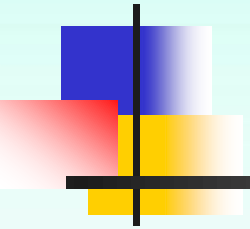
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек.2 2022 КІБ-19

МОДУЛЬНАЯ АРИФМЕТИКА # 1

Множество целых

$\mathbb{Z}$ - множество целых чисел

…. , -2, -1, 0, 1, 2, 3, …

$\mathbb{Z}^+$ - множество положительных целых чисел

1, 2, 3, …

$\mathbb{Z}^{\geq}$ - множество неотрицательных целых чисел

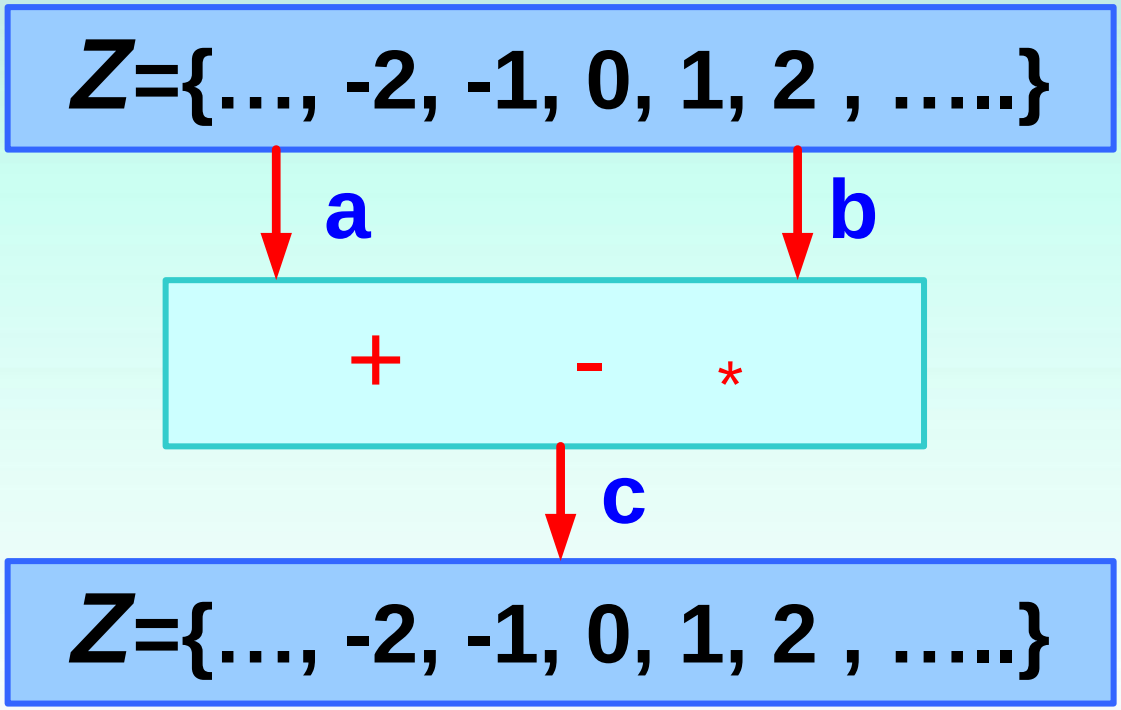
0, 1, 2, 3, …

Бинарные операции: сложение, вычитание, умножение.

Два входа (*a*, *b* - **операнды**) и **ОДИН** выход

c – результат операции.

Бинарные операции



Примеры:

Сложение: 5+9=? (-5)+9=? (5)+(-9)=? (-5)+(-9)=?

Вычитание: 5-9=? (-5)-9=? (5)-(-9)=? (-5)-(-9)=?

Умножение: 5*9=? (-5)*9=? (5)*(-9)=? (-5)*(-9)=?

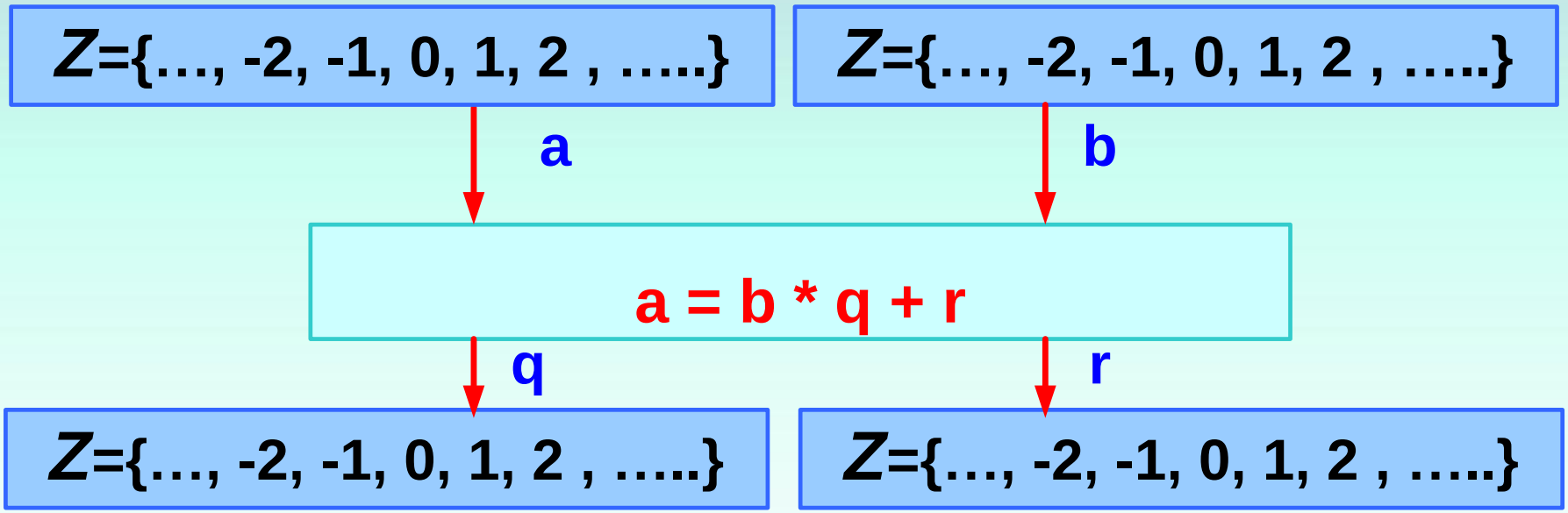
Деление: ДВА входа, ДВА выхода

ВХОД	ВЫХОД
a - делимое	q - частное (*Quotient*)
b - делитель	r - остаток (*Remainder*)

Соотношение:

$$a = b * q + r$$

Деление



Python→Целочисленное Деление:

q = a // b r = a % b

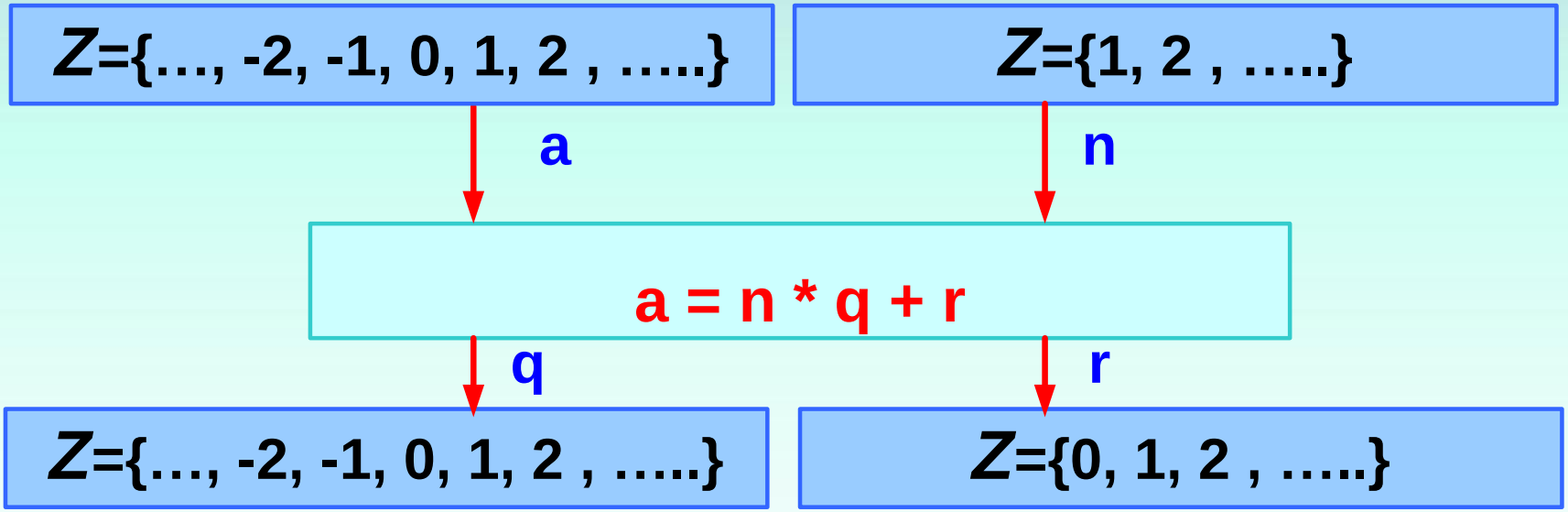
Примеры Деление:

a = 255, n= 23, q = ?, r = ?

a = -255, n= 23, q = ?, r = ?

a = -255, n= -23, q = ?, r = ?

Деление в криптографии



!!! Ограничения:

$$n > 0 \qquad r \geq 0 \qquad r < n$$

Примеры:

a = 255, n= 23, q = ?, r = ?

a = -255, n= 23, q = ?, r = ?

a = -255, n= -23, q = ?, r = ?

Сведения из теории делимости

Если (*вдруг!*) $a \neq 0$ $r = 0$
То $a = n * q$
n делит a **НАЦЕЛО ! БЕЗ ОСТАТКА!**
Обозначается: $n \mid a$

Если $a \neq 0$ $r = 1, 2, 3, \ldots$
То $a = n * q + r$
n НЕ делит a **НАЦЕЛО**
Обозначается: $n \nmid a$

Примеры:

$13 \mid 78$	$7 \mid 98$	$4 \mid 44$
$14 \nmid 78$	$8 \nmid 98$	$5 \nmid 44$

Сведения из теории делимости

Свойство 1: если $a|1$, то $a = \pm 1$

Свойство 2: если $a|b$ и $b|a$, то $a = \pm b$

Свойство 3: если $a|b$ и $b|c$, то $a|c$

Свойство 4: если $a|b$ и $b|c$,

то $a|(m * b + n * c)$

где m, n - произвольные целые числа

Примеры:

$3|15$, $15|45$ → ???

$3|15$, $3|9$ → ????

Сведения из теории делимости

Делители: пусть а положительное целое.

Свойство 1: а=1, то только ОДИН делитель = **а**
Свойство 2: а= любое целое положительное, то как минимум два делителя:

$$\mathbf{1}|a \qquad a|a$$

НО! Может и больше

Например а=32

1|32 , 2|32 , 4|32 , 8|32 , 16|32 , 32|32

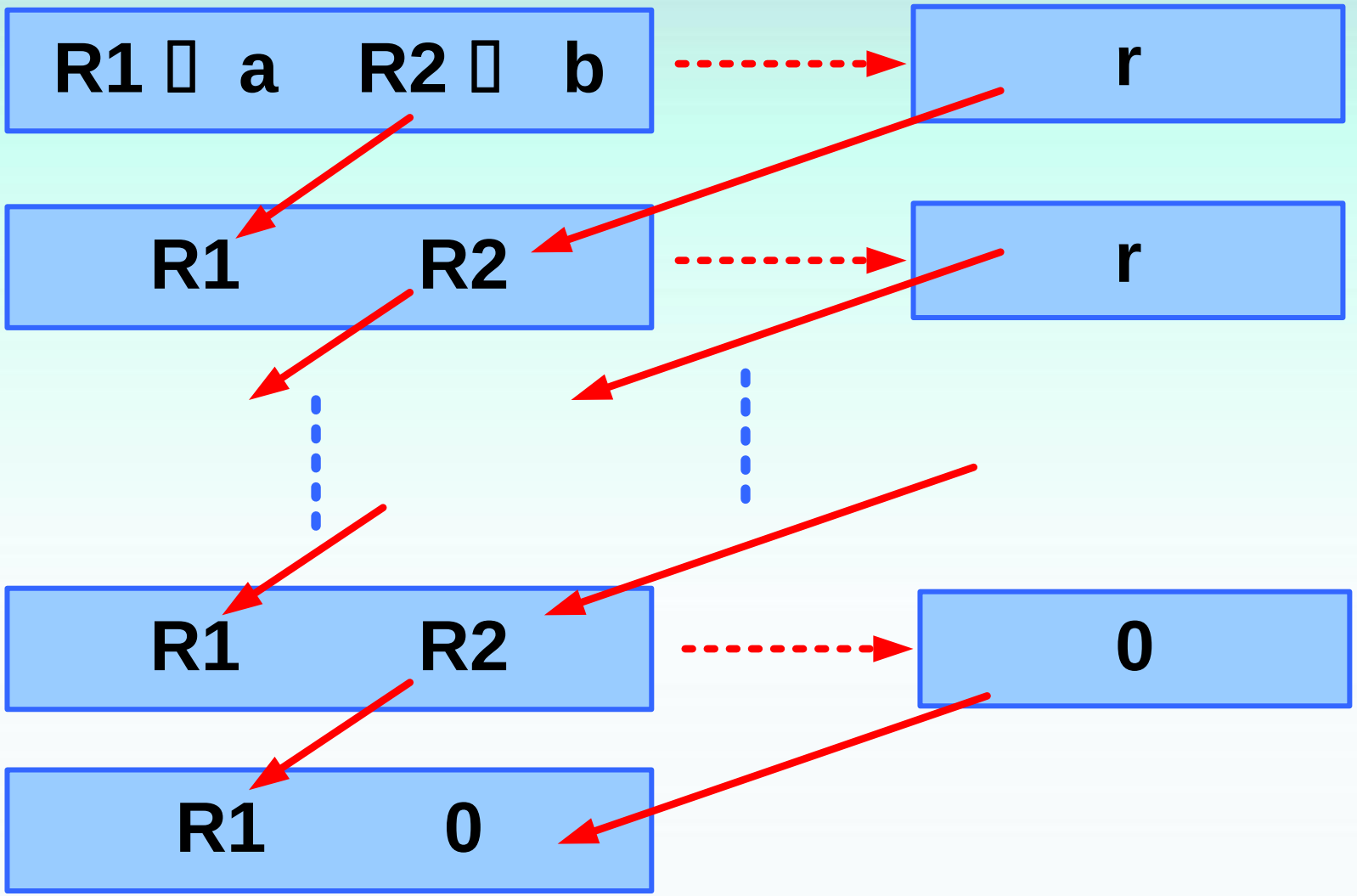
Наибольший общий делитель (НОД)

Общий делитель
Пусть **a , b** - положительные целые и
c|a и **c|b**
тогда **c** - общий делитель.

Важное целое → НОД!!
Обозначается *нод(a,b)* или *gcd(a,b).*
Максимальное положительное число ***d=gcd(a,b),***
такое что **d|a** и **d|b .** Исключая ***gcd*(0,0) = 0**

Примеры:
***gcd* (6, 15) = ????**
***gcd* (230, 450) = ????**

Алгоритм Эвклида [Euclid] (НОД)



$gcd(a,b) = R1$

Алгоритм Эвклида [Euclid] (НОД) примеры

R1 = a	R2 = b	R
36	10	6
10	6	4
6	4	2
4	2	0
2	0	

R1 = a	R2 = b	R
37	10	7
10	7	3
7	3	1
3	1	0
1	0	

Алгоритм Эвклида [Euclid] (НОД)
PYTHON

```
rem_1 = int_num_1
rem_2 = int_num_2
while rem_2 > 0 :
        q = rem_1 // rem_2
        r = rem_1 - q * rem_2
        rem_1 = rem_2
        rem_2 = r

gcd = rem_1
```

Расширенный алгоритм Эвклида

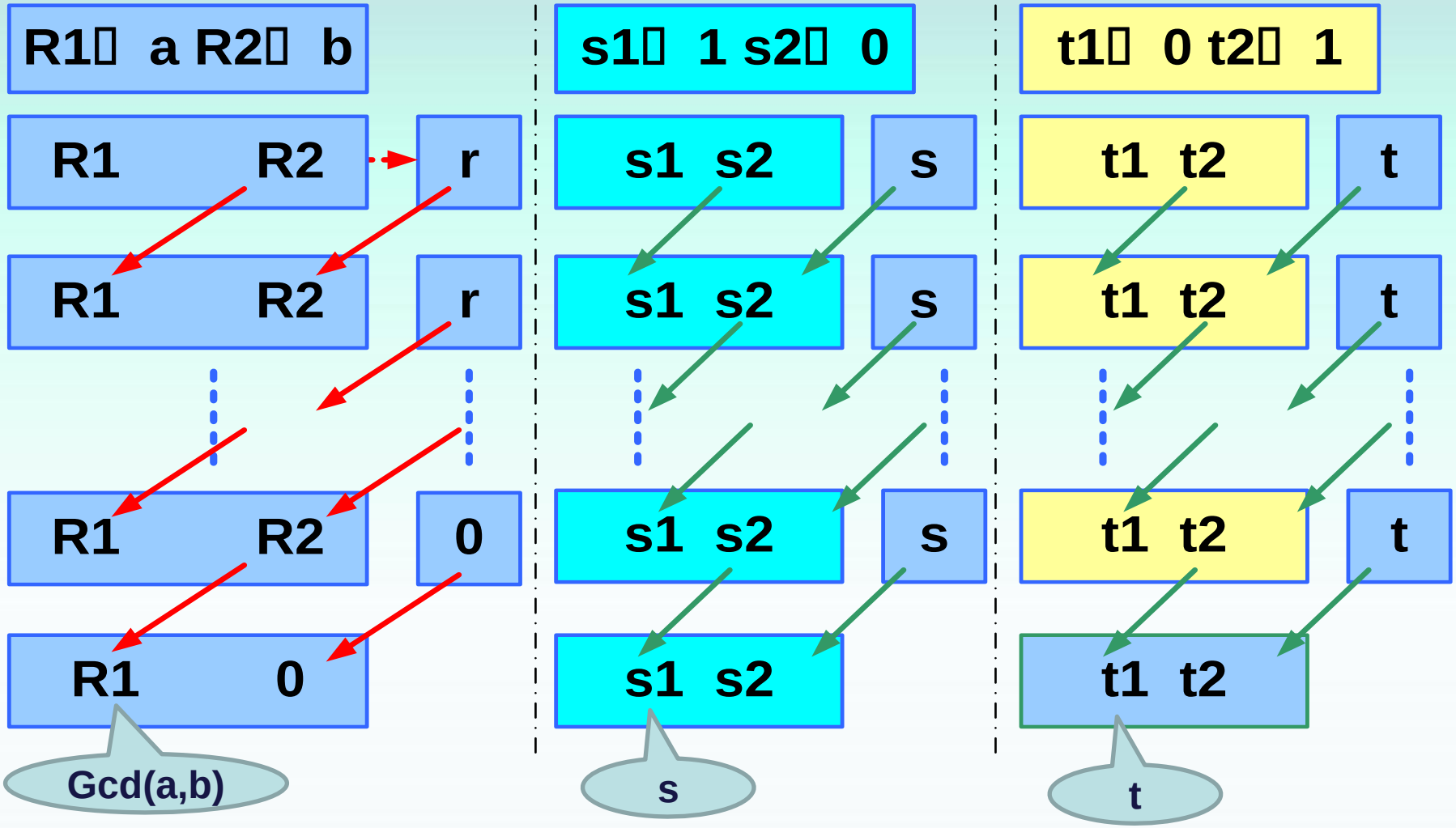
Пусть **a , b** - положительные целые .
Найти **s , t** - такие что

$$s * a + t * b = gcd(a, b)$$

То есть ищутся: ***gcd(a,b), s , t***

Используется **«утроение»** алгоритма Эвклида.

Расширенный алгоритм Эвклида



Здесь **q=r1//r2,**
r=r1-q*r2, s=s1-q*s2, t=t1-q*t2,

Расширенный Алгоритм Эвклида

Пример

r1	r2	r	q	s1	s2	s	t1	t2	t
36	10	6	3	1	0	1	0	1	-3
10	6	4	1	0	1	-1	1	-3	4
6	4	2	1	1	-1	2	-3	4	-7
4	2	0	2	-1	2	-5	4	-7	18
2	0		0	2			-7		

$gcd(36,10) = 2 \;,\quad s = 2 \;, d = -7$

$$s * a + t * b = gcd(a, b)$$

$$2*36 - 7*10 = 72 - 70 = 2$$

Наименьшее общее кратное

Общее кратное
Пусть **a , b** - положительные целые и
a|d и **b|d ,**
тогда **d** - общее кратное.

Наименьшее общее кратное – наименьшее целое, которое делится на **d** без остатка
Обозначается ***нок(a,b)*** или ***lcm(a,b).***

$$lcm(a,b) = \frac{a * b}{gcd(a,b)}$$

Вопросы:

- Укажите различие между $\mathbb{Z}$, $\mathbb{Z}^{+}$ и $\mathbb{Z}^{\geq}$.
- 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 # 2