1. (a). $A\times C = \{(a,c) \mid a\in A \vee c\in C\}$.

$a\in A \subseteq B$.

$c\in C \subseteq D$.

$\therefore (a,c)\in B\times D$.

$\therefore A\times C \subseteq B\times D$

(b). $\bigcap_{i=1}^{1} A_i \subseteq \bigcap_{i=1}^{1} B_i$

$A_1 \subseteq B_i$ ✓.

Assume $\bigcap_{i=1}^{k} A_i \subseteq \bigcap_{i=1}^{k} B_i$

WTS $\bigcap_{i=1}^{k+1} A_i \subseteq \bigcap_{i=1}^{k+1} B_i$

$\therefore \bigcap_{i=1}^{k+1} A_i = \bigcap_{i=1}^{k} A_i \cap A_{k+1}$ $\quad \bigcap_{i=1}^{k+1} B_i = \bigcap_{i=1}^{k} B_i \cap B_{k+1}$

$\bigcap_{i=1}^{k} A_i \subseteq \bigcap_{i=1}^{k} B_i$ $\quad A_{k+1}\subseteq B_{k+1}$.

$\therefore \bigcap_{i=1}^{k+1} A_i \subseteq \bigcap_{i=1}^{k+1} B_i$ $\quad \therefore \bigcap_{i=1}^{n} A_i \subseteq \bigcap_{i=1}^{n} B_i$ $n\in\mathbb{Z}^+$.

(c). (i). $\bigcup_{k=1}^{\infty} A_k = \{0,1,2,\cdots\infty\}$

$= \{0\}\cup N. = W.$

$\bigcap_{k=1}^{\infty} A_k = \{0,1,2,3,4,5,6,7\}$.

(ii). $\bigcup_{k=1}^{\infty} A_k = \{0,1,2,\cdots\infty\}$

$= W.$

$\bigcap_{k=1}^{\infty} A_k = \emptyset$

(iii). $k\to\infty$

$\frac{3}{k}\to 0$ $\quad 5k+2\to\infty$

$\bigcup_{k=1}^{\infty} A_k = (0,\infty)$.

$\bigcap_{k=1}^{\infty} A_k = [3,7)\cup\{10\}$.

(d). $f(n) = \begin{cases} n/2 & 2\mid n \\ 3n+1 & 2\nmid n \end{cases}$

2.(a) $(G,*)$

Group:

- Closure

$\forall x,y\in G$.

$x*y\in G$.

- Associativity

$\forall x,y,z\in G$

$(x*y)*z = x*(y*z)$

- Neutral.

$\forall x\in G$.

$x*\varepsilon = \varepsilon * x = x$.

- Invertibility

$\forall x\in G$ $\exists y\in G$.

$x*y = \varepsilon$.

(i) injection $f(x)=y$ at most one solution

$f(n)=4 \quad n=8$ or $n=1$

Not injective.

(ii) Surjection. $f(x)=y$ at least one solution.

$\therefore \forall y \in \mathbb{N} \exists 2y \in \mathbb{N}$

$\therefore f(2y)=y$ Surjective.

3. (a) congruent modulo :

two number have a same modulo when divided by a certain number

class of residues

all integers that have a same modulo when divided by a certain number

(b). $27,\ 27-83,\ 27+83 \rightarrow 110$ (with $+83$ → -56)

(c) gcd input two positive integers

$\downarrow\downarrow$

gcd(a, b)

by calculating modulo with one another

and stops when modulo = 0

the divisor is gcd(a, b).

$1680 \equiv 140 \pmod{1540}$

$1540 \equiv 0 \pmod{140}$

$\therefore \gcd(1680, 1540) = 140$

(d). $56x \equiv 23 \bmod 93$.

$\phi(93) = 2 \times 30 = 60$

$56^{60} \equiv 1 \pmod{93}$

$56^{-1} \equiv 56^{59} \equiv x \pmod{93}$

x^{-1}.

subgroup: $H \subset G$

$(H, *)$ satisfies a group.

H is a subgroup of G.

left coset.

Let $g \in G$.

$(H, *)$ a subgroup of $(G, *)$

gH is a left coset

$gH = \{g * h_i \mid h_i \in H\}$

(b) $g \in G$.

Assume. $g * g' = \varepsilon$

$g * g'' = \varepsilon$

g's inverse g', g''

$(g * g') * g'' = \varepsilon * g'' = g''$

$g * g' * g'' = (g * g'') * g = g'$.

$\therefore g'' = g'$. ! Only one inverse for g.

(c) $H = H_1 \cap H_2$.

$\forall x, y \in H$.

$x, y \in H_1 \ \wedge\ x, y \in H_2$.

Closure. $x * y \in H_1 \wedge x * y \in H_2$ ✓.

Associativity → $*$

Neutral → $\varepsilon \in H_1 \wedge \varepsilon \in H_2$

$\varepsilon \in H$.

Invertability $x \in H_1,\ x^{-1} \in H_1$.

$x \in H_2\ \ x^{-1} \in H_2$

$\therefore x^{-1} \in H$.

$\therefore y' \in H$.

$\therefore H$ is a group

$H \subseteq H_1 \subseteq G$.

$\downarrow$

subgroup of G.

gcd (56, 93)

p_i	q_i	s_i	t_i
93		1	0
56	1	0	1
37	1	1	-1
19	1	-1	2
18	1	2	-3
1	18	-3	5
0			

$1 = 56 \times 5 - 93 \times 3$

$= 280 - 279$

$= 1.$

$56^{-1} \equiv 56^{91} \equiv 5 \pmod{93}$

$5 \times 23 \equiv 115 \equiv 22 \pmod{93}$

$\therefore x = 22 + 93k. \quad k \in \mathbb{Z}.$

(e) $7^{62} \pmod{120}$

$120 = 2^3 \times 3 \times 5$

$\phi(120) = 120 \times (1-\frac{1}{2})(1-\frac{1}{3}) \times (1-\frac{1}{5})$

$= 120 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 32.$

$7^{32} \equiv 1 \pmod{120}$

$7^{64} \equiv 1 \pmod{120}$

$7^{63} = 7^{-1} \equiv ? \pmod{120}$

p_i	q_i	s_i	t_i
120		1	0
7	17	0	1
1	7	1	-17
0			

$1 = 120 - 17 \times 7$

$7^{-1} \equiv -17 \pmod{120}$

$\equiv 103 \pmod{120}$

$7^{-2} \equiv 103^2 \pmod{120}$

$\equiv 10609 \pmod{120}$

$= 49 \pmod{120}$

$\therefore 7^{62} \equiv 49 \pmod{120}$

(d) Closure: for $\forall g_1 \in R$, $g_1 \neq -1$.

if $g_1 * g_2 = g_1 + g_2 + g_1 g_2 = -1$.

$g_1 g_2 + g_1 + g_2 + 1 = 0$

$(g_1 + 1)(g_2 + 1) = 0.$

$g_1 = -1$ or $g_2 = -1$.

Contrary to $g_i \neq -1$.

$\therefore g_1 * g_2 \neq -1.$

$g_1 + g_2 + g_1 g_2$ is a real number. not equal to -1 ✓

Associativity

$g_1 * (g_2 * g_3)$

$= g_1 * (g_2 + g_3 + g_2 g_3)$

$= g_1 + g_2 + g_3 + g_2 g_3 + g_1 (g_2 + g_3 + g_2 g_3)$

$= g_1 g_2 + g_1 g_3 + g_2 g_3 + g_1 g_2 g_3 + g_1 + g_2 + g_3)$

$= (g_1 + g_2 + g_1 g_2) * g_3$

$= (g_1 * g_2) * g_3$ ✓

Neutral. $g_1 * 0 = g_1 + 0 + 0 \times g_1 = g_1$

$0 * g_1 = 0 + g_1 + 0 \times g_1 = g_1$

0 neutral element.

Invertibility.

$g_1 + g_1' + g_1 g_1' = 0$

$g_1 + g_1'(g_1 + 1) = 0$

$g_1'(g_1 + 1) = -g_1$

$g_1' = \frac{-g_1}{g_1 + 1}$

$\because g_1 \neq -1.$

$\therefore \frac{-g_1}{g_1 + 1} \in R.$

✓

(ii) $g = 5. \quad e = 0$

$5 + g_2 + 5g_2 = 0 \quad 6g_2 = -5$

$g_2 = \frac{-5}{6}$

(f) $x^7 \equiv 2 \pmod{21}$

$\phi(21) = 21 \times \frac{2}{3} \times \frac{6}{7} = 12$

$x = \sqrt[7]{2} = 2^{7^{-1}} \pmod{21}$

$y \equiv 7^{-1} \pmod{\phi(21)} \equiv 7^{-1} \pmod{12}$

$\gcd(7,12) = 1 = 7 \times 7 - 12 \times 4$

$7^{-1} \pmod{12} \equiv 7 \pmod{12}$

$\therefore y \equiv 7 \pmod{12}$

$x \equiv 2^7 \pmod{21} \equiv 128 \pmod{21}$

$\equiv 2 \pmod{21}$

$x = 2 + 21k \quad (k \in \mathbb{Z})$

(g) $7^{30} \equiv 1 \pmod{31}$

$\phi(31) = 30$

4. (a). Partition: divide Set S ⇓ set of subsets S' such that each element appears only once in S''s element sets

Relation

a collection of order pairs from two sets, with one element from each one of them.

Equivalence relation

Reflexivity $\forall x E(x,x)$

Symmetry $\forall x,y \; E(x,y) \to E(y,x)$

Transitivity $\forall x,y,z \; E(x,y) \vee E(y,z) \to E(x,z)$

Equivalence class.

a subset of form $\{x \in X : E(x,a)\}$

where E is a equivalence relation.

a is an element of X

(b). Assume not form a partition.

Then $\exists a \in E_1, \; a \in E_2$. (not same class)

$\downarrow e_1 \qquad \downarrow e_2$.

$E(a,e_1) \vee E(a,e_2)$

$\to E(e_1,e_2)$

$\to E_1 = E_2$ not true.

Contradiction.

(c). Reflexivity

(i) $xRx \to x - x = 0 \in \mathbb{Z}$.

Symmetry

$xRy \to x - y = k \in \mathbb{Z}$

$yRx \to y - x = -k \in \mathbb{Z}$

Transitivity

$xRy \to x - y = k_1 \in \mathbb{Z}$

$yRz \to y - z = k_2 \in \mathbb{Z}$

$xRz = x - z = x + y + y - z = k_1 + k_2 \in \mathbb{Z}$.

(ii) $\{x \mid x = \sqrt{2} + k \quad (k \in \mathbb{Z})\}$

5.

(a). $\sigma = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 3&1&2&6&7&4&8&5 \end{pmatrix}$ $\quad \tau = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 8&4&6&2&5&7&3&1 \end{pmatrix}$

$\sigma\tau = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 5&6&4&1&7&8&2&3 \end{pmatrix}$ $\quad \tau\sigma = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 6&8&4&7&3&2&1&5 \end{pmatrix}$ $\quad \tau^{-1} = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 8&4&7&2&5&3&6&1 \end{pmatrix}$

(d) Prove: $a \equiv b \pmod{n}$.

$a = k_1 n + m$

$b = k_2 n + m$.

$a^2 = k_1^2 n^2 + 2k_1 nm + m^2$

$b^2 = k_2^2 n^2 + 2k_2 nm + m^2$

Same modulo

(b) $\sigma = (1\ 3\ 2)(4\ 6)(5\ 7\ 8)$

$\tau = (1\ 8)(2\ 4)(3\ 6\ 7)(5)$.

(c) order$(\sigma) = 6$

order$(\tau) = 6$

(d) $\sigma = (1\ 3)(3\ 2)(4\ 6)(5\ 7)(7\ 8)$

$\tau = (1\ 8)(2\ 4)(3\ 6)(6\ 7)$

(e) $\sigma^{2240} = \sigma^{6\times 373+2} = \sigma^2 = (1\ 2\ 3)(5\ 8\ 7)$

$\tau^{10395} = \tau^{6\times 1732+3} = \tau^3 = (1\ 8)(2\ 4)$

(f) σ, τ both even.

(g) ...

7. (a). eigenvalue λ

eigenvector v.

$\lambda v = Av$. $v \neq 0$

(b). $Av - \lambda v = 0$

$|A - \lambda E| = 0$

$$\begin{vmatrix} a-\lambda & b \\ b & -a-\lambda \end{vmatrix} = 0$$

$(a-\lambda)(-a-\lambda) - b^2 = \lambda^2 - a^2 - b^2 = \lambda^2 - 1 = 0$.

$\lambda = 1$ or $\lambda = -1$.

$$\begin{vmatrix} a-1 & b \\ b & -a-1 \end{vmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

v

$(a-1)x + by = 0$

$bx - (a+1)y = 0$

$(a-1)bx + b^2 y = 0$

$b(a-1)x - (a^2-1)y = 0$

(c). $121 \equiv 81 \pmod 4$

$11 \not\equiv 9 \pmod 4$

6. (a) $\begin{cases} x - w = 2 \\ y - z + w = 3 \\ az = 1 \\ y + bw = 0 \end{cases}$

$w = x - 2$

$x + y - z = 5$.

$az = 1$

$y + bx = 2b$.

$\begin{cases} (b-1)x + z = 2b - 5 \\ az = 1 \end{cases}$

$a = 0$ or $b = 1$ $a \neq -\frac{1}{3}$

(b) $a \neq 0$ && $b \neq 1$

$z = \frac{1}{a}$ $(b-1)x = 2b - 5 - \frac{1}{a}$

$x = \frac{2b - 5 - \frac{1}{a}}{b-1}$

$w = \frac{2b-5-\frac{1}{a}}{b-1} - \frac{2b-2}{b-1}$

$= \frac{-3-\frac{1}{a}}{b-1} = -\frac{3+\frac{1}{a}}{b-1}$

$y = 2b - \frac{2b^2 - 5b - \frac{b}{a}}{b-1}$

$= \frac{2b^2 - 2b - 2b^2 + 5b + \frac{b}{a}}{b-1}$.

$= \frac{3b + \frac{b}{a}}{b-1}$.

(c). $b = 1$ $a = -\frac{1}{3}$

$x \in R$.

$z = -3$

$y = -x + 2$

$w = x - 2$

(d) $\begin{cases} x - w = 2. & ① \\ y - z + w = 3 & ② \\ 2z = 1. & ③ \\ y + 5w = 0 & ④ \end{cases}$

① × 5 + ④ $5x - 5w = 10$

$(b^2+a^2-1)y=0 \quad y\in R.$

$x=\dfrac{(a+1)y}{b}$

let $y=1 \quad x=\dfrac{a+1}{b}$

$v=\begin{pmatrix}\frac{a+1}{b}\\1\end{pmatrix}$

$5x+y=10$ ⑤

① + ② $x+y-z=5$

③ $z=\frac{1}{2}$

$x+y=\frac{11}{2}$ ⑥

⑤ - ⑥ $4x=\frac{9}{2}$

$x=\frac{9}{8}$

$y=\frac{44}{8}-\frac{9}{8}=\frac{35}{8}$

$w=\frac{9}{8}-2=-\frac{7}{8}$

$\lambda=-1.$

$\begin{pmatrix}a+1 & b\\ b & -a+1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$

$(a+1)x+by=0$

$bx+(-a+1)y=0$

$(a+1)bx+b^2y=0$

$b(a+1)x+(-a+1)(a+1)=0$

$b^2y-(1-a^2)y=0$

$(b^2-1+a^2)y=0$

$x=\dfrac{(a-1)}{b}y$

let $y=1$ $v=\begin{pmatrix}\frac{a-1}{b}\\1\end{pmatrix}$

(c). $A^2=\begin{pmatrix}a & b\\ b & -a\end{pmatrix}\begin{pmatrix}a & b\\ b & -a\end{pmatrix}$

$=\begin{pmatrix}a^2+b^2 & ab-ab\\ ab-ab & a^2+b^2\end{pmatrix}$

$=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

identity matrix

$A^3=A$