Math/CS 103 Professor: Padraic Bartlett

Homework 17: Elliptic Curves

Due Friday, week 10 *UCSB 2014*

Homework Problems.

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

1. Suppose that P, Q are two distinct points on an elliptic curve $y^2 = x^3 + ax + b$. Let L be the straight line segment drawn through P, Q. Prove that L intersects our elliptic curve in at most one other place.

2. Take any point $P = (x, y)$ on an elliptic curve $y^2 = x^3 + ax + b$. Prove that the point $-P = (x, -y)$ is also on our elliptic curve. Furthermore, prove that the line through P and $-P$ does not intersect our curve at any other points.

3. Suppose that P is a point on an elliptic curve $y^2 = x^3 + ax + b$. Let L be the line through P that is tangent to our elliptic curve at P. Prove that L intersects our elliptic curve in at most one other location.

4. Explain why problems 1-3 mean that the group operation we defined in class on elliptic curves is well-defined. In other words, explain why if P, Q are any two points in our elliptic curve group and we look at $P + Q$, the result exists and is some other point in our group.

5. What is the identity 0 in an elliptic curve group? Prove that this element 0 is in fact the identity (i.e. show that for any other point P in our group, $0 + P = P$.)

6. Show that any elliptic curve group has inverses: i.e. that for any P in such a group, there is some other point $-P$ such that $P + -P = 0$.

7. Show that our elliptic curve group is associative: i.e. show that for any three points P, Q, R, we have $(P + Q) + R = P + (Q + R)$.

   A useful diagram to consider may be the following: take any elliptic curve, and draw the following nine lines. Why does this diagram imply associativity?