Congruences and Linear Congruences

We say that a and b are congruent to each other modulo m,

$$a \equiv b \mod m$$

if $m \mid (a-b)$.

For example,

$$\begin{aligned} -2 &\equiv 5 \mod 7 \qquad -2-5=-7, \quad 7 \mid -7 \\ 10 &\equiv 6 \mod 6 \qquad 10-6=4, \quad 4 \mid 4 \\ 10 &\equiv 2 \mod 4 \qquad 10-2=8, \quad 4 \mid 8 \end{aligned}$$

Theorem : (4.1)

If $a \equiv b \mod m$, then there exists k such that $a = b + km$.

Proof. By definition, $m \mid (a-b)$. Then, $a - b = mk$ by divisibility. Therefore, $a = mk + b$. □

Theorem : (4.2)

There is a unique r, call this the least residue modulo m.

$$a \equiv r \mod m$$

$$r \in \{0, 1, 2, \ldots, m-2, m-1\}$$

Proof. By the division theorem with a, m, there are unique integers k and r such that:

$$a = km + r, \quad 0 \leq r < m$$

Thus, $a \equiv r \mod m$ by the previous theorem. □

Example

What is the residue of:

$$44 \mod 3, \qquad 44 \mod 4, \qquad 44 \mod 5$$

In the first case, $44 \equiv 2 \mod 3$

In the second case, $44 \equiv 0 \mod 3$

In the third case, $44 \equiv 4 \mod 5$.

Theorem : (4.3)

$a \equiv b \mod m$ if and only if they have the same remainder when divided by m.

Proof. Suppose a and b have the same remainder when divided by m.

$$a = q_1 m + r \qquad b = q_2 m + r$$

By the division algorithm,

$$\begin{aligned} a - b &= (q_1 m + r) - (q_2 m + r) \\ &= q_1 m - q_2 m \\ &= m\,(q_1 - q_2) \end{aligned}$$

Thus, $m \mid (a - b)$ by definition. Then, $a \equiv b \mod m$ by definition.

Now, suppose that $a \equiv b \mod m$. Then, $a \equiv b \equiv r \mod m$, where r is the least residue modulo m. Then, from Theorem 4.1, we have that:

$$a = q_1 m + r \quad \text{and} \quad b = q_2 m + r$$

For some integers q_1 and q_2, since $0 \leq r < m$. Thus, a and b have the same remainder when divided by m. □

Lemma : (4.1)

For integers a, b, c, d, we have that:

- $a \equiv a \mod m$
- If $a \equiv b \mod m$, then $b \equiv a \mod m$
- If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$
- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$
- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$

Theorem : (4.4)

This is listed as a lemma in the in-person notes.

Suppose $ab \equiv ac \mod m$, then if $(a, m) = 1$, then $b \equiv c \mod m$.

Proof. By the definition of congruence, $m \mid (ac - bc)$ or $m \mid c\,(a - b)$. From Theorem 1.5, this means that $m \mid (a - b)$ since $(m, c) = 1$. Therefore, by the definition of congruence, $a \equiv b \mod m$. □

Example

a) What values of x satisfy $2x \equiv 4 \mod 7$.
b) What values of x satisfy $2x \equiv 1 \mod 7$.

---

a) Since $(2, 7) = 1$, Theorem 4.4 gives us that $x \equiv 2 \mod 7$.
b) Note that $2x \equiv 1 \equiv 8 \mod 7$. Since $(2, 7) = 1$, Theorem 4.4 gives us that $x \equiv 4 \mod 7$.

Theorem : (4.5)

This is listed as a lemma in the in-person notes.

If $ac \equiv bc \mod m$ and $(c, m) = d$, then $a \equiv b \mod \frac{m}{d}$.

Proof. If $ac = bc \mod m$, then $m \mid c(a-b)$ and $\frac{m}{d} \mid \left(\frac{c}{d}\right)(a-b)$. Since we know that $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, Theorem 1.5 gives us that $\frac{m}{d} \mid (a-b)$. Therefore, by the definition of congruence, $a \equiv b \mod \frac{m}{d}$ □

Example

Which x will satisfy $3x \equiv 15 \mod 9$?

By Theorem 4.5, we have that

$$\begin{aligned} 3x &\equiv 15 \mod 9 \\ x &\equiv 5 \mod 3 \\ x &\equiv 2 \mod 3 \end{aligned}$$