CCS Discrete Math I | Professor: Padraic Bartlett

Homework 16: Elliptic Curves

Due Friday, Week 9 | *UCSB 2014*

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

1. In class, we proved that if E is an elliptic curve and P, Q are two distinct points on E such that the line L through P, Q was not vertical, then L intersects E at some third point R. This problem considers what happens if $P = Q$; that is, if we pick a point P and choose L to be the tangent line to E at P!

   Proposition. Suppose that P is a point with nonzero y-coördinate on an elliptic curve E given by $y^2 = x^3 - ax + b$. Take the tangent line L to E at P. There are two possibilities:

   - L intersects E at exactly one other point on the curve. If we graph L by $y = mx + b$, which we can do because at points with nonzero y-coördinate we have shown that the slopes of tangent lines exist and are finite, we have that $p(x) = (x^3 - ax + b) - (mx + b)^2$ can be factored into something of the form $(x - r_1)^2(x - r_2)$, where r_1 is the $x-$coördinate of P, and r_2 is the x-coördinate of the unique other point on the curve we cross.
   - L never intersects E at any other points on our curve. If we graph L by $y = mx + b$, we have that $p(x) = (x^3 - ax + b) - (mx + b)^2$ can be factored into something of the form $(x - r_1)^3$, where r_1 is the $x-$coördinate of P.

   Prove this proposition!

2. In class, Connor asked if the names "elliptical curve" and "ellipse" are related terms. I said that they were in a sense, but didn't know the full reason off the top of my head.

   As it turns out, there's actually a beautiful story here! To do this problem, go to

   http://www.maa.org/sites/default/files/pdf/upload_library/2/Rice-2013.pdf

   and read the attached paper, which explains how these terms are related. Give me a two-three paragraph summary of this paper to solve this problem!

3. Take the elliptic curve E defined by $y^2 = x^3 + 1$ for this problem.

   (a) Show that the only points on this curve that have integer coördinates are $(-1, 0), (0, \pm 1), (2, \pm 3)$.

   (b) Take these five points, along with the sixth point O that is the "point at infinity" as defined in the notes/in class on Wednesday. Show that these six points, under the point-addition operation defined in class, form a subgroup of the elliptic curve group. Give me a group table for these six points.