MAT 301 Problem Set 3

[Posted: February 08, 2012. Due: February 17, 2012. Worth: 100 points]

Note: I value *succinct* and *clearly written* solutions *without unnecessary verbiage*. Such solutions will be rewarded with bonus points.

Note the Friday deadline. The problem sets are due in the beginning of the tutorial, at 10am on Friday.

1. **Exponentiation and Finding Roots (30 points)**
   - (5 points) Find $2^{65} \pmod{97}$. Show your work.
   - (15 points) Find the 65^{th} root of 2 mod 97. Show your work.

2. **Square Roots and Factoring (40 points)**
   - (1 point) How many solutions does the equation $x^2 = 1 \pmod 7$ have? What are they?
   - (1 point) How many solutions does the equation $x^2 = 3 \pmod 7$ have? What are they?
   - (2 points) How many solutions does the equation $x^2 = 1 \pmod 8$ have? What are they?
   - (11 points) If N is prime and $a \in \mathbb{Z}_N^*$, how many solutions does the equation $x^2 = a \pmod N$ have?
   - (30 points) I am going to hand over to you a number N which is a product of two distinct prime numbers. I will also give you two numbers x_1 and x_2 such that

$$\begin{aligned} x_1^2 &= x_2^2 \pmod N \\ x_1 &\neq x_2 \pmod N \\ x_1 &\neq -x_2 \pmod N \end{aligned}$$

     How will you find the prime factors of N using this information?

3. $\phi(N)$ **and Factoring (30 points)** I am going to hand over to you a number N which is a product of two distinct prime numbers. I will also give you $\phi(N)$, the Euler Totient function of N.
   - How will you find the prime factors of N using this information?
   - How many basic computational steps does your algorithm take (you can express your answer in terms of the Big-Oh $O(\cdot)$ notation)?

   (Note: Since you can easily compute $\phi(N)$ given the factorization of N, this problem is asking you to prove that finding $\phi(N)$ is computationally as hard as factoring N).