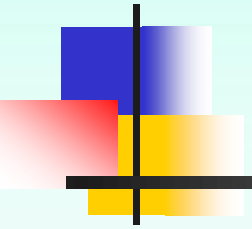
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек.3 2022 КІБ-19

МОДУЛЬНАЯ АРИФМЕТИКА

~~Целочисленное деление:~~
~~ДВА входа, ДВА выхода~~

Модульное «деление»:
ОДИН выход - остаток

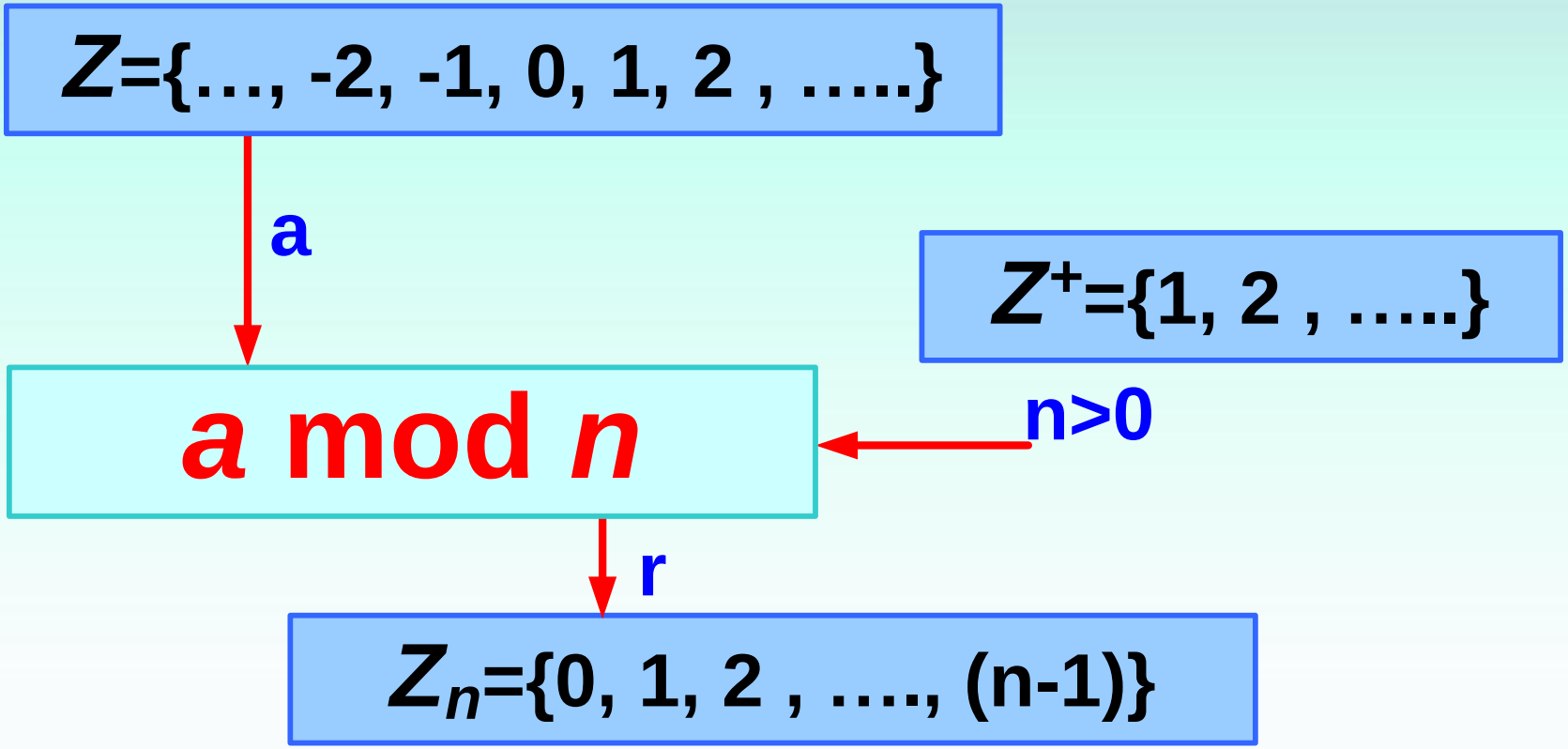
ВХОД	ВЫХОД
a – делимое (целое)	
n – делитель (*n*>0) МОДУЛЬ	
	r - остаток (*r*>0) ВЫЧЕТ

Соотношение:

$$a \bmod n = r$$

Python → **r = a % n**

Модуль по … n



Множество вычетов - система вычетов по модулю n

$$\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$$

Множество вычетов

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots,\}$$

$$\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$$

Примеры:

$$\mathbb{Z}_2 = \{0, 1\}$$
$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$
$$\mathbb{Z}_{10} = \{0, 1, 2, \dots, 9\}$$
$$\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$$

*Одно **бесконечное** множество целых и **бесконечное** множество **конечных** множеств вычетов*

Сравнения

!!!

$3 \mod 10 = 3$ $\qquad$ $3 \mod 12 = 3$

$13 \mod 10 = 3$ $\qquad$ $15 \mod 12 = 3$

$23 \mod 10 = 3$ $\qquad$ $27 \mod 12 = 3$

Целые 3, 13, 23 сравнимы по модулю 10

Целые 3, 15, 27 сравнимы по модулю 12

Оператор сравнения $(\equiv)$

$3 \equiv 13 (\mod 10)$ $\qquad$ $3 \equiv 23 (\mod 10)$

$3 \equiv 15 (\mod 12)$ $\qquad$ $3 \equiv 27 (\mod 12)$

Оператор сравнения $(\equiv)$ отображает $\mathbb{Z}$ в $\mathbb{Z}_n$

Система вычетов

Система вычетов [a] (или $[a]_n$) - множество целых чисел, сравнимых по модулю *n*. Иначе это набор таких целых *x* , что

$$x = a \pmod n$$

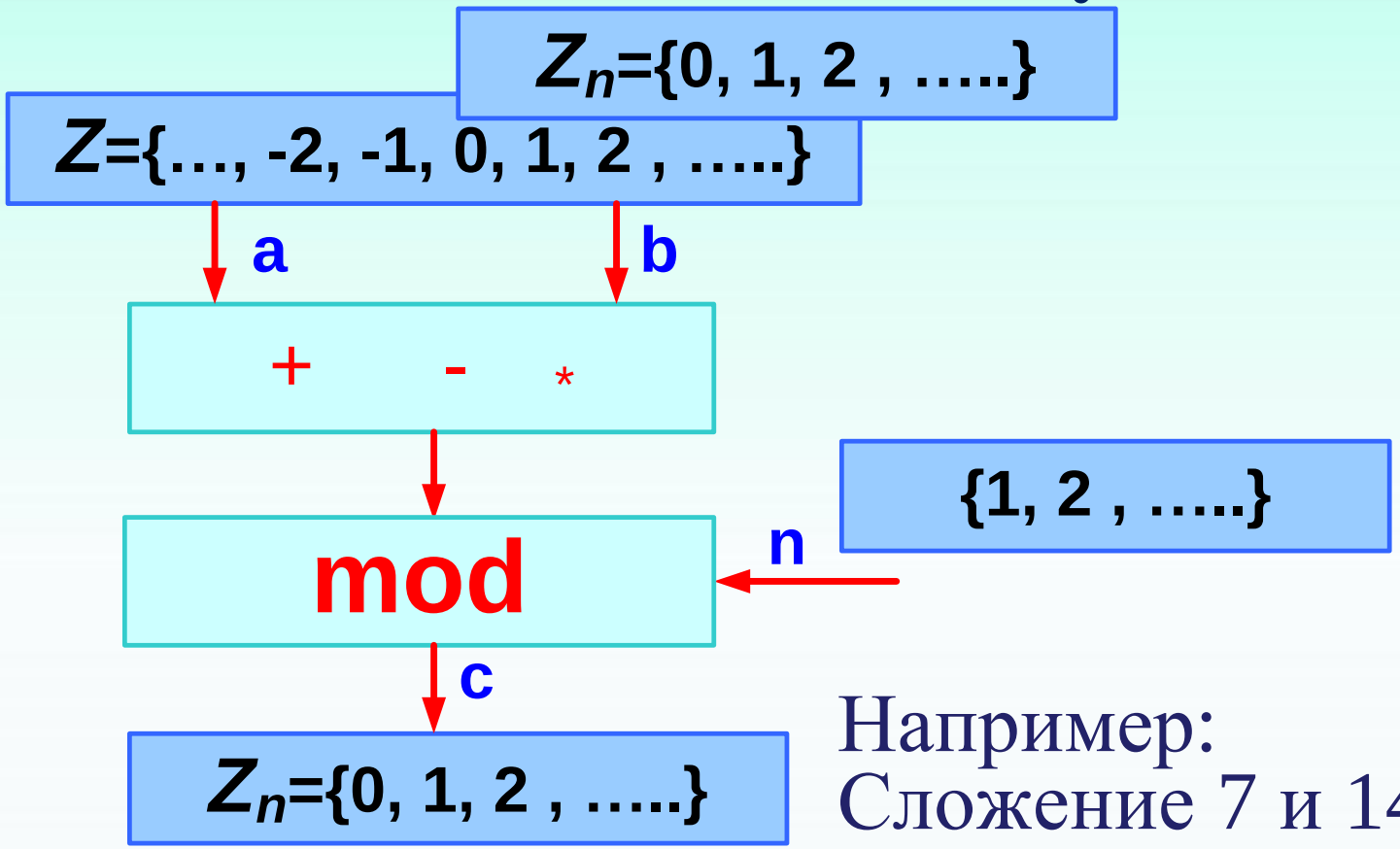
Например: для *n*=5 $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ **и**

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

Операторы в $\mathbb{Z}_n$

Бинарные операторы:

сложение, вычитание, умножение.



Например:
Сложение 7 и 14 в Z_{15}
(7 + 14) ***mod*** 15 →
(21) ***mod*** 15 = **6**

Операторы в $\mathbb{Z}_n$

Бинарные операторы:

сложение, вычитание, умножение.

Важные свойства

$$(a + b)\,\boldsymbol{mod}\, n = [(a\,\boldsymbol{mod}\, n) + (b\,\boldsymbol{mod}\, n)]\,\boldsymbol{mod}\, n$$

$$(a - b)\,\boldsymbol{mod}\, n = [(a\,\boldsymbol{mod}\, n) - (b\,\boldsymbol{mod}\, n)]\,\boldsymbol{mod}\, n$$

$$(a * b)\,\boldsymbol{mod}\, n = [(a\,\boldsymbol{mod}\, n) * (b\,\boldsymbol{mod}\, n)]\,\boldsymbol{mod}\, n$$

Операторы в $\mathbb{Z}_n$
Остаток от степени числа 10

Найти $\boldsymbol{10^k mod\ n}$

Например, найти:

$$\boldsymbol{10^1 mod\ 3 \quad 10^2 mod\ 3 \quad 10^3 mod\ 3 \quad \ldots.}$$

Свойство

$$(a * b)\boldsymbol{mod}\ n = [(a\ \boldsymbol{mod}\ n) * (b\ \boldsymbol{mod}\ n)]\boldsymbol{mod}\ n$$

$$\boldsymbol{10^2 mod\ 3 = (10 * 10) mod\ 3}$$
$$\boldsymbol{= (10 mod\ 3 * 10 mod\ 3) mod\ 3}$$
$$\boldsymbol{= (10 mod\ 3)^2\ mod\ 3}$$

$$\boldsymbol{10^k mod\ n = (10 mod\ n)^k mod\ n}$$

Операторы в $\mathbb{Z}_n$
Инверсные (обратные) операции

Обычная арифметика.

Вычитание - операция инверсная сложению:

$$a + b = 0 \qquad b = -a$$

Деление - операция инверсная умножению:

$$a * b = 1 \qquad b = \frac{1}{a} = a^{-1}$$

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Инверсные операции

Аддитивная инверсия в $\mathbb{Z}_n$.
Два числа аддитивны, если:

$$a + b \equiv 0 (mod\ n)$$

Или

$$b = n - a$$

Например: в $\mathbb{Z}_{10}$
a = 3 b = 10-3 = 7
!! пары взаимно аддитивных в $\mathbb{Z}_{10}$
(0,0) (1,9) (2,8) (3,7) (4,6) (5,5)

В $\mathbb{Z}_n$ каждое целое имеет ОДНУ аддитивную инверсию (м.б. само число)

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Инверсные операции

Таблица сложения в $\mathbb{Z}_{10}$.

n=10	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Инверсные операции

Мультипликативная инверсия в $\mathbb{Z}_n$.

Два числа мультипликативные, если:

$$a * b \equiv 1 (mod\ n)$$

n=10	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

в $\mathbb{Z}_{10}$:
(1,1)
(3,7)
(9,9)

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Инверсные операции

Доказано для $\mathbb{Z}_n$.
Два числа мультипликативные в $\mathbb{Z}_n$, если:
$$gcd(n, a) = 1$$

N =10	gcd(10,a)
1	1
2	2
3	1
4	2
5	5
6	2
7	1
8	2
9	1

N =11	gcd(11,a)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1

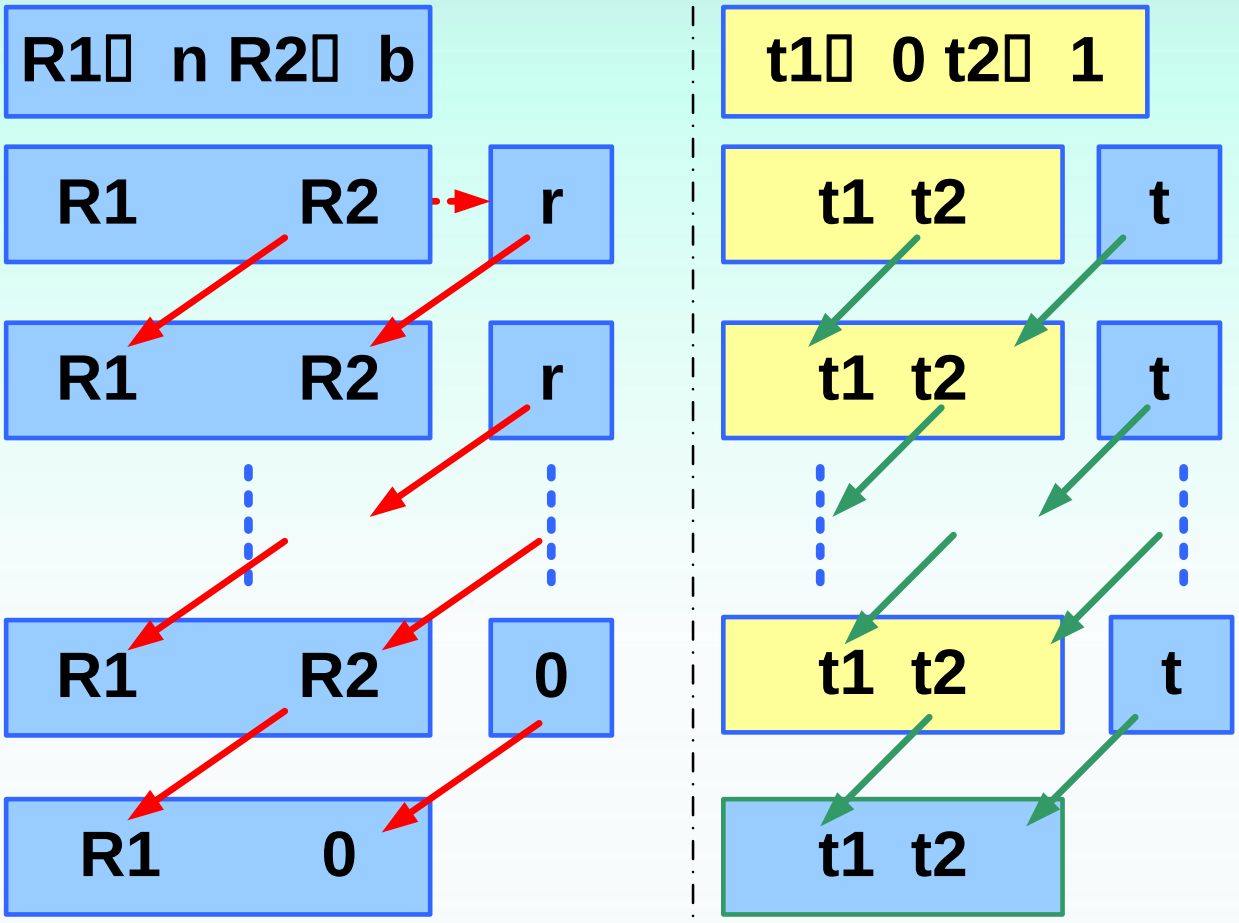
Операторы в $\mathbb{Z}_n$. Модульная арифметика: Мультипликативная инверсия.

Расширенный алгоритм Эвклида может найти мультипликативную инверсию для заданного ***b*** в $\mathbb{Z}_n$ **(! Если инверсия существует) .**

$$s * n + t * b = gcd(n, b) = 1$$
$$(s * n + t * b) \bmod n = 1 \bmod n$$
$$[(s * n) \bmod n + (t * b) \bmod n] \bmod n = 1 \bmod n$$
$$0 + (t * b) \bmod n = 1$$
$$(t * b) \bmod n = 1$$

Т.е. ***t*** мультипликативная инверсия ***b***, при ***gcd(n,b)=1***

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Мультипликативная инверсия. (Эвклид)



Здесь **q=r1//r2, r=r1-q*r2, t=t1-q*t2,**

Если **R1 = 1** то $\boldsymbol{b^{-1} = t1}$

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Мультипликативная инверсия. (Эвклид)

Найти b^{-1} для b = 11 в $\mathbb{Z}_{26}$

r1	r2	r
26	11	4
11	4	3
4	3	1
3	1	0
1	0	

q
2
2
1
3

t1	t2	t
0	1	-2
1	-2	5
-2	5	-7
5	-7	26
-7		

$$t1 = -7 \notin \mathbb{Z}_{26} . (-7) mod\ 26 = 19$$

$$11^{-1} = 19\ in\ \mathbb{Z}_{26}$$

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Мультипликативная инверсия. (Эвклид)

Пример:
Найти b^{-1} для **b = 23** в $\mathbb{Z}_{100}$

$$t1 = -13 \notin \mathbb{Z}_{100}. \quad (-13) mod\ 100 = 87$$

Проверка:

$$(23 * 87) mod\ 100 = 2001 mod 100 = 1$$

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Мультипликативная инверсия.

Обозначим $\mathbb{Z}_{n*}$ подмножество $\mathbb{Z}_n$ целых чисел имеющих мультипликативную инверсию

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}. \quad \mathbb{Z}_{6*} = \{1, 5\}.$$

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

$$\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$
$$\mathbb{Z}_{11*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

Операторы в $\mathbb{Z}_n$. Модульная арифметика: Мультипликативная инверсия.

Обозначим $\mathbb{Z}_p$ множество целых, где p **ПРОСТОЕ** число.

Например

$$\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

И, соответственно, $\mathbb{Z}_{p*}$ множество целых по модулю p (ПРОСТОЕ), имеющих мультипликативную инверсию.

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

Матрицы в линейной алгебре

Матрица $A = \begin{pmatrix} a_{0,0} & \cdots & a_{0,m-1} \\ \vdots & \ddots & \vdots \\ a_{n-1,0} & \cdots & a_{n-1,m-1} \end{pmatrix}$

где n – строк, m – столбцов.

Если $n = m$ - квадратная

Если $n = 1$ –строка (вектор – строка)

Если $m = 1$ – столбец (вектор – столбец)

Равенство матриц

$$A = B \text{ , } if \ a_{i,j} = b_{i,j}$$

для всех i, j .

Матрицы в линейной алгебре

Сложение, вычитание

$$C = A + B \quad / \quad C = A - B$$

$$c_{i,j} = a_{i,j} + b_{i,j} \quad / \quad c_{i,j} = a_{i,j} - b_{i,j}$$

!!! Одинаковые n , m

Умножение $C = A \times B$

!!! Число столбцов A равно числу строк B

$$c_{i,k} = \sum_{j=0}^{m-1} a_{i,j} * b_{j,k}$$

$i=0,1,\ldots,n-1$

$k=0,1,\ldots,l-1$

Матрицы в линейной алгебре

Скалярное умножение $\boldsymbol{C = n \times A}$

$$\boldsymbol{c_{i,j} = n \times a_{i,j}}$$

Детерминант $\boldsymbol{\det(A)}$
КВАДРАТНОЙ матрицы $\boldsymbol{A}$

$$\text{if } \boldsymbol{n = 1}\text{ , } \boldsymbol{det\,(A) = a_{0,0}}$$

$$\text{if } \boldsymbol{n > 1}$$

$$\boldsymbol{\det\,(A) = \sum_{i=0}^{m-1}(-1)^{i+j} \times a_{i,j} \times det(A_{i,j})}$$

Матрицы в линейной алгебре

Аддитивная инверсия матриц

Матрица $\boldsymbol{C}$ аддитивно инверсна $\boldsymbol{A}$, если $\boldsymbol{A + C = 0}$ или $\boldsymbol{c_{i,j} = -a_{i,j}}$. Обозначается $\boldsymbol{-A}$.

Мультипликативная инверсия матриц

Матрица $\boldsymbol{C}$ мультипликативно инверсна $\boldsymbol{A}$, если $\boldsymbol{A \times C = C \times A = I}$. Обозначается $\boldsymbol{A^{-1}}$.

Существует только для **квадратных** матриц, если $\boldsymbol{\det(A) \neq 0}$.

Матрицы в $\mathbb{Z}_n$. Матрицы вычетов

Особенность:

Мультипликативная инверсия матриц

Матрица A , где все $a_{i,j} \in \mathbb{Z}_n$, имеет мультипликативную инверсию, только если $\det(A)$ имеет мультипликативную инверсию в $\mathbb{Z}_n$.

Матрицы в $\mathbb{Z}_n$. Матрицы вычетов

Сравнение матриц:

$$A \equiv C \bmod n$$

Две матрицы A и C сравнимы по модулю n, если они имеют одинаковое число строк и столбцов и все их элементы сравнимы по модулю n . То есть

$$a_{i,j} \equiv c_{i,j} \bmod n \quad \forall\, i, j$$

Вопросы:

- Укажите различие между $\boldsymbol{Z}$ и $\boldsymbol{Z_n}$.
- Укажите четыре свойства теории делимости целых чисел .
- Определите понятие наибольшего общего делителя двух целых чисел.
- Опишите алгоритм Эвклида определения НОД .
- Опишите расширенный алгоритм Эвклида .
- Определите понятие наименьшего общего кратного .

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 3