Definition (Prime or Prime Number)

An integer $p>1$ is called a prime number, or simply prime, if its only positive divisors are 1 and p.

Remarks:

- An integer $n>1$ is called called a composite number if n is not a prime. ie. it has a divisor d such that $1<d<n$.
- $n=1$ is a unit number, it's neither prime nor composite.)

Lemma (Composite Number Lemma)

If n is composite, then $\exists$ a prime p such that $p|n$.

Proof: Since n is composite, $\exists\, d \in \mathbb{Z}$ s.t $1<d<n$ and $d|n$. Let $S=\{d \mid 1<d<n \;\&\; d|n\}$.

Clearly, $S \neq \phi$.

WOP $\Rightarrow$ $\exists$ a smallest element in S, say p.

Claim: p is prime.

Suppose not $\Rightarrow \exists\, s \in \mathbb{Z}$ s.t. $1<s<p$ & $s|p$.

Hence $s|n$ and s is smaller than p. $\divideontimes$.

Theorem: (Prime Divisibility Lemma)

If p prime and $p|ab$, then $p|a$ or $p|b$.

Proof:

If $p|a$, we are done. Suppose $p\nmid a$.

Since only positive divisor of p are 1 and p.

$\therefore \gcd(a,p)=1$. (In general, $\gcd(p,a)=1$ or $\gcd(p,a)=p$.)

So by Euclid's Lemma: $p|b$. ∎

Corollary No.1:

If p prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some k where $1 \leq k \leq n$.

Proof: We proceed by induction on n, the number of factors.

For $n=1$. (The result holds trivially)

For $n=2$. The theorem (Prime Divisibility Theorem).

Let $n>2$.

Suppose that the result holds for all numbers less than n.

If $p \mid a_1 a_2 \cdots a_k$, $\forall k<n$, then $p \mid a_i$ for $1 \leq i \leq k$. — $(*)$

$(*)$ is our inductive hypothesis.

Claim: if $p \mid a_1 a_2 \cdots a_{n-1} a_n$, then $p \mid a_j$ for some j, $1 \leq j \leq n$

$p \mid (a_1 a_2 \cdots a_{n-1}) a_n \Rightarrow p \mid a_1 a_2 \cdots a_{n-1}$ or $p \mid a_n$. (our theorem)

If $p \mid a_n$, we are done; if not, then

$p \mid a_1 a_2 \cdots a_{n-1}$ which implies $p \mid a_i$ for $1 \leq i \leq n-1$.

($\because$ of our induction hypothesis.). ∎

Corollary No.2:

If $p, q_1, q_2, \ldots, q_n$ are primes and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.

Proof: By corollary no.1, we know that $p \mid q_k$ for some k, $1 \leq k \leq n$. Being a prime q_k is not divisible by any positive number other than 1 and q_k.

Since, $p>1$, we are forced to conclude $p = q_k$. ∎

Theorem (Fundamental Theorem of Arithmetic): Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order of factors.

Proof: Let $n > 1$. Then, n is either prime or composite.
If n is prime, there is nothing to prove, we are done.
Suppose n is composite.
Then, $\exists$ a prime p_1 s.t. $p_1 | n$ ie. $n = p_1 n_1$, $1 < n_1 < n$.
If now n_1 is prime, we are done; otherwise,
$\exists$ a prime p_2 s.t. $n_1 = p_2 n_2$, $1 < n_2 < n_1$.

$$\therefore n = p_1 p_2 n_2$$

We are getting a decreasing sequence:
$$n > n_1 > n_2 > \cdots > 1.$$
This cannot continue indefinitely, so for some n_k, n_k is itself is prime. ie.
$$n = p_1 p_2 \cdots p_k.$$
We now prove the uniqueness of factorization.
Suppose two factorizations: all p's and q's prime.
$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \text{, where } r \leq s \text{, and}$$
$$p_1 \leq p_2 \leq \cdots \leq p_r \text{ and } q_1 \leq q_2 \leq \cdots \leq q_s.$$
Since, $p_1 | q_1 q_2 \cdots q_s \Rightarrow p_1 = q_k$ for some k.
Hence, $p_1 \geq q_1$. Similarly, $q_1 = p_{\bar{k}}$ for some $\bar{k}$,
$\therefore q_1 \geq p_1$.
Hence $p_1 = q_1$
$$\therefore p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$
Suppose: $r < s$
$\Rightarrow 1 = q_{r+1} q_{r+2} \cdots q_s$. ※. Hence, $r = s$.
Hence, $p_1 = q_1$, $p_2 = q_2$, …, $p_r = q_r$. ∎

Corollary: (A Version of Fundamental Theorem of Arithmetic)

Any positive integer $n > 1$ can be written uniquely in the canonical form:

$$n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$ where for $i = 1, 2, \ldots, r$, and

each k_i is a positive integer and each p_i a prime with

$p_1 < p_2 < \cdots < p_r$.

Proof: Exercise!

Comment: $4725 = 3^3 \times 5^2 \times 7^1$ and $17460 = 2^3 \times 3^2 \times 5^1 \times 7^2$ and
$2093 = 7 \times 13 \times 23$.

Remark: (The Pythagorean Theorem): The number $\sqrt{2}$ is irrational.

Proof:

Suppose $\sqrt{2}$ rational i.e. $\sqrt{2} = a/b$. WLOG: $\gcd(a,b) = 1$.

Squaring $a^2 = 2b^2 \Rightarrow b \mid a^2$.

If $b > 1$, then by the Fundamental Theorem of Arithmetic there exists a prime $p \mid b$. Therefore $p \mid a^2$.

Hence $p \mid a$ ($\because$ Prime Divisibility Lemma)

$\therefore \gcd(a,b) \geq p$. This is a contradiction. ※

$\therefore b = 1$.

But then $a^2 = 2$ which is impossible.

Hence, our supposition is false. ■

→ Euclid's Famous Theorem and Its Proof:

Theorem: (Infinity of Primes)

There are infinitely many primes.

Proof:

Suppose that the theorem is false. ie. there are finitely many primes, say $p_1, p_2, \ldots, p_N$.

Let $N = p_1 p_2 \cdots p_N + 1$.

If N is prime, then $N > p_N$, the largest prime. ※

So, N is composite.

Hence, it must be divisible by some prime, say p.

ie. $p \mid N$, but then p is not in our list. Hence, $p > p_N$.

This is a contradiction.

$\therefore$ there are infinitely many primes. ■

The Famous Prime Number Theorem (PNT):

Let $\pi(x)$ = the number of primes $\le x$, $x \in \mathbb{R}$.

Then, $\displaystyle\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$.

Proof: Beyond the scope of the course.

see. Any advanced book on Analytic Number Theory.

Remark: The first rigorous proof was given in 1896 using the work of B. Riemann by J. Hadamard and de la Vallée Poussin.

CS CamScanner

Definition (Congruence modulo n)
Let n be a fixed positive integer. Two integers a and b are said to be **congruent modulo n**, symbolized by

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

if n divides the difference $a-b$. ie. $a-b=kn$, for some $k \in \mathbb{Z}$.

Remarks:

1) $3 \equiv 24 \pmod{7}$, $5 \equiv 2 \pmod{3}$, $-15 \equiv -64 \pmod{7}$
2) We say a is incongruent to b mod n if $n \nmid (a-b)$, we denote it by $a \not\equiv b \pmod{n}$.
3) Any two integers are congruent mod 1, whereas two integers are congruent mod 2 if both even or both odd.
4) Given an integers a and $n>1$, let q and r be its quotient and remainder upon division by n:
$$a = qn + r \quad , 0 \leq r < n.$$
Then, $a \equiv r \pmod{n}$.
Hence every integer is congruent modulo n to exactly one of the values: $0, 1, 2, \ldots, n-1$.
The set of integers: $0, 1, 2, \ldots, n-1$ is called the set of **least positive residues modulo n**.
5) **Exercise:** Show that congruence mod n is an equivalence relation on the set of integers $\mathbb{Z}$. What are the equivalence classes.
6) **Congruence** may be viewed as a generalization of equality.

CamScanner

Theorem (A):

For any arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the same non-negative remainder when divided by n.

Proof:

"$\Rightarrow$": Suppose $a \equiv b \pmod{n}$, then $a = b + kn$, for some $k \in \mathbb{Z}$.

Upon division by n, b leaves remainder r:

$$b = qn + r \qquad 0 \leq r < n.$$

$$\therefore \quad a = b + kn = qn + r + kn$$
$$= (q+k)n + r.$$

$\therefore$ a leaves the same remainder upon division by n.

"$\Leftarrow$": Conversely, suppose that a and b leave same remainder upon division by n: r.

$$a = q_1 n + r \quad , \; 0 \leq r < n.$$
$$b = q_2 n + r$$

$$\therefore \quad a - b = (q_1 - q_2)n$$
$$\therefore \quad n \mid (a-b)$$

Hence, $a \equiv b \pmod{n}$. ∎

Theorem (B) (Properties of Congruence):

Let $n > 0$ be fixed and $a, b, c, d \in \mathbb{Z}$.
Then the following properties hold:

1) $a \equiv a \pmod{n}$.
2) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
4) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a+c) \equiv (b+d) \pmod{n}$, and $ac \equiv bd \pmod{n}$.
5) If $a \equiv b \pmod{n}$, then $(a+c) \equiv (b+c) \pmod{n}$ and $ac \equiv bc \pmod{n}$.
6) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Proof: **Exercise!**

Ex: Show that 41 divides $2^{20} - 1$.

Ex: Find the remainder obtained upon dividing the sum $1! + 2! + 3! + 4! + \cdots + 99! + 100!$ by 12.

Theorem (C):

If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof: By our assumption: $c(a-b) = ca - cb = kn$, for some $k \in \mathbb{Z}$.

From $d = \gcd(c,n) \Rightarrow$ relatively prime r and s such that $c = rd$, $n = sd$.

$$\therefore \; rd(a-b) = sdk$$
$$\Rightarrow \; r(a-b) = sk$$
$$\Rightarrow \; s \mid r(a-b) \text{ and } \gcd(r,s) = 1.$$
$$\Rightarrow \; s \mid (a-b)$$
$$\Rightarrow \; a \equiv b \pmod{s}$$
$$\Rightarrow \; a \equiv b \pmod{n/d}.$$

Corollary 1: If $ca \equiv cb \pmod{n}$ & $\gcd(c,n) = 1$, then $a \equiv b \pmod{n}$.

Corollary 2: If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is prime, then $a \equiv b \pmod{p}$.

Proof: The condition $p \nmid c$ & prime $\Rightarrow \gcd(c,p) = 1$.

CamScanner

Ex: Show that 41 divides $2^{20}-1$.

Note that $2^5 \equiv -9 \pmod{41} \Rightarrow (2^5)^4 \equiv (-9)^4 \pmod{41}$,
because Theorem B 6: $a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n$.

$$\therefore\ 2^{20} \equiv 81 \cdot 81 \pmod{41} \quad —(*)$$

But $81 \equiv -1 \pmod{41}$.

(+) — $\therefore\ 81 \cdot 81 \equiv (-1)(-1) \pmod{41}$ ($\because$ theorem B 6).

Hence $2^{20} \equiv 1 \pmod{41}$ ($\because$ (*) & (+) & transitivity).

$\therefore\ 2^{20}-1 \equiv 0 \pmod{41}$ ($\because$ theorem B 5: $a \equiv b \pmod n$, then $a+c \equiv b+c \pmod n$).

■

Ex: Find the remainder obtained upon dividing the sum $1!+2!+3!+4!+\cdots+99!+100!$ by 12.

Note that $4! \equiv 24 \equiv 0 \pmod{12}$.

For $k \geqslant 4$: we have

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}.$$

Therefore,

$$1!+2!+3!+4!+\cdots+100! \equiv 1!+2!+3!+0+\cdots+0 \equiv 9 \pmod{12}$$

Hence, $1!+2!+3!+4!+\cdots+100! \equiv 9 \pmod{12}$, i.e. the sum $1!+2!+3!+\cdots+100!$ leave a remainder of 9 when divided by 12.

■

Exercises

Ex: If $a \equiv b \pmod{n}$ & $m|n$, then $a \equiv b \pmod{m}$.

Ex: If $a \equiv b \pmod{n}$ & $c>0$, then $ca \equiv cb \pmod{cn}$.

Ex: If $a \equiv b \pmod{n}$ & a, b, n are all divisible by $d>0$, then
$a/d \equiv b/d \pmod{n/d}$.

Ex: Show that 41 divides $2^{20}-1$.

Ex: Find the remainders of 2^{50} and 41^{65} when divided by 7.

Ex: Find the remainder obtained upon dividing the sum
$1!+2!+3!+4!+\cdots+99!+100!$ by 12.

Ex: What is the remainder when the sum
$1^5+2^5+3^5+\cdots+99^5+100^5$ is divided by 4?

Ex: If $a \equiv b \pmod{n}$ prove that $\gcd(a,n)=\gcd(b,n)$.

Ex: Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

CS CamScanner