DAY 3: WHEN ADDITION LOOPS BACK

CURVES THAT CLASSIFY GEOMETRY PROBLEMS J-LO MC2022

Let E be an elliptic curve, and $E(\mathbb{Q})$ the set of rational points of E. Yesterday we saw that $E(\mathbb{Q})$ is a group, so we can generate new rational points from existing ones. So maybe we could start with a single point P and keep adding to itself over and over to get infinitely many points!

The problem: it's possible for this process to loop back to where it started.

Definition. For any natural number m, let

$$mP := \underbrace{P \oplus P \oplus \cdots \oplus P}_{m \text{ times}}.$$

The **order** of P is the smallest positive integer m such that $mP = O$; P has infinite order if no such m exists.

Points of the form $P = (x, 0)$ have order 2, and problem (13) from yesterday has an example of a point with order 6. So can we know whether a point will be able to keep generating new points, or whether we'll eventually get stuck? Today's goal is to prove the following condition that guarantees we will find infinitely many new points:

Theorem 1 (Nagell-Lutz, 1935)**.** *Let E be an elliptic curve defined by*

$$y^2 = x^3 + ax^2 + bx + c, \qquad \text{with } a, b, c \in \mathbb{Z}.$$

If the coordinates of $P \in E(\mathbb{Q})$ are not integers, then P has infinite order.

This will take a bit of work to prove; the issue is that elliptic curve addition feels pretty complicated, so it's very hard to predict where the multiples of P will go. The key idea is that we will show that if we "zoom out" far enough, elliptic curve addition starts to look like regular addition of rational numbers!

The cuspidal cubic

(1) For any nonzero $u \in \mathbb{Q}$, show that there is a change of variables relating the following two elliptic curves:

$$y^2 = x^3 + ax^2 + bx + c \qquad \text{and} \qquad y'^2 = x'^3 + u^2 a x'^2 + u^4 b x' + u^6 c.$$

A point (x, y) on the first curve corresponds to what point on the second curve?

By taking u to be very small, the elliptic curve gets closer and closer to the **cuspidal cubic**, a curve defined by $C : y^2 = x^3$. Let $C_{\text{sm}}(\mathbb{Q})$ denote the set of all rational points on C, including O, but *not* including $(0,0)$.[1] For all $P \in C_{\text{sm}}(\mathbb{Q})$ we can define

$$t(P) = \begin{cases} \frac{x}{y} & \text{if } P = (x,y), \\ 0 & \text{if } P = O, \end{cases} \qquad s(P) = \begin{cases} \frac{1}{y} & \text{if } P = (x,y), \\ 0 & \text{if } P = O. \end{cases}$$

(2) The function t has an *inverse*: for each $r \in \mathbb{Q}$, what $P \in C_{\text{sm}}(\mathbb{Q})$ satisfies $t(P) = r$?

(3) Suppose P, Q, R are points in $C_{\text{sm}}(\mathbb{Q})$ that are also on a line $y = mx+v$. Prove that the points $(t(P), s(P))$, $(t(Q), s(Q))$, and $(t(R), s(R))$ satisfy equations

$$s = \alpha t + \beta, \qquad s = t^3$$

for some α and β.

(4) Using the two equations above, prove that $t(P) + t(Q) + t(R) = 0$.

(5) If we define $P \oplus Q$ on $C_{\text{sm}}(\mathbb{Q})$ the same way as for elliptic curves (i.e. as $(P \star Q) \star O$), prove that

$$t(P) + t(Q) = t(P \oplus Q).$$

In other words, t is an *isomorphism* between $\mathbb{Q}$ and $C_{\text{sm}}(\mathbb{Q})$.

How not to prove infinite order

Since $\mathbb{Q}$ has no points of finite order, neither does $C_{\text{sm}}(\mathbb{Q})$. This suggests a way to prove that all points of finite order on an elliptic curve E have to be relatively close to the origin. If P is far enough from $(0,0)$, then we can zoom out so far that the elliptic curve is well approximated by $y^2 = x^3$, so addition in $E(\mathbb{Q})$ will be approximated by addition in $C_{\text{sm}}(\mathbb{Q})$. Since P looks like a point on $C_{\text{sm}}(\mathbb{Q})$, which has infinite order, P itself must have infinite order.

There are many issues with this argument. Even if we ignore the fact that "well-approximated" is kind of vague, there is one serious flaw with this argument:

(6) Let $P \in C_{\text{sm}}(\mathbb{Q})$. As $m \to \infty$, show that mP converges to $(0,0)$.

In other words, as you add P to itself, the approximation necessarily gets worse and worse, because it brings you closer to the region around $(0,0)$. The problem here is that no matter how small $t(P)$ is, we can add it to itself many times to get a very

[1]The subscript "sm" stands for "smooth;" the curve is smooth everywhere except at $(0,0)$, where it is bent.

large value. However, if we replace *size* with *divisibility*, this problem goes away: if $t(P)$ is divisible by p, then every multiple of $t(P)$ is also divisible by p!

p-ADIC VALUATION

Definition. Fix a prime p; then any nonzero rational number r can be written in the form $r = \frac{m}{n}p^k$, where m, n, k are integers with m, n relatively prime to p. The integer k is the **p-adic valuation** of r, written $k = \mathrm{ord}_p(r)$. We also define $\mathrm{ord}_p(0) = \infty$.[2]

Examples: $\mathrm{ord}_2(12) = 2$, $\mathrm{ord}_3(\frac{17}{54}) = -3$, $\mathrm{ord}_5(\frac{6}{7}) = 0$.

(7) Prove the following properties:
   (a) $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$ for all $a, b \in \mathbb{Q}$.
   (b) $\mathrm{ord}_p(a+b) \geq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$ for all $a, b \in \mathbb{Q}$.
   (c) If $\mathrm{ord}_p(a) < \mathrm{ord}_p(b)$, then $\mathrm{ord}_p(a+b) = \mathrm{ord}_p(a)$.

Important intuition: if $\mathrm{ord}_p(r)$ is *large*, you should think of r as being *close to zero*.[3]

We'll need one important fact about the p-adic valuations of rational points on elliptic curves.

(8) Let (x, y) be a rational point on $y^2 = x^3 + ax^2 + bx + c$, where a, b, c are all integers. If either $\mathrm{ord}_p(x)$ or $\mathrm{ord}_p(y)$ is negative, prove that there is an integer $n \geq 1$ such that $\mathrm{ord}_p(x) = -2n$ and $\mathrm{ord}_p(y) = -3n$.

FURTHER EXPLORATION (OPTIONAL)

There is much less to explore today, so feel free to go back to problems from yesterday that you didn't have time to finish.

(9) Consider the "nodal cubic" C' defined by $y^2 = x^3 + x^2$. Prove that $C'_{\mathrm{sm}}(\mathbb{Q})$ is isomorphic to the multiplicative group of nonzero rational numbers.

Definition. Let $R_{(p)}$ denote the set of $r \in \mathbb{Q}$ with $\mathrm{ord}_p(r) \geq 0$ (that is, with denominator not divisible by p). For $n > 0$, let $p^n R$ denote the set of $r \in \mathbb{Q}$ with $\mathrm{ord}_p(r) \geq n$ (that is, with numerator divisible by p^n).

Examples: $\frac{3}{19}$, 46, and $-\frac{12}{75}$ are in $R_{(2)}$, but $\frac{1}{2}$ is not. Of these numbers, 46 and $-\frac{12}{75}$ are in $2R_{(2)}$, $-\frac{12}{75}$ is in $4R_{(2)}$, and none of them are in $8R_{(2)}$.

(10) For all n, prove that $p^n R_{(p)}$ is a subgroup of $\mathbb{Q}$.

---

[2]Another definition of $\mathrm{ord}_p(r)$ is "the largest integer k such that when you write $\frac{r}{p^k}$ in lowest terms, the denominator is not divisible by p." If $r = 0$ then you can divide by p as many times as you want and the denominator will always be 1!

[3]Zero is divisible by p infinitely often, so the more divisible by p a number is, the more similar to zero it is. This can be formalized by defining the *p-adic absoltue value*, $|r|_p := p^{-\mathrm{ord}_p(r)}$. This function satisfies the triangle inequality, and as $\mathrm{ord}_p(r) \to \infty$ we have $|r|_p \to 0$.