MODULAR FORMS LECTURE 8: TORSION POINTS ON THE CONGRUENT NUMBER ELLIPTIC CURVES

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> Dirichlet allein, nicht ich, nicht Cauchy, nicht Gauß, weiß, was ein vollkommen strenger Beweis ist, sondern wir lernen es erst von ihm. Wenn Gauß sagt, er habe etwas bewiesen, so ist es mir sehr wahrscheinlich, wenn Cauchy es sagt, ist ebensoviel pro als contra zu wetten, wenn Dirichlet es sagt, ist es gewiß; ich lasse mich auf diese Delikatessen lieber gar nicht ein.
>
> Jacobi, writing to von Humboldt

Last time, we defined the elliptic curves $E_n\colon y^2 = x^3 - n^2x$. We have seen that the existence of rational points on E_n with $y \neq 0$ controls whether n is congruent. We also say that any elliptic curve group splits up as a torsion part and a power of $\mathbb{Z}$. Finally, we have seen that there are 4 two-torsion points on E_n, 3 of which have $y = 0$. It turns out that these are all of the torsion points.

Theorem. *For any n, we have $E_n^{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Corollary. *n is congruent if and only if $E_n(\mathbb{Q})$ has a point of infinite order. That is, iff $E_n(\mathbb{Q})$ has rank $r \geq 1$.*

Corollary. *If n is congruent, then there are infinitely many rational right triangles with area n.*

Remark. *Assuming BSD, we'll see tests for when the rank is positive via modular forms later.*

Proof. We have already seen that there are 4 torsion points. Since the three points on the x-axis have order 2, these form a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We need to show that there are no other torsion points.

Goal: Construct a group homomorphism

$$E_n^{\text{tors}}(\mathbb{Q}) \to E_n(\mathbb{F}_p)$$

which is "usually" injective. For such p, by Lagrange's Theorem we have $\#E_n^{\text{tors}}(\mathbb{Q}) \mid \#E_n(\mathbb{F}_p)$.

Lemma. *If $q = p^r$, $p \nmid 2n$, $q \equiv 3 \pmod 4$, then*

$$\#E_n(\mathbb{F}_q) = q + 1.$$

Proof. We already have 4 points of order dividing 2: ∞, $(0,0)$, and $(\pm n, 0)$. Now count those points (x,y) with $x \neq 0, \pm n$. Arrange the $q-3$ remaining x's into pairs $\{x, -x\}$. Then $f(x) = x^3 - n^2x$ is an odd function, and since -1 is **not a square** in $\mathbb{F}_q$ (this is a basic elementary number theory fact we'll assume which holds since $q \equiv 3 \pmod 4$), exactly one of the $f(x)$, $f(-x)$ is a square in $\mathbb{F}_q$. (Note: In $\mathbb{F}_q^\times$, the squares are a subgroup of order 2, so a product of two squares is a square, etc). This gives $(q-3)/2$ pairs, or $q-3$ points on the curve, plus the original 4 points of order 2, for a total of $q+1$ points. (Note; We'll return to the case $q \equiv 1 \pmod 4$ later as we'll need it for other purposes). □

Now if $\#E_n^{\text{tors}}(\mathbb{Q}) \mid \#E_n(\mathbb{F}_p)$ for most p, then we'll have for most $p \equiv 3 \pmod 4$ that $\#E_n^{\text{tors}}(\mathbb{Q}) | p+1$. If for instance, the size of the torsion group was 12, this would mean that for most primes $p \equiv 3 \pmod 4$, we have $p = 12k - 1 \implies p \equiv 11 \pmod{12}$, which is false.

We now need to switch to projective coordinates. We consider a map from

$$\mathbb{P}^2_{\mathbb{Q}} \to \mathbb{P}^2_{\mathbb{F}_p}.$$

For this, we can pick for each point in the codomain representative homogenous coordinates $P = (x, y, z) \in \mathbb{P}^2_{\mathbb{Q}}$ with relatively prime integer coordinates (by clearing out denominators and dividing out common factors), and this is unique up to a factor of ± 1. The map then sends each of x, y, z to their reductions mod p in $\mathbb{F}_p$. As x, y, z are relatively prime, p can't divide all three of them, so that we don't get $(0,0,0)$ as disallowed in projective coordinates. Denote this new point $\overline{P} = (\bar{x}, \bar{y}, \bar{z}) \in \mathbb{P}^2_{\mathbb{F}_p}$. For example, last time we considered the point $(25/4, 35/8, 1)$ on E_6 and take the prime $p = 7$, then we rescale this to $(50, 35, 8)$ and then reduce mod 7 to get $(1, 0, 1) \in \mathbb{P}^2_{\mathbb{F}_7}$. The equation $y^2 = x^3 - 36x$ mod 7 becomes $y^2 = x^3 - x$, and so $(1,0)$ is a point on the curve mod 7.

In general, $P \in E_n(\mathbb{Q}) \implies \overline{P} \in E_n(\mathbb{F}_p)$ (reduce the equations defining the curve mod p). Writing the addition law on an elliptic curve algebraically shows that $\overline{P_1 + P_2} = \overline{P}_1 + \overline{P}_2$, i.e., that this gives a homomorphism

$$E_n(\mathbb{Q}) \to E_n(\mathbb{F}_p)$$

for any prime $p \nmid 2n$ (this is to avoid primes where the discriminant $64n^6 \equiv 0 \pmod p$). That is, if we avoid finitely many **bad places**, this is a homomorphism of elliptic curves.

To study when this map is injective, we give a useful criterion for the reduction of two points to be equal.

Lemma (Injectivity Lemma)**.** *We have that*

$$\overline{P}_1 = \overline{P}_2 \iff P_1 \times P_2 \text{ is divisible by } p,$$

where the $\times$ on the right hand side denotes cross product in $\mathbb{R}^3$.

Proof. Suppose that $p \mid P_1 \times P_2 = (y_1z_2 - y_2z_1, x_2z_1 - x_1z_2, x_1y_2 - x_2y_1)$.

Case 1: If $p|x_1$, then $p|x_2z_1, x_2y_1$, and so $p|x_2$ (otherwise, $p|x_1, y_1, z_1$, which is a contradiction). Now either y_1 or z_1 is not divisible by p, WLOG say y_1 isn't.By rescaling in projective coordinates we have

$$\overline{P}_2 = (0, \overline{y}_2, \overline{z}_2) = (0, \overline{y}_1\overline{y}_2, \overline{y}_1\overline{z}_2) = (0, \overline{y}_1\overline{y}_2, \overline{y}_2\overline{z}_1) = (0, \overline{y}_1, \overline{z}_1),$$

where we used the cross product relation $p|(y_1z_2 - y_2z_1)$.

Case 2: If $p \nmid x_1$, then by rescaling in projective coordinates we find

$$\overline{P}_2 = (\overline{x}_1\overline{x}_2, \overline{x}_1\overline{y}_2, \overline{x}_1\overline{z}_2) = (\overline{x}_1x_2, \overline{x}_2\overline{y}_1, \overline{x}_2\overline{z}_1) = (\overline{x}_1, \overline{y}_1, \overline{z}_1) = \overline{P}_1.$$

Conversely, if $\overline{P}_1 = \overline{P}_2$, then WLOG assume $p \nmid x_1$ (since it doesn't divide some component). Since $\overline{P}_1 = \overline{P}_2$, we deduce $p \nmid x_2$. Thus,

$$(\overline{x}_1\overline{x}_2, \overline{x}_1\overline{y}_2, \overline{x}_1\overline{z}_2) = \overline{P}_2 = \overline{P}_1 = (\overline{x}_2\overline{x}_1, \overline{x}_2\overline{y}_1, \overline{x}_2\overline{z}_1).$$

Since the first coordinates are equal, these two points can be equal if and only if the second and third components are also equal (no rescaling allowed). This happens iff

$$p \mid x_1y_2 - x_2y_1, x_1z_2 - x_2z_1.$$

Finally, we need to show $p \mid (y_1z_2 - y_2z_1)$. If p divides both y_1 and z_1, this is trivial. Otherwise, repeat the argument with x_1, x_2 replaces by y's or z's. □

Now we are ready to prove our main result. Suppose that $E_n(\mathbb{Q})$ has a torsion point of order greater than 2. Then either it has a point of odd order or the subgroup of points of order dividing 4 has either 8 or 16 elements. Thus, there would be a non-trivial subgroup of $E_n^{\text{tors}}(\mathbb{Q})$ or order 8 or with an odd number of elements. No matter what, there is a subgroup of order m where $m = 8$ or m is an odd number bigger than 1 . Call the points in this subgroup $S = \{P_1, \dots P_m\}$, where $P_i = (x_i, y_i, z_i)$. For each pair of i, j, the P_i, P_j are distinct in projective coordinates. Thus, as $\mathbb{R}^3$ vectors they aren't proportional and so $P_i \times P_j \neq 0$. Let n_{ij} be the gcd of the coordinates of $P_i \times P_j$. By the above lemma,

$$\overline{P}_i = \overline{P}_j \iff p|n_{ij}.$$

Thus, if p is a point **of good reduction** (it doesn't divide the discriminant of $E(\mathbb{Q})$ so that $E(\mathbb{F}_p)$ is an elliptic curve), bigger than all the n_{ij}, we have an **injection**

$$S \hookrightarrow E_n(\mathbb{F}_p).$$

So for all but finitely many primes $p \equiv 3 \pmod 4$, we have

$$m \mid \#E_n(\mathbb{F}_p) = p + 1 \implies p \equiv -1 \pmod m.$$

This is (case-by-caser) a contradiction to **Dirichlet's Theorem on primes in arithmetic progressions**! If $m = 8$, this implies that there are only finitely many primes of the form $8k + 3$. If m is odd, then there are either finitely many primes of the form $4mk + 3$ (if $3 \nmid m$) or $12k + 7$ (if $3|m$). □

In order to see how to test whether there is a point of infinite order on an elliptic curve, we will have to learn more about modular forms. Next time, we will begin the study of modular forms from scratch.