8 Theory of Congruence's

Defintion of Congruent

Definition 8.1. Let m be a positive integer. We say that a is congruent to b modulo m denoted as $a \equiv b \pmod{m}$, if $m \mid (a-b)$, where a and b are integers.

Example 8.1. We want to check if $a \equiv b \pmod{m}$

1. $25 \equiv 1 \pmod{4}$ since $4 \mid 25-1$.
2. $25 \not\equiv 2 \pmod{4}$ since $4 \nmid 25-2$.
3. $1 \equiv -3 \pmod{4}$ since $4 \mid 1-(-3)$.
4. If n is even $n \equiv 0 \pmod{2}$.
5. If n is odd $n \equiv 1 \pmod{2}$.

Theorem 8.1. *If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.*

Proof. ($\Rightarrow$): Suppose $a \equiv b \pmod{m} \Rightarrow m \mid (a-b) \Rightarrow a-b = km \Rightarrow a = b+km$
($\Leftarrow$) suppose that there exists an integer k such that $a = b+km \Rightarrow a-b = km \Rightarrow m \mid (a-b)$. Then

$$a \equiv b \pmod{m}$$

□

Theorem 8.2. *For $m > 0$ and for all integers a and b:*

$$a \equiv b \pmod{m} \iff a \pmod{m} = b \mod m.$$

$a \pmod{m} = r$ where r is the remainder given by the Division Algorithm when m is divided by m.

Example 8.2. It is 11 PM, and you want to sleep for 8 hours. To determine when to set your alarm, you need to compute the time 8 hours after 11 PM.

First, we add 8 hours to 11 PM:

$$11 + 8 = 19$$

Since time is typically measured on a 12-hour clock, we need to take the result modulo 12:

$$19 \pmod{12} = 7$$

Thus, you should set your alarm for 7 AM.

Example 8.3. To what least residue (mod 11) is each of 23, 29, 31, 37, and 41 congruent?

Sol. We will compute the remainder when each number is divided by 11.

$$23 \div 11 = 2 \text{ remainder } 1 \quad \Rightarrow \quad 23 \equiv 1 \pmod{11}$$

$$29 \div 11 = 2 \text{ remainder } 7 \quad \Rightarrow \quad 29 \equiv 7 \pmod{11}$$

$$31 \div 11 = 2 \text{ remainder } 9 \quad \Rightarrow \quad 31 \equiv 9 \pmod{11}$$

$$37 \div 11 = 3 \text{ remainder } 4 \quad \Rightarrow \quad 37 \equiv 4 \pmod{11}$$

$$41 \div 11 = 3 \text{ remainder } 8 \quad \Rightarrow \quad 41 \equiv 8 \pmod{11}$$

Thus, the least residues modulo 11 are:

$$23 \equiv 1 \pmod{11}, \quad 29 \equiv 7 \pmod{11}, \quad 31 \equiv 9 \pmod{11}, \quad 37 \equiv 4 \pmod{11}, \quad 41 \equiv 8 \pmod{11}.$$

□

Theorem 8.3. *Let m be a positive integer. If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then:*

$$a + c \equiv b + d \ (mod\ m).$$

Proof.

$$a \equiv b \pmod{m} \iff m \mid (a-b) \iff (a-b) = k_1 \cdot m \quad \text{for some integer } k_1.$$

$$c \equiv d \pmod{m} \iff m \mid (c-d) \iff (c-d) = k_2 \cdot m \quad \text{for some integer } k_2.$$

Now, consider the expression $(a+c)-(b+d)$:

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

Since $m \mid [(a+c)-(b+d)]$, by the equivalent definition of congruence, we conclude that:

$$a+c \equiv b+d \pmod{m}.$$

□

Example 8.4.

$$10001 + 20000005 + 3004 \equiv ? \pmod{10}$$

Sol. First, we calculate each number modulo 10:

$$10001 \equiv 1 \pmod{10}$$

$$20000005 \equiv 5 \pmod{10}$$

$$3004 \equiv 4 \pmod{10}$$

Now, add them together modulo 10:

$$10001 + 20000005 + 3004 \equiv 1+5+4 \pmod{10} \equiv 10 \pmod{10} \equiv 0 \pmod{10}$$

□

Theorem 8.4. *Let m be a positive integer. If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then:*

$$ac \equiv bd \ (mod\ m).$$

Proof.

$$a \equiv b \pmod{m} \iff m \mid (a-b) \iff (a-b) = k_1 \cdot m \quad \text{for some integer } k_1.$$

$$c \equiv d \pmod{m} \iff m \mid (c-d) \iff (c-d) = k_2 \cdot m \quad \text{for some integer } k_2.$$

Now, consider the expression $ac - bd$:

$$ac - bd = ac - ad + ad - bd = a(c-d) + d(a-b).$$

We can factor out m from both terms:

$$ac - bd = a \cdot m \cdot k_2 + d \cdot m \cdot k_1 = m \cdot (a \cdot k_2 + d \cdot k_1).$$

Since $m \mid (ac - bd)$, by the equivalent definition of congruence, we conclude that:

$$ac \equiv bd \pmod{m}.$$

□

Example 8.5. Compute $10001 \times 20000005 \mod 13$.

Sol. First, compute each number modulo 13:

$$10001 \equiv 4 \pmod{13}$$

$$20000005 \equiv 12 \pmod{13}$$

Now, multiply these values:

$$10001 \times 20000005 \equiv 4 \times 12 \pmod{13}$$

$$\equiv 48 \pmod{13}.$$

Since $48 \div 13 = 3$ with a remainder of 9, we conclude:

$$48 \equiv 9 \pmod{13}.$$

Thus,

$$10001 \times 20000005 \equiv 9 \pmod{13}.$$

□

8.1 Exercises of Theory of Congruence's

Exercises

1. If $a \equiv b \pmod{m}$ and $n \mid m$, prove that $a \equiv b \pmod{n}$.
2. Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, prove that $a + c \equiv b + d \pmod{m}$.
3. Find $46, 59, 61, 77,\ and\ 58 \pmod{39}$.
4. Find the least nonnegative residue modulo 13
   (a) $22 \mod 13$
   (b) $-1 \mod 13$
   (c) $-100 \mod 13$
5. What time does a clock read: (1). 29 hours after it reads 11 o'clock? (2) 50 hours before it reads 6 o'clock?