

Elliptic curves: what are they and why should we care?

Ravi Ramakrishna

Notes by Adeel Ahmad Khan

23 October 2010

Notes from a short lecture given by Ravi Ramakrishna at SUMS 2010, James Madison University.

The basic problem in number theory is solving equations of the form $f(x_1, \dots, x_n) = 0$ in integers. The problem $x^n + y^n = z^n$ was posed by Fermat and solved by Wiles in 1994.

Pell's equation. Let's talk about a different type of Diophantine equation: $x^2 - 2y^2 = 1$. Two trivial solutions are $(1, 0)$ and $(3, 2)$. Note that if we don't restrict ourselves to the rationals, we can factor

$$x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2}) = 1.$$

Squaring both sides, we get

$$(x^2 + 2y^2 + 2xy\sqrt{2})(x^2 + 2y^2 - 2xy\sqrt{2}) = 1,$$

and

$$(x^2 + 2y^2)^2 - 2(2xy)^2 = 1.$$

Thus for any solution (x, y) we can generate a new solution $(x^2 + 2y^2, 2xy)$. For example, the solution $(3, 2)$ generates the solution $(17, 12)$.

Now let's say we have two solutions, (r, s) and (u, v) . Then

$$(r^2 - 2s^2)(u^2 - 2v^2) = 1.$$

Factoring each of these as above, we can rewrite this as

$$(r + s\sqrt{2})(r - s\sqrt{2})(u + v\sqrt{2})(u - v\sqrt{2}) = 1,$$

and we can rewrite this as

$$(ru + 2sv)^2 - 2(rv + su)^2 = 1.$$

Again, we have a way to generate a third solution given two known solutions. In fact we have a group here, that has composition given by $(r, s) \circ (u, v) = (ru + 2sv, rv + su)$.

It turns out that *all* solutions to the equation are given by this method.

Pythagorean triples. Now let's go back to $a^n + b^n = c^n$, and look at the case where $n = 2$. Some solutions to this are $(3, 4, 5)$, $(6, 8, 10)$.

Let's dehomogenize the equation by setting $x := a/c$, $y := b/c$. Then we get the equation $x^2 + y^2 = 1$. This way we only look at primitive solutions. It turns out that $(0, 1)$, $(0, -1)$, $(1, 0)$, $(-1, 0)$ are solutions that actually generate all solutions. For example, let's start with $(0, 1)$.

Consider lines $y = mx + 1$ through $(0, 1)$ with rational slope m . We can calculate the second intersection of the line with the circle $x^2 + y^2 = 1$. We can substitute to get

$$x((m^2 + 1)x + 2m) = 0,$$

so that $x = 0$, or

$$(x, y) = \left(-\frac{2m}{m^2 + 1}, \frac{-m^2 + 1}{m^2 + 1} \right)$$

This generates (almost) all solutions to the equation. Thus we (almost) have a bijection between lines $y = mx + 1$ and solutions to $x^2 + y^2 = 1$. But what about $(0, -1)$? The line joining $(0, 1)$ and $(0, -1)$ has equation $x = 0$ and cannot be written as $y = mx + 1$. This is why we missed the solution $(0, -1)$.

The complex case. Let's find complex solutions to $x^2 + y^2 = 1$ now. It's the exact same procedure. We get one solution for each $m \in \mathbb{C}$. But this time we have to avoid $m = \pm i$. It's

because we dehomogenized $a^2 + b^2 = c^2$. If we rehomogenize the equation, the solution

$$(x, y) = \left(-\frac{2m}{m^2 + 1}, \frac{-m^2 + 1}{m^2 + 1} \right)$$

becomes

$$(a, b, c) = (-2m, -m^2 + 1, m^2 + 1).$$

The $x = 0$ solution gives $(x, y) = (0, -1)$ which corresponds to $(0, -1, 1)$. We also get a solution corresponding to $m = \infty$, actually, so the solutions to $a^2 + b^2 = c^2$ correspond to $\mathbb{C} \cup \{\infty\}$, the Riemann sphere.

Let f be a homogeneous degree d polynomial with rational coefficients, e.g. $a^d + b^d - c^d$. We want to find all the “not the same” solutions to $f(a, b, c) = 0$ in \mathbb{Q} . It turns out the answer is governed by the geometry of the “not the same” complex solutions.

For $f(a, b, c) = a^2 + b^2 - c^2 = 0$ we saw the complex solutions formed the surface of a sphere. The number of holes in the space of complex solutions is called the *genus* of the surface. The $d = 2$ case corresponds to genus 0. Finding rational points on genus 0 curves is relatively easy. An example of a genus 1 surface is a donut (torus).

L.J. Mordell conjectured that if the “not the same” complex solutions to a degree d homogeneous equation $f = 0$ is a surface whose genus $g > 1$, then the number of “not the same” solutions to $f = 0$ in \mathbb{Q} is finite. Faltings proved the conjecture. His proof was not “effective” in the sense that, given f , from this data there is known way to tell when we’ve found all the solutions, e.g. check all $a, b, c \in \mathbb{Q}$ with numerator and denominator at most d^{d^2} , the sum of the absolute values of coefficients of f .

Elliptic curves. In a sense, elliptic curves are “what’s left”, since genus 0 and genus > 1 have been solved. It turns out that elliptic curves also form a group. Consider $y^2 = x^3 - 9x + 9$ which has homogenization $b^2c = a^3 - 9ac^2 + 9c^3$. The “extra” point at infinity is $(0, 1, 0)$.

The group composition \circ is defined by taking the intersection of the line through P_1 and P_2 , and then reflecting over the x -axis. Thus all solutions to the equation are rational because we have two rational solutions $P_1 = (1, 1)$ and $P_2 = (3, 3)$. In this case we get $P_1 \circ P_2 = (-3, 3)$. Then we get more solutions, $(-3, 3) \circ (1, 1) = (9/4, -3/8)$, and $(-3, 3) \circ (9/4, -3/8) = (57/49, -111/343)$.

For a general elliptic curve E with dehomogenized form $y^2 = x^3 + \alpha x + \beta$ with $\alpha, \beta \in \mathbb{Q}$, let $E(\mathbb{Q})$ denote all rational solutions.

By the way, there is a theorem that basically states that it is impossible to solve general diophantine equations. That's why we're sticking to three variables.

Theorem (Mordell-Weil). $E(\mathbb{Q})$, the different solutions to the homogenized equation is the direct sum of the "finite part" and \mathbb{Z}^r , $r \in \mathbb{Z}$.

How can we determine r from α, β ? We don't know, but there is an algorithm to do this. Unfortunately it only terminates if the Tate-Shafarevich group is finite. We believe this but it has only been proven in some cases.

How big can r be? We don't know. Currently we know of an elliptic curve with $r = 28$, but we believe there are elliptic curves for r as large as we like.

The Birch and Swinnerton-Dyer conjecture is as follows. For a given elliptic curve E , the r -value is equal to the order of vanishing of the L -function $L(E, s)$ of E at $s = 1$. Essentially the conjecture asserts the number of solutions is finite iff $L(E, 1) \neq 0$.

In conclusion we note three points.

1. Solution sets of diophantine equations often have a nice group structure.
2. Geometry and arithmetic are intertwined.
3. Elliptic curves are not understood well.