



Mathematics for Computer Science
MIT 6.042J/18.062J

Congruences: arithmetic (mod n)




Albert R Meyer, March 9, 2015 congruence.1




Congruence mod n

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

example: $30 \equiv 12 \pmod{9}$
since
9 divides $(30 - 12)$




Albert R Meyer, March 9, 2015 congruence.2




Congruence mod n

example:
 $66666663 \equiv 788253 \pmod{10}$

WHY?

$$\begin{array}{r} 6666666\boxed{3} \\ - 788253 \\ \hline \text{XXXXXXXX}0 \end{array}$$



Albert R Meyer, March 9, 2015 congruence.3




Remainder Lemma

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

example: $30 \equiv 12 \pmod{9}$
since
 $\text{rem}(30, 9) = 3 = \text{rem}(12, 9)$



Albert R Meyer, March 9, 2015 congruence.4




Remainder Lemma

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


iff

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

abbreviate: $r_{b,n}$



Albert R Meyer, March 9, 2015 congruence.5




proof: (\Leftarrow)


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

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

if rem's are =, then

$$a - b = (q_a - q_b)n \text{ so } n \mid (a - b)$$


Albert R Meyer, March 9, 2015 congruence.6




proof: (\Rightarrow)

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


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

conversely,

$n \mid (a - b)$ means



Albert R Meyer, March 9, 2015 congruence.9




proof: (only if)

$$|r_{a,n} - r_{b,n}| < n$$


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

$n \mid$ so $n \mid$

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



Albert R Meyer, March 9, 2015 congruence.10



Remainder Lemma


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

iff

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

QED

CC BY SA Albert R Meyer, March 9, 2015 congruence.11



Corollaries


symmetric

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

transitive

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

CC BY SA Albert R Meyer, March 9, 2015 congruence.12



Remainder arithmetic


Corollary:

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

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

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

CC BY SA Albert R Meyer, March 9, 2015 congruence.13



Congruence mod n


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

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

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

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

CC BY SA Albert R Meyer, March 9, 2015 congruence.14




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

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

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


Albert R Meyer, March 9, 2015 congruence.16




Congruence mod n

Corollary:


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

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

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



Albert R Meyer, March 9, 2015 congruence.17




Congruence mod n

Cor: If $a \equiv a' \pmod{n}$,


then replacing a by a'

in any arithmetic

formula gives an

$$\equiv \pmod{n} \text{ formula}$$


Albert R Meyer, March 9, 2015 congruence.18




Congruence mod n


So arithmetic (\pmod{n})

a lot like ordinary


arithmetic




Albert R Meyer, March 9, 2015 congruence.19




Remainder arithmetic
 important: congruence &
 $a \equiv \text{rem}(a,n) \pmod{n}$
 keeps $(\text{mod } n)$ arithmetic
 in the remainder range
 $[0,n)$



Albert R Meyer, March 9, 2015 congruence.20



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 $r_{9,4} = 1$
 $= 3 \pmod{4}$



Albert R Meyer, March 9, 2015 congruence.21

MIT OpenCourseWare
<http://ocw.mit.edu>

6.042J / 18.062J Mathematics for Computer Science
Spring 2015

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.