Rational points on elliptic curves over the rationals

A tutorial

B. Allombert

IMB
CNRS/Université de Bordeaux

11/01/2022

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 and on Tom Fisher's algorithm for the Cassels pairing. The function returns $[r, R, s, L]$ such that the rank is between r and R (both included), s is the rank of $Ш[2]/2Ш[4]$ and L is a list of independent, non-torsion rational points on the curve.

```
? E = ellinit([-289,1]);
? ellrank(E)
%2 = [5,5,0,[[-3,29],[-7,41],[-1,17],[-15,31]
%          ,[-16,23]]]
```

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

ellrank

```
? ellrank(ellinit([0,-1,0,-260,-1530]))
%3 = [1,1,2,[[27,102]]]
```

Favorable case: the rank is 1 and a $\mathbb{Q}$-basis is known. We also find that the Tate-Shafarevich group is non-trivial.

ellrank

```
? E = ellinit([-127^2,0]);
? ellrank(E)
%5 = [1,1,0,[]]
```

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)
%6 = [-3874920201187348447014 3/3063173263398676380 1
%     6787216246729685308042328086048 65/536114241355
? ellrank(E,5)
%7 = [1,1,0,[[611429153205013185025/949212184820544
%     151188364575969024427376980708 80/9247939007005
```

ellrank

```
? E = ellinit([1,0,0,-150752,-22541610]);
? [r,R,s,L]=ellrank(E,1)
%9 = [1,3,0,[[-136433699/608400,53209293359/4745520
```

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)
%10 = [1,11.564255722521984467602889781900189064]
```

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

```
? A[2]/ellbsd(E)/ellheight(E,L[1])
%11 = 16.000000000000000000000000000000000
```

technical explanation

The algorithm computes (exactly) three quantities:

- the rank C of the 2-Selmer group.
- the rank T of the 2-torsion subgroup.
- the rank s of $G[2]/2G[4]$, using the Cassels pairing.

The quantities that we are interested in are:

- the quantity $R = C - T - s$.
- the rank r of $E(\mathbb{Q})$
- the 2-rank of $Ш$ (S) (conjecturally even).

The following formula holds: $C = T + r + S$, so $R + s = r + S$. Here $R = 3$, $r = 1$, $s = 0$, so $S = 2$. Since $s = 0$, $Ш[2]/2Ш[4]$ is trivial so the 4-rank of $Ш$ is at least 2, so $|Ш| \geq 16$, and we can conclude under BSD that $Ш(E) \cong (\mathbb{Z}/4\mathbb{Z})^2$.

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)
%13 = [2,2,0,[[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
%14 = 2
? [Q,M] = C[1]; Q
%15 = -15436*x^4-102956*x^3+370501*x^2+1808116*x-47
? M
%16 = [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)
%17 = [[-54021/8738,4481688/1122833]]
```

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

```
? P=substvec(M,[x,y],p[1])
%18 = [944714533055503/1296432036,28017982815190504
? ellisoncurve(E,P)
%19 = 1
? ellrank(E,,[P])
%20 = [2,2,[[55989637/144,360928708609/1728],
% [435106449118 51/9548100,2867096122751424454 31/295
```

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)
%22 = [3,3,0,[[-1,3],[-3,0],[11,35]]]
? S=ellsaturation(E,R[4],500)
%23 = [[1,-1],[2,-1],[0,-3]]
```

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

Computing the full group

```
? r1=matdet(ellheightmatrix(E,R[4]))
%24 = 3.7542920288254557283540759015628405708
? r2=matdet(ellheightmatrix(E,S))
%25 = 0.41714355875838396981711954461809339675
? r1/r2
%26 = 9.000000000000000000000000000000000000
```

We have found a group which is 3 times larger.

Using ellrankinit

`ellrankinit` allows to initialize the number field data needed by `ellrank`. This allows to experiment with ellrank without recomputing it.

```
? E=ellinit([0,-nextprime(2^40)]);
? #
? F=ellrankinit(E);
time = 473 ms.
? ellrank(F)
time = 25 ms.
%29 = [0,2,0,[]]
? ellrank(F,4)
time = 296 ms.
%30 = [2,2,0,[[43818155260030368829460138 6/33800590
```

Using ellrankinit

F can also be used to compute ranks of twists of *E*:

```
? { for(d=1,25,
      if(isfundamental(d),
        print(d,":",ellrank([F,elltwist(E,d)]))))
  }
1:[0,2,0,[]]
5:[1,1,0,[]]
8:[0,2,0,[]]
12:[1,1,0,[]]
13:[2,2,0,[[1306169126831 27/595213609,1311121066178
17:[1,1,2,[[5448056139214 39032/379193629369,4017598
21:[0,0,2,[]]
24:[0,0,2,[]]
time = 320 ms.
```