① Show that $(a+b, a-b)$ is either 1 or 2, if and only if $(a,b)=1$

② Find all integers n such that n^2+1 is divisible by $n+1$

$$
\begin{array}{r|l}
 & n-1 \\
\hline
(n+1) & n^2+1 \\
 & \underline{-n^2 \pm n} \\
 & \quad -n+1 \\
 & \quad \underline{\mp n \mp 1} \\
 & \qquad 2
\end{array}
$$

$\therefore (n+1) \mid \{(n+1)(n-1) - 2\}$

$\Rightarrow (n+1) \mid (-2)$

$\Rightarrow (n+1) \in \{-2, -1, 1, 2\}$

$\Rightarrow n \in \{-3, -2, 0, 1\}$ $\leftarrow$ Ans.

③ Show that for all odd integers n, $\gcd(3n, 3n+2) = 1$

④ Prove that the sum of the first n natural numbers cannot be prime $(n > 2)$

Let $S_n = 1 + 2 + 3 + \dots + n$ — ①

$= n + (n-1) + (n-2) + \dots + 1$ — ②

Adding ① and ② $2S_n = \underbrace{(n+1) + (n+1) + \dots + (n+1)}_{n\text{-times}} \Rightarrow S_n = \frac{n(n+1)}{2}$

Let S_n be prime $\Rightarrow \frac{n}{2} = 1$ or $\frac{n+1}{2} = 1$ or $\frac{n(n+1)}{2} = 1$

$\Rightarrow n = 2$ or $n = 1$ or $n = 1$.

But $n > 2$ (given) $\Rightarrow S_n$ cannot be prime.

QED

⑤ Prove that n^2+23 is divisibly by 24 for infinitely many integers n.

$24 \mid (n^2 + 23)$

$\Rightarrow 24 \mid (n^2 + 24 - 1)$

$\Rightarrow 24 \mid (n^2 - 1)$

$\Rightarrow 24 \mid (n-1)(n+1)$

$\Rightarrow 24 \mid (n-1)$ or $24 \mid (n+1)$

$\Rightarrow n \equiv 1 \pmod{24}$ or $n \equiv 23 \pmod{24}$

The residue classes $\bar{1}$ and $\overline{23}$ of $\mathbb{Z}_{24}$ have infinitely many integers. Since $n \in \bar{1}$ or $n \in \overline{23}$, $24 \mid (n^2+23)$ for infinitely many integers n

QED

⑥ Find all primes of the form n^3-1 for integer $n>1$

Let a prime integer $p = n^3-1$, $n \in \mathbb{N}$

$$p = n^3-1 = (n-1)(n^2+n+1)$$

$\Rightarrow$ $n-1=1$ or $n^2+n+1=1$

$\Rightarrow$ $n=2$ or $n^2+n=0$

$\Rightarrow$ $n=2$ or $n \in \{-1,0\} \notin \mathbb{N}$

For $n=2$, $p=7$.

$\therefore$ 7 (seven) is the only prime of the form n^3-1, $n \in \mathbb{N}$

⑦ Use Euclidean algorithm to calculate gcd(a,b) and hence express it as $au+bv$ for some $u,v \in \mathbb{Z}$ for the following a, b.

a) 12378, 3054

$12378 = 4(3054)+162.$

$3054 = 18(162)+138.$

$162 = 1(138)+24$

$138 = 5(24)+18.$

$24 = 1(18)+6.$

$18 = 3(6)+0$

gcd $= 6$

$6 = 24-18 = 24-\{138-5(24)\}$

$= 6(24)-138 = 6\{162-138\}-138$

$= 6(162)-7(138) = 6(162)-7\{3054-18(162)\}$

$= 132(162)-7(3054) = 132\{12378-4(3054)\}-7(3054)$

$= 132(12378)-535(3054)$

Ans: gcd$(12378, 3054) = 6 = 132(12378)-535(3054)$

b) 272, 1479

$1479 = 5(272)+119$

$272 = 2(119)+34$

$119 = 3(34)+17$

$34 = 2(17)+0$

$17 = 119-3(34) = 119-3\{272-2(119)\}$

$= (119)7-(272)3 = 7\{1479-5(272)\}-(272)3$

$= 7(1479)-38(272)$

Ans: gcd$(272, 1479) = 17 = 7(1479)-38(272)$

c) 42823, 6409

$42823 = 6(6409)+4369$

$6409 = (4369)+2040$

$4369 = 2(2040)+289$

$2040 = 7(289)+17$

$289 = 17(17)+0$

$17 = 2040-7(289) = 2040-7\{4369-2(2040)\}$

$= 15(2040)-7(4369)$

$= 15(6409)-22(4369)$

$= -22(42823)+147(6409)$

Ans: gcd$(42823, 6409) = 17 = -22(42823)+147(6409)$

d) 1819, 3587

$3587 = (1819) + 1768$

$1819 = (1768) + 51$

$1768 = 34(51) + 34$

$51 = (34) + 17$

$34 = 2(17)$

$17 = 51 - 34 = 51 - \{1768 - 34(51)\}$

$= 35(51) - 1768 = 35\{1819 - 1768\} - 1768$

$= 35(1819) - 36(1768) = 35(1819) - 36\{3587 - 1819\}$

$= 71(1819) - 36(3587)$

$\gcd(1819, 3587) = 17 = 71(1819) - 36(3587)$

⑧ Find integers x, y, z satisfying $\gcd(198, 288, 512) = 198x + 288y + 512z$

- $288 = (198) + 90$

  $198 = 2(90) + 18$

  $90 = 5(18)$

- $512 = (288) + 224$

  $288 = (224) + 64$

  $224 = 3(64) + 32$

  $64 = 2(32)$

- $32 = (18) + 14$

  $18 = (14) + 4$

  $14 = 3(4) + 2$

  $4 = 2(2)$

$\gcd(198, 288, 512) = 2.$

- $18 = 198 - 2(90)$

  $= 3(198) - 2(288)$ — ①

- $32 = 224 - 3(64)$

  $= 4(224) - 3(288)$

  $= 4(512) - 7(288)$ — ②

- $2 = 14 - 3(4)$

  $= 4(14) - 3(18)$

  $= 4(32) - 7(18)$ — ③

Using ① and ② in ③

$2 = 4\{4(512) - 7(288)\} - 7\{3(198) - 2(288)\}$

$\therefore \gcd(198, 288, 512) = 2 = -21(198) - 14(288) + 16(512)$ ← Ans.

⑨ Find the general solution in integers for $56x + 72y = 40$

$72 = (56) + 16$

$56 = 3(16) + 8$

$16 = 2(8)$

$8 \mid 40 \Rightarrow$ solⁿ exists

$8 = 56 - 3(16) = 4(56) - 3(72)$

$\therefore 40 = 20(56) - 15(72)$

General solution $(x, y) = (20 - 9t, -15 + 7t) \ \forall t \in \mathbb{Z}$

← Ans.

⑩ Find the general solution in integers for $24x + 138y = 18$

$138 = 5(24) + 18$

$24 = (18) + 6$

$18 = 3(6)$

$6 \mid 18 \Rightarrow$ solⁿ exists

$6 = 24 - 18 = 6(24) - 138$

$\therefore 18 = 18(24) - 3(138)$

General solution $(x, y) = (18 - 23t, -3 + 4t) \ \forall t \in \mathbb{Z}$

← Ans.

(11) Find general solution in integers for $221x + 35y = 11$

$221 = 6(35) + 11$

$35 = 3(11) + 2$

$11 = 5(2) + 1$

$2 = 2(1)$

$1 | 11 \Rightarrow$ solⁿ exists

$1 = 11 - 5(2) = 16(11) - 5(35) = 16(221) - 101(35)$

$\therefore 11 = 176(221) - 1111(35)$

General solution $(x, y) = (176 + 35t, -1111 - 221t) \ \forall t \in \mathbb{Z}$ ← Ans.

(12) Find $\tau(360)$, $\sigma(360)$, $\tau(1482)$, $\sigma(1225)$, $\tau(1932)$, $\sigma(7007)$

- $360 = 2^3 \cdot 3^2 \cdot 5$

  $\tau(360) = (3+1)(2+1)(1+1) = \underline{24}$

  $\sigma(360) = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = 15\left(\frac{26}{2}\right)\left(\frac{24}{4}\right) = \underline{1170}$

- $1482 = 2 \cdot 3 \cdot 13 \cdot 19$

  $\tau(1482) = (1+1)^4 = \underline{16}$

- $1225 = 5^2 \cdot 7^2$

  $\sigma(1225) = \frac{5^3-1}{5-1} \cdot \frac{7^3-1}{7-1} = 1 = \left(\frac{124}{4}\right)\left(\frac{342}{6}\right) = \underline{1767}$

- $1932 = 2 \cdot 3 \cdot 7 \cdot 23$

  $\tau(1932) = (1+1)^4 = \underline{16}$

- $7007 = 7^2 \cdot 11 \cdot 13$

  $\sigma(7007) = \frac{7^3-1}{7-1} \cdot \frac{11^2-1}{11-1} \cdot \frac{13^2-1}{13-1} = \frac{342}{6} \cdot \frac{120}{10} \cdot \frac{168}{12} = \underline{9576}$

(13) Show that $2903^n - 803^n - 464^n + 261^n$ is divisible by 1897 for all $n \in \mathbb{N}$

(14) Find the least positive residue in $3^{36} \pmod{77}$

(15) Use the theory of congruences to prove $7 \mid (2^{5n+3} + 5^{2n+3})$ for all $n \geq 1$

(16) Solve the linear congruence

a) $15x \equiv 9 \pmod{18}$ $\Rightarrow$ $15x - 18y = 9$, $x, y \in \mathbb{Z}$

$18 = (15) + 3$ $\qquad$ $3 = 18 - 5$

$15 = (3)5$ $\qquad$ $\therefore 9 = 3(18) - 3(5)$

$3 \mid 9 \Rightarrow$ sol^n exists $\qquad$ General solution $(x,y) = (-3-6t, -3-5t)$ $\forall t \in \mathbb{Z}$

Solutions for $15x \equiv 9 \pmod{18}$, are $(-3-6t) \pmod{18}$ for $t = \{0,1,2\}$.

i.e. $x \in \{3 \bmod 18, 9 \bmod 18, 15 \bmod 18\}$ $\leftarrow$ Ans.

b) $28x \equiv 63 \pmod{105}$ $\Rightarrow$ $28x - 105y = 63$ $\quad x, y \in \mathbb{Z}$

$105 = 3(28) + 21$ $\qquad$ $7 = 28 - 21 = 4(28) - 105$

$28 = (21) + 7$ $\qquad$ $\therefore 63 = 36(28) - 9(105)$

$21 = 3(7)$ $\qquad$ General solution $(x,y) = (36 - 15t, -9 - 4t)$ $\forall t \in \mathbb{Z}$

$7 \mid 63 \Rightarrow$ sol^n exists

Solutions for $28x \equiv 63 \pmod{105}$ are $(36 - 15t) \pmod{105}$ for $t \in [0,6]$

i.e. $x \in \{\bar{6}, \bar{21}, \bar{36}, \bar{51}, \bar{66}, \bar{81}, \bar{96}\}$ of $\mathbb{Z}_{105}$ $\quad \leftarrow$ Ans.

(17) Solve the system of linear congruences.

a) $x \equiv 1 \pmod 3$; $x \equiv 2 \pmod 5$; $x \equiv 3 \pmod 7$

- $N = 3 \cdot 5 \cdot 7 = 105$
- $y_0 = 35$; $y_1 = 21$; $y_2 = 15$
- $z_0 = 2$; $z_1 = 1$; $z_2 = 1$

$\therefore x \equiv (70 + 42 + 45) \pmod{105} \equiv 52 \pmod{105}$.

b) $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 5 \pmod 8$

- $N = 3 \cdot 5 \cdot 7 = 105$
- $y_0 = 35$; $y_1 = 21$; $y_2 = 15$
- $z_0 = 2$; $z_1 = 1$; $z_2 = 1$

$\therefore x \equiv (140 + 63 + 60) \pmod{105} \equiv 53 \pmod{105}$

c) $x \equiv 2 \pmod 5$; $x \equiv 3 \pmod 7$; $x \equiv 5 \pmod 8$

- $N = 5 \cdot 7 \cdot 8 = 280$
- $y_0 = 56$; $y_1 = 40$; $y_2 = 35$
- $z_0 = 1$; $z_1 = 3$; $z_2 = 3$

$\therefore x \equiv (112 + 360 + 525) \pmod{280} \equiv 157 \pmod{280}$

d) $x \equiv 5 \pmod 6$; $x \equiv 4 \pmod{11}$; $x \equiv 3 \pmod{17}$

- $N = 6 \cdot 11 \cdot 17 = 1122$
- $y_0 = 187$; $y_1 = 102$; $y_2 = 66$
- $z_0 = 1$; $z_1 = 4$; $z_2 = 8$

$\therefore x \equiv (935 + 1632 + 1584) \pmod{1122} \equiv 785 \pmod{1122}$

(18) Find the number of less than n and prime to n for the following n

$\phi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$ for $n \in \mathbb{Z}$ and prime factors p_i of n gives the number of integers less than n and prime to n

- $256 = 2^8 \Rightarrow \phi(256) = 256\,(1/2) = 128$.
- $324 = 2^2 \cdot 3^4 \Rightarrow \phi(324) = 324\,(1/2)(2/3) = 108$
- $900 = 2^2 \cdot 3^2 \cdot 5^2 \Rightarrow \phi(900) = 900\,(1/2)(2/3)(4/5) = 240$
- $2048 = 2^{11} \Rightarrow \phi(2048) = 2048\,(1/2) = 1024$
- $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \Rightarrow \phi(5040) = 5040\,(1/2)(2/3)(4/5)(6/7) = 1152$.
- $7200 = 2^5 \cdot 3^2 \cdot 5^2 \Rightarrow \phi(7200) = 7200\,(1/2)(2/3)(4/5) = 960$

(19) Find the least positive residue in $2^{41} \pmod{23}$

By Fermat's Theorem, $2^{22} \equiv 1 \pmod{23} \Rightarrow 2^{44} \equiv 1 \pmod{23} \equiv 24 \pmod{23}$

$\therefore 2^{41} \equiv 3 \pmod{23}$ Ans: 3 (three)

(20) Use congruence to find the remainder when $2^{73} + 14^3$ is divided by 11

(21) Prove that the eigth power of any integer is of the form $17k$ or $17k+1$

(22) Show that $a^{12} - b^{12}$ is divisible by 91 if both a and b are prime to 91

Since a is prime to 91, a is prime to 13 and 7 [$91 = 13 \times 7$]

By Fermat's Theorem $a^{12} \equiv 1 \pmod{13}$ and $a^6 \equiv 1 \pmod{7}$

$\Rightarrow a^{12} \equiv 1 \pmod{13}$ and $a^{12} \equiv 1 \pmod{7}$

$\Rightarrow a^{12} \equiv 1 \pmod{91}$ — (1)

Similarly for b, $b^{12} \equiv 1 \pmod{91}$ — (2)

From (1) and (2), $a^{12} - b^{12} \equiv 0 \pmod{91} \Rightarrow 91 \mid (a^{12} - b^{12})$ QED

(23) If n is a prime > 7, prove that $n^6 - 1$ is divisible by 504 [corrected Q]

(24) Show that $4(29)! + 5!$ is divisible by 31

$$30! + 1 \equiv 0 \pmod{31}$$

$$\Rightarrow 30! \equiv 30 \pmod{31}$$

$$\Rightarrow 29! \equiv 1 \pmod{31}$$

$$\Rightarrow 4(29!) \equiv 4 \pmod{31}$$

$$\Rightarrow 4(29)! + 120 \equiv 124 \pmod{31} \equiv 0 \pmod{31}$$

$$\Rightarrow 31 \mid 4(29!) + 5!$$

QED

(25) Use congruence to find the remainder when 4444^{4444} is divided by 9

(26) Prove that $641 \mid 2^{32} + 1$

(27) Prove that $7 \mid 2222^{5555} + 5555^{2222}$.

QED

(28) If p is a prime, prove that $2(p-3)! + 1 \equiv 0 \pmod p$

$(p-1)! + 1 \equiv 0 \pmod p$ [Wilson's Theorem]

$(p-1)(p-2)(p-3)! \equiv -1 \equiv (p-1) \pmod p$

$(p-2)(p-3)! \equiv 1 \pmod p$

$p(p-3) - 2(p-3)! - 1 \equiv 0 \pmod p$

$2(p-3)! + 1 \equiv 0 \pmod p$ QED.

Poset and Lattice

(1) Let S be the set of all lines in 3-space. A relation ρ is defined on S by "$l \rho m$ iff l lies on the plane of m" for $l, m \in S$.
Examine if ρ is an equivalence relation

S : set of all lines in 3D

ρ : relation in S such that $l\rho m \Leftrightarrow l$ lies in the plane of m for $l, m \in S$

(Transitive property) Let $l, m, k \in S$ and $l \rho m$ and $m \rho k$.

i.e. l lies on the plane of m, and
m lies on the plane of k.
l may or may not lie on the plane of k. (see figure)
Thus $l\rho m$ and $m \rho k \not\Rightarrow l \rho k$.
$\Rightarrow \rho$ is not transitive
$\Rightarrow \rho$ is <u>not</u> an equivalence relation ← Ans.

$l\rho m$ and $m \rho k$
$\not\Rightarrow l \rho k$

(2) Define a relation R on $\mathbb{Z}$ by mRn iff $m^2 = n^2$. Is R a partial order?

R : relation in $\mathbb{Z}$ such that $mRn \Leftrightarrow m^2 = n^2$

(Antisymmetric property) Let mRn and nRm for $m, n \in \mathbb{Z}$

$\Rightarrow m^2 = n^2$ and $n^2 = m^2$.

$\Rightarrow m^2 - n^2 = 0$

$\Rightarrow (m-n)(m+n) = 0$

$\Rightarrow m = n$ or $m - n$.

Thus R is not antisymmetric as mRn and $nRm \not\Rightarrow m = n \quad \forall m, n \in \mathbb{Z}$

R is <u>not</u> a partial order ← Ans.

③ Define a relation ρ on $\mathbb{C}$ by "$(a+ib)\,\rho\,(c+id)$ iff $a \le c$ and $b \le d$" for $a+ib,\ c+id \in \mathbb{C}$. Show that ρ is a partial order relation.

- (Reflexive) Let $a+ib \in \mathbb{C}$, then $a \le a$ and $b \le b$

$\Rightarrow (a+ib)\,\rho\,(a+ib) \quad \forall (a+ib) \in \mathbb{C}$

Thus, ρ is reflexive. — ①

- (Antisymmetric) Let $(a+ib), (c+id) \in \mathbb{C}$

$(a+ib)\,\rho\,(c+id)$ and $(c+id)\,\rho\,(a+ib)$

$\Rightarrow (a \le c$ and $b \le d)$ and $(c \le a$ and $d \le b)$

$\Rightarrow a = c$ and $b = d$

$\Rightarrow (a+ib) = (c+id)$

i.e. $(a+ib)\,\rho\,(c+id)$ and $(c+id)\,\rho\,(a+ib) \Rightarrow (a+ib) = (c+id) \quad \forall (a+ib), (c+id) \in \mathbb{C}$

Thus, ρ is antisymmetric. — ②

- (Transitive) Let $a+ib,\ c+id,\ g+if \in \mathbb{C}$ and $(a+ib)\,\rho\,(c+id)$, $(c+id)\,\rho\,(g+if)$

$(a+ib)\,\rho\,(c+id) \Rightarrow a \le c$ and $b \le d$

$(c+id)\,\rho\,(g+if) \Rightarrow c \le g$ and $d \le f$

$\therefore a \le g$ and $b \le f$

$\Rightarrow (a+ib)\,\rho\,(g+if)$

Thus, ρ is transitive — ③

From ①, ②, ③ ρ is a partial order relation

④ Let D_{30} be the set of all positive divisors of 30. Define a relation "$\le$" on D_{30} by "$x \le y$ iff x divides y". Prove that $(D_{30}, \le)$ is a poset. Draw the Hasse diagram

D_{30}: set of positive divisors of 30 $\Rightarrow D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

$\le$: relation in D_{30} such that $x \le y \Leftrightarrow x \mid y$; $x, y \in D_{30}$

- (Reflexive) Let $x \in D_{30}$ then $x \mid x$

$\therefore x \le x \quad \forall x \in D_{30} \quad \therefore \le$ is reflexive

- (Antisymmetric) Let $x, y \in D_{30}$ and $(x \le y$ and $y \le x)$

$\Rightarrow x \mid y$ and $y \mid x \Rightarrow x = y$

$\therefore x \le y$ and $y \le x \Rightarrow x = y \quad \forall x, y \in D_{30} \quad \therefore \le$ is antisymmetric

- (Transitive) Let $x, y, z \in D_{30}$ and $(x \le y$ and $y \le z)$

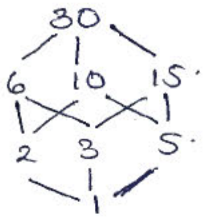
$\Rightarrow x \mid y$ and $y \mid z \Rightarrow y = xk_1$ and $z = yk_2$ for some $k_1, k_2 \in \mathbb{Z}$

$\Rightarrow z = xk_1k_2 \Rightarrow x \mid z$

$\therefore x \le y$ and $y \le z \Rightarrow x \le z \quad \forall x, y, z \in D_{30} \quad \therefore \le$ is transitive

Thus, $(D_{30}, \le)$ is a poset.

Hasse Diagram of $(D_{30}, \leq)$



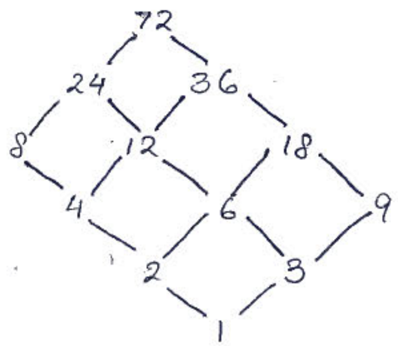
⑤ Let S be the set of all positive divisors of 72. Define a relation $\leq$ on S by "$x \leq y$ iff x divides y" for $x, y \in S$. Prove $(S, \leq)$ is a poset. Draw Hasse diag.

S: set of +ve divisors of 72 $\Rightarrow S = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$.

$\leq$: relation on S such that $x \leq y \Leftrightarrow x \mid y \quad \forall x, y \in S$

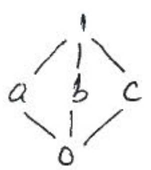
As proved in the prev Q, $\leq$ is a partial order relation. Hence $(S, \leq)$ is a poset

Hasse Diagram of $(S, \leq)$



⑥ Define 'distributive lattice'. Give an example. Is the lattice with the given Hasse diagram distributive? Justify

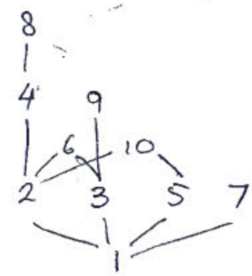
- A lattice $(S, \leq)$ is called distributive if it satisfies the distributive property:
  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad \forall a, b, c \in S$
- Example: $(D_{30}, \leq)$ of Q4 and $(S, \leq)$ of Q5.



- $a \wedge (b \vee c) = a \wedge 1 = a$
  $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$

$\Big\} \Rightarrow$ given lattice is not distributive

⑦ Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Let $x \leq y : x \mid y$.
Find the maximal element(s) in the poset $(S, \leq)$



Maximal elements $= \{6, 7, 8, 9, 10\}$

⑧ Show that the poset given in the following Hasse diagram is a lattice. Is it distributive and complemented

- Every pair of elements has a valid lub and glb. Thus, it is a lattice
- Complement of c does not exist. $\Rightarrow$ lattice is not complemente
- $a \vee (b \wedge c) = a \vee 0 = a$
  $(a \vee b) \wedge (a \vee c) = 1 \wedge d = d$ $\Big\}$ $\Rightarrow$ lattice is not distributive

Morphisms, Ring and Field

① Show that the groups $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Q}, + \rangle$ are not isomorphic

② Determine whether the given map ϕ is a homomorphism

a) $\phi : \mathbb{R} \to \mathbb{Z}$ under addition given by $\phi(x)$ = greatest integer $\leq x$

$\phi(a) + \phi(b) \neq \phi(a+b)$ if frac{a} + frac{b} ≥ 1 $\quad \forall a, b \in \mathbb{R}$

Example : $\phi(3.6) + \phi(2.4) = 5 \neq \phi(3.6 + 2.4) = 6$

$\therefore$ not a homomorphism.

b) $\phi : \mathbb{R}^* \to \mathbb{R}^*$ under multiplication given by $\phi(x) = |x|$

$\phi(ab) = |ab| = |a| \cdot |b| = \phi(a) \cdot \phi(b) \quad \forall a, b \in \mathbb{R}^*$

$\therefore$ it is a homomorphism

c) $\phi : M_n(\mathbb{R}) \to \mathbb{R}$ under addition given by $\phi(A) = \det(A)$

$\phi(a+b) = \det(a+b) \neq \det(a) + \det(b) = \phi(a) + \phi(b) \quad \forall a, b \in M_n(\mathbb{R})$

Example : $a = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $b = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$, ③ Show that $8\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}_9$

Let $\phi : 8\mathbb{Z} \to \mathbb{Z}_9$ be defined as $\phi(8x) = x \pmod 9 \quad \forall x \in \mathbb{Z}$

- (Isomorphism) Let $8a, 8b \in 8\mathbb{Z}$

  $\phi(8a + 8b) = (a+b) \pmod 9 \equiv a \pmod 9 +_9 b \pmod 9 = \phi(8a) +_9 \phi(8b)$

  $\therefore$ ϕ is a homomorphism

- (Onto) $\forall\, x \pmod 9 \in \mathbb{Z}_9 \quad \exists\, 8x \in 8\mathbb{Z}$ such that $\phi(8x) = x \pmod 9$

  $\therefore$ ϕ is an epimorphism

- By 1st Isomorphism Theorem, $\cdot/\mathrm{Ker}(\phi) \simeq \mathbb{Z}_9$

  $\mathrm{Ker}(\phi) = \{8x \in 8\mathbb{Z} : \phi(8x) = 0 \bmod 9\}$

  $= \{8x \in 8\mathbb{Z} : x \equiv 0 \bmod 9\}$

  $= \{8x \in 8\mathbb{Z} : x = 9y \text{ for } y \in \mathbb{Z}\}$

  $= \{72y \in 8\mathbb{Z}\}$

  $= 72\mathbb{Z}$

Thus, $8\mathbb{Z}/72\mathbb{Z} \simeq \mathbb{Z}_9$ QED

④ Prove that $\mathbb{Z}_8$ is not a homomorphic image of $\mathbb{Z}_{15}$.

⑤ Prove that the cancellation law holds in a ring R iff R has no divisors of 0

- Proving cancellation law holds in $R \Rightarrow R$ has no divisors of 0

Let $a, b \in R$ such that $a \cdot b = 0$

$\Rightarrow a \cdot b = a \cdot 0$ or $a \cdot b = 0 \cdot b$

$\Rightarrow b = 0$ (LCL) or $a = 0$ (RCL)

$\Rightarrow a = 0$ or $b = 0$ i.e. R has no divisors of 0 — ①

- Proving R has no divisors of $0 \Rightarrow$ cancellation law holds in R

Let $a, b, c \in R$ with $a \neq 0$ such that $a \cdot b = a \cdot c$

$\Rightarrow a \cdot b - a \cdot c = 0$

$\Rightarrow a \cdot (b - c) = 0$ [distributive property]

$\Rightarrow b - c = 0$

$\Rightarrow b = c$ ∴ left cancellation law holds in R

Similarly, right-cancellation law holds in R — ②

From ① and ② cancellation law holds in $R \Leftrightarrow R$ has no divisors of 0

⑥ Show that the ring of matrices $\left\{ \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ contains divisors of zero and does not contain the unity

Let $A = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$ and $B = \begin{pmatrix} 2p & 0 \\ 0 & 2q \end{pmatrix}$ for $a, b, p, q \in \mathbb{Z}$

- Let $AB = 0$ for $A \neq 0$, $B \neq 0$

$\Rightarrow \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} \begin{pmatrix} 2p & 0 \\ 0 & 2q \end{pmatrix} = \begin{pmatrix} 4ap & 0 \\ 0 & 4bq \end{pmatrix} = 0 \Rightarrow 4ap = 0$ and $4bq = 0$

$\Rightarrow a = 0$ and $q = 0$ i.e. $A = \begin{pmatrix} 0 & 0 \\ 0 & 2b \end{pmatrix}$ and $B = \begin{pmatrix} 2p & 0 \\ 0 & 0 \end{pmatrix}$
or $b = 0$ and $p = 0$ i.e. $A = \begin{pmatrix} 2a & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 2q \end{pmatrix}$ } which give divisors of zero taken simultaneously

- Let I be the identy matrix $= \begin{pmatrix} 2i & 0 \\ 0 & 2j \end{pmatrix}$ $i, j \in \mathbb{Z}$

$AI = A \Rightarrow \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} \begin{pmatrix} 2i & 0 \\ 0 & 2j \end{pmatrix} = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$

$\Rightarrow \begin{pmatrix} 4ai & 0 \\ 0 & 4bj \end{pmatrix} = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$

$\Rightarrow i = 1/2, \ j = 1/2$

Since $1/2 \notin \mathbb{Z}$, identity I does not exist

⑦ Examine if the ring $R = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ contains divisors of zero

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in R$ and $B = \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \in R \Rightarrow AB = \begin{pmatrix} ax + 2by & ay + bx \\ 2bx + ay) & 2by + ax \end{pmatrix}$

Let $A \neq 0$ and $B \neq 0$ but $AB = 0 \Rightarrow ax + 2by = 0$ and $ay + bx = 0$

Solution (wrt x, y) exists in $\mathbb{R}$ if $\begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = 0 \Rightarrow a = \pm\sqrt{2}b$ which is true for several $a, b \in \mathbb{R}$

Thus R contains divisors of zero

⑧ Prove that $\mathbb{Z}[x]$: ring of all polynomials with integer coefficients is an integral domain

- (Divisors of zero) $\forall f, g \in \mathbb{Z}[x]$, $fg = 0 \Rightarrow f = 0$ or $g = 0$
- (Commutativity) $\forall f, g \in \mathbb{Z}[x]$, $fg = gf$ is true
- (Identity) $\forall f \in \mathbb{Z}[x]$, $f1 = 1f = f$ and $1 \in \mathbb{Z}[x]$

Thus, $\mathbb{Z}[x]$ is an integral domain

⑨ Prove that the ring $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a field

- Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in R$ and $B = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in R \Rightarrow AB = \begin{pmatrix} ax - by & ay - bx \\ -bx - ay & -by + ax \end{pmatrix} = BA$

  Thus, R is commutative with multiplication

- Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in R \Rightarrow \exists A' = \frac{1}{|A|} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in R$ if $|A| \neq 0$

  $|A| = 0 \Rightarrow a^2 + b^2 = 0 \Rightarrow a = 0$ and $b = 0 \Rightarrow A = 0$

  Thus if $A \neq 0$, $|A| \neq 0$ and A' exists such that $AA' = A'A = I$ where identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Thus, multiplicative inverse exists $\forall A \in R, A \neq 0$

- Thus, R is a field

Q.(11) Examine if the ring of matrices, $R = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in X \right\}$ is a where
(i) $X = \mathbb{Q}$ (ii) $X = \mathbb{R}$

- $\forall A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}, B = \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \in R \quad AB = \begin{pmatrix} ax + 2by & ay + bx \\ 2(bx + ay) & 2by + ax \end{pmatrix} = BA$

$\therefore$ R is commutative

- $\forall A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in R \quad \exists A^{-1} = \frac{1}{|A|} \begin{pmatrix} a & -2b \\ -b & a \end{pmatrix} \in R$ if $|A| \neq 0$

(i) $a, b \in \mathbb{Q}$ and $|A| = 0 \Rightarrow a^2 - 2b^2 = 0$ which is true for $a = 0, b = 0$ i.e $A = 0$

$\Rightarrow \forall A \in R - \{0\} \; \exists A' \in R$ such that $AA' = A'A = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ i.e. identity

(ii) $a, b \in \mathbb{R}$ and $|A| = 0 \Rightarrow a^2 - 2b^2 = 0$ which is true for infinitely many a, b

Example : $A = \begin{pmatrix} \sqrt{2} & 1 \\ 2 & \sqrt{2} \end{pmatrix}$ gives $|A| = 0$

$\Rightarrow$ (i) R is a field (ii) R is not a field

(12) Prove that a set $S = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$ is a subring of the ring $M_2(\mathbb{Z})$

- Additive identity $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S \subseteq M_2(\mathbb{Z})$
- $\forall A = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, B = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in S. \left\{ \begin{array}{l} A - B = \begin{pmatrix} a-x & 0 \\ b-y & c-z \end{pmatrix} \in S. \\ AB = \begin{pmatrix} ax & 0 \\ bx + cy & cz \end{pmatrix} \in S. \end{array} \right.$

Thus S is a subring of $M_2(\mathbb{Z})$

(13) Prove that the ring $\langle \mathbb{Z}_n \rangle$ is an integral domain iff n is prime

- Proving $\langle \mathbb{Z}_n \rangle$ is an integral domain $\Rightarrow$ n is prime

Alternatively, n is not prime $\Rightarrow \langle \mathbb{Z}_n \rangle$ is not an integral domain

Let $n = pq \; ; \; p, q \in \mathbb{Z}^+ : 1 < p, q < n \quad \Rightarrow \bar{p}, \bar{q} \in \mathbb{Z}_n$.

But, $\bar{p} \cdot \bar{q} = \bar{n} = 0. \Rightarrow$ divisors of zero exist $\Rightarrow \langle \mathbb{Z}_n \rangle$ is not an integral domain — (1)

- Proving n is prime $\Rightarrow \langle \mathbb{Z}_n \rangle$ is an integral domain

Alternatively $\langle \mathbb{Z}_n \rangle$ is not an integral domain $\Rightarrow$ n is not prime

Let $\bar{p}, \bar{q} \in \mathbb{Z}_n$ such that $\bar{p} \cdot \bar{q} = 0 \Rightarrow \exists p' \in \bar{p}$ and $q' \in \bar{q}$ such that $n = p'q'$

$\Rightarrow$ n is not prime for $(p', q') \neq (1, n)$ or $(p', q') \neq (n, 1)$ — (2)

- From (1) and (2) $\langle \mathbb{Z}_n \rangle$ is an integral domain $\Leftrightarrow$ n is prime

(14) Prove that the ring $\mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\}$ i.e. the ring of Gaussian integers is an integral domain

$\forall\ A = (a+ib),\ B = (c+id) \in \mathbb{Z}[i].,\quad AB = 0 \Rightarrow$

$\Rightarrow\ (a+ib)(c+id) = 0$

$\Rightarrow\ (ac-bd) + i(bc+ad) = 0$

$\Rightarrow\ ac - bd = 0$ and $bc + ad = 0$

This has a sol^n (wrt c,d) if $\begin{vmatrix} a & -b \\ b & a \end{vmatrix} = 0 \Rightarrow a^2+b^2 = 0 \Rightarrow a=0, b=0 \Rightarrow A=0$

Similarly, if $A \neq 0$, $B = 0$

Thus, $AB = 0 \Rightarrow A=0$ or $B=0$ $\forall A,B \in \mathbb{Z}[i]$

$\Rightarrow \mathbb{Z}[i]$ does not have any divisors of zero

$\Rightarrow \mathbb{Z}[i]$ is an integral domain

QED

(15) Prove that $\langle \mathbb{Z}_{11} \rangle$ is a field. Find the multiplicative inverses of all non-zero elements in $\langle \mathbb{Z}_{11} \rangle$

Using result of Q13 with prime $n = 11$, $\langle \mathbb{Z}_{11} \rangle$ is an integral domain

Theorem: Every finite integral domain is a field

Since $\langle \mathbb{Z}_{11} \rangle$ is finite and integral domain, $\langle \mathbb{Z}_{11} \rangle$ is a field

Non-zero elements in $\langle \mathbb{Z}_{11} \rangle$	1	2	3	4	5	6	7	8	9	10
Multiplicative inverse	1	6	4	3	9	2	8	7	5	10

(16) Prove that the centre of a ring is a subring

Let R be the ring and S be its center. i.e. $S = \{x \in R : ax = xa\ \forall a \in R\}$

- Let $x, y \in S \subseteq R$. $\Rightarrow ax = xa$ and $ay = ya$ $\forall a \in R$,

$\Rightarrow ax - ay = xa - ya$

$\Rightarrow a(x-y) = (x-y)a$

$\Rightarrow (x-y) \in S$.

- Let $x, y \in S \Rightarrow a(xy) = (ax)y = x(ay) = (xy)a$ $\forall a \in R$. $\Rightarrow (xy) \in S$.

$\therefore S$ is a subring of R

(17) In ring $\langle \mathbb{Z}_n \rangle$, $[m]$ is a unit iff $\gcd(m,n)=1$

- Proving $\bar{m}$ is a unit in $\mathbb{Z}_n \Rightarrow \gcd(m,n)=1$

  $\bar{m}$ is a unit $\Rightarrow \exists \bar{k} \in \mathbb{Z}_n : \bar{m}\bar{k} = \bar{1}$

  Let $\gcd(m,n)=d$. Take $m \in \bar{m}$, $k \in \bar{k}$ $\Rightarrow mk = 1 \pmod{n}$

  $d \mid m \Rightarrow d \mid mk \Rightarrow d \mid (nt+1) \ \forall t \in \mathbb{Z}$.

  $\therefore d \mid n$ and $d \mid 1 \Rightarrow d=1$ $\quad \therefore \gcd(m,n)=1$

- Proving $\gcd(m,n)=1 \Rightarrow \bar{m}$ is a unit in $\mathbb{Z}_n$

  $\gcd(m,n)=1 \Rightarrow mu + nv = 1$ for $u, v \in \mathbb{Z}$

  $\Rightarrow mu = 1 \pmod{n} \Rightarrow \forall\, m \in \bar{m}$, $\exists\, u \in \bar{u}$ such that $mu = 1$

  $\Rightarrow \bar{m}\bar{u} = \bar{1} \Rightarrow \bar{m}$ is a unit in $\mathbb{Z}_n$

- Thus, $\bar{m}$ is a unit in $\mathbb{Z}_n \Leftrightarrow \gcd(m,n)=1$

(18) If in a ring R with unity, $(xy)^2 = x^2y^2 \ \forall x,y \in R$ show that R is commutative

$$\left.\begin{aligned} (xy)^2 &= (xy)(xy) = x(yx)y \\ x^2y^2 &= (xx)(yy) = x(xy)y \end{aligned}\right\} \Rightarrow xy = yx \ \forall x, y \in R$$

[R is an associative ring with identity]

(19) Prove that in a field F, $a^2 = b^2 \Rightarrow a = b$ or $a = -b$ for $a, b \in F$

$a^2 = b^2 \Rightarrow a^2 - b^2 = (a-b)(a+b) = 0 \Rightarrow a = \pm b$ [as F cannot have divisors of 0]

(22) A) Show that set of idempotents of a commutative ring is closed under multiplication

Let R be the ring and $S = \{a \in R : a^2 = a\}$.

R is commutative $\Rightarrow$ S is commutative under the operation of R

Let $a, b \in S \Rightarrow a^2 = a,\ b^2 = b$ and $ab = ba$.

$a^2 b^2 = (aa)(bb) = a(ab)b = a(ba)b = (ab)(ab)$

But $a^2 b^2 = ab \Rightarrow (ab)(ab) = ab \Rightarrow ab = e \in S$ as $e^2 = e \in R$

$\therefore$ set of idempotents of a commutative ring is closed under multiplication

B) Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$

Let $S(X)$ be the set of idempotents in X

$S(\mathbb{Z}_6) = \{0, 1, 3, 4\}$ and $S(\mathbb{Z}_{12}) = \{0, 1, 4, 9\}$

$S(\mathbb{Z}_6 \times \mathbb{Z}_{12}) = S(\mathbb{Z}_6) \times S(\mathbb{Z}_{12}) = \{(0,0), (0,1), (0,4), (0,9), (1,0), (1,1), (1,4), (1,9),$
$(3,0), (3,1), (3,4), (3,9), (4,0), (4,1), (4,4), (4,9)\}$

(23) Let R be a ring with characteristic 3. Compute and simplify $(a+b)^6 : a, b \in R$

$(a+b)^6 = \{(a+b)^3\}^2 = \{a^3 + b^3 + 3ab(a+b)\}^2 = (a^3+b^3)^2 = a^6 + b^6 + 2a^3b^3$ — Ans

$[\because 3a = 0\ \forall a \in R]$

(24) Prove that the intersection of two subrings is a subring

Let R be a ring and S, T be its subrings

- $S \subseteq R,\ T \subseteq R \Rightarrow S \cap T \subseteq R$.
- $0 \in S,\ 0 \in T \Rightarrow 0 \in S \cap T$
- $\forall a, b \in S \cap T \left\{\begin{array}{l} a-b \in S \text{ and } ab \in S \\ a-b \in T \text{ and } ab \in T \end{array}\right\} \Rightarrow a-b,\ ab \in S \cap T$

Thus, the intersection of two subrings is a subring