

Numbers

$$\mathbb{N} = \{1, 2, 3, \dots\}, \text{ Null}$$

$$\mathbb{W} = \{0, 1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$$

\mathbb{Z}^+

$$2 + _ = 2 \quad \times$$

$$3 - 4 = ? \quad \times$$

$$4 \times _ = 1 \quad \times$$

$x, -x$

Additive inverse : number + (additive inverse) = additive identity
 number + additive identity = number
 (Zero)

Multiplicative identity : number \times MI = number

$$\mathbb{Q} = \left\{ \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0 \right\} \rightarrow x^2 - 2 = 0 \quad ?$$

$$\mathbb{R}, \mathbb{Q}^c = \left\{ \text{numbers not in the form of } \frac{p}{q} \right\} \rightarrow \pi, e?$$

Terminating = $\frac{p}{2^m 5^n}$ format $m, n \in \mathbb{Z}^+$

Transcendental numbers

Real numbers $\rightarrow \mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c \rightarrow x^2 + 2 = 0$

Complex number $\rightarrow \mathbb{C} : \{ a + bi, a, b \in \mathbb{R} \}$

Properties

- (1) Closure \rightarrow Integer closed under addition
- (2) Commutative $\rightarrow x + y = y + x \quad / \quad x \cdot y = y \cdot x$
- (3) Associative $\rightarrow x + (y + z) = (x + y) + z \quad / \quad x(yz) = (xy)z$
- (4) Identity \rightarrow
 - additive } zero
 - multiplicative } one
- (5) Distributive $\rightarrow x(y + z) = xy + xz \quad | \quad (x + y)z = xz + yz$

Properties of divisibility

- (1) $x|y$ and $y|z \Rightarrow x|z$
- (2) $x|y$ and $x|z \Rightarrow x|(my + nz), m, n \in \mathbb{Z}$
- (3) $x|y$ and $y|x \Rightarrow x = \pm y$
- (4) $x|y, x, y > 0, \text{ then } x \leq y$
- (5) $x|y \Rightarrow x|yz, \text{ for any } z \in \mathbb{Z}$
- (6) $x|y$ iff $nx|ny$ for any $n \in \mathbb{Z}, n \neq 0$

Numbers

Division algorithm $\rightarrow a = bq + r, 0 \leq r < b$

HCF / GCD $\rightarrow c|a \& c|b, c \rightarrow$ common divisor

GCD (1) $d|a \& d|b$
 (2) If $c|a \& c|b$, then $c|d$ } $c = \{2, 3, 6\}$
 $d = 6$
 $c|d, c|d$

Properties

(1) If $(b, c) = g$, and d is any common divisor, then $d|g$

(2) For $m > 0, (mb, mc) = m(b, c), m \in \mathbb{Z}$

(3) If $d|b, d|c, d > 0$ then $(\frac{b}{d}, \frac{c}{d}) = \frac{1}{d}(b, c)$

(4) If $(b, c) = g$, then $(\frac{b}{g}, \frac{c}{g}) = 1$

(5) If $(b, c) = g$, then $\exists m, n \in \mathbb{Z}, g = mb + nc$

$(12, 18) = 6, 6 = 12m + 18n, m = 5, n = -3$

(6) If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$

(7) If $(a, bc) = 1$, and $(a, b) = 1$, then $(a, c) = 1$

Prime

(1) $p > 1$

(2) p has no divisors except 1 and itself

(+) Integers = $\{1\} \cup \{\text{Composites}\} \cup \{\text{Primes}\}$

$(4, 9) = 1$ neither 4 nor 9 is prime but $(4, 9)$ is co-prime

$(3, 5), (11, 13), (17, 19), (41, 43), \dots$ (Twin prime conjecture)

Fundamental theorem of arithmetic

$35 = 1 \times 5 \times 7$
 $12 = 1 \times 2^2 \times 3$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, number of divisors

is given by $d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$

$96 \rightarrow 2^5 \times 3^1, d(96) = (5+1)(1+1) = 12$

$200 \rightarrow 2^3 \times 5^2, d(200) = (3+1)(2+1) = 12$

$120 \rightarrow 2^3 \times 3 \times 5, d(120) = 4 \times 2 \times 2 = 16$

Numbers

Properties
of $d(n)$

(1) for square numbers, $d(n) = \text{odd}$

$$9 = 3^2 \quad d(9) = 2+1=3$$

(2) if n is not a perfect square, $d(n) = \text{even}$

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \dots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right) = \text{sum of factors}$$

GIF Greatest Integer function (step function)

$$[8.72] = 8, \quad [7.02] = 7, \quad [x]$$

$$[-2.5] = -3, \quad [-6.87] = -7$$

Fractional part function $\{x\}$ $\{8.72\} = 0.72$

$$x = [x] + \{x\}$$

$$-6.87 = -7 + \{x\}$$

$$\Rightarrow \{x\} = \underline{0.13}$$

GIF

(1) $[x+m] = [x] + m$, if m is an integer

(2) $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$

$$\begin{array}{ccc} [5.6] & [6.5] & [12.1] \\ \downarrow & \downarrow & \downarrow \\ 5 & + & 6 & \neq & 12 \end{array}$$

(3) $[x] + [-x] = 0$

if $x \in \mathbb{Z}$

else, $[x] + [-x] = -1$

(4) $\left[\frac{[x]}{m} \right] = \left[\frac{x}{m} \right]$ if $x \in \mathbb{Z}$

\rightarrow If $a \in \mathbb{R}$ & $c \in \mathbb{N}$, then $\left[\frac{[a]}{c} \right] = \left[\frac{a}{c} \right]$

\rightarrow If $x \in \mathbb{R}$, $\left[\frac{x}{2} \right] + \left[\frac{x+1}{2} \right] = [x]$

Q Find the highest power of 3 contained in $1000!$

$p=3, n=1000$

$$\left[\frac{n}{p} \right] = \left[\frac{1000}{3} \right] = \underline{333}$$

$$\left[\frac{n}{p^2} \right] = \left[\frac{333}{3} \right] = \underline{111}$$

$$\left[\frac{n}{p^3} \right] = \left[\frac{111}{3} \right] = \underline{37}$$

$$\left[\frac{n}{p^4} \right] = \underline{12}$$

$$\left[\frac{n}{p^5} \right] = \underline{4}$$

$$\left[\frac{n}{p^6} \right] = \underline{1}$$

$$\left[\frac{n}{p^7} \right] = \underline{0}$$

498

Numbers

Let a, b be odd integers. If 4 doesn't divide $(a-b)$
show 4 doesn't divide $(a^3 - b^3)$

Suppose $4 \nmid (a-b)$, then

$$\begin{aligned} a^3 - b^3 &= (a-b)(a^2 + ab + b^2) \\ &= (a-b)((a+b)^2 - 3ab) \end{aligned}$$

If a, b are odd, $(a+b)^2$ is even & $3ab$ is odd

$$\therefore (a+b)^2 - 3ab = \text{odd}$$

$$a^3 - b^3 = (\text{not a multiple of } 4) \times (\text{odd number})$$

$\Rightarrow (a^3 - b^3)$ is not divisible by 4

Show that the sum of first n natural numbers ($n \geq 3$)
is never prime.

$$\text{Sum of naturals upto } n = \frac{n(n+1)}{2}$$

This is clearly composite \rightarrow If n is even, $n(n+1)$ is even

If n is odd, $(n+1)$ is even, $n(n+1)$ is even

Modular arithmetic (congruence)

$$a \equiv b \pmod{m} \rightarrow m \text{ divides } (a-b)$$

Properties (1) If $a \equiv b \pmod{m}$, then
 $a+c \equiv b+c \pmod{m}$
 $ac \equiv bc \pmod{m}$ } $c \in \mathbb{Z}$

Converse? (*)

$$\begin{aligned} a &= 10, b = 4, m = 2 \\ c &= 3 \end{aligned}$$

$$\begin{aligned} 10+3 &\equiv 4+3 \pmod{2} \\ \Rightarrow 13 &\equiv 7 \pmod{2} \quad \text{true} \end{aligned}$$

$$10 \times 3 \equiv 4 \times 3 \pmod{2} \Rightarrow 30 \equiv 12 \pmod{2} \quad (\text{true})$$

(2) If $m|a$, then $a \equiv 0 \pmod{m}$

Numbers

(3) If $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$, then

$$a+c \equiv b+d \pmod{m}$$

$$a-c \equiv b-d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

(4) If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$, $k \in \mathbb{Z}^+$

(5) Every integer is congruent to itself $a \equiv a \pmod{m}$

(6) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

(7) If $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

(8) $(a+b)^p \equiv (a^p + b^p) \pmod{p}$, where p is prime

(Fermat's theorem)

$$(9) \quad a^p \equiv a \pmod{p}$$

[Fermat's little theorem]

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

$$(10) \quad (p-1)! + 1 \equiv 0 \pmod{p} \quad [Wilson's theorem]$$

$p > 1$

Converse of Wilson's theorem is true.

Euler's function The number of integers $\leq n$, and
co-prime to n

Result $\phi(p) = p-1$ if p is prime

$$\phi(8) = 4$$

1, 3, 5, 7

co-prime

$$(1, 8) = 1$$

$$\phi(n) = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right) \cdot n$$

Q Find the number of positive integers ≤ 3600 coprime to it

$$3600 = (60)^2 = (2^2 \times 3 \times 5)^2 = 2^4 \times 3^2 \times 5^2$$

$$\phi(3600) = 3600 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right)$$

$$= 3600 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 960$$

Numbers

$$(1) \phi(p^k) = p^k \left(1 - \frac{1}{p}\right) \quad , p \text{ is prime}$$

$$(2) \phi(a)\phi(b) = \phi(ab) \text{ if } a, b \text{ co-prime}$$

(3) For $m > 2$, $\phi(m)$ is even

$\phi(m)$ is odd only for $m=1, 2$

(1) let $n \in \mathbb{N}$. If $(2n+1)$ & $(3n+1)$ are perfect squares then show n is divisible by 40.

(2) If $N = 12^3 \times 3^4 \times 5^2$, find total even factors of N

→ Square difference of odd numbers is divisible by 8

(1) let the odd numbers be $(2m+1), (2n+1), m, n \in \mathbb{Z}^+$

$$\begin{aligned}(2m+1)^2 - (2n+1)^2 &= (2m+1+2n+1)(2m+1-2n-1) \\ &= (2m+2n+2)(2m-2n) \\ &= 4(m+n+1)(m-n)\end{aligned}$$

$m, n \rightarrow$ could be both odd or even / one odd one even

(1) If m, n both odd $\rightarrow ((m-n), 2) > 1$

(2) If m, n both even $\rightarrow ((m-n), 2) > 1$

(3) If one of them is odd $\rightarrow ((m+n+1), 2) > 1$

Anyway, $(2m+1)^2 - (2n+1)^2 = 8k$, for $k \in \mathbb{Z}$

$$\begin{aligned}(2) \quad (2m+1)^2 - (2n+1)^2 &= 4m(m+1) + 1 - 4n(n+1) - 1 \\ &= 4[m(m+1) - n(n+1)]\end{aligned}$$

For any $m \in \mathbb{Z}$, $m(m+1)$ is even

$$\therefore (2m+1)^2 - (2n+1)^2 = 8k, \text{ for } k \in \mathbb{Z}$$

Numbers

Show that $n^2 - 3n - 19$ is not a multiple of 289 for any n

$$\text{let } 17^2 \mid n^2 - 3n - 19$$

$$\begin{aligned} n^2 - 3n - 19 &= n^2 - 3n - 70 + 51 \\ &= (n+7)(n-10) + 51 \end{aligned}$$

$$\text{we know } (n+7) \equiv (n-10) \pmod{17}$$

$$\therefore 17 \mid (n+7)(n-10) \quad \therefore 17 \mid \{(n+7)(n-10) + 51\}$$

$$\begin{aligned} &17^2 \mid (n+7)(n-10) + 51 \quad (\text{from assumption}) \\ \hookrightarrow &17^2 \mid 51 \quad (\text{contradiction}) \end{aligned}$$

Numbers