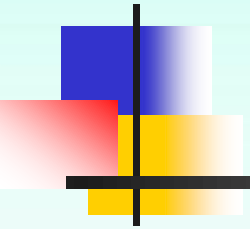
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Практ. 1 2022 КІБ-19

МОДУЛЬНАЯ АРИФМЕТИКА

НОД

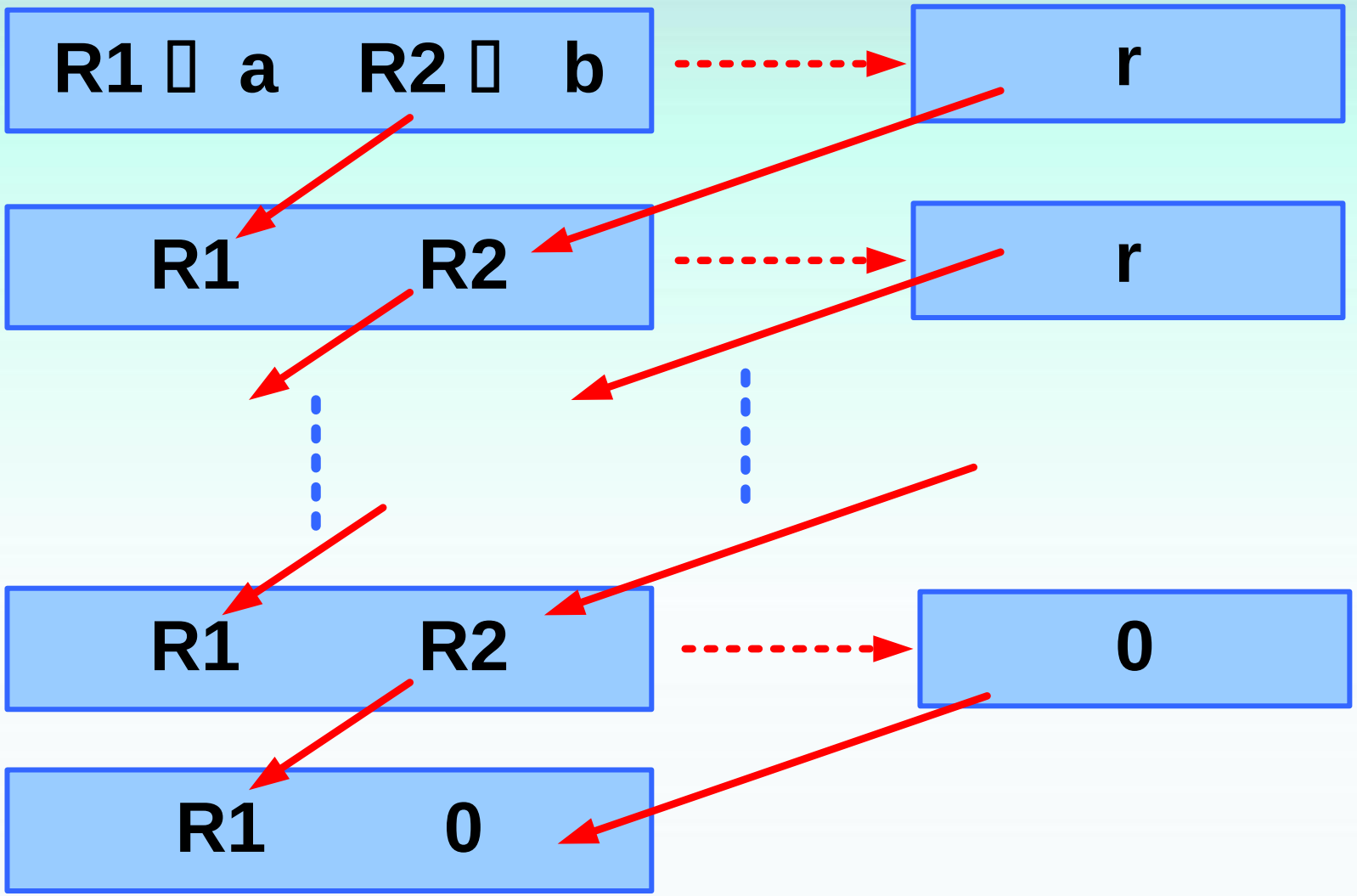
Найти частное и остаток

	a	n>0	q	r≥0
1	237	27		
2	861	13		
3	-1024	25		
4	-1025	25		
5	999	19		
6	-999	27		
7	666	110		
8	256	8		
9	-256	9		
10	74385	323		

Проверить правильность

	a	true	false
1	27|237		
2	13|861		
3	25|-1024		
4	25|-1025		
5	999|19		
6	-999|27		
7	666|110		
8	256|8		
0	-256|9		
10	74385|323		

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	

Найти НОД

	a	b	Gcd(a,b)
1	88	220	
2	300	42	
3	24	320	
4	401	700	
5	231	192	
6	457	27	
7	2300	110	
8	256	8	
9	834	458	
10	785	323	

НОД трех и более чисел

Пусть **a** , **b, c** положительные целые.

Найти ***gcd(a,b,c)***

Можно показать, что

$$gcd(a,b,c) = gcd(gcd(a,b),c)$$

Найти НОД

	a	b	c	gcd(a,b,c)
1	88	220	18	
2	300	42	16	
3	24	320	16	
4	401	700	14	
5	231	192	36	
6	457	27	22	
7	2300	110	25	
8	256	8	32	
9	834	458	56	
10	785	323	432	

Используя расширенный алгоритм Эвклида найти $gcd(a,b)$, s , t

	a	b	gcd(a,b)	s	t
1	88	220			
2	300	42			
3	24	320			
4	401	700			
5	231	192			
6	457	27			
7	2300	110			
8	256	8			
9	834	458			
10	785	323			

END # 1