Gherasim Ana-Teodora

Tema portofoliu
(seminar 2)

1) Numărul maxim de pași pentru algoritmul lui Euclid

$d = (a, b)$

$a = 0$ sau $b = 0 \Rightarrow d = a$ respectiv b (numărul minim de pași = 0)

T.Î.R $\Rightarrow a = bq_0 + r_0$ $\begin{cases} r_0 = 0 \Rightarrow d = b \\ r_0 \neq 0 \Rightarrow \text{repetăm împărțirea} \end{cases}$

...

$r_{n-2} = r_{n-1} \cdot q_n + r_n$

$r_{n-1} = r_n \cdot q_{n+1}$

Lemă:
$\exists\, n \in \mathbb{N}$, a.î. $r_n \neq 0$ și $r_{n+1} = 0$. Atunci algoritmul se oprește după $n+1$ pași și $r_n = (a, b)$

2) Numărul de operații elementare pt. alg. lui Euclid.
(= nr. operații modulo)

Corolar
Fie $a, b \in \mathbb{Z}^*$, $|b| \leq |a|$. Fie $k = \lfloor \log_2 b \rfloor + 1$ nr. biților necesari pentru scrierea lui b în baza 2. Atunci algoritmul lui Euclid se oprește după $2k$ împărțiri.

6) 15) $d = (\overset{b}{66778}, \overset{a}{88776})$

$88776 = 66778 \cdot 1 + 21998$

$66778 = 21998 \cdot 3 + 784$

$21998 = 784 \cdot 28 + 46$

$784 = 46 \cdot 17 + 2$

$46 = 2 \cdot 23 + 0$

$d = 2$

$X_{88776} = (1,0)$, $X_{66778} = (0,1)$

$X_{21998} = (1,0) - 1 \cdot (0,1) = (1,-1)$

$X_{784} = (0,1) - 3 \cdot (1,-1) = (-3,4)$

$X_{46} = (1,-1) - 28 \cdot (-3,4) =$

$= (1+28 \cdot 3, -1-4 \cdot 28) =$

$= (85, -113)$

$X_2 = (-3,4) - 17 \cdot (85,-113)$

$= (-3,4) + (-1445, 1921)$

$= (-1448, 1925)$

$2 = 784 - 46 \cdot 17 = (66778 - 3 \cdot 21998) - (21998 - 28 \cdot 784) \cdot 17$

$= b - 3 \cdot (a-b) - 17 [a-b - 28 (b - 3 \cdot 21998)] =$

$= b - 3a + 3b - 17 (a - b - 28b + 3 \cdot 28 (a-b)) =$

$= 4b - 3a - 17a + 17b + 28 \cdot 17b - 3 \cdot 28 \cdot 17 (a-b) =$

$= 3786 - 20a - 1071a + 1071b =$

$= 1449b - 1091a$

7) inversul lui 42 mod 61

$61 = 42 \cdot 1 + 19$

$42 = 19 \cdot 2 + 4$

$19 = 4 \cdot 4 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 3 \cdot 1 + 0$

$(\underset{a}{42}, \underset{b}{61}) = 1 \Rightarrow$ 42 inversabil modulo 61

$1 = 4 - 3 \cdot 1 = (42 - 19 \cdot 2) - (19 - 4 \cdot 4) = (a - 2(b-a)) - (b-a) - 4(a - 19 \cdot 2))$

$= a - 2b + 2a - b + a + 4a - 4 \cdot 2 \cdot 19 =$

$= 8a - 3b - 8(b-a) = 8a - 3b - 8b + 8a = 16a - 11b$

$a^{-1} = 16$