COL 202: DISCRETE MATHEMATICAL STRUCTURES

LECTURE 13

NUMBER THEORY V: EULER'S THEOREM

JAN 30, 2024 | ROHIT VAISH

LINEAR COMBINATION V/S COMMON DIVISOR

Greatest common divisor

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

Smallest positive integer linear combination

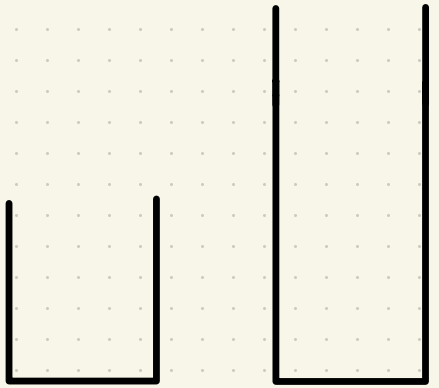
$spc(n,m)$ = smallest positive integer d such that $d = s \cdot n + t \cdot m$

s, t integers

Theorem : $gcd(n,m) = spc(n,m)$

APPLICATION I : WATER FILLING

FAUCET/TAP



aL bL

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

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

$$p_1 \leq p_2 \leq \cdots \leq p_k.$$

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 $n \mid (a-b)$

... resembles equality

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

• 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**

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

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

$$8 \equiv 3 \pmod{10}$$ ✗

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

k and n have no common factors > 1

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

$\forall a, b \; ak \equiv bk \pmod n \implies a \equiv b \pmod n$

$\gcd(k, n) = 1 \iff k$ has an inverse $\pmod n \iff k$ is cancellable $\pmod n$

k and n have no common factors > 1

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

$\forall a, b \; ak \equiv bk \pmod n \Rightarrow a \equiv b \pmod n$

How many numbers have an inverse mod n?

How many numbers have an inverse mod n?

Euler's function

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

How many numbers have an inverse mod n?

Euler's function

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

$gcd1\{n\} :=$ Set of " " " "

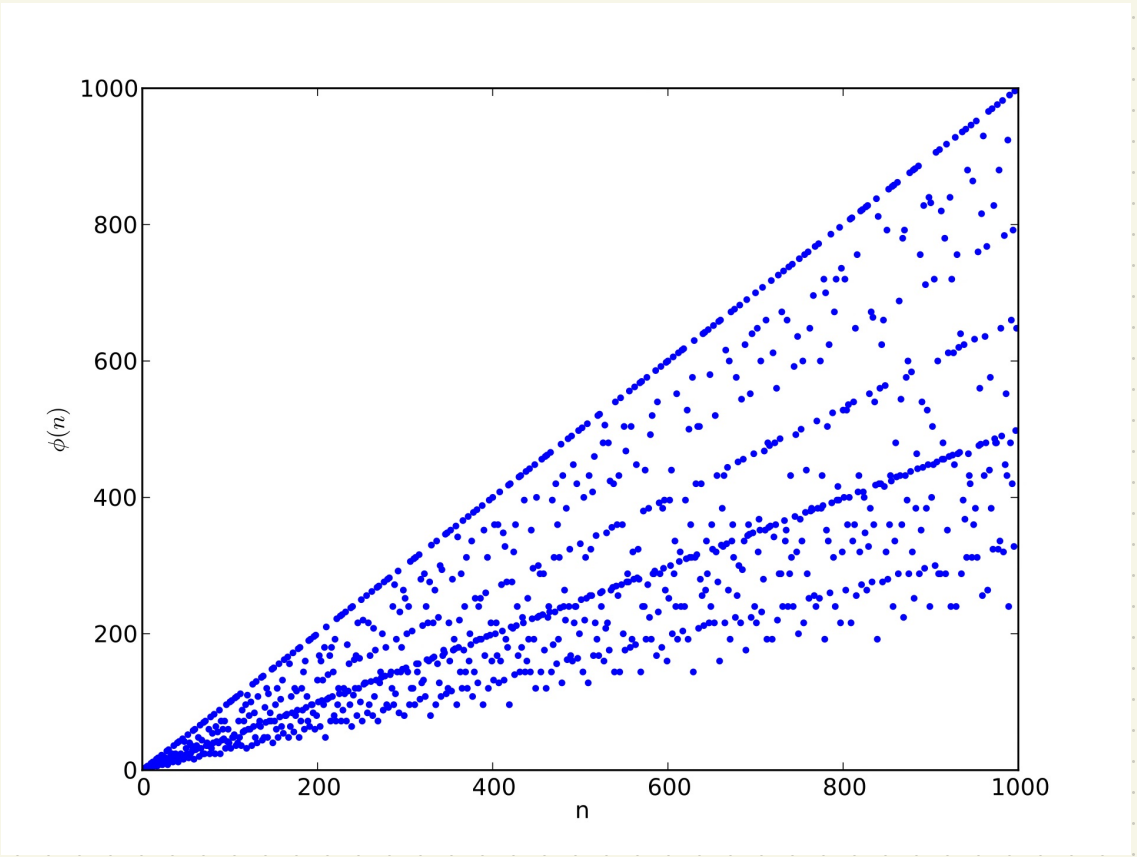
Euler's Function

$$\phi(12) = 4$$

p is prime $\quad \phi(p) = p - 1$

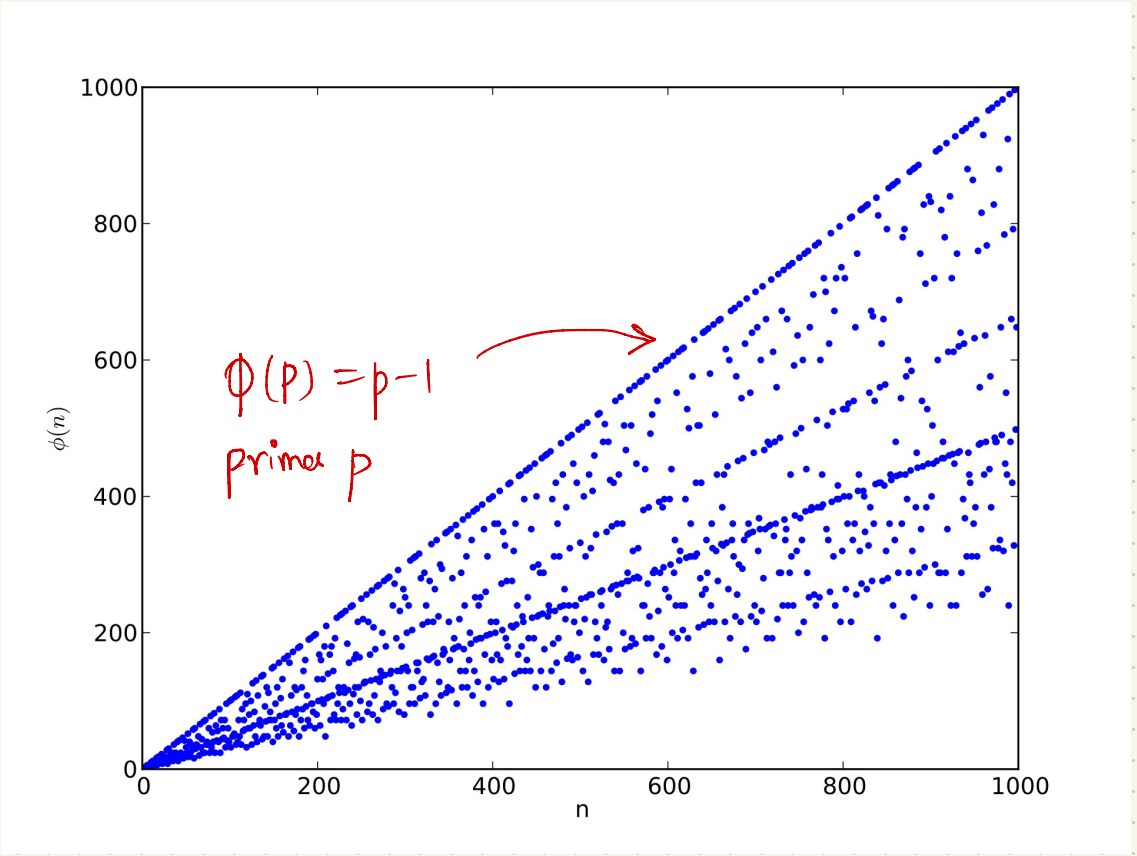
Measure of **breakability** of a number

Euler's function



Source: Wikipedia article on "Euler's Totient Function" (Jan 29, 2023)

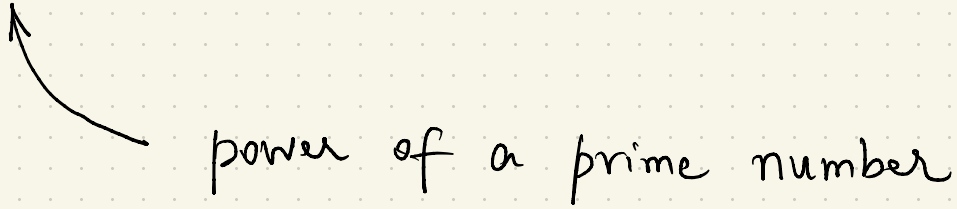
Euler's function



Source: Wikipedia article on "Euler's Totient Function" (Jan 29, 2023)

EULER'S FUNCTION

$\phi(q) =$



EULER'S FUNCTION

$\phi(9) =$

k is relatively prime to 9

if and only if

k is relatively prime to 3

EULER'S FUNCTION

$\phi(9) =$

k is relatively prime to 9
if and only if
k is relatively prime to 3

3 divides every 3rd number ~~0~~ 1 2 ~~3~~ 4 5 ~~6~~ 7 8

EULER'S FUNCTION

$$\phi(9) = 9 - \frac{9}{3} = 6$$

k is relatively prime to 9

if and only if

k is relatively prime to 3

3 divides every 3rd number ~~0~~ 1 2 ~~3~~ 4 5 ~~6~~ 7 8

EULER'S FUNCTION

p is prime, $k \geq 1$

$$\phi(p^k) = p^k - \frac{p^k}{p}$$

$$= p^k - p^{k-1}$$

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof : Any number not relatively prime to pq must be a multiple of p or a multiple of q.

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof : Any number not relatively prime to pq must be a multiple of p or a multiple of q.

In the set $\{0, 1, 2, \ldots, pq-1\}$, there are

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof : Any number not relatively prime to pq must be a multiple of p or a multiple of q.

In the set $\{0, 1, 2, \ldots, pq-1\}$, there are

* q multiples of p,

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof : Any number not relatively prime to pq must be a multiple of p or a multiple of q.

In the set $\{0, 1, 2, \ldots, pq-1\}$, there are

* q multiples of p,
* p multiples of q

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof : Any number not relatively prime to pq must be a multiple of p or a multiple of q.

In the set $\{0, 1, 2, \ldots, pq-1\}$, there are

* q multiples of p,
* p multiples of q
* 1 Common multiple of p and q

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof : Any number not relatively prime to pq must be a multiple of p or a multiple of q.

In the set $\{0, 1, 2, \ldots, pq-1\}$, there are

* q multiples of p,
* p multiples of q
* 1 Common multiple of p and q

p and q are relatively prime →

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof : Any number not relatively prime to pq must be a multiple of p or a multiple of q.

In the set $\{0, 1, 2, \ldots, pq-1\}$, there are

* q multiples of p,
* p multiples of q
* 1 Common multiple of p and q

$p+q-1$ numbers are NOT relatively prime to pq.

p and q are relatively prime →

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof :

$$\phi(pq) = pq - (p + q - 1)$$

EULER'S FUNCTION

Lemma : For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof :

$$\begin{aligned} \phi(pq) &= pq - (p + q - 1) \\ &= (p-1)(q-1) \end{aligned}$$

EULER'S FUNCTION

Lemma: For p, q primes such that $p \neq q$

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$$

Proof:

$$\begin{aligned} \phi(pq) &= pq - (p + q - 1) \\ &= (p-1)(q-1) \\ &= \phi(p) \cdot \phi(q). \end{aligned}$$

EULER'S FUNCTION

Lemma : For a, b relatively prime (Multiplicativity)

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

EULER'S FUNCTION

Lemma : For a, b relatively prime (Multiplicativity)

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

Proof : Exercise.

EULER'S FUNCTION

Lemma: For a, b relatively prime (Multiplicativity)

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

E.g., Recall $\phi(12) = 4$ $\quad$ $\gcd 1\{12\} = \{1, 5, 7, 11\}$

EULER'S FUNCTION

Lemma: For a, b relatively prime (Multiplicativity)

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

E.g., Recall $\phi(12) = 4$ $\quad \gcd 1\{12\} = \{1, 5, 7, 11\}$

Here's another way:

$$\phi(12) = \phi(3) \cdot \phi(2^2) = (3-1) \cdot (2^2 - 2^{2-1})$$
$$= 2 \cdot (4-2)$$
$$= 4$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

E.g., $n = 12$ $\quad \phi(12) = 4$ $\quad \gcd\{12\} = \{1, 5, 7, 11\}$.

$$1^4 \equiv 1 \pmod{12}$$
$$5^4 \equiv 1 \pmod{12}$$
$$7^4 \equiv 1 \pmod{12}$$
$$11^4 \equiv 1 \pmod{12}$$

$$17^4 \equiv 1 \pmod{12}$$

Euler's Theorem

Lemma 1: For k relatively prime to n and any subset $S \subseteq \{0, 1, \ldots, n-1\}$,

$$|kS| = |S|$$

Euler's Theorem

Lemma 1: For k relatively prime to n and any subset $S \subseteq \{0, 1, \dots, n-1\}$,

$$|kS| = |S|$$

$n = 5$ $\quad S = \{0, 2, 3\}$ $\quad |S| = 3$

$k = 2$ $\quad kS = \{0, 4, 1\}$ $\quad |kS| = 3$

$\uparrow$ mod n

Euler's Theorem

Lemma 1: For k relatively prime to n and any subset $S \subseteq \{0, 1, \cdots, n-1\}$,

$$|kS| = |S|$$

Proof: For any $s_1, s_2 \in S$, by cancelability of k,

$$ks_1 \equiv ks_2 \pmod{n} \iff s_1 \equiv s_2 \pmod{n}$$

Euler's Theorem

Lemma 1: For k relatively prime to n and any subset $S \subseteq \{0, 1, \cdots, n-1\}$,

$$|kS| = |S|$$

Proof: For any $s_1, s_2 \in S$, by cancelability of k,

$$ks_1 \equiv ks_2 \pmod{n} \iff s_1 \equiv s_2 \pmod{n}$$

$$\iff s_1 = s_2 \quad (\text{since } 0 \le s_1, s_2 < n)$$

Euler's Theorem

Lemma 1: For k relatively prime to n and any subset $S \subseteq \{0, 1, \cdots, n-1\}$,

$$|kS| = |S|$$

Proof: For any $s_1, s_2 \in S$, by cancelability of k,

$$ks_1 \equiv ks_2 \pmod{n} \iff s_1 \equiv s_2 \pmod{n}$$

$$\iff s_1 = s_2 \quad (\text{since } 0 \le s_1, s_2 < n)$$

Distinct elements in S are mapped to distinct elements in kS.

∎

Euler's Theorem

Lemma 2: For $i, j \in \{0, 1, \cdots, n-1\}$

$i \in gcd1\{n\}$ and $j \in gcd1\{n\} \Rightarrow i \cdot j \pmod n \in gcd1\{n\}$.

Euler's Theorem

Lemma 2: For $i, j \in \{0, 1, \cdots, n-1\}$

$i \in gcd1\{n\}$ and $j \in gcd1\{n\} \Rightarrow i \cdot j \pmod n \in gcd1\{n\}$.

Proof: By prime factorization result,

i and n have no common prime factors

j and n have _____

Euler's Theorem

Lemma 2: For $i, j \in \{0, 1, \cdots, n-1\}$

$i \in \text{gcd1}\{n\}$ and $j \in \text{gcd1}\{n\} \Rightarrow i \cdot j \pmod{n} \in \text{gcd1}\{n\}$.

Proof: By prime factorization result,

i and n have no common prime factors

j and n have ——————

$\Rightarrow$ $i \cdot j$ and n have ——————.

Euler's Theorem

Lemma 2: For $i, j \in \{0, 1, \cdots, n-1\}$

$i \in \text{gcd1}\{n\}$ and $j \in \text{gcd1}\{n\} \Rightarrow i \cdot j \pmod n \in \text{gcd1}\{n\}$.

Proof: By prime factorization result,

i and n have no common prime factors

j and n have ——————

$\Rightarrow$ $i \cdot j$ and n have ——————.

$\Rightarrow$ $i \cdot j \pmod n$ and n have ——————. ∎

Euler's Theorem

Lemma 2: For $i, j \in \{0, 1, \cdots, n-1\}$

$$i \in gcd1\{n\} \text{ and } j \in gcd1\{n\} \Rightarrow i \cdot j \pmod{n} \in gcd1\{n\}.$$

NOT true for $i + j$

$i = 2$

$j = 3$

$n = 5$

Euler's Theorem

Corollary: For any $k \in \text{gcd1}\{n\}$,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Euler's Theorem

Corollary: For any $k \in \text{gcd1}\{n\}$,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Proof: By Lemma 1 $\quad |k \cdot \text{gcd1}\{n\}| = |\text{gcd1}\{n\}|.$

Euler's Theorem

Corollary: For any $k \in \text{gcd1}\{n\}$,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Proof: By Lemma 1 $\quad |k \cdot \text{gcd1}\{n\}| = |\text{gcd1}\{n\}|$.

By Lemma 2, for any $i \in \text{gcd1}\{n\}$, $k \cdot i \in \text{gcd1}\{n\}$.

Euler's Theorem

Corollary: For any $k \in \text{gcd1}\{n\}$,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Proof: By Lemma 1 $\quad |k \cdot \text{gcd1}\{n\}| = |\text{gcd1}\{n\}|.$

By Lemma 2, for any $i \in \text{gcd1}\{n\}$, $k \cdot i \in \text{gcd1}\{n\}$.

$$\Rightarrow \quad k \cdot \text{gcd1}\{n\} \subseteq \text{gcd1}\{n\}.$$

Euler's Theorem

Corollary: For any $k \in \text{gcd1}\{n\}$,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Proof: By Lemma 1 $\quad |k \cdot \text{gcd1}\{n\}| = |\text{gcd1}\{n\}|$.

By Lemma 2, for any $i \in \text{gcd1}\{n\}$, $k \cdot i \in \text{gcd1}\{n\}$.

$$\Rightarrow \quad k \cdot \text{gcd1}\{n\} \subseteq \text{gcd1}\{n\}.$$

Thus, $k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}$. ∎

Euler's Theorem

Corollary: For any $k \in \text{gcd1}\{n\}$,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Eg., $n = 5$ $\quad \text{gcd1}\{n\} = \{1, 2, 3, 4\}$

$k = 3$ $\quad k\text{gcd1}\{n\} = \{3, 1, 4, 2\}$

Euler's Theorem

Corollary: For any $k \in \text{gcd1}\{n\}$,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Eg., $n = 5$ $\quad \text{gcd1}\{n\} = \{1, 2, 3, 4\}$

$k = 3$ $\quad k\text{gcd1}\{n\} = \{3, 1, 4, 2\}$

multiplying by k reorders / permutes the original set of elements.

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof: By Corollary,

$$k \cdot \gcd\{1\{n\}\} = \gcd\{1\{n\}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof: By Corollary,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Consider

$$\prod_{s \in k \cdot \text{gcd1}\{n\}} s$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof: By Corollary,

$$k \cdot \text{gcd1}\{n\} = \text{gcd1}\{n\}.$$

Consider

$$\prod_{s \in k \cdot \text{gcd1}\{n\}} s \equiv \prod_{s \in \text{gcd1}\{n\}} s \pmod{n}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$\prod_{s \in k \cdot \gcd\{n\}} s \equiv \prod_{s \in \gcd\{n\}} s \pmod{n}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$\prod_{s \in k \cdot \gcd\{n\}} s \equiv \prod_{s \in \gcd\{n\}} s \pmod{n}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$\prod_{s \in k \cdot \gcd\{n\}} s \equiv \prod_{s \in \gcd\{n\}} s \pmod{n}$$

$$\Rightarrow \prod_{s \in \gcd\{n\}} ks \equiv \prod_{s \in \gcd\{n\}} s \pmod{n}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$\prod_{s \in k \cdot \text{gcd1}\{n\}} s \equiv \prod_{s \in \text{gcd1}\{n\}} s \pmod{n}$$

$$\Rightarrow \prod_{s \in \text{gcd1}\{n\}} ks \equiv \prod_{s \in \text{gcd1}\{n\}} s \pmod{n}$$

$$\Rightarrow k^{\phi(n)} \cdot \prod_{s \in \text{gcd1}\{n\}} s \equiv \prod_{s \in \text{gcd1}\{n\}} s \pmod{n}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$k^{\phi(n)} \cdot \prod_{s \in \gcd\{1\}\{n\}} s \equiv \prod_{s \in \gcd\{1\}\{n\}} s \pmod{n}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$k^{\phi(n)} \underbrace{\prod_{s \in \text{gcd1}\{n\}} s}_{} \equiv \underbrace{\prod_{s \in \text{gcd1}\{n\}} s}_{} \pmod{n}$$

$$\in \text{gcd1}\{n\} \quad \text{(by Lemma 2)}$$

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$k^{\phi(n)} \cdot \underbrace{\prod_{s \in \gcd 1\{n\}} s}_{s \in \gcd 1\{n\}} \equiv \underbrace{\prod_{s \in \gcd 1\{n\}} s}_{s \in \gcd 1\{n\}} \pmod{n}$$

$\in \gcd 1\{n\} \longrightarrow$ Cancelable

Euler's Theorem

Theorem: For k relatively prime to n,

$$k^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof:

$$k^{\phi(n)} \underbrace{\prod_{s \in \gcd 1\{n\}} s}_{s \in \gcd 1\{n\}} \equiv \underbrace{\prod_{s \in \gcd 1\{n\}} s}_{s \in \gcd 1\{n\}} \pmod{n}$$

$s \in \gcd 1\{n\} \longrightarrow$ Cancelable

$$\Longrightarrow \quad k^{\phi(n)} \equiv 1 \pmod{n}$$