Chapter 5 NUMBER THEORY

1. <u>**Introduction**</u>: Terminologies

Lexeme	**Meaning**
Plaintext	Original message to be sent in a secret way, or string of symbols in a given alphabet representing the message or text to be enciphered
Ciphertext	Modified, disguised version of the plaintext
Encipher, (encrypt)	Convert a plaintext into a ciphertext
Decypher, decrypt	Convert a ciphertext into a plaintext
Cipher	*Method* used to convert a plaintext into a ciphertext
Key	Data determining both a particular enciphering and the correpending deciphering rule, among all the possible ones: in the first case it is called *cipher key*, in the second *decipher key*
Cryptology	Science of enciphering messages
Cryptanalysis	Science of interpreting enciphered messages

Caesar cipher

The letters of the alphabet are shifted by some fixed amount.

Example:

`plaintext`	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
`ciphertext`	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D .

Then the message "ONE IF BY LAND AND TWO IF BY SEA"

Becomes "SRI MJ FC PERH ERH XAS MJ FC WIE"

A *Caesar cipher* is especially easy to implement on a computer using a scheme known as arithmetic mod 26.

$$m \bmod n$$

means the "remainder" we get when we divide m by n.

Theorem 1.1 (Euclid's division theorem)

For every integer m and positive integer n, there exist unique integers q and r such that $m = nq + r$ and $0 \le r < n$.

Definition 1.1

For integers m and n, we say $r = m \bmod n$ if $m - r$ is a multiple of n.

Exercise 1.1-1 Use The definition of m mod n to compute 10 mod 7 and -10 mod 7. What are q and r in each case?

Does $(-m)$ mod $n = -\,(m$ mod $n)$?

Exercise 1.1-2

How can you use the idea of m mod n to implement a Caesar cipher?

2. Modular Arithmetic

Goal: understand basic arithmetic operations, addition, subtraction, multiplication, division, and exponentiation behave when all arithmetic is done in mod n.

Exercise 2.1-1 Compute $21 \bmod 9$, $38 \bmod 9$,
$(21 \cdot 38) \bmod 9$, $(21 \bmod 9) \cdot (38 \bmod 9)$,
$(21+38) \bmod 9$, $(21 \bmod 9)+(38 \bmod 9)$.

Any observations?

Lemma 2.1 $i \bmod n = (i + kn) \bmod n$ for any integer k.

Lemma 2.2

$$
\begin{aligned}
(i+j) \bmod n &= [i + (j \bmod n)] \bmod n \\
&= [(i \bmod n) + j] \bmod n \\
&= [(i \bmod n) + (j \bmod n)] \bmod n
\end{aligned}
$$

$$
\begin{aligned}
(i \cdot j) \bmod n &= [i \cdot (j \bmod n)] \bmod n \\
&= [(i \bmod n) \cdot j] \bmod n \\
&= [(i \bmod n) \cdot (j \bmod n)] \bmod n
\end{aligned}
$$

We will use the notation Z_n to represent the integer set

$$\{0, 1, \ldots, n-1\}$$

In Z_n, addition and multiplication are defied by

$$+_n \qquad \text{and} \qquad \cdot_n$$

More precisely,

$$i +_n j = (i + j) \bmod n, \qquad i \cdot_n j = (i \cdot j) \bmod n$$

Theorem 2.3

Addition and multiplication mod *n* satisfy the commutative and associative laws, and multiplication distributes over addition.

Plaintext	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
Numerical equivalent	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

Caeser ciphers

Sender:

1. Transform plaintext to numerical equivalences.
2. Choose a key k, and use the corresponding cipher $C_k(p)=p+k \bmod n$, to cipher the numbers.

Receiver

1. Determine the decipher $D_k(c)=c-k \bmod n$, and decipher the numbers.
2. Transform the numbers back to original message.

Plain text	attacktoday
Numerical equivalent	0 19 19 0 2 10 19 14 3 0 24
Ciphertext (numerical) $C_5(p) = p + 5 \mod 26$	5 24 24 5 7 15 24 19 8 5 3
Ciphertext	FYYFHPYTIFD
Deciphered text (numerical) $D_5(c) = c - 5 \mod 26$	0 19 19 0 2 10 19 14 3 0 24
Deciphered text	attacktoday

3. Inverse and GCD

Affine cipher

Sender:

1. Transform plaintext to numerical equivalences.
2. Choose a key $k=(a,b)$, where a and n are **relative primes**.
3. Use the corresponding cipher
   $C_k(p)=ap+b$ mod n, to cipher the numbers.

Receiver

1. **There is a unique a' in Z_n such that $a'a=1$ mod n.**
2. Determine the decipher $D_k(c)=a'(c-b)$ mod n,
   and decipher the numbers.
3. Transform the numbers back to original message.

Plain text	attackatdawn
Numerical equivalent	0 19 19 0 2 10 0 19 3 0 22 13
Ciphertext (numerical) $C_{(7,10)}(p) = 7p + 10 \mod 26$	10 13 13 10 24 2 10 13 5 10 8 23
Ciphertext	KNNKYCKNFKIX
Deciphered text (numerical) $D_{(7,10)}(c) = 15c + 6 \mod 26$	0 19 19 0 2 10 0 19 3 0 22 13
Deciphered text	attackatdawn

Questions:

Q1. What is relative prime?

Q2. When a and n are relative primes, why there is a unique a' in Z_n such that $a'a=1 \bmod n$?

Q3. Why $D_k(c)=a'(c-b) \bmod n$ is the right decipher?

Answer to Q1

Definition Let $m_1,\ldots,m_k$ be integers which are not all 0. Their greatest common divisor (GCD) is the largest integer that divides all of $m_1,\ldots,m_k$.

Example gcd(24,8,12)=4, gcd(2,3)=1, gcd(-15,6)=3.

Definition Two integers m,n are called relative primes if

gcd(m,n)=1.

Answer to Q3

Lemma 3.1 If $a'a=1$ mod n, *then*

$$ax=b \bmod n$$

has the unique solution

$$x=a'b \bmod n$$

in Z_n.

Definition a' is called the multiplicative inverse of a in Z_n if $a'a=1$ mod n

Theorem 3.2 If an element of Z_n has a multiplicative inverse, then it has exactly one inverse.

Remark Theorem 3.2 answers the uniqueness part of Q2.

It remains to answer the existence part of Q2:

If a and n are relative primes, i.e. gcd(a,n)=1, then there exists a' such that $a'a=1$ mod n.

Theorem 3.3 A number a has a multiplicative inverse in Z_n iff there are integers x and y such that $ax + ny = 1$.

Lemma 3.4 Given a and n, if there exist integers x and y such that $ax + ny = 1$ then $gcd(a, n) = 1$.

We would like to show that if $gcd(a,n)=1$, then
There exists x,y such that $ax+ny=1$.

Recall Euclid's division theorem

For every integer m and positive integer n, there exist unique integers q and r such that $m = nq + r$ and $0 \leq r < n$.

The argument follows from Euclidean algorithm.