581d -- elliptic curves in sage, October 11, 2010

Reminder: Office hours today 2:30-4:30; next week is ECC http://2010.eccworkshop.org/

(Probably next week will be: "Hidden Markov Models", which are a powerful statistical tool, which contain some surprising ideas. Their complete implementation in Sage provides a good case study of how to use Cython to write new very fast code in the context of Sage.)

Motivation: Elliptic curves look pretty simple. They are just cubic curves of the form

$$y^2 = x^3 + a*x + b,$$

with x,y the variables and a,b fixed constants in some field (e.g., typically the rational numbers, complex numbers, or in a finite field). But these curves are the quintessential central object of number theory in the sense that they are intertwined with everything else:

* cryptography: making cryptosystems (extremely important -- these are the *best*); it is only because of a fast algorithm of Schoof, Elkies, and Atkin for counting solutions that we can really use curves this way safely.
* cryptanalysis: integer factorization (critical algorithm)
* Diophantine equations: when a,b are integers, an elliptic curve is a special case of Diophantine equation (a polynomial equation with integer coefficients, who study goes back two thousand years). Amazingly, elliptic curves correspond to *solutions* to various Diophantine equations, e.g., x^n + y^n = z^n, and were used to prove Fermat's Last Theorem.
* Galois representations: one can associate representations of Galois groups of extensions of the rational numbers to elliptic curves.   Amazingly, these all turn out to be deeply related to "modular forms".

Elliptic curves are especially relevant because it is massively easier to compute with them than with general Diophantine equations or Galois representations.

Plan for the next three lectures:

1. TODAY:
    * how to create an elliptic curve in Sage:
        * Weierstrass form, Cremona tables
    * group law
    * visualizing elliptic curves in Sage
    * some of what is missing

Please, you should at least read through the last chapter of my undergrad number theory book:

2. WEDNESDAY: elliptic curves over finite fields
    * counting points mod p for lots of p
        - Sato-Tate, illustrated
    * integer factorization (Lenstra's algorithm)
    * fast point counting (Schoff-Elkies-Atkin) for counting points mod p for large p
    * structure of group of points
    * some of what is missing/slow
2. FRIDAY: elliptic curves over the rational numbers and number fields
    * Mordell-Weil groups

        * Regulator
    * Integer points
    * Tate's algorithm:
        * conductor
        * root number
        * Tamagawa numbers
    * Sha
    * Omega
    * Heegner points
    * L-function
    * some of what is missing/slow

How to create an elliptic curve in Sage:

```
   EllipticCurve?
   EllipticCurve([a,b]) makes y^2 = x^3 + a*x + b
```

There is a more general form in which to *specify* a curve, which is important when working over fields of characteristic 2 or 3, e.g., GF(2) or GF(3):

```
   EllipticCurve([a1,a2,a3,a4,a6])
   EllipticCurve(F, [a1,a2,a3,a4,a6])     # where F is a field (or ring)
```

Also, you can make an elliptic curve with given "j invariant":

```
   EllipticCurve_from_j(j)
```

Also:

```
   EllipticCurve_from_c4c6(c4, c6)
```

Other things:

```
   EllipticCurve_from_plane_cubic, EllipticCurve_from_plane_curve(C, P)   # but caveat!
```

Group Law:

How to make a point on a curve, do arithmetic, etc.

- do example over QQ, which illustrates components getting big
- example over RR or CC or intervals
- example over finite field
- generic example, which recovers the formula?
- proof of group axioms, generically

Visualizing elliptic curves in Sage:

- how to plot a curve over QQ, RR
- plot over GF(p); what fun!   (show interacts)
- do some sort of 3d plot using implicit plot, which will look ugly?

Some of what is missing/slow:

- cubic to curve: but Tanja Lange's student is almost done with this...
- working in terms of other coordinates, e.g., Edwards coords -- see [Bernstein, Lange]
- 3d visualization?
- benchmark basic arithmetic over a few rings compared to magma; does sage suck?