Math/Cmsc 456, Jeffrey Adams
Test II, May 12, 2008
For full credit you must show your work.
Calculators allowed but not required

1. [20 points] Recall that if I have a random function from a set with m elements to a set with n elements, the probability that it is injective (one-to-one) is approximately $e^{-m^2/2n}$.

   (a) I have a list of 10^{10} random numbers, each between 1 and 10^{30}. What is the approximate probability that two of the numbers are the same?

   (b) I want to choose m so that if I have a list of m random numbers, each between 1 and 10^{30}, then the probability that two of them are the same is very high, close to 100%. What is a reasonable value for m? (The question is not precise, so only a rough answer is needed.)

   (c) I want to choose m so that if I have a list of m random numbers, each between 1 and 10^{30}, then two of them are *guaranteed* to be the same. What is the minimal value for m?

2. [20 points]

   (a) Suppose $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ where a_0, a_1, a_2 and a_3 are unknown. Suppose the points $(1, -3), (2, 5), (3, 10)$ and $(4, 12)$ are on the curve. Write down a matrix equation for the coefficients $a_0, \dots, a_3$. It is *not* necessary to solve for the coefficients.

   (b) Consider polynomials $f(x) = a_0 + a_1x + \dots$ defined $\pmod{13}$. Find a polynomial $f(x)$ of degree 3 such that $f(1) = f(2) = f(3) = 0$ and $f(4) = 1$. What is $f(5)$?

3. [20 points] Suppose E is an elliptic curve defined $\pmod{401}$. (Note: 401 is prime.)

   (a) What are all the possibilites for the number of points N of E?

   (b) Suppose you find a point P on E of order 7. How many possibilities are there for N?

   (c) Suppose in addition to the point P of order 7, you find another point Q of order p for some prime $p \neq 7$. What is the *smallest* value of p which will determine N exactly? If there is such a point, what is N?

4. [20 points] Naive Nelson tries to make a zero knowledge scheme as follows. He picks primes p, q, both equivalent to 3 (mod 4), and sends $n = pq$ to Victor. He wants to prove to Victor that he knows the factorization of n. He has Victor pick a random x, compute $y = x^2 \pmod{n}$, and send him y. He computes a square root z of y, and sends it to Victor. Victor confirms that $z^2 = y$, and concludes that Victor must know the factorization of n.

   (a) Briefly, how does Nelson compute z? In particular it should be clear how he uses p, q and not just n.

   (b) Suppose Eve is eavesdropping and intercepts n, y and z. Can she factor n?

   (c) Show that Victor has a 50% chance of factoring n (so this is not a valid zero knowledge protocol).

5. [20 points] Consider the elliptic curve E: $y^2 = x^3 + 2x + 4 \pmod{31}$.

   (a) Compute $(9, 10) + (9, -10)$ on E.

   (b) Compute $\infty + (9, 10)$ on E.

   (c) Compute $(2, 4) + (7, 12)$ on E.

   (d) Find all points of the form $(8, y)$ on E.

   You may use the addition formulas on the curve $y^2 = x^3 + ax + b$: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$

   where

$$m = \begin{cases} (3x_1^2 + a)/(2y_1) & x_1 = x_2, y_1 = y_2 \\ (y_2 - y_1)/(x_2 - x_1) & else \end{cases}$$

   There are additional special cases when P and/or $Q = \infty$, and when $m = \infty$.