4.2 Rational Numbers

Definition:- A real number x is a rational number if it can be expressed in the form $\frac{p}{q}$, where $p, q \in \mathbb{Z}$, $q \neq 0$.

A rational number $\frac{p}{q}$ is usually written in its lowest form, i.e. $\gcd(p, q) = 1$.

$\mathbb{Q}$ ← Set of rational numbers.

$-\frac{1}{3} \in \mathbb{Q}$

$\frac{721}{488} \in \mathbb{Q}$

$\pi \notin \mathbb{Q}$

$e \notin \mathbb{Q}$

$\pi = 3.1415926\ldots$

$\pi \approx \frac{22}{7}$

$3.14285\ldots$

$\pi \approx \frac{355}{113}$

$= 3.14159292\ldots$

Q Show the sum of two rational numbers is also a rational number.

Proof - Let $m, n \in \mathbb{Q}$

Hence, $m = \frac{p}{q}$ and $n = \frac{r}{s}$ for some $p, q, r, s \in \mathbb{Z}$ $q, s \neq 0$.

$$m+n = \frac{p}{q} + \frac{r}{s} = \frac{ps+rq}{qs}$$

$ps + rq \in \mathbb{Z}$

$qs \in \mathbb{Z}$ $qs \neq 0$ since $q \neq 0$, $s \neq 0$

$\therefore m+n = \frac{ps+rq}{qs} \in \mathbb{Q}$

Theorem:- Every integer is a rational number.

Proof:- Let $x \in \mathbb{Z}$

$$x = \frac{x}{1} \in \mathbb{Q}.$$

---

25 Show that if r is a rational number, then $3r^2 - 2r + 4$ is a rational number.

Proof:- Let $r = \frac{p}{q} \in \mathbb{Q}$. $p, q \in \mathbb{Z}$, $q \neq 0$

$$3r^2 - 2r + 4 = 3\left(\frac{p}{q}\right)^2 - 2\left(\frac{p}{q}\right) + 4$$

$$= \frac{3p^2}{q^2} - \frac{2p}{q} + 4$$

$$= \frac{3p^2 - 2pq + 4q^2}{q^2}$$

$3p^2 - 2pq + 4q^2 \in \mathbb{Z}$

$q^2 \in \mathbb{Z}$

$q^2 \neq 0$ since $q \neq 0$.

$\therefore 3r^2 - 2r + 4 = \frac{3p^2 - 2pq + 4q^2}{q^2} \in \mathbb{Q}$.

$\frac{\pi}{e}, \frac{\pi}{2} \notin \mathbb{Q}$

4.3 Divisibility

Given two integers a and b, what does it mean, when we say "a divides b"?

Definition:- An integer a divides another integer b iff $\exists$ an integer c, such that $\boxed{ac = b}$. We denote this as

$a \mid b$ ← "divides"

$3 \mid 6$

$3 \nmid 7$

Theorem:- For integers a, b, and c. if $a \mid b$, and $b \mid c$, then $a \mid c$.

Proof:- $a \mid b \Rightarrow b = ak$ for some $k \in \mathbb{Z}$

$b \mid c \Rightarrow c = bl$ for some $l \in \mathbb{Z}$

$\Rightarrow c = a(kl)$

$kl \in \mathbb{Z} \Rightarrow a \mid c$

Theorem :- For all integers a and b, if a and b are positive and $a \mid b$, then $a \leq b$.

Proof :- Let $a, b \in \mathbb{Z}$ $a, b > 0$

$a \mid b \Rightarrow b = ak$ for some $k \in \mathbb{Z}$

$\Rightarrow k > 0$ since $a, b > 0$.

$k \geq 1$

$\Rightarrow ak \geq a$

$\Rightarrow b \geq a$

$\Rightarrow a \leq b$.

Theorem :- Any integer $n > 1$ is divisible by a prime number.

Proof :- If n is a prime number then $n \mid n$

If n is composite, then let $a \mid n$.

By previous theorem $a \leq n$.

If a is a prime number then the theorem is true.

If a is composite, then suppose $a_1 \mid a$. Then $a_1 \leq a$ and we continue the process.

$$1 \leq \cdots \leq a_2 \leq a_1 \leq a \leq n$$

Exp - $6 \mid 12$ $\quad$ $5 \mid 15$

$3 \mid 6$

Fundamental Theorem of Algebra.

Any integer $n > 1$ can be uniquely factored into products of powers of prime numbers.

i.e.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, \ldots, p_k$ are prime numbers and $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 0$.

Proof:- By previous theorem, let a prime p_1 divide n. Then $n = p_1 q$ for some $q \in \mathbb{Z}$.

Now let a prime $p_2 \mid q$. Then $q = p_2 r$ for $r \in \mathbb{Z}$

$\therefore n = p_1 p_2 r$

Continuing this process yields the expression of the theorem.

Uniqueness requires substantial work hence we will take it for granted.

Ex:- $20 = 2^2 \cdot 5^1$

$168 = 2^3 \cdot 21$

$= 2^3 \cdot 3^1 \cdot 7^1$

Q There are infinitely many prime numbers.

A Proving by contradiction. (Euler)

On the contrary suppose there are finitely many prime numbers. Let's call them

$p_1, p_2, \dots, p_k$

let $N = (p_1 p_2 \cdots p_k) + 1$ $\quad 2 \cdot 3 \cdot 5 \cdot 7$

$p_i < N$

By the FTA, $\exists$ some prime number $p \mid N$.

Hence $p = p_i$ for some $1 \le i \le k$.

$\Rightarrow p \mid p_1 p_2 \cdots p_k$ $\quad 3 \mid 15$, $3 \mid 6$

$\Rightarrow p \mid (N - p_1 p_2 \cdots p_k)$ $\quad \Rightarrow a \mid b$

$\Rightarrow p \mid 1$ $\quad b = ak \Rightarrow a \mid c$

$c = al$ $\quad a \mid (b - c)$

$b - c = a(k - l)$

$\Rightarrow a \mid (b - c)$

Contradiction since $p \ge 2$

Hence, there are infinitely many prime numbers.

27 For all integers a, b, and c, if $a \mid (b+c)$ then $a \mid b$ or $a \mid c$.

Fake since $2 \mid (5+3)$, however

$2 \nmid 5$ or $2 \nmid 3$.

---

29 For all integers a and b, if $a \mid b$, then $a^2 \mid b^2$.

True Proof:- $a \mid b \Rightarrow b = ak$ for $k \in \mathbb{Z}$

$\Rightarrow b^2 = a^2 k^2$

$\Rightarrow a^2 \mid b^2$ since $k^2 \in \mathbb{Z}$.

4.4 Division into Cases and Quotient-Remainder Theorem.

Theorem (Quotient-Remainder Theorem)

Given any integer n and a positive integer d there exists unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.

$n = 21$, $d = 4$

$21 = 4 \cdot 5 + 1$ (q, r)

$0 \leq 1 < 4$

$21 = 4 \cdot 3 + 9$

$n = -28$, $d = 5$

$-28 = 5 \cdot (-6) + 2$

n = dividend
d = divisor
q = quotient
r = remainder

$$4 \overline{)21} \quad 5 \text{ r } 1 \qquad 4 \overline{)21} \quad 3+2$$

odd integer $= 2k+1$ $\quad k \in \mathbb{Z}$

Even integer $= 2k$ $\quad k \in \mathbb{Z}$

n divided by 5

remainders $= \{0, 1, 2, 3, 4\}$

$$n = \begin{cases} 5k & k \in \mathbb{Z} \\ 5k+1 & k \in \mathbb{Z} \\ 5k+2 & \vdots \\ 5k+3 & \| \\ 5k+4 & \| \end{cases}$$

$6k$	✓ E
$6k+1$	O
$6k+2$	✓ E
$6k+3$	O
$6k+4$	✓ E
$6k+5$	O

n div d = quotient obtained when n is divided by d.

n mod d = remainder obtained when n is divided by d.

15 div $3 = 5$

16 mod $3 = 1$.

38 For any integer n, n^2+5 is not divisible by 4.
Prove the statement.

Proof :- Case 1 $n = 2k+1$ for some $k \in \mathbb{Z}$

$$n^2+5 = (2k+1)^2+5$$
$$= 4k^2+4k+1+5$$
$$= 4k^2+4k+6$$
$$= 4k^2+4k+4+2$$
$$= 4(k^2+k+1)+2$$
$$= 4l+2$$

Hence $4 \nmid (n^2+5)$.

Case 2 $n = 2k$ $k \in \mathbb{Z}$

$$n^2+5 = (2k)^2+5$$
$$= 4k^2+5$$
$$= 4k^2+4+1$$
$$= 4(k^2+1)+1$$
$$= 4l+1$$

Hence $4 \nmid (n^2+5)$

24 Prove that for all integers m and n, if $m \bmod 7 = 5$ and $n \bmod 7 = 6$, then $mn \bmod 7 = 2$.

Proof :-

$m \bmod 7 = 5 \Rightarrow m = 7k + 5$ for $k \in \mathbb{Z}$

$n \bmod 7 = 6 \Rightarrow n = 7l + 6$ for $l \in \mathbb{Z}$.

$$\begin{aligned} mn &= (7k+5)(7l+6) \\ &= 49kl + 42k + 35l + 30 \\ &= 49kl + 42k + 35l + 28 + 2 \\ &= 7(7kl + 6k + 5l + 4) + 2 \\ &= 7r + 2 \qquad r \in \mathbb{Z} \end{aligned}$$

$\Rightarrow mn \bmod 7 = 2$