Math/Cmsc 456, Jeffrey Adams
Test II, May 12, 2008 SOLUTIONS

1. (a) Here $m = 10^{10}$ and $n = 10^{30}$. The probability of being injective is $e^{-m^2/2n} = e^{-10^{20}/2\times 10^{30}} = e^{-\frac{1}{2\cdot 10^{10}}} = 1/e^{\frac{1}{2\cdot 10^{10}}}$ is very close to $1/e^0 = 1$. So the probability that two numbers are the same, i.e. it is not injective is 1 minus this, which is very close to 0.

   (b) We have to take $m^2 \simeq n$, i.e. $m \simeq \sqrt{n} = \sqrt{10^{30}} = 10^{15}$. To be safe take n a bit bigger, say 10^{16}.

   (c) We need to take $m = 10^{30}+1$. The first 10^{30} could all be different, but the next one would have to be a duplicate.

2. (a)
$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \\ 1 & 4 & 16 & 64 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} -3 \\ 5 \\ 10 \\ 12 \end{pmatrix}$$

   (b) This is a Lagrange interpolation polynomial. Take $f_0(x) = (x-1)(x-2)(x-3)$, so $f(1) = f(2) = f(3) = 0$, and this has degree 3. Then $f_0(4) = 6$, so divide by this to give
$$f(x) = \frac{1}{6}(x-1)(x-2)(x-3).$$
   Since $2 \times 6 = -1$, $\frac{1}{6} = -2$, so this becomes
$$f(x) = -2(x-1)(x-2)(x-3).$$
   It is easy to compute $f(5) = -2(4 \times 3 \times 2) = -48 = 4 \pmod{13}$. Note it is *much* easier to do this than to use matrix computations.

3. (a) By Hasse's theorem $|N - (p+1)| \leq 2\sqrt{p}$. Since $\sqrt{401}$ is slightly bigger than 20, this gives $|N - (402)| \leq 40$, so $362 \leq N \leq 442$.

(b) The order of E is a multiple of 7. The number of possibilities for N was $442 - 362 + 1 = 81$, and $81/7 > 11$, so the answer is approximately 11. In fact the multiples of 7 in the range are $357, 364, \ldots, 420$, of which there are 10. The

(c) If there are points P of order 7 and Q of order p, then $P + Q$ has order $7p$. Therefore $7p$ divides N, so if $7p > 81$, there is only one multiple of $7p$ between 362 and 442. Taking $p = 5$ clearly doesn't work, but taking $p = 11$, we find only one multiple 385, of 77 between 362 and 442.

4. (a) He computes the square roots of y mod p and q, and combines them using the Chinese Remainder Theorem. That is he sets $z_1 = \pm y^{\frac{p+1}{4}} \pmod{p}$ and $z_2 = \pm y^{\frac{q+1}{4}} \pmod{q}$. Then $z_1^2 = y \pmod{p}$ and $z_2^2 = y \pmod{q}$. He then solves $z = z_1 \pmod{p}$ and $z = z_2 \pmod{q}$ by the CRT.

(b) No, she only knows a number and one square root of it, which is not enough information.

(c) Nelson knows a square root x of y. If $z \neq \pm x$ then $\mathrm{GCD}(z - x, y)$ is a non-trivial factor of n. There is a 50% of this, since there are four square roots $\pm x, \pm x'$ of y.

5. (a) This is $P + (-P) = \infty$.

(b) Since ∞ is like 0, this is $(9, 10)$.

(c) First of all $m = (12 - 4)/(7 - 2) = 8/5 \pmod{31}$. We need $5^{-1} \pmod{35}$. Clearly $5 \times 6 = -1 \pmod{31}$, so $5^{-1} = -6 = 25 \pmod{31}$. So $m = 8 \times 25 = 200 = 14 \pmod{31}$, and $x_3 = 14^2 - 2 - 7 = 1 \pmod{31}$. Then $y_3 = 14(2-1) - 4 = 10 \pmod{31}$. So the solution is $(1, 10)$.

(d) Solve $y^2 = 8^3 + 16 + 4 = 5 \pmod{31}$. This is easy: $31 + 5 = 36$, so $y = 6$ is a solution. So there are exactly two solutions $y = \pm 6$.