TEMĂ 1

CMMDC

⑤. (56789, 98761) $X_{98761} = (1,0)$ $X_{56789} = (0,1)$

$98761 = 56789 \cdot 1 + 41972$

$X_{41972} = (1,0) - (0,1) = (1,-1)$

$56789 = 41972 \cdot 1 + 14817 \Rightarrow X_{14817} = (0,1) - (1,-1) = (-1,2)$

$41972 = 14817 \cdot 2 + 12338 \Rightarrow X_{12338} = (1,-1) - 2 \cdot (-1,2) = (3,-5)$

$14817 = 12338 \cdot 1 + 2479 \Rightarrow X_{2479} = (-1,2) - (3,-5) = (-4,7)$

$12338 = 2479 \cdot 4 + 2422 \Rightarrow X_{2422} = (3,-5) - 4 \cdot (-4,7) = (19,-33)$

$2479 = 2422 \cdot 1 + 57 \Rightarrow X_{57} = (-4,7) - (19,-33) = (-23,40)$

$2422 = 57 \cdot 42 + 28 \Rightarrow X_{28} = (19,-33) - 42 \cdot (-23,40) = (985,-1713)$

$57 = 28 \cdot 2 + 1 \Rightarrow X_1 = X_{57} - 2 \cdot X_{28} = (-23, 40) - (1970, -3426)$

$= (-1993, 3466)$

$28 = 1 \cdot 28 + 0$

$1 = -1993 \cdot 98761 + 3466 \cdot 56789$

Inversul unui nr. în $\mathbb{Z}_n$

(5). Inversul lui 6 mod 19.

$(6, 19) = 1 \qquad 6x \equiv 1 \pmod{19}$

$X_{19} = (1, 0) \quad ; \quad X_6 = (0, 1)$

$19 = 3 \cdot 6 + 1 \Rightarrow X_1 = X_{19} - 3 \cdot X_6 = (1, 0) - 3 \cdot (0, 1) = (1, -3)$

$x \equiv 6^{-1} \cdot 1 \pmod{19}$

$1 = 1 \cdot 19 + (-3) \cdot 6 \ / \pmod{19}$

$1 \equiv (-3) \cdot 6 \pmod{19}$

$1 \equiv 16 \cdot 6 \pmod{19}$