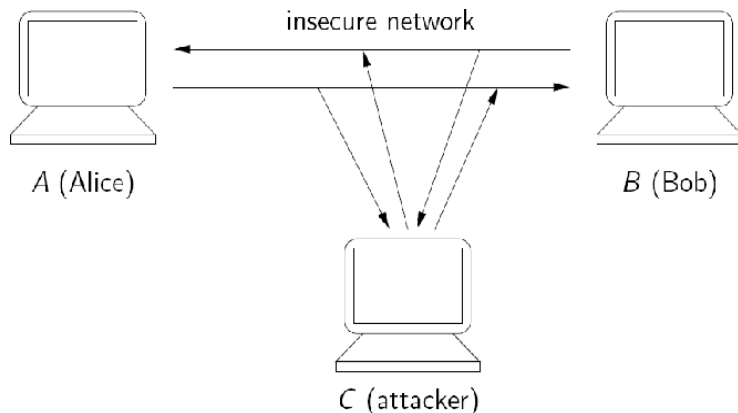INT202
Complexity of Algorithms
Number Theory and Cryptography

2020-2021

These Lectures

1. Review of math basics

2. Fundamentals of number theory

3. Encryption/decryption schemes

Security of Communications

Alice talks to Bob on an insecure network.

⇒ Use cryptography to make communications secure;
for example, encrypt messages to preserve secrets.

Security of Communications (cont.)

To protect sensitive information, we must ensure the following goals are met:

- ➢ **Data Integrity:** Information should not be altered without detection.

- ➢ **Authentication:** Agents involved in the communication must be identified.

- ➢ **Authorization:** Agents operating on sensitive information must be authorised to perform those operations.

- ➢ **Nonrepudiation:** If binded by contracts, agents cannot drop out of their obligations without being detected.

- ➢ **Confidentiality:** Sensitive information must be kept secret from agents that are not authorised to access it.

Security of Communications (cont.)

▷ To protect sensitive information, techniques based on algorithms and communication protocols have been developed.

▷ Many of these techniques use number theory, e.g., the popular RSA (Rivest Shamir Adleman) scheme.

▷ It is not only about number theory! Security protocols need be proven correct; this uses formal methods (another area of computer science that will not be addressed here).

REVIEW OF MATH BASICS

1   INTEGER ARITHMETIC

In integer arithmetic, we use a set and a few operations. You are familiar with this set and the corresponding operations, but they are reviewed here to create a background for modular arithmetic.
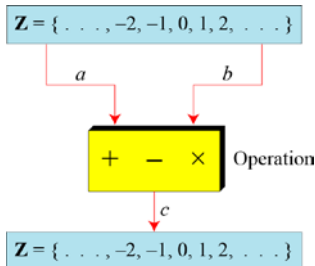
1.1 Set of Integers

The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity.

Figure *The set of integers*

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

In cryptography, we are interested in three binary operations applied to the set of integers. A binary operation takes two inputs and creates one output.

Figure *Three binary operations for the set of integers*

1.2   Continued

The following shows the results of the three binary operations on two integers. Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

What about in their inverse operations?

1.2   Continued

Example

The following shows the results of the three binary operations on two integers. Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

What about in their inverse operations?

What about division?

$3 \div 2 =?$ not an integer!

1.3 Integer Division

$$a = q \times n + r$$

In integer arithmetic, if we divide a by n, we can get q and r.

Example *finding the quotient and the remainder*

$$0 \leq r < |n|$$

Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm.

1.3 Continued

Figure *Division algorithm for integers*

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

a

n (positive) → $a = q \times n + r$ → r (nonnegative)

q

$$Z = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$$
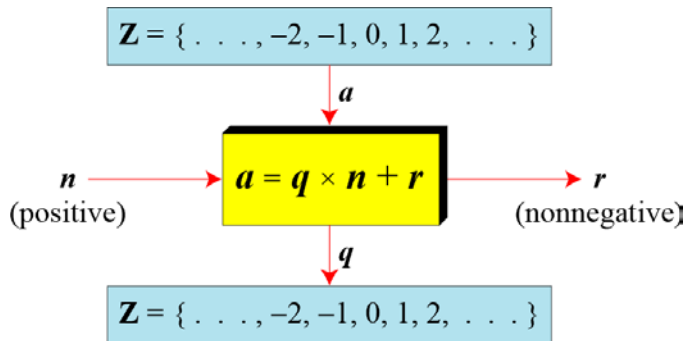
Example

r and q are negative when a is negative.
How can we apply the restriction that r needs to be positive?
The value of q - 1 ↔ r + n, to make r positive.

$$-255 = (-23 \times 11) + (-2) \qquad \leftrightarrow \qquad -255 = (-24 \times 11) + 9$$

1.4 Divisbility

If a is not zero and we let r = 0 in the division relation, we get

$$a = q \times n$$

If the remainder is zero, $\quad n \mid a$ ← The divisibility of a by n is denoted by the symbol

If the remainder is not zero, $\quad n \nmid a$

1.4 *Continued*

Example

a. The integer 4 divides the integer 32 because $32 = 8 \times 4$. We show this as

$$4 \mid 32$$

b. The number 8 does not divide the number 42 because $42 = 5 \times 8 + 2$. There is a remainder, the number 2, in the equation. We show this as

$$8 \nmid 42$$

a. We have $13 \mid 78$, $7 \mid 98$, $-6 \mid 24$, $4 \mid 44$, and $11 \mid (-33)$.

b. We have $13 \nmid 27$, $7 \nmid 50$, $-6 \nmid 23$, $4 \nmid 41$, and $11 \nmid (-32)$.

1.4   Continued

Properties

Property 1: if a|1, then a = ±1.

Property 2: if b|a and a|b, then a = ±b.

Property 3: if b|a and c|b, then c|a.

Property 4: if a|b and a|c, then
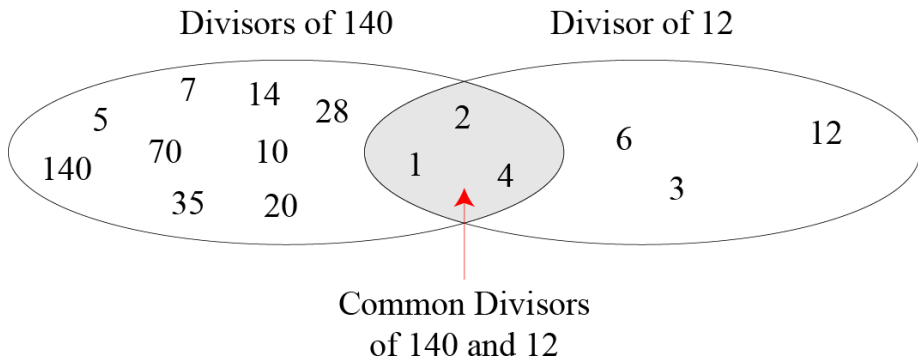*a| (m × b + n × c), where m*
and n are arbitrary integers

1.4 Continued

a. Since 3|15 and 15|45,

   according to the third property, 3|45.

b. Since 3|15 and 3|9,

   according to the fourth property,

   $3|(15 \times 2 + 9 \times 4)$, which means 3|66.

1.4 Continued

Common divisors of twointegers

Divisors of 140   Divisor of 12

7   14   28   2
5   6   12
140   70   10   1   4
35   20   3

Common Divisors
of 140 and 12

1.4   Continued

Note   **Greatest Common Divisor**

The greatest common divisor of two positive integers is the largest integer that can divide both integers.

Note   **Euclidean Algorithm**

Fact: gcd (a, 0) = a

Lemma: Let a, b, q, and r be integer such that $a = bq + r$ and $b \neq 0$. Then gcd(a, b) = gcd(b, r).

1.4 Continued

Lemma: Let a, b, q, and r be integer such that
a = bq + r and b ≠ 0. Then gcd(a, b) =
gcd(b, r).

Proof. Let d = gcd(a, b) and e = gcd(b, r). We need to show that d = e.

Since d|a and d|b, d divides a − bq = r.

So d is a common divisor of b and r. Hence d ≤ e.

Similarly, as e|b and e|r, e divides bq + r =a.

Thus, e is a common divisor of both a and b, so e ≤ d.

This proves that d = e.

Note

When gcd (a, b) = 1, we say that a and b
are relatively prime.

20

1.4 Continued

1. Given $26 = 6 \times 4 + 2$,find the gcd (26,6) and gcd(6,2).

Solution

a=26 , b=6, r=2

common divisors of 26 and 6: (1,2)

common divisors of 6 and 2: (1,2)

gcd(a,b)=2, gcd(b,r)=2

2. Given $60 = 24 \times 2 + 12$ Find the gcd (60,24) and gcd (24,12).

Solution

a=60 , b=24, r=12

common divisors of 60 and 24: (1,2,3,4,6,12)

common divisors of 24 and 12: (1,2,3,4,6,12)

gcd(a,b)=12, gcd(b,r)=12

21

1.4   Continued

```
def gcd(a,b)
    assert a>=b and b>=0 and a+b>0
    return gcd(b, a%b) if b>0 else a
```

modulo

Example

Find the greatest common divisor of 25 and 60.

Solution

$r1 = 60, r2 = 25,$ $q = 2,$ $r = 10$
$r1 = 25, r2 = 10,$ $q = 2,$ $r = 5$
$r1 = 10, r2 = 5,$ $q = 2,$ $r = 0$
$r1 = 5, r2 = 0$
We have gcd (25, 60) = 5.

1.4 Continued

Extended Euclidean Algorithm

Given two integers a and b, we often need to find other two integers, s and t, such that

$$s \times a + t \times b = \gcd(a, b)$$

The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.

1.4   Continued

Extended Euclidean Algorithm

$$s \times a + t \times b = \gcd(a, b)$$

$$r_1 \leftarrow a; \quad r_2 \leftarrow b;$$
$$s_1 \leftarrow 1; \quad s_2 \leftarrow 0; \quad \text{(Initialization)}$$
$$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$$

while $(r_2 > 0)$
{

   $q \leftarrow r_1 / r_2;$

   $r \leftarrow r_1 - q \times r_2;$
   $r_1 \leftarrow r_2; \ r_2 \leftarrow r;$ (Updating r's)

   $s \leftarrow s_1 - q \times s_2;$
   $s_1 \leftarrow s_2; \ s_2 \leftarrow s;$ (Updating s's)

   $t \leftarrow t_1 - q \times t_2;$
   $t_1 \leftarrow t_2; \ t_2 \leftarrow t;$ (Updating t's)

}

$\gcd(a, b) \leftarrow r_1; \ s \leftarrow s_1; \ t \leftarrow t_1$

1.4   Continued

Example

1. Given a = 161 and b = 28, find gcd (a, b) and the values of s and t.

Solution

We get gcd (161, 28) = 7, $s = -1$ and $t = 6$.

2. Given a = 391 and b = 299 , find gcd (a, b) and the values of s and t.

Solution

We get gcd (391, 299) = 23, s = -3, and t = 4.

2   MODULAR ARITHMETIC

The division relationship ($a = q \times n + r$) discussed in the previous section has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are interested in only one of the outputs, the remainder r.

2.1 Modulo Operator

The modulo operator is shown as mod (or % in some languages). The second input (n) is called the modulus. The output r is called the residue.

Division algorithm and modulo operator
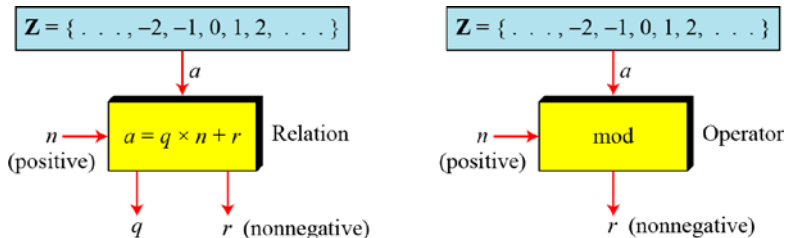
2.2 Set of Residues

The modulo operation creates a set, which in modular arithmetic is referred to as *the set of least residues modulo n, or Z_n.*

Some Z_n sets

$$\mathbf{Z}_n = \{\, 0, 1, 2, 3, \ \ldots, \ (n-1) \,\}$$

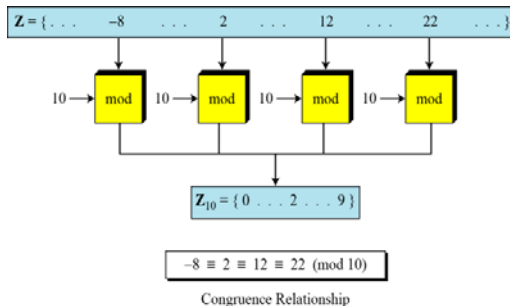| $\mathbf{Z}_2 = \{\, 0, 1 \,\}$	$\mathbf{Z}_6 = \{\, 0, 1, 2, 3, 4, 5 \,\}$	$\mathbf{Z}_{11} = \{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \,\}$

2.3 Congruence

*To show that two integers are congruent, we use the
congruence operator (≡): a≡b(mod m)*
A is congruent to B modulo m
For example, we write:

$$2 \equiv 12 \ (\text{mod } 10) \qquad 13 \equiv 23 \ (\text{mod } 10)$$

$$3 \equiv 8 \ (\text{mod } 5) \qquad 8 \equiv 13 \ (\text{mod } 5)$$

Congruence Relationship

2.3 Continued

Residue Classes

A residue class [a] or [a]ₙ is the set of integers congruent modulo n:

$$\{\ldots, a - 3n, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \ldots\}.$$

$$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$
$$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$
$$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$
$$[3] = \{\ldots, -12, -7, -5, 3, 8, 13, 18, \ldots\}$$
$$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

2.4 Operation in Z_n

The three binary operations that we discussed for the set Z can also be defined for the set Z_n. The result may need to be mapped to Z_n using the mod operator

Binary operations in Z_n

Operations

| $(a + b) \bmod n = c$ |
| $(a - b) \bmod n = c$ |
| $(a \times b) \bmod n = c$ |

$\mathbf{Z}_n = \{ 0, 1, 2, \ldots, (n-1) \}$
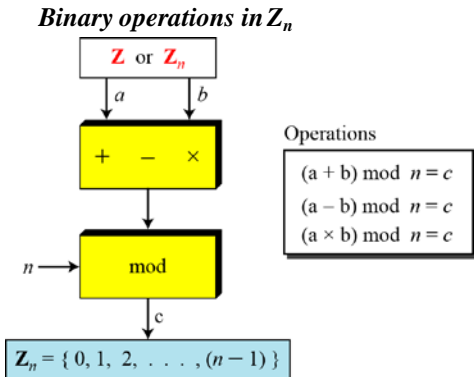
2.4 Continued

Properties of mod operator

First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Example

The following shows the application of the above properties:

$(37 + 99) \bmod 6 = 136 \bmod 6 = 4$
$[(37 \bmod 6) + (99 \bmod 6)] \bmod 6 = (1+3) \bmod 6 = 4$

2.4   *Continued*

Example

In arithmetic, we often need to find the remainder of powers of 10 when divided by an integer.

$$10^n \bmod x = (10 \bmod x)^n \qquad \text{Applying the third property } n \text{ times.}$$

$$10 \bmod 3 = 1 \quad \rightarrow \quad 10^n \bmod 3 = (10 \bmod 3)^n = 1$$
$$10 \bmod 9 = 1 \quad \rightarrow \quad 10^n \bmod 9 = (10 \bmod 9)^n = 1$$
$$10 \bmod 7 = 3 \quad \rightarrow \quad 10^n \bmod 7 = (10 \bmod 7)^n = 3^n \bmod 7$$

2.4 Continued

Example

We have been told in arithmetic that the remainder of an integer divided by 3 is the same as the remainder of the sum of its decimal digits. We write an integer as the sum of its digits multiplied by the powers of 10.

$$a = a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0$$

For example: $6371 = 6 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 1 \times 10^0$

$a \bmod 3 = (a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0) \bmod 3$

Prop.2
$= (a_n \times 10^n) \bmod 3 + \cdots + (a_1 \times 10^1) \bmod 3 + (a_0 \times 10^0) \bmod 3$
$= (a_n \bmod 3) \times (10^n \bmod 3) + \cdots + (a_1 \bmod 3) \times (10^1 \bmod 3) +$

Prop.3
$(a_0 \bmod 3) \times (10^0 \bmod 3)$
$= a_n \bmod 3 + \cdots + a_0 \bmod 3$
$= (a_n + \cdots + a_1 + a_0) \bmod 3$

2.5   *Inverse*

Additive Inverse

In Z_n, two numbers a and b are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

Note

In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n.

2.5   Inverse
Multiplicative Inverse

In Z_n, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

Note

In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo n.

2.5   Inverse

Example

Example 1
Find the multiplicative inverse of 8 in Z_{10}.
• Solution
  There is no multiplicative inverse because gcd $(10, 8) = 2 \neq 1$.

Example 2
Find all multiplicative inverses in Z_{10}
• Solution
(1, 1), (3, 7) and (9, 9).

2.5   *Inverse*

The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and
gcd (n, b) = 1.
The multiplicative inverse of b is the value of t after being mapped to Z_n.

Denote the multiplicative inverse of an element b by $b^{-1} (mod\ n)$

2.5.1 Inverse - *extended Euclidean algorithm*

Using extended Euclidean algorithm to
find multiplicative inverse

$$r_1 \leftarrow n; \quad r_2 \leftarrow b;$$
$$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$$

while $(r_2 > 0)$
{
$$q \leftarrow r_1 \ / \ r_2;$$

$$r \leftarrow r_1 - q \times r_2;$$
$$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$$

$$t \leftarrow t_1 - q \times t_2;$$
$$t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$$
}
if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

2.5.1 Continued

Find the multiplicative inverse of 11 in Z_{26}.

Answer:
So b=11 and n=26. Now we use the Extended Euclidean Algorithm with
a=n=26 and b=11.

Column b on the last row has the value 1, so
gcd(n, b) = 1.
So we need the value of column t_2 on the last
row. This is -7.
t_2 mod n = (-7) mod 26 = 19.
The multiplicative inverse of 11 modulo 26 is 19.

	n	b	q	r	t1	t2
Row 1	26	11	2	4	0	1
Row 2	11	4	2	3	1	-2
Row 3	4	3	1	1	-2	5
Row 4	3	1	3	0	5	-7

$r_1 \leftarrow n; \quad r_2 \leftarrow b;$
$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$

while ($r_2 > 0$)
{
  $q \leftarrow r_1 / r_2;$

  $r \leftarrow r_1 - q \times r_2;$
  $r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

  $t \leftarrow t_1 - q \times t_2;$
  $t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$

}
if ($r_1 = 1$) then $b^{-1} \leftarrow t_1$

2.5.1 Continued

Example

Find the multiplicative inverse of 11 in Z_{26}.

Answer:
So b=11 and n=26. Now we use the Extended Euclidean Algorithm with a=n=26 and b=11.

Column b on the last row has the value 1, so gcd(n, b) = 1.

So we need the value of column t2 on the last row. This is -7.

t2 mod n = (-7) mod 26 = 19.

The multiplicative inverse of 11 modulo 26 is 19.

	n	b	q	r	t1	t2
Row 1	26	11	2	4	0	1
Row 2	11	4	2	3	1	-2
Row 3	4	3	1	1	-2	5
Row 4	3	1	3	0	5	-7

$r_1 \leftarrow n; \quad r_2 \leftarrow b;$
$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$

while $(r_2 > 0)$
{
  $q \leftarrow r_1 / r_2;$

  $r \leftarrow r_1 - q \times r_2;$
  $r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

  $t \leftarrow t_1 - q \times t_2;$
  $t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$
}
if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

41

2.5.1 Continued

Example

Find the multiplicative inverse of 11 in Z_{26}.

Answer:
So b=11 and n=26. Now we use the Extended Euclidean Algorithm with
a=n=26 and b=11.

Column b on the last row has the value 1, so
gcd(n, b) = 1.
So we need the value of column t2 on the last
row. This is -7.
t2 mod n = (-7) mod 26 = 19.
The multiplicative inverse of 11 modulo 26 is 19.

	n	b	q	r	t1	t2
Row 1	26	11	2	4	0	1
Row 2	11	4	2	3	1	-2
Row 3	4	3	1	1	-2	5
Row 4	3	1	3	0	5	-7
	1	0	-	-	-7	-

$r_1 \leftarrow n; \quad r_2 \leftarrow b;$
$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$

while $(r_2 > 0)$
{
$\quad q \leftarrow r_1 / r_2;$

$\quad r \leftarrow r_1 - q \times r_2;$
$\quad r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

$\quad t \leftarrow t_1 - q \times t_2;$
$\quad t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$
}
if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

42

2.6   Different Sets

Some Z_n and Z_{n*} sets

$$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n : \gcd(a, n) = 1\}$$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$Z_6^* = \{1, 5\}$

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$Z_{10}^* = \{1, 3, 7, 9\}$

We need to use Zn when additive inverses are needed; we need to use Zn when multiplicative inverses are needed.*

Cryptography often uses two more sets: Z_p and Z_p^*. The modulus in these two sets is a prime number.

$$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
$$Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

3 MATRICES

In cryptography we need to handle matrices.
This topic belongs to a special branch of algebra called
linear algebra.

3.1 Definition

A matrix of size $l \times m$

m columns

Matrix **A**: l rows

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix}$$

Examples of matrices

$$\begin{bmatrix} 2 & 1 & 5 & 11 \end{bmatrix}$$
Row matrix

$$\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}$$
Column matrix

$$\begin{bmatrix} 23 & 14 & 56 \\ 12 & 21 & 18 \\ 10 & 8 & 31 \end{bmatrix}$$
Square matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$
0

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
I
Identity matrix

3.2   Operations and Relations

Example

The following figure shows an example of addition and subtraction.

Addition and subtraction of matrices

$$\begin{bmatrix} 12 & 4 & 4 \\ 11 & 12 & 30 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} + \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

C = A + B

$$\begin{bmatrix} -2 & 0 & -2 \\ -5 & -8 & 10 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} - \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$
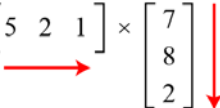
D = A − B

3.2   Continued

Example

The following figure shows the product of a row matrix (1✕3) by a column matrix (3✕1). The result is a matrix of size 1 ✕1.

Figure *Multiplication of a row matrix by a columnmatrix*

$$\begin{bmatrix} 53 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \end{bmatrix} \times \begin{bmatrix} 7 \\ 8 \\ 2 \end{bmatrix}$$

In which: $53 = 5 \times 7 + 2 \times 8 + 1 \times 2$

3.2   Continued

Example

The following figure shows the product of a 2 × 3 matrix by a 3 × 4 matrix. The result is a 2 × 4 matrix.

Figure *Multiplication of a 2 × 3 matrix by a 3 × 4 matrix*

$$
\underset{\mathbf{C}}{\begin{bmatrix} 52 & 18 & 14 & 9 \\ 41 & 21 & 22 & 7 \end{bmatrix}} = \underset{\mathbf{A}}{\begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix}} \times \underset{\mathbf{B}}{\begin{bmatrix} 7 & 3 & 2 & 1 \\ 8 & 0 & 0 & 2 \\ 1 & 3 & 4 & 0 \end{bmatrix}}
$$

3.2 Continued

Example

The following figure shows an example of scalar multiplication.

Figure *Scalar multiplication*

$$\begin{matrix} \mathbf{B} & & k & & \mathbf{A} \end{matrix}$$

$$\begin{bmatrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{bmatrix} = 3 \times \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix}$$

3.3 Determinant

The determinant of a **square matrix A** *of size m* $\times$ *m denoted as det (A) is a scalar calculated recursively as shown below:*

1. If $m = 1$, det $(\mathbf{A}) = a_{11}$

2. If $m > 1$, det $(\mathbf{A}) = \displaystyle\sum_{i=1...m} (-1)^{i+j} \times a_{ij} \times$ det $(\mathbf{A}_{ij})$

   where A_{ij} is a matrix obtained from A by deleting the i-th row and j-th column.

Note

The determinant is defined only for a square matrix.

3.4   Residue Matrices

Cryptography uses residue matrices:
In Zn, all operations on residue matrices are
performed the same as for the integer matrices
except that the operations are done in modular
arithmetic.
A residue matrix has a multiplicative inverse if the
determinant of the matrix has a multiplicative inverse
in Zn => gcd(det(A), n) = 1.

4 LINEAR CONGRUENCE

Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in Z_n.

How to solve linear equation?

4.1 Single-Variable Linear Equations

Equations of the form ax ≡ b (mod n) might have no solution or a limited number of solutions.

Assume that the gcd $(a, n) = d.$

If $d \nmid b$, there is no solution.

If $d \mid b$, there are d solutions.

Example

Solve the equation 10 $x \equiv$ 2(mod 15).

Solution

First we find the gcd (10, 15) = 5. Since 5 does not divide 2, we have no solution.

Example

Solve the equation 14 $x \equiv$ 12 (mod 18).

Solution

Division in $\mathbb{Z}_n^*$ is defined by the equation $a/b \equiv ab^{-1} \pmod{n}$.

$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod 9 \quad \rightarrow \ x \equiv 6 \, (7^{-1}) \pmod 9$

$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod 9 = 6$

$x_1 = x_0 + 1 \times (18/2) = 15$

4.1   Continued

Solve the equation $3x + 4 \equiv 6 \pmod{13}$.

Solution

First we change the equation to the form $ax \equiv b \pmod{n}$. We add
−4 (the additive inverse of 4) to both sides, which give $3x$
$\equiv 2 \pmod{13}$. Because gcd (3, 13) = 1, the equation has only
one solution, which is $x_0 = (2 \times 3^{-1}) \bmod 13 = (2 \times 9) \bmod 13$
= 5. We can see that the answer satisfies the original equation: 3
$\times 5 + 4 \equiv 6 \pmod{13}$.