

Elliptic curves: final exercise

Due: 17 December 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise. Pick your favorite integer $N > 1$, and explain why this is your favorite integer. Now construct a prime p and an elliptic curve E/\mathbf{F}_p such that $\#E(\mathbf{F}_p) = N$. Your code should end with a verification that the curve has the right number of points by using a standard Sage function which counts the number of points of your elliptic curve.

Grading. The grade is based on the size of N (bigger is better) and on the sophistication of your algorithm (write down comments and explain your tricks).

How to hand in. Share your Sage worksheet with ajavan, martindalecr, wzhuang.new and hand in a printed version.

Remark. You are allowed to use any function in Sage as long as it doesn't trivially solve the problem.