Homework 7, 550.371/650.471 Cryptology and Coding, Spring 2017

You may discuss generalities of mathematics and MATLAB with others in the class, but the solutions and code that you submit should be entirely your own.

Problem 1: Write a MATLAB program to perform exponent factorization; in particular, the input should be positive integers a, k, and n such that $a^k = 1 \bmod n$, and the output (if all goes well) should be nontrivial factors d_1 and d_2 such that $n = d_1 \cdot d_2$. Use your algorithm to factor $n = 68309797$ using $k = 341466300$ with base $a = 2$ and again with base $a = 5$.

Problem 2: Prove that if m and n are relatively prime positive integers then $\phi(mn) = \phi(m) \cdot \phi(n)$.
(Hint: Use induction on mn. Also note the correspondence between divisors of mn and pairs (d, d') such that d is a divisor of m and d' is a divisor of n; specifically, $d \cdot d'$ is a divisor of mn.)

Problem 3: Using the previous problem (and a problem from a previous homework), find a formula for $\phi(n)$ and a formula for $\frac{\phi(n)}{n}$ in terms of positive integer n's prime factorization. Simplify the latter formula as much as possible. What does $\frac{\phi(n)}{n}$ have to do with the fraction of members of Z_n that are in Z_n^*?

Problem 4: (Problem 16 on page 194 in Trappe and Washington text) Suppose two users Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e_A and e_B are relatively prime. Charles wants to send the message m to Alice and Bob, so he encrypts to get $c_A = m^{e_A} \bmod n$ and $c_B = m^{e_B} \bmod n$. Show how Eve can find m if she intercepts c_A and c_B.

Problem 5: Suppose $n = p_1 p_2 p_3 \cdots p_m$ for distinct prime numbers p_1, p_2, $\ldots p_m$. Prove that if $p_i - 1 | n - 1$ for all $i = 1, 2, \ldots, m$ then n is a Carmichael number.