4. $n|m \quad m = k*n \quad (k \in \mathbb{Z})$

(a) $\gcd(a,b) \quad \exists t \; t|a \wedge t|b \wedge \neg\forall n \in \mathbb{N} \; n > t \wedge n|a \wedge n|b$

$t = \gcd(a,b)$

(b). $[5] = \{9n+5 \mid n \in \mathbb{Z}\}$

$[7] = \{9n+7 \mid n \in \mathbb{Z}\}$

$A = [5]+[7]$

$A = \{9(n_1+n_2)+12 \mid n_i \in \mathbb{Z}\}$

$= \{9(n_1+n_2+1)+3 \mid n \in \mathbb{Z}\}$

$A = [3]$ 3, 12, 21.

(c) (i) $95x \equiv 33 \pmod{142}$.

$95^{-1} \equiv k \pmod{142}$

$\gcd(95, 142) = 1$.

142		1	0
95	1	0	1
47	2	1	-1
1	47	-2	3
0			

$1 = 142 \times (-2) + 95 \times 3$

$95^{-1} \equiv 3 \pmod{142}$

$x = 95^{-1} \times 33 \pmod{142}$

$= 99 \pmod{142}$

$x = 99 + 142k \quad (k \in \mathbb{Z})$

(ii) $7x \equiv 4 \pmod{15}$

$1 = 15 - 2 \times 7$.

$7^{-1} \equiv -2 \pmod{15}$

$\equiv 13 \pmod{15}$.

$13 \times 4 = 52 \equiv 7 \pmod{15}$

$x \equiv 7 \pmod{15}$

$x = 7 + 15k \quad (k \in \mathbb{Z})$

(d). $\gcd(a,b) = k$.

$(\gcd(a,b))^2 = k^2$.

$k|a \quad \therefore k^2|a^2$

$k|b. \quad k^2|b^2$.

if k^2 is not the largest

k^2 divides $\gcd(a^2, b^2)$

if it is

k^2 divides itself

5(c) $p=17 \quad q=3 \quad n = 17 \times 3 = 51$.

$\phi(51) = 16 \times 2 = 32$.

$a = 9$.

$9^{-1} \pmod{32}$

injective $f: X \to Y$.

for every element y in co-domain, there is at most one x in domain X that maps to y.

$| f(x) = y$ has at most one solution for x.

Surjective $f: X \to Y$

at least

$b = 32 - 7 = 25$. $32 \times 2 - 7 \times 9 = 1$.

$9^{-1} \equiv -7 \pmod{32}$

$M = 5$.

$5^9 \pmod{51} = 16 \times 5 \pmod{51}$

$= 29 \pmod{51}$

$29^{25} \pmod{51}$

$X = \mathbb{R}$ $Y = \mathbb{R}$.

$$f(x) = \begin{cases} (2x)^2 & x \le 0 \\ x^2 & x > 0 \end{cases}$$

injective. $f(x) = 16$. $x = -2$ or 4.

Such that not injective.

$f(x) = -1$. no solution not surjective.

no right inverse

least one solution for x.

$Y = [0, \infty)$

$$f(x) = \begin{cases} (2x)^2 & x \le 0 \\ x^2 & x > 0 \end{cases}$$

yes.

$y = f(x) = 4x^2$ $x \le 0$

$x = \sqrt{\frac{y}{4}} = -\frac{\sqrt{y}}{2}$

$y = f(x) = x^2$ $x > 0$

$x = \sqrt{y}$.

$\therefore g(x) = -\frac{\sqrt{x}}{2}$

$g(x) = \sqrt{x}$.

$f(x) = x * (h * h^{-1}) = x = x'$

$f(x') = x' * (h * h^{-1})$

$f(x h^{-1}) = (x * h^{-1}) * h$

$= x$.

(a) Let $a \in (A \cap B) \Delta A$.

$= ((A \cap B) \setminus A) \cup (A \setminus (A \cap B))$

$\because (A \cap B) \subseteq A$.

$\therefore (A \cap B) \setminus A = \emptyset$

$\therefore a \in A \setminus (A \cap B)$

$a \in A$ $a \notin A \cap B \subseteq B$

$a \notin B$

$\therefore a \in A \setminus B$

$b \in A \setminus B$ $b \in A$ $b \notin B$

$b \notin A \cap B$

$b \in A \setminus (A \cap B)$

$b \in ((A \cap B) \setminus A) \cup (A \setminus (A \cap B))$

$\emptyset$

$\therefore b \in (A \cap B) \Delta A$.

(b) (i). $\{z \mid \{-1, 10, 33\}\} \setminus (z \setminus \{2, 3, 6\})$

$\{2, 6\}$

(ii) $\bigcap_{i \in \mathbb{N}} \{i, i+1, i+2\} = \emptyset$

(c). $\left(\bigcap_{i \in I} A_i\right)^c \subseteq \bigcup_{i \in I} A_i^c$

$a \in \left(\bigcap_{i \in I} A_i\right)^c$

$\exists i$ $a \notin A_i$

$\therefore a \in \bigcup_{i \in I} A_i^c$

$\bigcup_{i \in I} A_i^c \subseteq \left(\bigcap_{i \in I} A_i\right)^c$.

$a \in \bigcup_{i \in I} A_i^c$

$\exists i$ $a \notin A_i$

$\therefore a \notin \bigcap_{i \in I} A_i$

$\therefore a \in \left(\bigcap_{i \in I} A_i\right)^c$

$\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c$

$a \in \left(\bigcup_{i \in I} A_i\right)^c$ $a \notin \bigcup_{i \in I} A_i$ $b \in \bigcap_{i \in I} A_i^c$

$\forall i \quad a \notin A_i$

$\therefore \forall i \quad a \in A_i^c$

$\therefore a \in \bigcap_{i \in I} A_i^c$

$b \notin A_i \quad \forall i$

$\therefore b \notin \bigcup_{i \in I} A_i$

$\therefore b \in \left(\bigcup_{i \in I} A_i\right)^c$

$$\begin{bmatrix} 3 & 0 & 2 \\ 2 & 0 & -2 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 0 & 0 \\ 2 & 0 & -2 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 0 & -2 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 0.2 & 0.2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 0.2 & 0.2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 0.2 & 0.2 & 0 \\ -0.4 & 0.6 & 2 \\ 0 & 0 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 0.2 & 0.2 & 0 \\ -0.2 & 0.3 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 0.2 & 0.2 & 0 \\ -0.2 & 0.3 & 1 \\ 0.4 & -0.6 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0.2 & 0.2 & 0 \\ -0.2 & 0.3 & 1 \\ 0.2 & -0.3 & 0 \end{bmatrix}$$

$$\left[\begin{array}{ccc|ccc} -2 & -2 & 1 & 1 & 0 & 0 \\ -4 & -8 & 4 & 0 & 1 & 0 \\ -1 & 5 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} -4 & -4 & 2 & 2 & 0 & 0 \\ -4 & -8 & 4 & 0 & 1 & 0 \\ -1 & 5 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 4 & -2 & 2 & -1 & 0 \\ -4 & -8 & 4 & 0 & 1 & 0 \\ -1 & 5 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 4 & -2 & 2 & -1 & 0 \\ -4 & -8 & 4 & 0 & 1 & 0 \\ -4 & 20 & 0 & 0 & 0 & 4 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 4 & -2 & 2 & -1 & 0 \\ -4 & -8 & 4 & 0 & 1 & 0 \\ 0 & 28 & -4 & 0 & -1 & 4 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 8 & -4 & 4 & -2 & 0 \\ -4 & -8 & 4 & 0 & 1 & 0 \\ 0 & 28 & -4 & 0 & -1 & 4 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 8 & -4 & 4 & -2 & 0 \\ -4 & -8 & 4 & 0 & 1 & 0 \\ 0 & 28 & 0 & -4 & 1 & 4 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 2 & -1 & 1 & -0.5 & 0 \\ -1 & -2 & 1 & 0 & 0.25 & 0 \\ 0 & 1 & 0 & -0.2 & 0.05 & 0.2 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 0 & -1 & 1.4 & -0.6 & -0.4 \\ -1 & -2 & 1 & 0 & 0.25 & 0 \\ 0 & 1 & 0 & -0.2 & 0.05 & 0.2 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 0 & 1 & -1.4 & 0.6 & 0.4 \\ -1 & -2 & 1 & 0 & 0.25 & 0 \\ 0 & 1 & 0 & -0.2 & 0.05 & 0.2 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 0 & 1 & -1.4 & 0.6 & 0.4 \\ -1 & 2 & 0 & -1.4 & 0.35 & 0.4 \\ 0 & 1 & 0 & -0.2 & 0.05 & 0.2 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 0 & 0 & 1 & -1.4 & 0.6 & 0.4 \\ 1 & 0 & 0 & -1 & 0.25 & 0 \\ 0 & 1 & 0 & -0.2 & 0.05 & 0.2 \end{array}\right]$$

$$A^{-1} = \begin{bmatrix} -1 & 0.25 & 0 \\ -0.2 & 0.05 & 0.2 \\ -1.4 & 0.6 & 0.4 \end{bmatrix}$$

$$\left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} A_i^c$$

$a \in$ $\quad a \notin \bigcap_{i \in I} A_i$

$$\begin{bmatrix}3&0&2\\1&0&0\\1&1&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$\begin{bmatrix}3&0&2\\1&0&0\\0&1&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\0&-1&1\end{bmatrix}$$

$$\begin{bmatrix}1&0&2\\0&1&0\\0&0&1\end{bmatrix}$$

$\exists i$ a & Ai

$\exists v \neq 0 \; \exists \lambda \in R$

$\lambda v = A v$.

$m = n \cdot k \quad (k \in \mathbb{Z})$.

$\operatorname{sgn}(\sigma) = (-1)^k$ $k = \operatorname{order}(\sigma)$

$\phi(n)$

the number of $\{d \mid d \in [1, n] \wedge d \in \mathbb{Z}^+$

$\gcd(d, n) = 1\}$ coprime.

$\phi(n) = |d|$

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&4&3&2&7&6&5\end{pmatrix}$$

(1 8 5 2)(3 4)(6 7)

4 2 2

0 ψ 2

(1 8)(8 5)(5 2)(3 4).