Math/CS 103 Professor: Padraic Bartlett

Homework 18: Elliptic Curves over Finite Fields

Due Friday, week 10 *UCSB 2014*

Homework Problems.

Pick **two** of the following **four** problems to solve!

1. Consider the following three elliptic curves:

   - $y^2 = x^3 - x + 1$,
   - $y^2 = x^3 - 4x + 2$,
   - $y^2 = x^3 + 2x$.

   For each curve, draw the collection of all of its points over $(\mathbb{Z}/5\mathbb{Z})^2$.

2. Pick a curve from the above set of three curves. Create a group table corresponding to that curve's points (i.e. create a table that tells someone how to add any two points on the curve.)

3. In a group $\langle G, + \rangle$, an element g is said to **generate** that group if we can write any element in the group as just a repeated sum of g's. For example, $\langle \mathbb{Z}/4\mathbb{Z}, + \rangle$ is generated by the element 1, because we can write $1 + 1 = 2, 1 + 1 + 1 = 3, 1 + 1 + 1 + 1 = 4 \cong 0$ mod 4.

   (a) Find an elliptic curve that is generated by one element.

   (b) Find an elliptic curve that is not generated by any one element.

4. What is the maximum number of points an elliptic curve over $\mathbb{Z}/5\mathbb{Z}$ can contain? What is the minimum?