Mathematics for Computer Science

MIT 6.042J/18.062J

Congruences: arithmetic (mod n)

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

Congruence mod n

example:

$66666663 \equiv 788253 \pmod{10}$

WHY?

$$\begin{array}{r} 66666663 \\ -\quad 788253 \\ \hline \text{xxxxxxx}0 \end{array}$$

Remainder Lemma

$a \equiv b \pmod{n}$

iff

rem(a,n) = rem(b,n)

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

since

rem(30,9) = 3 = rem(12,9)

Remainder Lemma

$a \equiv b \pmod{n}$

iff

rem(a,n) = rem(b,n)

abbreviate: $r_{b,n}$

proof: (if)

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

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

if rem's are =, then

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

(only if) proof similar

Remainder Lemma

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

QED

Remainder arithmetic

Corollary:

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

pf: $0 \leq r_{a,n} < n$, so
$rem(r_{a,n},n) = r_{a,n}$

More Corollaries

- *symmetric*
  $a \equiv b \pmod{n}$ implies
  $b \equiv a \pmod{n}$
- *transitive*
  $a \equiv b$ & $b \equiv c \pmod{n}$
  implies $a \equiv c \pmod{n}$

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

Corollary:

If $a \equiv b \pmod{n}$ &
$c \equiv d \pmod{n}$,
then $a+c \equiv b+d \pmod{n}$

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

Cor: if $a \equiv a'$ (mod n), then replacing a by a′ in any arithmetic formula gives an $\equiv$ (mod n) formula

Remainder arithmetic

important: congruence &

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

keeps (mod n) arithmetic in the remainder range

0 to n-1

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 $r_{9,4} = 1$

$= 3 \pmod{4}$

Congruence mod n

So arithmetic (mod n) a lot like ordinary arithmetic

the main difference:

$8 \cdot \not{2} \equiv 3 \cdot \not{2} \pmod{10}$

$8 \not\equiv 3 \pmod{10}$

no arbitrary cancellation

cancellation (mod n)

When can you cancel k?

--when k has no common factors with n

inverses (mod n)

If gcd(k,n)=1, then have k′

$k \cdot k' \equiv 1 \pmod{n}$.

k′ is an *inverse* mod n of k

pf: sk + tn = 1, so

just let k′ ::= s

cancellation (mod n)

If $a \cdot k \equiv b \cdot k \pmod{n}$
and $\gcd(k,n) = 1$, then
multiply by k':

$(a \cdot k) \cdot k' \equiv (b \cdot k) \cdot k' \pmod{n}$

$a \cdot 1 \equiv b \cdot 1$

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

cancellation (mod n)

summary:

k is *cancellable* (mod n) iff
k has an *inverse* (mod n) iff
k is *relatively prime* to n

arithmetic mod a prime

If p is prime & k not a multiple of p, can cancel k. So

$1 \cdot k, 2 \cdot k, \ldots, (p-1) \cdot k$

are all different (mod p).

So their remainders on division by p are all different.

arithmetic mod a *prime*, p

so if p does not divide k, then multiplying

$1, 2, \ldots, (p-1)$

by k and taking remainders just permutes them.

permuting (mod 7)

·	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4

Fermat's Little Theorem

so ~~$1 \cdot 2 \cdots (p-1)$~~ $= r_{k,p} \cdot r_{2k,p} \cdots r_{(p-1)k,p}$

$\equiv 1k \cdot 2k \cdots (p-1)k \pmod{p}$

$= (k^{p-1})$ ~~$1 \cdot 2 \cdots (p-1)$~~ $\pmod{p}$

now cancel $1 \cdot 2 \cdots (p-1)$:

$$1 \equiv k^{p-1} \pmod{p}$$

inverses (mod prime)

so k^{p-2} is a (mod p) inverse of k

--an alternative to finding inverses with the pulverizer

Remainder arithmetic

$28^{99885} \equiv ?$ (mod 5)

$[r_{28,5} = 3]$

Remainder arithmetic

$3^{99885} \equiv ?$ (mod 5)

$= 3^{4\cdot q+\text{rem}(99885,4)}$

$= (3^4)^q \cdot 3^{\text{rem}(99885,4)}$

Remainder arithmetic

$3^{99885} \equiv ?$ (mod 5)

$= 3^{4\cdot q+\text{rem}(99885,4)}$

$= (3^4)^q \cdot 3^{\text{rem}(99885,4)}$

$\equiv (1)^q \cdot 3^{\text{rem}(99885,4)}$

[Fermat]

Remainder arithmetic

$3^{99885} \equiv 3$ (mod 5)

$= 3^{4\cdot q+\text{rem}(99885,4)}$

$= (3^4)^q \cdot 3^{\text{rem}(99885,4)}$

$\equiv (1)^q \cdot 3^{\text{rem}(99885,4)}$

$\equiv 3^{\text{rem}(99885,4)} = 3^1$

Team Problems

Problems 1—3

6.042J / 18.062J Mathematics for Computer Science
Spring 2010