

18.781

21 Feb 2003

Congruences

 $a \equiv b \pmod{m}$ means $m \mid a-b$ Ex: The equation $x^2 - 21x + 1 = 0$ has no soln in the integer.If such an integer existed, it would solve $x^2 \equiv -1 \pmod{7}$ So we square $\{0, 1, 2, 3, 4, 5, 6\}$ + check they're not $\equiv -1 \pmod{7}$

$$0^2 \equiv 0 \quad 1^2 \equiv 1 \quad 2^2 \equiv 4 \quad 3^2 \equiv 9 \equiv 2 \quad 4^2 \equiv 16 \equiv 2 \quad 5^2 \equiv 25 \equiv 4 \quad 6^2 \equiv 36 \equiv 1$$

Prop let f be a polynomial with integer coeff, and say $a \equiv b \pmod{m}$.Then $f(a) \equiv f(b) \pmod{m}$.Proof: $f(z) = c_0 + c_1 z + \dots + c_n z^n$

$$a \equiv b \pmod{m} \Rightarrow a^r \equiv b^r \pmod{m}, \forall r$$

$$c_0 + c_1 a + \dots + c_n a^n \quad c_0 + c_1 b + \dots + c_n b^n$$

We have $c_r a^r \equiv c_r b^r \pmod{m}$, and we know sums of congruent things are still congruent.

Thm:

$$(i) \quad ax \equiv ay \pmod{m} \text{ iff } x \equiv y \pmod{\frac{m}{(a,m)}}$$

$$(ii) \quad \text{Given } m_1, \dots, m_r. \text{ Then } x \equiv y \pmod{m_i}, \forall i \text{ iff } \\ x \equiv y \pmod{[m_1, \dots, m_r]}$$

Proof:

$$(i) \quad \text{Last time, } ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$$

$$\text{conversely, if } x \equiv y \pmod{\frac{m}{(a,m)}} \Rightarrow x-y = \frac{m}{(a,m)}z$$

$$ax-ay = m \left(\frac{a}{(a,m)}z\right) \Rightarrow m \mid (ax-ay) \Rightarrow ax \equiv ay \pmod{m}$$

(ii) $x \equiv y \pmod{m_i} \forall i \Rightarrow m_i \mid x-y$, for all $i \Rightarrow x-y$ is common multiple of m_i 's. Since every common mult. is a mult. of least common multiple,

$$[m_1, \dots, m_r] \mid x-y \Rightarrow x \equiv y \pmod{[m_1, \dots, m_r]}$$

$$\text{conversely, if } x \equiv y \pmod{[m_1, \dots, m_r]}, [m_1, \dots, m_r] \mid x-y \Rightarrow$$

$$m_i \mid x-y, \forall i \text{ since } [m_1, \dots, m_r] = m_i c_i \text{ for all } i \Rightarrow x \equiv y \pmod{m_i} \forall i$$

Residue classes:

Def. If $x \equiv y \pmod{m}$, then y is called a residue of $x \pmod{m}$.Recall: For any x , $\exists!$ residue of x in the set $\{0, \dots, m-1\} \pmod{m}$

Def. A set $\{x_1, \dots, x_m\}$ is called a complete residue system (mod m) if for any n , $\exists! x_i$ s.t. $n \equiv x_i \pmod{m}$

ex. $\{2, 3, \dots, m+1\}$ is also complete residue system.

Def. The congruence class (residue class) of $n \pmod{m}$ is the set $\{n+mx \mid x \in \mathbb{Z}\}$

Prop. If $b \equiv c \pmod{m}$, then $(b, m) = (c, m)$.

Proof. $b \equiv c \pmod{m} \Rightarrow b = c + mx$ some x .

$$(b, m) = (c + mx, m) = (c, m).$$

Def. A reduced residue system (mod m) is a set of integers r_i with $(r_i, m) = 1$ s.t. for any n with $(n, m) = 1$, $\exists! r_i$ s.t. $n \equiv r_i \pmod{m}$.

ex. $\{r_i \mid 0 < r_i < m \text{ and } (r_i, m) = 1\}$ is a reduced residue syst.

Def. $\phi(m)$ is the number of elts. in any reduced residue syst. (mod m), which is the number of integers $0 < r < m$ which are prime to m

Thrm: If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$

cor. If p prime, $\phi(p) = p-1$. If p prime, $p \nmid a$ then $a^p \equiv a \pmod{p}$

Equivalently, $a^{p-1} \equiv 1 \pmod{p}$. (Fermat's Little Thrm)