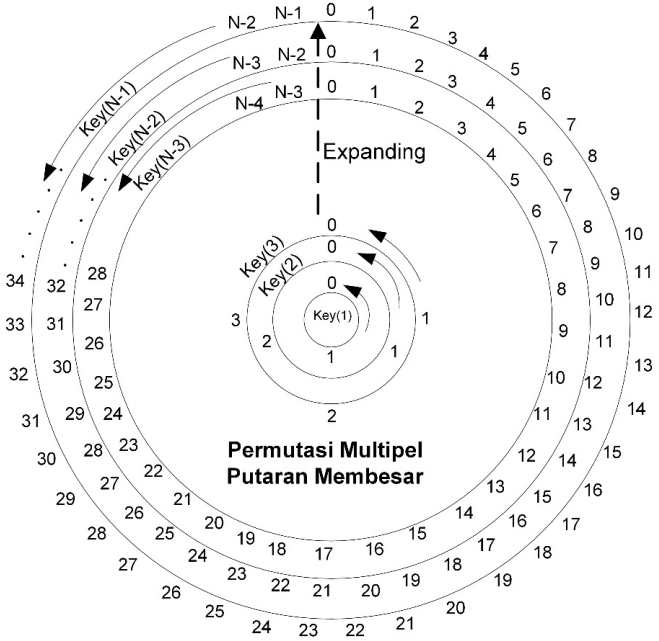


Dr. Yohan Suryanto, S.T, M.T

Semester Genap 2019/2020

MATHEMATICS OF CRYPTOGRAPHY

Modular Arithmetic, Congruence, and Matrices

source:

1. Behrouz Foroyzan, The McGraw-Hill Companies
2. Stallings, William. "Cryptography and Network Security“

Outline

1. Integer Arithmetic
2. Modular Arithmetic
3. Matrices
4. Linear Congruence

1 INTEGER ARITHMETIC

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.

Topics:

1. Set of Integers
2. Binary Operations
3. Integer Division
4. Divisibility
5. Euclidean Algorithm
6. Linear Diophantine Equations

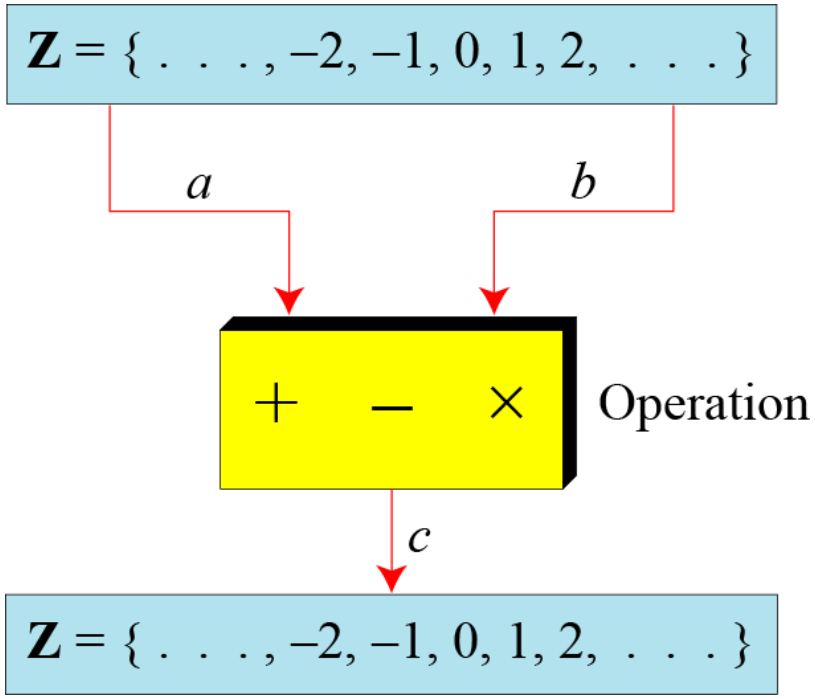
Set of Integers

The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity (Figure 2.1).

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

Binary Operations

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.



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.

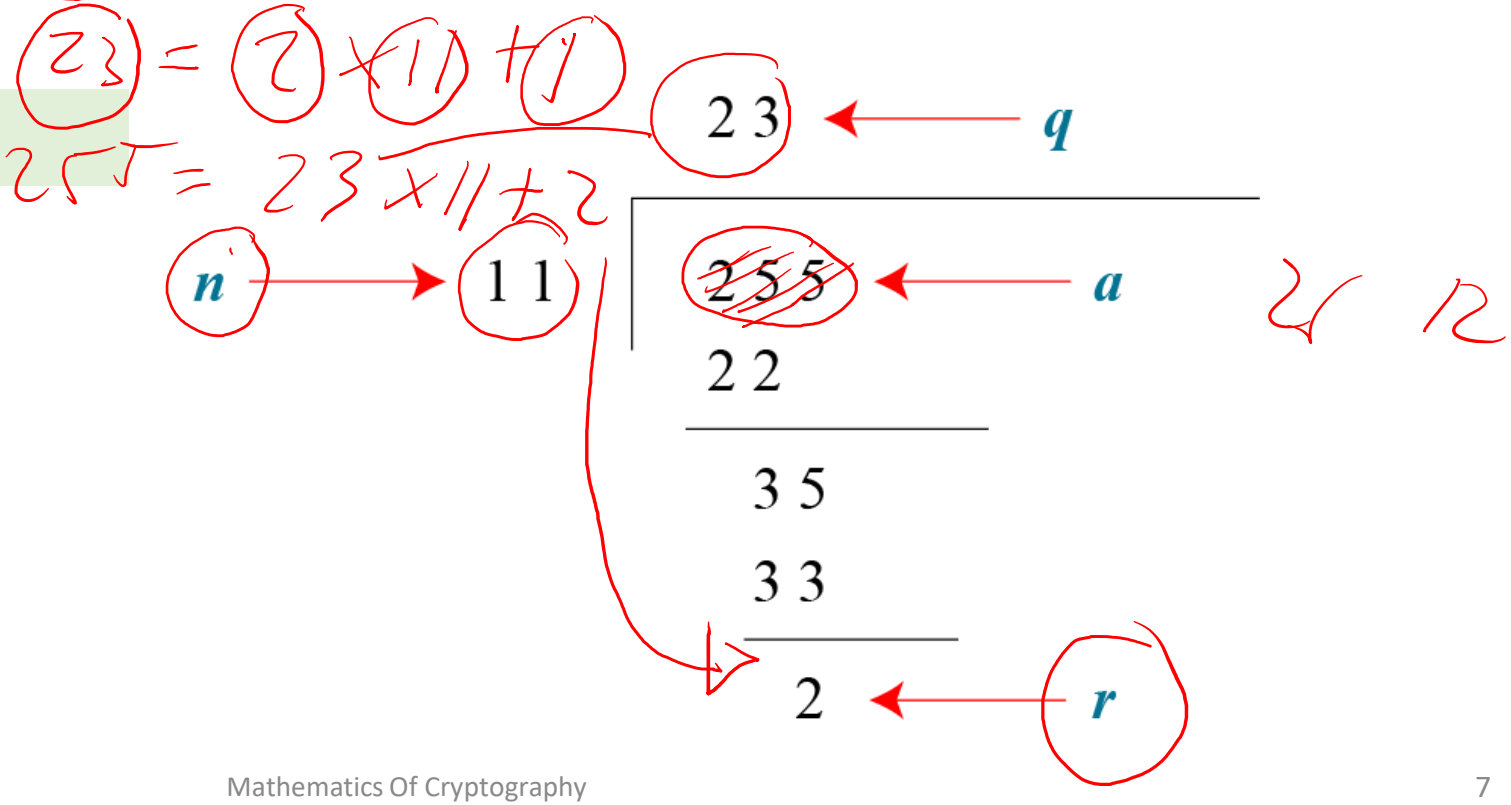
Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

Integer Division

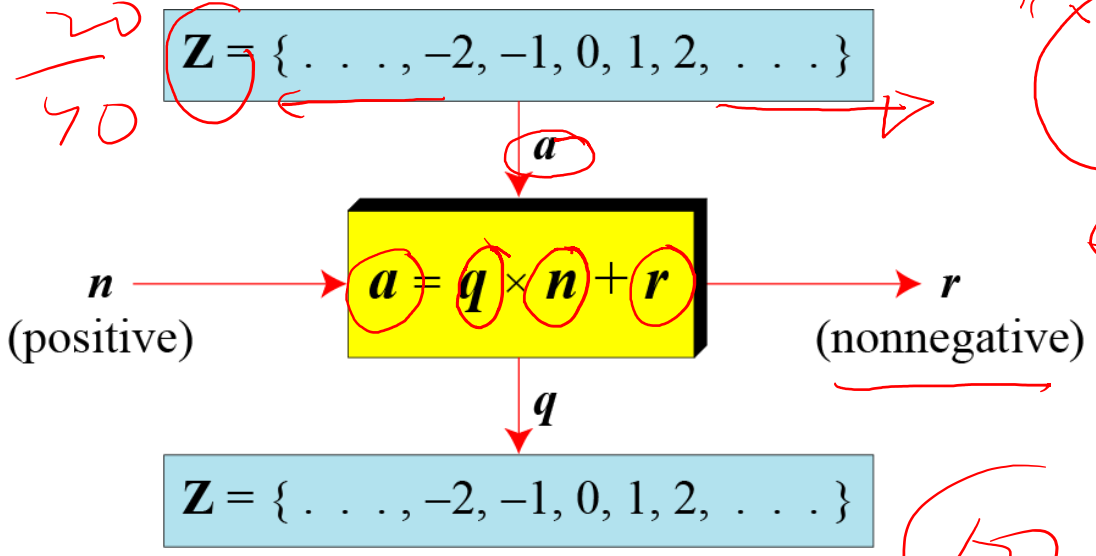
In integer arithmetic, if we divide a by n, we can get q and r . The relationship between these four integers can be shown as

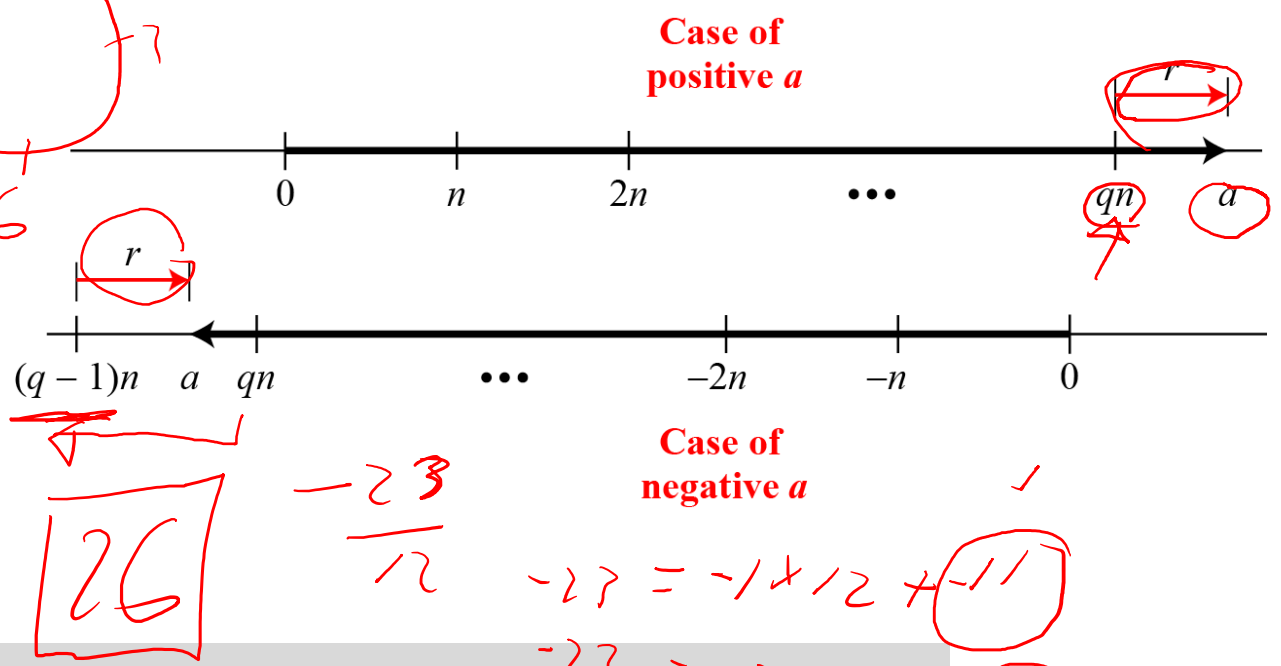
$$a = q \times n + r$$

255 = 23 x 11 + 2



Integer Division: non negative r





For negative r → q-1 and n+r, example:

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

Divisibility

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, $n|a$; *example:* $4|32$

If the remainder is not zero, $n \nmid a$; *example:* $8 \nmid 42$

Property 1: if $a|1$, *then* $a = \pm 1$.

Property 2: if $a|b$ *and* $b|a$, *then* $a = \pm b$.

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

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

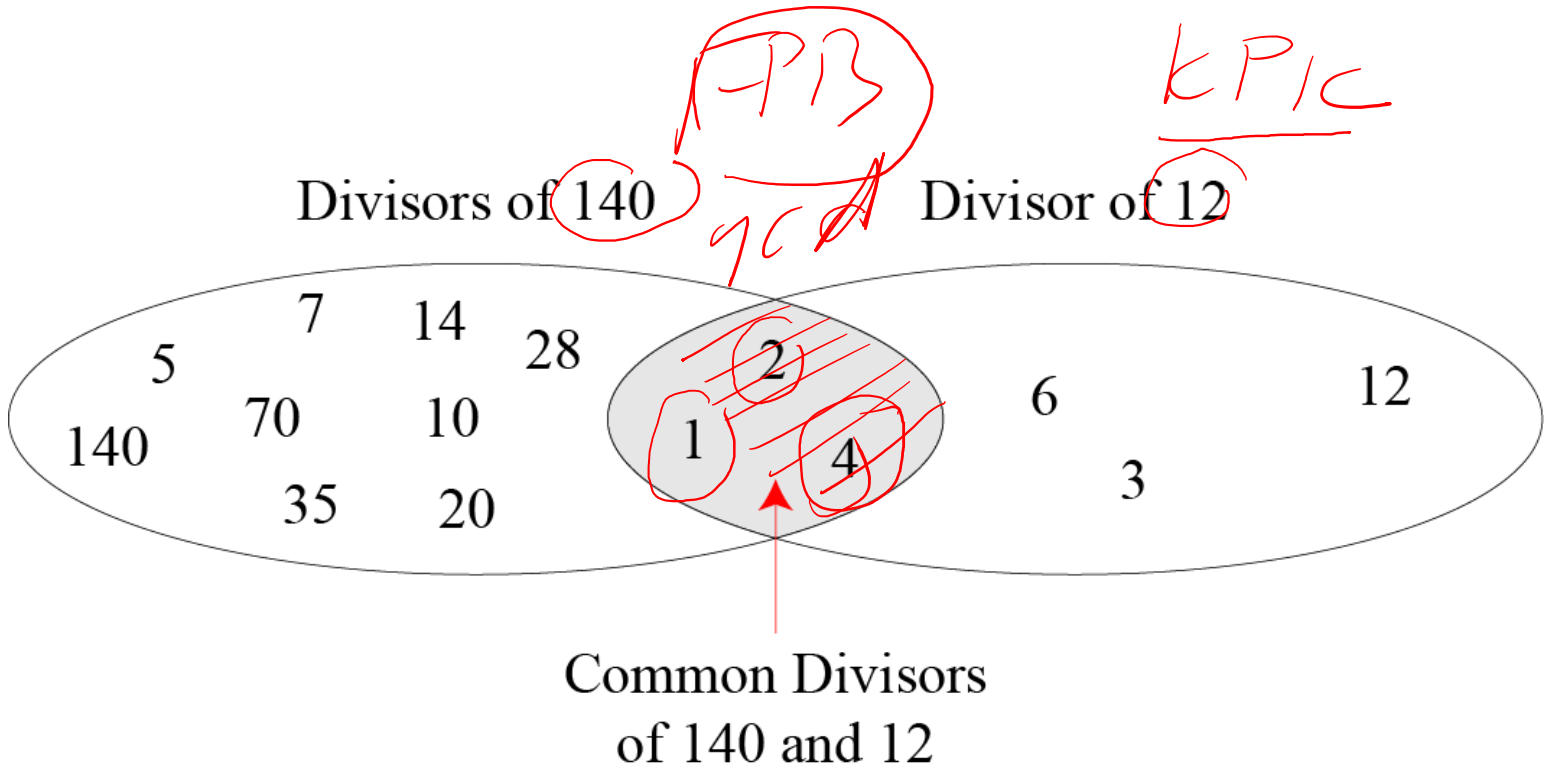
Divisibility Example

1. Since 3|15 and 15|45, then according to third property 3|45
2. Since 3|9 and 3|15, then according to fourth property 3|24

Fact 1: The integer 1 has only one divisor, itself.

Fact 2: Any positive integer has at least two divisors, 1 and itself (but it can have more).

Common divisors of two integers



Faktor Prima

140	
2	70
2	35
5	7
7	1

Faktor Prima

12	
2	6
2	3
3	1

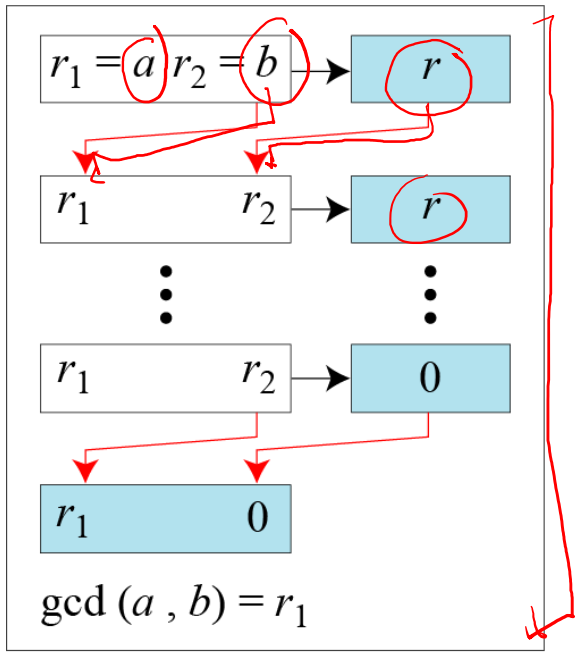
FPB (GCD) 2x2 = 4

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

Euclidean Algorithm

Fact 1: gcd (a, 0) = a

Fact 2: gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b



a. Process

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$ (Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

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

$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$

}

gcd (a, b) $\leftarrow r_1$

b. Algorithm

gcd(140,12) = gcd(12,8)
= gcd(8,4)
= gcd(4,0)
= 4

gcd(35,11) = gcd(11,2)
= gcd(2,1)
= gcd(1,0)
= 1

gcd(75,5) = gcd(5,0)
= 5

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

Finding gcd using euclidian

Find the greatest common divisor of 2740 and 1760.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

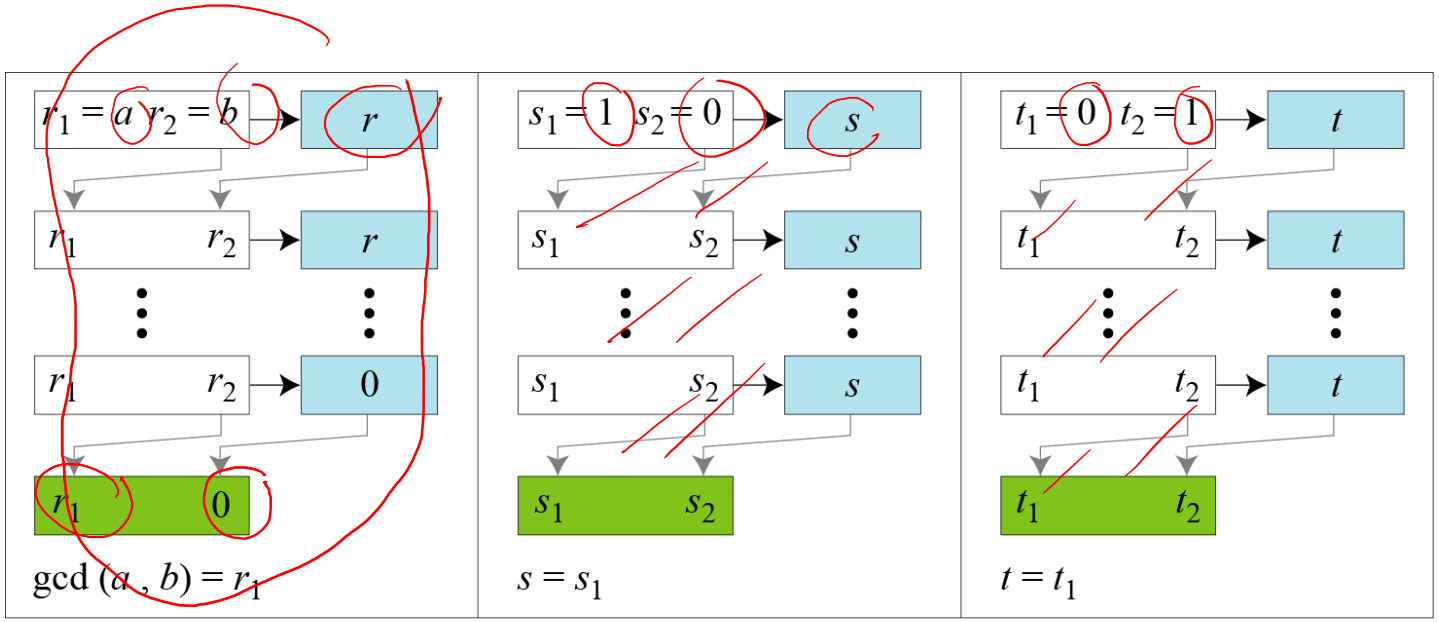
We have gcd (2740, 1760) = 20.

Find the greatest common divisor of 25 and 60.

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

We have gcd (25, 65) = 5.

Extended Euclidean Algorithm



a. Process

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

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

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

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

Extended Euclidean Algorithm: example

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

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

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

Linear Diophantine Equation

A linear Diophantine equation of two variables is ax + by = c.

Particular solution:

$x_0 = (c/d)s$ and $y_0 = (c/d)t$

General solutions:

$x = x_0 + k\,(b/d)$ and $y = y_0 - k(a/d)$ where k is an integer

Find the particular and general solutions to the equation

21x + 14y = 35.

Gcd(21,14) = 7; since 7|35

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$

General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$

Linear Diophantine Equation Cont

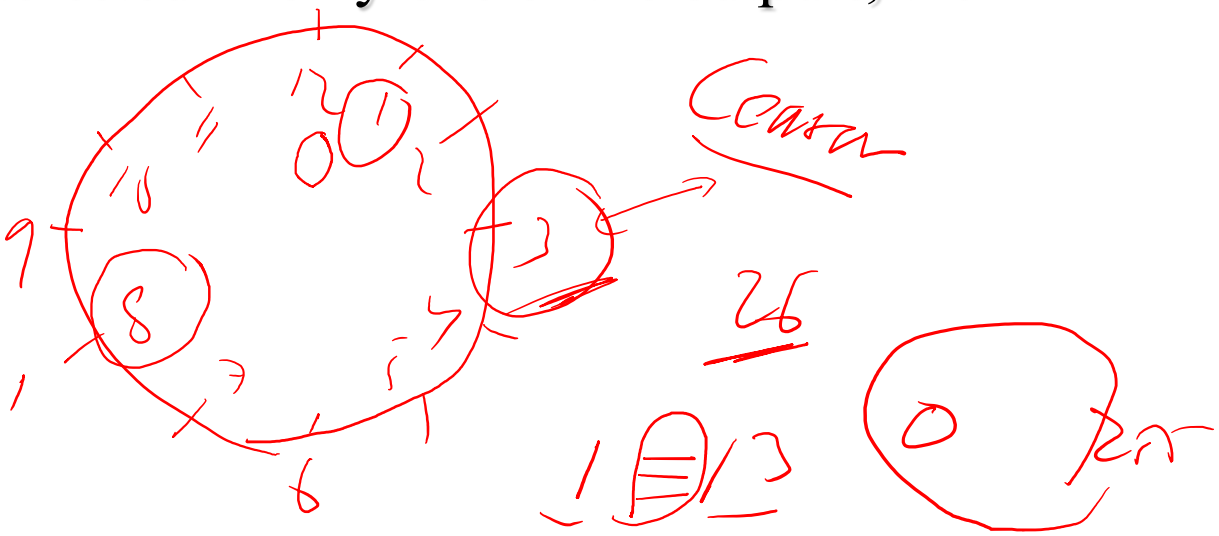
For example, imagine we want to cash a $100 check and get some $20 and some $5 bills. We have many choices, which we can find by solving the corresponding Diophantine equation 20x + 5y = 100. Since d = gcd (20, 5) = 5 and 5 | 100, the equation has an infinite number of solutions, but only a few of them are acceptable in this case The general solutions
with x and y nonnegative are

(0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0).

2 MODULAR ARITHMETIC

MODULAR ARITHMETIC

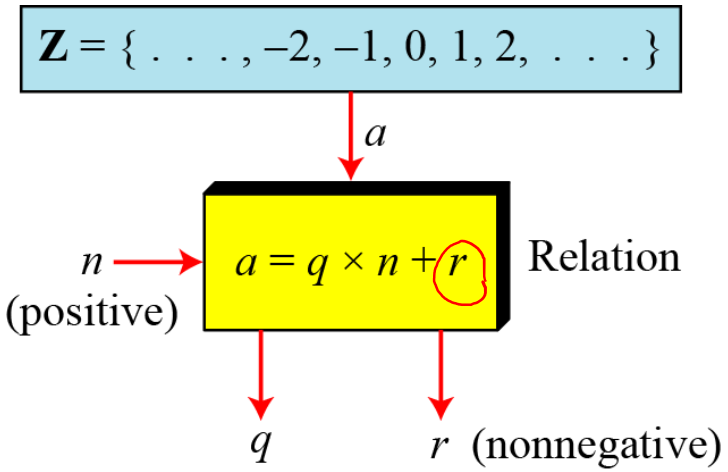
The division relationship ($a = q \times n + r$) discussed in the previous section has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are interested in only one of the outputs, the remainder r.

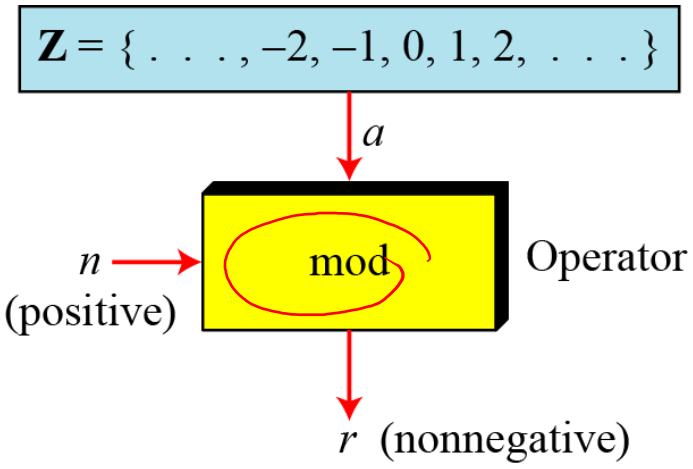


Topics:

1. Modular Operator
2. Set of Residues
3. Congruence
4. Operations in Z_n
5. Addition and Multiplication Tables
6. Different Sets

Modulus Operator





The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.

Examples:

a. 27 mod 5 = 2

b. 36 mod 12 = 0

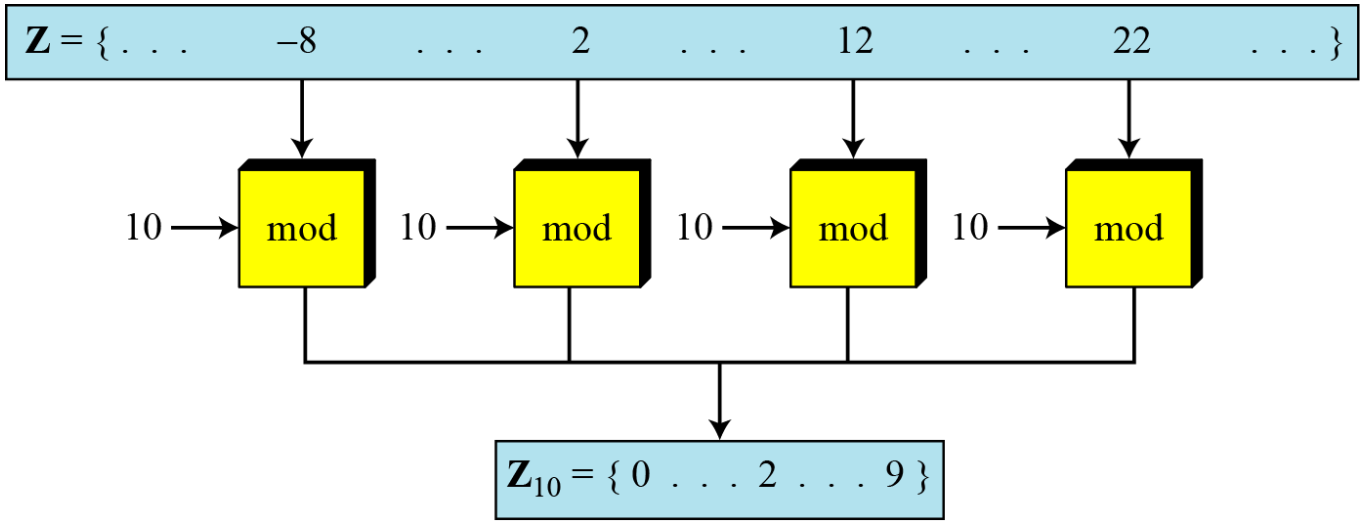
c. –18 mod 14 = 10

d. –7 mod 10 = 3

Set of Residues

- The set of least residues modulo n, or Z_n.
- To show that two integers are congruent, we use the congruence operator (≡). For example, we write:

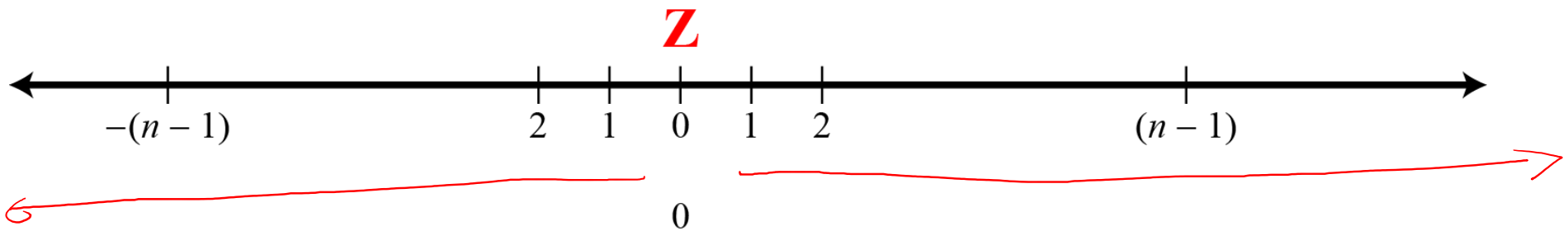
$2 \equiv 12 \bmod 10$; $5 \equiv 15 \bmod 10$

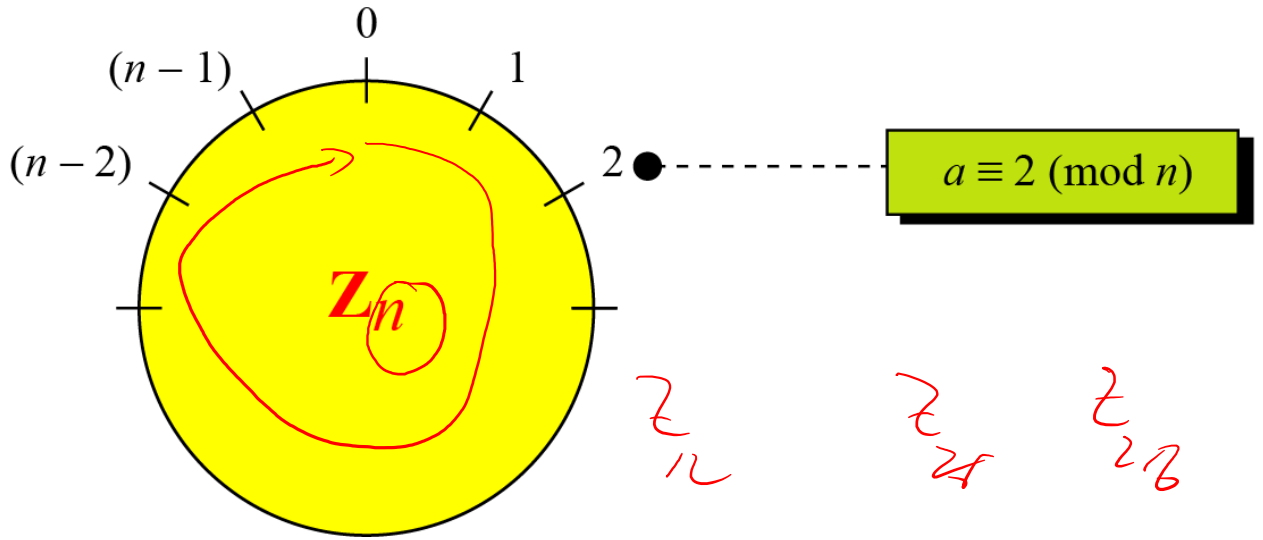


$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

Set of Residues Cont





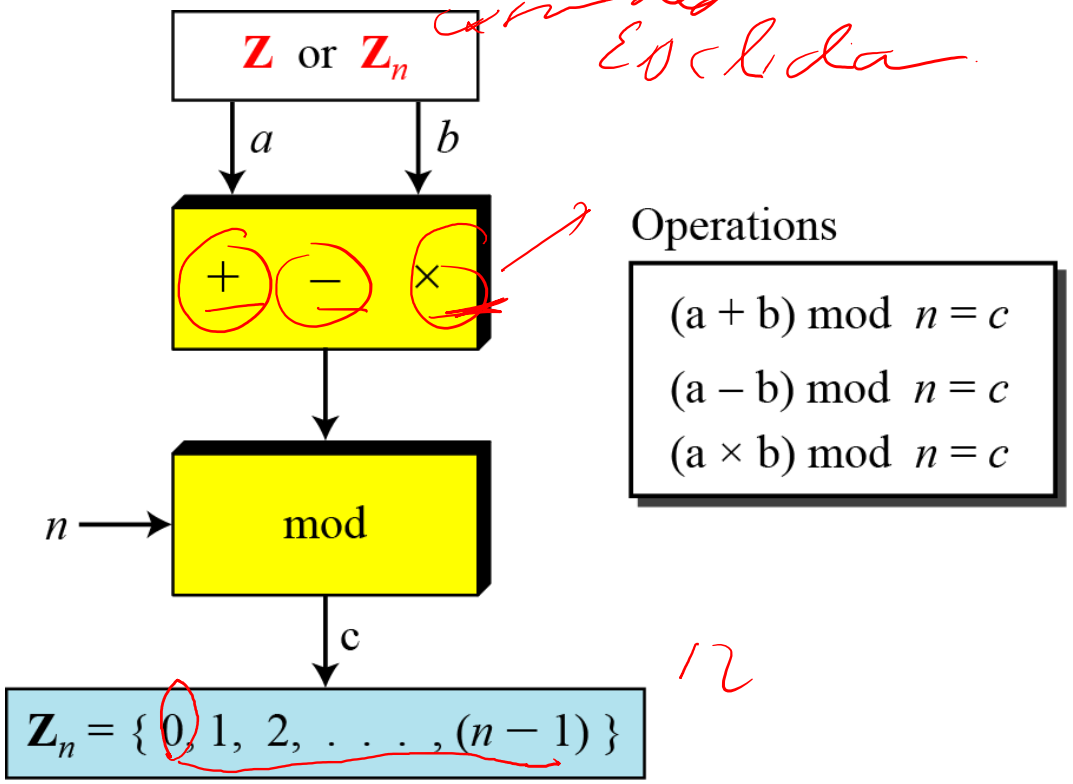
Example in daily day life: clock

A residue class [a] or $[a]_n$ is the set of integers congruent modulo n.

For n = 5; [2] = { …,-8,-3,2, 7, 12, …}

Operation in Zn

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



Examples:

a. Add 7 to 14 in Z_{15}

   21 mod 15 = 6

b. Subtract 11 from 7 in Z_{13}

   -4 mod 13 = 9

c. Multiply 11 by 7 in Z_{20}.

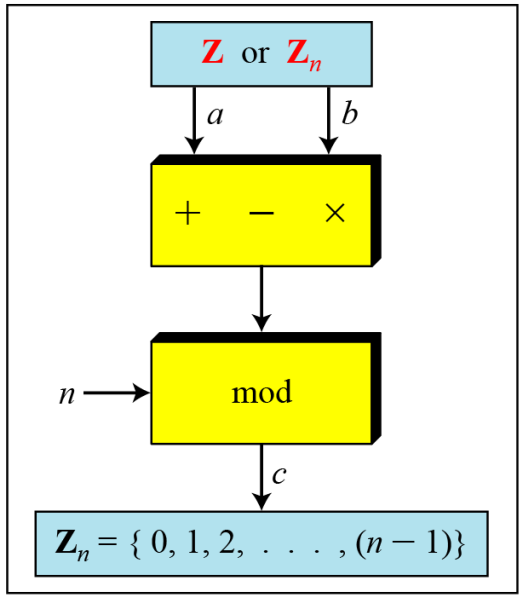
   77 mod 20 = 17

Properties of Modulus Operation

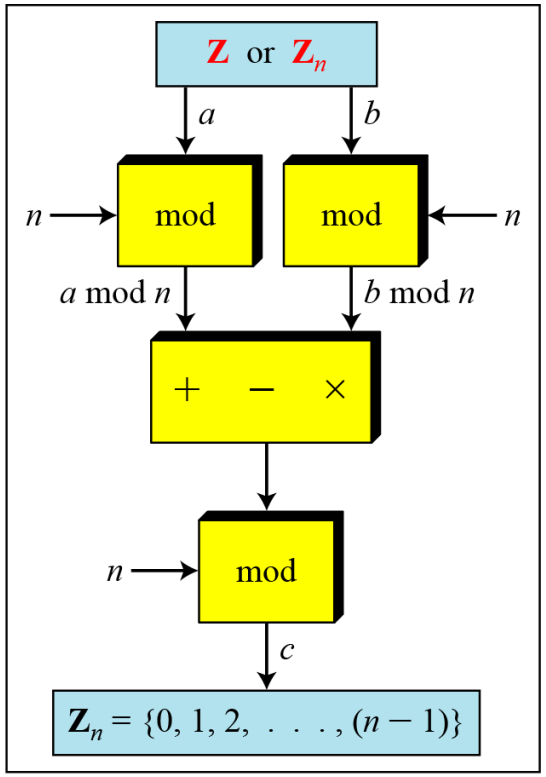
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$



a. Original process



b. Applying properties

Examples:

1. $(35 + 48) \bmod 11 = (2 + 4) \bmod 11 = 6$
2. $(33 - 17) \bmod 16 = (1 - 1) \bmod 11 = 0$
3. $(33 \times 17) \bmod 16 = (1 \times 1) \bmod 11 = 1$

Properties of Modulus Operation Cont

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

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

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

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

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

Example:

Since $6371 = 6 \times 10^3 + 3 \times 10^2 + 7\ 10^1 + 1$

Then $6371 \bmod 3 = ((6 \times 10^3 \bmod 3) + (3 \times 10^2) \bmod 3 + (7 \times 10^1) \bmod 3 + 1 \bmod 3) \bmod 3$

$= (6 \bmod 3 + 3 \bmod 3 + 7 \bmod 3 + 1 \bmod 3) \bmod 3$

$= (0 + 0 + 1 + 1) \bmod 3$

$= 2$

Inverses

Additive Inverse

$a + b \equiv 0 \bmod n$

Multiplicative Inverse

$a \times b \equiv 1 \bmod n$

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

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.

Example of the Inverse

Find all additive inverse pairs in Z_{10}.

Solution

The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

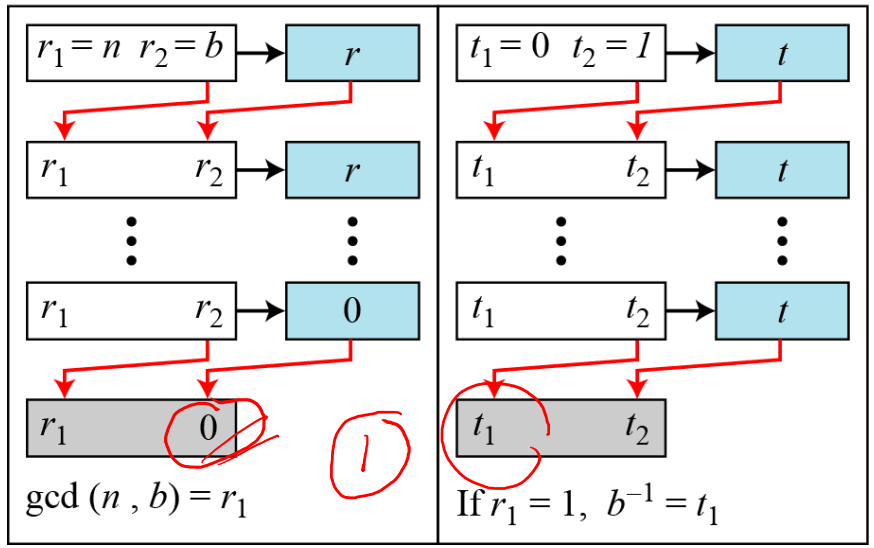
Find multiplicative inverse 7 in Z_{10}.

Solution

$$3 \text{ since } 7 \times 3 \bmod 10 = 21 \bmod 10$$
$$= 1$$

Finding Inverses Multiplicative

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.



a. Process

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

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

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

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

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

b. Algorithm

Finding Inverses Multiplicative: Examples

1. Find the inverse of 12 in Z_{26}.

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	−2
6	12	2	0	1	−2	13
	2	0		−2	13	

The gcd (26, 12) is 2; the inverse does not exist.

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

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

The gcd (26, 11) is 1; the inverse of 11 is –7 or 19.

Zn and Zn* sets

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbf{Z}_6^* = \{1, 5\}$

$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

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

$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$

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

Matrices

In cryptography we need to handle matrices. Although this topic belongs to a special branch of algebra called linear algebra, the following brief review of matrices is necessary preparation for the study of cryptography.

Topics:

1. Definitions
2. Operations and Relations
3. Determinants
4. Residue Matrices

Definitions

m columns

Matrix **A**: l rows

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

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

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

Operations and Relations

Addition and subtraction of matrices

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

$$\mathbf{C = A + B}$$

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

$$\mathbf{D = A - B}$$

Multiplication of a row matrix by a column matrix

$$\underset{\mathbf{C}}{\begin{bmatrix} 53 \end{bmatrix}} = \underset{\mathbf{A}}{\begin{bmatrix} 5 & 2 & 1 \end{bmatrix}} \times \underset{\mathbf{B}}{\begin{bmatrix} 7 \\ 8 \\ 2 \end{bmatrix}}$$

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

Linear Diophantine Equation Cont

Multiplication Result of a n × m matrix by a m × l matrix is n x l matrix

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

Scalar multiplication

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

$$\begin{bmatrix} 4 & 3 \\ 7 & 8 \end{bmatrix} x. \begin{bmatrix} 2 & 7 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 8 & 21 \\ 21 & 40 \end{bmatrix}$$

Determinant

The determinant is defined only for a square matrix.

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

1. If $m = 1$, $\det(\mathbf{A}) = a_{11}$
2. If $m > 1$, $\det(\mathbf{A}) = \sum_{i=1\ldots m} (-1)^{i+j} \times a_{ij} \times \det(\mathbf{A}_{ij})$

Where $\mathbf{A}_{ij}$ is a matrix obtained from $\mathbf{A}$ by deleting the ith row and jth column.

Calculating the determinant

Matrix 2 x 2:

$$\det\begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det[\,4\,] + (-1)^{1+2} \times 2 \times \det[\,3\,] \longrightarrow 5 \times 4 - 2 \times 3 = 14$$

or

$$\det\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

Matrix 3 x 3:

$$\det\begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det\begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det\begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det\begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$

$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

Inverse and Residue Matrices

Multiplicative inverses are only defined for square matrices.

Cryptography uses residue matrices: matrices where all elements are in Z_n.
A residue matrix has a multiplicative inverse if gcd (det(A), n) = 1.
Inverse matrix is residue of rounding (t x det(A) x inv(A) in modulus n

$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \det(\mathbf{A}) = 21$$

$$\mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix} \qquad \det(\mathbf{A}^{-1}) = 5$$

Modulus 26

4 LINEAR CONGRUENCE

LINEAR CONGRUENCE

Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in Z_n. This section shows how to solve equations when the power of each variable is 1 (linear equation).

Topics:

1. Single-Variable Linear Equations
2. Set of Linear Equations

Single-Variable Linear Equations

Equations of the form $ax \equiv b \pmod{n}$ 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 $10\,x \equiv 2 \pmod{15}$.
Solution:
First we find the gcd (10 and 15) = 5. Since 5 does not divide 2, we have no solution.

Solve the equation $14\,x \equiv 12 \pmod{18}$.
Solution: since gcd (14 and 18) = 2 and $2 \mid 18$ then there are two solutions

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \quad x \equiv 6\,(7^{-1}) \pmod{9}$$
$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$
$$x_1 = x_0 + 1 \times (18/2) = 15$$

Single-Variable Linear Equations

We can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible.

$$
\begin{aligned}
a_{11}x_1 &+ a_{12}x_2 + \ldots + a_{1n}x_n \equiv b_1 \\
a_{21}x_1 &+ a_{22}x_2 + \ldots + a_{2n}x_n \equiv b_2 \\
&\vdots \qquad\quad \vdots \qquad\qquad \vdots \quad \vdots \\
a_{n1}x_1 &+ a_{n2}x_2 + \ldots + a_{nn}x_n \equiv b_n
\end{aligned}
$$

a. Equations

$$
\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

b. Interpretation

$$
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}^{-1} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

c. Solution

Single-Variable Linear Equations

Solve the set of following three equations:

$$3x + 5y + 7z \equiv 3 \pmod{16}$$
$$x + 4y + 13z \equiv 5 \pmod{16}$$
$$2x + 7y + 3z \equiv 4 \pmod{16}$$

$$A = \begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 15 & 14 & 11 \\ 9 & 5 & 0 \\ 1 & 11 & 9 \end{bmatrix}$$

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 15 & 14 & 11 \\ 9 & 5 & 0 \\ 1 & 11 & 9 \end{bmatrix} * \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} \; modulus\ 16$$

x = 15, y =4 dan z = 14

Lifelong Learning

THANKS YOU

Sources

- ***Forouzan, Behrouz A., and Debdeep Mukhopadhyay. Cryptography and Network Security (Sie). McGraw-Hill Education, 2011.***

- ***Stallings, William. "Cryptography and Network Security. 2005." ISBN: 0-13-187316-4.***