ENTRI

NUMBER THEORY

Fundamental Principle of Counting

If an operation can be performed in m ways, following which another operation can be performed in n ways, then, the two operations can be performed together mn ways

GCD of two positive integers

Let $a, b \in \mathbb{N}$, then the greatest common divisor of a and b is denoted by $\gcd(a, b)$ or (a, b)

Note

1. If $(a, b) = 1$, then we say a and b are relatively prime numbers
2. Let $(a, b) = d$, then the equation $ax + by = d,\ x, y \in \mathbb{Z}$ has at least one solution. If (x_1, y_1) is a solution to the equation, then $\left(x_1 + \frac{b}{d}k, y_1 - \frac{a}{d}k\right)$ is also a solution for any $k \in \mathbb{Z}$
3. The least number of the of the set $\{ax + by : x, y \in \mathbb{Z}\}$ is d

Fermat's Number

Let $n \in \mathbb{N} \cup \{0\}$, then Fermat's number is given by $F_n = 2^{2^n} + 1$

1. F_n is odd $\forall n$
2. F_n is not a perfect square for every n
3. For $n \geq 2$, the unit digit of F_n is 7. ie, $F_n \equiv 7\ (mod\ 10)$ for $n \geq 2$
4. For $n \geq 1, F_n + 1$ is divisible by 6
5. For $n \geq 1, F_n = (F_{n-1} - 1)^2 + 1$
6. If $m \neq n, \gcd(F_n, F_m) = 1$
7. If $2^n + 1$ is a prime then n is power of 2

Fundamental Theorem of Arithmetic

Every composite number can be factorized as a product of primes, and this factorization is unique, apart from the order in which the prime factors occur

$$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \dots p_r^{n_r}$$

Where p_i's are distinct primes and $n_i \geq 1\ \forall i$

Euclidean Lemma

Any positive integer is either a prime or a product of primes. Let $n \in \mathbb{N}$, then n can be expressed as

$$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \dots p_r^{n_r}$$

Where p_i's are distinct primes and $n_i \geq 1\ \forall i$

ENTRI

Special functions define on $\mathbb{N}$

Let $n \in \mathbb{N}, n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \dots p_r^{n_r}$

- $d(n)$ is the number of positive divisors of n

$$d(n) = (n_1 + 1)(n_2 + 1) \dots (n_r + 1)$$

$d(n)$ is odd iff n is a perfect square

- $\sigma(n)$ is the sum of divisors of n

$$\sigma(n) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \frac{p_2^{n_2+1} - 1}{p_2 - 1} \dots \frac{p_r^{n_r+1} - 1}{p_r - 1}$$

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \cdots + p_1^{n_1}\right)\left(1 + p_2 + p_2^2 \dots + p_2^{n_2}\right) \dots \left(1 + p_r + p_r^2 + \cdots + p_r^{n_r}\right)$$

Result

- Let $n \in \mathbb{N}$ and p be a prime such that $p < n$, then the exponent of p (number of p's) in $n!$ is

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{m}{p^3}\right] + \cdots$$

- The number of zeros at the end of $n!$ is

$$\left[\frac{n}{5}\right] + \left[\frac{n}{5^2}\right] + \cdots$$

This is also equal to no. of 5's and no. of 10's in $n!$

Euler's Totient Function

$\phi(n)$ is the number of positive integers $\leq n$ and relatively prime to n

$$\phi(n) = p_1^{n_1-1} p_2^{n_2-1} p_3^{n_3-1} \dots p_r^{n_r-1}(p_1 - 1)(p_2 - 1) \dots (p_r - 1)$$

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

Properties

- $\phi(n)$ is even $\forall n > 2$
- $\phi(p) = p - 1$
- $\phi(p^k) = p^k - p^{k-1}$
- $\phi(2^k) = 2^{k-1}$
- $\phi(n^k) = n^{k-1}\phi(n)$
- $\phi(mn) = \phi(m)\phi(n)$ iff $\gcd(m, n) = 1$
- $\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)}$, where $d = \gcd(m, n)$
- If $d_1, d_2, \dots, d_r$ be divisors of n, then $\sum_{i=1}^{r} \phi(d_i) = n$

- For $m, n \in \mathbb{N}$ such that m/n then $\phi(m)/\phi(n)$,
  Converse need not be true

CONGUENCE

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

$$a \equiv b(\text{mod } n)$$

If n divides the difference $a - b$

That is provided that $a - b = kn$ for some integer k

- When n does not divides $a - b$, we say that a is incongruent to b modulo n

Result

Every integer is congruent modulo n to exactly one of the values $0,1,2, \dots, n-1$

In particular, $a \equiv 0(mod\ n)$ if and only if n/a

- The set of n integers $0,1,2, \dots, n-1$ is called the set of least non negative residues modulo n
- A collection of n integers $a_1, a_2, \dots, a_n$ is said to form a complete set of residues modulo n if every integer is congruent modulo n to one and only one of the a_k

Theorem

For arbitrary integer a, b, $a \equiv b(mod\ n)$ if and only if a and b leave same non negative remainder when divided by n

Results

- $a \equiv a(mod\ n)$
- If $a \equiv b(mod\ n)$, then $b \equiv a(mod\ n)$
- If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$
- If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$, then $a + c \equiv b + d(mod\ n)$ and $ac \equiv bd(mod\ n)$
- If $a \equiv b(mod\ n)$, then $a + c \equiv b + c(mod\ n)$ and $ac \equiv bc(mod\ n)$
- If $a \equiv b(mod\ n)$, then $a^k \equiv b^k(mod\ n)$
- If $ca \equiv cb(mod\ n)$, then $a \equiv b\left(mod \frac{n}{d}\right)$, where $d = gcd(c, n)$
- If $ab \equiv 0(mod\ n)$ and $gcd(a, n) = 1$, then $b \equiv 0(mod\ n)$
- If $ab \equiv 0(\boldsymbol{mod\ p})$, prime $\boldsymbol{p}$, then either $\boldsymbol{a \equiv 0(mod\ p)}$ or $\boldsymbol{b \equiv 0(mod\ p)}$
- If $\boldsymbol{ca \equiv cb(mod\ p)}$ and $\boldsymbol{p \nmid c}$, then $\boldsymbol{a \equiv b(mod\ p)}$

ENTRI

Euler's Theorem

Let $\boldsymbol{a, n} \in \mathbb{N}, \boldsymbol{\gcd(a, n) = 1}$ then

$$\boldsymbol{a^{\phi(n)} \equiv 1 \ (mod \ n)}$$

Fermat's Little Theorem

Let $\boldsymbol{a} \in \mathbb{N}$ and $\boldsymbol{p}$ be a prime such that, $\boldsymbol{\gcd(a, p) = 1}$, then

$$\boldsymbol{a^{p-1} \equiv 1 \ (mod \ p)}$$

Fermat's Theorem

Let $\boldsymbol{a} \in \mathbb{N}$ and $\boldsymbol{p}$ be a prime such that, $\boldsymbol{\gcd(a, p) = 1}$, then

$$\boldsymbol{a^{p} \equiv a (mod \ p)}$$

Note

- Primes of the form $2^p - 1$ where p is prime are known as **Mersenne primes**
- If p and q are distinct primes with $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$, then $a^{pq} \equiv a(mod\ pq)$
- Converse of Fermat's theorem does not hold

Pseudo Prime

A composite number n is called pseudo prime whenever $n \mid 2^n - n$.

- If n is an odd pseudo prime, then $M_n = 2^n - 1$ is a larger one
- An absolute pseudo prime is square-free

Wilson's Theorem

Let $\boldsymbol{n} \in \mathbb{N}$ and $\boldsymbol{n}$ be a prime iff $\boldsymbol{(n-1)! = (-1)(mod\ n)}$

Results

- Unit digits of $2^n = \begin{cases} 2, & n = 4k+1 \\ 4, & n = 4k+2 \\ 8, & n = 4k+3 \\ 6, & n = 4k+4 \end{cases}$

  This results can also be used to find the unit digits of $\boldsymbol{4^n}$ and $\boldsymbol{8^n}$

- Unit digits of $3^n = \begin{cases} 3, & n = 4k+1 \\ 9, & n = 4k+2 \\ 7, & n = 4k+3 \\ 1, & n = 4k+4 \end{cases}$

- Unit digits of $7^n = \begin{cases} 7, & n = 4k+1 \\ 9, & n = 4k+2 \\ 3, & n = 4k+3 \\ 1, & n = 4k+4 \end{cases}$

Solution of Linear Congruence

Let $\boldsymbol{a, b, n} \in \mathbb{N}$, then the linear congruence $\boldsymbol{ax \equiv b\ (mod\ n)}$ has solution iff $\boldsymbol{\gcd(a, n)}$ divides $\boldsymbol{b}$

a) If $\boldsymbol{\gcd(a, n) = 1}$, then $\boldsymbol{ax \equiv b\ (mod\ n)}$ has a unique solution, given by

$$\boldsymbol{x \equiv ba^{\phi(n)-1} (mod\ n)}$$

b) If $\boldsymbol{\gcd(a, n) = d > 1}$, then $\boldsymbol{ax \equiv b\ (mod\ n)}$ has $\boldsymbol{d}$ incongruent solutions

Chinese Reminder Theorem

Let $\boldsymbol{n_1, n_2, \ldots, n_r}$ be positive integers such that $\boldsymbol{\gcd(n_i, n_j) = 1}$ for $\boldsymbol{i \neq j}$. Then the system of linear congruence

$$\boldsymbol{x \equiv a_1 (mod\ n_1)}$$

$$\boldsymbol{x \equiv a_2 (mod\ n_2)}$$

$$\vdots$$

$$\boldsymbol{x \equiv a_r (mod\ n_r)}$$

Has a unique solution modulo $\boldsymbol{(n_1 n_2 \ldots n_r)}$

Primitive root modulo

Consider the multiplicative group $\boldsymbol{(Z_p^*, \times_p)}$. An element $\boldsymbol{a \in Z_p^*}$ is said to be a primitive root modulo $\boldsymbol{p}$, if $\boldsymbol{a}$ is a generator of this group or

$\boldsymbol{a^{p-1} \equiv 1 (mod\ p)}$ and $\boldsymbol{a^k \not\equiv 1 (mod\ p), 1 < k < p-1}$

- If $\boldsymbol{a}$ is a primitive root modulo $\boldsymbol{p}$, then other primitive root modulo $\boldsymbol{p}$ are of the form $\boldsymbol{a^k}$, where $\boldsymbol{\gcd(k, p-1) = 1}$

Roots of unity

$\boldsymbol{U_n = \{z \in \mathbb{C}, z^n = 1\}}$ is the set of all root of unity, $\boldsymbol{U_n}$ is a cyclic group under usual multiplication.

Also it is isomorphic to $\boldsymbol{(Z_n, +_n)}$

ENTRI

Primitive n^{th} root of Unity

The generators of $\boldsymbol{U_n}$ are called Primitive n^{th} root of unity

$\alpha = e^{\frac{2\pi i}{n}}$ is a generator of U_n

- Other generators are $\alpha^k, \gcd(k, n) = 1$
- The number of primitive roots of unity is $\phi(n)$

Results

Let $\alpha = e^{\frac{2\pi i}{n}}$

- $1 + \alpha + \alpha^2 + \cdots + \alpha^n = 0$
- $1 \cdot \alpha \cdot \alpha^2 \cdots \alpha^n = (-1)^{n+1}$
- $(1 - \alpha)(1 - \alpha^2) \ldots (1 - \alpha^{n-1}) = n$

- The n^{th} roots of unity lie on the unit circle and they form a regular n-gon

- The number of primitive roots of (-1) = number of primitive $(2n)^{th}$ roots of (1)