18.781 Problem Set 5 - Fall 2008

Due Tuesday, Oct. 14 at 1:00

1. Create your own public-key cryptosystem by picking two primes p_1, p_2 (they don't need to be large!), setting $n = p_1 p_2$, and picking an exponent $(d, \phi(n)) = 1$. Illustrate the encryption and decryption procedure by picking a message $m < n$.

2. (Niven 2.5.3) If you are able to factor $n = p_1 p_2$, then it is easy to calculate $\phi(n) = (p_1 - 1)(p_2 - 1)$. Show that this also works in reverse: If you are given $n = p_1 p_2$ and the value of $\phi = (p_1 - 1)(p_2 - 1)$, solve for p_1 and p_2.

3. (Niven 2.5.5) If m is not squarefree, show that there exist a_1, a_2 such that $a_1 \not\equiv a_2 \pmod{m}$, but $a_1^k \equiv a_2^k \pmod{m}$ for $k \geq 2$.

4. (Niven 2.8.2) Find a primitive root of 23.

5. (Niven 2.8.3) How many primitive roots does 13 have?

6. (Niven 2.8.9 & 2.8.15)

   (a) Show that $3^8 \equiv -1 \pmod{17}$. Explain why this implies that 3 is a primitive root modulo 17.

   (b) Prove that if a has order h modulo p, and h is even, then $a^{\frac{h}{2}} \equiv -1 \pmod{p}$.

(Bonus) Prove that if p is prime, then

$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid k, \\ -1 \pmod{p} & \text{if } (p-1) \mid k. \end{cases}$$