① Găsiți CMMDC pentru 77711 și 88789 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

$88789 = 77711 \cdot 1 + 11078$

$77711 = 7 \cdot 11078 + 165$

$11078 = 67 \cdot 165 + 23$

$165 = 7 \cdot 23 + 4$

$23 = 5 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

$CMMDC(77711, 88789) = 1$

# TEMA 1

$X_{77711} = (1,0)$ , $X_{88789} = (0,1)$

$X_{88789} = X_{77711} \cdot 1 + X_{11078} \Rightarrow X_{11078} = (0,1) - (1,0) = (-1,1)$

$X_{77711} = X_{11078} \cdot 7 + X_{165} \Rightarrow X_{165} = (1,0) - (-1,1) = (2,-1)$

$X_{11078} = 67 \cdot X_{165} + X_{23} \Rightarrow X_{23} = (-1,1) - 67(2,-1) = (-135, 68)$

$X_{165} = 7 \cdot X_{23} + X_4 \Rightarrow X_4 = (2,-1) - 7(-135, 68) = (947, -477)$

$X_{23} = 5X_4 + X_3 \Rightarrow X_3 = (-135, 68) - 5(947, -477) = (4870, 2453)$

$X_4 = X_3 + X_1 \Rightarrow X_1 = (947, -477) - (4870, 2453) = (-3923, 2930)$

$1 = -3923 \cdot 88789 + 2930 \cdot 77711$

② Calculează inversul lui 26 în modulo 107.

$X_{107} = (1,0)$ , $X_{26} = (0,1)$

$107 = 4 \cdot 26 + 3 \Rightarrow X_3 = X_{107} - 4X_{26} = (1,0) - 4(0,1) = (1,-4)$

$26 = 8 \cdot 3 + 2 \Rightarrow X_2 = X_{26} - 8X_3 = (0,1) - 8(1,-4) = (-8, 33)$

$3 = 1 \cdot 2 + 1 \Rightarrow X_1 = X_3 - X_2 = (1,-4) - (-8,33) = (9,-37) \Rightarrow 1 = 9 \cdot 107 - 37 \cdot 26 \Rightarrow$

$\Rightarrow 26^{-1} \equiv -37 \pmod{107} \Rightarrow 26^{-1} \equiv 70 \pmod{107}$

Scanned with CamScanner

① a) Convertiți numărul 10010 din baza 2 în baza 10.

$$10010_{(2)} = 1\cdot2^4+0\cdot2^3+0\cdot2^2+1\cdot2^1+0\cdot2^0 = 16+2=18_{(10)}$$

b) Convertiți numărul 4A din baza 16 în baza 10.

$$4A_{(16)} = 4\cdot16^1+10\cdot16^0 = 64+10 = 74_{(10)}$$

c) Convertiți numărul 125 din baza 7 în baza 4.

$$125_{(7)} = 1\cdot7^2+2\cdot7^1+5\cdot7^0 = 49+14+5 = 68_{(10)}$$

68 : 4 = 17 r 0
17 : 4 = 4 r 1
4 : 4 = 1 r 0
1 : 4 = 0 r 1

$\Rightarrow 125_{(7)} = 1010_{(4)}$

d) Scădeți numerele 27 și 13 în baza 8.

$27_{(8)} = 2\cdot8^1+7\cdot8^0 = 23_{(10)}$
$13_{(8)} = 1\cdot8^1+3\cdot8^0 = 11_{(10)}$

$23-11 = 12_{(10)}$

12 : 8 = 1 r 4
1 : 8 = 0 r 1

$\Rightarrow 12_{(10)} = 14_{(8)}$

TEMA 2

Scanned with CamScanner

1) Folosiți algoritmul Miller-Rabin pentru a verifica dacă numărul 88129 este prim sau compus.

$88129 - 1 = 2^K \cdot m \quad , m, K \in \mathbb{Z}$

$\frac{88128}{2^1} = 44064 \in \mathbb{Z}$

$\frac{88128}{2^2} = 22032 \in \mathbb{Z}$

# TEMA 3

$\frac{88128}{2^3} = 11016 \in \mathbb{Z}$

$\frac{88128}{2^4} = 5508 \in \mathbb{Z}$

$\frac{88128}{2^5} = 2754 \in \mathbb{Z}$

$\frac{88128}{2^6} = 1377 \in \mathbb{Z}$

$\frac{88128}{2^7} = 688{,}5 \notin \mathbb{Z} \Rightarrow K = 6 , m = 1377$

$1 < a < 88128$

$a^m \bmod 88129 = \pm 1$

$\underline{a = 2}$

$2^{1377} \bmod 88129 = 85656 \neq \pm 1$

$\underline{a = 3}$

$3^{1377} \bmod 88129 = 80541 \neq \pm 1$

$\underline{a = 4}$

$4^{1377} \bmod 88129 = 34828 \neq \pm 1$

$\underline{a = 5}$

$5^{1377} \bmod 88129 = 64122 \neq \pm 1$

$\underline{a = 6}$

$6^{1377} \bmod 88129 = 81776 \neq \pm 1$

Scanned with CamScanner

(25.) Găsiți factorizarea în numere prime a numărului 16903.

Nu există o astfel de factorizare deoarece 16903 este un număr prim.

TEMA 4

Scanned with CamScanner