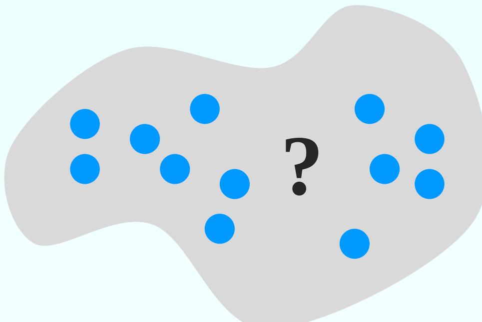
Modular Arithmetic

Integers Modulo n and Group, Ring, Field

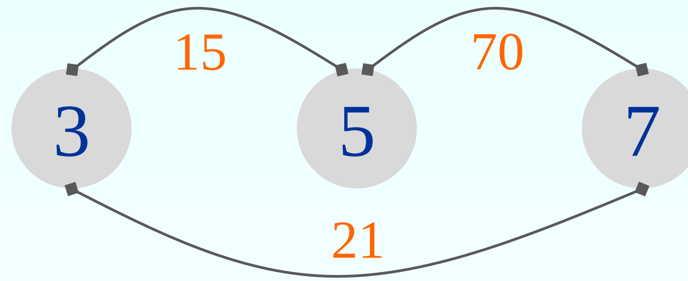
부산대학교
PUSAN NATIONAL UNIVERSITY

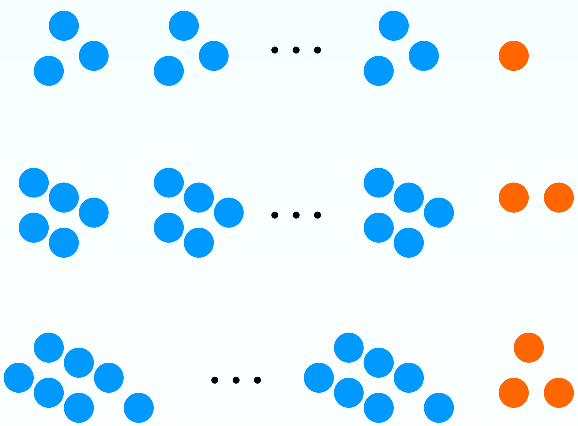
Chinese Remainder Theorem

병사 점호 방법



5,7 공배수 중에서 3으로
나누면 나머지가 1이 되는
가장 작은 수





$$a \times 70 + b \times 21 + c \times 15 = n$$

$$1 \times 70 + 2 \times 21 + 3 \times 15 = 157$$

$$157 + k\,\mathrm{LCM}(3,5,7) \ \ ?$$

$$157 + (-1)\,105 \ = \ 52$$

Congruence Modulo n

- **Definition**

  Let $n \in Z^+$, $n > 1$.

  For $a, b \in Z$, we say that a is congruent to b modulo n, and we write $a \equiv b \bmod n$, if $n|(a-b)$, or equivalently, $a = b + kn$ for some $k \in Z$

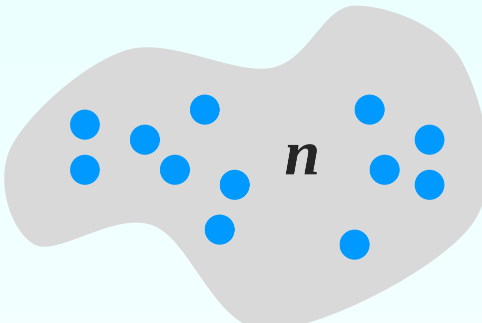
  $17 \equiv 2 \bmod 5$; $17 = 2 + 3 \cdot 5$

  $-7 \equiv -49 \bmod 6$; $-7 = -49 + 7 \cdot 6$

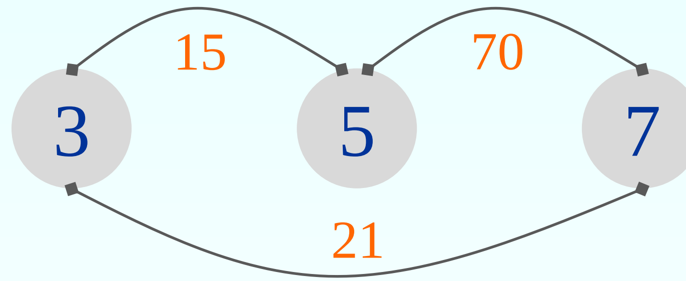
(note) $m|n$: m divides n, for $m, n \in Z$, $m \neq 0$

Chinese Remainder Theorem

병사 점호 방법



$k \times \mathrm{LCM}(5,7) \equiv 1 \bmod 3$ 인 가장 작은 수



$$n \equiv 1 \bmod 3$$

$$n \equiv 2 \bmod 5$$

$$n \equiv 3 \bmod 7$$

$$1\times 70 \;+\; 2\times 21 \;+\; 3\times 15 \;=\; 157$$

$$157 \bmod \mathrm{LCM}(3,5,7) \;\Rightarrow\; 52$$

(**Theorem**) If the moduli are relatively prime in pairs (ie., $gcd(m_i, m_j) = 1$ for $i \neq j$), then the system has a unique solution mod $m_1 m_2 \ldots M_k$.

Congruence Modulo n

- **Theorem 1**

  Congruence modulo n is an equivalence relation on $\mathbf{Z}$

  $\mathbf{Z} \times \mathbf{Z}$

  R = { …, $(-n,0)$, $(0,0)$, $(0,n)$, $(n,2n)$, …,
  $(1-n,1)$, $(1,1)$, $(1,1+n)$, $(1+n,1+2n)$, …,
  $(2-n,2)$, $(2,2)$, $(2,2+n)$, $(2+n,2+2n)$, … }

  $(a,a) \in R \Rightarrow$ Reflexive

  (a,b) & $(b,a) \in R \Rightarrow$ Symmetric

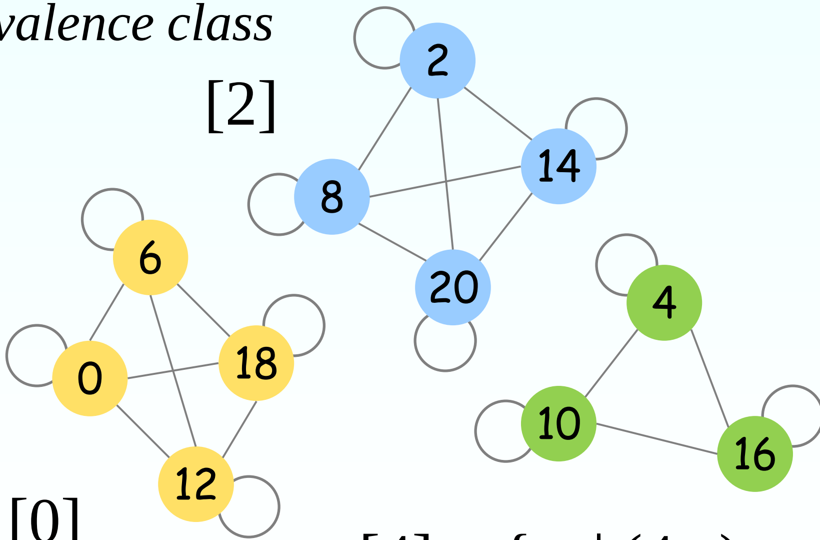
  (a,b) & (b,c) & $(a,c) \in R \Rightarrow$ Transitive

  $$a = b + kn = (c + ln) + kn = c + (l+k)n$$

(Example)

❖ 20 이하의 짝수 자연수 집합 A 에 대하여 (congruence modulo 3) relation R ?

Equivalence class of 2



Quotient set of A modulo R

A / R = { [0], [4], [2] }

= { {0,6,12,18}, {4,10,16}, {2,8,14,20} }

∴ a *partition* of $\boldsymbol{A}$

[4] = { x | (4,x) ∈ R }

= { 4, 10, 16 }

[10] = { y | (10,y) ∈ R } ?

Equivalence Classes

Note that an equivalence relation on a set induces a partition of the set

Congruence modulo n ($\geq$ 2) partitions Z into the n equivalence classes

$[0] = \{\ 0+nx \mid x \in Z\ \} = \{.., -n, 0, n, ..\}$

$[1] = \{\ 1+nx \mid x \in Z\ \} = \{.., 1-n, 1, 1+n, ..\}$

$[2] = \{\ 2+nx \mid x \in Z\ \} = \{.., 2-n, 2, 2+n, ..\}$

$\vdots$

$[n-1] = \{\ (n-1)+nx \mid x \in Z\ \} = \{..,-1, n-1, 2n-1, ..\}$

(***Theorem***) If $\mathcal{R}$ is an equivalence relation on a set A, then the set of distinct equivalence classes, $A/\mathcal{R}$, is a partition of A.

Equivalence Classes

$$[x]_{\mathcal{R}} = \{\, y \in A \mid (x, y) \in \mathcal{R} \}$$
$$= \{\, y \in A \mid y = x + kn \,,\; k \in \mathbf{Z} \,\}$$

- $[t] = [r]$ where $t = r + kn$ $(0 \le r < n)$
  - An integer $l \in [r]$ can be written as $l = r + pn$ for some $p \in Z$

    Since $l = r + pn = (t-kn) + pn = t + (p-k)n$, so $l \in [t]$. Thus $[r] \subseteq [t]$
  - Conversely, an integer $m \in [t]$ can be also represented, for some $q \in Z$, as $m = t + qn = (r + kn) + qn = r + (p + q)n$

    So $m \in [r]$ and $[t] \subseteq [r]$
  - Therefore, $[t] = [r]$

There are the only n distinct equivalence classes

Z_n and Operators

- $Z_n = \{ [0], [1], \ldots, [n-1] \}$

  Two closed operators on Z_n : $+$ and $\cdot$

  $[a] + [b] = [a+b]$ and $[a]\cdot[b] = [a][b] = [ab]$

  - For $n = 7$, $[2] + [6] = [2+6] = [8] = [1]$, and $[2][6] = [12] = [5]$

$< Z_n, +, \cdot >$ Ring, Field ?

Z_n : ring or field ?

❖ Theorem 2

For $n \in Z^+$, $n > 1$, under the two closed operators, Z_n is a commutative ring with unity [1] (and additive identity [0])

(Ex.) $< Z_5, +, \cdot >$ ➔ Field

C
A
I
I
C

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

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

D
C
A
I
I
C

(Note) Inverse : for nonzero elements

continued

(Ex.) < Z_6, +, · > ➔ Not Field

CAIIC

+	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

·	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

DCAIIC

proper divisors of zero

Unity vs. Unit

It has the multiplicative inverse

Z_n with a prime n

- **Theorem 3**

  Z_n is a field if and only if n is a prime

  (Proof of ←)

  If n is a prime, $\gcd(a, n) = 1$ for $0 < a < n$.

  There are some integers s, t with $as + tn = 1$,
  so $as \equiv 1 \bmod n$, or $[as] = [1] = [a][s]$.
  Since $[a]$ is a unit, Z_n is a field

(Note 1) $as + bt = \gcd(a, b)$ ← (Theorem 4.6) in Text

For all $a, b \in Z^+$, the following equation is satisfied.

$\gcd(a, b) = as + bt$, for some $s, t \in Z$

(Note 2) Unit

The element that has the multiplicative inverse, in a ring with unity

Z_n with a prime n

- **Theorem 3**

Z_n is a field if and only if n is a prime.

(Proof of →)

If Z_n is a field, $[a]$ is a unit for $0 < a < n$.

Then there is an integer s $(0 < s < n)$ such that $[a][s] = [1]$. So $as \equiv 1 \bmod n$ and $as = 1 + tn$.

Then, 1 $(= as + n(-t))$ is the smallest element in the set $\{ ax+ny \mid x,y \in Z,\ ax+ny > 0 \}$

Therefore, $\gcd(a,n) = 1$ and n is a prime.

(Theorem 4.6) in Text

Unit in Z_n

- **Theorem 4**

  In Z_n, $[a]$ is a unit if and only if $\gcd(a, n) = 1$.

  (Proof)

← $\gcd(a, n) = 1 = as + tn$, for some $s, t \in Z$. Then, $as = 1 - tn$ and $[a][s] = [1]$. So $[a]$ is a unit.

→ Let $[a] \in Z_n$ and $[a]^{-1} = [s]$. Then $[as] = [a][s] = [1]$, so $as \equiv 1 \bmod n$ and $as = 1 + tn$, for some $t \in Z$. Therefore, $\gcd(a, n) = 1$ $(= as + n(-t))$.

(Ex) Find $[25]^{-1}$ in Z_{72}. $[36]^{-1}$?

$$1 = 25(-23) + 72(8) \Rightarrow [25][-23] \equiv 1 \bmod 72$$

Therefore, $[25]^{-1} = [-23] = [-23+72] = [49]$

Unit in Z_n

(Ex.) $< Z_6, +, \cdot >$ ➔ Not Field

But $\gcd(5,6) = 1$.

$1 = (5)(5)+(-4)(6)$,

so $[5]^{-1} = [5]$.

$\cdot$	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

$\gcd(2,6) \neq 1$,

$\gcd(3,6) \neq 1$,

$\gcd(4,6) \neq 1$. not unit

proper divisors of zero

Euler's Phi Function

- **Definition**

  For $n \in Z^+$ and $n \geq 2$, let $\phi(n)$ be the number of positive integers m, where $1 \leq m < n$ and m, n are relatively prime. This function is known as Euler's phi function.

  When $p_1, \ldots, p_t$ are distinct primes and $e_i \geq 1$ for all $1 \leq i \leq t$,

$$\phi(n) = \prod_{p_i | n} (p_i^{e_i} - p_i^{e_i - 1}) = n \prod_{p_i | n} (1 - 1/p_i) \qquad n = \prod_{i=1}^{t} p_i^{e_i}$$

(Note) relatively prime

For $m, n \in Z^+$ and $1 \leq m < n$, if $\gcd(m, n) = 1$, then m, n are called relatively prime.

Examples

- $\phi(72)$?

  $= \phi(2^3 3^2) = (2^3 - 2^2)(3^2 - 3^1) = 4 \cdot 6 = 24$

  or $= 2^3 3^2 (1 - 1/2)(1 - 1/3) = (72)(1/2)(2/3) = 24$

- $\phi(20)$?

  $= \phi(2^2 5) = (20)(1 - 1/2)(1 - 1/5)$

  $= (20)(1/2)(4/5) = 8$

  1, 3, 7, 9, 11, 13, 17, 19

Corollary

- Let p be a prime and $e \geq 1$.

  If $n = p^e$, $\phi(n) = p^{e-1}(p-1)$.

  If $n = p$, $\phi(p) = p-1$.

  – $\phi(27) = \phi(3^3) = 3^2(3-1) = 18$, $\phi(11) = 11 - 1 = 10$

- If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\,\phi(n)$.

  – $m = 10 = 2 \cdot 5$, $n = 27 = 3^3$,

  $$\begin{aligned}\phi(270) &= \phi(10 \cdot 27) = \phi(2 \cdot 5 \cdot 3^3) \\ &= (2-1)(5-1)(3^3-3^2) = \phi(10)\,\phi(27)\end{aligned}$$

Z_n^* vs. $\phi(n)$

- **Definition of Z_n^***

  The set of all equivalence classes $[m]$ in Z_n is called Z_n^*, where m is relatively prime to n

  $$Z_n^* = \{ [m] \mid \gcd(m, n) = 1,\ 1 \le m < n \}$$

  Note that $|Z_n^*| = \phi(n)$. Z_n = ?

  - $Z_{10}^* = \{ 1,3,7,9 \}$

    $\phi(10) = \phi(2 \cdot 5) = (2-1)(5-1) = 4$
  - $Z_{15}^* = \{ 1,2,4,7,8,11,13,14 \}$

    $\phi(15) = \phi(3 \cdot 5) = (3-1)(5-1) = 8$

Example

❖ **Multiplication Table of Z_{15}^***

·	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4			1	8
8	8	1	2		4	?	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

< Z_{15}^*, · >

Abelian Group

1) Closed

2) Associative

3) Identity ?

4) Inverse

5) Commutative

$$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow eb = ec \Rightarrow b = c$$

$$b \neq c \Rightarrow ab \neq ac$$

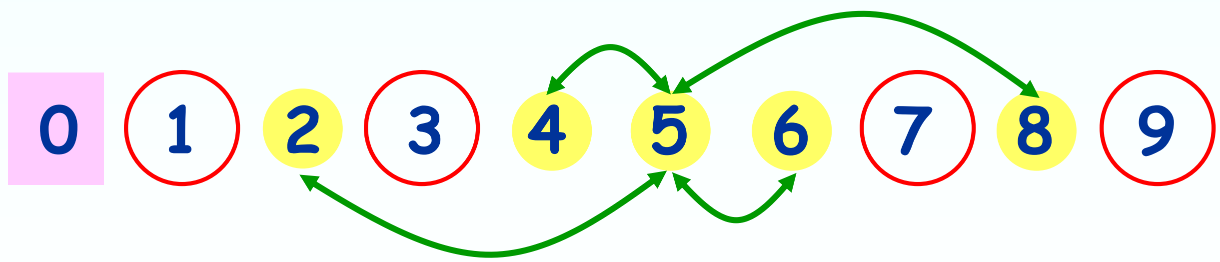
$\mathcal{Z}_n$ vs. $\phi(n)$

- In general,

  For any $n \in \mathcal{Z}^+$, $n > 1$, there are $\phi(n)$ units and $n - \phi(n) - 1$ proper divisors of zero in $\mathcal{Z}_n$.

  – $\mathcal{Z}_{10}^* = \{ 1,3,7,9 \}$

    $\phi(10) = \phi(2 \cdot 5) = (2-1)(5-1) = 4$



중간 요약

Z_n	Z_p	Z_n^*
Commutative Ring with Unity	Field	Abelian Group for multiplication
$\phi(n)$ units	$\phi(p) = p-1$ units	
$n-1-\phi(n)$ proper divisors of zero		

relatively prime or not

Euclidean Algorithm (1)

- **Base Theorem**

For $m, n \in Z^+$,

if $\gcd(m, n) = 1$, $\gcd(m, n) = \gcd(n, m \bmod n)$.

(Proof)

Let $m \bmod n = r$ for $0 \le r < n$. Then $m = kn + r$ for $k \in N$. Let $\gcd(n, r) = g$. Then $n = dg$, $r = eg$, and $m = kn + r = kdg + eg = (kd + e)g$, for $d, e \in Z^+$. So m and n have a common divisor g. However, $\gcd(m, n) = 1$, so $g = 1$ and $\gcd(n, r) = \gcd(n, m \bmod n) = 1$.

Therefore, $\gcd(m, n) = \gcd(n, m \bmod n)$.

Euclidean Algorithm (2)

- **Theorem**

  For $m, n \in Z^+$,

  $$\gcd(m,n) = \gcd(n,\ m \bmod n)$$

  (Proof)

  Let assume that $r = \gcd(m,n)$, $m = ar$, $n = br$, $\gcd(a,b) = 1$, for $r,a,b \in Z^+$. Then, $m \bmod n = (a \bmod b)r = r'r$ for $0 \le r' < b$.

  From the base theorem, $\gcd(a,b) = \gcd(b,\ a \bmod b) = \gcd(b,r') = 1$. Then, $\gcd(n,\ m \bmod n) = \gcd(br, r'r) = r$.

  Therefore, $\gcd(m,n) = \gcd(n,\ n \bmod m)$.

Euclidean Algorithm (3)

- Recursive Euclidean Algorithm

Euclid (a,b)

  if b = 0 then return a

  else return Euclid (b, a mod b) fi

4

– Euclid (76,16) ; 76 = 4x16 + 12

Euclid (16,12) ; 16 = 1x12 + 4

Euclid (12,4) ; 12 = 3x4 + 0

Euclid (4,0) 4

Finding Multiplicative Inverse

- Find $[25]^{-1}$ in Z_{72}

  By the Euclidean algorithm,

$$72 = 2(25) + 22$$
$$25 = 1(22) + 3$$
$$22 = 7(3) + 1$$

Euclid (72,25) ➔ Euclid (25,22) ➔ Euclid (22,3) ➔ Euclid (3,1) ➔ Euclid (1,0) ➔ 1

$$1 = 22 - 7(3) = 22 - 7[25 - 22] = (-7)(25) + (8)(22)$$
$$= (-7)(25) + 8[72 - 2(25)] = 8(72) - 23(25)$$

$$8 = 8$$
$$-23 = (-7) - 2(8)$$

$$1 = 8(72) - 23(25) \Rightarrow 1 \equiv (-23)(25) \bmod 72$$
$$\therefore [1] = [-23][25] \quad \& \quad [25]^{-1} = [-23] = [49]$$

Extended Euclidian Algorithm

- Given a,b, the extended Euclidian algorithm computes d,x,y such that

$$d = \gcd(a,b) = ax + by$$

```
Ext-Euclid (a,b)
    if b = 0 then return (a,1,0) fi
    (d',x',y' ) = Ext-Euclid (b, a mod b)
    (d,x,y) = (d', y', x'- ⌊a/b⌋ y' )
return (d,x,y)
```

Example

- Ext-Euclid(72,25)

a	b	$\lfloor a/b \rfloor$	d	x	y
72	25	2	1	8	-23
25	22	1	1	-7	8
22	3	$\boxed{7}$	1	1	-7 $= 0 - 7 \cdot 1$
3	1	3	1	$\boxed{0}$	$\boxed{1}$
1	0	-	1	1	0

$$(d,\ x,\ y) = (d',\ y',\ x' - \lfloor a / b \rfloor\, y')$$

Finding Inverses

- **Theorem**

  Given a, n such that $\gcd(n, a) = 1$

  $$a^{-1} \bmod n$$

  can be computed from the Ext-Euclid algorithm.

  (1) Find x, y such that $nx + ay = \gcd(n, a) = 1$ by the Ext-Euclid(n, a)

  (2) Then $n \mid (ay-1)$. So, $ay \equiv 1 \bmod n$.

  (3) Thus $a^{-1} = y \bmod n$.

$1 = \gcd(72,25)$	$25^{-1} = (-23) \bmod 72$	$25 \cdot 49$
$= 72 \cdot 8 + 25 \cdot (-23)$	$= (72-23) \bmod 72 = 49$	$= 72 \cdot 17 + 1$

이산수학 쉽터

- Encryption / Decryption
  - *Caesar cipher*

LFDPHLVDZLFRQTXHUHG

a	b	c	d	e	…	x	y	z	
0	1	2	3	4	…	23	24	25	
d	e	f	g	h	…	a	b	c	: rotate left 3 times
3	4	5	6	7	…	0	1	2	
D	E	F	G	H	…	A	B	C	: convert to capital letters

icameisawiconquered

LFDPHLVDZLFRQTXHUHG

$$E(k) = (k+3) \bmod 26 = m$$

$$D(m) = (m-3) \bmod 26 = k$$

이산수학 쉼터

- Affine cipher

06 02 20 12 11 24 12 14 22 12 11 17 04 20 06 ?

$$E(k) = (\alpha k+\beta) \bmod 26 = m, \quad \gcd(\alpha,26) = 1$$

$$D(m) = \alpha^{-1}(m-\beta) \bmod 26 = k$$

$$E(k) = (3k + 12) \bmod 26$$

$$D(m) = 9(m - 12) \bmod 26$$

$$1 = 26\cdot(-1) + 3\cdot 9$$

$$[3]^{-1} = [9] \text{ in } \mathbb{Z}_{26}$$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

⇕

12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0	3	6	9