# Computing Elliptic Curve Isogenies

URSS 2009

by Jenny Cooley

supervised by John Cremona

My task was to write code that calculated relationships called isogenies between elliptic curves, and then to implement it into the open source mathematical software package Sage to be used, free of charge, by researchers, teachers and students of mathematics and other sciences the world over.

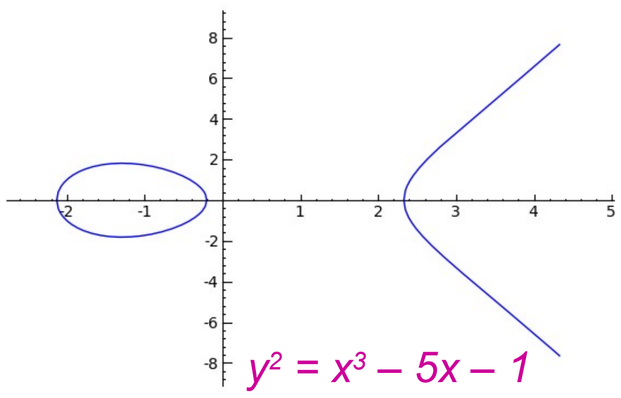
**Sage** A mathematician does not take for granted that a theorem is true without seeing the proof, especially if he or she is intending to use said theorem in some research of his or her own. And yet, many commercial mathematics programs ask you to do exactly that, hiding the code that is doing the calculating. This is not in the spirit of mathematics, or research in general. Sick of smug commercial packages such as Mathematica, which told them that the hidden code was too complicated for them to understand, and even not-for-profit packages such as Magma, which wouldn't let them implement all the things that would be useful to them in their research, academics sought a better solution. Thus was born **Sage.**

Sage is completely free, open source mathematical software that anyone may use, anyone may see how it works and anyone may add to. During my project I implemented **four new functions** into Sage, all concerning **elliptic curve isogenies.**

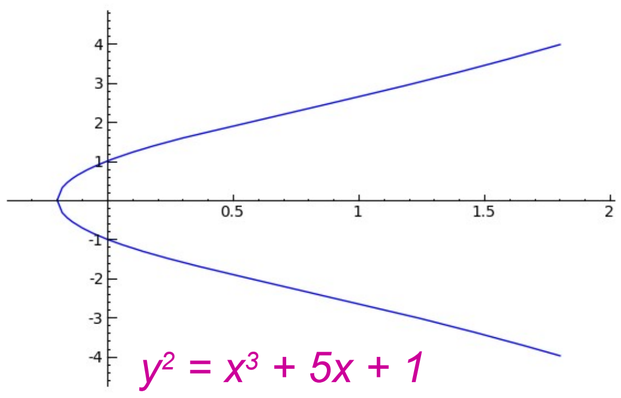
**Elliptic curves** can usually be written in the form:

$$y^2 = x^3 + Ax + B$$

and look a bit like this:



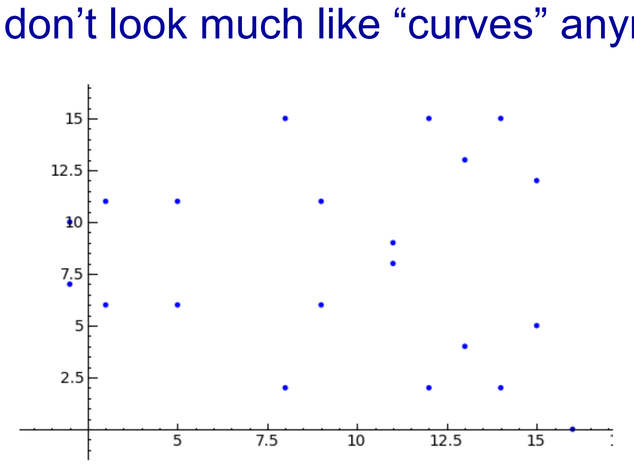

$y^2 = x^3 - 5x - 1$

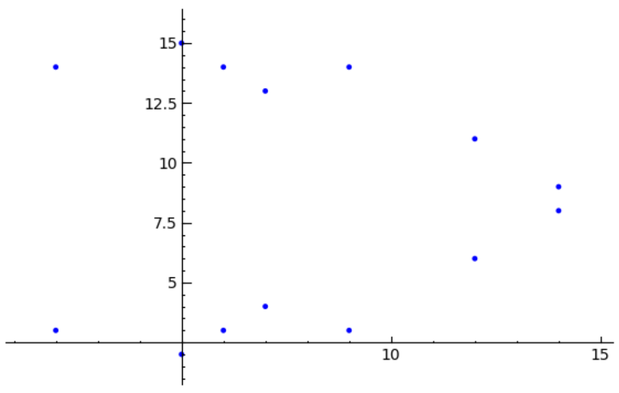



$y^2 = x^3 + 5x + 1$

These are examples of elliptic curves defined over the *rational numbers*. A rational number is a whole number or a fraction, so 4, ½, -7 and 1.3 are rational numbers, but π and √2 are not. An elliptic curve being defined over the field of rational numbers means that if you take any point on the curve, both the *x* and *y* coordinates will be rational numbers and the coefficients *A* and *B* (see above) must be rational numbers too.

Elliptic curves can also be defined over other types of numbers. Some of the code I wrote concerned elliptic curves over *finite fields*. Numbers in finite fields work a little bit like the numbers on a clock. For example the finite field of size 17 contains the numbers 0,1,2,3,…,15,16. In this finite field 10+12 is not 22, but rather 5, like on a clock where if you add 20 hours to 5 o'clock, you don't get 25 o'clock, you get 1 o'clock, this is because every time you get to 12, you go back down to 1 again. Here are a couple of examples of elliptic curves over the finite field of size 17 (N.B. they don't look much like "curves" anymore!):




**Isogenies** are relationships between elliptic curves. They are formulae that input the points of one curve and output the points of another. If an isogeny exists between two elliptic curves they are known as *isogenous*. Over finite fields two elliptic curves are isogenous if and only if they have the same number of points, thus it is relatively simple to tell whether or not they are isogenous. We can see quite easily that the two examples of elliptic curves over the finite field of size 17, pictured above, are *not* isogenous.

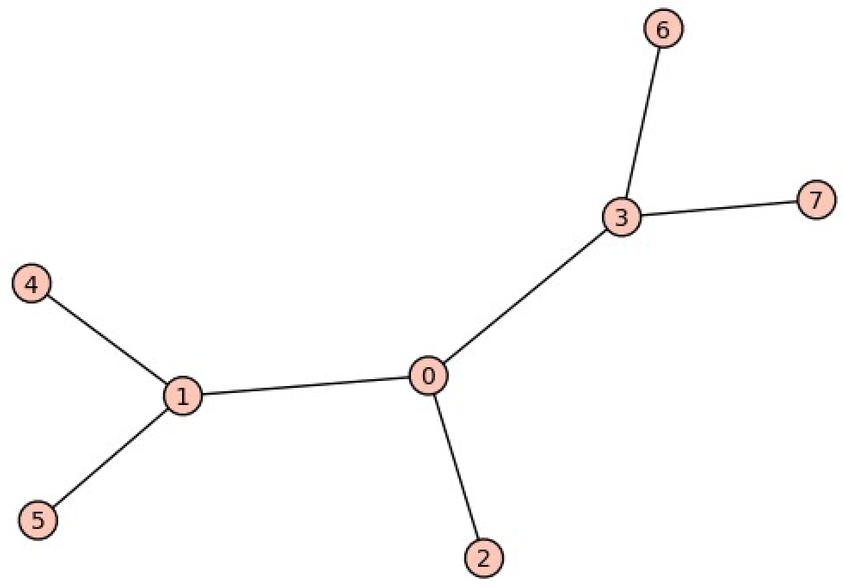
**My project** involved implementing the following four functions into Sage:

***l*_isogenies** gives a list of all the isogenies of degree *l* from the given elliptic curve. The *degree* is the number of points on the first curve that the isogeny maps to "zero" on the second curve.

**is_isogenous** outputs True or False to inform the user whether or not two elliptic curves are isogenous.

**isogeny_degree** returns the degree of the isogeny between two given curves.

Below, the numbered circles represent elliptic curves and the lines represent isogenies of degree 2 (2-isogenies).




**isogeny_class_new** returns a list of all the elliptic curves in the same *isogeny class* as the given elliptic curve.

The isogeny class of an elliptic curve is the set of all the curves it is isogenous to. The diagram above shows an isogeny class.

Probably my most significant **Project outcome** was that my isogeny_class_new code was used to verify the correctness and completeness of a database of around 800,000 elliptic curves, which was created by my supervisor five years ago and is used and referenced by Number Theorists around the globe. The database had been generated originally using code that, unlike our new code, only worked to a certain precision. Happily, after several hours of testing using **nine** computer processors, the database was found to be all correct. Mathematicians may continue to use the curves in the database without fear!

"My **experience** as an **Undergraduate Scholar** has been **hugely rewarding…**" "It appears to have given a **genuine taste** of academic research." "…and as a result of a **recommendation from my supervisor**, John, I have a topic and supervisor for a 3rd year dissertation."