DAY 4: PROVING POINTS HAVE INFINITE ORDER

CURVES THAT CLASSIFY GEOMETRY PROBLEMS J-LO MC2022

Approximating addition by size

Remember that our goal is to prove the following result:

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.

For any $P \in E(\mathbb{Q})$ that is not of the form $(x, 0)$, we can define

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

Observation 2. *If $t(P)$ and $t(Q)$ are both very close to zero, then the distance between $t(P \oplus Q)$ and $t(P) + t(Q)$ is very very very close to zero.*

The rough argument for this is that E can be well-approximated by the cuspidal cubic $C : y^2 = x^3$, and on C we have an exact equality $t(P \oplus Q) = t(P) + t(Q)$. The only issue is that this approximation $t(mP) \approx mt(P)$ gets worse and worse as m increases, so this will not help us determine the order of P.

Approximating addition by divisibility

We can fix this problem by changing what we mean by "close." Yesterday we defined the p-adic valuation ord_p, and will declare a rational number to be "small" if its p-adic valuation is large.

Observation 3. *If $t(P)$ and $t(Q)$ are both very divisible by p, then the distance between $t(P \oplus Q)$ and $t(P) + t(Q)$ is very very very divisible by p.*

We can make this more precise as follows. Let $E(p)$ be the set of rational points of E such that at least one of the coordinates has denominator divisible by p, as well as the point O.

Lemma 4 (Addition Lemma)**.** *Let $P, Q \in E(p)$, and suppose that $t(P)$ and $t(Q)$ both have p-adic valuation greater than or equal to n for some integer $n > 0$. Then $P+Q$ is also in $E(p)$, and*

$$\operatorname{ord}_p(t(P) + t(Q) - t(P+Q)) \geq 3n.$$

The proof is not that difficult, but is a bit tedious: it basically involves taking the work we did with the cuspidal cubic yesterday, throwing in a bunch of extra terms, and keeping track of how divisible by p everything is. If you want to work through the details, feel free to ask for a supplemental handout that walks through a proof.

Completing the proof

We can now use the lemma to finish proving the theorem. Suppose either coordinate of $P = (x, y)$ is not an integer. Then the corresponding denominator must be divisible by some prime p. So by problem (8) from yesterday, there is an integer $n \geq 1$ such that $\operatorname{ord}_p(x) = -2n$ and $\operatorname{ord}_p(y) = -3n$, and therefore $P \in E(p)$ and $\operatorname{ord}_p(t(P)) = n$.

(1) Using the addition lemma and induction, prove that for all positive integers m, we have

$$\operatorname{ord}_p(mt(P) - t(mP)) \geq 3n.$$

That is, unlike with our first attempt, the p-adic approximation $mt(P) \approx t(mP)$ stays good no matter how big m is![1]

(2) If P has order m, with m not divisible by p, prove that this would imply $\operatorname{ord}_p(t(P)) \geq 3n$. Why is this impossible?

(3) If P has order p, prove that this would imply $\operatorname{ord}_p(t(P)) \geq 3n - 1$. Why is this impossible?

(4) Prove that it is impossible for P to have finite order. (Hint: if P has order m with m divisible by p, consider the point $\frac{m}{p}P$.)

The above exercises show that P can't have any finite order, finishing the proof of Nagell-Lutz.

Infinitely many primitive triangles

By problem (14) on day 2, a rational point (x, y) on the curve $E_{3,4} : y^2 = x(x-9)(x-16)$ produces a triangle with integer side lengths a, b, c, integer area A, and $\frac{a}{b} = \frac{3}{4}$ by the change of variables

$$a = b\frac{m}{n}, \qquad c = b\frac{(m+n)(mn-x)}{n(mn+x)}, \qquad A = b^2\frac{m(m+n)y}{n(mn+x)^2},$$

[1] This is a nice feature of measuring distances p-adically: errors don't accumulate.

where b is whatever it needs to be in order to clear denominators.

(5) Prove that there are infinitely many rational points on $E_{3,4}$.

(6) Prove that $P = (x, y) \in E_{3,4}(\mathbb{Q})$ corresponds to a valid triangle (i.e. to *positive* values $a, b, c, A > 0$) if and only if $0 < x < 9$ and $y > 0$; that is, if P is "on the upper half of the egg."

(7) Prove that there are bijections between the sets of rational points lying on the upper half of the egg, the lower half of the egg, the upper half of the long branch, and the lower half of the long branch. (Hint: use $P \mapsto -P$ and $P \mapsto P + (0, 0)$.)

(8) Conclude that there are infinitely many primitive triangles with integer side lengths, integer area, and two sides in a ratio of 3 to 4.

By contrast, there is only a single triangle with integer side lengths a, b, c, integer area A, and $\frac{a}{b} = \frac{4}{5}$. This is somewhat difficult to prove and we will not discuss it in this course.

More facts about finite order points

Definition. Given a cubic polynomial $f(x) = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$, we define the **discriminant**,

$$D := -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Theorem 5 (Nagell-Lutz, 1935)**.** *Let E be an elliptic curve defined by*

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

and let D be the discriminant of $x^3 + ax^2 + bx + c$. If $P = (x, y) \in E(\mathbb{Q})$ has finite order, then $x, y \in \mathbb{Z}$, and either $y = 0$ or $y^2 \mid D$.

See problem (11) if you want to prove this result. Note that there are only finitely many integers y satisfying $y^2 \mid D$, and for each of these, at most 3 rational solutions to $y^2 = x^3 + ax^2 + bx + c$, so this gives a bound on how many points of finite order there can be! Now given any $P \in E(\mathbb{Q})$, there is a fast way to detect whether it is finite order or not: start computing $2P$, $3P$, etc. As soon as we find a point with non-integer coordinates, or a point (x, y) with $x, y \in \mathbb{Z}$, $y \neq 0$, and $y^2 \nmid D$, then P must have infinite order.

One of the further exploration problems on day 1 was to prove that a rational conic section has 0, 1, or ∞ rational points. The corresponding result for elliptic curves is significantly harder to prove.[2]

[2] This gets really meta: each elliptic curve with a rational point of order n corresponds to *a rational*

Theorem 6 (Mazur, 1977). *The number of rational points of finite order (including O) on an elliptic curve $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Q}$ is*

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, \textit{ or } 16.$$

So the total number of rational points is either one of these numbers, or ∞, depending on whether a rational point of infinite order exists.

Further exploration (optional)

(9) For each integer $n > 0$, let $E(p^n)$ denote the set of rational points P in $E(p)$ such that $t(P) \in p^n R_{(p)}$ (the group $p^n R_{(p)}$ was defined on yesterday's handout; roughly speaking, it's the set of rational numbers with numerator divisible by p^n). Use the addition lemma to prove the following facts.

(a) For all n, $E(p^n)$ is a subgroup of $E(\mathbb{Q})$.

(b) The function t defines an injective homomorphism of quotient groups:

$$t : \frac{E(p^n)}{E(p^{3n})} \to \frac{p^n R_{(p)}}{p^{3n} R_{(p)}}.$$

(c) The quotient group $E(p^n)/E(p^{3n})$ is isomorphic to the finite cyclic group $\mathbb{Z}/p^k\mathbb{Z}$ for some integer k.

(10) Suppose $f(x) = x^3 + ax^2 + bx + c$ can be factored as $(x - r_1)(x - r_2)(x - r_3)$. Prove that the discriminant of $f(x)$ is equal to

$$(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2,$$

and conclude that the curve $y^2 = f(x)$ is an elliptic curve if and only if $D \neq 0$.

(11) This problem outlines a proof of the full version of Nagell-Lutz (theorem 5).

(a) If $P = (x, y)$ has $y \neq 0$, let $2P = (X, Y)$. Using the elliptic curve addition formula, find a polynomial $\phi(x)$ satisfying $X = \frac{\phi(x)}{4f(x)}$.

(b) If additionally $P = (x, y)$ has finite order, explain why X must be an integer. Conclude that $f(x) \mid \phi(x)$.

(c) Check that

$$(3x^3 - ax^2 - 5bx + 2ab - 27c)f(x) - (3x^2 + 2ax + 4b - a^2)\phi(x) = D,$$

and conclude that $y^2 \mid D$.

point on a curve! These curves that classify elliptic curves are called **modular curves**. Mazur's proof boils down to showing that for sufficiently large n, the corresponding modular curve has no rational points, and therefore there are no elliptic curves with a point of order n.