Modular Arithmetic

Often we really care about remainder only.

Ex: Given it is 5pm what time will it be in 500 hours?

seems this is a lot of work, but really is not. We only care about the remainder when divided by 24.

$$\frac{500}{24} = 20 \qquad 500 - 24 \cdot 20 = \boxed{20}$$

20 hours after 5 pm it will be 1pm.

We have special symbols for remainders: $a \bmod n$ e.g. we found

$500 \bmod 24 = 20$.

Def: If $a, b \in \mathbb{Z}$ $m \in \mathbb{Z}^+$ then a is congruent to b modulo m if $m \mid (a-b)$. We use the notation $a \equiv b \pmod{m}$.

We say $a \equiv b \bmod m$ is a congruence, m is the modulus.

If a is not congruent to b then we write $a \not\equiv b \bmod m$.

The congruence idea is saying a & b have the same remainder after division by m. hence $m \mid (a-b)$ a, b have same remainder so difference is a multiple of m,

Ex: $20 \equiv 500 \bmod 24$ $\qquad 13 \equiv 5 \bmod 8$

Its worth noting! $500 \bmod 24 = 20$ & $20 \equiv 500 \bmod 24$

are different statements. $\nearrow$ is a function $\rightarrow$ is a relationship between integers

Theorem: Let $a, b \in \mathbb{Z}$ $m \in \mathbb{Z}^+$ $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.

Ex: Does $17 \equiv 5 \bmod 6$? $24 \equiv 14 \bmod 6$?

$$\begin{array}{r} 17 \\ -5 \\ \hline 12 \end{array} = 2 \cdot 6 \text{ so}$$

$17 \equiv 5 \bmod 6$ ✓

$$\begin{array}{r} 24 \\ -14 \\ \hline 10 \end{array} \neq a \cdot 6 \quad a \in \mathbb{Z} \text{ so}$$

$24 \not\equiv 14 \bmod 6$.

Theorem Let $m \in \mathbb{Z}^+$. a, b are congruent mod m if and only if

$\exists k \in \mathbb{Z}$ s.t. $a = b + km$.

pf: $(\Rightarrow)$ $a \equiv b \bmod m \Rightarrow m \mid (a-b) \Rightarrow \exists k \in \mathbb{Z}$ $a - b = k \cdot m$ so $a = b + km$.

$(\Leftarrow)$ If $\exists k$ s.t. $a = b + km \Rightarrow km = a - b \Rightarrow m \mid (a-b) \Rightarrow a \equiv b \bmod m$. $\square$

We can also do arithmetic:

Theorem: Let $m \in \mathbb{Z}^+$ $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \bmod m$ & $c \equiv d \bmod m$ then

$a + c \equiv b + d \bmod m$ & $ac \equiv bd \bmod m$.

prove this yourself!

Ex: $7 \equiv 2 \bmod 5$ & $11 \equiv 1 \bmod 5$

$18 = 7+11 \equiv 2+1 = 3 \bmod 5$

Corollary: $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$

$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

For simplicity we have conventions for modular arithmetic.

$\mathbb{Z}_m$ or $\mathbb{Z}/m\mathbb{Z}$ – the set of non negative integers less than m.

$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$

Books defines $+_m$ & $\cdot_m$ $\quad a +_m b = a+b \bmod m$

$a \cdot_m b = ab \bmod m$

No one does that. It is understood $a+b$ in $\mathbb{Z}_m$ is modulo m.

Ex: Find $7+9$ & $7 \cdot 9$ mod 11.

$7+9 = 16 \equiv 5 \bmod 11$

$7 \cdot 9 = 63 \equiv 8 \bmod 11$

$+$ & $\cdot$ satisfy all nice properties: $a, b \in \mathbb{Z}_m \Rightarrow a+b$ & $a \cdot b \in \mathbb{Z}_m$

$(a+b)+c = a+(b+c)$ & $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$a+b = b+a$ $\quad a \cdot b = b \cdot a$ $\quad 1, 0 \in \mathbb{Z}_m$ meaning $1 \cdot a = a$ $\quad 0+a = a$

If $a \in \mathbb{Z}_m$ $\; -a \in \mathbb{Z}_m$ $(-a = m-a)$ so that $a + -a = a + m - a$

$\equiv 0 \bmod m$

$c(a+b) = ca + cb$

These properties are very strong. They give that $\mathbb{Z}_m$ is a ring

this is a mathematical structure used heavily in fun stuff like crypto.

Ex: Suppose $a, b \in \mathbb{Z}$ & $a \equiv 11 \mod 19$ $\quad b \equiv 3 \mod 19$

find $c \in \mathbb{Z}_{19}$ s.t.

a. $c \equiv 13 \cdot a \mod 19 \quad = 13 \cdot 11 = 143 \equiv 10 \mod 19$

b. $c \equiv 8b \mod 19 \quad = 8 \cdot 3 = 24 \equiv 5 \mod 19$

c. $c \equiv a - b \mod 19 \quad = 11 - 3 \equiv 8 \mod 19$

d. $c = 7a + 3b \mod 19 \quad = 7 \cdot 11 + 3 \cdot 3 = 77 + 9 = 86 \equiv 10 \mod 19.$

Ex: Show, if $a, b, c, n, m \in \mathbb{Z}$ $\quad n, m > 1$. If $n \mid m$ & $a \equiv b \mod m$ then

$a \equiv b \mod n$.

pf: $n \mid m \Rightarrow m = n \cdot k$ some $k \in \mathbb{Z}$ $\quad a \equiv b \mod m \Rightarrow m \mid (a-b)$

$\Rightarrow (a-b) = m \cdot p$ some $p \in \mathbb{Z} \Rightarrow a - b = n \cdot k \cdot p \Rightarrow n \mid (a-b)$

$\Rightarrow a \equiv b \mod n.$

Ex: Find counter examples to:

(i) If $ac \equiv bc \mod m$, $a, b, c, m \in \mathbb{Z}$ $m \geq 2$ then $a \equiv b \mod m$.

choose $a = 5$ $b = 1$ $\mod 6$ $\quad c = 3$

$a \cdot c = 15 \quad b \cdot c = 3$

$15 \mod 6 \equiv 3 \quad$ but $5 \not\equiv 1$.