CS 655 Fall, 2017, Homework 2

Due: Thursday, October 12, 2017

1. Use Shanks' baby-step-giant-step method to solve the discrete logarithm problem $2^x \equiv 82 \pmod{107}$. Show all your work, including two tables of 11 pairs of numbers. (Answer $x = 41$.)

2. Consider the curve $y^2 = x^3 - 7x + 15$. Let $P = (1, 3)$, $Q = (2, 3)$, $R = (1, -3)$. Compute $2P$, $P + Q$, $P + R$ and $Q + R$. Be sure to check that the given point and your answers all lie on the curve.

3. Consider the curve $y^2 \equiv x^3 + 4x + 4 \pmod{11}$. Let $P = (1, 8)$. Compute $2P$, $3P$ and $4P$. What is the smallest positive integer k with $kP = \infty$? Find the number of points on the elliptic curve. Be sure to check that the given point and your answers all lie on the curve.

4. Show that the elliptic curve $y^2 = x^3 - x$ over the integers modulo p has exactly $p+1$ points when the prime p is $\equiv 3$ mod 4. (Hint: When $p \equiv 3$ mod 4, -1 is a quadratic non-residue, so for all $0 < a < p$ exactly one of a, $p - a$ is a quadratic residue. Treat $x = 0$ and the point at infinity separately.)