TEMĂ

SEMINARUL 1

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

Fie $a, b \in \mathbb{Z}_+$, $a > b$.

Numărul minim de pași este atins atunci când a și b sunt consecutive în șirul lui Fibonacci.

$\phi = \frac{1+\sqrt{5}}{2}$ (proporția de aur)

Nr. minim de pași $= O(\log_\phi b)$

Dacă a și b sunt prime între ele, atunci este atins numărul maxim de pași, și anume $O(\log_2 b)$.

2. Găsiți cel mai mare divizor comun al lui 12345 și 54321 folosind algoritmul lui Euclid extins pentru a determina coeficienții Bezout.

$x_{54321} = (1,0) \quad x_{12345} = (0,1)$

$x_{4941} = x_{5432} - 4 \cdot x_{12345} = (1,0) - 4(0,1) = (1,-4)$

$x_{2463} = x_{12345} - 2x_{4941} = (0,1) - 2(1,-4) = (-2,9)$

$x_{15} = x_{4941} - 2x_{2463} = (1,-4) - 2(-2,9) = (5,-22)$

$x_3 = x_{2463} - 164x_{15} = (-2,9) - 164(5,-22) = (-822, 3617)$

$$\begin{array}{r|l} 54321 & 12345 \\ 49380 & 4 \\ \hline 4941 & \end{array}$$

$$\begin{array}{r|l} 12345 & 4941 \\ 9882 & 2 \\ \hline 2463 & \end{array}$$

$$\begin{array}{r|l} 4941 & 2463 \\ 4926 & 2 \\ \hline 15 & \end{array}$$

$$\begin{array}{r|l} 2463 & 15 \\ 2460 & \\ \hline 3 & \end{array}$$

$$\begin{array}{r|l} 15 & 3 \\ 15 & 5 \\ \hline == & \end{array}$$

3. Găsiți inversul modular al lui 7 modulo 11.

$7x \equiv 1 \pmod{11}$

$(7, 11) = 1$

$11 = (1,0) \quad 7 = (0,1)$

$$\begin{array}{r|l} 11 & 7 \\ \underline{7} & 1 \\ 4 & \end{array} \qquad x_4 = x_{11} - 1 \cdot x_7 = (1,0) - (0,1) = (1,-1)$$

$$\begin{array}{r|l} 7 & 4 \\ \underline{4} & 1 \\ 3 & \end{array} \qquad x_3 = x_7 - 1 x_4 = (0,1) - (1,-1) = (-1,2)$$

$$\begin{array}{r|l} 4 & 3 \\ \underline{3} & 1 \\ 1 & \end{array} \qquad x_1 = x_4 - 1 \cdot x_3 = (1,-1) - (-1,2) = (2,-3)$$

$1 = 2 \cdot 11 - 3 \cdot 7 \ \Big| \pmod{11} \Rightarrow 1 \equiv -3 \cdot 7 \pmod{11}$

$-3 \equiv 11 - 3 \pmod{11} \equiv 8 \pmod{11}$