MATH 3320, HOMEWORK #4

DUE FRIDAY, SEPTEMBER 21

To ensure that you get full credit, be sure to *show your work* in the problems that require calculations. Very little credit is given for answers without justification. Please write in complete sentences to help us understand what you are doing.

You may collaborate with classmates in solving the problems, including the extra credit problems. If you do so, please list their names on your assignment. However, you should not consult *any* other people (except the instructors or TAs), or use online resources. (Seriously, it's very obvious to us when this occurs, and there are drastic consequences, so don't do it!) If you use results that were not proved in class, please provide your own proof.

1. (10 points) Let p be a prime number. Suppose that a and n are positive numbers such that $\gcd(a, p) = 1$ and $\gcd(n, p - 1) = 1$. Determine the number of solutions of the congruence $x^n \equiv a \pmod{p}$.

2. (20 points) Let m be a positive integer with a prime factorization

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

Determine the number of solutions of $x^2 \equiv 1 \pmod{m}$.

3. (15 points) Let a and m be relatively prime positive integers. Prove that a is a primitive root modulo m if and only if $a^{\phi(m)/p} \not\equiv 1 \pmod{m}$ for all prime factors p of $\phi(m)$.

4.

(a) (5 points) Prove that 3 is a primitive root modulo 17.
(b) (10 points) Solve the congruence $8x^5 \equiv 5 \pmod{17}$.
(c) (10 points) Find all integers x such that $7^x \equiv 4 \pmod{17}$.

5. **(Extra Credit)** A positive number m is called a *pseudoprime* (a.k.a. *Carmichael number*, see p. 169 of Davenport) if it satisfies the following two conditions:

(i) m is a composite number;
(ii) $a^{m-1} \equiv 1 \pmod{m}$ for all integers a which are relatively prime to m.

For (15 points), show that m is a Carmichael number if and only if m is a product of at least two distinct primes $p_1, p_2, \ldots, p_r$ such that $p_i - 1$ divides $m - 1$ for $i = 1, 2, \ldots, r$.

In the Section 1 lecture, we called n a pseudoprime, if it is a composite number such that only $2^n \equiv 2$ $(modn)$. Use the definition given in Problem 5 for the extra credit, not the one given in class.