

Tema 1

1. Utilizați algoritmul lui Euclid extins pentru a calcula $\text{cmmdc}(22231, 33227)$, găsiți coeficienții Bezout

$$\begin{aligned} 33227 &= 22231 \cdot 1 + 10996 \\ 22231 &= 10996 \cdot 2 + 24 \\ 10996 &= 24 \cdot 457 + 8 \\ 24 &= 8 \cdot 3 + 0 \quad \Rightarrow \text{c.m.m.d.c.}(22231, 33227) = 8 \end{aligned}$$

Vom aplica alg. lui Euclid:

$$ax + by = \text{cmmdc}(a, b)$$

$$\begin{aligned} 8 &= 10996 - 457 \cdot 24 \\ 8 &= 10996 - 457 \cdot (22231 - 10996 \cdot 2) \\ 8 &= 10996 - 457 \cdot 22231 + 457 \cdot 10996 \cdot 2 \\ 8 &= 3 \cdot 10996 - 457 \cdot 22231 \end{aligned}$$

\Rightarrow Coeficienții Bezout: $(3, -457)$

2. Calculați complexitatea algoritmului lui Euclid extins:

$$O(\log(\min(a, b))), \text{ unde } a, b \text{ sunt numere}$$

unde a, b sunt cele două numere ptu care se calculează cmmdc .

În alg. lui Euclid extins, fiecare pas implică operații simple: înmulțiri, adunări și scăderi cu o complexitate neglijabilă, în comparație cu complexitatea alg. lui Euclid clasică.

\Rightarrow Complexitatea este eficientă.

3. Găsiți inversul lui 21 (mod 83)

Vom folosi Euclid extins

$$ax + by = \text{cmmdc}(a, b) \quad \begin{array}{l} a = 83 \\ b = 21 \end{array}$$

Pas 1: Alg. Euclid:

$$83 = 21 \cdot 3 + 20$$

$$21 = 20 \cdot 1 + 1$$

$$20 = 1 \cdot 20 + 0$$

Pas 2: Lucrăm în sens invers pentru coeficientii Bezout:

$$1 = 21 - 20$$

$$1 = 21 - (83 - 21 \cdot 3)$$

$$1 = 21 \cdot 4 - 83$$

$$\Rightarrow x = 4 \quad \Rightarrow \text{inversul: } 21 (\text{mod } 83) \equiv 4^{-1}$$