Tema2_Criptografie

Ioana Ilie

28 February 2026

1 Ex2 si Ex4

Teoremă. Fie $a, b \in \mathbb{Z}^*$, cu $|b| \leq |a|$. Algoritmul lui Euclid se oprește după cel mult $2k$ pași, unde $k = [\log_2 |b|] + 1$ este numărul de biți ai lui b.

Demonstrație.

Presupunem $|b| \leq |a|$ și notăm

$$r_0 := |b|.$$

Algoritmul lui Euclid produce relațiile:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < r_0,$$

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1,$$

$$\dots$$

$$r_{k-1} = r_k q_{k+1} + r_{k+1}, \quad 0 \leq r_{k+1} < r_k.$$

Există $n \in \mathbb{N}$ astfel încât $r_n \neq 0$ și $r_{n+1} = 0$. Atunci algoritmul se oprește după $n + 1$ pași și

$$r_n = (a, b).$$

Din propoziția de la curs avem:

$$r_{k+2} < \frac{r_k}{2}, \quad \forall k \in \{0, 1, \dots, n-1\}.$$

Aplicând recursiv această inegalitate obținem:

$$r_{2i} < \frac{r_0}{2^i}.$$

Algoritmul se oprește când $r_{2i} < 1$. Deoarece resturile sunt numere naturale, aceasta implică:

$$\frac{r_0}{2^i} < 1.$$

Rezultă:

$$r_0 < 2^i,$$

$$i > \log_2 r_0.$$

Prin urmare, numărul de pași n satisface:

$$n \leq 2 \log_2 r_0.$$

Dacă notăm

$$k = [\log_2 |b|] + 1,$$

atunci

$$n \leq 2k.$$

Concluzie. Algoritmul lui Euclid se oprește după cel mult $2k$ împărțiri, unde k este numărul de biți ai lui b. Prin urmare, algoritmul are complexitate polinomială în lungimea numerelor de intrare. □

Observație (cazul în care se obține numărul maxim de pași).

Numărul maxim de pași ai algoritmului lui Euclid se obține atunci când câturile q_i din împărțirile succesive sunt toate egale cu 1.

References

[1] Curs Criptografie - Elemente de aritmetică, Lițcanu R.