Elliptic curves: an overview

Shahed Sharif

October 13, 2009

1 Algebraic basics

The basic problem we'd like to deal with is finding all solutions to a system of polynomial equations over $\mathbb{Q}$ (or some other chosen, non-algebraically closed field). Linear equations are easy to solve. Conics, though quite a bit trickier, are still easy: take for example the problem of finding all integer Pythagorean triples. That is, we want all rational solutions to

$$x^2 + y^2 = 1.$$

This has one easy solution, namely $(-1, 0)$. We project from that point onto the line $x = 0$; that is, for every point P on the circle ($P \neq (-1, 0)$), we construct the line from $(-1, 0)$ to P and see where it intersects $x = 0$. By degree considerations, there will always be another point of intersection. If P has rational coordinates, then the point we obtain on the line must have rational coordinates. Conversely, suppose we start with a point Q on the line $x = 0$ and connect it to $(-1, 0)$. If Q has rational coordinates, then the line has a rational equation. The intersection points with the circle give rational degree 2 equations in x and y respectively. But for each quadratic, one of the roots is rational (given by $(-1, 0)$), hence the other must be also. Therefore the other intersection with the circle has rational coordinates. One can make this entirely explicit: the point $(0, t)$ on the line corresponds to the point

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right)$$

on the circle.

This idea works for any conic, provided the conic has at least one rational point to begin with, and is not degenerate (for example, $x^2 + y^2 = 0$ is degenerate).

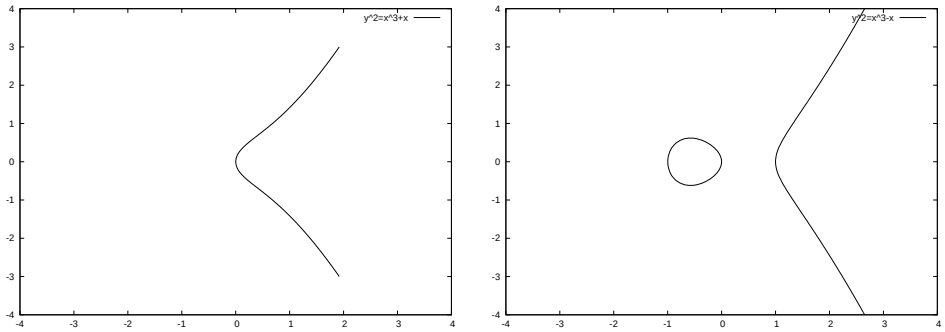
The next step is to look at cubics—and this is where things get interesting. Any cubic without singularities (cusps or nodes) can be put in the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;$$

this is known as Weierstrass form. In fact, by a change of variable we may put it in the nicer form

$$y^2 = x^3 + ax + b.$$

Henceforth we let $f = x^3 + ax + b$. The real points can have two basic shapes:



Let us consider the example $y^2 = x^3 - 21x - 20$, which looks roughly like the right curve above; we call this curve E for short. We wish to find its rational points. Inspection reveals the following solutions:

$$(-1, 0) \quad (5, 0) \quad (-4, 0) \quad (-3, 4).$$

We use the same sort of idea, with the added twist that "most" lines will intersect our curve in 3 points. For example, the line through $(-1, 0)$ and $(-3, 4)$ must intersect the curve in a third point, as we obtain a rational cubic equation in x and y. Two of the roots are rational, for example -1 and -3 for the x-coordinate, so the third point of intersection must have rational coordinates; it is $(8, -18)$. Repeating this procedure with the points $(-1, 0)$ and $(5, 0)$ we get $(-4, 0)$; this is the least interesting case (along with its permutations). Constructing the line through $(8, -18)$ and $(-3, 4)$, say, we get $(-1, 0)$ back. This isn't so great. But observe from the equation that if (x, y) is on the curve, then so is $(x, -y)$. Thus we may construct the line through $(8, 18)$ and $(-3, 4)$ to obtain[1]

$$(-409/121, 4680/1331).$$

Repeating with the reflection of the latter point and $(-3, 4)$, we get

$$(210152/529, 96332166/12167),$$

and so on. We may also use the tangent to a point, so for example the tangent to $(-3, 4)$ intersects the curve at one other rational point,

$$(105/16, 715/64);$$

the tangent to *this* point gives the new point

$$(337805601/32718400, 5500308411599/187149248000).$$

[1] All calculations were done with `gp/pari`.

It turns out that we can use these constructions to put an abelian group structure on the points of E. Namely, for P, Q points of E, we define $P + Q$ to be the point defined by first taking the line through P and Q, finding the third point of intersection, then *reflecting* across the x-axis. If $P = Q$, then we use the tangent line.

What is the identity of this group? Well, consider a vertical line through a given point (x, y). It intersects the curve at *one* other point, $(x, -y)$. If there were a third point of intersection O, then we'd have $(x, y) + O = (x, y)$; hence we introduce a point at infinity which lies on every vertical line and acts as the identity. Algebraically, this can be done by considering our curve in projective space.

We further observe from this example that $-(x, y) = (x, -y)$. That means that a point $P = (x, y)$ is a 2-torsion point if and only if $y = 0$. (These two observations show why the form $y^2 = f(x)$ is so nice.) Does this work more generally? Well, we saw using $(-3, 4)$ that the points $2^n(-3, 4)$ seemed to be getting more complicated, in the sense that they had more digits; and in fact $(-3, 4)$ has infinite order.

It turns out that the set of rational points is a finitely generated abelian group—this is the *Mordell-Weil Theorem*. That means that

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$$

where T is finite and r is some nonnegative integer, called the *rank*, or sometimes *algebraic rank*. The computation of T is not that hard; the determination of r, on the other hand, is the content of the *Birch and Swinnerton-Dyer conjecture*, one of the Millennium problems.

Singular cubics This approach works for every *nonsingular* cubic; we take nonsingular here to mean that the gradient is nonvanishing. If our curve is in the form $y^2 = f(x)$ for f a cubic, the nonsingularity is equivalent to f having no multiple roots, which is equivalent to the nonvanishing of its discriminant. If the curve is singular, then there are two cases: the curve is a *nodal* cubic if f has only two distinct roots, and it is *cuspidal* if it only has one root. These cases are quite easy to deal with, and are essentially the same as conics: we just project from the singular point.

Henceforth we look at nonsingular cubics. If a curve given by such a cubic has at least one rational point, we call it an *elliptic curve*. We consider these as projective objects, so for curves given by $y^2 = x^3 + Ax + B$, the point at infinity furnishes the required rational point.

Galois representation attached to 2-torsion Now let us look at the torsion points on E, including those which are not rational over the base field. In the case of 2-torsion, we see that determining these is equivalent to finding roots of f. Thus

$$E[2] \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Because our group law is defined over $\mathbb{Q}$, the natural Galois action on $E[2]$ respects addition of points. Thus the Galois action factors through a subgroup of

$$\mathrm{GL}_2(\mathbb{Z}/2).$$

On the other hand, the Galois group of a cubic equation (namely $f(x)$) is a subgroup of S_3. Since

$$\mathrm{GL}_2(\mathbb{Z}/2) \cong S_3$$

we have an explicit way of writing down the representation of the Galois group on the 2-torsion points.

This works more generally for higher torsion, as we shall see.

2 Analytic theory

It turns out that an elliptic curve is an example of a genus 1 curve. One definition of the genus is the dimension of the space of everywhere holomorphic differentials; in the case of $y^2 = f(x)$, with f a cubic with distinct roots, such a differential is provided by

$$\frac{dx}{y}.$$

But there is also a topological characterization of genus 1, as a torus. To that end, we shift gears and look at a complex analytic situation.

Let $\Lambda \subset \mathbb{C}$ be a *lattice*; that is, a rank 2 $\mathbb{Z}$-module which spans $\mathbb{C}$ over $\mathbb{R}$. For example, $\Lambda = \mathbb{Z} + \mathbb{Z}i$, the Gaussian integers. In general, we need only consider $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ for $\operatorname{im}\tau > 0$. Consider the Riemann surface $\mathbb{C}/\Lambda$; topologically, of course, this is just a torus. I claim that this Riemann surface has the structure of an algebraic curve. To show this, it is sufficient to find a complex-analytic embedding into projective space, and show the image is an algebraic curve. To find such an embedding, we must first understand the ring of meromorphic functions on $\mathbb{C}/\Lambda$.

A given meromorphic function on $\mathbb{C}/\Lambda$ is the "same" as a meromorphic doubly-periodic function on $\mathbb{C}$, with the periods given by Λ. The problem of finding such functions was solved by Weierstrass: attached to Λ is the *Weierstrass $\mathscr{P}$-function*

$$\mathscr{P} = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2},$$

and the ring generated by $\mathscr{P}$ and $\mathscr{P}'$ yields the set of all such functions. Now we consider the map $z \mapsto (\mathscr{P}(z), \mathscr{P}'(z)/2)$, which induces an embedding of $\mathbb{C}/\Lambda$ into projective space. (In projective coordinates, $z \mapsto [\mathscr{P}(z) : \mathscr{P}'(z)/2 : 1]$.) The poles of $\mathscr{P}$ and $\mathscr{P}'$ are exactly the points in Λ, hence only $0 \pmod{\Lambda}$ maps to a point at ∞ in $\mathbb{P}^2$. Is the image algebraic? Well, Weierstrass showed that

there is a single algebraic relationship between $\mathscr{P}$ and $\mathscr{P}'$. It is a cubic equation of the form

$$\left(\frac{\mathscr{P}'}{2}\right)^2 = \mathscr{P}^3 + A\mathscr{P} + B$$

for some constants A, B which depend on Λ. This of course looks like the elliptic curve

$$E : y^2 = x^3 + Ax + B.$$

Thus $z \mapsto (\mathscr{P}(z), \mathscr{P}'(z)/2)$ gives an isomorphism between $\mathbb{C}/\Lambda$ and the complex-valued points of E.

But the relationship is even stronger than that: it turns out that the isomorphism is as a *group*, where $\mathbb{C}/\Lambda$ has the additive structure inherited from $\mathbb{C}$.

What does this tell us about the rational points? Well, we can immediately conclude that

$$E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n,$$

since this is true for $\mathbb{C}/\Lambda$ (generated by $\frac{1}{n}$ and $\frac{\tau}{n}$ in the case $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$). If $A, B \in \mathbb{Q}$, then just as in the 2-torsion case, this allows us to attach to E a representation of the Galois group of $\mathbb{Q}$

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n).$$

Now suppose $A, B \in \mathbb{R}$. In this case, the map $z \mapsto (\mathscr{P}, \mathscr{P}'/2)$ respects complex conjugation. Looking at a fundamental domain for $\mathbb{C}/\Lambda$, one sees that there are two possibilities for the fixed points under complex conjugation: there are either one or two components. If $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, then these are $\mathbb{R}$ and possibly $\mathbb{R} + \tau/2$ (for example, if $\tau = i$ then the latter is fixed by conjugation; in general, the condition is $\overline{\tau/2} \equiv \tau/2 \pmod{\Lambda}$ if and only if there are 2 components). But this agrees with our picture from before. Notice also that two 2-torsion points lie on the "second" component; thus, the real points of E are disconnected if and only if $E[2]$ is entirely real.

The construction works in reverse, too; that is, given any elliptic curve E with equation $y^2 = x^3 + Ax + B$, there is a lattice Λ for which all of the above holds. In fact, Λ can be taken to be the group generated by the periods of the differential $dx/2y$. Note, for example, that the pullback of $dx/2y$ by the Weierstrass $\mathscr{P}$-map is

$$\frac{d\mathscr{P}}{\mathscr{P}'} = \frac{\mathscr{P}' dz}{\mathscr{P}'} = dz.$$

One last mention: we may take the exponential map $e^{2\pi i z}$ on $\mathbb{C}/\Lambda$, which yields an isomorphism with $\mathbb{C}^*/q^{\mathbb{Z}}$ for some complex number q; the latter representation of E is sometimes more useful, and is called the *Tate curve* for E with *Tate parameter* q.