Some code used in the talk

Mateo Crabit Nicolau

March 2026

Here are some lines of code used in the introductory talk of the 2026 Leiden Gross–Zagier formula study group to test the BSD conjecture. The code is in PARI/GP, a free software you can download here `https://pari.math.u-bordeaux.fr/download.html`.

For each of the functions used below, we warmly recommend the reader to use ?? followed by the name of the function to get some extra information on how it works and how to use it. For more details there are a lot of tutorials available here! `https://pari.math.u-bordeaux.fr/tutorials.html`

Have fun coding!

0.1 Creating an elliptic curve in PARI/GP

The command is 'ellinit'. You can either give the equation ie

$$E = \text{ellinit}([a_1, a_2, a_3, a_4, a_6]),$$

where

$$Y^2 + a_1.XY + a_3.Y = X^3 + a_2.X^2 + a_4.X + a_6$$

is the equation of your elliptic curve. Or you can use Cremona's notation

$$E = \text{ellinit}(\text{"36a1"}).$$

Example 1.

You can also construct a twist for your elliptic curve. For example, to define the elliptic curve given in [GZ86] Proposition 7.4 by the equation

$$-139Y^2 = X^3 + 10X^2 - 20X + 8$$

you first define

$$E = \text{ellinit}([0, 10, 0, -20, 8]),$$

then you twist by -139 using

$$E_{-139} = \text{elltwist}(E, -139).$$

0.2 Computing the rank

We now give the functions to compute the algebraic and analytic rank of an elliptic curve defined as before. In particular, this means that we can test the BSD conjecture on examples!

For the analytic rank, PARI/GP compute an approximation of $L^{(r)}(E,1)$, with

lfun(E,1,r)

if it is small enough it will consider it to be 0[1]. The function

ellanalyticalrank(E)

will return the first r such that this value is non-zero. You can decide yourself what small enough means and use

ellanalyticalrank(E,e)

instead, PARI/GP will consider that the L function vanishes if and only if the computed value is less than e.

Example 2. *With the same example as before, ellanalyticalrank(E) returns*

$$[0, 0.72568106193615278233620554102639654874]$$

this means that

$$L(E,1) = 0.72568106193615278233620554102639654874 \neq 0.$$

According to PARI/GP, the analytic rank of E is 0. For E_{-139} it returns

$$[3, 110.57662417722233412350474177616982773],$$

the rank of E_{-139} is 3, as stated by [GZ86] Proposition 7.4. Furthermore

$$L^{(3)}(E,1) = 110.57662417722233412350474177616982773 \neq 0.$$

We can also try to compute the algebraic rank using

ellrank(E)

PARI/GP will also try to give generators of $E(\mathbb{Q})$.

Example 3. ellrank(E_{-139}) *will give*

$$[3, 3, 0, [[-162, 620], [2502, 77284], [5838, 386420]]]$$

the first 2 elements of the list tell you that the rank r should satisfy

$$3 \leq r \leq 3.$$

The 3 brackets give coordinates of 3 linearly independent points.

[1] In particular, this is not a proof of the vanishing of the L-function. We can only test that it is close to zero for a given precision (you can use \p to change it.)

When the curve is of rank 1 we can use

$$\text{ellheegner(E)}$$

to obtain a non-torsion rational point on E using Heegner points. The fact that they are non-torsion is a direct consequence of the Gross-Zagier formula!

Example 4. *Let*

$$E_2 = \text{ellinit}([-157^2, 0]),$$

be the elliptic curve defined by

$$y^2 = x^3 - 157^2 x$$

ellrank(E_2) returns

$$[1, 1, 0, []]$$

meaning that the curve is of rank 1 but it did not manage to find a non-torsion point (you can ask it to try harder using ellrank(E_2,10)). However, ellheegner(E_2) returns

$$[69648970982596494254458225/16613623166818526754080 4,$$
$$5389624350896046150780043072587852 18335/6771681655607745599922849543574240 8]$$

the coordinate of a rational non torsion point of E_2.

References

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84:225–320, 1986. ↑1, 2.