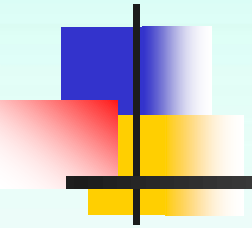
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Практ. 2 2022 КІБ-19

ПРАКТИКА

«МОДУЛЬНАЯ АРИФМЕТИКА»

Напоминание: Инверсные операции в $\mathbb{Z}_n$

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

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

Или

$$b = n - a\ (mod\ n)$$

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)

Примеры: Найти аддитивную инверсию a в $\mathbb{Z}_n$

	a	N	-a
1	180	37	?
2	86	31	?
3	97	23	?

Напоминание: Инверсные операции в $\mathbb{Z}_n$

Мультипликативная инверсия в $\mathbb{Z}_n$.
Два числа мультипликативные, если:

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

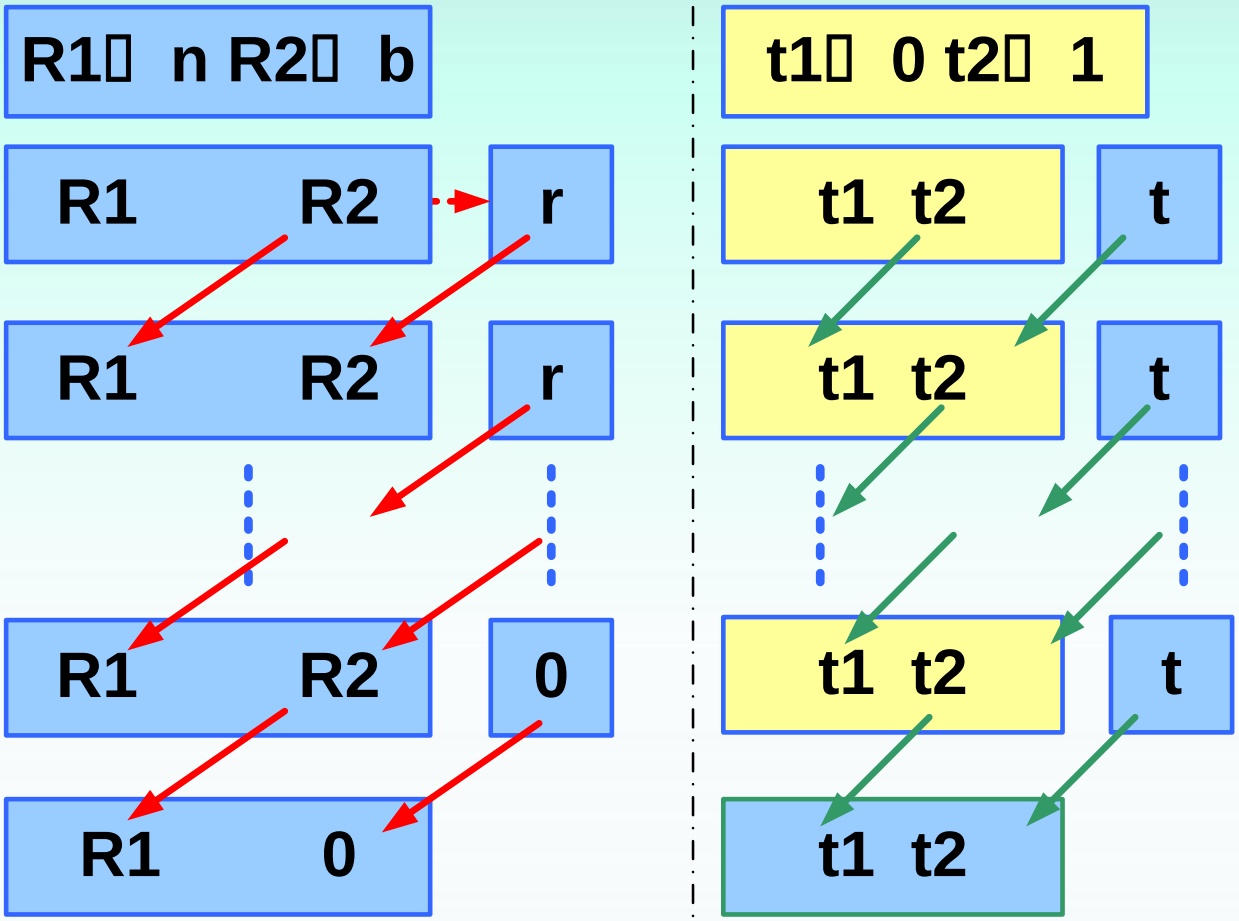
Расширенный алгоритм Эвклида может найти мультипликативную инверсию для заданного b в $\mathbb{Z}_n$

$$s * n + t * b = gcd(n, b) = 1$$

$$(t * b) mod\ n = 1$$

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

Напоминание: Инверсные операции в $\mathbb{Z}_n$ (Эвклид)



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

Если **R1 = 1** то $b^{-1} = t1$

Напоминание: Инверсные операции в $\mathbb{Z}_n$ (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		

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

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

Напоминание: Инверсные операции в $\mathbb{Z}_n$ (Эвклид)

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

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

Проверка:

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

Примеры: Найти мультипликативную инверсию a в $\mathbb{Z}_n$

	A	n	a^{-1}
1	38	101	?
2	86	47	?
3	24	97	?

Напоминание: Линейное уравнение

Уравнение вида

$$a\,x \equiv b\ (mod\ n)$$

$a\ , b, n$ **- заданные целые!**

Может :

а) не иметь решения

б) ограниченное число решений.

Пусть $d = gcd(a, n)$

Тогда

а) если $d \nmid b$ **- нет решения**

б) если $d|b$ **- есть** d **решений**

Напоминание: Линейное уравнение

Уравнение вида

$$a\,x \equiv b\ (mod\ n)$$

Алгоритм решения:

а) сокращаем уравнение – делим на d

б) умножаем обе стороны на мультипликативную инверсию $\left(\frac{a}{d}\right)^{-1}$ – находим решение x_0 .

Общее решение имеет вид

$$x = x_0 + k * \frac{n}{d}, \qquad k = 0, 1, \dots, (d-1)$$

Напоминание: Линейное уравнение

Пример.

$$14\,x \equiv 12\ (mod\ 18)$$

Находим $d = gcd(14, 18) = 2$

Сокращаем на $d = 2$

$$7\,x \equiv 6\ (mod\ 9)$$

Или

$$x_0 \equiv 6 * 7^{-1}\ (mod\ 9) \quad ,\rightarrow 7^{-1}\ (mod\ 9) = 4$$

То есть $x_0 \equiv 6 * 4\ (mod\ 9) = 6$

Общее решение имеет вид

$$x = 6 + k * 9, \qquad k = 0, 1$$

Примеры: Найти все решения уравнения $a*x \equiv b \pmod{n}$

	a	b	n	X =
1	38	38	180	?
2	37	38	130	?
3	24	41	97	?

Напоминание: Система линейных уравнений

Уравнение вида

$$A * X \equiv B \pmod{n}$$

или

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} * \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \pmod{n}$$

Если (**?**) есть A^{-1} мультипликативная инверсия матрицы A, то

$$X \equiv A^{-1}B \pmod{n}$$

Напоминание: Система линейных уравнений

Особенность:

Мультипликативная инверсия матриц

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

Напоминание: Система линейных уравнений

Последовательность поиска инверсной матрицы.

Пусть $[\boldsymbol{det(A)}]^{-1}$ **в** $\mathbb{Z}_{\boldsymbol{n}}$ **есть !** и найдены все алгебраические дополнения $a^*_{j,i}$.

Для каждого ***i,j*** решаем линейное уравнение

$$det\,(A) * \boldsymbol{a^{-1}_{j,i}} \equiv a^*_{j,i}(\boldsymbol{mod\ n})$$

Таким образом формируется матрица $(\boldsymbol{A})^{-1}$

Найти инверсную матрицу A^{-1} в $\mathbb{Z}_n$

$$A = \begin{matrix} 3 & 0 \\ 1 & 1 \end{matrix}, \qquad n = 10$$

$$A = \begin{matrix} 4 & 2 \\ 1 & 1 \end{matrix}, \qquad n = 10$$

Решить систему линейных уравнений

$$3x + 5y \equiv 4 \ (mod 5)$$
$$2x + 1y \equiv 3 \ (mod 5)$$

$$3x + 2y \equiv 5 \ (mod 7)$$
$$4x + 6y \equiv 4 \ (mod 7)$$

$$2x + 5y \equiv 4 \ (mod 8)$$
$$1x + 6y \equiv 3 \ (mod 8)$$

END # 2