DAY 2: ELLIPTIC CURVES

CURVES THAT CLASSIFY GEOMETRY PROBLEMS J-LO MC2022

When stereographic projection fails

Consider the collection of triangles with integer side lengths, integer area, and two sides in a ratio of 3 to 4. It turns out (see problem (14)) that primitive solutions can be classified by rational points on the curve

$$E : y^2 = x(x-9)(x-16).$$

Definition. A curve defined by an equation of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial with three distinct roots,[1] is called an **elliptic curve**.

(1) The line $y = 2x$ passes through the rational point $(0, 0)$ on the elliptic curve E defined above. Where else does this line intersect? Do you get a rational point?

If we intersect a line $y = mx + v$ with an elliptic curve $y^2 = f(x)$, we end up with an cubic equation in x:

$$0 = f(x) - (mx+v)^2 = x^3 + (a-m^2)x^2 + (b-2mv)x + (c-v^2).$$

This cubic will factor as $(x-r_1)(x-r_2)(x-r_3)$ for some $r_1, r_2, r_3 \in \mathbb{C}$, where r_1, r_2, r_3 will be the x-coordinates of the intersection points. Stereographic projection fails because even if r_1 is rational, it's possible for r_2 and r_3 not to be. However, if r_1 and r_2 are both rational, then r_3 will be as well!

(2) Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are rational points on an elliptic curve $y^2 = x^3 + ax^2 + bx + c$. Assume $x_1 \neq x_2$ and set $m = \frac{y_2 - y_1}{x_2 - x_1}$. Prove that the line through P and Q also intersects the rational point (x_3, y_3) where

$$x_3 = m^2 - a - x_1 - x_2, \qquad y_3 = m(x_3 - x_1) + y_1.$$

Defining an operation

Given two rational points, problem (2) gives us a third. This suggests we can define an *operation* on rational points: $P \star Q$ is defined to be the third point on the line connecting P and Q. But how should we define $P \star Q$ if $x_1 = x_2$?

[1] Tomorrow we'll see what can happen if $f(x)$ does not have three distinct roots.

(3) Intersect the line $y = 4x - 40$ with the elliptic curve $y^2 = x(x-9)(x-16)$ (Hint: $x = 8$ gives one solution). What do you notice about the roots r_1, r_2, r_3? What is happening geometrically?
(4) Using the previous problem as inspiration, come up with a reasonable definition and formula for $P \star P$.[2]

What if $P \neq Q$ but they have the same x-coordinate, k? In this case, intersecting $y^2 = f(x)$ with the line $x = k$ gives us a *quadratic* equation in y, not a cubic. So there are only two intersection points, even if we count multiplicity.

To fix this, we introduce a new point.

Definition. There is a point O, called the **point at infinity**, with the following properties:

- O is not a point in the plane.
- O *is* a rational point on every elliptic curve (so every rational point of E is either O or (x, y) for some $x, y \in \mathbb{Q}$).
- Every vertical line in the plane passes through O.
- $O \star O = O$.

(This is a bit of a hack, but it works! If you want a more satisfying explanation for the point at infinity, see problem (16).)

Definition. Given an elliptic curve E, we write $E(\mathbb{Q})$ to denote the set of rational points of E, including the point at infinity.

(5) Convince yourself that $P \star Q$ is now defined for any $P, Q \in E(\mathbb{Q})$. (Some cases to consider: What if $Q = O$? What if $P = Q = (x, 0)$ for some $x \in \mathbb{Q}$?)
(6) For any $P, Q \in E(\mathbb{Q})$, prove that $(P \star Q) \star Q = P$.
(7) On the curve $E : y^2 = x(x-9)(x-16)$, compute $(0,0) \star ((8,8) \star (18,18))$ and $((0,0) \star (8,8)) \star (18,18)$.

Some of these properties make $\star$ rather messy to work with. We can fix some of these issues as follows.

[2]While it's possible to solve this purely algebrically, the most straightforward solution uses some tools that are not required to know as prerequisite for this class. If you don't want to work out the details yourself, I'm happy to just give you the answer for this problem.

DEFINING A BETTER OPERATION

Definition. The operation of **elliptic curve addition** is defined by

$$P \oplus Q := (P \star Q) \star O.$$

(8) Check that $\oplus$ is commutative.
(9) For all rational points P, check that $P \oplus O = P$.
(10) Given any rational point P, find a rational point $\ominus P$ satisfying $P \oplus (\ominus P) = O$.

If you've taken group theory, you may notice that with these properties are very close to making the set of rational points into an abelian group! The only condition we're missing is associativity. This property also happens to be true, but proving it rigorously is going to take too long for this class.

(11) Experiment with the "Elliptic curve associativity" applet (use the QR code at the top of this worksheet to find it) to convince yourself that $(P \oplus Q) \star R = P \star (Q \oplus R)$ for all $P, Q, R \in E(\mathbb{Q})$, and therefore that associativity holds.
(12) Sketch an elliptic curve, choose a point P on the curve, and draw all the lines that are needed in order to compute $P \oplus P \oplus P$.
(13) The point $P = (2, 3)$ is on the curve $y^2 = x^3 + 1$. Compute $P \oplus P$, $P \oplus P \oplus P$, etc. What do you observe?

FURTHER EXPLORATION (OPTIONAL)

There's a lot to explore today! I recommend skimming through all the problems and just trying the ones that look most interesting to you. We'll use the results of (14) and (15) tomorrow, so if you don't like being told to assume things without proof, then you should do them, but the rest are purely for exploration.

(14) Fix positive integers m and n, and consider the collection of triangles with integer side lengths a, b, c, integer area A, and $\frac{a}{b} = \frac{m}{n}$. We will relate these triangles to rational points on an elliptic curve.
   (a) Relate A, a, b, c using Heron's formula. Show that any solution corresponds to a rational point on the curve

   $$C_1 : w^2 = (z + m + n)(z + m - n)(z - m + n)(-z + m + n)$$

   for an appropriate definition of the variables z and w.
   (b) Set $z = \frac{1}{v} - m - n$ and $w =$??? to obtain

   $$C_2 : u^2 = (2mv - 1)(2nv - 1)(2(m + n)v - 1).$$

(c) Finally, use horizontal/vertical translations/stretches to obtain

$$E_{m,n} : y^2 = x(x - m^2)(x - n^2).$$

(d) Not all rational points on $E_{m,n}$ give valid primitive solutions. What extra conditions on x and y are required in order to guarantee that the corresponding values of a, b, c, A are all positive integers?

(15) Using the previous problem, we will generate new triangles with a ratio $\frac{a}{b} = \frac{3}{4}$ — but something will go wrong if we try to do the same thing with $\frac{a}{b} = \frac{4}{5}$.

(a) Let $m = 3$ and $n = 4$. Starting with the solution $(a, b, c, A) = (3, 4, 5, 6)$, trace through the variable changes from the previous problem; what is the corresponding rational point $P \in E_{3,4}(\mathbb{Q})$?

(b) Compute a few small multiples of P using elliptic curve addition. Use these to find new primitive triangles with integer side lengths and area with two sides in a ratio of 3 to 4.

(c) This time let $m = 4$ and $n = 5$. Starting with the solution $(a, b, c, A) = (4, 5, 3, 6)$, what is the corresponding rational point $P \in E_{4,5}(\mathbb{Q})$?

(d) Can you find any new primitive triangles with integer side lengths and area with two sides in a ratio of 4 to 5? What goes wrong in this case?

(16) This problem gives a very brief introduction to projective geometry, and an explanation for the point at infinity. Consider the following equation in three variables, where a, b, c are integers:

$$\mathcal{E} : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

(a) Show that solutions to $\mathcal{E}$ come in lines through the origin: that is, if $(X, Y, Z) \in \mathbb{R}^3$ is a solution, then so is (tX, tY, tZ) for all $t \in \mathbb{R}$.

(b) Show that there is a bijection between points $(x, y) \in \mathbb{R}^2$ satisfying

$$E : y^2 = x^3 + ax^2 + bx + c$$

and lines through the origin contained in $\mathcal{E}$, with one exception: which line in $\mathcal{E}$ does not correspond to any point in the plane?

(c) Fix a constant k, and intersect $\mathcal{E}$ with the equation $X = kZ$. What are the lines of intersection? Compare your result to what you get if you intersect E with $x = k$.

(d) Intersect $\mathcal{E}$ with the equation $Z = 0$. What are the lines of intersection?

(17) If you feel comfortable with projective geometry, look up the "Cayley–Bacharach theorem" then (a) see if you can figure out why it implies $\oplus$ is associative, and (b) try to prove it.

(18) Did you go to Eric's colloquium and feel sad that he didn't explain the change of variables to you? Then here's your chance to fill in the details! To recap, we are trying to find positive integers a, b, c satisfying

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = 4.$$

(a) Setting $u = \frac{a+c}{c}$ and $v = \frac{b}{c}$, show (u, v) is a rational point on the curve

$$F_1 : u^3 - 3u^2v - 3uv^2 + v^3 + (u-1)(v-6u) = 0.$$

(b) If $v \neq 6u$, set $r = \frac{u}{v-6u}$ and $s = \frac{1}{v-6u}$ and show that (r, s) is a rational point on

$$F_2 : s^2 - rs = 91r^3 + 69r^2 + 15r + 1.$$

(c) The last step may look like black magic: I pulled some change of variables out of nowhere and suddenly one of the variables has degree only 2! Can you figure out why this happened? Why would I have suggested a change of variables of this form? What's going on geometrically?
(Hint: find all the points on F_1 that satisfy $v = 6u$, and think about points at infinity.)

(d) Complete the square on the left, then use some translations and stretches to get the elliptic curve

$$F_3 : y^2 = x^3 + 109x^2 + 224x.$$

(e) What conditions on x and y will guarantee that $a, b, c > 0$?