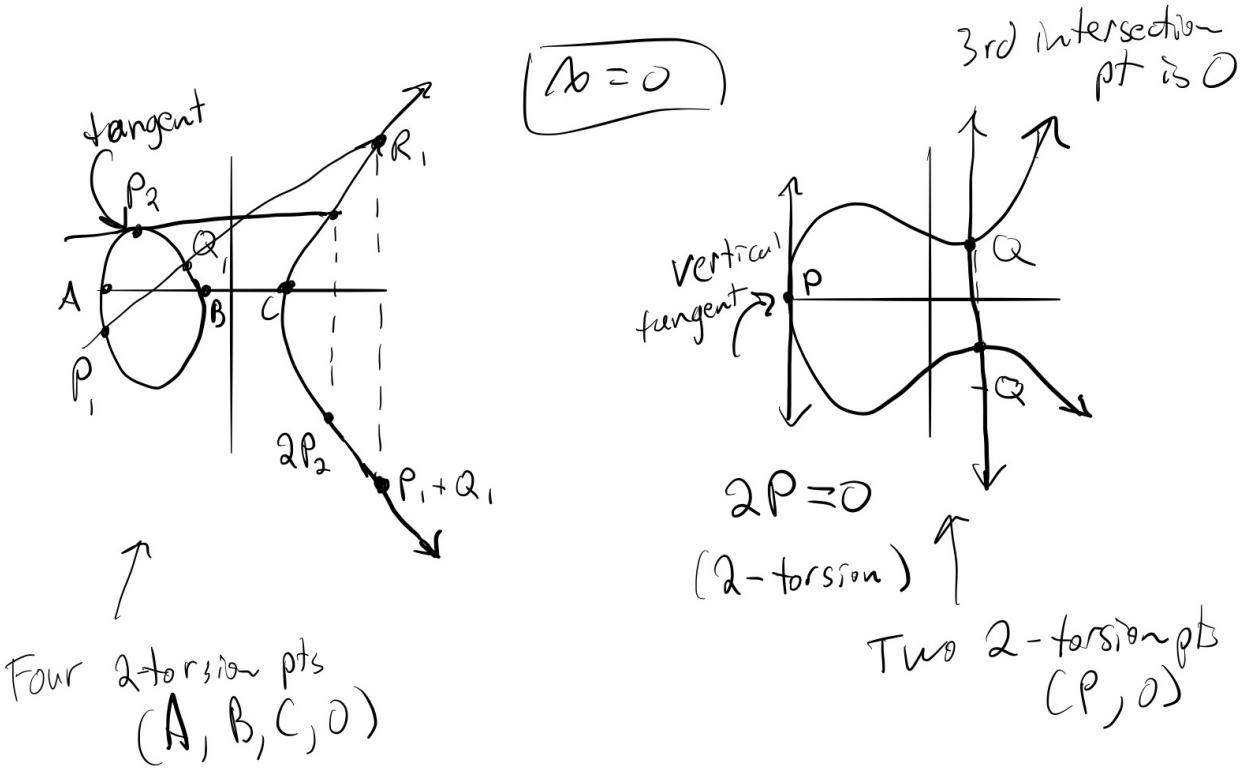
Theorem (Bezout's Theorem)**.** *Given two algebraic projective plane curves of degrees d_1 and d_2, if they don't share a common component (equivalently, the defining polynomials are relatively prime), then counting with multiplicity they have* **exactly** *$d_1 d_2$ intersection points.*

For example, we have the following.



In the case of elliptic curves, we take the identity as the point at ∞, which if you solved the exercise from last time, is the point $(0 : 1 : 0)$. If we take two points P and Q on the curve, we can draw a straight line between them. This line has degree 1, and the elliptic curve has degree 3, so they will intersect in 3 points. It might seem like we should then define $P + Q$ to be this third point, call it R. This is *almost* right. We actually define $P + Q$ to be the **reflection** of R across the x-axis.

Here are a few examples. Note that to double a point, that is, to compute $P + P$, we draw a tangent line at P, to negate a point, we reflect across the x-axis, and that 2-torsion points (where the double of the point is zero) are exactly where there is a vertical tangent, which is also just where $y = 0$.



This group law is very special, and very deep. It also happens to have practical importance, as its the structure exploited by **Elliptic Curve Cryptography** (which may be used by your chip on your credit card, and is becoming increasingly common in internet security). Although this looks geometric, its secretly completely algebraic. That is, I could write down equations down for these intersection points, and then these equations would be valid over **any field**, regardless of whether I can draw a picture.

Exercise 1. *Prove that this procedure defines an abelian group over any field. Fair warning: this is one of those weird situations where showing commutativity is easy, but showing associativity is much harder (its tedious).*