Rational points on elliptic curves over the rationals

A tutorial

B. Allombert

IMB
CNRS/Université de Bordeaux

02/06/2021

ellrank

The GP function `ellrank` attempts to compute the rank of the the Mordell-Weil group attached to a curve. This is based on Denis Simon's GP script for 2-descent. The function returns $[r, R, L]$ such that the rank is between r and R (both included) and L is a list of independent, non-torsion rational points on the curve.

```
? E = ellinit([-289,1]);
? ellrank(E)
%2 = [5,5,[[-3,29],[-7,41],[-1,17],[-15,31]
%          ,[-16,23]]]
```

Favorable case: the rank is 5 and a $\mathbb{Q}$-basis is known.

ellrank

```
? E = ellinit([-127^2,0]);
? ellrank(E)
%4 = [1,1,[]]
```

Here the rank is 1 but no point is known. We can find the point either with `ellheegner` (if the conductor is small enough) or by asking ellrank to insist by setting the `effort` parameter to a moderate value.

```
? ellheegner(E)
%5 = [-3874920201187348447014 3/3063173263398676380 1
%     6787216246729685308042328086048 65/536114241355
? ellrank(E,5)
%6 = [1,1,[[611429153205013185025/949212184820544 1,
%     151188364575969024427376980708 80/9247939007005
```

ellrank

```
? E = ellinit([0,-1,0,-260,-1530]);
? ellrank(E)
%8 = [1,3,[[27,102]]]
```

Here the rank is either 1 or 3 and one point is known. Here the conductor is small so we can check the analytic rank:

```
? A=ellanalyticrank(E)
%9 = [1,4.258599044044049230727399816153311674]
```

We find that the analytic rank is 1 so the rank is 1 and we have a $\mathbb{Q}$-basis, and $Ш_E$ is even

```
? A[2]/ellbsd(E)/ellheight(E,[27,102])
%10 = 4.000000000000000000000000000000000000
```

So we can conclude under BSD that $|Ш(E)| = 4$

Using ell2cover

The function `ell2cover` returns a basis of the set of everywhere locally soluble 2-covers of the curve. A cover is given by a pair $[Q, M]$. The 2-cover is given by the quartic $y^2 = Q(x)$ and M is a map from the quartic to the curve. Finding a point on the cover allows to find a point on the curve.

```
? E=ellinit([1,0,1,-32866776356,-2293423702808798])
? ellrank(E)
%12 = [2,2,[[55989637/144,360928708609/1728]]]
```

The rank is 2 but we have only one point. We can try to find the second point manually with `ell2cover`.

Using ell2cover

```
? C=ell2cover(E); #C
%13 = 2
? [Q,M] = C[1]; Q
%14 = -15436*x^4-102956*x^3+370501*x^2+1808116*x-47
? M
%15 = [1615672980/y^2*x^4+10776272788/y^2*x^3-38779
% 170143328/y^3*x^6-255214992/y^3*x^5+((-807836490*
```

So the cover is given by

$$y^2 = -15436x^4 - 102956x^3 + 370501x^2 + 1808116x - 4760868$$

Using ell2cover

We use `hyperellratpoints` to find a point on the cover:

```
? p=hyperellratpoints(Q,10^5,1)
%16 = [[-54021/8738,4481688/1122833]]
```

We use the map M to send it to the curve:

```
? P=substvec(M,[x,y],p[1])
%17 = [944714533055503/1296432036,28017982815190504
? ellisoncurve(E,P)
%18 = 1
? ellrank(E,,[P])
%19 = [2,2,[[55989637/144,360928708609/1728],
% [435106449118 51/9548100,28670961227514244543 1/295
```

Computing the full group

Even if the points found by `ellrank` have full rank, they might generate a subgroup (of finite index) of the Mordell-Weil group. The function `ellsaturation` attempts to obtain the full group

```
? E=ellinit([0,0,1,-7,6]);
? R=ellrank(E)
%21 = [3,3,[[-1,3],[-3,0],[11,35]]]
? S=ellsaturation(E,R[3],500)
%22 = [[1,-1],[2,-1],[0,-3]]
```

The number 500 means we only check that no prime $p < 500$ divides the index of the subgroup.

Computing the full group

```
? r1=matdet(ellheightmatrix(E,R[3]))
%23 = 3.7542920288254557283540759015628405708
? r2=matdet(ellheightmatrix(E,S))
%24 = 0.41714355875838396981711954461809339675
? r1/r2
%25 = 9.000000000000000000000000000000000000
```

We have found a group which is 3 times larger.