



MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Established by Dr. Nawal El Deghdy

Cryptography

ECE5632 - Spring 2026

Lecture 2A

Dr. Farah Raad

ECE5632 - Spring 2026-Dr. Farah Raad

The First British Higher Education in Egypt



Lecture Topic

Modular Arithmetic and More Historical Ciphers

Short Introduction to Modular Arithmetic

Why do we need to study modular arithmetic?

- Extremely important for asymmetric cryptography (RSA, elliptic curves etc.)
- Some historical ciphers can be elegantly described with modular arithmetic (Caesar and affine cipher).



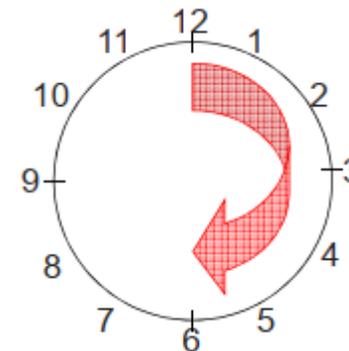
Short Introduction to Modular Arithmetic

- Generally speaking, most cryptosystems are based on **sets of numbers** that are
 - 1. discrete** (sets with integers are particularly useful)
 - 2. finite** (i.e., if we only compute with a finely many numbers)

Seems too abstract? --- Let's look at a finite set with discrete numbers we are quite familiar with: a clock. Consider the hours on a clock. If you keep adding one hour, you obtain:

$1h, 2h, 3h, \dots, 11h, 12h, 1h, 2h, 3h, \dots, 11h, 12h, 1h, 2h, 3h, \dots$

- ✓ Even though we keep adding one hour, we never leave the set.



Short Introduction to Modular Arithmetic

- We develop now an arithmetic system which allows us to **compute** in finite sets of integers
- It is crucial to have an operation which keeps the numbers within limits“, i.e., after addition and multiplication they should never leave the set .

Let's look at a general way of dealing with arithmetic in such finite sets.

Example : We consider the set of the nine numbers: $\{0,1,2,3,4,5,6,7,8\}$

We can do regular arithmetic as long as the results are smaller than 9. For instance:

$$2 \times 3 = 6 \quad \& \quad 4+4 = 8$$

But what about 8+4?

Since $8+4 = 12$, and $12/9$ has a remainder of 3, we write: **$8+4 \equiv 3 \pmod{9}$**



Modulus Operation

Definition: Modulus Operation

Let a, r, m be integers and $m > 0$. We write
$$a \equiv r \pmod{m}$$

if $(a-r)$ is divisible by m . $\ggg m/(a-r) = \text{integer}$

- “ m ” is called the **modulus**
- “ r ” is called the **remainder**

$$\begin{aligned}x \bmod n &= r \\ a \bmod m &= r\end{aligned}$$

❖ (\equiv) is mean the reading of equation be $(a \bmod m \text{ equal } r)$

Examples for modular reduction.

- Let $a= 12$ and $m= 9$: $12 \equiv 3 \pmod{9}$
- Let $a= 34$ and $m= 9$: $34 \equiv 7 \pmod{9}$
- Let $a= -7$ and $m= 9$: $-7 \equiv 2 \pmod{9}$

✓ (you should check whether the condition m divides $(r-a)$ holds in each of the 3 cases)



Modulus Operation

Computation of the Remainder

$$a = q \cdot m + r \quad \text{for } 0 \leq r < m$$

Since; $a - r = q \cdot m$ (m divides $a-r$)

$$r = a - q \cdot m$$

we can now write: $a \equiv r \pmod{m}$

✓ Note that $r \in \{0, 1, 2, \dots, m-1\}$.

Example: Let $a = 42$ and $m = 9$.

Then $42 = 4 \cdot 9 + 6$ and therefore $42 \equiv 6 \pmod{9}$.



Properties of Modular Arithmetic (1)

➤ The Remainder Is Not Unique

It is somewhat surprising that for every given modulus m and number a , there are (infinitely) many valid remainders.

$$r = a \pm m$$

Example: We want to reduce 12 modulo 9. Here are several results which are correct according to the definition:

- $12 \equiv 3 \pmod{9} \rightarrow 3$ is a valid remainder since $9 \mid (3-12)$ >>>> $12-9=3$
- $12 \equiv 21 \pmod{9} \rightarrow 21$ is a valid remainder since $9 \mid (21-12)$ >>>> $12+9=21$
- $12 \equiv -6 \pmod{9} \rightarrow -6$ is a valid remainder since $9 \mid (-6-12)$ >>>> $12-9=3 - 9= -6$
- “ x/y ” means “ x divides y ”. There is a system behind this behavior. The set of numbers

$$\{\dots, -24, -15, -6, 3, 12, 15, 24, \dots\}$$

- There are eight other equivalence classes for the modulus 9 (*equivalence class*)

$$\{\dots, -27, -18, -9, 0, 9, 18, 27, \dots\}$$

$$\{\dots, -26, -17, -8, 1, 10, 19, 28, \dots\}$$

...

$$\{\dots, -19, -10, -1, 8, 17, 26, 35, \dots\}$$



Properties of Modular Arithmetic (2)

➤ Which remainder do we choose?

By convention, we usually agree on the **smallest positive integer** r as remainder. This integer can be computed as

$$a = qm + r \quad \text{where } 0 \leq r < m$$

Diagram illustrating the division equation $a = qm + r$. A box labeled "quotient" points to q , and a box labeled "remainder" points to r . The condition $0 \leq r < m$ is written to the right.

- Example: $a=12$ and $m=9$

$$12 = 1 \times 9 + 3 \quad \rightarrow r = 3$$

- ✓ Remark: This is just a convention. Algorithmically we are free to choose any other valid remainder to compute our crypto functions.



Properties of Modular Arithmetic (3)

➤ How do we perform modular division?

First, note that rather than performing a division, we prefer to multiply by the inverse.

$$b / a \equiv b \times a^{-1} \pmod{m}$$

The inverse a^{-1} of a number a is defined such that:

$$a \times a^{-1} \equiv 1 \pmod{m}$$

Ex: What is $5 / 7 \pmod{9}$?

The inverse of $7 \pmod{9}$ is 4 since $7 \times 4 \equiv 28 \equiv 1 \pmod{9}$, hence:

$$5 / 7 \equiv 5 \times 4 = 20 \equiv 2 \pmod{9}$$



Properties of Modular Arithmetic (4)

➤ Modular reduction can be performed at any point during a calculation

Let's look first at an example. We want to compute $3^8 \bmod 7$ (note that exponentiation is extremely important in public-key cryptography).

1. Approach: Exponentiation followed by modular reduction

$$3^8 = 6561 \equiv 2 \pmod{7}$$

✓ Note that we have the intermediate result 6561 even though we know that the final result can't be larger than 7.

2. Approach: Exponentiation with intermediate modular reduction

$$3^8 = 3^4 \times 3^4 = 81 \times 81$$

At this point we reduce the intermediate results 81 modulo 7:

$$3^8 = 81 \times 81 \equiv 4 \times 4 \pmod{7}$$

$$4 \times 4 = 16 \equiv 2 \pmod{7}$$

General rule: For most algorithms it is advantageous to reduce intermediate results as soon as possible.



Integer Rings

➤ An Algebraic View on Modulo Arithmetic: The Ring Z_m (1)

We can view modular arithmetic in terms of sets and operations in the set. By doing arithmetic modulo m we obtain the **integer ring Z_m** with the following properties:

- **Closure:** We can add and multiply any two numbers and the result is always in the ring.
- Addition and multiplication are **associative**, i.e., for all $a, b, c \in Z_m$
$$a + (b + c) = (a + b) + c$$
$$a \times (b \times c) = (a \times b) \times c$$
and addition is **commutative**: $a + b = b + a$
- The **distributive law** holds: $a \times (b + c) = (a \times b) + (a \times c)$ for all $a, b, c \in Z_m$
- There is the **neutral element 0 with respect to addition**, i.e., for all $a \in Z_m$
$$a + 0 \equiv a \pmod{m}$$
- For all $a \in Z_m$, there is always an **additive inverse element $-a$** such that
$$a + (-a) \equiv 0 \pmod{m}$$
- There is the **neutral element 1 with respect to multiplication**, i.e., for all $a \in Z_m$
$$a \times 1 \equiv a \pmod{m}$$
- The **multiplicative inverse a^{-1}**
$$a \times a^{-1} \equiv 1 \pmod{m}$$
exists only for some, but not for all, elements in Z_m .



Integer Rings

➤ An Algebraic View on Modulo Arithmetic: The Ring Z_m (2)

Roughly speaking, a ring is a structure in which we can always add, subtract and multiply, but we can only divide by certain elements (namely by those for which a multiplicative inverse exists).

Ex: We consider the ring $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

The elements 0, 3, and 6 do not have inverses since they are not coprime to 9.

The inverses of the other elements 1, 2, 4, 5, 7, and 8 are:

$$1^{-1} \equiv 1 \pmod{9}$$

$$2^{-1} \equiv 5 \pmod{9}$$

$$4^{-1} \equiv 7 \pmod{9}$$

$$5^{-1} \equiv 2 \pmod{9}$$

$$7^{-1} \equiv 4 \pmod{9}$$

$$8^{-1} \equiv 8 \pmod{9}$$



Integer Rings

➤ Notes

1. Mathematical operation ■ \gggg (+, -, *, /, exp)

$$X \blacksquare Y \bmod m = r$$

$$[X \bmod m \blacksquare Y \bmod m] \bmod m = r$$

Example: $7 + 8 \bmod 4 = [7 \bmod 4 + 8 \bmod 4] \bmod 4 = [3 + 0] \bmod 4 = 3$

2. if $a < m$ □ $r = a$ **Not need for Computation**

Example: $3 = r \bmod 8$ □ $r = 3$

3. $-a = r \bmod m$ a is -ve □ $r = -a + m$

Example: $-3 = r \bmod 10$ $r = -3 + 10 = 7$

4. $a = r \bmod a$ $m = a$ □ $r = 0$

Example: $10 = r \bmod 10$ $r = 0$



More Historical Ciphers

- Two historical ciphers to introduce modular arithmetic with integers.
- A very popular special case of the substitution cipher is the **Caesar cipher and Affine Cipher.**



Shift (or Caesar) Cipher

- Ancient cipher, allegedly used by Julius Caesar to communicate with his army.
- Replaces each plaintext letter by another one. It simply shifts the letters in the alphabet by a constant number of steps.

Let $k, x, y \in \{0, 1, \dots, 25\}$

- Encryption: $y = e_k(x) \equiv x + k \pmod{26}$
- Decryption: $x = d_k(x) \equiv y - k \pmod{26}$

- Replacement rule is very simple: Take letter that follows after k positions in the alphabet
Needs mapping from letters \rightarrow numbers:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25



Shift (or Caesar) Cipher

Example Let the key be $k = 17$, and the plaintext is:

$$\text{ATTACK} = x_1, x_2, \dots, x_6 = 0, 19, 19, 0, 2, 10.$$

The ciphertext is then computed as

$$y_1, y_2, \dots, y_6 = 17, 10, 10, 17, 19, 1 = \text{rkkrtb}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25



Is the shift cipher secure?

No! several attacks are possible, including:

- Exhaustive key search (key space is only 26!)
- Letter frequency analysis, similar to attack against substitution cipher



Affine Cipher

- Extension of the shift cipher: rather than just adding the key to the plaintext, we also multiply by the key
- We use for this a key consisting of two parts: $k = (a, b)$

Let $k, x, y \in \{0, 1, \dots, 25\}$

- Encryption: $y = e_k(x) \equiv a x + b \pmod{26}$
- Decryption: $x = d_k(y) \equiv a^{-1}(y - b) \pmod{26}$

The decryption is easily derived from the encryption function:

$$a \cdot x + b \equiv y \pmod{26}$$

$$a \cdot x \equiv (y - b) \pmod{26}$$

$$x \equiv a^{-1} \cdot (y - b) \pmod{26}$$

$$a \times a^{-1} \equiv 1 \pmod{26}$$



Affine Cipher

Example Let the key be $k = (a, b) = (9, 13)$, and the plaintext be

$$\text{ATTACK} = x_1, x_2, \dots, x_6 = 0, 19, 19, 0, 2, 10.$$

The inverse a^{-1} of a exists and is given by $a^{-1} = 3$. The ciphertext is computed as

$$y_1, y_2, \dots, y_6 = 13, 2, 2, 13, 5, 25 = \text{nccnfz}$$

Let $k, x, y \in \{0, 1, \dots, 25\}$

- Encryption: $y = e_k(x) \equiv a x + b \pmod{26}$
- Decryption: $x = d_k(y) \equiv a^{-1}(y - b) \pmod{26}$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25



Is the affine cipher secure?

No! The key space is only a bit larger than in the case of the shift cipher:

$$\begin{aligned}\text{key space} &= (\# \text{values for } a) \times (\# \text{values for } b) \\ &= 12 \times 26 = 312\end{aligned}$$

- Again, several attacks are possible, including:
 - Exhaustive key search and letter frequency analysis, similar to the attack against the substitution cipher



Example: Suppose that an Affine cipher $E(x) = (ax + b) \pmod{26}$ enciphers h as **X** and q as **Y**. Find the cipher (that is, determine a and b).

Ans. : $C=E(p)=(k_1 \times p + k_2) \pmod{26}$, suppose that $k_1=a$, $p=x$, $k_2=b$.

Plaintext Alphabet	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
Plaintext Value	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

We see that $h \rightarrow X$ means $E(7) = 23$ and $q \rightarrow Y$ means $E(16) = 24$.

That is, $a \cdot 7 + b \equiv 23 \pmod{26}$ and $a \cdot 16 + b \equiv 24 \pmod{26}$.

Subtracting gives $16a - 7a \equiv 1 \pmod{26}$

$\pmod{26} = 9a \equiv 1 \pmod{26}$. So that $9a \equiv 1 \pmod{26}$. Therefore, $a = 9^{-1}$

Finally, we substitute $a = 3$ into either of the earlier equations and solve for b,

i.e., $3 \cdot 7 + b \equiv 23 \pmod{26}$ implies $b = 2$.

In summary, $E(x) = (3x + 2) \pmod{26}$.



Thank You!

See You next Lectures!!
Any Question?

THE FIRST BRITISH HIGHER EDUCATION IN EGYPT

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt

Tel: +202383711146 **Fax:** +20238371543 **Postal code:** 12451

Email: info@msa.eun.eg **Hotline:** 16672 **Website:** www.msa.edu.eg

