1 41-Inversul modular al lui 53 modulo 131

Aplicăm algoritmul lui Euclid extins pentru $(131, 53)$:

$$\begin{aligned} 131 &= 53 \times 2 + 25 \\ 53 &= 25 \times 2 + 3 \\ 25 &= 3 \times 8 + 1 \\ 3 &= 1 \times 3 + 0 \end{aligned}$$

Deci $\gcd(131, 53) = 1$, deci inversul există.

Calculăm coeficienții Bézout:

$$\begin{aligned} x_{25} &= (1, 0) - 2 \cdot (0, 1) = (1, -2) \\ x_3 &= (0, 1) - 2 \cdot (1, -2) = (-2, 5) \\ x_1 &= (1, -2) - 8 \cdot (-2, 5) = (17, -42) \end{aligned}$$

Deci:

$$17 \cdot 131 + (-42) \cdot 53 = 1$$

Luând egalitatea $\pmod{131}$, obținem:

$$(-42) \cdot 53 \equiv 1 \pmod{131}$$

Deoarece $-42 \equiv 89 \pmod{131}$, rezultă:

$$53^{-1} \equiv 89 \pmod{131}$$