MODULAR FORMS LECTURE 7: CONNECTION WITH ELLIPTIC FUNCTIONS AND THE CONGRUENT NUMBER PROBLEM

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> Number theory swarms with bugs, waiting to bite the tempted flower-lovers who, once bitten, are inspired to excesses of effort!
>
> Barry Mazur

Why are they called "elliptic" curves? We have seen what elliptic curves really are, genus 1 non-singular curves, and we've seen a preview of why that is an interesting case to study. Why are they called "elliptic"? It has to do with elliptic functions.

To see why, let's look over $\mathbb{C}$. Fix a lattice Λ. Previously, we saw that there is a differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

Elliptic functions are invariant under Λ, and so they give well-defined functions on $\mathbb{C}/\Lambda$ (represented by a fundamental domain). As we saw when we integrated around the boundary of this region, opposite sides of the parallelogram Π are equivalent under Λ. Geometrically, when we identify opposite sides, we get a *torus*:

We then have a map between $\mathbb{C}/\Lambda$ and the elliptic curve

$$E_\Lambda \colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

given in homogenous coordinates by

$$z \mapsto (\wp(z), \wp'(z), 1) \quad z \neq 0,$$

$$0 \mapsto (0, 1, 0).$$

The fact that $\wp, \wp'$ are elliptic functions implies that this is well-defined, and the differential equation implies that the image actually lies on the curve. Thus, the Weierstraß $\wp$-function gives a way to **parameterize** elliptic curves over $\mathbb{C}$ as tori.

The Congruent Number Problem. We now discuss one of our motivating examples of elliptic curves and modular forms.

Question. *When is n the area of a rational right triangle?*

The first observation is that we can rescale triangles by a constant (similar triangles), and it scales the area by a square, so we can clear out denominators of n to get an integer, and we can get rid of square factors and assume that n is square-free. Then if the sides of the triangle are x, y, z (with z being the hypotenuse), we are asking to simultaneously solve the pair of Diophantine equations:

$$\begin{cases} x^2 + y^2 = z^2 \\ \frac{xy}{2} = n \end{cases} \qquad (x, y, z) \in \mathbb{Q}^3.$$

WLOG, say that $x < y < z$.

The reason these are called "congruent" numbers is due to the following connection with squares in arithmetic progressions. Any two squares are of course in an arithmetic progression, and its impossible for four squares to be in an arithmetic progression (this can be proven using elliptic curves, and is a short proof if you use a big result on partial progress towards the Birch and Swinnerton-Dyer conjecture (BSD); see here: `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/4squarearithprog.pdf`).

Congruent numbers correspond to triples of squares in arithmetic progression. That is, there is a correspondence between rational triangles with area n and triples $a-n, a, a+n$ of squares. This works as follows. A triple of 3 squares in a progression with common difference n can be written as r^2, s^2, t^2 where $s^2 - r^2 = t^2 - s^2 = n$. Adding these two equations gives $t^2 - r^2 = (t + r)(t - r) = 2n$. But then $n = \frac{(t-r)(t+r)}{2}$. That looks like the equation we had above for the area, so we could try $x = t - r$, $y = t + r$ (since y was chosen to be larger). If we do that, then $x^2 + y^2 = (t - r)^2 + (t + r)^2 = 2t^2 + 2r^2 = 2(t^2 + r^2) = 4s^2 = (2s)^2$, so that we have a triangle (x, y, z) satisfying the Diophantine equations. This plus some more algebra on the converse leads to the following.

Theorem. *There is a one-to-one correspondence*

$$\big\{(x, y, z) \colon x^2 + y^2 = z^2, xy/2 = n\big\} \leftrightarrow \big\{(r, s, t) \colon s^2 - r^2 = t^2 - s^2 = n\big\}$$

given by

$$(r, s, t) \mapsto (t - r, t + r, 2s)$$

in one direction and

$$(x, y, z) \mapsto \left(\frac{y - x}{2}, \frac{z}{2}, \frac{y + x}{2}\right)$$

in the other.

Exercise 1. *Check the details of this.*

As an example, 6 is a congruent number as its the area of the $3-4-5$ Pythagorean triangle, and this maps to $(1/2, 5/2, 7/2)$. This gives the arithmetic progression $\frac{1}{4}, \frac{25}{4}, \frac{49}{4}$ with common difference 6. After scaling by 4 (a square), this is the arithmetic progression $1, 25, 49$ of squares you may have recognized before.

We will now see another way to characterize congruent numbers, one which will be very fruitful.

Relation to elliptic curves. Consider the special family of elliptic curves:

$$E_n \colon y^2 = x^3 - n^2 x.$$

The curve E_1 is called the **congruent number elliptic curve**. This is a very special family. In fact, all of them are **quadratic twists** of E_1. This means that they are isomorphic over a quadratic extension of $\mathbb{Q}$, but not over $\mathbb{Q}$. This observation will be critical later.

Exercise 2. *In general, the n-th quadratic twist of $y^2 = x^3 + ax + b$ is $ny^2 = x^3 + ax + b$. The first curve is recovered from the second by letting $y \mapsto y/\sqrt{n}$, which you can do over $\mathbb{Q}(\sqrt{n})$ but not over $\mathbb{Q}$. Show that the quadratic twists*

$$ny^2 = x^3 - x$$

become E_n when they are transformed into Weierstraß normal form.

The explicit relation to congruent numbers is given in the following.

Theorem. *For $n > 0$, there is a one-to one correspondence*

$$\left\{(a, b, x) \colon a^2 + b^2 = c^2,\ \frac{ab}{2} = n\right\} \leftrightarrow \left\{(x, y) \colon y^2 = x^3 - n^2 x,\ y \neq 0\right\}$$

given by

$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$$

and

$$(x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

Proof. This is also just a straightforward algebra check. Note that $c \neq a$ as the hypotenuse of a triangle can't equal a side length, and its clear we need $y \neq 0$ in the second set.

Exercise 3. *Check the algebra.*

□

This correspondence also preserves positivity and rationality. Thus, we have:

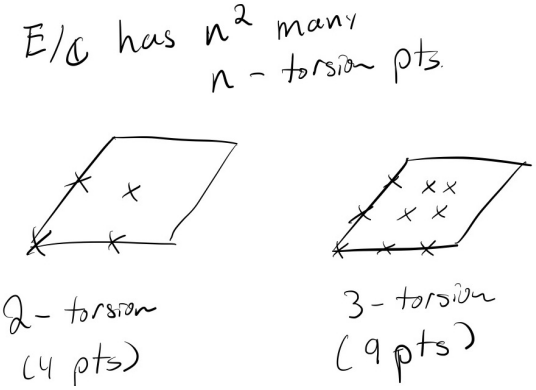
Corollary. *The number n is congruent if and only if E_n has a rational point with non-zero y-coordinate.*

Note that E_n always has a few "easy" rational points; exactly those with $y = 0$! To find these, we solve $x^3 - n^2x = x(x^2 - n^2) = 0$, giving $x = 0, \pm n$. As we saw earlier, these are just the **2-torsion points** (excluding ∞) since $x \mapsto -x$ on an elliptic curve reflects across the x-axis.

In terms of the pictures from before, E_n always has an egg piece. We say that E_n has **full 2-torsion**. Why? The maximum number of n-torsion points is n^2, as if we extend all the way to $\mathbb{C}$, then $E \cong \mathbb{C}/\Lambda$ where Λ is the unique lattice (later, we'll be able to show it exists and how to tell when two elliptic curves are isomorphic over $\mathbb{C}$) such that

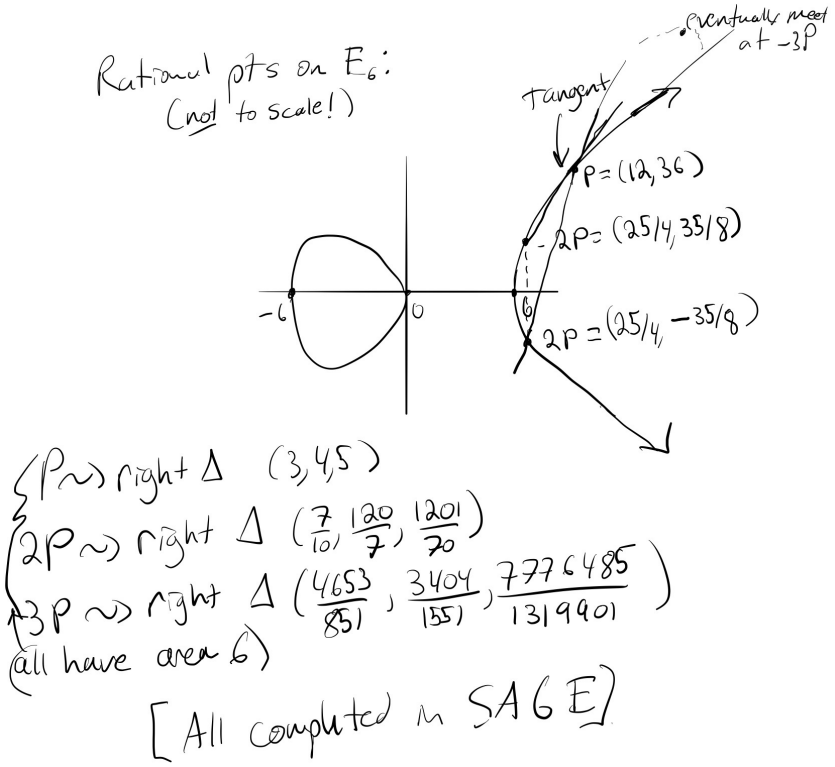
$$g_2(\Lambda) = \pm a, \quad g_3(\Lambda) = \pm b.$$

There are n^2 torsion points over $\mathbb{C}$, as illustrated in these pictures:



N.B.: Elliptic curves are much "nicer" if they have full 2-torsion. There is also "extra symmetry" which makes E_n **really** nice.

As an example of this correspondence, using the $3 - 4 - 5$ triangle representing 6 as congruent, we know that $y^2 = x^3 - 36x$ must have a rational solution with $y \neq 0$. One such point is $(12, 36)$. This allows us to find more triangles with area 6. For instance, we can double and triple this point:



The structure of groups of rational elliptic curves $E/\mathbb{Q}$ has a very specific shape. This can be proved easily for 2-torsion (even basically elementary), is not so bad when there is one point of order 2, and is more serious when there is trivial 2-torision. It is also true over number fields, but requires even more technology to prove. Studying the following theorem and its proof in some level of generality would be a good **final project idea**.

Theorem (Mordell-Weil)**.** *For any elliptic curve $E/\mathbb{Q}$, the set of $\mathbb{Q}$-rational points $E(\mathbb{Q})$ is a finitely generated abelian group.*

Thus, from algebra, we have the following decomposition

$$E(\mathbb{Q}) \cong E^{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^r,$$

where E^{tors} is the **torsion subgroup** consisting of points of finite order, and $r \geq 0$ is called the **rank**. There is a really amazing result, whose proof is beyond the scope of what we'll be able to do this semester.

Theorem (Mazur)**.** *All possible groups for $E^{\text{tors}}(\mathbb{Q})$ are completely classified. There are finitely many of them. given a curve, its also "easy" to check which torsion group it has.*

There is **no known algorithm** that computes the rank and is guaranteed to terminate (unless you assume **BSD**).

We've mentioned BSD a few times. What does this say? It says that an **analytic object** connected to modular forms tells us r. The famous **Modularity Theorem** of

Wiles et al. proves that all elliptic curves are connected to modular forms through this analytic object. This is part of a general mantra in number theory: Many things are revealed by connections between the algebraic/geometric world (like elliptic curves) and the analysis world (like modular forms).

Next time, we will completely determine the torsion subgroups of E_n. We will then use this to give a criterion for n to be congruent in terms of the rank of n. Then, we will return to the world of modular forms, and later see where this rank connects to something we can actually compute in modular forms, if we assume BSD.