Mathematics for Computer Science

MIT 6.042J/18.062J

Prime Factorization Congruences

Prime Divisibility

Lemma: If p is prime, and

$$p \mid a \cdot b,$$

then $p \mid a$ or $p \mid b$.

pf: in earlier lecture. follows from

$$\gcd(p,a) = xa + yp$$

Prime Divisibility

Cor : If p is prime, and

$$p \mid a_1 \cdot a_2 \cdots a_m$$

then $p \mid a_i$ for some i.

pf: By induction on m.

Unique Prime Factorization

Fundamental Theorem of Arithmetic

Every integer > 1 factors *uniquely* into a weakly increasing sequence of primes.

Unique Prime Factorization

Fundamental Theorem of Arithmetic

Example:

$61394323221 =$

$3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 37 \cdot 37 \cdot 37 \cdot 53$

Unique Prime Factorization

pf: suppose not. choose smallest $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

$$p_1 \le p_2 \le \cdots \le p_k$$

$$q_1 \le q_2 \le \cdots \le q_m$$

can assume $q_1 < p_1$

so $q_1 \neq p_i$ all i

Unique Prime Factorization

pf: $n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$

now $p_1 | n$, so by Cor., $p_1 | q_i$.

so $p_1 = q_i$ with $i > 1$.

so $\underbrace{p_2 \cdots p_k}_{<n} = q_1 \cdot q_2 \cdots q_{i-1} \cdot q_{i+1} \cdots q_m$ and $q_1 \neq p_2$

contradiction!

Unique Prime Factorization

Cor: if $n = p_1 \cdot p_2 \cdots p_k$,
and $m | n$, then

$$m = p_{i_1} \cdot p_{i_2} \cdots p_{i_j}$$

Team Problem

Problem 1

Congruences

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

Lemma: If $a \equiv b \pmod n$, then
$a+c \equiv b+c \pmod n$.

pf: $n | (a - b)$ implies
$n | ((a+c) - (b+c))$

Congruences

Lemma:

If $a \equiv b \pmod n$, then
$a \cdot c \equiv b \cdot c \pmod n$.

Congruences

Lemma:

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

important: keeps (mod n) calculations in the range

0 to n-1

Congruences

Cor : $a \equiv b \pmod n$ iff

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

Cor : $a \equiv a \pmod n$.

If $a \equiv b$ & $b \equiv c \pmod n$,

then $a \equiv c \pmod n$

Congruences

So $\equiv \pmod n$ a lot like $=$.

main diff: can't cancel

$4 \cdot 2 \equiv 1 \cdot 2 \pmod 6$

$4 \not\equiv 1 \pmod 6$

No general cancellation

Relatively prime cancellation

If $\gcd(k,n)=1$, then have k'

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

k' is an *inverse* mod n of k

pf: $sk + tn = 1$.

just let $k' = s$.

Relatively prime cancellation

Cor:

If $i \cdot k \equiv j \cdot k \pmod n$,

and $\gcd(k,n) = 1$,

then $i \equiv j \pmod n$

Fermat's Little Theorem

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

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

are all different (mod p).

So their remainders on division by p are all different (mod p).

Fermat's Little Theorem

This means that

$\text{rem}(k, p), \text{rem}(2k, p), \ldots, \text{rem}((p-1)k, p)$

must be a *permutation* of

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

Fermat's Little Theorem

so $1 \cdot 2 \cdots (p-1) =$

$\text{rem}(k,p) \cdot \text{rem}(2k,p) \cdots \text{rem}((p-1)k,p)$

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

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

so

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

Team Problems

Problems 2–4