Mathematics for Computer Science

MIT 6.042J/18.062J

Congruences: arithmetic (mod n)

Congruence mod n

Def: $a \equiv b \pmod{n}$ iff $n|(a-b)$

example: $30 \equiv 12 \pmod{9}$

since

9 divides (30 − 12)

Congruence mod n

example:

$66666663 \equiv 788253 \pmod{10}$

WHY?

```
  66666663
-   788253
----------
  xxxxxxx0
```


Remainder Lemma

$a \equiv b \pmod{n}$

iff

$\text{rem}(a,n) = \text{rem}(b,n)$

example: $30 \equiv 12 \pmod{9}$

since

$\text{rem}(30,9) = 3 = \text{rem}(12,9)$

Remainder Lemma

$a \equiv b \pmod{n}$

iff

$\text{rem}(a,n) = \text{rem}(b,n)$

abbreviate: $r_{b,n}$

proof: ($\Longleftarrow$)

$a = q_a n + r_{a,n}$

$b = q_b n + r_{b,n}$

if rem's are =, then

$a-b=(q_a-q_b)n$ so $n|(a-b)$

proof: ($\Longrightarrow$)

$a = q_a n + r_{a,n}$

$b = q_b n + r_{b,n}$

conversely,

$n|(a-b)$ means

proof: (only if)

$|--| < n$

$n|((q_a-q_b)n + (r_{a,n}-r_{b,n}))$

$n|$ so $n|$

IMPLIES $r_{a,n} = r_{b,n}$

Remainder Lemma

$a \equiv b \pmod{n}$

iff

$\text{rem}(a,n) = \text{rem}(b,n)$

QED

Corollaries

symmetric

$a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

transitive

$a \equiv b$ & $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

Remainder arithmetic

Corollary:

$a \equiv \text{rem}\ a,n \pmod{n}$

pf: $0 \leq r_{a,n} < n$, so

$r_{a,n} = \text{rem}(r_{a,n},n)$

Congruence mod n

If $a \equiv b \pmod{n}$, then

$a+c \equiv b+c \pmod{n}$

pf: $n \mid (a-b)$ implies

$n \mid ((a+c)-(b+c))$

Congruence mod n

If $a \equiv b \pmod{n}$, then

$a \cdot c \equiv b \cdot c \pmod{n}$

pf: $n \mid (a - b)$ implies

$n \mid (a - b) \cdot c$, and so

$n \mid ((a \cdot c) - (b \cdot c))$

Congruence mod n

Corollary:

If $a \equiv b \pmod{n}$ &

$c \equiv d \pmod{n}$,

then $a \cdot c \equiv b \cdot d \pmod{n}$

Congruence mod n

Cor: If $a \equiv a' \pmod{n}$, then replacing a by a' in any arithmetic formula gives an

$\equiv \pmod{n}$ formula

Congruence mod n

So arithmetic (mod n) a lot like ordinary arithmetic

Remainder arithmetic

important: congruence &

$a \equiv \text{rem}(a,n) \pmod{n}$

keeps (mod n) arithmetic in the remainder range

[0,n)

Remainder arithmetic

example: $287^9 \equiv ? \pmod{4}$

$287^9 \equiv 3^9$ since $r_{287,4} = 3$

$= ((3^2)^2)^2 \cdot 3$

$\equiv (1^2)^2 \cdot 3$ since $r_{9,4} = 1$

$= 3 \pmod{4}$