Math 412 Homework 7

your name

Due date: Oct 23, 2015

Solve the following problems. Please remember to use complete sentences and good grammar.

1. (4 points) Determine the order of 9 modulo 25.
2. (4 points) Let a be an odd integer and integer $l \geq 3$. Show that the order of a modulo 2^l is a divisor of 2^{l-2}. (In other words, $a^{2^{l-2}} \equiv 1 \mod 2^l$.)
3. (4 points) Let p be a prime divisor of the Fermat number $F_n = 2^{2^n} + 1$.
(a) show that $ord_p 2 = 2^{n+1}$.
(b) From part (a), conclude that $2^{n+1}|(p-1)$, so that p must be of form $2^{n+1}k + 1$.
4. (4 points) Show that if n is a positive integer and a and b are integers relatively prime to n such that $(ord_n a, ord_n b) = 1$, then $ord_n(ab) = ord_n a \cdot ord_n b$.
5. (6 points) Let p be a prime and the prime decomposition of $\phi(p) = p-1$ be $p-1 = q_1^{t_1} q_2^{t_2} \dots q_r^{t_r}$, where $q_1, q_2, \dots, q_r$ are primes.
(a) Show that there are integers $a_1, a_2, \dots, a_r$ such that $ord_p a_i = q_i^{t_i}$, for $i = 1, 2, \dots, r$.
(b) Show that $a = a_1 a_2 \dots a_r$ is a primitive root modulo p.
(c) Follow the procedure outlined in part (a) and (b) to find a primitive root modulo 29.
6. (4 points) Let n be a positive integer possessing a primitive root. Using this primitive root, prove that the product of all positive integers less than n and relatively prime to n is congruent to -1 modulo n.
7. (bonus, 4 points) Find the remainder r, $1 \leq r \leq 13$, when 2^{1985} is divided by 13.