Elliptic Curves

Outline

Hopefully, this talk is going to give answer to the following questions:

1. What are elliptic curves?

2. How is arithmetic done?

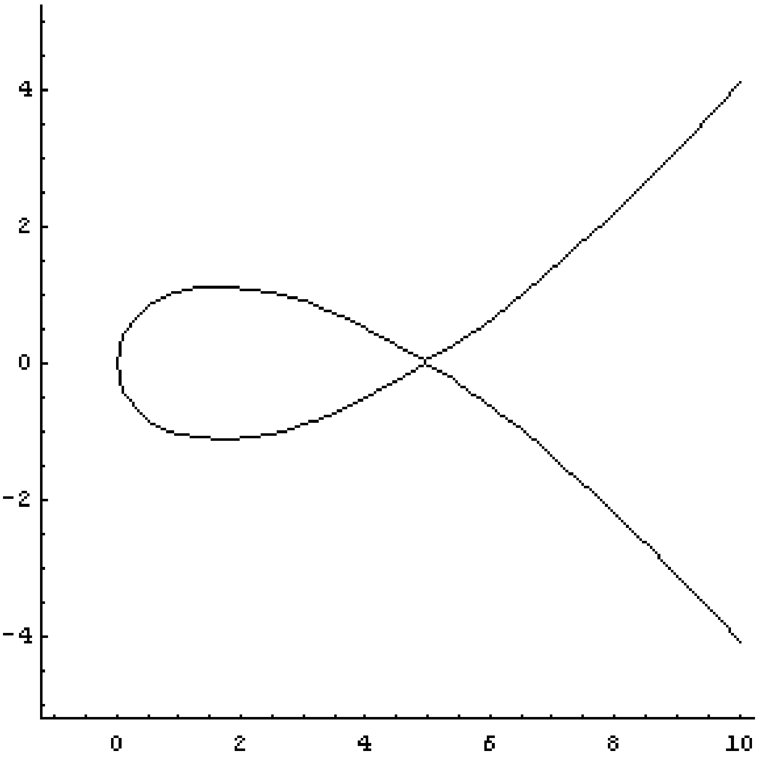
3. What are the applications of elliptic curves (e.g. in cryptography, number theory and the proof of Fermat's Last Theorem)

1. What are elliptic curves?

Let $f(x, y)$ be a polynomial of degree 3 in the two indeterminates x and y with coefficients in some field $\mathbb{F}$. Then the solution set to

$$f(x, y) = 0$$

is a cubic curve. For example, over $\mathbb{R}$, a cubic curve could look like this:

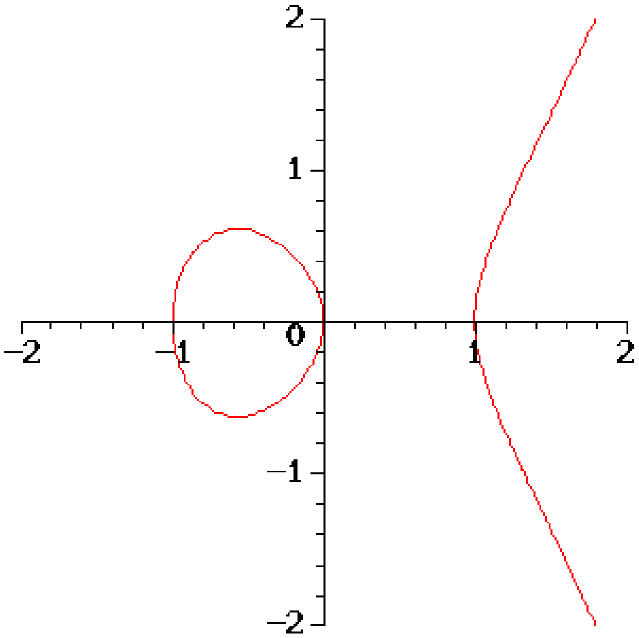


This figure is a plot of the curve

$$15y^2 = x(x - 5)^2.$$

This curve has a self-intersection at the point $(5, 0)$. As we shall see in a minute, we don't want elliptic curves to have cusps or self-intersections. Therefore, we call a cubic curve without such "bad" properties an *elliptic curve.*

Hence, an elliptic curve could look as follows:



This is the graph of the curve

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

We are now going to have a look at the "group law for elliptic curves"...

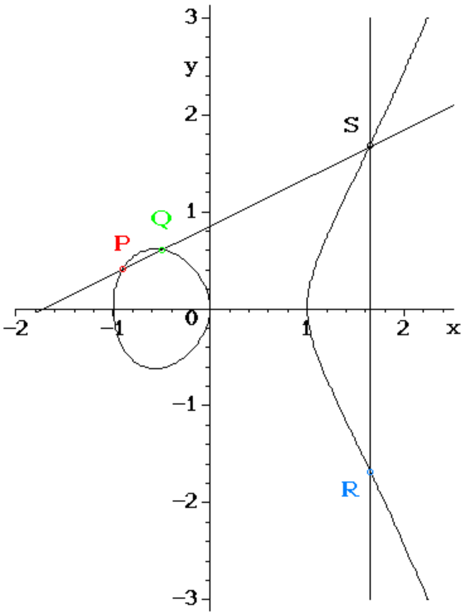
2. How is arithmetic done?

   As we can see from the last picture, any line that intersects an elliptic curve twice, will intersect it three times (counting multiplicities and the point at infinity).

   So we can define an operation on an elliptic curve by saying that we map two point onto the third intersection of the line through them.

   However, this will not be associative. But if we reflect that last point in the x-axis, then we will get an associative operation. This operation will have inverses for any given point, and thus turns the set of points on an elliptic curve into an abelien group.

   This is a picture of how it works (the elliptic curve is the same as in the last picture):



   Here, R will be the sum of P and Q. Of course, since $P = Q$ is possible, we can define what we mean by integer multiples of an arbitrary point on the curve. We will meet this idea again in the section on cryptography.

3. Applications

   Let us consider Cryptography first.

   Suppose we have an elliptic curve over a finite field at hand and we let P be a point on it. Then we can use the group law to define $k \cdot P$ as the sum of k copies of P (note that this can be done for all integers k).

   The ECDLP (Elliptic curve discrete logarithm problem) can be stated as follows:

   Let Q and P be points on the same elliptic curve, and assume Q is an integer multiple of P. Find $k \in \mathbb{Z}$ such that $k \cdot P = Q$.

   This task is an NP-Problem, so it is believed to be unsolvable is polynomial time. Furthermore, it is even harder than the factorization of large natural numbers, used by the *RSA*-Algorithm.

   Let us have a quick glance into Fermat's Last Theorem. Stated by Pierre de Fermat in the 17^{th} century, it remained a conjecture until 1995, when Andrew Wiles presented a proof.

   He proved a part of the Taniyama-Shimura-Theorem (the remaining bits have been proven until now) which implies Fermat's Last Theorem.