Math 115B Homework 5

1) Find the order of

a) 2 modulo 11

b) 3 modulo 13

c) 8 modulo 15

d) 9 modulo 17

2) Let $a, m \in \mathbb{Z}$ with $m > 0$. If a' is the inverse of a modulo m, prove that $\text{ord}_m(a) = \text{ord}_m(a')$. Deduce that if r is a primitive root modulo m, then r' is a primitive root modulo m.

3) Let m be a positive integer and let $a \in \mathbb{Z}$ with $(a, m) = 1$.

a) Prove that if $\text{ord}_m(a) = xy$ (with x and y positive integers), then $\text{ord}_m(a^x) = y$.

b) Prove that if $\text{ord}_m(a) = m - 1$, then m is a prime number.

4) Let a and n be positive integers with $a > 1$. Prove that $n | \phi(a^n - 1)$. *Hint: consider* $\mathit{ord}_{(a^n-1)}(a)$.

5) Let p be an odd prime number and let r be an integer with $p \nmid r$. Prove that r is a primitive root modulo p if and only if $r^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$.

6) Determine the number of incongruent primitive roots modulo each number below.

a) 60

b) 61

c) 62

d) 63

7) Let p be an odd prime.

a) Prove that any primitive root r mod p is a quadratic nonresidue mod p.

b) Prove that there are exactly $\frac{p-1}{2} - \phi(p - 1)$ incongruent quadratic nonresidues mod p that are not primitive roots mod p.

8) Let m be a positive integer. If a primitive root modulo m exists, prove that the product of all positive integers not exceeding m and relatively prime to m is congruent to -1 mod m.

9) How difficult was this homework? How long did it take?