31.10.25 ЕВКЛИД

ЗАД. 4 ИЗ ДЗ

$НОД(a,b) = НОД(a-b, b)$

$НОД(a,b) = d$

$a = k_1 d$

$b = k_2 d$

$a - b = (k_1 - k_2) d \Rightarrow a-b \vdots d$

ПОКАЖ., ЧТО $\nexists D > d$: $НОД(a-b, b) = D$

ПРЕДП. ПР., Т. Е. $a - b = m_1 D$

$b = m_2 D$

$a - b + b = m_1 D + m_2 D = (m_1 + m_2) D = a$

ПРОТИВОРЕЧИЕ

N 5 ИЗ ДЗ

$a_1, a_2, \dots, a_n$

$НОД(a_1, \dots, a_n) = d$

$a_1 = m_1 d$

$a_2 = m_2 d$

$\dots$

$a_n = m_n d$

$m_1^i d, m_2^i d, \dots,$

$\mathbb{N}$

НА КАЖД. ШАГЕ НОД НЕ МЕНЯЕТСЯ

Алгоритм Евклида

ВХОД: $a, b \in \mathbb{N}$; $a, b > 0$; $len(max(a,b)) = n$

ВЫХОД: $НОД(a,b)$

ВОПРОСЫ: 1) КОРРЕКТНОСТЬ 0) АЛГОРИТМ

2) СЛОЖНОСТЬ

```
def euclid(a, b):
    if(a==b):
        return a
    a, b = max(a,b), min(a,b)

    return euclid(a-b, b)
```

// if(b>a):
    a,b=b,a

e(15, 9)
e(6, 9)
e(3, 6)
e(3, 3)
return 3

РАБОТАЕТ! НО ЗА $O(2^n)$

ПРИМЕР:

$a = 2^n - 1$, $b = 1$) $2^n - 2$ ШАГОВ

a	b
15	1
14	1
13	1
...	...

КАК СДЕЛАТЬ БЫСТРЕЕ? ЗАМЕНИТЬ ВЫЧИТАНИЕ НА ОСТ. ПО МОД.

```
def euclid(a, b):
    if(a==b):
        return a
    a, b = max(a,b), min(a,b)

    return euclid(a mod b, b)
```

$\underbrace{a \bmod b}_{O(n^2)}$

СУММ. АСИМП. $O(n^3)$

$11 // 3 = 3$

$11_2 = 1011$

$3_2 = 11$

divide(1011, 11) ret(10, 1) (10,0)
divide(101, 11) ret(0, 11) (0, 10)
divide(10, 11) ret(0, 1)
divide(1, 11) ret(0, 1)
divide(0, 11); ret(0,0)

УР. РЕК.	x	y	q	r	ret vals
1	1011	11	~~10~~ 11	~~100~~ ~~101~~ 10	(11, 10)
2	101	11	~~0~~ 1	~~100~~ ~~101~~ 10	(1, 10)
3	10	11	0	10	(0, 10)
4	1	11	0	1	(0, 1)
5	0	11	–	–	(0, 0)

$x = y \cdot q_{fin} + r_{fin}$

$O(n^2)$

ПУСТЬ $a > b$ – НЕ БОЛЕЕ ЧЕМ n-БИТ. ЧИСЛА

$\overleftrightarrow{\quad n \text{ БИТ} \quad}$

$a = 11010\ldots$

$b = 1100$

$a \bmod b$ БУДЕТ ИМЕТЬ 0 НА n-М БИТЕ

$T(n) = T(n-1) + cn^2 \leq n \cdot cn^2 = O(n^3)$

$7^{13} \bmod 167$

$7^{-1} \bmod 167$

$A^{-1} \cdot A = \mathbb{I}$

$a \cdot a^{-1} = 1$

ДЕЛИТЕЛИ НУЛЯ

// $a \cdot b \equiv 0 \mod q$

$7^{-1} \equiv x \mod 17$

$7x \equiv 1 \mod 17$ // $7x = 167k + 1$

$\mathbb{Z}_6$

$5 \equiv 5^{-1} \mod 6$

$1 \equiv 1^{-1} \mod 6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}_5$

$3 \cdot 2 \equiv 1 \mod 5$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$7^{-1} \equiv x \mod 17$

$7x \equiv 1 \mod 17$

$17x + 7x \equiv 1 \mod 17$

$24x \equiv 18 \mod 17$

$4x \equiv 3 \mod 17$

$4x \equiv 20 \mod 17$

$x \equiv 5 \mod 17$

$24x = k \cdot 17 + 18$

$6(4x - 3) = k \cdot 17$

$4x - 3 = \frac{k}{6} \cdot 17$

$4x \equiv 3 \mod 17$

$7 \cdot 5 = 35 \equiv 1 \mod 17$

$7^{-1} \equiv 5 \mod 17$

РАСШИРЕННЫЙ АЛГОРИТМ ЕВКЛИДА

$ax + by = d$; $a, b - ?$

УР. БЕЗ РЕШ.: $\underbrace{2x + 4y}_{\vdots 2} = \underbrace{3}_{\not\vdots 2}$ $\quad a \cdot 2 + b \cdot 4 = 3$

$a, b \in \varnothing$

$x_k \longrightarrow x_{k+1} = y_k$

$y_k \longrightarrow y_{k+1} \equiv x_k \mod y_k$

$y_{k+1} = x_k - \left\lfloor \frac{x_k}{y_k} \right\rfloor y_k \qquad x_k = \left\lfloor \frac{x_k}{y_k} \right\rfloor \cdot y_k + y_{k+1}$

$a_k x_k + b_k y_k = d$

$a_{k+1} x_{k+1} + b_{k+1} y_{k+1} = d$

$a_{k+1} y_k + b_{k+1} \left(x_k - \left\lfloor \frac{x_k}{y_k} \right\rfloor y_k \right) = d$

$a_{k+1} y_k + b_{k+1} x_k - b_{k+1} \left\lfloor \frac{x_k}{y_k} \right\rfloor y_k = d$

$b_{k+1} x_k + \left(a_{k+1} - b_{k+1} \left\lfloor \frac{x_k}{y_k} \right\rfloor \right) y_k = d$

$\Rightarrow$ $a_k = b_{k+1}$

$b_k = a_{k+1} - b_{k+1} \left\lfloor \frac{x_k}{y_k} \right\rfloor \cancel{y_k}$ ОПЕЧАТКА

ОТВЕТ

x	y	a	b	$\lfloor \frac{x}{y} \rfloor$	d
9	15	2	$-1-2\cdot 0=-1$	0	3
15	9	-1	$1-(-1)\cdot 1=2$	1	3
9	6	1	$0-1\cdot 1=-1$	1	3
6	3	0	$1-0\cdot\ldots=1$	2	3
3	0	1	0	–	3

$$a\cdot x+b\cdot y=d$$

$$2\cdot 9+(-1)\cdot 15=3$$