① .23. Calculați CMMDC al lui 55579 și 66569 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout

CMMDC (55579, 66569) $X_{55579} = (1,0)$ $X_{66569} = (0,1)$

$66569 = 55579 \cdot 1 + 10990$

$55579 = 10990 \cdot 5 + 629$

$10990 = 629 \cdot 17 + 297$

$629 = 297 \cdot 2 + 35$

$297 = 35 \cdot 8 + 17$

$35 = 17 \cdot 2 + 1$ $\Rightarrow$ CMMDC(55579, 66569) = 1

$X_{10990} = X_{66569} - X_{55579} \cdot 1 = (0,1) - (1,0) = (-1,1)$

$X_{629} = X_{55579} - 5X_{10990} = (1,0) - 5(-1,1) = (1,0) - (-5,5)$
$= (6,-5)$

$X_{297} = X_{10990} - 17 \cdot X_{629} = (-1,1) - 17 \cdot (6,-5) = (-1,1) - (102,-85)$
$= (-103,86)$

$X_{35} = X_{629} - 2 \cdot X_{297} = (6,-5) - 2(-103,86) = (212,-177)$

$X_{17} = X_{297} - 8 \cdot X_{35} = (-103,86) - 8 \cdot (212,-177) = (-1799,1502)$

$X_1 = X_{35} - 2 \cdot X_{17} = (212,-177) - 2(-1799,1502) = (3810,-3181)$

$1 = \underline{3810} \cdot 66569 - \underline{3181} \cdot 55579$

② .23. Inversul lui 24 în modulo 101

$(24,101) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ a.î.

$1 = 24u + 101v \,/_{\text{mod } 101}$ $\Rightarrow 1 \pmod{101} = 24u \pmod{101} \Rightarrow$

$\Rightarrow 24^{-1} \equiv u \pmod{101}$

$X_{101} = (1,0)$, $X_{24} = (0,1)$

$101 = 24 \cdot 4 + 5 \Rightarrow X_5 = X_{101} - 4 \cdot X_{24} = (1,0) - 4(0,1) = (1,-4)$

$24 = 5 \cdot 4 + 4 \Rightarrow X_4 = X_{24} - 4 \cdot X_5 = (0,1) - (4,-16) = (-4,17)$

$5 = 4 \cdot 1 + 1 \Rightarrow X_1 = X_5 - X_4 = (1,-4) - (-4,17) = (5,-21)$

$1 = 5 \cdot 101 - 21 \cdot 24 \Rightarrow \underline{u = -21} \Rightarrow 24^{-1} \equiv -21 \pmod{101} \Rightarrow$

$\Rightarrow 24^{-1} \equiv 80 \pmod{101}$