Numbers

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

$W = \{0, 1, 2, 3, \cdots\}$

$\mathbb{Z} = \{\cdots, -1, 0, 1, \cdots\}$ $\quad \mathbb{Z}^+$

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

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

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

$x, -x$

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

number + additive identity = number
(zero)

Multiplicative identity : number × MI = number

$\mathbb{Q} = \{ p/q,\ p, q \in \mathbb{Z},\ q \neq 0 \}$ $\longrightarrow$ $x^2 - 2 = 0$?

$\mathbb{P}, \mathbb{Q}^c = \{$ numbers not in the form of $p/q \}$ $\longrightarrow$ π, e ?

Transcendental numbers

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

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

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

Properties

(1) Closure $\rightarrow$ Integer closed under addition

(2) Commutative $\rightarrow$ $x + y = y + x$ / $x \cdot y = y \cdot x$

(3) Associative $\longrightarrow$ $x + (y + z) = (x + y) + z$ / $x(yz) = (xy)z$

(4) Identity $\rightarrow$ additive, multiplicative $\}$ zero, one

(5) Distributive $\longrightarrow$ $x(y + z) = xy + xz$ | $(x + y)z = xz + yz$

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) $x | y$, $x, y > 0$, then $x \leq y$

(5) $x | y \Rightarrow x | yz$, for any $z \in \mathbb{Z}$

(6) $x | y$ iff $nx | ny$ for any $n \in \mathbb{Z}, n \neq 0$

Numbers

Division algorithm $\longrightarrow$ $a = bq + r$, $0 \le r < b$

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

GCD
(1) $d|a$ & $d|b$
(2) If $c|a$ & $c|b$, then $c \mid d$

12, 18
$c = \{2, 3, 6\}$
$d = 6$
$c_1|d$, $c_2|d$

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 $\left(\frac{b}{d}, \frac{c}{d}\right) = \frac{1}{d}(b,c)$

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

(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

$\oplus$ Integers $= \{1\} \cup \{\text{Composites}\} \cup \{\text{Primes}\}$

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

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

Fundamental theorem of arithmatic

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

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, number of divisors is given by $d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$

$96 \longrightarrow 2^5 \times 3^1$. $d(96) = (5+1)(1+1) = 12$

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

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

Numbers

Properties of $d(n)$

(1) for square numbers, $d(n)$ = odd

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

(2) if n is not a perfect square, $d(n)$ = even

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

GIF Greatest Integer function (step function) $[x]$

$[8.72] = 8$, $[7.02] = 7$,

$[-2.5] = -3 \qquad [-6.87] = -7$

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

$x = [x] + \{x\} \qquad -6.87 = -7 + \{x\}$

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

GIF

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

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

$\underset{5}{[5.6]} + \underset{6}{[6.5]} \neq \underset{12}{[12.1]}$

(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 $x \in \mathbb{Z}$

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

→ 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 $1000!$

$p = 3$, $n = 1000$

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

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

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

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

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

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

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

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

$$a^3-b^3 = (a-b)(a^2+ab+b^2)$$
$$= (a-b)\left((a+b)^2-3ab\right)$$

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.

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

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

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

Modular arithmatic (congruence)

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

Properties

converse? ⊛

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

$$\left.\begin{aligned} a+c &\equiv b+c \pmod{m} \\ ac &\equiv bc \pmod{m} \end{aligned}\right\} \quad c \in \mathbb{Z}$$

$a = 10, b = 4, m = 2$

$c = 3$

$10+3 \equiv 4+3 \pmod{m}$

$\Rightarrow 13 \equiv 7 \pmod{2}$ true

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

(2) If $m \mid a$, 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) $(a+b)^p = (a^p + b^p) \bmod p$, where p is prime

(Fermat's theorem)

(9) $a^p \equiv a \pmod{p}$ [Fermat's little theorem]

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

(10) $(p-1)! + 1 \equiv 0 \pmod{p}$ [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

$n = 8$

$\phi(8) = 4$

1, 3, 5, 7

co-prime

$(1, 8) = 1$

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

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

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

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

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

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

Numbers

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

(2) $\phi(a)\phi(b) = \phi(ab)$ if a, b 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

$= 2^6 \times 3^7 \times 5^2$

$(6+1)(7+1)(2+1) = \underline{168}$

$(1+1)(2+1) = \underline{24}$

→ square difference of odd numbers is divisible by 8

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

$$(2m+1)^2 - (2n+1)^2 = (2m+1+2n+1)(2m+1-2n-1)$$
$$= (2m+2n+2)(2m-2n)$$
$$= 4(m+n+1)(m-n)$$

$m, n \rightarrow$ 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 $k \in \mathbb{Z}$

2 $$(2m+1)^2 - (2n+1)^2 = 4m(m+1) + 1 - 4n(n+1) - 1$$
$$= 4[m(m+1) - n(n+1)]$$

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

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

Numbers

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

let $17^2 \mid n^2-3n-19$

$$n^2-3n-19 = n^2-3n-70+51$$
$$= (n+7)(n-10)+51$$

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

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

$17^2 \mid (n+7)(n-10)+51$ (from assumption)

$\hookrightarrow\ 17^2 \mid 51$ (Contradiction)

HW!

$2n+1 = x^2,\quad 3n+1 = y^2$ — (1), (2)

x^2 odd $\to$ x odd, let $x = 2a+1$

$2n+1 = (2a+1)^2$

$\Rightarrow 2n+1 = 4a^2+4a+1$

$\Rightarrow n = 2(a^2+a)$

$3n+1 \to$ odd

$y^2 \to$ odd, y odd

(1) − (2) $\to$ $n = y^2-x^2$ $\therefore$ n is divisible by 8

Eliminating n from (1) & (2) : $3x^2-2y^2 = 1$

Squares of odd numbers end with 1, 5 or 9

$3x^2$ ends with $\to$ 3, 5 or 7

$2y^2$ ends with $\to$ 2, 0, or 8

$\Rightarrow$ y^2-x^2 ends with zero

$\Rightarrow$ y^2-x^2 is divisible by 5 $\Rightarrow$ n is divisible by 5

$2d = \frac{z-y}{2}\cdot\frac{z+y}{2}$, d, z, y even

$\Rightarrow 2d = \frac{z^2-y^2}{4}$

$= \frac{\cancel{4}(k_1^2-k_2^2)}{\cancel{4}}$

$z = 2k_1$

$y = 2k_2$

$d = 2a$

$4a = RHS$

$\Rightarrow$ Even $= (k_1+k_2)(k_1-k_2)$

Sets

Null set = ϕ

$A \cup B \rightarrow$ all elements in A, B & common

$A \cap B \rightarrow$ common elements

$A - B \rightarrow$ set difference

All finite sets are countable, but all countable sets are not finite

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

1. $\bar{\bar{A}}$ [or $(A^c)^c$] $= A$, $A \cap A^c = \phi$ and $A \cup A^c = U$ $\longrightarrow$ compliment
2. $A \cup \phi = A$ and $A \cap \phi = \phi$ $\longrightarrow$ null set
3. $A \cup U = U$ and $A \cap U = A$ $\longrightarrow$ universal
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. $\overline{A \cup B} = \bar{A} \cap \bar{B}$
7. $\overline{A \cap B} = \bar{A} \cup \bar{B}$

} De Morgan's Rules

$$R = \{(x,y),\ x \in A,\ y \in B,\ xRy\} \subseteq A \times B$$

Types of relations

(1) Binary $\quad A \neq \{\phi\}$, $A \times A$

(2) Reflexive $\quad xRx \in A$ for $\forall x \in A$

(3) Symmetric $\quad xRy = yRx$, $x \in A, y \in B$

(4) Antisymmetric $\quad xRy$ or yRx $\Rightarrow$ $x = y$ or $y = x$

(5) Transitive $\quad xRy,\ yRz \Rightarrow xRz$

(6) Inverse $\quad xRy,\ yRx$

(7) Equivalence $\rightarrow$ (2), (3), (5)

(8) Partial order relation $\rightarrow$ (2), (4), (5)

HW $\quad x \sim y$, x, y are triangles. Show '$\sim$' is equivalence.

Functions