116 - Number Theory
Spring 2007

Homework 8 Solutions

Name: _____
Instructor: Travis Kelm

Section 7.3 - Perfect Numbers and Mersenne Primes

1. From Class: Show that every Mersenne prime greater than three ends in either a 1 or a 7.

Solution: Note that if M is a Mersenne prime other than three, then $M = 2^p - 1$ where p is an odd integer. We claim that 2^{odd} always ends in a 2 or an 8. It should be clear how the result about Mersenne primes follows from this claim.

We will prove the claim using induction. We can easily verify several base cases, namely, $2^3 = 8$, $2^5 = 32$, $2^7 = 128$. For the induction, assume that 2^{2k-1} ends in a 2 or an 8. This is equivalent to saying that $2^{2k-1} \equiv 2$ or $8 \pmod{10}$. The next power of 2 with odd exponent is 2^{2k+1}. Note that $2^{2k+1} = 4 \cdot 2^{2k-1}$ and thus

$$2^{2k+1} = 4 \cdot 2^{2k-1} \equiv 4 \cdot (2 \text{ or } 8) \pmod{10}$$

Finally notice that $4 \cdot 2 \equiv 8 \pmod{10}$ and $4 \cdot 8 \equiv 2 \pmod{10}$. Thus we have proven the inductive case, and have shown that 2^{odd} always ends in a 2 or an 8. □

Section 9.1 - Orders and Primitive Roots

2. Exercise 2: Determine each of the following:

(a) $\text{ord}_{11}(3)$

Solution: $\text{ord}_{11}(3)$ must divide $\phi(11) = 10$ so our candidates are 1, 2, 5, and 10. Note that $3^2 \equiv -2 \pmod{11}$ and thus $3^5 \equiv (-2)^2(3) \equiv 1$. Thus $\boxed{\text{ord}_{11}(3) = 5}$

(b) $\text{ord}_{17}(2)$

Solution: $\text{ord}_{17}(2)$ must divide $\phi(17) = 16$ so our candidates are 1, 2, 4, 8, and 16. Both 2^2 and 2^4 are less than 17 so they don't cut it. Next $2^8 = (2^4)^2 \equiv (-1)^2 = 1 \pmod{17}$ Thus $\boxed{\text{ord}_{17}(2) = 8}$

(c) $\text{ord}_{21}(10)$

Solution: $\text{ord}_{21}(10)$ must divide $\phi(21) = 12$ so our candidates are 1, 2, 3, 4, 6, and 12. Note that $10^2 \equiv -5 \pmod{21}$ and thus $10^3 \equiv -50 \equiv -8$. Next, $10^4 \equiv (-5)^2 \equiv 4$. Then $10^6 \equiv (-8)^2 \equiv 1$. Thus $\boxed{\text{ord}_{21}(10) = 6}$

(d) $\text{ord}_{25}(9)$

Solution: $\text{ord}_{25}(9)$ must divide $\phi(25) = 20$ so our candidates are 1, 2, 4, 5, 10 and 20. Note that $9^2 \equiv 6 \pmod{25}$ and thus $9^4 \equiv 6^2 \equiv 11$. Next, $9^5 \equiv (11)(9) \equiv -1$. This means that $9^{10} = (9^5)^2 \equiv (-1)^2 = 1$. Thus $\boxed{\text{ord}_{25}(9) = 10}$

3. Exercise 4: Find a primitive root modulo each of the following:

(a)	4	(d)	13
(b)	5	(e)	14
(c)	10	(f)	18

Solution:

(a) $3^2 \equiv 1 \pmod{4}$ thus 3 is a primitive root.

(b) Since $\phi(5) = 4$ the possible orders of elements is 1, 2, and 4. Note $2^2 = 4$ so the order of 2 is not two, hence it must be four. This makes 2 a primitive root. (Note that it also makes 3 a primitive root, since 3 is inverse of 2.)

(c) Since $\phi(10) = 4$ the possible orders of elements are 1, 2, and 4. Clearly $3^2 \not\equiv 1$ thus the order of 3 must be four, so 3 is primitive. (Note that 7 is also primitive.)

(d) Since $\phi(13) = 12$ the possible orders of elements are 1, 2, 3, 4, 6, and 12. Now $2^2 = 4$, $2^3 = 8$, $2^4 \equiv 3$, and $2^6 \equiv 12$. Thus 2 is a primitive root.

(e) Since $\phi(14) = 6$ the possible orders of elements are 1, 2, 3, and 6. Since $3^2 = 9$ and $3^3 \equiv 13$ it follows that 3 is a primitive root.

(f) Since $\phi(18) = 6$ the possible orders of elements are 1, 2, 3, and 6. Since $5^2 \equiv 7$ and $5^3 \equiv 17$ it follows that 5 is a primitive root.

□

4. **Exercise 6:** Show that 20 has no primitive roots.

Solution: The reduced residue system is $\{1, 3, 7, 9, 11, 13, 17, 19\}$ and the orders of the residues are listed in the following table

n	1	3	7	9	11	13	17	19
$\text{ord}_{20}(n)$	1	4	4	2	2	4	4	2

Since there is no residue of order 8, there are no primitive roots.

5. **Exercise 8:** Find a maximal set of incongruent primitive roots modulo 13.

Solution: First note that there will be $\phi(\phi(13)) = \phi(12) = 4$ primitive roots. We must proceed more or less by trial and error. The first candidate for being a primitive root is 2 so let's give it a try. We must show that $\text{ord}_{13}(2) = 12$. Also recall that $\text{ord}_{13}(2)$ must be a divisor of 12. Now compute

$$2^2 = 4 \qquad 2^3 = 8 \qquad 2^4 \equiv 3$$

the order of 2 is not 2, 3, or 4. Next $2^6 \equiv 3 \cdot 4 \equiv 12$. Thus $\text{ord}_{13}(2)$ is *not* 1,2,3,4, or 6. Hence $\text{ord}_{13}(2) = 12$ so 2 is a primitive root of 13.

Finally, by Corollary 9.4.1 we know that $2^1 = 1, 2^5 = 6, 2^7 = 11$ and $2^{11} = 7$ are all of the primitive roots. □

6. **Exercise 14:** Show that if m is a positive integer and if $a > 0$ is relatively prime to m with $\text{ord}_m(a) = m - 1$ then m is prime.

Solution: If a is relatively prime to m then we know that $\text{ord}_m(a) \leq \phi(m)$. Thus $\text{ord}_m(a) = m - 1$ implies that $\phi(m) = m - 1$, which in turn implies that m is prime. □

7. **Exercise 16:** Show that if r is a primitive root modulo m then the modular inverse of r is also a primitive root modulo m.

Solution: Let r be a primitive root modulo m. Thus $\phi(m)$ is the smallest integer satisfying $r^x \equiv 1 \pmod{m}$. First note that a modular inverse of r is $r^{\phi(m)-1}$. Indeed,

$$r \cdot r^{\phi(m)-1} = r^{\phi(m)} \equiv 1 \pmod{m}$$

Thus any modular inverse of r must be congruent to $r^{\phi(m)-1}$ modulo m, so it suffices to so that $r^{\phi(m)-1}$ is a primitive root. By theorem 9.4 we have that

$$\begin{aligned} \text{ord}_m(r^{\phi(m)-1}) &= \frac{\text{ord}_m(r)}{\gcd(\phi(m) - 1, \text{ord}_m(r))} \\ &= \frac{\phi(m)}{\gcd(\phi(m) - 1, \phi(m))} \\ &= \phi(m)/1 \end{aligned}$$

Thus $r^{\phi(m)-1}$ is a primitive root of m. □

8. **Primitive Existence:** Among the first 16 integers, which have primitive roots and which do not?

Solution: The following integers have primitive roots: 2,3,4,5,6,7,9,10,11,13, and 14. The rest do not. □