Tema 1
Valachi Emilia, M532

1) Găsiți numărul minim și maxim de pași pentru algoritmul lui Euclid.

1. Complexitatea $\Rightarrow \Theta(\log(\min(a,b)))$

Dacă avem $a, b \in \mathbb{Z}$, cu $a < b$,
iar k = numărul de pași ai algoritmului
pt a afla c.m.m.d.c.-ul pt. a și b,

$\Rightarrow$ cu fiecare pas k, $a \cdot b \geq 2^k$

$\Rightarrow$ $\boxed{k \leq \log_2 a + \log_2 b}$

[redacted]
această relatie determină numărul aproximativ de pași – k.

2. Numărul minim de pași

[redacted]

Contează distanța dintre numere, nu mărimea acestora:

Ex: $(2000, 2001) = ?$

1) $2001 = 1 \cdot 2000 + 1$ $\Rightarrow$ $(2000, 2001) = 1$
2) $2000 = 2000 \cdot 1 + 0$

3. Numărul maxim de pași

Numerele Fibonacci consecutive solicită cel mai mare număr de pași în cadrul algoritmului.

Ex: $(5, 8) = ?$

1) $8 = 5 \cdot 1 + 3$
2) $5 = 3 \cdot 1 + 2$
3) $3 = 2 \cdot 1 + 1$
4) $2 = 1 \cdot 2 + 1$
5) $1 = 1 \cdot 1 + 0$

2) Det. c.m.m.d.c. al 55667 și 77665 folosind alg. lui Euclid. Găsiți coef. Bezout.

Nr. 14

$x_{77665} = (1, 0) \quad x_{55667} = (0, 1)$

1) $77665 = 1 \cdot 55667 + \underline{21998}$

$x_{21998} = (1, 0) - (0, 1) = (1, -1)$

2) $55667 = 21998 \cdot 2 + \underline{11671}$

$x_{11671} = (0, 1) - 2(1, -1) = (-2, 3)$

3) $21998 = 11671 \cdot 1 + \underline{10327}$

$x_{10327} = (1, -1) - (-2, 3) = (3, -4)$

4) $11671 = 10327 \cdot 1 + \underline{1344}$

$x_{1344} = (-2, 3) - (3, -4) = (-5, 7)$

5) $10327 = 1344 \cdot 7 + \underline{919}$

$x_{919} = (3, -4) - 7(-5, 7) = (38, -53)$

6) $1344 = 919 \cdot 1 + \underline{425}$

$x_{425} = (-5, 7) - (38, -53) = (-43, 60)$

7) $919 = 425 \cdot 2 + \underline{69}$

$x_{69} = (38, -53) - 2(-43, 60) = (124, -173)$

8) $425 = 69 \cdot 6 + \underline{11}$

$x_{11} = (-43, 60) - 6 \cdot (124, -173) = (-43, 60) - (744, -1038) =$
$= (-787, 1098)$

9) $69 = 11 \cdot 6 + \underline{3}$

$x_3 = (124, -173) - 6 \cdot (-787, 1098) = (124, -173) -$
$- (-4722, 6588) = (4846, -6761)$

10) $11 = 7 \cdot 8 + 2$

$x_2 = (-787, 1098) - 7(4846, -6761) =$

$= (-787, 1098) - (14538, -20.283) = (-15325, 21381)$

11) $7 = 2 \cdot 3 + \boxed{1}$

$x_1 = (4846, -6761) - (-15325, 21381) = (20.171, -28142)$

12) $2 = 1 \cdot 2 + 0$

$\Rightarrow (55667, 77665) = 1$

Coef. Bezout:

$1 = \underline{20.171} \cdot 77665 \underline{-28142} \cdot 55667$

Am luat din greșeală ex. ② 14 de la mate în loc de mate-info. Dar nu este nimeni cu nr. 14 la mate, așa că sper să nu fie o problemă...

③ Calculați inversul modular

Găsește inversul lui 15 în $\mathbb{Z}_{59}$.

$(15, 59) = 1 \Rightarrow \exists\, u, v \in \mathbb{Z}$ a.î.

$15 \cdot u + 59 \cdot v = 1 \mid \bmod 59$

$15^{-1} \equiv u \pmod{59}$

$(a,n) = 1$

$\Rightarrow \exists\, u, v \in \mathbb{Z}$ a.î.

$au + nv = 1 \mid \bmod n$

$au \equiv 1 \pmod n$

$u = a^{-1} \pmod n$

Euclid: $x_{59} = (1,0) \quad x_{15} = (0,1)$

1) $59 = 3 \cdot 15 + \underline{14}$

$x_{14} = (1,0) - 3(0,1) = (1, -3)$

2) $15 = 14 \cdot 1 + 1$

$x_1 = (0,1) - (1,-3) = (-1, 4)$

3) $14 = 1 \cdot 14 + 0$

$\Rightarrow 1 = \underline{(-1)} \cdot 59 + \underline{4} \cdot 15 \qquad \Rightarrow u = 4$

$\Rightarrow 15^{-1} = 4 \pmod{59} = \boxed{4}$