Tutorial -1

SOEN-321

Modular Arithmetic

- For integer a, b, m; we say:

  $a \equiv b \; mod \; m$ iff $a - b = km$ where k is an integer

- Examples:

  $17 \equiv 12 \; mod \; 5 \quad 17 - 12 = 1 \times 5$

  $12 \equiv 17 \; mod \; 5 \quad 12 - 17 = -1 \times 5$

  $2 = 12 \; mod \; 5$ 2 is the *residue* of $12 \; mod \; 5$ and $17 \; mod \; 5$

- The residue is an integer in $\{0,1, \ldots, m-1\}$
- Operations are $+, -, \times$; no division

Modular Arithmetic

Addition

- $(a + b) mod\ m = (a\ mod\ m + b\ mod\ m\ ) mod\ m$
- $(15 + 18)\ mod\ 7 \rightarrow 33\ mod\ 7 = 5$
- $(15\ mod\ 7 + 18\ mod\ 7\ ) mod\ 7 = (1 + 4)\ mod\ 7 = 5$

Subtraction

- $13 - 6\ \ mod\ 9 = 7$
- $5 - 35\ \ mod\ 9 = -30$ remember residue must be in {0,1,…,8}
- Add multiples of 9 to -30 till the result is in range {0,…,8}
- $-30 + 9 + 9 + 9 + 9 = 6$
- $5 - 35\ mod\ 9 = 6$

Modular Arithmetic

Multiplication

- $a \times b \, mod \, m = (a \, mod \, m \times b \, mod \, m \,) mod \, m$
- $3 \times 12 \, mod \, 4 \rightarrow 3 \times 0 \, mod \, 4 = 0$
- $5 \times 4 \, mod \, 6 \rightarrow 20 \, mod \, 6 = 2$

Question 1

Decrypt the ciphertext “GUVFPYNFFVFSHA” which was encrypted using the shift cipher?

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

$$C = (P + k) \; mod \; 26$$
$$P = (C - k) \; mod \; 26$$

Hints:

- Brute-force: Try all possible key values [0..25]
- $k = 0$ is trivial; $P = C$
- Decrypt first few letters and see if you can recognize a valid word or part of it

Question 1

Decrypt the ciphertext “GUVFPYNFFVFSHA” which was encrypted using the shift cipher?

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

$$C = (P + k) \ mod \ 26$$
$$P = (C - k) \ mod \ 26$$

K=1

G $\rightarrow (6 - 1) \ mod \ 26 = \ 5 \rightarrow F$

U $\rightarrow (20 - 1) \ mod \ 26 = 19 \rightarrow T$

V $\rightarrow (21 - 1) \ mod \ 26 = 20 \rightarrow U$

F $\rightarrow (5 - 1) \ mod \ 26 = 4 \rightarrow E$

K=2

G $\rightarrow (6 - 2) \ mod \ 26 = 4 \rightarrow E$

U $\rightarrow (20 - 2) \ mod \ 26 = 18 \rightarrow S$

V $\rightarrow (21 - 2) \ mod \ 26 = 19 \rightarrow T$

F $\rightarrow (5 - 2) \ mod \ 26 = 3 \rightarrow$D

K=3

G $\rightarrow (6 - 3) \ mod \ 26 = 3 \rightarrow D$

U $\rightarrow (20 - 3) \ mod \ 26 = 17 \rightarrow R$

V $\rightarrow (21 - 3) \ mod \ 26 = 18 \rightarrow S$

F $\rightarrow (5 - 3) \ mod \ 26 = 2 \rightarrow$C

Question 1

Decrypt the ciphertext “GUVFPYNFFVFSHA” which was encrypted using the shift cipher?

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

$$C = (P + k) \; mod \; 26$$
$$P = (C - k) \; mod \; 26$$

K=13

G → $(6 - 13) \; mod \; 26 = 19 \rightarrow T$

U → $(20 - 13) \; mod \; 26 = 7 \rightarrow H$

V → $(21 - 13) \; mod \; 26 = 8 \rightarrow I$

F → $(5 - 13) \; mod \; 26 = 18 \rightarrow S$

P → $(15 - 13) \; mod \; 26 = 2 \rightarrow C$

Y → $(24 - 13) \; mod \; 26 = 11 \rightarrow L$

N → $(13 - 13) \; mod \; 26 = 0 \rightarrow A$

F → $(5 - 13) \; mod \; 26 = 18 \rightarrow S$

F → $(5 - 13) \; mod \; 26 = 18 \rightarrow S$

V → $(21 - 13) \; mod \; 26 = 8 \rightarrow \mathrm{I}$

F → $(5 - 13) \; mod \; 26 = 18 \rightarrow S$

S → $(18 - 13) \; mod \; 26 = 5 \rightarrow F$

H → $(7 - 13) \; mod \; 26 = 20 \rightarrow U$

A → $(0 - 13) \; mod \; 26 = 13 \rightarrow \mathrm{N}$

Plaintext = THISCLASSISFUN

Question 2

Recover the key of an affine cipher if $p_1 = 5;\ p_2 = 7;\ c_1 = 12; c_2 = 8$

$$C = (\alpha P + \beta) \ \ mod\ 26$$

$$12 = (5\alpha + \beta) \ \ mod\ 26 \ \ (1)$$

$$8 = (7\alpha + \beta) \ \ mod\ 26 \ \ (2)$$

Subtract (2) – (1)

$$-4 = 2\alpha\ mod\ 26$$
$$22 = 2\alpha\ mod\ 26$$
$$11 = \alpha\ mod\ 13 \quad \rightarrow \alpha = 11$$

Division! How?
Check the end of slide

Substitute in (1)

$$12 = 5 \times 11 + \beta\ \ mod\ 26$$
$$-43 = \beta\ mod\ 26 \quad \rightarrow \beta = 9$$

Question 3

Recover the key of a Hill cipher when $P = \begin{bmatrix} 5 & 6 \\ 1 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 23 & 24 \\ 4 & 13 \end{bmatrix}$?

$$\begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} mod\ 26$$

$$\begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix}^{-1} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\frac{1}{p_1 p_4 - p_2 p_3} \begin{bmatrix} p_4 & -p_2 \\ -p_3 & p_1 \end{bmatrix} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\frac{1}{5-6} \begin{bmatrix} 1 & -6 \\ -1 & 5 \end{bmatrix} \begin{bmatrix} 23 & 24 \\ 4 & 13 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$-1 \begin{bmatrix} 1 & -6 \\ -1 & 5 \end{bmatrix} \begin{bmatrix} 23 & 24 \\ 4 & 13 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 6 \\ 1 & -5 \end{bmatrix} \begin{bmatrix} 23 & 24 \\ 4 & 13 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\begin{bmatrix} -23 + 6 \times 4 & -24 + 6 \times 13 \\ 23 - 5 \times 4 & 24 - 5 \times 13 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 54 \\ 3 & -41 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 11 \end{bmatrix} = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

Special Case of Division in Question 2

- When we have expression like: $a = bx \; mod \; m$, and $\gcd(a, b, m) = \alpha$, then you can factor out α from both sides
- Example

  $22 = 2a \; mod \; 26$ implies that $22 = 2a + 26k$ for some integer k

  The last expression is not modular arithmetic, so we can use division!

  So, we get $11 = a + 13k$, which we can convert it back to modular arithmetic as $11 = a \; mod \; 13$

  Also, since 26 is a multiple of 13, then $11 \; mod \; 13 \; \equiv 11 \; mod \; 26$.

  Therefore, residues in $mod \; 13$ are valid residues in $mod \; 26$