WORKSHEET #9 – MATH 5405
SPRING 2016

DUE THURSDAY, MARCH 24TH

Let's get a little practice with the group law on an elliptic curve.

Consider the elliptic curve defined by the equation

$$y^2 = x^3 + 1$$

1. Draw this elliptic curve to the best of your ability (presumably this is greater than my ability to draw elliptic curves as you have observed today).

2. Verify that the points. $P = (-1, 0), Q = (0, 1), -Q = (0, -1), R = (2, 3), -R = (2, -3)$ are all on the curve (and of course the point at infinity O is there too).

3. Make an addition (like a multiplication table) for the 6 points $P, Q, -Q, R, -R, O$. This is a 6×6 table and hence verify that these 6 points form a subgroup of points on the elliptic curve.

4. Show that if you relable this table in an appropriate way, you get the integers mod 6. In other words, show that these 6 points form a group *isomorphic* to $\mathbb{Z}/6$.