Exercise 1

We consider the ring $\mathbb{Z}_{34} = \{0, 1, 2, \ldots, 33\}$ of integers modulo 34.

1. List all numbers in $\mathbb{Z}_{34}$ that are coprime to 34.
2. Find the multiplicative inverse of 3, 13, and 29 in $\mathbb{Z}_{34}$.
   Given the encryption function $E(a, x) = x \cdot a \bmod 34$

Letter	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
Code	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Letter	r	s	t	u	v	w	x	y	z	=	(	)	²	°	E	D	space
Code	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

3. Determine the number of possible keys.
4. Derive the decryption function corresponding to $E(a, x)$.
5. Encrypt the following message using $a = 13$:
   - $E = mc^2$

Solution

1. Finding All Comprime Integers Of 34

Number Of Comprime

$$34 = 2^1 \times 17^1$$

$$\phi(34) = 34 \times \left(1 - \tfrac{1}{2}\right) \times \left(1 - \tfrac{1}{17}\right) = \boxed{16}$$

There are 16 numbers coprime to 34. These numbers are not divisible by 2 or 17

$$\text{Coprime Numbers} = \{\ 1\ ,\ 3\ ,\ 5\ ,\ 7\ ,\ 9\ ,\ 11\ ,\ 13\ ,\ 15\ ,\ 19\ ,\ 21\ ,\ 23\ ,\ 25\ ,\ 27\ ,\ 29\ ,\ 31\ ,33\}$$

2. Finding Multiplicative

$$a^{-1} \cdot a = 34 \cdot k + 1$$

$$\boxed{a^{-1} = \frac{34 \cdot k + 1}{a}}$$

a = 3

for $k = 2$ we have :

$$a^{-1} = \frac{34 \cdot 2 + 1}{3} = \boxed{23}$$

a = 13

for $k = 8$ we have :

$$a^{-1} = \frac{34 \cdot 8 + 1}{13} = \boxed{21}$$

Euclid Methods

a = 29

$$34 = 29 \times 1 + 5$$
$$29 = 5 \times 5 + 4$$
$$5 = 4 \times 1 + 1$$

Back-substituting to express 1 as a linear combination of 34 and 29:

$$1 = 5 - 4 \times 1$$

$4 = 29 - 5 \times 5$, we substitute:

$$1 = 5 - (29 - 5 \times 5)$$

$5 = 34 - 29$, we substitute:

$$1 = (34 - 29) - (29 - (34 - 29) \times 5)$$
$$1 = 34 - 29 - 29 + 5(34 - 29)$$
$$1 = 34(6) + 29(\boxed{-7})$$

Thus, the modular inverse of 29 modulo 34 is (-7 mod 34) = $\boxed{27}$.

3. Number Of Possible Keys

Number of possible keys is the same as number of coprime numbers with 34 which we previously found was $\boxed{16}$

4. Decryption Function

$$\boxed{D(a^{-1}, y) = y \cdot a^{-1} \bmod 34}$$

5. Encryption

Plain Text	E	=	m	c	2
Code	31	26	12	2	29
a • Code	403	338	156	26	377
mod 34	29	32	20	26	3
Ciphered Text	2	D	u	=	d