Modular Arithmetic and Euclidean Algorithm

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

Today's Objectives

- Modular Arithmetics
- Euclidean Algorithm
- Residue Classes
- Finding Inverse Modulo m
- General Caesar Cipher
- Affine Cipher

Modular Arithmetics

Set of Integers

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Note: Integer by integer is not always integer

Example

There is no integer n such that $1/2 = n$

Definition

We say that $a (\neq 0)$ divides b, written as $a|b$, if there is an integer k with $b = ka$

- Examples: $2|4$, $(-7)|7$, and $6|0$

Basic Properties of Divisibility

- If $a|b$, then $a|bc$ for any c
- If $a|b$ and $b|c$, then $a|c$
- If $a|b$ and $a|c$, then $a|(xb + yc)$ for any x and y
- If $a|b$ and $b|a$, then $a = \pm b$
- If $a|b$, and $a, b > 0$, then $a \leq b$
- For any $m \neq 0$, $a|b$ is equivalent to $(ma)|(mb)$

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Example

- Positive divisors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$
- Positive divisors of 42 are $1, 2, 3, 6, 7, 14, 21, 42$
- Common (positive) divisors are $1, 2, 3, 6$
- $GCD(30, 42) = 6$

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Example

- 7 and 12 are relatively prime
- But, 8 and 32 are not relatively prime
- 11 and 13 are relatively prime

Basic facts about greatest common divisors

- If $m > 0$, then $GCD(ma, mb) = m \times GCD(a, b)$
- If $d > 0$ divides both a and b, then $GCD(a/d, b/d) = GCD(a, b)/d$
- If both a and b relatively prime to m, then so is ab
- For any integer x, $GCD(a, b) = GCD(a, b + ax)$
- If $c|ab$ and b, c are relatively prime, then $c|a$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{k-1} &= q_k r_k + r_k + 1 \\
r_k &= q_{k+1} r_{k+1}
\end{aligned}$$

Then $d = GCD(a, b)$ is equal to the last nonzero remainder, r_{k+1}

- **Linear Combination**: There exist integers x and y such that $d = ax + by$

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

$$6 = 30 - 2 \times (42 - 1 \times 30)$$

Hence, $6 = 30 \times 3 - 42 \times 2$

That is, $x = 3$ and $y = -2$

Residue Classes

Definition

If m is a positive integer and m divides $(b - a)$, then we say that

- a and b are congruent modulo m
- we write $a \equiv b \pmod{m}$

Examples:

- $3 \equiv 9 \pmod{6}$, since 6 divides $9 - 3 = 6$
- $-2 \equiv 28 \pmod{5}$, since 5 divides $28 - (-2) = 30$
- $0 \equiv -666 \pmod{3}$, since 3 divides $-666 - 0 = -666$

If m does not divide $b - a$, we say a and b are not congruent mod m, and write $a \not\equiv b \pmod{m}$

- $2 \not\equiv 7 \pmod{3}$, because 3 does not divide $7 - 2 = 5$

Residue Classes

- $a = q_1 m + r_1$ and $b = q_2 m + r_2$,
  where $0 \leq r_1 \leq m - 1$ and $0 \leq r_2 \leq m - 1$.
- $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.
- $r_1 = a \pmod{m}$ denotes the remainder.
- Thus, $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Definition (Residue Class)

If a is an integer and $a \equiv b \pmod{m}$, we say that b is a residue of a mod m.

- The residue class of a modulo m, denoted $\bar{a}$, is the collection of all integers congruent to a modulo m.
- Observe that $\bar{a} = \{a + km, k \in \mathbb{Z}\}$.

Set of Residue Class

- The residue class of a modulo m, denoted $\bar{a}$, is the collection of all integers congruent to a modulo m.
- Observe that $\bar{a} = \{a + km, k \in \mathbb{Z}\}$.

Set of residue class $\{0, 1, 2, \ldots, m-1\}$ modulo m is denoted by $\mathbb{Z}_m$, that is,

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

- Addition and Multiplication works exactly like real addition and multiplication, except reduce modulo m.
- $11 \times 13 = 143$ in $\mathbb{Z}_{16}$, and reduce it to modulo 16:
  $143 = 8 \times 16 + 15$, so $143 \pmod{16} = 15 \in \mathbb{Z}_{16}$

Definition (Inverse of an element)

Suppose $a \in \mathbb{Z}_m$. The multiplicative inverse of a is an element $a^{-1} \in \mathbb{Z}_m$ such that $aa^{-1} = a^{-1}a = 1 \pmod{m}$

Finding Inverse Modulo m

Theorem (Multiplicative Inverse Modulo m)

a and m relatively primes if and only if a^{-1} modulo m exists

Proof.

Suppose a and m are relatively prime

Then, $GCD(a, m) = 1$

There exists x and y such that $1 = ax + my$

Now apply modulo m, we get $1 = (ax + 0) \pmod{m}$

That is, $1 = ax \pmod{m}$

Means, there exists x such that $ax = 1 \pmod{m}$

Therefore, x is inverse of a modulo m

$\square$

Example: Finding Inverse Modulo m

Find multiplicative inverse of $a = 8$ modulo $m = 11$

Finding $8^{-1} \pmod{11}$ using Euclidean Algorithm

$$m = qa + r$$
$$a = q_1 r + r_1$$

- $11 = (1) \times 8 + 3$
- $8 = (2) \times 3 + 2$
- $3 = (1) \times 2 + 1$
- $2 = (2) \times 1 + 0$

Rewrite

- $3 = 11 - (1) \times 8$
- $2 = 8 - (2) \times 3$
- $1 = 3 - (1) \times 2$

Reverse the process:
find $1 = 8x + 11y$ form

$$\begin{aligned} 1 &= 3 - (1) \times 2 \\ &= 3 - (1) \times [8 - (2) \times 3] \\ &= (-1) \times 8 + (3) \times 3 \\ &= (-1) \times 8 + (3) \times [11 - (1) \times 8] \\ &= (-4) \times 8 + (3) \times 11 \end{aligned}$$

$$x = -4 \pmod{11} = 7 = 8^{-1} \pmod{11}$$

Finding Inverse

Find Inverse of 7 modulo 26

Remainder Form

$$26 = (3) \times 7 + 5$$
$$7 = (1) \times 5 + 2$$
$$5 = (2) \times 2 + 1$$
$$2 = (2) \times 1 + 0$$

Rewrite

$$5 = 26 - (3) \times 7$$
$$2 = 7 - (1) \times 5$$
$$1 = 5 - (2) \times 2$$

Reverse Process

$$1 = 5 - (2) \times 2$$
$$1 = 5 - (2) \times [7 - (1) \times 5]$$
$$1 = (-2) \times 7 + (3) \times 5$$
$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$
$$1 = (-11) \times 7 + (3) \times 26$$

$x = -11 \pmod{26} = 15 = 7^{-1} \pmod{26}$

Finding Inverse

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
  where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
  $x = 5^{-1} = -5 \pmod{26} = 21$

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet *a* - *z*, respectively.

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26} = \{0, 1, 2, \ldots, 25\}$
  Z_{26} - set of remainders when divide by 26
- Encryption function $E_k : \mathcal{P} \rightarrow \mathcal{C}$ and
  decryption function $D_k : \mathcal{C} \rightarrow \mathcal{P}$, where $k \in \mathcal{K}$, defined as follows:

$$
\begin{aligned}
C &= E_k(m) = (m + k) \pmod{26} \\
m &= D_k(C) = (C - k) \pmod{26}
\end{aligned}
$$

where $m, C \in Z_{26}$

Note that, if key $k = 3$, it is simply a Caesar cipher.

General Caesar Cipher

Example

Find the Caesar cipher of a simple message m = *"crypto"* with the key $k = 3$

- Assume that $m = m_1 m_2 \dots m_n$
  the plaintext message with n letters m_1 to m_n
- Then $m_1 = c, m_2 = r, m_3 = y, m_4 = p, m_5 = t, m_6 = o$
- Suppose the corresponding ciphertext letters are C_1 to C_n

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

m = "crypto" and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$
\begin{aligned}
C_1 &= E_k(m_1) = (2+3) \pmod{26} = 5 \pmod{26} = 5 = F \\
C_2 &= E_k(m_2) = (17+3) \pmod{26} = 20 \pmod{26} = 20 = U \\
C_3 &= E_k(m_3) = (24+3) \pmod{26} = 27 \pmod{26} = 1 = B \\
C_4 &= E_k(m_4) = (15+3) \pmod{26} = 18 \pmod{26} = 18 = S \\
C_5 &= E_k(m_5) = (19+3) \pmod{26} = 22 \pmod{26} = 22 = W \\
C_6 &= E_k(m_6) = (14+3) \pmod{26} = 17 \pmod{26} = 17 = R
\end{aligned}
$$

The ciphertext C is *"FUBSWR"*, that is, $E_3(crypto) = FUBSWR$

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, and
$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : GCD(a, 26) = 1\}$

$$\begin{aligned} C &= E_k(m) = (am + b) \pmod{26} \\ m &= D_k(C) = a^{-1}(C - b) \pmod{26} \end{aligned}$$

where $m, C \in \mathbb{Z}_{26}$

Correctness proof:

$$\begin{aligned} D_k(E_k(m)) &= D_k(am + b) \pmod{26} \\ &= a^{-1}((am + b) - b) \pmod{26} \\ &= a^{-1}(am) \pmod{26} \\ &= (a^{-1}a)m \pmod{26} \\ &= m \pmod{26} \\ &= m \end{aligned}$$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Remainder Form

$$26 = (3) \times 7 + 5$$
$$7 = (1) \times 5 + 2$$
$$5 = (2) \times 2 + 1$$
$$2 = (2) \times 1 + 0$$

Reverse Process

$$1 = 5 - (2) \times 2$$
$$1 = 5 - (2) \times [7 - (1) \times 5]$$
$$1 = (-2) \times 7 + (3) \times 5$$
$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$
$$1 = (-11) \times 7 + (3) \times 26$$

$x = -11 \pmod{26} = 15$

Correctness

$$\begin{aligned} D_k(C) &= 15(C - 3) \pmod{26} \\ &= 15([7m + 3] - 3) \pmod{26} \\ &= 105m \pmod{26} \\ &= m \end{aligned}$$

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m: "*crypto*"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z	T	U

That is, $E_K(crypto) = MJSZTU$.

- The decryption function is $m = D_k(C) = 5^{-1}(C - 2) \pmod{26}$
- We have to find the value of $5^{-1} \pmod{26}$

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
  where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
  $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C-2)$	210	147	336	483	357	378
$21(C-2) \pmod{26}$	2	17	24	15	19	14
plaintext	c	r	y	p	t	o

Remark: If $a = 1$, the Affine cipher becomes simply a Caesar cipher, that is, $C = E_K(m) = x + b \pmod{26}$.

Thank You