SOLUTIONS

Congruence mod n and Modular Arithmetic

1. Given integers a and b and $n \in \mathbb{N}$, we say $a \equiv b (\text{mod} n)$ if $n \mid (a-b)$.

2. Review of the division algorithm:

   (a) The Division Algorithm: Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = q \cdot b + r$, and $0 \leq r < b$.

   (b) What do q and r stand for in the division algorithm? $q =$ quotient, $r =$ remainder

   (c) For $a = 367$ and $b = 6$, find q and r.

   $$367 = 6 \cdot \underbrace{61}_{q} + \underbrace{1}_{r}$$

3. If the remainder when a is divided by n and the remainder when b is divided by n are the same, then $a \equiv b (\text{mod} n)$.

4. For each of the integers $m = 17$, $m = 7$, $m = -7$ and $m = -45$, find the integer r in $\{0, 1, 2, 3\}$ such that $m \equiv r (\text{mod} 4)$.

   $17 \equiv 1 (\text{mod} 4)$

   $7 \equiv 3 (\text{mod} 4)$

   $-7 \equiv 1 (\text{mod} 4)$

   $-45 \equiv 3 (\text{mod} 4)$

5. List the set of elements in $\mathbb{Z}$ that are congruent to 0 modulo 3. Then write that set in set-builder notation. Do the same for the integers that are congruent to 1 modulo 3 then again for the integers that are congruent to 2 modulo 3.

   $\{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\} = \{3n : n \in \mathbb{Z}\}$ (set of integers congruent to 0 (mod 3))

   $\{\ldots -7, -3, 1, 4, 7, \ldots\} = \{3n+1 : n \in \mathbb{Z}\}$ (set of integers congruent to 1 (mod 3))

   $\{-8, -2, 2, 6, \ldots\} = \{3n+2 : n \in \mathbb{Z}\}$ (set of integers congruent to 2 (mod 3))

6. There are a couple of common ways to determine if two numbers are congruent modulo n. One way is to reduce each of them modulo n to a number in $\{0, 1, 2, \ldots, n-1\}$ and then compare. Another is to find their difference and see if it is a multiple of n. Try using each of these methods to determine if $342 \equiv 482 (\text{mod} 7)$.

method 1: use division algorithm: $342 = 48 \cdot 7 + 6$

$482 = 68 \cdot 7 + 6$

Same remainder, so $342 \equiv 482 \text{ mod } 7$

method 2: $482 - 342 = 140 = 20 \cdot 7$. So $7 \mid (482-342)$. Thus $342 \equiv 482 (\text{mod } 7)$

7. It can be shown that if $a \equiv b(\bmod n)$ and $c \equiv d(\bmod n)$ then $(a+c) \equiv (b+d)(\bmod n)$. Use this idea to calculate $(582+385)(\bmod 10)$ without first adding.

$582 \equiv 2 \pmod{10}$; $385 \equiv 5 \pmod{10}$

$(582+385) \pmod{10} \equiv (2+5) \pmod{10} \equiv 7$

8. Similarly to the problem above, it can be shown that if $a \equiv b(\bmod n)$ and $c \equiv d(\bmod n)$ then $(ac) \equiv (bd)(\bmod n)$ (This is problem 24 of Chapter 5.) Use this idea to calculate $(182 \times 4931)(\bmod 3)$.

$182 \equiv 2 \pmod 3$

$4931 \equiv 2 \pmod 3$

$182 \times 4931 \equiv (2 \times 2) \pmod 3 \equiv 4 \pmod 3 \equiv 1 \pmod 3$

9. Calculate $11^3(\bmod 4)$. Give the answer as a number in the set $\{0,1,2,3\}$ that is congruent to $11^3(\bmod 4)$.

$11 \equiv 3 \pmod 4$

$11^3 \equiv 3^3 \pmod 4 \equiv 27 \pmod 4 \equiv 3 \pmod 4$

10. Determine the last digit in 7^{55}.

$7^1 \equiv 7 \pmod{10}$

$7^2 \equiv 49 \pmod{10} \equiv 9 \pmod{10}$

$7^4 \equiv 81 \pmod{10} \equiv 1 \pmod{10}$

$7^8 \equiv 1 \pmod{10}$

$7^{16} \equiv 1 \pmod{10}$

$7^{32} \equiv 1 \pmod{10}$

$7^{55} = 7^{32} \cdot 7^{16} \cdot 7^4 \cdot 7^2 \cdot 7^1$

$\equiv 1 \cdot 1 \cdot 1 \cdot 9 \cdot 7 \pmod{10}$

$\equiv 63 \pmod{10}$

$\equiv 3 \pmod{10}$

11. Much like in standard addition, there is an additive identity modulo n and numbers have additive inverses modulo n. What is the additive identity modulo n? What is the additive inverse of 5 modulo 7?

additive identity $= 0$. additive inverse of $5 \pmod 7 = -5 \pmod 7 \equiv 2 \pmod 7$

12. Much like in standard multiplication, there is a multiplicative identity modulo n and some numbers have multiplicative inverses modulo n. What is the multiplicative identity modulo n? Find the inverses of the numbers modulo 5. Do the same for the numbers modulo 6.

multiplicative identity is 1. multiplicative inverse means the product is 1.

mod 5: 0 has no inverse

1 is its own inverse

$2 \cdot 3 = 6 \equiv 1 \bmod 5$, so 2 and 3 are inverses of each other.

$4 \cdot 4 = 16 \equiv 1 \pmod 5$, so 4 is its own inverse.

mod 6: 0 has no inverse.

1 is its own inverse.

5 is its own inverse.

2, 3, 4 have no inverse.