NUMBER THEORY

MOBIUS INVERSION FORMULA

For a positive integer n, define μ by rule

$$\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n \mid p^2 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \end{cases}$$

PRIMITIVE ROOT

If $\gcd(a,n)=1$ find a is order of $\phi(n)$ modulo n then a is called primitive root

PYQ 20

Find the primitive Roots of 7

EXPONENT OF PRIME $n!$

If $n>0$ integer and p is prime then exponent of Highest power of p that divides $n!$

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

PYQ 2018

Find $E_{10}(131)$. The exponent of 13 in $100!$

Concept:-

Verify that $1000!$ terminates after 249 zeros

WILSON THEOREM

If p is prime then $(p-1)! \equiv -1 \pmod p$

PYQ 2019

If $\gcd(a,51)=1$ Then prove that $a^{32} \equiv 1 \pmod{51}$

Find the remainder when 15! divided by 17

Find the Remainder of 3^{256} divided by 100.

EULER THEOREM

Let $m>1$ integer and $m \nmid a$ then $a^{\phi(m)} \equiv 1 \pmod m$

FERMAT THEOREM

Let p be prime And $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$

PRIMES

$2, 3, 5, 7, 11, 13, 17, 19, 21, 23, 29, 31, 37, 41, 47, \ldots$

PYQ: 2019

These are infinitely many primes. CHALO PROOF KARO!

Proof: Suppose on contrary that primes are finite.

Let $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$ be primes in ascending order with P_n be last prime.

Consider an +ve integer $P>1$ as given.

$P = P_1 P_2 P_3 \cdots P_n + 1$

So every p divides P exactly

$\Rightarrow P \mid p$ —— (1)

All prime are finite then p must be one of $P_1, P_2, P_3 \cdots P_n$

$\Rightarrow P \mid P_1 P_2 P_3 \cdots P_n$ —— (2)

By (1) and (2) we get

$\Rightarrow P \mid P - P_1 P_2 P_3 \cdots P_n$

$\Rightarrow P \mid P_1 P_2 P_3 \cdots P_n + 1 - P_1 P_2 P_3 \cdots P_n$

$\Rightarrow P \mid 1$

$\Rightarrow P = 1$

Contradiction that P is prime. So Supposition is wrong.

Hence, There are infinitely many primes.

BAAT BAN GYI!

Theorem 4.10. Euler's Totient theorem. a, n are positive integers. Then the following propositions:

(a) a is a primitive root of n.

(b) a is a primitive root of n if and only if a is a primitive root of p^k for every prime factor p of n and a is a primitive root of 2 if n is even and a is a primitive root of 4 if $n = 4$.

(c) a is a primitive root of n if and only if a is a primitive root of n to the power $\phi(n)$ is congruent to 1 modulo n and a to the power $\phi(n)/p$ is not congruent to 1 modulo n for every prime factor p of $\phi(n)$.

(d) a is a primitive root of n if a is a primitive root of n to the power $\phi(n)$ is congruent to 1 modulo n and a to the power $\phi(n)/2$ is congruent to -1 modulo n.

(e) a is a primitive root of n if a is a primitive root of n to the power $\phi(n)$ is congruent to 1 modulo n and a to the power $\phi(n)/q$ is not congruent to 1 modulo n for every prime factor q of $\phi(n)$.

$\phi(n) = 1 \cdot 2 \cdot 2 \cdot 2 = 8$

(a) 1, 3, 5, 7

(b) 1, 3

(c) 1, 3

(d) 5, 7, 3, 3, 3

Q: Write the prime factorization of (a) 1234

Q: Which of the following are primes

(a) 617

(b) 1

(c) 100

(d) 507000

CONCEPT SAMJNA!

Q: find the Remainder when 2^{30} divided by 7

$2 \equiv 2 \pmod 7$

$(2)^2 \equiv 4 \pmod 7$

$2^3 \equiv 8 \equiv 1 \pmod 7$

$2^3 \equiv 1 \pmod 7$

$(2^3)^{10} \equiv (1)^{10} \pmod 7$

$2^{30} \equiv 1 \pmod 7$

$2^{30} \cdot 2^1 \equiv 2^1 \pmod 7$

$2^{100} = \boxed{4} \pmod 7$

Remainder

PYQ:

Q: Find the Remainder when 44444^{44444} divided by 9

$a \equiv a \pmod n$

$44444 \equiv 44444 \pmod 9$

$44444 \equiv 7 \pmod 9$

$(44444)^4 \equiv (7)^4 \pmod 9$ ← 1

$44444^4 \equiv 2401 \pmod 9$

$(44444^4)^{11} \equiv (7)^{11} \pmod 9$

$44444^{44} \equiv 7^4 \cdot 7^4 \cdot 7^3 \pmod 9$

$\equiv 7 \cdot 7 \cdot 7^3 \pmod 9$

$44444^{44} \equiv 7^5 \pmod 9$

$44444^{44} \equiv 7^2 \pmod 9$

$44444^{44} \equiv 49 \pmod 9$

$(44444^{44})^{44} \equiv (4)^{44} \pmod 9$

$44444^{44 \cdot 44} \equiv (4^3)^{32} \cdot 4^2 \pmod 9$

$4 \equiv 4 \pmod 9$

$4^2 \equiv 16 \equiv 7 \pmod 9$

$4^3 \equiv 64 \equiv 1 \pmod 9$

$4^{101} \equiv (4^3)^{33} \cdot 4^2$

$44444^{44444} \equiv (1)^{11} \cdot 4^2 \pmod 9$

$44444^{44444} \equiv 1 \pmod 9$

Remainder

PYQ: 2020

Q: Find the Remainder when $(23)^{18}$ divided by 8

PYQ: 2021

Q: Find the Last two digits of $(2022)^{2023}$

SAWAAL

Solve System of congruence

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

CONGRUENCES

congruent modulo "n"

$a \equiv b \pmod n$ if $n \mid a-b$ OR $a-b = kn$, $k \in \mathbb{Z}$

Properties

Theorem 4.12. Let a, b be integers, n, d be positive integers. Then the following propositions:

(a) $a \equiv b \pmod n$.

(b) $a \equiv b \pmod d$ and $d \mid n$.

(c) $a \equiv b \pmod{\gcd(a,n)}$ and $\gcd(a,n) = \gcd(b,n)$.

(d) $a \equiv b \pmod{\gcd(a-b,n)}$.

(e) $a \equiv b \pmod{\gcd(a,n)}$ and $\gcd(a,n) = \gcd(b,n)$.

(f) $a \equiv b \pmod{\gcd(a-b,n)}$ and $\gcd(a,n) = \gcd(b,n)$.

CHINESE REMAINDER THEOREM

Let $n_1, n_2, \ldots n_k$ be +ve integers such that $\gcd(n_i, n_j) = 1$ then system of linear congruence

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

$\vdots$

$x \equiv a_k \pmod{n_k}$

has simultaneous solution x which is unique.

Divisibility

- $d \mid n$ means there is an integer k such that $n = dk$
- $d \mid n \neq d/n$ (fraction)
- $d \mid n$ — d divides n; d is divisor of n; d is factor of n; n is multiple of d

Division Algorithm

- If a and b are integers and $b>0$ then $\exists$ unique q and r satisfying $a = bq + r$, $0 \le r < b$
- Find q & r $0 \le r < b$
- $a = bq + r$, $0 \le r < b$
- q = quotient
- r = Remainder
- a is divided by b
- $m \mid n \pmod q$
- If $d \mid a$ and $d \mid b$ then $d \mid a-b$

GREATEST COMMON DIVISOR

- Largest number that is divisor of both a and b called gcd of a and b denoted as $\gcd(a,b)$
- $\gcd(a,b) = ?$
- $\gcd(36,48) = ?$
- $12 = 2 \times 2 \times 3$
- $2 \times 2 \times 3 \times 2 \times 2 \times 3$
- $\gcd(a,b) = 1$ — Coprime divisor
- If $\exists$ any n divisor $\gcd(a,b)$
- $\gcd(m \times n, k) = k \cdot \gcd(m,n)$
- If $\gcd(m,n) = 1$ then $\gcd(m \cdot n, k) = \gcd(m,k) \cdot \gcd(n,k)$
- If $\gcd(m,n) = 1$ and $\gcd(m,k) = 1$ then $\gcd(m, nk) = 1$
- If $d \mid a_1 a_2$ and $\gcd(d, a_1) = 1$ then $d \mid a_2$
- $\gcd(0,0) = (|0|+|0|)$

Euclidean Algorithm

- Let $a \ge b > 0$ then apply E-algorithm to GCD of a and b
- $a = q_1 b + r_1$, $0 \le r_1 < b$
- If $r_1 = 0$ then stop. find $\gcd(a,b) = b$
- If $r_1 \ne 0$ then divide b with r_1 to get q_2
- find r_2, $0 \le r_2 < r_1$
- $b = q_2 r_1 + r_2$, $0 \le r_2 < r_1$
- If $r_2 = 0$ then stop. otherwise proceed
- $r_1 = q_3 r_2 + r_3$, $0 \le r_3 < r_2$
- $r_{n-2} = q_n r_{n-1} + r_n$, $0 \le r_n < r_{n-1}$
- $r_{n-1} = q_{n+1} r_n + 0$
- Last non-zero remainder is the gcd (a,b)

Linear Diophantine Eq^n

Linear Diophantine Eq^n $ax + by = c$

Eq solution exists if $a \mid c$ and $b \mid c$

If x_0 and y_0 are any particular solution then other solutions are

$x = x_0 + \left(\frac{b}{d}\right)t$, $t \in \mathbb{Z}$

$y = y_0 - \left(\frac{a}{d}\right)t$

EULER ϕ-Function

- For $n \ge 1$, $\phi(n)$ be number of positive integers not exceeding n that are relatively prime to n.
- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$
- $\phi(5) = 4$
- If n is prime then $\phi(n) = n-1$
- If p is prime and $k > 0$ then $\phi(p^k) = p^k - p^{k-1}$
- $\phi(n)$ is multiplication function.

31

$\phi(31) = 30$

$\phi(41) = 40$

SUM OF DIVISORS

- $\sigma(n)$
- $\sigma(12) = 28$
- $\sigma(n) = n+1$ iff n is prime
- $\sigma(n) = \left(\frac{p^{n+1}-1}{p-1}\right)$ $\left(\frac{p_1^{n_1+1}-1}{p_1-1}\right)$

NUMBER OF DIVISORS

- $\tau(n)$
- $\tau(n) = 2$ iff n is prime
- If $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ then $\tau(n) = (n_1+1)(n_2+1) \cdots (n_k+1)$