Criptografie

Grigorian Iuliana-Elena

February 2026

1 Cerința

Determinați inversul modular al lui 41 modulo 43.

2 Rezolvare

$$
\begin{aligned}
43 : 41 &= 1 \text{ rest } 2 \\
43 &= 1 \cdot 41 + 2 \\
x_{43} &= (1, 0) \\
x_{41} &= (0, 1) \\
41 &= 20 \cdot 2 + 1 \\
x_2 &= x_{43} - x_{41} = (1, -1) \\
x_1 &= x_{41} - 20 \cdot x_2 = (0, 1) - 20 \cdot (1, -1) = (-20, 21) \\
1 &= -20 \cdot 43 + 21 \cdot 41
\end{aligned}
$$

$21 \cdot 41 \equiv 1 \pmod{43}$, deci $41^{-1} \equiv 21 \pmod{43}$