Tema 1 (2.9) Det CMMDC al lui 90127 și 32107 fol. alg lui Euclid extins și det. coef. Bezout.

$X_a = (1,0)$, $X_b = (0,1)$

$90127 = 2 \cdot 32107 + 25913$ — $X_r = (1,0) - 2\cdot(0,1) = (1,-2)$

$32107 = 1 \cdot 25913 + 6194$ — $X_1 = (0,1) - 1\cdot(1,-2) = (-1,3)$

$25913 = 4 \cdot 6194 + 1137$ — $X_2 = (1,-2) - 4\cdot(-1,3) = (5,-14)$

$6194 = 5 \cdot 1137 + 509$ — $X_2 = (-1,3) - 5\cdot(5,-14) = (-26,73)$

$1137 = 2 \cdot 509 + 119$ — $X_1 = (5,-14) - 2\cdot(-26,73) = (57,-160)$

$509 = 4 \cdot 119 + 33$ — $X_2 = (-26,73) - 4(57,-160) = (-254,713)$

$119 = 3 \cdot 33 + 20$ — $X_2 = (57,-160) - 3(-254,713) = (819,-2299)$

$33 = 1 \cdot 20 + 13$ — $X_2 = (-254,713) - (819,-2299) = (-1073,3012)$

$20 = 1 \cdot 13 + 7$ — $X_2 = (819,-2299) - (-1073,3012) = (1892,-5311)$

$13 = 1 \cdot 7 + 6$ — $X_2 = (-1073,3012) - (1892,-5311) = (2965,-8323)$

$7 = 1 \cdot 6 + 1$ — $X_2 = (1892,-5311) - (2965,-8323) = (4857,-13634)$

$6 = 6 \cdot 1 + \boxed{0}$

$1 = 4857 \cdot 90127 + (-13634) \cdot 32107$

(3.9.) Det inversul lui 10 modulo 37.

$(10, 37)$: $37 = 3\cdot 10 + 7$

$10 = 1\cdot 7 + 3$

$7 = 2\cdot 3 + \boxed{1} \Rightarrow (10,37) = 1 \Rightarrow$ 7 inversul lui 10 mod 37

$3 = 3\cdot 1 + 0$

$1 = ua + vM \Leftrightarrow 1 = 10u + 37v \Leftrightarrow 1 \equiv 10u \pmod{37} \Rightarrow$ (u = inversul)

~~$37 \cdot 3 = 111 = 110 + 1$~~

~~$111 = 110 + 1 = 10 \cdot 11 + 1$~~

~~$\equiv$~~

$37 \cdot 7 = 259$

$10 \cdot 26 = 260$ $\Rightarrow 1 + 259 = 10 \cdot 26$

$\equiv 0 \bmod 37$

$1 = 10 \cdot 26 \bmod 37 \Rightarrow$ (u = 26)