DAY 5: ON BEYOND ON BEYOND 1

CURVES THAT CLASSIFY GEOMETRY PROBLEMS J-LO MC2022

On beyond genus 1

Here's another classification problem: pairs of triangles with integer side lengths, one right and one isosceles, that have equal area and equal perimeter.

(1) Using the classification of Pythagorean triples from day 1, prove that the right triangle has side lengths $(k(1-t^2), 2kt, k(1+t^2))$ for some rational t, k, and the isosceles triangle has side lengths $(2\ell(1-x^2), \ell(1+x^2), \ell(1+x^2))$ for some rational x, ℓ. (Warning: we are not assuming the height of the isosceles triangle is an integer!) Conclude that we must have a solution to the equations

$$\tfrac{k}{\ell}(1+t) = 2, \qquad \left(\tfrac{k}{\ell}\right)^2 t(1-t^2) = 2x(1-x^2).$$

(2) Set $v = \frac{k}{\ell}$. Solving for t in the first equation and plugging it into the second, show that we obtain a rational point on the curve

$$4v^2 - 2(x^3 - x + 6)v + 8 = 0.$$

(3) By completing the square, change variables to

$$y^2 = (x^3 - x + 6)^2 - 32.$$

An equation of the form $y^2 = f(x)$, where $f(x)$ has degree at least 5 and has distinct roots, is called a *hyperelliptic curve.*

(4) There are two rational points with $x = \frac{5}{6}$. Use one of these to produce a solution to the original problem.

(5) Find as many rational points as you can, and determine which of them result in valid triangles.

Classification of curves

Any smooth curve can be classified by its *genus.* The technical definition of genus is beyond the scope of this course,[1] but for curves of the form $y^2 = f(x)$ (where $f(x)$ has distinct roots), the genus equals $\lfloor \frac{d-1}{2} \rfloor$.

[1] Essentially, the genus is the number of holes in the set of complex solutions (including points at infinity). Conic sections are spheres, elliptic curves are tori, genus 2 curves are 2-holed surfaces, etc.

Genus 0. A smooth curve of genus 0 with one rational point has infinitely many, and these can be found by stereographic projection.

Genus 1. A smooth curve of genus 1 is an elliptic curve. The number of rational points of finite order is $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 16$ (Mazur), and it is easy to find all the points of finite order (Nagell-Lutz).

Theorem 1 (Mordell, 1922)**.** *If E is an elliptic curve with rational coefficients, then $E(\mathbb{Q})$ is* finitely generated*. That is, there exists a finite list $P_1, \ldots, P_r \in E(\mathbb{Q})$ of points of infinite order with the property that every rational point can be written in the form*

$$n_1P_1 + \cdots + n_rP_r + Q$$

for exactly one choice of integers $n_1, \ldots, n_r$ and one choice of point Q of finite order.

However, there is no known algorithm that is guaranteed to determine the number r. There are techniques to compute upper and lower bounds for r,[2] and for most elliptic curves this is enough to nail down r exactly, but no one has proven that this will always occur. There is also a conjectural formula for r that has not yet been proven or disproven (Birch and Swinnerton-Dyer conjecture).

Genus ≥ 2. Another extremely difficult theorem:

Theorem 2 (Faltings, 1983)**.** *If a curve defined by a polynomial with rational coefficients has genus greater than 1, then it has finitely many rational points.*

Unfortunately, there is no general algorithm that is guaranteed to find them all, and no way in general to prove that you've found them all. There are techniques that work in very special cases; for instance, it was proven in 2018 that the curve $y^2 = (x^3 - x + 6)^2 - 32$ from the previous section has exactly *eight* rational points (not counting points at infinity), and therefore that there is only one solution to the corresponding triangle problem.[3]

On beyond dimension 1

Probably my favorite open math problem. We're going to classify boxes with integer side lengths and diagonals; these are called "perfect cuboids." That is, we

[2] Lower bounds are obtained by using a computer to search for more rational solutions, and using a "height pairing" to prove that the points found so far are independent. Upper bounds are trickier in general; see problem (8) for one example of an upper bound proof.

[3] Hirakawa, Y. and Matsumura, H. "A unique pair of triangles." *Journal of Number Theory*, Vol. 194, Elsevier, Jan. 2019. pgs. 297—302

need integers a, b, c such that $a^2 + b^2, a^2 + c^2, b^2 + c^2$, and $a^2 + b^2 + c^2$ are all squares. It is an open problem to determine whether any such box exists.

(6) Once again using the classification of Pythagorean triples, prove that there is a one-to-one correspondence between primitive perfect cuboids and triples (r, s, t) of rational numbers satisfying

$$\left(\frac{1-r^2}{2r}\right)^2 + \left(\frac{1-s^2}{2s}\right)^2 = \left(\frac{1-t^2}{2t}\right)^2$$

(and some inequalities).

Rather than a curve in the plane, this defines a *surface* in space (sometimes called the "box variety"). Finding rational points on a surface is considerably harder than for a curve. Maybe one of you will find a new way to find rational points!

Further Exploration (optional)

There is one remaining problem from day 1 that we haven't yet discussed: right triangles with integer side length and perfect square area. We will prove that no solutions exist using a process called "infinite descent," and use this to find our first example of an elliptic curve where we can *prove* that it has only finitely many points.

(7) Let's first prove that there are no right triangles with integer sides lengths and square area. To do this, we assume there is a solution, and take the one with smallest area. By the classification of Pythagorean triples, the side lengths can be written in the form $p^2 - q^2$, $2pq$, and $p^2 + q^2$ for some relatively prime integers p, q with $p > q$.

(a) If p and q were both odd, show that replacing p and q with $\frac{p+q}{2}$ and $\frac{p-q}{2}$ would give a smaller scaled copy of the original triangle. So since we started with the smallest example, p and q must have had opposite parity.

(b) By considering the area of the triangle, prove that p, q, $p+q$, and $p-q$ are all perfect squares.

(c) Set $r^2 = p + q$, $s^2 = p - q$, $u = \frac{r+s}{2}$, and $v = \frac{r-s}{2}$. Prove that u and v are the side lengths of a right triangle with integer side lengths and square area that is smaller than the original. This contradicts the fact that we started with a solution with smallest possible area. Hence no solution can exist.

(8) We can use the previous problem to prove a specific elliptic curve has only finitely many rational points (or in other words that it has rank 0).

(a) A right triangle with integer sides and square area corresponds to integers a, b, c, k satisfying $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = k^2$. By solving for b in the second equation and plugging the result into the first, show that primitive solutions correspond to rational points on the curve

$$u^4 + 4 = v^2.$$

(b) Set $v = w + u^2$ in order to cancel the u^4 terms. Multiply the resulting equation by $\frac{2}{w^3}$ to obtain the curve

$$y^2 = x^3 - x.$$

(c) Prove that the elliptic curve $y^2 = x^3 - x$ has exactly four rational points.

REFERENCES

A lot of the material from these worksheets — especially the material about the Nagell-Lutz theorem — was based on the book *Rational points on elliptic curves* by Silverman and Tate.