9 Congruent Modulo

Properties of Congruence Modulo m

Theorem 9.1. *Let $m \in \mathbb{Z}$. For all $a, b, c \in \mathbb{Z}$, the following properties hold:*

1. ***Reflexivity:*** $a \equiv a \pmod{m}$.
2. ***Symmetry:*** *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$.
3. ***Transitivity:*** *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

Proof. We prove each property separately.

1. Reflexivity: By definition, $a \equiv b \pmod{m} \Rightarrow m \mid a - b$. Setting $b = a$, we have $m \mid a - a = 0 \Rightarrow m \mid 0$. Therefore, $a \equiv a \pmod{m}$.

2. Symmetry: H.W

3. Transitivity: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then we have:

$$m \mid (a - b) \quad \text{and} \quad m \mid (b - c).$$

This means there exist integers k_1 and k_2 such that:

$$a - b = k_1 m, \quad b - c = k_2 m.$$

Adding these two equations:

$$(a - b) + (b - c) = k_1 m + k_2 m.$$

Simplifying, we obtain:

$$a - c = (k_1 + k_2)m.$$

Since m divides $a - c$, it follows that $a \equiv c \pmod{m}$. □

Theorem 9.2. *If $a \equiv b \pmod{n}$, then for any positive integer $k \in \mathbb{Z}^+$,*

$$a^k \equiv b^k \pmod{n}.$$

Proof. We proceed by induction on k.

Base Case ($k = 1$): If $k = 1$, then $a^1 = a$ and $b^1 = b$, so $a \equiv b \pmod{n}$.

Inductive Step: Assume that for some $k = m$, the statement holds:

$$a^m \equiv b^m \pmod{n}.$$

We need to show that it holds for $k = m + 1$, i.e.,

$$a^{m+1} \equiv b^{m+1} \pmod{n}.$$

By the induction hypothesis,

$$a^m \equiv b^m \pmod{n}.$$

Multiplying both sides by a, we get:

$$a^m \cdot a \equiv b^m \cdot a \pmod{n}.$$

Since $a \equiv b \pmod{n}$, replacing a with b in the right-hand term gives:

$$b^m \cdot a \equiv b^m \cdot b \pmod{n}.$$

Thus,

$$a^{m+1} \equiv b^{m+1} \pmod{n}.$$

By induction, the theorem holds for all $k \in \mathbb{Z}^+$. □ □

Theorem 9.3. *Let m be a positive integer and a, b be integers. Then,*

$$(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m.$$

Proof. Clearly, we have:

$$a \equiv a \pmod m, \quad \text{and} \quad b \equiv b \pmod m.$$

Thus, adding both congruences,

$$a + b \equiv (a \mod m) + (b \mod m) \pmod m.$$

□

Theorem 9.4. *Let m be a positive integer and a, b be integers. Then,*

$$(a \cdot b) \mod m = ((a \mod m) \cdot (b \mod m)) \mod m.$$

Proof: *H.W*

Example 9.1. What is $2008^{2008} \mod 3$?

Sol.

$$2008^{2008} = \underbrace{(2008 \times 2008 \times \cdots \times 2008)}_{\text{(2008 times)}} \mod 3$$

Using the property of modular arithmetic:

$$= \underbrace{((2008 \mod 3) \times \cdots \times (2008 \mod 3))}_{\text{(2008 times)}} \mod 3$$

Since $2008 \mod 3 = 1$, we have:

$$= (1 \times 1 \times \cdots \times 1) \mod 3$$

Thus,

$$= 1^{2008} \mod 3 = 1 \mod 3 = 1.$$

So, $2008^{2008} \mod 3 = 1$. ☐

Example 9.2. Find the remainder when $1! + 2! + \cdots + 100!$ is divided by 15.

Sol. Notice that when $k \geq 5$, $k! \equiv 0 \pmod{15}$. Therefore,

$$1! + 2! + \cdots + 100! \equiv 1! + 2! + 3! + 4! + 0 + \cdots + 0 \pmod{15}.$$

Now, compute the factorials modulo 15 for $1!$, $2!$, $3!$, and $4!$:

$$1! = 1, \quad 2! = 2, \quad 3! = 6, \quad 4! = 24.$$

Thus, we have:

$$1! + 2! + 3! + 4! \equiv 1 + 2 + 6 + 24 \pmod{15}.$$

Simplifying the sum:

$$1 + 2 + 6 + 24 = 33.$$

Now, take modulo 15:

$$33 \mod 15 = 3.$$

Therefore, the remainder when the given sum is divided by 15 is 3. ☐

Example 9.3. Find the remainder when 16^{53} is divided by 7.

Sol. First, reduce the base to its least residue modulo 7:

$$16 \equiv 2 \pmod{7}.$$

So,

$$16^{53} \equiv 2^{53} \pmod{7}.$$

we can write 53 as $53 = 3 \times 17 + 2$, so:

$$2^{53} = 2^{3 \cdot 17+2} = (2^3)^{17} \cdot 2^2.$$

Since $2^3 \equiv 1 \pmod 7$, we have:

$$(2^3)^{17} \equiv 1^{17} \equiv 1 \pmod 7.$$

Therefore:

$$2^{53} \equiv 1 \cdot 2^2 \equiv 4 \pmod 7.$$

Thus, $16^{53} \equiv 4 \pmod 7$, by the transitive property.

Therefore, the remainder when 16^{53} is divided by 7 is 4. □

9.1 Exercises of Congruent modulo

Exercises

1. If $a \equiv b \pmod m$, prove that $b \equiv a \pmod m$.

2. Let m be a positive integer and a, b be integers. Prove that,

$$(a \cdot b) \mod m = ((a \mod m) \cdot (b \mod m)) \mod m.$$

3. Find the remainder when 3^247 is divided by 17.

4. Find the value of each of the following:

   (a) $2^{32} \mod 7$.

   (b) $10^{35} \mod 7$.

   (c) $3^{35} \mod 7$.

5. If $a \equiv 4 \pmod 7$ and $b \equiv 5 \pmod 7$, what is $a+b \mod 7$? What is $a \times b \mod 7$?