Summation 3

20 January 2024 10:39

Q) Compute $\sum_{k\geq 0}\binom{1000}{3k}$

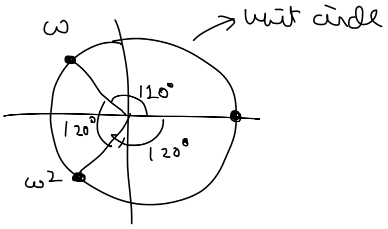
Ans:- $\sum_{k\geq 0}\binom{1000}{3k} = \sum_{k\geq 0}\binom{1000}{k} f(k)$

where $f(k) = \begin{cases} 1 & \text{if } k = 0 \pmod 3 \\ 0 & \text{otherwise} \end{cases}$

$x^3 = 1 \longrightarrow \omega^3 = 1,\ \omega^4 = \omega,\ \omega^5 = \omega^2$

$\searrow 1,\ \omega,\ \omega^2$

$\omega = e^{\frac{2}{3}\pi i}$



$f(k) = \frac{1}{3}(1^k + \omega^k + \omega^{2k})$

$$\sum_{k\geq 0}\binom{1000}{k} f(k) = \frac{1}{3}\sum_{k\geq 0}\binom{1000}{k}(1 + \overset{\omega^{0k}}{\omega^k} + \omega^{2k}) = \frac{1}{3}\sum_{k\geq 0}\left(\binom{1000}{k}\sum_{m=0}^{2}(\omega^{mk})\right)$$

$$= \frac{1}{3}\sum_{k\geq 0}\sum_{m=0}^{2}\binom{1000}{k}(\omega^{mk}) = \frac{1}{3}\sum_{m=0}^{2}\sum_{k\geq 0}\binom{1000}{k}(\omega^{mk})$$

$$= \frac{1}{3}\sum_{k\geq 0}\binom{1000}{k} + \frac{1}{3}\sum_{k\geq 0}\binom{1000}{k}\omega^k + \frac{1}{3}\sum_{k\geq 0}\binom{1000}{k}\omega^{2k}$$

$1 + \omega + \omega^2 = 0$

$1 + \omega = -\omega^2$

$1 + \omega^2 = -\omega$

$\omega + \omega^2 = -1$

$$\Rightarrow \sum_{k\geq 0}\binom{1000}{3k}$$

$$= \sum_{k\geq 0}\binom{1000}{k} f(k) = \frac{1}{3}\left[(1+1)^{1000} + (1+\omega)^{1000} + (1+\omega^2)^{1000}\right]$$

$$= \frac{1}{3}\left[2^{1000} + (-\omega^2)^{1000} + (-\omega)^{1000}\right]$$

$$= \frac{1}{3}\left[2^{1000} + \omega^{2000} + \omega^{1000}\right]$$

$$= \frac{1}{3}\left[2^{1000} - 1\right]$$

Summation modulo prime :-

$k < p$, p is prime $\Rightarrow$ smallest $n \in \mathbb{N}$ such that $kn \equiv 0 \pmod p$ is p

$k < p$, p is prime $\Rightarrow$ smallest $n \in \mathbb{N}$ such that $kn \equiv 0 \pmod p$ is p
$k \in \mathbb{N}$

Let $p = 7$, $k = 3$.
$k = 3$, $2k = 6$, $3k = 2$, $4k = 5$, $5k = 1$, $6k = 4$, $7k = 0$
$\{0, 1, 2, 3, 4, 5, 6\}$ all numbers are visited

Fermat's Little Theorem:-
Let p be a prime, then, $a^{p-1} \equiv 1 \pmod p$ whenever $\gcd(a,p) = 1$

Proof:- A good and rigourous proof can be found using Group Theory.

In (mod p) :- $a^p \equiv ((a-1)+1)^p \equiv (a-1)^p + 1^p = ((a-2)+1)^p + 1^p = (a-2)^p + 1^p + 1^p$

$$\sum_{k=0}^{p} \binom{p}{k} (a-1)^{p-k} 1^k = (a-1)^p + \underbrace{p(a-1)^{p-1} + \frac{p(p-1)}{2}(a-1)^{p-2} + \cdots + p(a-1)}_{\equiv\ 0 \pmod p} + 1^p$$

$\equiv ((a-3)+1)^p + 2 \equiv (a-3)^p + 3 = \cdots \equiv a \pmod p$

$a^p \equiv a \pmod p$
$\Rightarrow a^{p-1} \equiv 1 \pmod p$

Wilson's Theorem :-
For any prime p, $(p-1)! \equiv -1 \pmod p$

Proof:- HomeWork

- Let p be a prime and m be an integer. Then

$$1^m + 2^m + \cdots + (p-1)^m \equiv \begin{cases} 0 \pmod p & \text{if } (p-1) \nmid m \\ -1 \pmod p & \text{if } (p-1) \mid m \end{cases}$$

Solution:- $(p-1) \mid m \Rightarrow m = k(p-1)$

$a^{p-1} \equiv 1 \pmod{p}$ for $\underline{1 \le a \le p-1}$

$a^{2(p-1)} \equiv 1 \pmod{p}$

$\vdots$

$a^{k(p-1)} \equiv 1 \pmod{p}$

$$\Rightarrow 1^m + 2^m + \cdots + (p-1)^m = \underbrace{1+1+\cdots+1}_{p-1 \text{ times}} = p-1 \equiv -1 \pmod{p}$$

Now if $(p-1) \nmid m$, then,

Let g be a primitive root modulo p.

$$x^4 = 1 \to 1, \overset{\overset{i}{\uparrow}}{\omega}, \overset{\overset{-1}{\uparrow}}{\omega^2}, \overset{\overset{-i}{\uparrow}}{\omega^3}$$

ω = primitive root

$\omega^2 \neq$ primitive root

Then,

$$1^m + 2^m + \cdots + (p-1)^m$$

$$= 1 + g^m + \cdots + g^{(p-2)m} = \frac{g^{(p-1)m} - 1}{g^m - 1} \pmod{p}$$

$$g^{(p-1)} \equiv 1 \pmod{p} \Rightarrow g^{(p-1)m} \equiv 1 \pmod{p}$$

$$\Rightarrow \frac{g^{(p-1)m} - 1}{g^m - 1} = \frac{1-1}{g^m - 1} = 0 \to (p-1) \nmid m \Rightarrow g^m - 1 \neq 0$$

so it is valid solution

HomeWork:- Search primitive root and study it

HomeWork:- How many non-empty subsets of $\{1, 2, \ldots, 1000\}$ have sum divisible by 3?

Q> $\gcd(a,b) = 1 \Rightarrow \gcd(a^2, b^2) = 1$

Ans:- $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ $\qquad \gcd(a,b) = 1$

$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$ $\qquad \Rightarrow p_i \neq q_j \ \forall i,j$

$$\Rightarrow a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_n^{2\alpha_n}$$

$2\beta \qquad 2\beta_2 \qquad 2\beta_m$

$$\Rightarrow \quad a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_n^{2\alpha_n}$$

$$b^2 = q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_m^{2\beta_m}$$

Here also $p_i \neq q_j \ \forall \ i, j \Rightarrow \gcd(a^2, b^2) = 1$