Wednesday, September 4, 2024   12:29 PM

Direct Proofs

$$p \Rightarrow q$$

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$$

$a, b \in \mathbb{Z}$, $a \pm b \in \mathbb{Z}$ $a \cdot b \in \mathbb{Z}$

↳ "is an element of"

Def: An integer $n \in \mathbb{Z}$ is even if $n = 2.K$, for $K \in \mathbb{Z}$
(odd) $n = 2.K+1$,

Ex: $8 = 2.4$ "even"

$11 = 2.5 + 1$ "odd"

$0 = 2.0$ "even"

$-7 = 2.(-4) + 1$ "odd"

Proposition: The sum of two even integers is even.

Proof: Let $a = 2.p$, $b = 2.q$ two even numbers, then:

$$a + b = 2\cdot p + 2\cdot q$$
$$= 2\underbrace{(p+q)}$$
$$= 2 \cdot K$$

Therefore or Hence

↑

∴ $a+b$ is even.

∎ or q.e.d

Proposition The sum of two odd integers is even.

Let $a = 2p+1$, $b = 2q+1$ then

$$a + b = (2p+1) + (2q+1)$$
$$= 2(p+q) + 2$$

$$= 2[\underbrace{p+q+1}_{K}]$$

$$= 2 \cdot K$$

□

Proposition: If n is odd then n^2 is odd.

Proof: Since n is odd $\exists K \in \mathbb{Z}$ such that

$$n = 2K+1 \qquad (a \pm b)^2 = a^2 \pm 2ab + b^2$$

Then
$$n^2 = (2K+1)^2$$
$$= 4K^2 + 2 \cdot 2K \cdot 1 + 1$$
$$= 2[\underbrace{2K^2+2K}_{P}] + 1$$
$$= 2p + 1$$

$\therefore$ n^2 is odd. □

Proof by cases

Prop: If $n \in \mathbb{Z}$ then n^2+n+6 is even.

Proof: 1) $n = 2 \cdot K$

$$n^2+n+6 = 4K^2+2K+6$$
$$= 2[\underbrace{2K^2+2+3}_{P}]$$
$$= 2p.$$

"even"

2) $n = 2K+1$

$$n^2+n+6 = (2K+1)^2+2K+1+6$$
$$= 4K^2+4K+1+2K+1+6$$
$$= 4K^2+6K+8$$

$= 2\,[\underbrace{2k^2+3k+4}_{p}]$

$= 2\cdot p$

$\therefore\ n^2+n+6$ is always even.

Ex (Proof by cases): $n\in\mathbb{Z} \left< \begin{matrix}\text{even}\\ \text{odd}\end{matrix}\right.$

$f: X\to Y \left< \begin{matrix}\text{continuous}\\ \text{discontinuous}\end{matrix}\right.$

$\sum a_n \left< \begin{matrix}\text{converges}\\ \text{diverges}\end{matrix}\right.$

$X \left< \begin{matrix}\varnothing\\ \text{non-empty}\end{matrix}\right. \left< \begin{matrix}\text{finite}\\ \text{infinite}\end{matrix}\right.$

....

Divisibility

"a divides b"

Def: We say $a \mid b$ if $b = a\cdot k$, $k\in\mathbb{Z}$

"$a \nmid b$" → doesn't divide

Ex: $2 \mid 10$

$7 \mid 14$

$9 \mid 81$

$-2 \mid -4$

$11 \nmid 20$

$a \mid 0 \Rightarrow 0 = 0\cdot a$

$0 \nmid a$ if $a \neq 0$

Proposition (Transitive): Given $a,b,c\in\mathbb{Z}$.
If $a \mid b$ and $b \mid c$ then $\underline{\underline{a \mid c}}$.

Proof: $\underline{\underline{b = a\cdot k}}$, $\underline{\underline{c = b\cdot p}}$

$c = (ak)\cdot p$

$= a\cdot(\underbrace{kp}_{q})$

$= aq$

$\therefore \quad a \mid c.$

Theorem (Euclid's Algorithm): Given $a, b \in \mathbb{Z}$ with $b > a$, then $\exists\, q, r \in \mathbb{Z}$ such that:

$$b = a \cdot q + r \quad , \quad 0 \leq r < a$$

Ex:

$$8 = 2 \cdot \underline{\underline{3}} + \underline{\underline{2}}$$

$$21 = 4.5 + 1$$

$$33 = 2.16 + 1$$

$$\vdots$$

G.C.D

A number "d" is a divisoe of a numbee "n" if $d \mid n$. The greatest common divison (gcd) of two numbers a, b; represented by $\gcd(a,b)$, is the greatest divisoe among all common divisors of "a" and "b".

Ex: $\gcd(32, 50) = 2 = \underline{\underline{K}}\,32 + \ell\,50$

32: 1, 2, 16, 4, 8, 32

50: 1, 2, 5, 10, 25, 50

$$\gcd(-5, 20) = 5 = \overset{=3}{K}(-5) + \overset{=1}{\ell}.20$$

1, 5 | 1, 2, 4, 5, 10, 20

Theorem: Given a, b positive integers, then $\exists\, K, \ell \in \mathbb{Z}$ such that $\gcd(a,b) = Ka + b \cdot \ell$.

Idea: Consider all positive sums $xa + yb$, then

$$d = \min(xa + yb) = \underline{\underline{Ka + \ell b}}$$

$\vdash$ d is gcd.

Modular arithmetic (mod q)

Take $a \in \mathbb{Z}$: $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{q-1}$

$$\bar{a} = \{a + k \cdot q \mid k \in \mathbb{Z}\}$$

$\mathbb{Z} \bmod 2 \approx \mathbb{Z}_2$

$\bar{0} = \{2k \mid k \in \mathbb{Z}\}$ $\qquad \mathbb{Z} = \bar{0} \cup \bar{1}$

$\bar{1} = \{1 + 2k \mid k \in \mathbb{Z}\}$

$\boxed{\mathbb{Z}_3}$

$\bar{0} = \{3k \mid k \in \mathbb{Z}\} = \bar{3} = \bar{6} = \bar{9} = \overline{12} = \dots$

$\bar{1} = \{1 + 3k\}$

$\bar{2} = \{2 + 3k\}$

⋮

$\mathbb{Z}_q$

$\bar{0} = \{q \cdot k\}$

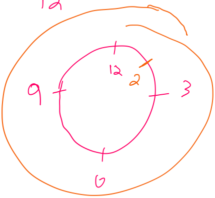
$\bar{1} = \{1 + q \cdot k\}$

⋮ ⋮

$\overline{q-1}$ $\{q-1 + q \cdot k\}$

Ex: $\mathbb{Z}_{12}$

$\overline{14} = \overline{12+2} = \overline{12} + \bar{2} = \bar{2}$



$\overline{18} = \bar{6}$

$\overline{23} = \overline{11}$

Ex: $\mathbb{Z}_5 = \{\underline{\underline{\bar{0}}}, \underline{\underline{\bar{1}}}, \underline{\underline{\bar{2}}}, \underline{\underline{\bar{3}}}, \underline{\underline{\bar{4}}}\}$

$\bar{a}, \bar{b} \in \mathbb{Z}_q$

$\bar{a} = a \pmod q$

$\bar{a} + \bar{b} = \overline{a+b}$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

$$\bar{a} = \bar{c} \;;\; \bar{b} = \bar{d} \qquad \bar{a} \cdot \bar{b} = \bar{c} \cdot \bar{d}$$

$$\bar{a} \pm \bar{b} = \bar{c} \pm \bar{d}$$

Ex: $\mathbb{Z}_{12}$

$$\bar{2} \cdot \bar{5} = \overline{14} \cdot \overline{17} = \overline{14} \cdot \bar{5} = \bar{2} \cdot \overline{17} = \ldots$$

Ex: $a = 2p \;,\; b = 2q + 1$

$$\begin{aligned} a + b &= 2p + 2q + 1 \\ &= 2\underbrace{(p+q)}_{K} + 1 \\ &= \underline{2K + 1} \end{aligned}$$

Ex:

$$\begin{aligned} 2p \cdot 2q &= 4pq \\ &= 2 \cdot \underbrace{(2pq)}_{K} \\ &= 2K \end{aligned}$$

Ex: $(2K)^2 = 4K^2 = \underline{\underline{2 \cdot 2K^2}}$