Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Congruences

Dr. V. Piramanantham
Professor
Department of Mathematics

Congruences: another form of divisibility

useful –

Definition: If an integer m, not zero, divides the difference $a-b$, then we say that a is congruent to b modulo m.

If a is congruent to b modulo m, we write

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

otherwise, $a \not\equiv b \pmod{m}$

Note: $m \mid a-b \iff a \equiv b \pmod{m}$

Define $a \sim b$ if $a \mid b$ $\Rightarrow$ '$\sim$' is partial order

$a, b > 0$

(i) $\sim$ is reflexive $\quad a \mid a$

(2) Anti symmetric $\quad a \mid b \;\&\; b \mid a \Rightarrow a = b$

(3) transitive.

W.

$a \mid b \;\&\; b \mid c \Rightarrow a \mid c.$

$a \sim b \;\&\; b \sim c \Rightarrow a \sim c.$

Define a relation R as follow:

$\cdot\, a R b \iff a \equiv b \pmod{m}.$

R is equivalent (Proof is left as exercise)

Example: $m = 7$, $\quad 16 \equiv 2 \pmod{7}$

$7 \equiv 0 \pmod{7}$

$6 \equiv 2 \pmod{-7}$
$5 \not\equiv 2 \pmod{-7}$

$15 \equiv 2 \pmod{7}$?

is 15 congruent to 2 modulo 7 ?

NO.

Remarks: $m \neq 0$. $m \mid a-b \iff -m \mid a-b$

we restrict m to be a +ve int.

modulus values $m > 0$

Recall. (Divisibility properties)

① $a \mid a$

④ $a \mid b, a \mid c \Rightarrow a \mid bx+cy$

(2) $a \mid b \Leftrightarrow a \mid -b$ ← 1

(3) $a \mid b$ & $b \mid c \Rightarrow a \mid c$

(5) $a \mid b$ & $c \mid d \Rightarrow ac \mid bd$

(6) $a \mid b$ & $c > 0$, $ac \mid bc$

Properties: Let a, b, c be any integers & $m > 0$.

(i) $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$

$\Leftrightarrow a - b \equiv 0 \pmod{m}$

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

$\overset{\text{By defn}}{\Longleftrightarrow} m \mid a - b$

$\Leftrightarrow m \mid -(a-b)$

$\Longleftrightarrow m \mid b - a$

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

$a \equiv b \pmod{m} \Longleftrightarrow m \mid a - b$

$\Longleftrightarrow m \mid (a-b) - 0$

$\Longleftrightarrow a - b \equiv 0 \pmod{m}$

② If $a \equiv b \pmod{m}$ & $b \equiv c \pmod{m}$

then $a \equiv c \pmod{m}$

② If $a \equiv b \pmod{m}$ & $b \equiv c \pmod{m}$

then $a \equiv c \pmod{m}$

Proof

$a \equiv b \pmod{m} \Rightarrow m \mid a-b$

$b \equiv c \pmod{m} \Rightarrow m \mid b-c$

$\left.\begin{array}{l} k \mid n \\ k \mid l \end{array}\right\} \Rightarrow \left.\begin{array}{l} k \mid nx + ly \\ x = y = 1 \Rightarrow k \mid n + l \end{array}\right\} \Rightarrow$

$\Rightarrow m \mid (a - \cancel{b}) + (\cancel{b} - c)$

$\Rightarrow m \mid a - c$

③ If $a \equiv b \pmod m$ & $c \equiv d \pmod m$

then $a+c \equiv b+d \pmod m$

$a=c$
$b=d$

$2a \equiv 2b \pmod m$

$a^2 \equiv b^2 \pmod m$

$ac \equiv bd \pmod m$

$a \equiv b$
$c \equiv d$

$\Rightarrow a+c = b+d$

$a=b$
$c=d$
$\Rightarrow a+c = b+d$
$ac = bd$

Proof

$a \equiv b \pmod m \Rightarrow m \mid a-b$

$c \equiv d \pmod m \Rightarrow m \mid c-d$

$\Rightarrow m \mid (a-b)+(c-d)$

$\Rightarrow m \mid (a+c)-(b+d)$

$\Rightarrow a+c \equiv b+d \pmod m$

$m \mid a-b$

$m \mid c$

$m \mid (a-b)x + (c-d)y$

$a \equiv b \pmod{m} \Rightarrow m \mid a-b$

$c \equiv d \pmod{m} \Rightarrow m \mid c-d$

$\Rightarrow m \mid (a-b)x + (c-d)y$ for any integers x & y.

$\left.\begin{matrix} x = c \\ y = b \end{matrix}\right\} \Rightarrow m \mid (a-b)c + (c-d)b$

$\Rightarrow m \mid ac - \cancel{bc} + \cancel{bc} - bd$

$\Rightarrow m \mid ac - bd$

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

(3*) If $a \equiv b \pmod m$, then for any +ve integer n,

$$na \equiv nb \pmod m$$

(repeated application of (3))

$$a^n \equiv b^n \pmod m$$

Proof: Hint $na = a + a + a \cdots$ n times

$a^n = a \cdot a \cdots$ n times

$a = c$, $b = d$ in property (3).

3** If $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$ is a polynomial with integral coefficients ($c_0, c_1, \ldots c_n$ are integers) and $a \equiv b \pmod{n}$, then

$$f(a) \equiv f(b) \pmod{m}$$

Proof

$$a \equiv b \pmod{m} \Rightarrow c_1 a \equiv c_1 b \pmod{m}$$

$$\Downarrow$$

$$a^2 \equiv b^2 \pmod{m} \Rightarrow c_2 a^2 \equiv c_2 b^2 \pmod{m}$$

$$\vdots$$

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

$$\Rightarrow c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0 \equiv c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 \pmod{m}$$

$$\Rightarrow f(a) \equiv f(b) \pmod{m}$$

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

then $a \equiv b \pmod{d}$

(the modulus m can be replaced by any of its divisor)

Proof $a \equiv b \pmod{m} \Rightarrow m \mid a-b$

Given that $d \mid m$

$\Rightarrow d \mid a-b$

(5) If $a \equiv b \pmod{m}$, then for any int $c > 0$

$$ac \equiv bc \pmod{m} \qquad 3(i)$$

$$ac \equiv bc \pmod{mc}$$

<u>proof</u> $a \equiv b \pmod{m} \Rightarrow m \mid a-b$

$$\Rightarrow m \mid c(a-b)$$

$$\Rightarrow m \mid ac-bc$$

$$\Rightarrow ac \equiv bc \pmod{m}$$

$$a \equiv b \pmod{m} \Rightarrow m \mid a-b$$

$$\Rightarrow mc \mid (a-b)c$$

$$\Rightarrow mc \mid ac-bc$$

$$\Rightarrow ac \equiv bc \pmod{m}$$

5* Let $c > 0$

$$ac \equiv bc \pmod{mc} \Rightarrow a \equiv b \pmod{m}$$

$a^2 = b^2$

$a = b.$

$a = b \Rightarrow ac = bc$

no restriction on c

c

$c \neq 0$

$ac = bc \Rightarrow a = b$

implication

6 If $ac \equiv bc \pmod{m}$, is it true that $a \equiv b \pmod{m}$

(need not be true)

Example $m = 6$

$6 \mid 56 - 14$

$6 \mid 42$

Example

$$m = 6$$

$$6 \mid 56-14$$
$$6 \mid 42$$

$$56 \equiv 14 \pmod{6}$$

$$\Rightarrow 2 \cdot 28 \equiv 2 \cdot 7 \pmod{6}$$

But $28 \not\equiv 7 \pmod{6}$

(a, m) – the gcd of a & m

Theorem: (1) $ax \equiv ay \pmod{m}$ if and only if

$$x \equiv y \left(\bmod \frac{m}{(a,m)}\right)$$

(2) If $ax \equiv ay \pmod{m}$ and $(a,m)=1$

then $x \equiv y \pmod{m}$

(3) Let $m_1, m_2, \ldots, m_r$ be +ve integers,

then $x \equiv y \pmod{m_i}$, $i = 1, 2, \ldots, r$

if and only if

Remark: $x \equiv y \pmod 3$ and $x \equiv y \pmod 4$

$\iff \quad x \equiv y \pmod{12}$

Proof

① $ax \equiv ay \pmod m$

$\Rightarrow \quad m \mid ax - ay$ congruence defn

$\exists$ an integer z s.t. divisor defn.

$ax - ay = mz$

$\Rightarrow a(x-y) = mz$

But (a, m) ...

So, $\dfrac{a}{(a,m)}(x-y) = \dfrac{m}{(a,m)} z$

If $a \mid bc$ & $(a,b)=1$, then $a \mid c$

$\Rightarrow \dfrac{m}{(a,m)} \;\Big|\; \dfrac{a}{(a,m)}(x-y)$ {defn of divisor

$\left(\dfrac{m}{(a,m)}, \dfrac{a}{(a,m)}\right) = 1$, $\dfrac{m}{(a,m)} \;\Big|\; x-y$

By congruence defn $\Rightarrow x \equiv y \left(\bmod \dfrac{m}{(a,m)}\right)$

By congruence thm $\Rightarrow \quad x \equiv y \left(\bmod \dfrac{m}{(a,m)}\right)$

Conversely

$\times (a,m)$

$$x \equiv y \left(\bmod \frac{m}{(a,m)}\right)$$

$$(a,m)\,x \equiv (a,m)\,y \pmod{m}$$

$\times \dfrac{a}{(a,m)}$

$$\frac{a}{\cancel{(a,m)}}\,\cancel{(a,m)}\,x \equiv \frac{a}{\cancel{(a,m)}}\,\cancel{(a,m)}\,y \pmod{m}$$

Here property (5) has been applied

$$\Rightarrow \quad ax \equiv ay \pmod{m}$$