1.
(a).
2(whenm = 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)
$\because d = gcd(x, y)$
$\therefore d|x, d|y$
$Then\ can\ derive\ that\ d|mx, d|ny\ \ with\ m, n \in Z$
$So\ can\ derive\ that\ d|mx + ny$
$\because\ m, n, x, y \in Z$
$\therefore\ mx + ny \in Z$
$So\ when\ some\ n = mx + ny, it\ can\ show\ that\ S_{x,y} \subseteq \{n :\ n \in Z\ and\ d|n\}$

(ii).
$\because d = gcd(x, y)$
$\therefore d|x, d|y$
$Then\ can\ derive\ that\ d|mx, d|ny\ \ with\ m, n \in Z$
$So\ can\ derive\ that\ d|mx + ny$
$when\ x, y\ are\ not\ both\ equal\ to\ 0:$
$\because\ S_{x,y} \subseteq \{mx + ny :\ m, n \in Z\}\ and\ z\ be\ the\ smallest\ positive\ number\ in\ \ S_{x,y}$
$\therefore\ z = mx + ny$
$Then\ d|z\ and\ it\ means\ k * d\ \ = z\ \ with\ k \in Z$
$\because\ d > 0\ and\ z > 0$
$\therefore\ k\ must\ be\ a\ positive\ integer$
$So\ d \leq z$
$when\ x = y =\ 0:$
$\because\ \ S_{x,y} = \{0*\mathrm{m} + 0*\mathrm{n}: \mathrm{m}, \mathrm{n} \in Z\}$
$\therefore There\ is\ not\ positive\ number\ in\ \ S_{x,y}$
$\therefore\ z = 0$
$\because\ d = gcd(0,0) = 0$
$\therefore\ z = d$
$\therefore\ \ d \leq z$

(d). (i).

$The\ Euclidean\ division\ of\ x\ by\ z\ may\ be\ written\ x = qz + r \quad with\ 0 \le r < z, q \in Z$

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

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

$r = x - qz$

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

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

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

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

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

$\therefore\ r = 0$

$\therefore\ then\ x = qz\ \ with\ q \in Z$

$\therefore\ z|x$

$The\ Euclidean\ division\ of\ x\ by\ z\ may\ be\ written\ y = qz + r \quad with\ 0 \le r < z, q \in Z$

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

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

$r = y - qz$

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

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

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

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

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

$\therefore\ r = 0$

$\therefore\ then\ y = qz\ \ with\ q \in Z$

$\therefore\ z|y$

(ii).

$\because z|x, z|y$

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

$So\ can\ derive\ that\ \mathrm{z}|mx + ny$

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

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

$\therefore\ z * k = d\ \ with\ k \in N$

$\therefore\ z \le d$

2.

(a).

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

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

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

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

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

(b).
$\because\ y|kx$
$according\ to\ the\ definition\ of\ Divisibility, there\ exist\ some\ a \in Z\ that\ a *$
$y = kx, so\ a = k\frac{x}{y}\ with\ a,x,y,kx \in Z$

$\because\ kx, x \in Z$
$\therefore\ k \in Z$
$\because\ gcd(x,y) = 1$
$\therefore\ x\ and\ y\ are\ relatively\ prime\ and\ \frac{x}{y} \notin z$
$\because \frac{x}{y} \notin z, k\frac{x}{y}, k, x \in Z$
$\therefore\ exist\ k\ equal\ to\ b*y\ with\ b \in Z\ that\ b*y*\frac{x}{y} = b*x \in Z$
$\because\ y > 1\ and\ y \in Z$
$\therefore\ y|by\ is\ hold$
$\therefore\ y|k$

(c).

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

$\because\ wx =_{(y)} 1$

$\therefore\ w_1x =_{(y)} 1, w_2x =_{(y)} 1$

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

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

3.

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

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

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

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

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

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

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

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

$Because\ we\ want\ to\ prove\ for\ all\ m, n \in N_{>0}\ with\ m \geq n, so\ the\ prove\ still\ stand\ when\ m\ take\ its\ smallest\ values = 1$

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

$and\ it\ equal\ to\ prove: r < n$

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

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

4.

(a).

A ∩ ∅

= A ∩ (A ∩ A^c)   Complement with ∩

= (A ∩ A) ∩ A^c Associativity of ∩

= A ∩ A^c Idempotence of ∩

= ∅ Complement with ∩

(b).

(A \ C) ∪ (B \ C)

= (A ∩ C^c) ∪ (B \ C)   Definition of \

= (A ∩ C^c) ∪ (B ∩ C^c)   Definition of \

= (C^c ∩ A) ∪ (B ∩ C^c)   Commutatitivity of ∩

= (C^c ∩ A) ∪ (C^c ∩ B)   Commutatitivity of ∩

= C^c ∩ (A ∪ B)   Distributivity of ∩ over ∪

= (A ∪ B) ∩ C^c Commutatitivity of ∩

= (A ∪ B) \ C   Definition of \

(c).

A ⊕ $\boldsymbol{\mathcal{U}}$

= (A ∩ $\boldsymbol{\mathcal{U}}^c$) ∪ ($A^c$ ∩ $\boldsymbol{\mathcal{U}}$)   Definition of ⊕

$= (A \cap (\mathcal{U}^c \cap \mathcal{U})) \cup (A^c \cap \mathcal{U})$ Identity of ∩
$= (A \cap (\mathcal{U} \cap \mathcal{U}^c)) \cup (A^c \cap \mathcal{U})$ Commutatitivity of ∩
$= (A \cap \emptyset) \cup (A^c \cap \mathcal{U})$ Complement with ∩
$= (A \cap \emptyset) \cup A^c$ Identity of ∩
$= A^c \cup (A \cap \emptyset)$ Commutatitivity of ∪
$= A^c \cup (A \cap (A \cap A^c))$ Complement with ∩
$= A^c \cup ((A \cap A) \cap A^c)$ Associativity of ∩
$= A^c \cup (A \cap A^c)$ Idempotence of ∩
$= A^c \cup \emptyset$ Complement with ∩
$= A^c$ Identity of ∩

(d).
Because: $(A \cap B) \cup (A \cap B^c) \cup (A^c \cap B) \cup (A^c \cap B^c)$
$= ((A \cap B) \cup (A \cap B^c)) \cup ((A^c \cap B) \cup (A^c \cap B^c))$ just add bracket
$= ((A \cap (B \cup B^c)) \cup ((A^c \cap B) \cup (A^c \cap B^c))$ Distributivity of ∩ over ∪
$= ((A \cap (B \cup B^c)) \cup (A^c \cap (B \cup B^c)))$ Distributivity of ∩ over ∪
$= ((A \cap \mathcal{U}) \cup (A^c \cap (B \cup B^c)))$ Complement with ∪
$= ((A \cap \mathcal{U}) \cup (A^c \cap \mathcal{U}))$ Complement with ∪
$= (A \cup (A^c \cap \mathcal{U}))$ Identity of ∩
$= (A \cup A^c)$ Identity of ∩
$= \mathcal{U}$ Complement with ∪

So: $(A^c \cap B^c)$
$= ((A \cap B) \cup (A \cap B^c) \cup (A^c \cap B))^c$ Complement with ∪
=my_prove

So:
$(A \cup B)^c$
$= ((A \cap \mathcal{U}) \cup B)^c$ Identity of ∩
$= ((A \cap (B \cup B^c)) \cup B)^c$ Complement with ∪
$= ((A \cap (B \cup B^c)) \cup (B \cap \mathcal{U}))^c$ Identity of ∩
$= ((A \cap (B \cup B^c)) \cup (B \cap (A \cup A^c)))^c$ Complement with ∪
$= (((A \cap B) \cup (A \cap B^c)) \cup (B \cap (A \cup A^c)))^c$ Distributivity of ∩ over ∪
$= (((A \cap B) \cup (A \cap B^c)) \cup ((B \cap A) \cup (B \cap A^c)))^c$ Distributivity of ∩ over ∪
$= (((A \cap B) \cup (A \cap B^c)) \cup ((A \cap B) \cup (B \cap A^c)))^c$ Commutatitivity of ∩
$= (((A \cap B) \cup (A \cap B^c) \cup (A \cap B)) \cup (B \cap A^c))^c$ Associativity of ∪
$= ((((A \cap B) \cup (A \cap B)) \cup (A \cap B^c)) \cup (B \cap A^c))^c$ Commutatitivity of ∪
$= (((A \cap B) \cup (A \cap B^c)) \cup (B \cap A^c))^c$ Idempotence of ∪
$= ((A \cap B) \cup (A \cap B^c) \cup (A^c \cap B))^c$ Commutatitivity of ∩
$= A^c \cap B^c$ my_prove

(e).
$((A \cup B) \cap (B \cup C)) \cap (C \cup A)$
$= ((B \cup A) \cap (B \cup C)) \cap (C \cup A)$ Commutatitivity of ∪

= ((B ∪ A) ∩ (B ∪ C)) ∩ (A ∪ C)   Commutatitivity of ∪
= (A ∪ C) ∩ ((B ∪ A) ∩ (B ∪ C))   Commutatitivity of ∩
= (A ∪ C) ∩ (B ∪ (A ∩ C))   Distributivity of ∪ over ∩
= ((A ∪ C) ∩ B) ∪ ((A ∪ C) ∩ (A ∩ C))Distributivity of ∩ over ∪
= (B ∩ (A ∪ C)) ∪ ((A ∪ C) ∩ (A ∩ C))Commutatitivity of ∩
= ((B ∩ A) ∪ (B ∩ C)) ∪ ((A ∪ C) ∩ (A ∩ C))   Distributivity of ∩ over ∪
= ((A ∩ B) ∪ (B ∩ C)) ∪ ((A ∪ C) ∩ (A ∩ C))   Commutatitivity of ∩
= ((A ∩ B) ∪ (B ∩ C)) ∪ (((A ∪ C) ∩ A) ∩ C)   Associativity of ∩
= ((A ∩ B) ∪ (B ∩ C)) ∪ ((A ∩ (A ∪ C)) ∩ C)   Commutatitivity of ∩
= ((A ∩ B) ∪ (B ∩ C)) ∪ (A ∩ C)   Duality
= ((A ∩ B) ∪ (B ∩ C)) ∪ (C ∩ A)   Commutatitivity of ∩

5.
(a).
$show\ the\ counterexample$:
$when\ X = \{0\}, Y = \{1\}, X \cup Y = \{0,1\}$
$X^* = \{\lambda, 0,00,000, \dots ,00 \dots 000\}$
$Y^* = \{\lambda, 1,11,111, \dots ,11 \dots 111\}$
$(X \cup Y)^* = \{\lambda, 0,1,00,11,01,10,000,111, \dots ,11 \dots 111\}$
$X^* \cup Y^* = \{\lambda, 0,1,00,11,000,111, \dots ,11 \dots 111\}$
$So\ (X \cup Y)^*\ exist\ element\ like\ 01\ or\ 10\ are\ not\ in\ set\ X^* \cup Y^*$

(b).
$show\ the\ counterexample$:
$when\ X = \{11\}, Y = \{111\}, X \cap Y = \{11,111\}$
$X^* = \{\lambda, 11,1111,111111, \dots ,11 \dots 1111\}$
$Y^* = \{\lambda, 111,111111, \dots ,11 \dots 111\}$
$(X \cap Y)^* = \{\lambda, 11,111,1111,11111,111111, \dots ,11 \dots 111\}$
$X^* \cap Y^* = \{\lambda, 11,111,1111,111111, \dots ,11 \dots 111\}$
$So\ (X \cup Y)^*\ exist\ element\ like\ \Sigma^5 = 11111\ are\ not\ in\ set\ X^* \cap Y^*$

(c).
$According\ to\ the\ set's\ Concatenation$:
$\mathrm{XY} = \{\mathrm{xy}: \mathrm{x} \in \mathrm{X}\ \mathrm{and}\ \mathrm{y} \in \mathrm{Y}\}$
$XZ = \{xz: x \in X\ and\ z \in Z\}$
$XY \cup XZ = \{\mathrm{xa}: \mathrm{x} \in \mathrm{X}\ \mathrm{and}\ \mathrm{a} \in \mathrm{Y}\ \mathrm{or}\ \mathrm{a} \in \mathrm{Z}\}$
$X(Y \cup Z) = \{\mathrm{xb}: \mathrm{x} \in \mathrm{X}\ \mathrm{and}\ \mathrm{b} \in \mathrm{Y}\ \mathrm{or}\ \mathrm{b} \in \mathrm{Z}\}$
$\because\ set\ X, Y, Z\ \subseteq \Sigma^*$
$\therefore\ XY \cup XZ\ and\ X(Y \cup Z)\ have\ the\ same\ domain$
$\therefore\ XY \cup XZ = X(Y \cup Z)$

6.
(a).

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

$\therefore f_1: \mathrm{a} \mapsto 0, \mathrm{b} \mapsto 0, \mathrm{c} \mapsto 0$
$f_2: \mathrm{a} \mapsto 1, \mathrm{b} \mapsto 0, \mathrm{c} \mapsto 0$
$f_3: \mathrm{a} \mapsto 0, \mathrm{b} \mapsto 1, \mathrm{c} \mapsto 0$
$f_4: \mathrm{a} \mapsto 0, \mathrm{b} \mapsto 0, \mathrm{c} \mapsto 1$
$f_5: \mathrm{a} \mapsto 1, \mathrm{b} \mapsto 1, \mathrm{c} \mapsto 0$
$f_6: \mathrm{a} \mapsto 1, \mathrm{b} \mapsto 0, \mathrm{c} \mapsto 1$
$f_7: \mathrm{a} \mapsto 0, \mathrm{b} \mapsto 1, \mathrm{c} \mapsto 1$
$f_8: \mathrm{a} \mapsto 1, \mathrm{b} \mapsto 1, \mathrm{c} \mapsto 1$

(b).
$\because Pow(a, b, c)\ is\ the\ set\ of\ all\ subsets\ of\ \{a, b, c\}$
$\therefore the\ subset\ of\ \{a, b, c\} means\ it\ will\ take\ one\ part\ of\ element\ in\ the\ \{a, b, c\}$
$\therefore$ $so\ it\ can\ consider\ as\ take\ one\ part\ and\ do\ not\ take\ others\ part, which\ is\ same\ as\ 1\ means\ take\ its\ element\ and\ 0\ means\ not\ take\ its\ element. And\ it\ is\ similar\ to\ the\ definition\ of$ $function$ $that\ s \in S\ only\ has\ one\ t\ that\ (s, t) \in R$
$\because it\ all\ operate\ the\ same\ set\ about\ \{a, b, c\}, and\ 1\ and\ 0\ means\ whether\ take\ it$
$\therefore Pow(a, b, c)'s\ element\ has\ the\ same\ amount\ of\ the\ result\ of\ (a)\ about\ 2^{|3|} = 8$

(c).
$\because \{ w \in \{0,1\}^* : length(w) = 3 \}$ 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 $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$
$\therefore$ so it can consider as the sutset contain the element with order $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$ and a, b, c can take the values of 0 or 1
$\therefore$ set of $\{ w \in \{0,1\}^* : length(w) = 3 \}$ has the *element* of *same amount of* the *result of* (a) *about* $2^{|3|} = 8$

7.

8.
(a).
$\because \mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3 \subseteq \mathrm{S} \times \mathrm{S}$
$\therefore \mathrm{R}_1; \mathrm{R}_2 \subseteq \mathrm{S} \times \mathrm{S}, \mathrm{R}_1; \mathrm{R}_2 \subseteq \mathrm{S} \times \mathrm{S}$
$\because \mathrm{R}_1; \mathrm{R}_2 \subseteq \mathrm{S} \times \mathrm{S}, R_3 \subseteq S \times S$
$\therefore (\mathrm{R}_1; \mathrm{R}_2); \mathrm{R}_3 \subseteq \mathrm{S} \times \mathrm{S}$
$\therefore (\mathrm{R}_1; \mathrm{R}_2); \mathrm{R}_3 = \{(\mathrm{a}, \mathrm{c}) : \text{ there is a } \mathrm{b}_1 \in \mathrm{S} \text{ with } (\mathrm{a}, \mathrm{b}_1) \in (\mathrm{R}_1; \mathrm{R}_2) \text{ and } (\mathrm{b}_1, \mathrm{c}) \in \mathrm{R}_3\}$
$= \{(\mathrm{a}, \mathrm{c}) : \text{ there is a } \mathrm{b}_2 \in \mathrm{S} \text{ with } (\mathrm{a}, \mathrm{b}_2) \in \mathrm{R}_1 \text{ and } (\mathrm{b}_2, \mathrm{b}_1) \in \mathrm{R}_2 \text{ and } (\mathrm{b}_1, \mathrm{c}) \in \mathrm{R}_3\}$
apply the same $\mathrm{b}_2, \mathrm{b}_1$ in the $\mathrm{R}_1; (\mathrm{R}_2; \mathrm{R}_3)$

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

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

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

(b).

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

according to the properties of Binary Relations $R \subseteq S \times S$ has reflexive: for all $x \in S$: $(x,x) \in R$

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

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

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

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

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

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

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

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

(c).

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

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

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

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

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

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

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

$\therefore\ b = b_3 \cup b_4$

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

(d).

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

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

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

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

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

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

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

$\therefore\ b = b_5 \cap b_6$

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