

NT 1-8

NT-1)  $\gcd(720, 450)$

$$i) \quad \underline{720} = \underline{450} \cdot 1 + \underline{270}$$

$$\underline{450} = \underline{270} \cdot 1 + \underline{180}$$

$$\underline{270} = \underline{180} \cdot 1 + \underline{90}$$

$$\underline{180} = \underline{90} \cdot 2 + \underline{0}$$

$$\gcd(720, 450) = 90$$

$$ii) \quad 720 = 2^4 \cdot 3^2 \cdot 5^1$$

$$450 = 2^1 \cdot 3^2 \cdot 5^2$$

$$\gcd(720, 450) = 2^1 \cdot 3^2 \cdot 5 = 90$$

NT-2) i)  $\gcd(21, 30)$

$$\underline{30} = \underline{21} \cdot 1 + \underline{9}$$

$$\underline{21} = \underline{9} \cdot 2 + \underline{3}$$

$$\underline{9} = \underline{3} \cdot 3 + \underline{0}$$

$$\gcd(21, 30) = 3$$

$$\underline{3} = m \cdot 30 + n \cdot 21$$

$$\underline{3} = \underline{21} - \underline{9} \cdot 2$$

$$\underline{3} = \underline{21} - 2(\underline{30} - \underline{21})$$

$$\underline{3} = 3 \cdot \underline{21} - 2 \cdot \underline{30}$$

$$\text{ii) } \gcd(126, 129)$$

$$\underline{129} = \underline{126} \cdot 1 + 3$$

$$\underline{126} = \underline{3} \cdot 42 + 0$$

$$\gcd(126, 129) = 3$$

$$\underline{3} = 1 \cdot \underline{129} - 1 \cdot \underline{126}$$

$$\text{NT-3) } 35^{-1} \text{ in } \mathbb{Z}/73\mathbb{Z}$$

$$\underline{73} = \underline{35} \cdot 2 + \underline{3}$$

$$\underline{1} = \underline{3} - \underline{2} \cdot \underline{1}$$

$$\underline{35} = \underline{3} \cdot 11 + \underline{2}$$

$$\underline{1} = \underline{3} - 1(\underline{35} - \underline{3} \cdot 11)$$

$$\underline{3} = \underline{2} \cdot 1 + \underline{1}$$

$$\underline{1} = 12 \cdot \underline{3} - \underline{35}$$

$$\underline{2} = \underline{1} \cdot 2 + 0$$

$$\underline{1} = -\underline{35} + 12(\underline{73} - 2 \cdot \underline{35})$$

$$\underline{1} = -25 \cdot \underline{35} + 12 \cdot \underline{73}$$

$$1 = (-25 \cdot \underline{35} + \cancel{12 \cdot \underline{73}}) \bmod 73$$

$$1 \equiv -25 \cdot 35 \bmod 73$$

$$\Rightarrow 1 \equiv 48 \cdot \underline{35} \bmod 73$$

$$\underline{35}^{-1} = 48 \text{ in } \mathbb{Z}/73\mathbb{Z}$$

NT-4)

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

 $\mathbb{Z}/6\mathbb{Z}$ 

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

NT-5)

$$\mathbb{Z}/\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

$$\mathbb{Z}/\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

$\mathbb{Z}^*$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}^*$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$$NT-6) \quad n = \{2 \dots 11\} \quad \mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

$$f_n(x) = nx$$

$$2x) \quad \{0, 2, 4, 6, 8, 10, 0, 2, 4, 6, 8, 10\}$$

$$\text{Range} = 6$$

$$3x) \quad \{0, 3, 6, 9, 0, 3, 6, 9, 0, 3, 6, 9\}$$

$$\text{Range} = 4$$

$$4x) \quad \{0, 4, 8, 0, 4, 8, 0, 4, 8, 0, 4, 8\}$$

$$\text{Range} = 3$$

$$5x) \quad \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$$

$$\text{Range} = 12$$

$$6x) \quad \{0, 6, 0, 6, \dots\}$$

$$\text{Range} = 2$$

$$7x) \quad \{0, 7, 2, \dots\}$$

$$\text{Range} = 12$$

$$8x) \quad \{0, 8, 4, 0, \dots\}$$

$$\text{Range} = 3$$

$$9x) \quad \{0, 9, 6, 3, 0, \dots\}$$

$$\text{Range} = 4$$

$$10x) \quad \{0, 10, 8, 6, 4, 2, 0, \dots\}$$

$$\text{Range} = 6$$

$$11x) \quad \text{Range} = 12$$

$$NT-7) \quad m = 2, 11, 22$$

$$NT-8) \mathbb{Z}/13\mathbb{Z}^* = \{1, 2, \dots, 12\}$$

$$(x \cdot 1) \bmod 13 = 1$$

$$1^{-1} = 1$$

$$(x \cdot 2) \bmod 13 = 1$$

$$2^{-1} = 7$$

$$(x \cdot 3) \bmod 13 = 1$$

$$3^{-1} = 9$$

$$(x \cdot 4) \bmod 13 = 1$$

$$4^{-1} = 10$$

$$(x \cdot 5) \bmod 13 = 1$$

$$5^{-1} = 8$$

$$(x \cdot 6) \bmod 13 = 1$$

$$6^{-1} = 11$$

$$(x \cdot 7) \bmod 13 = 1$$

$$7^{-1} = 2$$

$$(x \cdot 8) \bmod 13 = 1$$

$$8^{-1} = 5$$

$$(x \cdot 9) \bmod 13 = 1$$

$$9^{-1} = 3$$

$$(x \cdot 10) \bmod 13 = 1$$

$$10^{-1} = 4$$

$$(x \cdot 11) \bmod 13 = 1$$

$$11^{-1} = 6$$

$$(x \cdot 12) \bmod 13 = 1$$

$$12^{-1} = 12$$

$$13 = \underline{1} \cdot 13 + 0$$

$$\underline{13} = \underline{2} \cdot 6 + \underline{1}$$

$$\underline{2} = \underline{1} \cdot 2 + 0$$

$$\underline{13} = \underline{3} \cdot 4 + \underline{1}$$

$$\underline{3} = \underline{1} \cdot 3 + \underline{0}$$

$$1 = \underline{13} - \underline{2} \cdot 6 \bmod 13$$

$$11 \cdot 6 \bmod 13$$

$$1 = 13 - \underline{3} \cdot 4 \bmod 13$$

$$\downarrow$$
  

$$10 \cdot 4 \bmod 13$$