Criptografie-Tema1

guzurazvan

March 2024

I. 24. Determinați CMMDC al lui 66703 și 77687 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

$77687 = 66703 \cdot 1 + 10984,$
$66703 = 10984 \cdot 6 + 799,$
$10984 = 799 \cdot 13 + 597,$
$799 = 597 \cdot 1 + 202$
$597 = 202 \cdot 2 + 193$
$202 = 193 \cdot 1 + 9$
$193 = 9 \cdot 21 + 4$
$9 = 4 \cdot 2 + 1$
$4 = 1 \cdot 4 + 0$

$\Rightarrow cmmdc(77687, 66703) = 1$

$\mathrm{x}_{77687} = (1, 0)$
$x_{66703} = (0, 1)$
$x_{10984} = x_{77687} - 1 \cdot x_{66703} = (1, -1)$
$x_{799} = x_{66703} - 6 \cdot x_{10984} = (0, 1) - 6 \cdot (1, -1) = (-6, 7)$
$x_{597} = x_{10984} - 13 \cdot x_{799} = (1, -1) - 13 \cdot (-6, 7) = (79, -92)$
$x_{202} = x_{799} - 1 \cdot x_{597} = (-6, 7) - (79, -92) = (-85, 99)$
$x_{193} = x_{597} - 2 \cdot x_{202} = (79, -92) - 2 \cdot (-85, 99) = (249, -290)$
$x_9 = x_{202} - 1 \cdot x_{193} = (-85, 99) - (249, -290) = (-334, 389)$
$X_4 = x_{193} - 21 \cdot x_9 = (249, -290) - 21 \cdot (-334, 389) = (7263, -8459)$
$x_1 = x_9 - 2 \cdot x_4 = (-334, 389) - 2 \cdot (7263, -8459) = (-14860, 17307)$

$1 = 9 - 4 \cdot 2$
$1 = (202 - 193) + 4 \cdot (-2)$
$1 = (799 - 597) - (597 - 202 \cdot 2) + (193 - 9 \cdot 21) \cdot (-2)$
$1 = 799 + 597 \cdot (-2) + 202 \cdot 2 + 193 \cdot (-2) + 9 \cdot 42$
$1 = (66703 - 10984 \cdot 6) + (10984 - 799 \cdot 13) \cdot (-2) + (799 - 597) \cdot 2 + (597 - 202 \cdot 2) \cdot (-2) + (202 - 193) \cdot 42$

$1 = 66703 + 10984 \cdot (-6) + 10984 \cdot (-2) + 799 \cdot 26 + 799 \cdot 2 + 597 \cdot (-2) + 597 \cdot (-2) + 202 \cdot 4 + 202 \cdot 42 + 193 \cdot (-42)$
$1 = 66703 + 10984(-8) + 799 \cdot 28 + 597 \cdot (-4) + 202 \cdot 46 + 193 \cdot (-42)$
$1 = 66703 \cdot 1 + (77687 - 66703) \cdot (-8) + (66703 - 10984 \cdot 6) \cdot 28 + (10984 - 799 \cdot 13) \cdot (-4) + (799 - 597) \cdot 46 + (597 - 202 \cdot 2) \cdot (-42)$
$1 = 77687 \cdot (-8) + 66703 \cdot (1 + 8 + 28) + 10984 \cdot (-6 * 28 - 4) + 799 \cdot (52 + 46) + 597 \cdot (-46 - 42) + 202 \cdot 84$
$1 = 77687 \cdot (-8) + 66703 \cdot 37 + 10984 \cdot (-172) + 799 \cdot 98 + 597 \cdot (-88) + 202 \cdot 84$
$1 = 77687 \cdot (-8) + 66703 \cdot 37 + (77687 - 66703) \cdot (-172) + (66703 - 10984 \cdot 6) \cdot 98 + (10984 - 799 \cdot 13) \cdot (-88) + (799 - 597) \cdot 84$
$1 = 77687 \cdot (-8 - 172) + 66703 \cdot (37 + 172 + 98) + 10984 \cdot (-6 * 98 - 88) + 799 \cdot (13 * 88 + 84) + 597 \cdot (-84)$
$1 = 77687 \cdot (-180) + 66703 \cdot 307 + 10984 \cdot (-676) + 799 \cdot 1228 + 597 \cdot (-84)$
$1 = 77687 \cdot (-180) + 66703 \cdot 307 + (77687 - 66703) \cdot (-676) + (66703 - 10984 \cdot 6) \cdot 1228 + (10984 - 799 \cdot 13) \cdot (-84)$
$1 = 77687 \cdot (-180 - 676) + 66703 \cdot (307 + 676 + 1228) + 10984 \cdot (-6 * 1228 - 84) + 799 \cdot (13 * 84)$
$1 = 77687 \cdot (-856) + 66703 \cdot 2211 + 10984 \cdot (-7452) + 799 \cdot (1092)$
$1 = 77687 \cdot (-856) + 66703 \cdot 2211 + (77687 - 66703) \cdot (-7452) + (66703 - 10984 \cdot 6) \cdot 1092$
$1 = 77687 \cdot (-856 - 7452) + 66703 \cdot (2211 + 7452 + 1092) + 10984 \cdot (-6 * 1092)$
$1 = 77687 \cdot (-8308) + 66703 \cdot 10755 + 10984 \cdot (-6552)$
$1 = 77687 \cdot (-8308) + 66703 \cdot 10755 + (77687 - 66703) \cdot (-6552)$
$1 = 77687 \cdot (-8308 - 6552) + 66703 \cdot (10755 + 6552)$
$1 = 77687 \cdot (-14860) + 66703 \cdot 17307$

II. 24. Determină inversul lui 25 în modulo 103.

a = 25
n = 103
cmmdc(25, 103) = 1 (evident)
$\Rightarrow \exists 25^{-1} \in Z_n$
$\Rightarrow \exists u, v \in Z a.i. 25 \cdot u + 103 \cdot v = 1, 25^{-1} = u$
$103 = 25 \cdot 4 + 3$
$25 = 3 \cdot 8 + 1$
$3 = 1 \cdot 3 + 0$

$1 = 25 - 3 \cdot 8$
$1 = 25 - (103 - 25 \cdot 4) \cdot 8$
$1 = 25 - 103 \cdot 8 + 25 \cdot 32$
$1 = 25 \cdot 33 - 103 \cdot 8$
$\Rightarrow 25^{-1} = 33$