Isogeny Graphs

Chloe Martindale (Universiteit Leiden and Université de Bordeaux)
Supervised by Andreas Enge (Bordeaux), Peter Stevenhagen (Leiden)
and Marco Streng (Leiden)

October 16, 2015

Abstract

I will start by defining elliptic curves and isogenies and presenting an example. I will then explain how to draw an 'isogeny graph', whose vertices are elliptic curves and whose edges are isogenies, and say how these graphs are used in cryptography. Finally, I will give an idea of how to generalise these graphs to higher dimension.

Contents

1 Elliptic Curves and Isogenies **1**

2 Isogeny graphs **7**

These notes are from a talk presented at the PhD colloqium in Leiden University on 14th October 2015.

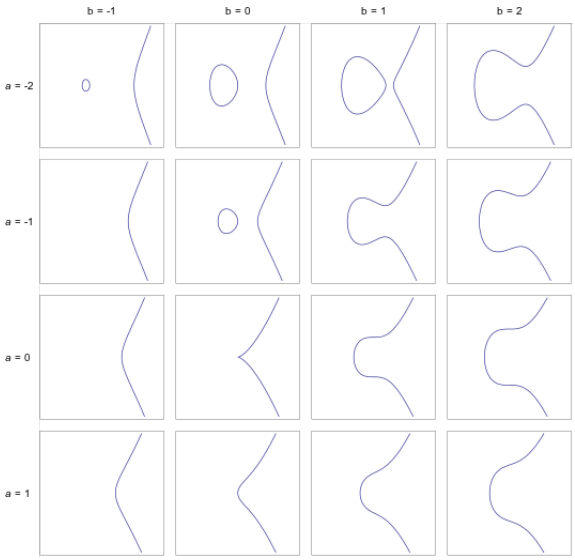
1 Elliptic Curves and Isogenies

Definition 1.1. An *elliptic curve* over $\mathbb{Q}$ is a non-singular curve that can be written as

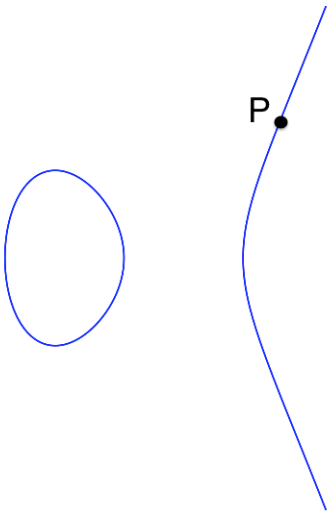
$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$.

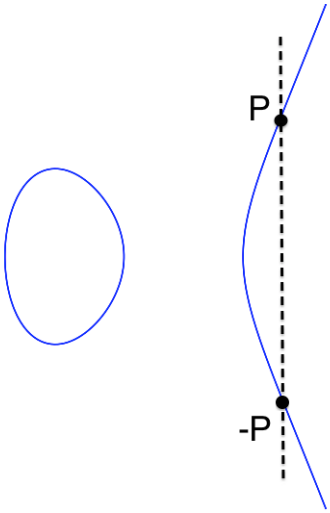
Remark 1.2. If you don't remember what 'non-singular' means, think of a any curve that has point which is not smooth i.e., a cusp or a node (self-intersection). You can see a curve with a cusp in the picture below (corresponding to $a = b = 0$).



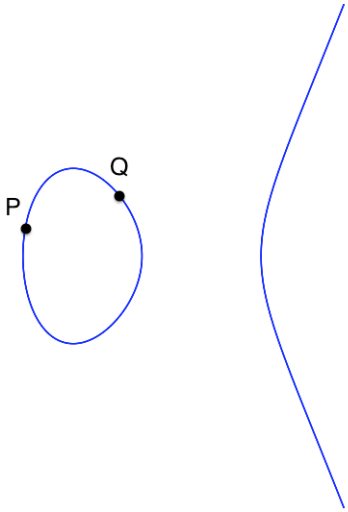
This picture is from [Tos]. This diagram shows the different forms that elliptic curves can take, i.e. a connected component topologically equivalent to a circle together with a line, or just a line. You can also see how you might transform one curve into another. If you haven't seen elliptic curves before, this might seem a fairly arbitrary thing to study, so let me try to convince that they are interesting objects! Historically, number theorists are interested in finding lots of rational (or integral) solutions to polynomials (think of Pythagoras' Theorem or Fermat's Last Theorem). With an elliptic curve, often knowing one rational point can help you find many others (sometimes infinitely many). To see this, imagine that you have an arbitrary elliptic curve and that you one rational point on it, P.



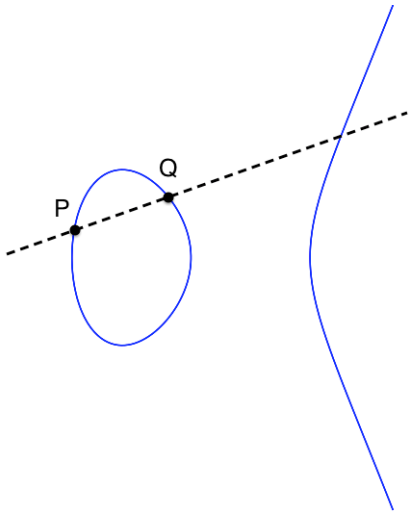
Then there is another rational point on the curve that is easy to find, which I will call $-P$, constructed as below:



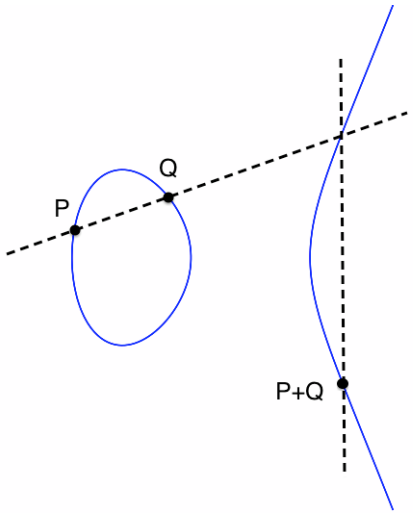
So now we have 2 points on the curve. But we would like a construction that we can repeat many times to get lots of rational points. Suppose now that we have managed to find 2 rational points of the curve, P and Q.



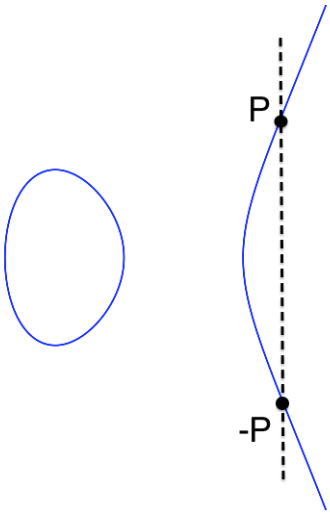
Given 2 points, there is an obvious geometrical construction that we can do to find another rational point..



but although this does give us a 3rd point, we can't take the construction any further since we only know these 3 points. But, if we combine the first construction we do get something useful, and so we define this point to be $P + Q$:



Now we can generate many more rational points, such as $2P+Q$ and $2Q+P$. Although in many cases this still gives us only finitely many rational points, it is also possible on some curves to find infinitely many rational points in this way. Now if we return to the picture defining $-P$,



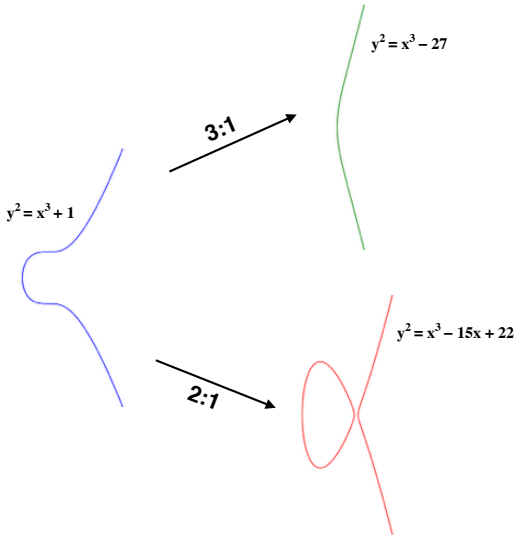
since we have defined a notion of addition, we should get that $P + (-P) = 0$, and so we define 'the point at infinity' to be the identity (i.e. zero).

Remark 1.3. This means that every elliptic curves has at least one point, 'the point at infinity'.

On some elliptic curves it may be very difficult to even find a first rational point, for example if it has a rational point with very large x and y coordinates. To get around this problem it is useful to be able to map one elliptic curve to another, motivating the following definition.

Definition 1.4. An *isogeny of elliptic curves* is a surjective morphism (i.e. a map that preserves addition and the point at infinity) between elliptic curves.

Here are 2 examples of isogenies:



These maps can be written down explicitly, for example the map from the blue curve to the green curve is given by

$$(x, y) \mapsto ((x^3 + 4)/x^2, (x^3y - 8y)/x^3).$$

Written above the map is '3:1', which means that for every (complex) point on the green curve there are 3 (complex) points on the blue curve which map to it.

Exercise 1.5. Which 3 points on the blue curve map to $(3, 0)$?

When an isogeny is $n : 1$, we say that it is an *n-isogeny*.

Definition 1.6. An isogeny from an elliptic curve to itself $E \to E$ is an *endomorphism*.

Example 1.7. Since we can add points on elliptic curves, we can also multiply (what would the geometrical construction be?), and so here are infinitely many examples of endomorphisms: let $n \in \mathbb{Z}$. Then

$$\begin{array}{ccc} E & \longrightarrow & E \\ P & \mapsto & nP \end{array}$$

is an endomorphism.

Definition 1.8. When endomorphisms in the example above are not the only endomorphisms on E, we say that E has *complex multiplication*.

2 Isogeny graphs

When we talk about graphs in this context, we are referring to a diagram made up of vertices and edges between the vertices, so before we can draw an isogeny graph we need to define what these vertices and edges represent.

Vertices
The vertices of the graph are elliptic curves with the coefficients a and b reduced mod p, where p is a prime which is not 2 or 3.

Remark 2.1. If you don't remember what 'reduced mod p' means, just think of a and b being an integer in the range $[0,p-1]$, together with the rule that $a+p=a$ and $b+p=b$.

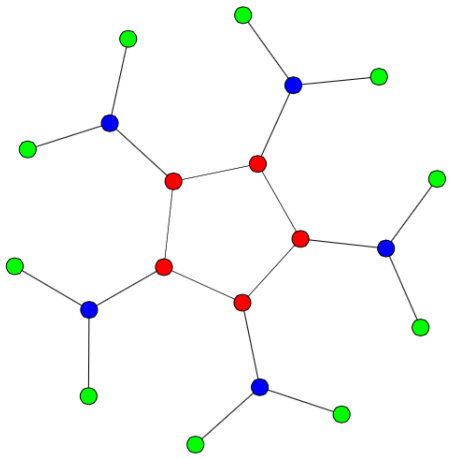
Remark 2.2. Because we have finitely many choices for our coefficients, we have finitely many choices for our elliptic curves, giving us a finite graph.

Remark 2.3. Elliptic curves of this form (with reduced coefficients) *always* have complex multiplication, so we have plenty of endomorphisms to play with!

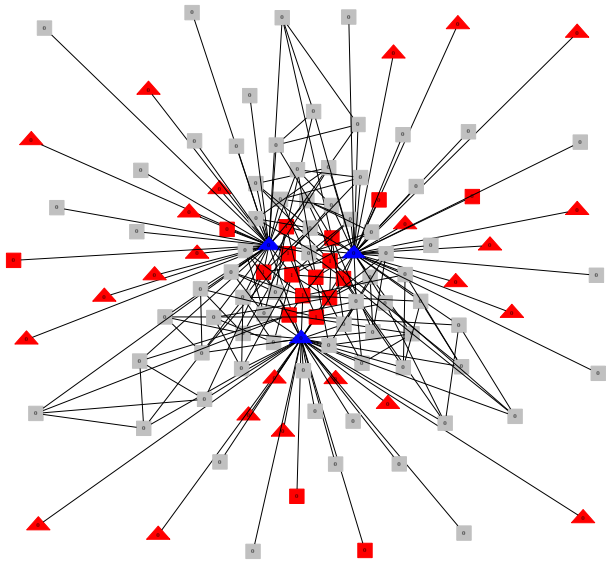
Edges
The edges of the graph are isogenies of degree ℓ, where ℓ is a prime different from p.

Remark 2.4. Recall that endomorphisms are isogenies, and if we draw all the endomorphisms on our graph (there are a lot!) it will look very messy, so we encode the data of the endomorphisms in a different way: we order our vertices by the amount of endomorphisms that they have. This is best explained by example, so here is an isogeny graph.

$\ell = 2$



In this picture, the red vertices have the most endomorphisms, and the green vertices have the least endomorphisms. When ordered in this way, isogeny graphs of elliptic curves are always this nice! In this picture ℓ must be 2 because there are always $\ell + 1$ edges from every vertex that is not at the end. The beautiful symmetry of this picture is why the graphs so useful for cryptography. If you have message encoded using elliptic curve cryptography with an elliptic curve E, you can easily draw the ℓ-isogeny graph containing E and so find all the curves isogeneous to E. But decrypting the message can be done on any of the curves in the graph, and there are some 'weak' curves which are easier to decrypt. Finally, my research is about computing these graphs in dimension 2, which means that the highest powers of x can be 5 or 6 rather than only 3, and that the graphs that we have to untangle look more like this one:



This was computed as part of a joint project with Ionica, Robert and Streng.

References

[Tos] "EllipticCurveCatalog" by Tos - Own work. Licensed under Public Domain via Commons - https://commons.wikimedia.org/wiki/File:EllipticCurveCatalog.svg /media/File:EllipticCurveCatalog.svg

[Koh] D. R. Kohel, Endomorphism rings of elliptic curves over finite fields, ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)University of California, Berkeley.

[Sut] A. V. Sutherland, Isogeny volcanoes. Algorithmic Number Theory Symposium (ANTS X), 2012. http://arxiv.org/abs/1208.5370