CCS Discrete Math I | Professor: Padraic Bartlett

Homework 17: Elliptic Curves over Finite Fields

Due Friday, Week 10 | *UCSB 2014*

Solve **three** of the following **six** problems. As always, prove your claims/have fun!

1. Consider the following three elliptic curves over $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.

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

   For each curve, draw the collection of all of its points. (Use separate plots for each curve, as it will be hard to distinguish two of the same curve.)

2. Choose any elliptic curve E in $\mathbb{F}_7[x] = (\mathbb{Z}/7\mathbb{Z})[x]$, and throw in the point at infinity $\mathcal{O}$. Find the group corresponding to this curve!

3. Recall, from earlier in the quarter, the following definition: 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?

5. (a) Create a finite field of order 9 using the methods described in class. (That is: find an irreducible polynomial $p(t)$ of degree 2 in $\mathbb{F}_3[t] = (\mathbb{Z}/3\mathbb{Z})[t]$, and then look at $\mathbb{F}_3[t]/p(t)$.) Call this field $\mathbb{F}_9$.

   (b) Consider the elliptic curve E given by all of the points $(x, y) \in \mathbb{F}_9$ that satisfy the equation $y^2 = x^3 + 2x + 2$. Find all of the points in E.

   (c) Add in a point at infinity $\mathcal{O}$ to E, and form the group table given by adding points in $E \cup \{\mathcal{O}\}$ together.

6. In class, we claimed that our elliptic curve operations were well-defined over the finite fields. Prove this! Namely, show that if E is an elliptic curve, then

   - If P, Q are two distinct points on E and the line L through P, Q is not tangent to E at either P, Q, then either L is a vertical line or there is a unique third point of intersection $R \neq P, Q$ between our line and our curve.
   - If P is any point on the curve E and L is the tangent to E through P, then either L is vertical, L goes through E at exactly one other point R, or P is a "triple-tangent:" that is, if we write $L : y = mx + c, E : x^3 - ax + b, P = (r, s)$, we have that $x^3 - ax + b - (mx + c)^2 = (x - r)^3$.