Resource I

Pari/gp

By Mordell's Theorem, the abelian group on an elliptic curve $\mathcal{E}(\mathbb{Q})$ over the rationals is finitely-generated, and so (by the structure theorem for finitely-generated abelian groups) it is expressible in the form

$$\mathcal{E}(\mathbb{Q}) = \mathbb{Z}^r \oplus T,$$

where T is a finite abelian group.

It is a straightforward matter to determine the torsion-group T; if the curve is given in standard form

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + ax^2 + bx + c$$

then each point $(x, y) \in T$ has integer coordinates x, y, and $y \mid \Delta$, the discriminant of the cubic.

But determination of the rank r is much more difficult. In fact there is no algorithm known that can compute the rank of any elliptic curve $\mathcal{E}(\mathbb{Q})$.

However, the Birch & Swinnerton-Dyer conjecture asserts that the rank is equal to the order of the zero of the L-function $L_{\mathcal{E}}(s)$ at $s = 1$. This is readily calculated (with a computer).

John Cremona, at the University of Warwick (in the UK) has drawn up complete data on several million elliptic curves.

The program `pari/gp` provides a simple entry into Cremona's tables. Here is a short example (run on the maths machine `hamilton`):

```
tim@hamilton:~> gp
? E = ellinit([1,1])
%1 = [0, 0, 0, 1, 1, 0, 2, 4, -1, -48, -864, -496, 6912/31,
  Vecsmall([1]), [Vecsmall([128, -1])], [0, 0, 0, 0, 0, 0, 0, 0]]
? ellanalyticrank(E)
%2 = [1, 1.7858094938692006870200553869231516042]
? quit
```

We start by describing the curve we are studying with the function `ellinit`. If the curve takes Weierstrass normal form

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + bx + c$$

then it is sufficient to give $[b, c]$ as argument to `ellinit`, as in the example above, which tells us that the curve

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + x + 1$$

has rank 0, ie the group is finite.

But if the curve is in the more general form

$$\mathcal{E}(\mathbb{Q}) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

then all 5 coefficients must be given, in correct order $[a_1, a_2, a_3, a_4, a_6]$.

$$\mathcal{E}(\mathbb{Q}) : y^2 + y = x^3 - x,$$

showing its rank is 1 (always, if we accept the Birch-Swinnerton-Dyer conjecture).

```
tim@hamilton:~> gp
? E2 = ellinit([0,0,1,0,-1])
%1 = [0, 0, 1, 0, -1, 0, 0, -3, 0, 0, 648, -243, 0,
  Vecsmall([1]), [Vecsmall([128, -1])], [0, 0, 0, 0, 0, 0, 0, 0]]
? ellanalyticrank(E2)
%2 = [1, 1.2901905903698635816913400201468347675]
? elltors(E2)
%3 = [1, [], []]
? quit
```

We've also found that the torsion group of this curve is trivial.

There are other functions one can apply; see `PariGpRefcard.pdf` (page 2) in `http://www.maths.tcd.ie/pub/Maths/Courseware/EllipticCurves/2016`

We can also use the program to look at elliptic curves over finite fields. Here we are looking at the curve

$$\mathcal{E}(\mathbb{F}_2) : y^2 + y = x^3 + 1.$$

```
tim@hamilton:~> gp
? E = ellinit([0,0,1,0,1],2)
%1 = [0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0,
  Vecsmall([4]), [1, [[Vecsmall([0, 1]), Vecsmall([0]),
  Vecsmall([0, 1])], Vecsmall([0, 1]), [Vecsmall([0, 1]),
  Vecsmall([0]), Vecsmall([0]), Vecsmall([0])]]], [0, 0, 0, 0]]
? E.no
%2 = 3
? E.gen
%3 = [[1, 1]]
? quit
```

We see that this curve over $\mathbb{F}_2$ has group C_3 with generator $(1, 1)$.

Exercises 9 Pari/gp

In exercises 1–5 determine the rank of the given rational elliptic curve.

** 1. $y^2 = x^3 + x + 1$.

** 2. $y^2 = x^3 - x + 1$.

** 3. $y^2 + y = x^3 + 1$.

** 4. $y^2 + y = x^3 + x$.

** 5. $y^2 + y = x^3 - x^2 - 2x$.

In exercises 6–10 determine the torsion group of the given rational elliptic curve.

** 6. $y^2 = x^3 + 1$.

** 7. $y^2 = x^3 - 1$.

** 8. $y^2 = x^3 + 4$.

** 9. $y^2 = x^3 + x + 2$.

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

In exercises 11–15 determine the group on the elliptic curve over the given finite field.

** 11. $\mathcal{E}(F_2) : y^2 + y = x^3$.

*** 12. $\mathcal{E}(F_4) : y^2 + y = x^3$.

** 13. $\mathcal{E}(F_5) : y^2 = x^3 + 2$.

** 14. $\mathcal{E}(F_7) : y^2 = x^3 + x + 1$.

** 15. $\mathcal{E}(F_{11}) : y^2 = x^3 + x^2 + 1$.