Note Title 8/8/2022

Lecture 5

Monday, 8/8/2022

§ Congruences: A 'congruence' is nothing more than a statement about divisibility. However, it often makes it easier to discover proofs. The theory of congruences was introduced by Carl Friedrich Gauss (1777–1855).

Definition: Let $m \geq 1$ be an integer. If a and b are two integers such that $m \mid (a-b)$, then we say that a is congruent to b modulo m, and we write $a \equiv b \pmod{m}$.

Example: $4 \equiv 1 \pmod{3}$, $-5 \equiv 2 \pmod{7}$, etc.

__Theorem 1:__ Let $m \geq 1$, and $a, b, c, d \in \mathbb{Z}$. Then:

(1) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are all equivalent statements.

(2) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

(3) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

(4) If $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$, then $a \equiv b \pmod{d}$.

(5) If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for $c > 0$.

__Proof:__ Easy.

__Corollary:__ congruence is an equivalence relation. #

Theorem 2: (1) $a \cdot x \equiv a \cdot y \pmod{m} \iff x \equiv y \left(\bmod \dfrac{m}{\gcd(a,m)}\right)$.

(2) If $ax \equiv ay \pmod{m}$, and $\gcd(a,m) = 1$, then $x \equiv y \pmod{m}$.

(3) $x \equiv y \pmod{m_i}$ for $i = 1, 2, \cdots, n$ if and only if

$$x \equiv y \pmod{\operatorname{lcm}(m_1, m_2, \cdots, m_n)}.$$

Proof: (1) $ax \equiv ay \pmod{m} \Rightarrow ax - ay = mz$ for some $z \in \mathbb{Z}$

$$\Rightarrow \frac{a}{\gcd(a,m)} \cdot x - \frac{a}{\gcd(a,m)} \cdot y = \frac{m}{\gcd(a,m)} \cdot z$$

$\Rightarrow \dfrac{m}{\gcd(a,m)} \,\Big|\, \dfrac{a}{\gcd(a,m)}(x-y)$. But $\gcd\left(\dfrac{a}{\gcd(a,m)}, \dfrac{m}{\gcd(a,m)}\right) = 1$

and hence $\dfrac{m}{\gcd(a,m)} \,\Big|\, (x-y) \Rightarrow x \equiv y \left(\bmod \dfrac{m}{\gcd(a,m)}\right)$.

Conversely, suppose that $x \equiv y \left(\bmod \dfrac{m}{\gcd(a,m)}\right)$.

$$\Rightarrow \quad ax \equiv ay \left(\bmod \frac{am}{\gcd(a,m)}\right) \longrightarrow (*)$$

Now, $$\frac{am}{\gcd(a,m)} = \frac{a}{\gcd(a,m)} \cdot m$$

$$\Rightarrow \quad m \;\Big|\; \frac{am}{\gcd(a,m)} \longrightarrow (**)$$

Hence, $(*)$ & $(**)$ $\Rightarrow$ $ax \equiv ay \pmod{m}$. This completes the proof of (1).

#

(2) This is a special case of (1).

(3) $x \equiv y \pmod{m_i}$, $i = 1, 2, \ldots, n \Rightarrow m_i \mid (x-y)$ $\forall i = 1, 2, \ldots, n$.

$\Rightarrow x - y$ is a common multiple of $m_1, m_2, \ldots, m_n$

$\Rightarrow \operatorname{lcm}(m_1, m_2, \ldots, m_n) \mid x - y$

$\Rightarrow x \equiv y \pmod{\operatorname{lcm}(m_1, m_2, \ldots, m_n)}$.

Conversely, if $x \equiv y \pmod{\operatorname{lcm}(m_1, m_2, \ldots, m_n)}$, then by Theorem 1, we have $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, n$ since $m_i \mid \operatorname{lcm}(m_1, m_2, \ldots, m_n)$ $\forall i$.

#

Ex: Find the last digit of 7^{358}

Solution: $7^2 = 49 \equiv -1 \pmod{10}$ $\qquad 358 = 2 \times 179$

$$\Rightarrow (7^2)^{179} \equiv (-1)^{179} \pmod{10}$$

$$\Rightarrow 7^{358} \equiv -1 \equiv 9 \pmod{10}.$$

$\therefore$ 9 is the last digit of 7^{358}. #

—— x ——

Let $m \geq 1$. Then, we see that every integer is congruent modulo m to one of the values $0, 1, 2, \ldots, m-1$. Also, it is clear that no two of these m integers are congruent modulo m. These m values constitute a complete residue system modulo m.

Definition: If $x \equiv y \pmod{m}$, then y is called a residue of x modulo m. A set $\{x_1, x_2, \ldots, x_m\}$ is called a complete residue system modulo m if for every y there is one and only one x_j such that $y \equiv x_j \pmod{m}$.

- It is obvious that there are infinitely many complete residue system modulo m.

- $\bar{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = m\mathbb{Z} = 0 + m\mathbb{Z}$

  $\bar{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = 1 + m\mathbb{Z}, \ldots, \overline{m-1} = (m-1) + m\mathbb{Z}.$

  For each $i = 0, 1, \ldots, m-1$, let $x_i \in i + m\mathbb{Z}$. Then $\{x_0, x_1, \ldots, x_{m-1}\}$ is a complete residue system modulo m. #

Theorem 3: If $b \equiv c \pmod{m}$, then $\gcd(b, m) = \gcd(c, m)$.

Proof: $b \equiv c \pmod{m} \Rightarrow b = c + km$ for some integer k.

Now, $\gcd(c, m) = \gcd(c + km, m)$ [using properties of gcd]

$= \gcd(b, m)$.

#

Definition: A reduced residue system modulo m is a set of integers r_i such that $\gcd(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ whenever $i \neq j$, and every x coprime to m is congruent modulo m to some member r_i of the set.

#

For $m \geq 1$, let $\varphi(m) = \#\{k \mid 1 \leq k \leq m,\ \gcd(k,m) = 1\}$.

<u>Theorem 4</u>: Let $m \geq 1$. Let $R = \{r_1, \ldots, r_k\}$ be a set of reduced residue system modulo m. Then, $\# R = k = \varphi(m)$.

x

In view of Theorem 3, it is clear that a reduced residue system modulo m can be obtained by deleting from a complete residue system modulo m those members that are not relatively prime to m.

Let $m = 8$. Then, $\{0, 1, 2, 3, 4, 5, 6, 7\}$ is a complete residue system modulo 8. Also, $\{1, 3, 5, 7\}$ is a reduced residue system modulo 8. #