116 - Number Theory
Spring 2007

Homework 9

Name: _____
Instructor: Travis Kelm

Section 9.2 - Primitive Roots for Primes

1. **Order Two:**
   (a) Show that for any positive integer $m > 2$ we have that $\text{ord}_m(m-1)=2$
   (b) Show that if p is an odd prime, then $p-1$ is the only residue that has order 2 modulo p.
   (c) Show by example that if m is not prime, then there may be two distinct residues both having order two modulo m.

2. Find the number of primitive roots of each of the following primes:
   (a) 109
   (b) 499

3. **Orders of Products:**
   (a) Show that $\text{ord}_m(ab) = \text{lcm}\,[\text{ord}_m(a) \cdot \text{ord}_m(b)]$
   (b) Use the previous part to find a primitive root of 29 by finding a residue of order 7 and a residue of order 4.

4. Let p be a prime greater than 3. What do you get (mod p) when you multiply all of the primitive roots of p together? Be sure to prove your claim.

Section 9.3 - Existence of Primitive Roots

5. **Exercise 2:** Which of the integers 8, 9, 12, 26, 27, and 33 have a primitive root?

6. **Exercise 4:** Find a primitive root of each of the following:
   (a) 121
   (b) 169
   (c) 17^2
   (d) 19^2

7. **Exercise 12:** Let p be an odd prime. Show that the numbers p^t and $2p^t$ have the same number of primitive roots.

8. **Exercise 16:** Find the smallest odd prime p such that p has a primitive root r where r is *not* a primitive root of p^2.

Section 9.4 - Index Arithmetic

9. **Exercise 1:** Write out a table of indices modulo 23 with respect to the primitive root 5.

10. **Exercise 2:** Find all of the solutions of the following:
    (a) $3x^5 \equiv 1 \pmod{23}$
    (b) $3x^{14} \equiv 2 \pmod{23}$

11. **Exercise 3:** Find all of the solutions of the following:
    (a) $3^x \equiv 2 \pmod{23}$
    (b) $13^x \equiv 5 \pmod{23}$

Section 9.5 - Primality Tests Using Orders

12. **Exercise 2:** Show that 211 is prime by using Lucas's converse of Fermat's Little Theorem with $x = 2$.

13. **Exercise 4:** Show that 257 is prime by using Corollary 9.18.1 with $x = 3$.

14. **Exercise 10:** Use Proth's Primality Test to show that 449 is prime.