COL 202: DISCRETE MATHEMATICAL STRUCTURES

LECTURE 12

NUMBER THEORY IV: CONGRUENCE & EULER'S FUNCTION

JAN 24, 2024 | ROHIT VAISH

LINEAR COMBINATION v/s COMMON DIVISOR

Greatest common divisor

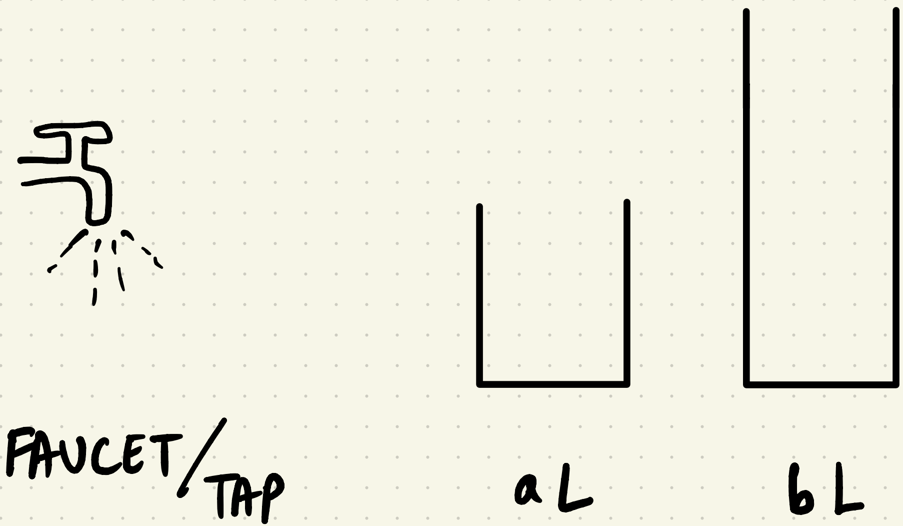
$\gcd(n,m)$ = largest number d such that $d \mid n$ and $d \mid m$.

Smallest positive integer linear combination

$spc(n,m)$ = smallest positive integer d such that $d = s.n + t.m$
s,t integers

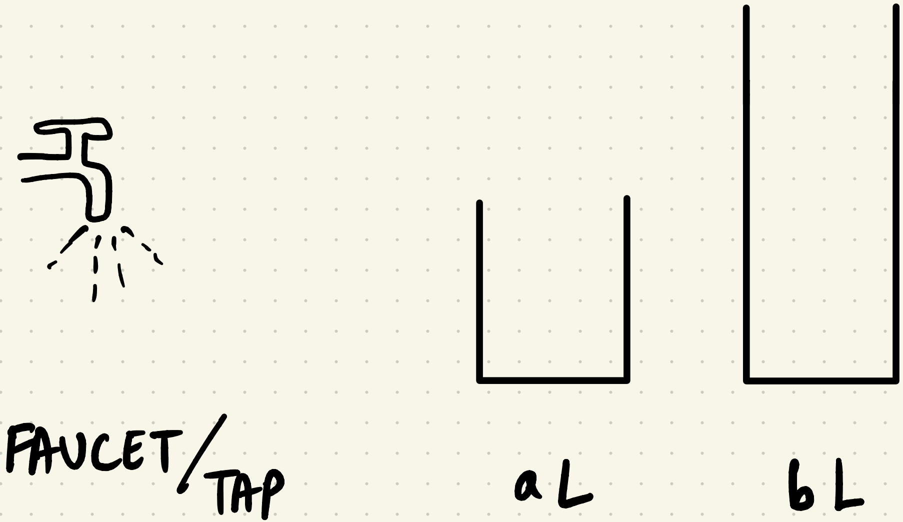
Theorem : $\boxed{\gcd(n,m) = spc(n,m)}$

APPLICATION I : WATER FILLING



GOAL : Fill one of the jugs with exactly c L of water.

APPLICATION I : WATER FILLING



Theorem

Given water jugs of capacity aL and bL, it is possible to have cL in a jug if and only if c is a multiple of $\gcd(a,b)$ s.t. $0 \leq c \leq b$.

APPLICATION II : PRIME FACTORIZATION

Every integer $n \geq 1$ has a unique factorization into primes $p_1, p_2, \cdots, p_k$ (possibly repeating) such that

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k \quad \text{and}$$

$$p_1 \geq p_2 \geq \cdots \geq p_k .$$

aka Fundamental Theorem of Arithmetic

CONGRUENCE

$a \equiv b \pmod{n}$ if and only if $n \mid (a-b)$

CONGRUENCE

$a \equiv b \pmod{n}$ if and only if $n \mid (a-b)$

$a \equiv b \pmod{n}$ if and only if $\text{rem}(a,n) = \text{rem}(b,n)$

(Remainder Lemma)

CONSEQUENCES OF REMAINDER LEMMA

Symmetric $\quad a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$

Transitive $\quad a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

(Yet another) Remainder Lemma $\quad a \equiv \text{rem}(a, n) \pmod{n}$

Congruence Operations

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

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

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

$\cdot$ If ____________________, then $a \cdot c \equiv b \cdot d \pmod{n}$.

CONGRUENCE v/s EQUALITY

Main difference : Cancellation

CONGRUENCE v/s EQUALITY

Main difference : Cancellation

$$16 \equiv 6 \pmod{10}$$

$$8 \cdot \cancel{2} \equiv 3 \cdot \cancel{2} \pmod{10}$$

$$8 \equiv 3 \pmod{10} \quad \times$$

CONGRUENCE v/s EQUALITY

Main difference : Cancellation

$$16 \equiv 6 \pmod{10}$$

$$8 \cdot \cancel{2} \equiv 3 \cdot \cancel{2} \pmod{10}$$

$$8 \equiv 3 \pmod{10} \quad \times$$

When can we cancel k in $ak \equiv bk \pmod{n}$?

CONGRUENCE v/s EQUALITY

Main difference : Cancellation

$$16 \equiv 6 \pmod{10}$$

$$8 \cdot \cancel{2} \equiv 3 \cdot \cancel{2} \pmod{10}$$

$$8 \equiv 3 \pmod{10} \quad \times$$

When can we cancel k in $ak \equiv bk \pmod{n}$? $\gcd(k, n) = 1$

Defn: k and k' are inverses (mod n) if $k \cdot k' \equiv 1 \pmod{n}$.

Defn: k and k' are inverses (mod n) if $k \cdot k' \equiv 1 \pmod{n}$.

Lemma: If $\gcd(k, n) = 1$, then there exists integer k' s.t.

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

Defn: k and k' are inverses (mod n) if $k \cdot k' \equiv 1 \pmod{n}$.

Lemma: If $\gcd(k, n) = 1$, then there exists integer k' s.t.

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

Proof:

Defn: k and k' are inverses (mod n) if $k \cdot k' \equiv 1 \pmod{n}$.

Lemma: If $\gcd(k,n)=1$, then there exists integer k' s.t.

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

Proof: $\gcd(k,n) = s \cdot k + t \cdot n = 1$

Defn: k and k' are inverses (mod n) if $k \cdot k' \equiv 1 \pmod{n}$.

Lemma: If $\gcd(k,n)=1$, then there exists integer k' s.t.

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

Proof:

$$\gcd(k,n) = s \cdot k + t \cdot n = 1$$

$$\Rightarrow \quad sk + tn \equiv 1 \pmod{n}$$

Defn: k and k' are inverses $(\mathrm{mod}\ n)$ if $k \cdot k' \equiv 1 \ (\mathrm{mod}\ n)$.

Lemma: If $\gcd(k, n) = 1$, then there exists integer k' s.t.

$$k \cdot k' \equiv 1 \ (\mathrm{mod}\ n).$$

Proof:

$$\gcd(k, n) = s \cdot k + t \cdot n = 1$$

$$\Rightarrow \quad sk + tn \equiv 1 \ (\mathrm{mod}\ n)$$

$$\Rightarrow \quad sk + t0 \equiv 1 \ (\mathrm{mod}\ n)$$

Defn: k and k' are inverses (mod n) if $k \cdot k' \equiv 1 \pmod{n}$.

Lemma: If $\gcd(k,n)=1$, then there exists integer k' s.t.

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

Proof:

$$\gcd(k,n) = s \cdot k + t \cdot n = 1$$

$$\Rightarrow \quad sk + tn \equiv 1 \pmod{n}$$

$$\Rightarrow \quad sk + t0 \equiv 1 \pmod{n}$$

$$\Rightarrow \quad sk \equiv 1 \pmod{n}$$

Defn: k and k' are inverses (mod n) if $k \cdot k' \equiv 1 \pmod{n}$.

Lemma: If $\gcd(k,n)=1$, then there exists integer k' s.t.

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

Proof:

$$\gcd(k,n) = s \cdot k + t \cdot n = 1$$

$$\Rightarrow \quad sk + tn \equiv 1 \pmod{n}$$

$$\Rightarrow \quad sk + t0 \equiv 1 \pmod{n}$$

$$\Rightarrow \quad sk \equiv 1 \pmod{n}$$

Choose $k' = s$.

$\blacksquare$

CANCELLATION (mod n)

Lemma: If K has an inverce mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \implies a \equiv b \pmod{n}.$$

CANCELLATION (mod n)

Lemma: If k has an inverse mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \implies a \equiv b \pmod{n}.$$

Proof: Let k' be the inverse $\pmod{n}$ of k.

CANCELLATION (mod n)

Lemma: If k has an inverse mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \implies a \equiv b \pmod{n}.$$

Proof: Let k' be the inverse (mod n) of k.

Multiply by k' : $\quad (a \cdot k) \cdot k' \equiv (b \cdot k) \cdot k' \pmod{n}$

CANCELLATION (mod n)

Lemma: If k has an inverse mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \Rightarrow a \equiv b \pmod{n}.$$

Proof: Let k' be the inverse (mod n) of k.

Multiply by k':

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

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

CANCELLATION (mod n)

Lemma: If k has an inverse mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \implies a \equiv b \pmod{n}.$$

Proof: Let k' be the inverse (mod n) of k.

Multiply by k':

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

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

Why?

$$a \cdot 1 \equiv b \cdot 1 \pmod{n}$$

CANCELLATION (mod n)

Lemma: If k has an inverse mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \implies a \equiv b \pmod{n}.$$

Proof: Let k' be the inverse (mod n) of k.

Multiply by k':

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

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

Why?

$$a \cdot 1 \equiv b \cdot 1 \pmod{n}$$

Because $n \mid k \cdot k' \cdot (a-b)$

and $k \cdot k' = q \cdot n + 1$ for some integer q.

CANCELLATION (mod n)

Lemma: If k has an inverse mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \implies a \equiv b \pmod{n}.$$

Proof: Let k' be the inverse (mod n) of k.

Multiply by k':

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

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

$$a \cdot 1 \equiv b \cdot 1 \pmod{n}$$

CANCELLATION (mod n)

Lemma: If k has an inverse mod n, then for any a, b

$$a \cdot k \equiv b \cdot k \pmod{n} \implies a \equiv b \pmod{n}.$$

Proof: Let k' be the inverse (mod n) of k.

Multiply by k' :

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

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

$$a \cdot 1 \equiv b \cdot 1 \pmod{n}$$

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

$\boxed{\text{Ke}}$

CANCELLATION (mod n)

So far,

$\gcd(k, n) = 1 \implies k$ has an inverse (mod n) $\implies k$ is cancellable (mod n)

k and n have no common factor > 1

$\exists k'$ s.t. $k \cdot k' \equiv 1 \pmod{n}$

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

CANCELLATION (mod n)

So far,

$$\gcd(k,n)=1 \Rightarrow k \text{ has an inverse } (\text{mod } n) \Rightarrow k \text{ is cancellable } (\text{mod } n)$$

$$\overset{?}{\Leftarrow} \qquad\qquad\qquad \overset{?}{\Leftarrow}$$

CANCELLATION (mod n)

Theorem: (Exercise)

k is cancellable (mod n) if and only if

k has an inverse (mod n) if and only if

$\gcd(k, n) = 1$ (a.k.a. k and n are relatively prime)

or co-prime

How many numbers have an inverse mod n?

Euler's function

EULER'S FUNCTION

$\phi(n) :=$ No. of integers in $\{0, 1, \ldots, n-1\}$ that are relatively prime to n.

EULER'S FUNCTION

$\phi(n) :=$ No. of integers in $\{0, 1, \ldots, n-1\}$ that are relatively prime to n.

$\mathbb{Z}_n^* := \{k \in \{0, 1, \ldots, n-1\} : \gcd(k, n) = 1\}$

EULER'S FUNCTION

$\phi(n) :=$ No. of integers in $\{0, 1, \ldots, n-1\}$ that are relatively prime to n.

gcd 1 {n}

$$\mathbb{Z}_n^* := \{k \in \{0, 1, \ldots, n-1\} : \gcd(k, n) = 1\}$$

EULER'S FUNCTION

$\phi(n) :=$ No. of integers in $\{0, 1, \dots, n-1\}$ that are relatively prime to n.

gcd1{n}

$\mathbb{Z}_n^* := \{k \in \{0, 1, \dots, n-1\} : \gcd(k, n) = 1\}$

$$\phi(n) = |\mathbb{Z}_n^*| = |\text{gcd1}\{n\}|$$

EULER'S FUNCTION

$\phi(n) :=$ No. of integers in $\{0, 1, \dots, n-1\}$ that are relatively prime to n.

gcd1{n}

$\mathbb{Z}_n^* := \{k \in \{0, 1, \dots, n-1\} : \gcd(k, n) = 1\}$

EULER'S TOTIENT FUNCTION

$$\phi(n) = |\mathbb{Z}_n^*| = |\mathrm{gcd1}\{n\}|$$

EULER'S FUNCTION

$\phi(n) :=$ No. of integers in $\{0, 1, \dots, n-1\}$ that are relatively prime to n.

gcd1{n}

$\mathbb{Z}_n^* := \{k \in \{0, 1, \dots, n-1\} : \gcd(k, n) = 1\}$

$$\phi(n) = |\mathbb{Z}_n^*| = |\mathrm{gcd1}\{n\}|$$

EULER'S TOTIENT FUNCTION

Latin for "that many / so many"

EULER'S FUNCTION

$\gcd 1\{7\} =$

EULER'S FUNCTION

$$\gcd 1\{7\} = \{1, 2, 3, 4, 5, 6\}$$

EULER'S FUNCTION

$$\gcd 1\{7\} = \{1, 2, 3, 4, 5, 6\}$$

$$\gcd 1\{12\} =$$

EULER'S FUNCTION

$$\mathrm{gcd1}\{7\} = \{1, 2, 3, 4, 5, 6\}$$

$$\mathrm{gcd1}\{12\} = \{1, 5, 7, 11\}$$

EULER'S FUNCTION

$$\gcd 1\{7\} = \{1, 2, 3, 4, 5, 6\}$$

$$\gcd 1\{12\} = \{1, 5, 7, 11\}$$

$$\phi(7) = 6$$

$$\phi(12) = 4$$

EULER'S FUNCTION

$$\gcd 1\{7\} = \{1, 2, 3, 4, 5, 6\}$$

$$\gcd 1\{12\} = \{1, 5, 7, 11\}$$

$$\phi(7) = 6$$

$$\phi(12) = 4$$

p is prime $\quad \phi(p) =$

EULER'S FUNCTION

$$\gcd 1\{7\} = \{1, 2, 3, 4, 5, 6\}$$

$$\gcd 1\{12\} = \{1, 5, 7, 11\}$$

$$\phi(7) = 6$$

$$\phi(12) = 4$$

p is prime $\phi(p) = p-1$ because $\gcd 1\{p\} = \{1, 2, --, p-1\}$

EULER'S FUNCTION

$$\gcd 1\{7\} = \{1, 2, 3, 4, 5, 6\}$$

$$\gcd 1\{12\} = \{1, 5, 7, 11\}$$

$$\phi(7) = 6$$

$$\phi(12) = 4$$

Intuitively, $\phi(n)$ is a measure of the "breakability" of n.

p is prime $\quad \phi(p) = p-1 \quad$ because $\gcd 1\{p\} = \{1, 2, --, p-1\}$