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 $\text{ord}_m(m-1)=2$

*Solution*: If $m > 2$, then $m - 1 > 1$, thus $\text{ord}_m(m-1) > 1$. The result then follows from an easy computation:

$$(m-1)^2 = m^2 - 2m + 1 \equiv 1 \pmod{m}$$

□

(b) Show that if $p$ is an odd prime, then $p-1$ is the only residue that has order 2 modulo $p$.

*Solution*: If $p$ is an odd prime, then obviously $p-1$ is even. Thus $2|p-1$. Using theorem 9.8, there are $\phi(2) = 1$ residues having order two. By the previous problem $\text{ord}_p(p-1) = 2$ and thus $p-1$ is the only residue having order two. □

(c) Show by example that if $m$ is not prime, then there may be two distinct residues both having order two modulo $m$.

*Solution*: Let $m = 12$. As we said in class the residues $5, 7, 11$ all have order 2. □

**2.** Find the number of primitive roots of each of the following primes:

(a) 109

*Solution*: A primitive root modulo 109 is a residue having order 108. Note that $498 = 2^2 \cdot 3^3$ and thus $\phi(108) = (2^2 - 2^1)(3^3 - 3^2) = 32$. Thus there are 32 primitive roots modulo 109. □

(b) 499

*Solution*: A primitive root modulo 499 is a residue having order 498. Note that $498 = 2 \cdot 3 \cdot 83$ and thus $\phi(498) = 1 \cdot 2 \cdot 82 = 164$. Thus there are 164 primitive roots modulo 499. □

**3. Orders of Products:**

(a) Show that $\text{ord}_m(ab) \leq \text{lcm}\,[\text{ord}_m(a) \cdot \text{ord}_m(b)]$

*Solution*: Let $t = \text{lcm}\,[\text{ord}_m(a) \cdot \text{ord}_m(b)]$. Since $t$ is a multiple of $\text{ord}_m(a)$ we know that $a^t \equiv 1$. Likewise, since $t$ is a multiple of $\text{ord}_m(b)$ we know that $b^t \equiv 1$. Thus $(ab)^t = a^t b^t \equiv 1$. Since $ab$ raised to the $t$ power if congruent to 1 we know from Theorem 9.1 that $\text{ord}_m(ab)|t$. □

**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.

*Solution*: The product of all primitive roots of $p$ must be congruent to 1 mod $p$. To see this note that as proved earlier, if $r$ is a primitive root of $p$ then the modular inverse $\hat{r}$ of $r$ is also a primitive root. As long as $p > 3$ there will be an even number of primitive roots and these roots will occur in inverse pairs $\{r, \hat{r}\}$. Thus in the product of all the primitive roots, each of the products of the inverse pairs will yield 1 mod $p$. Hence the entire product will be congruent to 1 mod $p$. □

## 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?

*Solution*: 9 (2 is primitive root), 26 (7 is primitive root), and 27 (2 is primitive root). □

**6. Exercise 4:** Find a primitive root of each of the following:

(a) 121

*Solution*: 2 □

(b) 169

*Solution*: 2 □

(c) $17^2$

*Solution*: 3 □

(d) $19^2$

*Solution*: 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.

*Solution*: Since $p$ is odd, so too is $p^t$ odd, thus as was shown on a previous homework, $\phi(p^t) = \phi(2p^t)$. It follows that $\phi(\phi(p^t)) = \phi(\phi(2p^t))$ and hence $p^t$ 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 $p^2$.

*Solution*: It is 29. 14 is a primitive root of 29 but $\text{ord}_{29^2}(14) = 28$ so 14 is not primitive modulo $29^2$. □

## Section 9.4 - Index Arithmetic

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

*Solution*:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\text{ind}_5(n)$ | 22 | 2 | 16 | 4 | 1 | 18 | 19 | 6 | 10 | 3 | 9 | 20 | 14 | 21 | 17 | 8 | 7 | 12 | 15 | 5 | 13 | 11 |

**10. Exercise 2:** Find all of the solutions of the following:

(a) $3x^5 \equiv 1 \pmod{23}$

*Solution*:

$$\begin{aligned} 3x^5 &\equiv 1 \pmod{23} \\ \text{ind}_5(3) + 5 \cdot \text{ind}_5(x) &\equiv \text{ind}_5(1) \pmod{22} \\ 16 + 5 \cdot \text{ind}_5(x) &\equiv 0 \pmod{22} \\ 5 \cdot \text{ind}_5(x) &\equiv 6 \pmod{22} \end{aligned}$$

Solving for $\text{ind}_5(x)$ one finds that $\text{ind}_5(x) = 10$. Thus we have that $x \equiv 9 \pmod{23}$. □

(b) $3x^{14} \equiv 2 \pmod{23}$

*Solution*:

$$\begin{aligned} 3x^{14} &\equiv 2 \pmod{23} \\ \text{ind}_5(3) + 14 \cdot \text{ind}_5(x) &\equiv \text{ind}_5(2) \pmod{22} \\ 16 + 14 \cdot \text{ind}_5(x) &\equiv 2 \pmod{22} \\ 14 \cdot \text{ind}_5(x) &\equiv 8 \pmod{22} \end{aligned}$$

Solving for $\text{ind}_5(x)$ one finds that $\text{ind}_5(x) = 10$ or 21. Thus we have that $x \equiv 9$ or $x \equiv 14 \pmod{23}$. □

**11. Exercise 3:** Find all of the solutions of the following:

(a) $3^x \equiv 2 \pmod{23}$

*Solution*:

$$\begin{aligned} 3^x &\equiv 2 \pmod{23} \\ x \cdot \text{ind}_5(3) &\equiv \text{ind}_5(2) \pmod{22} \\ x \cdot 16 &\equiv 2 \pmod{22} \end{aligned}$$

Solving for $x$ one finds that $x = 7$ or $x = 18$. Thus we have that $x \equiv 7$ or $x \equiv 18 \pmod{22}$. □

(b) $13^x \equiv 5 \pmod{23}$

*Solution*:

$$\begin{aligned} 13^x &\equiv 5 \pmod{23} \\ x \cdot \text{ind}_5(13) &\equiv \text{ind}_5(5) \pmod{22} \\ x \cdot 14 &\equiv 1 \pmod{22} \end{aligned}$$

Since the GCD of 14 and 22 does not divide 1 there are no solutions. □

## 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 $x = 2$.

*Solution*: The prime divisors of $211 - 1$ are 2,3,5, and 7. We'll choose our test number to be 2. First note that $2^{210} \equiv 1 \pmod{211}$. Then we compute $2^{\frac{210}{q}}$ for each of the prime divisors of 210 mentioned above. we get:

$$\begin{aligned} 2^{\frac{210}{2}} &\equiv 210 \\ 2^{\frac{210}{3}} &\equiv 196 \\ 2^{\frac{210}{5}} &\equiv 107 \\ 2^{\frac{210}{7}} &\equiv 171 \end{aligned}$$

Since none of these is 1 we conclude that 211 is prime. □

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

*Solution*: First $3^{256/2} = 2^{128} \equiv -1 \pmod{257}$. Then note the only prime divisor of 256 is 2, thus since $3^{256/2} \not\equiv 1$ we can conclude that 257 is prime. □

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

*Solution*: Note that $449 = 7 \cdot 2^6 + 1$. Thus what we need to do is find an integer $a$ such that $a^{448/2} \equiv -1 \pmod{449}$. $a = 3$ does the trick, so we can conclude that 449 is prime. □