

Tutorial -1

SOEN-321

Modular Arithmetic

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

$a \equiv b \pmod{m}$ iff $a - b = km$ where k is an integer

- Examples:

$$17 \equiv 12 \pmod{5} \quad 17 - 12 = 1 \times 5$$

$$12 \equiv 17 \pmod{5} \quad 12 - 17 = -1 \times 5$$

$2 \equiv 12 \pmod{5}$ 2 is the *residue* of $12 \pmod{5}$ and $17 \pmod{5}$

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

Modular Arithmetic

Addition

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

Subtraction

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

Modular Arithmetic

Multiplication

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

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

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

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

$$C = (P + k) \bmod 26$$

$$P = (C - k) \bmod 26$$

K=1

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

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

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

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

K=2

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

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

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

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

K=3

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

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

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

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

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

$$C = (P + k) \bmod 26$$

$$P = (C - k) \bmod 26$$

K=13

$$G \rightarrow (6 - 13) \bmod 26 = 19 \rightarrow T$$

$$U \rightarrow (20 - 13) \bmod 26 = 7 \rightarrow H$$

$$V \rightarrow (21 - 13) \bmod 26 = 8 \rightarrow I$$

$$F \rightarrow (5 - 13) \bmod 26 = 18 \rightarrow S$$

$$P \rightarrow (15 - 13) \bmod 26 = 2 \rightarrow C$$

$$Y \rightarrow (24 - 13) \bmod 26 = 11 \rightarrow L$$

$$N \rightarrow (13 - 13) \bmod 26 = 0 \rightarrow A$$

$$F \rightarrow (5 - 13) \bmod 26 = 18 \rightarrow S$$

$$F \rightarrow (5 - 13) \bmod 26 = 18 \rightarrow S$$

$$V \rightarrow (21 - 13) \bmod 26 = 8 \rightarrow I$$

$$F \rightarrow (5 - 13) \bmod 26 = 18 \rightarrow S$$

$$S \rightarrow (18 - 13) \bmod 26 = 5 \rightarrow F$$

$$H \rightarrow (7 - 13) \bmod 26 = 20 \rightarrow U$$

$$A \rightarrow (0 - 13) \bmod 26 = 13 \rightarrow N$$

Plaintext = THISCLASSISFUN

Question 2

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

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

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

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

Subtract (2) - (1)

$$-4 = 2\alpha \mod 26$$

$$22 = 2\alpha \mod 26$$

$$11 = \alpha \mod 13 \rightarrow \alpha = 11$$

Division! How?
Check the end of slide

Substitute in (1)

$$12 = 5 \times 11 + \beta \mod 26$$

$$-43 = \beta \mod 26 \rightarrow \beta = 9$$

Special Case of Division in Question 2

- When we have expression like: $a = bx \bmod m$, and $\gcd(a, b, m) = \alpha$, then you can factor out α from both sides
- Example
 - $22 = 2a \bmod 26$ 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 $11 = a \bmod 13$
 - Also, since 26 is a multiple of 13, then $11 \bmod 13 \equiv 11 \bmod 26$.
 - Therefore, residues in $\bmod 13$ are valid residues in $\bmod 26$