—x—

0) <u>Division algorithm</u>:

For any $n \in N$ and $q > 0$ $\exists$ unique $m, r \in N$ st

$$n = mq + r \quad \text{with} \quad 0 \le r < q .$$

I) <u>uniqueness</u>: Let there are pairs (m, r) and (m', r') with $0 \le r < q$ & $0 \le r' < q$ st

$$n = mq + r$$
$$n = m'q + r'$$

For contradiction assume $m \ne m'$

(case 1) Let $m > m'$

$\Rightarrow \quad m \ge m' + 1$

$\Rightarrow \quad n = mq + r$

$n \ge (m'+1) q + r$

$= m'q + (q+r)$

$n > m'q + \underbrace{r'}_{}$ $= n .$

relation between $(q+r)$ and r'

① $q + r \ge q$

From uniqueness → ② $q > r'$

$\Big]\ (q+r) > r'$

$\Rightarrow \quad n > n$ [contradiction]

$\Rightarrow \quad m = m'$

For proving integers: ① $n=0$ ② $n>0$ ③ $n<0$.

II) $(m-m')q = (r'-r)$ $\rightarrow$ $\Rightarrow (r'-r)$ is multiple of q $\Big]$ $m-m'=0$

$\rightarrow (r'-r)$ is between $-q$ & q

$-q < (r'-r) < q$ $\quad$ $[\because 0 \le r < q$ and $0 \le r' < q]$

$\Rightarrow m-m' = 0$

$\Rightarrow m = m'$

Generalization:

Let $p \in \mathbb{Z}$ and $q>0$. Then $\exists$ unique $m, r \in \mathbb{Z}$ with

$0 \le r < q$ s.t

$p = mq + r$

$-p = -(mq+r)$

$= -mq - r$ $\quad$ $0 \le r < q \Rightarrow 0 > -r > -q$

Def:

Def:
A sequence $a_0, a_1, \dots$ of $\mathbb{N}$ or $\mathbb{Z}$ or $\mathbb{Q}$ is said to be infinite descent iff $a_0 > a_1 > a_2 \dots\dots\dots$.

Lemma:
For natural numbers, we can't have any sequence that is infinite descent.

Proof:
Suppose that a_n is a sequence of natural numbers s.t.

$$a_n > a_{n+1} \quad \forall\, n \in \mathbb{N}$$
$$\Rightarrow a_n \geq a_{n+1} + 1$$
$$\Rightarrow a_{n+1} \leq a_n - 1$$

From induction $\quad a_n \leq a_0 - n \quad \forall\, n$

If $a_0 < n \Rightarrow a_n < 0$ which can't happen as $a_n \in \mathbb{N}$.
[CONTRADICTION]
↳ we can't have a ~~seqtot~~ sequence of natural numbers in infinite descent.

Proposition: [Interspersing of rationals inside integers]
Let x be a natural number. Then $\exists$ a unique integer $n \in \mathbb{Z}$ st

$$n \leq x < n+1.$$

In particular, $\exists$ a natural number N st.

$$x < N \quad \forall\, x \in \mathbb{Q}$$

Proof: Since $x \in \mathbb{Q}$, we have

$$x = p/q \quad \text{for some } p \in \mathbb{Z} \text{ and } q > 0 \in \mathbb{Z}\ (q \neq 0)$$

↳ $\because p \in \mathbb{Z}$ so we can form both +ve & -ve numbers.

Division Algorithm:

$$p = mq + r \quad \text{for } m, r \in \mathbb{Z} \text{ with } 0 \leq r < q$$

$$x = \frac{p}{q} = \frac{mq}{q} + \frac{r}{q}$$

$0 \leq r < q$

$\Rightarrow 0 \leq r/q < 1$

$$x = m + \frac{r}{q}$$

$$\geq m$$

Also $x < m+1$ $\quad [\because r/q < 1]$

$\Rightarrow \quad m \leq x < m+1$ for some integer m

Uniqueness:

Let us say $\exists \ m' \in \mathbb{Z}$ s.t.

$m' \leq x < m' + 1$

$m \leq x < m+1$

$\Rightarrow x < m'+1$ & $x \geq m$ $\quad$ | $\quad$ $x < m+1$ & $x \geq m'$

$m \leq x < m'+1$ $\quad$ | $\quad$ $m+1 > x \geq m'$

$\Rightarrow (m - m') < 1 \ldots (1)$ $\quad$ | $\quad$ $(m-m') > -1 \ldots (2)$

combine (1) and (2)

$\Rightarrow |m - m'| < 1$

$\Rightarrow m = m'$ $\quad (\because m, m' \in \mathbb{Z})$

- $m+1 > 0$ $\quad$ or ≤ 0

$N = m+1$ $\quad$ $N = 0$

∃ Infinitely many rationals between m and m+1 ($m \in \mathbb{Z}$). Prove it

Lemmas used to prove propositions which are used to prove theorems

Proposition :

For 2 rationals x & y s.t. $x < y$, $\exists$ another rational z s.t.

$x < z < y$.

Proof : choose $z = \frac{x+y}{2}$

is z rational? yes $\rightarrow$ $\left[\frac{\text{Rational}}{\text{Rational}} = \text{Rational}\right]$ $\left[x+y : \text{closure on rational}\right]$

$x < z < y$.

$z = \frac{x+y}{2} < \frac{y+y}{2} = y$

$z = \frac{x+y}{2} > \frac{x+x}{2} = x$.

$\Rightarrow x < z < y$.

This way we can prove there are many rationals in btween rationals.

Lemma :

There is no rational number x s.t. $x^2 = 2$.

Proof :

suppose there exists a rational $x = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ and $q \neq 0$ s.t.

$\left(\frac{p}{q}\right)^2 = 2$

or $p^2 = 2q^2$

we can take $p, q > 0$ " without loss of generality. "

$(p, q \in \mathbb{N} \setminus \{0\})$

$\hookrightarrow p^2 = 2q^2$: -ve number के लिए bhi true है।

Def :-

$p \in N$ is said to be even if $p = 2k$ for some $k \in N$.

$p \in N$ is said to be odd if $p = 2k+1$ for some $k \in N$

claim: Natural numbers can either be even or odd not both.

Proof: Assume no. is both even and odd.

So $p^2 = 2q^2$

$\Rightarrow p^2$ is even $\Rightarrow p$ is even.

↳ Assume $p^2 = odd \Rightarrow p = odd$ [contradiction]

$\because p$ is even $\Rightarrow \exists\ k \in N$ st $p = 2k$

$p^2 = 2q^2$

$4k^2 = 2q^2$

$q^2 = 2k^2$.

Also $p^2 = 2q^2 \Rightarrow p^2 > q^2 \Rightarrow p > q$ (as, $p, q > 0$)

We started with pair (p, q) st $p^2 = 2q^2$ and we got pair (q, k) st $q^2 = 2k^2$.

$(p, q) \rightarrow (p', q') \rightarrow (p'', q'') \longrightarrow \ldots$

st all are solutions of $p^2 = 2q^2$ st $p > p' > p''$.

which means we have constructed a sequence $p > p' > p''$ which is in infinite descent. This is a contradiction

$\Rightarrow \left(\frac{p}{q}\right)^2 \neq 2$ for any $p, q \in Z$ or $x \in Q$

○) Proposition:

For every rational $\varepsilon > 0$ there exists rational $x > 0$ s.t.

$$x^2 < 2 < (x+\varepsilon)^2$$

Proof:

Suppose for contradiction there does not exist $x > 0 \in \mathbb{Q}$ s.t for all $\varepsilon > 0$, $x^2 < 2 < (x+\varepsilon)^2$

This means that if $x^2 < 2$ then $(x+\varepsilon)^2 \leq 2$

We can't have $(x+\varepsilon)^2 = 2$ [as a $(\text{rational})^2 \neq 2$]

$$\Rightarrow (x+\varepsilon)^2 < 2$$

Now if $x = 0$

$$0^2 = 0 < 2 \Rightarrow (0+\varepsilon)^2 < 2 \iff \varepsilon^2 < 2$$

$$\therefore$$

if $x = \varepsilon \Rightarrow (2\varepsilon)^2 < 2$

$$\Downarrow$$

$$(n\varepsilon)^2 < 2 \quad \forall n \in \mathbb{N}$$

But $n\varepsilon$ is a +ve rational number

For each ε we can chose n s.t

$$2 < n\varepsilon$$

choose n s.t. $\cancel{n > \frac{\varepsilon}{2}}$ $n > \frac{2}{\varepsilon}$ $\Rightarrow 4 < (n\varepsilon)^2 < 2$

$\Rightarrow 4 < 2$ (Impossible) $\Rightarrow (x+\varepsilon)^2 > 2$