

Criptografia - Tema 1

2) CMMDC

cmmdc(12347, 54329)

$$X_{54329} = (1, 0), \quad X_{12347} = (0, 1)$$

$$\begin{array}{r} 54329 \\ 49388 \\ \hline 49388 \\ 5 \end{array} \quad \begin{array}{l} 54329 = 12347 \cdot 4 + 4937 \\ 4937 \end{array} \Rightarrow X_{4937} = X_{54329} - 4 \cdot X_{12347} = (1, -4)$$

$$\begin{array}{r} 12347 \\ 9882 \\ \hline 9882 \\ 2 \end{array} \quad \begin{array}{l} 12347 = 4937 \cdot 2 + 2465 \\ 2465 \end{array} \Rightarrow X_{2465} = X_{12347} - 2 \cdot X_{4937} = (0, 1) - 2(1, -4) = (-2, 9)$$

$$\begin{array}{r} 4937 \\ 4930 \\ \hline 4930 \\ 7 \end{array} \quad \begin{array}{l} 4937 = 2465 \cdot 2 + 11 \\ 11 \end{array} \Rightarrow X_{11} = X_{4937} - 2 \cdot X_{2465} = (1, -4) - 2(-2, 9) = (5, -22)$$

$$\begin{array}{r} 2465 \\ 2464 \\ \hline 2464 \\ 1 \end{array} \quad \begin{array}{l} 2465 = 11 \cdot 224 + 1 \\ 224 \end{array} \Rightarrow X_1 = X_{2465} - 224 \cdot X_{11} = (-2, 9) - 224 \cdot (5, -22) = (-1122, 4937)$$

$$\text{cmmdc}(12347, 54329) = 1$$

$$1 = (-1122) \cdot \frac{12347}{54329} + 4937 \cdot \frac{54329}{12347}$$

3) inversul lui 3 în \mathbb{Z}_{11}

$$(3, 11) = 1 \Rightarrow \exists \mu, \nu \in \mathbb{Z} \text{ a.i.}$$

$$1 = 3\mu + 11\nu \quad \Bigg/ \quad \text{mod } 11$$

$$1(\text{mod } 11) \equiv 3\mu(\text{mod } 11)$$

$$3^{-1} \equiv \mu(\text{mod } 11)$$

$$x_{11} = (1, 0), \quad x_3 = (0, 1)$$

$$11 = 3 \cdot 3 + 2 \quad \Rightarrow \quad x_2 = x_{11} - x_3 = (1, -3)$$

$$3 = 2 \cdot 1 + 1 \quad \Rightarrow \quad x_1 = x_3 - x_2 = (-1, 4)$$

$$1 = (-1) \cdot 11 + 4 \cdot 3 \quad \Rightarrow \quad \mu = +4 \Rightarrow$$

$$\Rightarrow 3^{-1} \equiv (+4)(\text{mod } 11) \Rightarrow \cancel{3^{-1} \equiv 10(\text{mod } 11)} \Rightarrow$$

$$\Rightarrow 3^{-1} = 4 \text{ în } \mathbb{Z}_{11}$$