

Forma 21

1. Determinați cmmdc al lui 34561 și 76549 folosind algoritmul lui Euclid extins și determinați coeficientii Bezout

$$x_{76549} = (1, 0), x_{34561} = (0, 1)$$

$$76549 = 2 \cdot 34561 + 7427 \Rightarrow 7427 = (1, 0) - 2(0, 1) = (1, -2)$$

$$34561 = 4 \cdot 7427 + 4853 \Rightarrow 4853 = (0, 1) - 4(1, -2) = (-4, 9)$$

$$7427 = 1 \cdot 4853 + 2574 \Rightarrow 2574 = (1, -2) - (-4, 9) = (5, -11)$$

$$4853 = 1 \cdot 2574 + 2279 \Rightarrow 2279 = (-4, 9) - (5, -11) = (-9, 20)$$

$$2574 = 1 \cdot 2279 + 295 \Rightarrow 295 = (5, -11) - (-9, 20) = (14, -31)$$

$$2279 = 7 \cdot 295 + 214 \Rightarrow 214 = (-9, 20) - 7(14, -31) = (-107, 232)$$

$$295 = 1 \cdot 214 + 81 \Rightarrow 81 = (14, -31) - (-107, 232) = (121, -268)$$

$$214 = 2 \cdot 81 + 52 \Rightarrow 52 = (-107, 232) - 2(121, -268) = (-349, 773)$$

$$81 = 1 \cdot 52 + 29 \Rightarrow 29 = (121, -268) - (-349, 773) = (470, -1041)$$

$$52 = 1 \cdot 29 + 23 \Rightarrow 23 = (-349, 773) - (470, -1041) = (-819, 1814)$$

$$29 = 7 \cdot 23 + 6 \Rightarrow 6 = (470, -1041) - (-819, 1814) = (1289, -2855)$$

$$23 = 3 \cdot 6 + 5 \Rightarrow 5 = (-819, 1814) - 3(1289, -2855) = (-4686, 10329)$$

$$6 = 1 \cdot 5 + 1 \Rightarrow 1 = (1289, -2855) - (-4686, 10329) = (5975, -13184)$$

$$= (5975, -13184)$$

2. Determina inversul lui 4 în modulo 13.

$$13 = 3 \cdot 4 + 1 \Rightarrow 1 = 1 \cdot 13 - 3 \cdot 4$$

$$4 \cdot 3 \equiv -1 \pmod{13} \quad (-1)$$

$$-4 \cdot 3 \equiv 1 \pmod{13}$$

$$4 \cdot (-3) \equiv 1 \pmod{13}$$

$$4 \cdot 10 \equiv 1 \pmod{13}$$

→ 10 inversul lui 4 (mod 13)