

1.

(a).

2 (when $m = n = 0$)

4 (when $m = n = 1$)

6 (when $m = n = 2$)

8 (when $m = n = 3$)

(b).

28 (when $m = n = 1$)

56 (when $m = n = 2$)

84 (when $m = n = 3$)

112 (when $m = n = 4$)

(c). (i)

$\because d = \gcd(x, y)$

$\therefore d|x, d|y$

Then can derive that $d|mx, d|ny$ with $m, n \in \mathbb{Z}$

So can derive that $d|mx + ny$

$\because m, n, x, y \in \mathbb{Z}$

$\therefore mx + ny \in \mathbb{Z}$

So when some $n = mx + ny$, it can show that $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$

(ii).

$\because d = \gcd(x, y)$

$\therefore d|x, d|y$

Then can derive that $d|mx, d|ny$ with $m, n \in \mathbb{Z}$

So can derive that $d|mx + ny$

when x, y are not both equal to 0:

$\because S_{x,y} \subseteq \{mx + ny : m, n \in \mathbb{Z}\}$ and z be the smallest positive number in $S_{x,y}$

$\therefore z = mx + ny$

Then $d|z$ and it means $k * d = z$ with $k \in \mathbb{Z}$

$\because d > 0$ and $z > 0$

$\therefore k$ must be a positive integer

So $d \leq z$

when $x = y = 0$:

$\because S_{x,y} = \{0 * m + 0 * n : m, n \in \mathbb{Z}\}$

\therefore There is not positive number in $S_{x,y}$

$\therefore z = 0$

$\because d = \gcd(0, 0) = 0$

$\therefore z = d$

$\therefore d \leq z$

(d). (i).

The Euclidean division of x by z may be written $x = qz + r$ with $0 \leq r < z, q \in \mathbb{Z}$

$\therefore z$ is in $S_{x,y}$

\therefore The remainder r is in $S_{x,y}$ because:

$$r = x - qz$$

$$= x - q(mx + ny) \text{ with } m, n \in \mathbb{Z}$$

$$= (1 - qm)x + (-qn)y$$

$\therefore r = (1 - qm)x + (-qn)y$ has the same form with $r = mx + ny$

It means r is in $S_{x,y}$

$\therefore z$ is the smallest positive number in $S_{x,y}$ and $0 \leq r < z$

$$\therefore r = 0$$

\therefore then $x = qz$ with $q \in \mathbb{Z}$

$$\therefore z|x$$

The Euclidean division of y by z may be written $y = qz + r$ with $0 \leq r < z, q \in \mathbb{Z}$

$\therefore z$ is in $S_{x,y}$

\therefore The remainder r is in $S_{x,y}$ because:

$$r = y - qz$$

$$= y - q(mx + ny) \text{ with } m, n \in \mathbb{Z}$$

$$= (1 - qn)y + (-qm)x$$

$\therefore r = (1 - qn)y + (-qm)x$ has the same form with $r = mx + ny$

It means r is in $S_{x,y}$

$\therefore z$ is the smallest positive number in $S_{x,y}$ and $0 \leq r < z$

$$\therefore r = 0$$

\therefore then $y = qz$ with $q \in \mathbb{Z}$

$$\therefore z|y$$

(ii).

$$\therefore z|x, z|y$$

Then can derive that $z|mx, z|ny$ with $m, n \in \mathbb{Z}$

So can derive that $z|mx + ny$

$\therefore z$ is one of the common divisor of x, y

$$\therefore d = \gcd(x, y)$$

$$\therefore z * k = d \text{ with } k \in \mathbb{N}$$

$$\therefore z \leq d$$

2.

(a).

for $x, y, m, n \in \mathbb{Z}$, have $S_{x,y} = \{mx + ny : mx + ny > 0\}$

if $\gcd(x, y) = 1$, according to the theme of Bezout's identity: $\gcd(x, y) = 1$ is one element in $S_{x,y}$

$$\therefore wx = {}_{(y)}1 \text{ equal to } wx = {}_{(y)}mx + ny$$

$\therefore y|(w-m)x - ny$
 $\because n \in \mathbb{Z}$
 $\therefore y|ny$
 $\therefore y|(w-m)x - ny$ can derive to $y|(w-m)x$
 if $w = m$: $y|(w-m)x$ equal to $y|0$ that is hold.

So there is at least one $w \in [0, y] \cap \mathbb{N}$ such that $wx = {}_{(y)}1$ when w
 $= m$ with the interger m : $0 \leq m < y$

(b).
 $\because y|kx$
 according to the definition of Divisibility, there exist some $a \in \mathbb{Z}$ that $a *$
 $y = kx$, so $a = k \frac{x}{y}$ with $a, x, y, kx \in \mathbb{Z}$
 $\because kx, x \in \mathbb{Z}$
 $\therefore k \in \mathbb{Z}$
 $\because \gcd(x, y) = 1$
 $\therefore x$ and y are relatively prime and $\frac{x}{y} \notin \mathbb{Z}$
 $\because \frac{x}{y} \notin \mathbb{Z}, k \frac{x}{y}, k, x \in \mathbb{Z}$
 \therefore exist k equal to $b * y$ with $b \in \mathbb{Z}$ that $b * y * \frac{x}{y} = b * x \in \mathbb{Z}$
 $\because y > 1$ and $y \in \mathbb{Z}$
 $\therefore y|by$ is hold
 $\therefore y|k$

(c).
 Assume there are two $w \in [0, y) \cap \mathbb{N}$ such that $wx = {}_{(y)}1$ and $w_1 \geq w_2$

$\because wx = {}_{(y)}1$
 $\therefore w_1x = {}_{(y)}1, w_2x = {}_{(y)}1$
 $\therefore y|w_1x - 1, y|w_2x - 1$
 $\therefore y|(w_1x - 1) - (w_2x - 1)$
 and it equal to $y|(w_1 - w_2)x$
 $\because d = \gcd(x, y) = 1$
 according to the prove in (2): $y|(w_1 - w_2)x$ equal to $y|(w_1 - w_2)$
 $\because 0 \leq w_2 \leq w_1 \leq y$
 $\therefore 0 \leq (w_1 - w_2) \leq y$
 $\because 0 \leq (w_1 - w_2) \leq y$ and $y|(w_1 - w_2)$
 $\therefore w_1 - w_2 = 0$
 $\therefore w_1 = w_2$

so there is at most one $w \in [0, y) \cap N$ such that $wx =_{(y)} 1$

3.

in order to prove: $\frac{3}{2}(n + (m \% n)) < m + n$

Equal to prove: $3n + 3(m \% n) < 2m + 2n$

equal to prove: $n + 3(m \% n) < 2m$

$\because 0 \leq (m \% n) < n$

suppose: $r = (m \% n)$

$\therefore m = qn + r$ with $q \geq 1$ because $m \geq n$

\therefore equal to prove: $n + 3r < 2qn + 2r$

and it equal to prove: $n + r < 2qn$

Because we want to prove for all $m, n \in N_{>0}$ with m

$\geq n$, so the prove still stand when m take its smallest values

$= 1$

\therefore the prove equal to $n + r < 2n$

and it equal to prove: $r < n$

$\because 0 \leq r = (m \% n) < n$

$\therefore \frac{3}{2}(n + (m \% n)) < m + n$

4.

(a).

$A \cap \emptyset$

$= A \cap (A \cap A^c)$ Complement with \cap

$= (A \cap A) \cap A^c$ Associativity of \cap

$= A \cap A^c$ Idempotence of \cap

$= \emptyset$ Complement with \cap

(b).

$(A \setminus C) \cup (B \setminus C)$

$= (A \cap C^c) \cup (B \setminus C)$ Definition of \setminus

$= (A \cap C^c) \cup (B \cap C^c)$ Definition of \setminus

$= (C^c \cap A) \cup (B \cap C^c)$ Commutativity of \cap

$= (C^c \cap A) \cup (C^c \cap B)$ Commutativity of \cap

$= C^c \cap (A \cup B)$ Distributivity of \cap over \cup

$= (A \cup B) \cap C^c$ Commutativity of \cap

$= (A \cup B) \setminus C$ Definition of \setminus

(c).

$A \oplus \mathcal{U}$

$= (A \cap \mathcal{U}^c) \cup (A^c \cap \mathcal{U})$ Definition of \oplus

$$\begin{aligned}
&= (A \cap (\mathbf{U}^c \cap \mathbf{U})) \cup (A^c \cap \mathbf{U}) \quad \text{Identity of } \cap \\
&= (A \cap (\mathbf{U} \cap \mathbf{U}^c)) \cup (A^c \cap \mathbf{U}) \quad \text{Commutativity of } \cap \\
&= (A \cap \emptyset) \cup (A^c \cap \mathbf{U}) \quad \text{Complement with } \cap \\
&= (A \cap \emptyset) \cup A^c \quad \text{Identity of } \cap \\
&= A^c \cup (A \cap \emptyset) \quad \text{Commutativity of } \cup \\
&= A^c \cup (A \cap (A \cap A^c)) \quad \text{Complement with } \cap \\
&= A^c \cup ((A \cap A) \cap A^c) \quad \text{Associativity of } \cap \\
&= A^c \cup (A \cap A^c) \quad \text{Idempotence of } \cap \\
&= A^c \cup \emptyset \quad \text{Complement with } \cap \\
&= A^c \quad \text{Identity of } \cap
\end{aligned}$$

(d).

$$\begin{aligned}
&\text{Because: } (A \cap B) \cup (A \cap B^c) \cup (A^c \cap B) \cup (A^c \cap B^c) \\
&= ((A \cap B) \cup (A \cap B^c)) \cup ((A^c \cap B) \cup (A^c \cap B^c)) \quad \text{just add bracket} \\
&= ((A \cap (B \cup B^c)) \cup ((A^c \cap B) \cup (A^c \cap B^c))) \quad \text{Distributivity of } \cap \text{ over } \cup \\
&= ((A \cap (B \cup B^c)) \cup (A^c \cap (B \cup B^c))) \quad \text{Distributivity of } \cap \text{ over } \cup \\
&= ((A \cap \mathbf{U}) \cup (A^c \cap (B \cup B^c))) \quad \text{Complement with } \cup \\
&= ((A \cap \mathbf{U}) \cup (A^c \cap \mathbf{U})) \quad \text{Complement with } \cup \\
&= (A \cup (A^c \cap \mathbf{U})) \quad \text{Identity of } \cap \\
&= (A \cup A^c) \quad \text{Identity of } \cap \\
&= \mathbf{U} \quad \text{Complement with } \cup
\end{aligned}$$

$$\begin{aligned}
&\text{So: } (A^c \cap B^c) \\
&= ((A \cap B) \cup (A \cap B^c) \cup (A^c \cap B))^c \quad \text{Complement with } \cup \\
&= \text{my_prove}
\end{aligned}$$

So:

$$\begin{aligned}
&(A \cup B)^c \\
&= ((A \cap \mathbf{U}) \cup B)^c \quad \text{Identity of } \cap \\
&= ((A \cap (B \cup B^c)) \cup B)^c \quad \text{Complement with } \cup \\
&= ((A \cap (B \cup B^c)) \cup (B \cap \mathbf{U}))^c \quad \text{Identity of } \cap \\
&= ((A \cap (B \cup B^c)) \cup (B \cap (A \cup A^c)))^c \quad \text{Complement with } \cup \\
&= (((A \cap B) \cup (A \cap B^c)) \cup (B \cap (A \cup A^c)))^c \quad \text{Distributivity of } \cap \text{ over } \cup \\
&= (((A \cap B) \cup (A \cap B^c)) \cup ((B \cap A) \cup (B \cap A^c)))^c \quad \text{Distributivity of } \cap \text{ over } \cup \\
&= (((A \cap B) \cup (A \cap B^c)) \cup ((A \cap B) \cup (B \cap A^c)))^c \quad \text{Commutativity of } \cap \\
&= (((A \cap B) \cup (A \cap B^c) \cup (A \cap B)) \cup (B \cap A^c))^c \quad \text{Associativity of } \cup \\
&= (((A \cap B) \cup (A \cap B)) \cup (A \cap B^c)) \cup (B \cap A^c))^c \quad \text{Commutativity of } \cup \\
&= (((A \cap B) \cup (A \cap B^c)) \cup (B \cap A^c))^c \quad \text{Idempotence of } \cup \\
&= ((A \cap B) \cup (A \cap B^c) \cup (A^c \cap B))^c \quad \text{Commutativity of } \cap \\
&= A^c \cap B^c \quad \text{my_prove}
\end{aligned}$$

(e).

$$\begin{aligned}
&((A \cup B) \cap (B \cup C)) \cap (C \cup A) \\
&= ((B \cup A) \cap (B \cup C)) \cap (C \cup A) \quad \text{Commutativity of } \cup
\end{aligned}$$

$$\begin{aligned}
&= ((B \cup A) \cap (B \cup C)) \cap (A \cup C) \quad \text{Commutativity of } \cup \\
&= (A \cup C) \cap ((B \cup A) \cap (B \cup C)) \quad \text{Commutativity of } \cap \\
&= (A \cup C) \cap (B \cup (A \cap C)) \quad \text{Distributivity of } \cup \text{ over } \cap \\
&= ((A \cup C) \cap B) \cup ((A \cup C) \cap (A \cap C)) \quad \text{Distributivity of } \cap \text{ over } \cup \\
&= (B \cap (A \cup C)) \cup ((A \cup C) \cap (A \cap C)) \quad \text{Commutativity of } \cap \\
&= ((B \cap A) \cup (B \cap C)) \cup ((A \cup C) \cap (A \cap C)) \quad \text{Distributivity of } \cap \text{ over } \cup \\
&= ((A \cap B) \cup (B \cap C)) \cup ((A \cup C) \cap (A \cap C)) \quad \text{Commutativity of } \cap \\
&= ((A \cap B) \cup (B \cap C)) \cup (((A \cup C) \cap A) \cap C) \quad \text{Associativity of } \cap \\
&= ((A \cap B) \cup (B \cap C)) \cup ((A \cap (A \cup C)) \cap C) \quad \text{Commutativity of } \cap \\
&= ((A \cap B) \cup (B \cap C)) \cup (A \cap C) \quad \text{Duality} \\
&= ((A \cap B) \cup (B \cap C)) \cup (C \cap A) \quad \text{Commutativity of } \cap
\end{aligned}$$

5.

(a).

show the counterexample:

$$\text{when } X = \{0\}, Y = \{1\}, X \cup Y = \{0,1\}$$

$$X^* = \{\lambda, 0, 00, 000, \dots, 00 \dots 000\}$$

$$Y^* = \{\lambda, 1, 11, 111, \dots, 11 \dots 111\}$$

$$(X \cup Y)^* = \{\lambda, 0, 1, 00, 11, 01, 10, 000, 111, \dots, 11 \dots 111\}$$

$$X^* \cup Y^* = \{\lambda, 0, 1, 00, 11, 000, 111, \dots, 11 \dots 111\}$$

So $(X \cup Y)^$ exist element like 01 or 10 are not in set $X^* \cup Y^*$*

(b).

show the counterexample:

$$\text{when } X = \{11\}, Y = \{111\}, X \cap Y = \{11, 111\}$$

$$X^* = \{\lambda, 11, 1111, 111111, \dots, 11 \dots 1111\}$$

$$Y^* = \{\lambda, 111, 111111, \dots, 11 \dots 111\}$$

$$(X \cap Y)^* = \{\lambda, 11, 111, 1111, 11111, 111111, \dots, 11 \dots 111\}$$

$$X^* \cap Y^* = \{\lambda, 11, 111, 1111, 111111, \dots, 11 \dots 111\}$$

So $(X \cap Y)^$ exist element like $\Sigma^5 = 11111$ are not in set $X^* \cap Y^*$*

(c).

According to the set's Concatenation:

$$XY = \{xy: x \in X \text{ and } y \in Y\}$$

$$XZ = \{xz: x \in X \text{ and } z \in Z\}$$

$$XY \cup XZ = \{xa: x \in X \text{ and } a \in Y \text{ or } a \in Z\}$$

$$X(Y \cup Z) = \{xb: x \in X \text{ and } b \in Y \text{ or } b \in Z\}$$

$$\because \text{set } X, Y, Z \subseteq \Sigma^*$$

$$\therefore XY \cup XZ \text{ and } X(Y \cup Z) \text{ have the same domain}$$

$$\therefore XY \cup XZ = X(Y \cup Z)$$

6.

(a).

according to the Definition of function, $f : S \rightarrow T$, that is, for all $s \in S$ there is exactly one $t \in T$ such that $(s, t) \in f$.

$$\therefore f_1: a \mapsto 0, b \mapsto 0, c \mapsto 0$$

$$f_2: a \mapsto 1, b \mapsto 0, c \mapsto 0$$

$$f_3: a \mapsto 0, b \mapsto 1, c \mapsto 0$$

$$f_4: a \mapsto 0, b \mapsto 0, c \mapsto 1$$

$$f_5: a \mapsto 1, b \mapsto 1, c \mapsto 0$$

$$f_6: a \mapsto 1, b \mapsto 0, c \mapsto 1$$

$$f_7: a \mapsto 0, b \mapsto 1, c \mapsto 1$$

$$f_8: a \mapsto 1, b \mapsto 1, c \mapsto 1$$

(b).

$\therefore \text{Pow}(a, b, c)$ is the set of all subsets of $\{a, b, c\}$

\therefore the subset of $\{a, b, c\}$ means it will take one part of element in the $\{a, b, c\}$

\therefore so it can consider as take one part and do not take others part, which is same as 1 means take its element and 0 means not take its element. And it is similar to the definition of function that $s \in S$ only has one t that $(s, t) \in R$

\therefore it all operate the same set about $\{a, b, c\}$, and 1 and 0 means whether take it

$\therefore \text{Pow}(a, b, c)$'s element has the same amount of the result of (a) about $2^{|3|}$
 $= 8$

(c).

$\therefore \{w \in \{0,1\}^* : \text{length}(w) = 3\}$ are the set of w contain the subset three ordered element which is either 0 or 1, and the amount of set is three.

\therefore the order of the set can be seen as $\{a, b, c\}$

\therefore so it can consider as the subset contain the element with order $\{a, b, c\}$ and a, b, c can take the values of 0 or 1

\therefore set of $\{w \in \{0,1\}^* : \text{length}(w) = 3\}$ has the element of same amount of the result of (a) about $2^{|3|} = 8$

7.

8.

(a).

$$\therefore R_1, R_2, R_3 \subseteq S \times S$$

$$\therefore R_1; R_2 \subseteq S \times S, R_1; R_2 \subseteq S \times S$$

$$\therefore R_1; R_2 \subseteq S \times S, R_3 \subseteq S \times S$$

$$\therefore (R_1; R_2); R_3 \subseteq S \times S$$

$$\therefore (R_1; R_2); R_3 = \{(a, c) : \text{there is a } b_1 \in S \text{ with } (a, b_1) \in (R_1; R_2) \text{ and } (b_1, c) \in R_3\}$$

$$= \{(a, c) : \text{there is a } b_2 \in S \text{ with } (a, b_2) \in R_1 \text{ and } (b_2, b_1) \in R_2 \text{ and } (b_1, c) \in R_3\}$$

apply the same b_2, b_1 in the $R_1; (R_2; R_3)$

$$\begin{aligned}
& \therefore R_1; (R_2; R_3) = \{(a, c) : \text{there is a } b_2 \in S \text{ with } (a, b_2) \in R_1 \text{ and } (b_2, c) \\
& \quad \in (R_2; R_3)\} \\
& = \{(a, c) : \text{there is } (a, b_2) \in R_1 \text{ and with a } b_1 \in S \text{ that } (b_2, b_1) \in R_2 \text{ and } (b_1, c) \\
& \quad \in R_3\} \\
& \therefore (R_1; R_2); R_3 = R_1; (R_2; R_3)
\end{aligned}$$

(b).

$$\therefore R_1, R_2, R_3 \subseteq S \times S$$

according to the properties of Binary Relations R
 $\subseteq S \times S$ has reflexive: for

all $x \in S$: $(x, x) \in R$

$$\therefore I; R_1 = \{(a, c) : \text{there is a } b \in S \text{ with } (a, b) \in I \text{ and } (b, c) \in R_1\}$$

$$\therefore I = (x, x) : x \in R$$

$$\therefore a = b \text{ and } I; R_1 = \{(a, c) : \text{there is a } a \in S \text{ with } (a, a) \in I \text{ and } (a, c) \in R_1\}$$

$$\text{and } R_1; I = \{(a, c) : \text{there is a } b \in S \text{ with } (a, b) \in R_1 \text{ and } (b, c) \in I\}$$

$$\therefore I = (x, x) : x \in R$$

$$\therefore b = c \text{ and } R_1; I = \{(a, c) : \text{there is a } c \in S \text{ with } (a, c) \in R_1 \text{ and } (c, c) \in I\}$$

$$\therefore R_1 = \{(a, c)\}$$

$$\therefore I; R_1 = R_1; I = R_1$$

(c).

$$\therefore R_1, R_2, R_3 \subseteq S \times S$$

$$\therefore (R_1 \cup R_2) \subseteq S \times S, R_1; R_2 \subseteq S \times S, R_1; R_3 \subseteq S \times S, R_2; R_3 \subseteq S \times S$$

$$\therefore (R_1 \cup R_2) \subseteq S \times S, R_3 \subseteq S \times S$$

$$\therefore (R_1 \cup R_2); R_3 \subseteq S \times S$$

$$\therefore (R_1 \cup R_2); R_3 = \{(a, c) : \text{there is a } b \in S \text{ with } (a, b) \in (R_1 \cup R_2) \text{ and } (b, c) \in R_3\}$$

$$\therefore (R_1; R_3) \cup (R_2; R_3) = \{(a, c) : \text{there is a } b_3 \in S \text{ with } (a, b_3) \in R_1 \text{ and } (b_3, c) \in R_3 \text{ and there is a } b_4 \in S \text{ with } (a, b_4) \in R_2 \text{ and } (b_4, c) \in R_3\}$$

$$\therefore b, b_3, b_4 \in S, \text{ and } (a, b) \in (R_1 \cup R_2), (a, b_3) \in R_1, (a, b_4) \in R_2$$

$$\therefore b = b_3 \cup b_4$$

$$\therefore (R_1 \cup R_2); R_3 = (R_1; R_3) \cup (R_2; R_3)$$

(d).

$$\therefore R_1, R_2, R_3 \subseteq S \times S$$

$$\therefore (R_2 \cap R_3) \subseteq S \times S, R_1; R_2 \subseteq S \times S, R_1; R_3 \subseteq S \times S, R_2; R_3 \subseteq S \times S$$

$$\therefore (R_2 \cap R_3) \subseteq S \times S, R_1 \subseteq S \times S$$

$$\therefore R_1; (R_2 \cap R_3) \subseteq S \times S$$

$$\therefore R_1; (R_2 \cap R_3) = \{(a, c) : \text{there is a } b \in S \text{ with } (a, b) \in R_1 \text{ and } (b, c) \in (R_2 \cap R_3)\}$$

$$\therefore (R_1; R_2) \cap (R_1; R_3) = \{(a, c) : \text{there is a } b_5 \in S \text{ with } (a, b_5) \in R_1 \text{ and } (b_5, c) \in R_2 \text{ and there is a } b_6 \in S \text{ with } (a, b_6) \in R_1 \text{ and } (b_6, c) \in R_3\}$$

$$\therefore b, b_5, b_6 \in S, \text{ and } (b, c) \in (R_2 \cap R_3), (b_5, c) \in R_2, (b_6, c) \in R_3$$

$$\therefore b = b_5 \cap b_6$$

$$\therefore R_1; (R_2 \cap R_3) = (R_1; R_2) \cap (R_1; R_3)$$