* SZÜNET UTÁN KEDD 2H ?

MINTA ZH

NOV. 2.

- 11 : OTTHONI ✓
- 1 : OTTHONI

- EUKLIDESZI ALGO.
- GYORS HATVÁNYOZÁS
- KÍNAI TT.
- PRÍMTESZTELÉS

EUKL. ALGO.

INPUT: $a, b \in \mathbb{Z}_0^+$

OUTPUT: $d \in \mathbb{Z}^+ : \text{LNKO}(a, b)$

```
def eu(a,b):                                  ← if b==0:
    a', b' = b, a mod b                           return a
    return eu(a', b')
```

PL:

a	b
28	12
12	4
4	0 ←

BŐVÍTETT EUKLIDESZI ALGO:

INPUT: a, b

OUTPUT: d, x, y $\quad d = LNKO(a, b)$

LIN. KOMB.

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

TRÜKK: minden új számnál: b' - hoz $\exists x', y'$:

$$\downarrow$$

$$b' = ax' + by'$$

172,62

d	x	y	// $d = ax + by$
$a = 172$	1	0	
$b = 62$	0	1	
$172 - 62 \cdot 2 = 48$	$1 - 0 \cdot 2 = 1$	$0 - 1 \cdot 2 = -2$	
$62 - 48 \cdot 1 = 14$	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-2) = 3$	
$48 - 14 \cdot 3 = 6$	4	-11	
$14 - 6 \cdot 2 = 2$	-9	$+25$	← RET.
$6 - 2 \cdot 3 = 0$			

$172 = 172 \cdot 1 + 62 \cdot 0$ (A)

$62 = 172 \cdot 0 + 62 \cdot 1$ (B)

$48 = 172 \cdot (1 - 2 \cdot 0) + 62 \cdot (0 - 2 \cdot 1)$ (A) $- 2 *$ (B)

ott:

$d=2 \qquad x=-9 \qquad y=+25$

$2 = 172 \cdot (-9) + 62 \cdot (+25)$

OLYAN FELADATNÁL, HOGY

$a \cdot z \equiv c \pmod{b}$ ← felírás:

$z = ?$

↓ kongruens

↓ modulo

a, b bővített EUKL.:

$d = LNKO = ax + by$

Ha $d=1$: „nyertünk”:

$a \cdot z \equiv c \pmod{b} \qquad / \cdot x$

$a \cdot x \cdot z = x \cdot c \pmod{b}$

$x \equiv x' \pmod{m}$

$\Uparrow$

$x \,\%\, m = x' \,\%\, m$

$\Updownarrow$

m osztója $(x - x')$-nek

1

$$z \equiv x \cdot c \ (b) \qquad a \cdot x \equiv a \cdot x + by \equiv 1 \ (b)$$

Př.

$$\underset{a}{3} \cdot x \equiv \underset{c}{7} \ (\underset{b}{10})$$

$$\text{LNKO}(3,10) = 1 = 3 \cdot (-3) + 10 \cdot (+1)$$

$$3 \cdot x \equiv 7 \ (10) \qquad / \cdot (-3)$$

$$(-3) \cdot 3 \cdot x \equiv 7 \cdot (-3) \equiv 9 \pmod{10}$$

$$x \equiv 9 \ (10)$$

KÍNAI MARADÉKTÉTEL:

$$\begin{cases} x \equiv a_1 \quad (m_1) \\ x \equiv a_2 \quad (m_2) \end{cases}$$

Pl.:

$x \equiv 7 \quad (23)$

$x \equiv 2 \quad (29)$

Bőv EUKL. ALGO:

$(m_1, m_2) \quad : \quad d = 1 = m_1 \cdot s + m_2 \cdot t$

ow: d, s, t

$$x \equiv m_1 \cdot s \cdot a_2 + m_2 \cdot t \cdot a_1 \qquad (m_1 m_2)$$

$(m_1 \cdot s a_2 + m_2 \cdot t \cdot a_1) \,\%\, m_1 = m_2 \cdot t \cdot a_1$

$(m_2 \cdot t) \,\%\, m_1 = (m_2 \cdot t + m_1 \cdot s) \,\%\, m_1 = 1$

$\Rightarrow x \equiv a_1 \quad (m_1)$ ✓

$x \equiv m_1 \cdot s \cdot a_2 + m_2 \cdot t \cdot a_1$

$29 \cdot 4 \cdot 7 + 23 \cdot (-5) \cdot 2$

$= 582$

a_2 m_2

$x \equiv 7 \quad (23)$

$x \equiv 2 \quad (29)$

a_1 m_1

	s	t
29	1	0
23	0	1
$29 - 23 \cdot 1 = 6$	1	-1
$23 - 6 \cdot 3 = 5$	-3	4
$6 - 5 \cdot 1 = 1$	4	-5
$5 - 1 \cdot 5 = 0$		

$// \; 1 = 29 \cdot 4 + 23 \cdot (-5)$

$116 - 115$

GYORSHATVÁNYOZÁS: $a^n \bmod m = ?$

n páros: $a^n = (a^{n/2})^2$

n páratlan: $a^n = \left(a^{\frac{n-1}{2}}\right)^2 \cdot a$

$a^{1000} = (a^{500})^2$

$a^{1001} = (a^{500})^2 \cdot a$

```
def pow(a, n):
    if n == 1:
        return a
    if n % 2 == 1:
        return (a^((n-1)/2))^2 * a
    else
        return (a^(n/2))^2
```

(rek) →

n

PRÍMTESZTELÉS :

- TRIVIÁLIS: van-e osztója 2 és $(n-1)$ közt?
- FERMAT-teszt:

TÉTEL: p prím, a nem osztható p-vel:

$$a^{p-1} \,\%\, p == 1$$

TESZT: RND a:

$$a^{p-1} \,\%\, p \stackrel{?}{=} 1$$

N

NEM PRÍM

VÉGE

IGAZAN PRÍM

```
R:
for (i in 2:(n-1))
{

}
```

```
for(i=2; i<n; i++) {

;

}
```

C++

R

$n=4$:	$i=2, i=3$	$i=2, i=3$ ✓
$n=3$:	$i=2$	$i=2$ ✓
$n=2$:	∅	$i=2, i=1$???