Elliptic Curves with Sage
Prof. Shahed Sharif

Arithmetic on elliptic curves is typically very tedious to work out, so we will instead use Sage’s built-in elliptic curve arithmetic capabilities. You can use any of the syntax in this handout on your homework.

We generally work over finite fields. Sage refers to $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{Zmod}(p)$. Note that if we put in a composite number in place of $p$, we will not get a field. For convenience, I like to assign the above field to a variable:

$$K = \mathbb{Zmod}(23)$$

Next, we define the elliptic curve $y^2 = x^3 + Ax + B$ over the field $K$. As above, I like to assign a variable name to the elliptic curve; say, let $E$ be the curve with equation $y^2 = x^3 + x + 11$:

$$E = \text{EllipticCurve}(K, [1,11])$$

To add points on the elliptic curve, I’d like to use the natural syntax: for instance, $(1, 6) + (5, 7)$. (You can check that both points are on the elliptic curve.) But Sage doesn’t know that the coordinates are in $\mathbb{Z}/23\mathbb{Z}$, nor does it know that $+$ means addition on the elliptic curve as opposed to, for example, vector addition. So we have to specify that these are two points on the elliptic curve. The simplest way to do this is by writing $E(x, y)$ for the point $(x, y)$ on the curve; so our sum would look like

$$E(1, 6) + E(5, 7)$$

You’ll notice that the sum looks weird: you should get $(7 : 4 : 1)$. These are projective coordinates for the sum, which we won’t cover in this course. For the most points, just ignore the 3rd coordinate. In Sage, you can do this with

$$(E(1, 6) + E(5, 7))[:2]$$

The one exception is $(0 : 1 : 0)$; this refers to the point at infinity, so don’t use the method above!

For more complicated arithmetic, I like to assign points to variables first, to make later typing easier:

$$P, Q = E(1, 6), E(5, 7)$$

$$2*P - 3*Q$$