Exercise Set 8:

Elliptic Curves, part 1

Math 414, Winter 2010, University of Washington

Due Wednesday, March 3, 2010

1. Write down an equation $y^2 = x^3 + ax + b$ over a field K such that $-16(4a^3+27b^2) = 0$. Precisely what goes wrong when trying to endow the set $E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with a group structure?

2. One rational solution to the equation $y^2 = x^3 - 11$ is $(3, 4)$. Find a rational solution with $x \neq 3$ by drawing the tangent line to $(3, 4)$ and computing the second point of intersection.

3. Let E be the elliptic curve over the finite field $K = \mathbb{Z}/7\mathbb{Z}$ defined by the equation
$$y^2 = x^3 + x.$$
   (a) List all 8 elements of $E(K)$.
   (b) Is the finite abelian group $E(K)$ cyclic or not?