Seminar 2 - 05 martie 2024

**Ex#1** Pentru operația

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 6 & 1 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod 26$$

găsiți regula de decriptare /cheia de decriptare.

OBS O matrice cu elementele în $\mathbb{Z}_n$ este inversabilă ddacă $\det(M)$ este inversabil în $\mathbb{Z}_n$, ie dacă $\gcd(n, \det(M)) = 1$.

Dem

Notăm $M = \begin{bmatrix} 6 & 1 \\ 5 & 1 \end{bmatrix}$.

Calculăm $\det(M) = 6 - 5 = 1$. Evident, 1 este inversabil în $\mathbb{Z}_n$, deci matricea este inversabilă.

OBS Pentru a afla inversul unei matrice 2x2 de tipul

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; \det A = ad - bc$$

ce avem de făcut este să inversăm pozițiile elementelor de pe diagonala principală, semnele elementelor de pe diagonala secundară, iar noua matrice astfel obținută să o înmulțim cu inversul determinantului

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Așadar

$$M^{-1} = \begin{bmatrix} 1 & -1 \\ -5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 25 \\ 21 & 6 \end{bmatrix} \text{ modulo } 26$$

Prin urmare, ce avem de făcut este să înmulțim la stânga cu $M^{-1}$.

□

$\boxed{\text{EX\#2}}$ Fie un alfabet $\#A = 26$ litere și blocuri de lungime 2 deci criptarea va fi de tipul $x_1 x_2 \mapsto y_1 y_2$. Identificăm $A$ cu $\mathbb{Z}_{26}$. Operația
$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod 26$$
nu este bună pentru a realiza o criptare liniară pentru că $\gcd(26, \det M) = 2$ deci $M$ nu este inversabilă. Găsiți două blocuri $x_1 x_2$ și $x_1' x_2'$ care se duc în același bloc $y_1 y_2$.

Dem Notăm $M = \begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix}$

Dacă nu puteam sigur că $M$ nu este inversabilă, verificăm
$$\det M = 12 - 10 = 2$$
Observăm că ~~det~~ $\gcd(26, 2) \neq 1$, deci $M$ e adevărat nu este inversabilă

Exemplu de două blocuri care se duc în același loc sunt $\begin{bmatrix} x \\ 0 \end{bmatrix}$ și $\begin{bmatrix} x \\ 13 \end{bmatrix}$. $\forall x$.

Verificăm $\begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} 6x \\ 5x \end{bmatrix}$ și
$$\begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} x \\ 13 \end{bmatrix} = \begin{bmatrix} 6x + 26 \\ 5x + 26 \end{bmatrix} = \begin{bmatrix} 6x \\ 5x \end{bmatrix} \bmod 26.$$
$\square$

## Lema Chineză a Resturilor

Fie $p \geq 2$, $n_i$, $i = \overline{1,p}$ întregi pozitivi cu $\gcd(n_i, n_j) = 1$, $\forall i,j = \overline{1,p}$, $i \neq j$. Atunci oricare ar fi $a_1, \dots, a_p$ numere întregi, există un întreg $x$ soluție a următorului sistem
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_p \pmod{n_p} \end{cases}$$
În plus, toate soluțiile $x$ ale sistemului sunt congruente mod $N = n_1 \cdots n_p$

$\boxed{\text{EX\#3}}$ Mihai vrea să își țină vârsta secretă. Prietenii lui știu că
- Acum un an, vârsta lui Mihai era divizibilă cu 3
- În doi ani, vârsta lui va fi multiplu de 5
- În patru ani, va fi multiplu de 7

Câți ani are Mihai?

Dem: Notăm $x$ = vârsta lui Mihai

Rescriem condițiile: $\begin{cases} x-1 \equiv 0 \mod 3 \\ x+2 = 0 \mod 5 \\ x+4 = 0 \mod 7 \end{cases}$

Sau, altfel, avem $\begin{cases} x = 1 \mod 3 \\ x = -2 \mod 5 \\ x = -4 \mod 7 \end{cases} \Leftrightarrow \begin{cases} x = 1 \mod 3 \\ x = 3 \mod 5 \\ x = 3 \mod 7 \end{cases}$

Observăm că 3, 5 și 7 sunt prime între ele, deci putem aplica LCR și avem

OBS Nu mai facem demonstrația LCR, dar de acolo reiese forma lui $x$. Mai exact: → Definim $b_i = N/n_i$ (produsul celorlalți $n_j$, $j \neq i$)

→ Definim $b_i' = b_i^{-1}$ (mod $n_i$)

→ Găsim $x = \sum_{i=1,n} a_i b_i b_i^{-1}$ (mod $N$) soluție unică.

$x = (1 \cdot 5 \cdot 7 \cdot ((5 \cdot 7)^{-1} \bmod 3) +$
$3 \cdot 3 \cdot 7 \cdot ((3 \cdot 7)^{-1} \bmod 5) +$
$3 \cdot 3 \cdot 5 \cdot ((3 \cdot 5)^{-1} \bmod 7)) \bmod (3 \cdot 5 \cdot 7) \Leftrightarrow$

$x = (35 \cdot (35^{-1} \bmod 3) + 63 \cdot (21^{-1} \bmod 5) + 45 \cdot (15^{-1} \bmod 7)) \bmod 105$

Luăm separat
$35^{-1} \bmod 3 = 2^{-1} \bmod 3 = 2$
$21^{-1} \bmod 5 = 1^{-1} \bmod 5 = 1$
$15^{-1} \bmod 7 = 1^{-1} \bmod 7 = 1$

Revenim și avem $x = (35 \cdot 2 + 63 + 45) \bmod 105$
$x = (70 + 108) \bmod 105$
$x = (70 + 3) \bmod 105$
$x = 73 \bmod 105.$ □

$\boxed{\text{Ex \#4}}$ Aflați $x$ astfel încât $\begin{cases} x = 2 \mod 5 \\ x = 3 \mod 7 \\ x = 10 \mod 11 \end{cases}$

Dem $N = 5 \cdot 7 \cdot 11 = 385$

$x = (2 \cdot 7 \cdot 11 \cdot (77^{-1} \bmod 5) + 3 \cdot 5 \cdot 11 \cdot (55^{-1} \bmod 7) + 10 \cdot 5 \cdot 7 \cdot (35^{-1} \bmod 11)) \bmod 385$

$77^{-1} \bmod 5 = 2^{-1} \bmod 5 = 3 \bmod 5$
$55^{-1} \bmod 7 = 6^{-1} \bmod 7 = 6 \bmod 7$
$35^{-1} \bmod 11 = 2^{-1} \bmod 11 = 6 \bmod 11$

$x = (154 \cdot 3 + 165 \cdot 6 + 350 \cdot 6) \bmod 385$
$x = 3552 \bmod 385 = (385 \cdot 9 + 87) = 87 \bmod 385.$ □

## Algoritmul de exponențiere rapidă

Calculăm $b^r$ mod n pentru $b, r, n \in \mathbb{N}$. Primul lucru pe care îl facem este să descompunem r în baza doi

$$r = \sum_{j=\overline{0,k}} a_j 2^j$$

Apoi vrem să calculăm $c = b^r \pmod n$. Facem:

PAS INIȚIAL: Fie $b_0 = b$ și $c = \begin{cases} 1, & \text{dacă } a_0 = 0 \\ 0, & \text{dacă } a_0 = 1 \end{cases}$

Pentru $j = \overline{1,k}$ facem:

PAS j: Calculăm restul pozitiv $b_j$ pentru $b_{j-1}^2$ mod n. Dacă $a_j = 1$, atunci înlocuim c cu $cb_j$ și reducem rezultatul mod n. Dacă $a_j = 0$, lăsăm c nemodificat. Așadar, la pasul j, avem

$$c_j = b^{r_j} \pmod n$$

unde $c_j$ este restul pozitiv pentru $b_j$ mod n și

$$r_j = \sum_{i=\overline{0,j}} a_i 2^i$$

Așadar, la pasul k am calculat $c = b^r \pmod n$.

$\boxed{\text{Ex \#5}}$ Folosind algoritmul de exponențiere rapidă, calculați $5^{117}$ mod 19.

Dem

PAS 1 Scriem 117 în baza 2.

$$\begin{array}{l}
117 : 2 = 58,\ \text{rest } \boxed{1} \\
58 : 2 = 29,\ \text{rest } \boxed{0} \\
29 : 2 = 14,\ \text{rest } \boxed{1} \\
14 : 2 = 7,\ \text{rest } \boxed{0} \\
7 : 2 = 3,\ \text{rest } \boxed{1} \\
3 : 2 = 1,\ \text{rest } \boxed{1} \\
\boxed{1}
\end{array}$$

Deci $117_{(10)} = 1110101_{(2)}$, de unde, ca sumă de puteri de 2, avem

$$117 = 2^0 + 2^2 + 2^4 + 2^5 + 2^6$$
$$117 = 1 + 4 + 16 + 32 + 64$$

Așadar $5^{117} \bmod 19 = 5^{(1+4+16+32+64)} \bmod 19$

$$5^{117} \bmod 19 = 5 \cdot 5^4 \cdot 5^{16} \cdot 5^{32} \cdot 5^{64} \bmod 19$$

PAS 2: Calculăm

- $5^1 \bmod 19 = 5$
- $5^4 \bmod 19 = 5^2 \cdot 5^2 \bmod 19$

$5^2 \bmod 19 = 25 \bmod 19 = 6$

$5^4 \bmod 19 = 6 \cdot 6 \bmod 19 = 36 \bmod 19 = 17$

- $5^{16} \bmod 19 = 5^8 \cdot 5^8 \bmod 19$

$5^8 \bmod 19 = 5^4 \cdot 5^4 \bmod 19 = 17 \cdot 17 \bmod 19 = 289 \bmod 19 = 4$

$5^{16} \bmod 19 = 4 \cdot 4 \bmod 19 = 16$

- $5^{32} \bmod 19 = 5^{16} \cdot 5^{16} \bmod 19 = 16 \cdot 16 \bmod 19 = 256 \bmod 19 = 9$
- $5^{64} \bmod 19 = 5^{32} \cdot 5^{32} \bmod 19 = 9 \cdot 9 \bmod 19 = 81 \bmod 19 = 5$

PAS 3: Facem calculul final

$$\begin{aligned}
5^{117} \bmod 19 &= 5 \cdot 5^4 \cdot 5^{16} \cdot 5^{32} \cdot 5^{64} \bmod 19 = \\
&= 5 \cdot 17 \cdot 16 \cdot 9 \cdot 5 \bmod 19 = \\
&= 17 \cdot 80 \cdot 45 \bmod 19 = \\
&= 17 \cdot 4 \cdot 7 \bmod 19 = \\
&= 68 \cdot 7 \bmod 19 = \\
&= 11 \cdot 7 \bmod 19 = \\
&= 77 \bmod 19 = \\
&= 1 \bmod 19.
\end{aligned}$$

$\square$

$\boxed{\text{EX \#6}}$ Calculați $7^{256} \bmod 13$.

Dem

Deci $256 = 2^8$.

| | |
|---|---|
| 256 | 2 |
| 128 | 2 |
| 64 | $2^3$ |
| 8 | $2^3$ |
| 1 | |

În acest caz, calculăm:

1) $7^2 = 49 \bmod 13 = 10$
2) $7^4 = 7^2 \cdot 7^2 = 10 \cdot 10 = 100 \bmod 13 = 9$
3) $7^8 = 7^4 \cdot 7^4 = 9 \cdot 9 = 81 = 3 \bmod 13$
4) $7^{16} = 7^8 \cdot 7^8 = 3 \cdot 3 = 9 \bmod 13$
5) $7^{32} = 7^{16} \cdot 7^{16} = 9 \cdot 9 = 3 \bmod 13$
6) $7^{64} = 7^{32} \cdot 7^{32} = 3 \cdot 3 = 9 \bmod 13$
7) $7^{128} = 7^{64} \cdot 7^{64} = 9 \cdot 9 = 3 \bmod 13$
8) $7^{256} = 7^{128} \cdot 7^{128} = 3 \cdot 3 = 9 \bmod 13$.

Deci $7^{256} \bmod 13 = 9$

$\square$

Ex#7

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A | 0 | I | 8 | Q | 16 | Y | 24 |
| B | 1 | J | 9 | R | 17 | Z | 25 |
| C | 2 | K | 10 | S | 18 | Ă | 26 |
| D | 3 | L | 11 | T | 19 | Î | 27 |
| E | 4 | M | 12 | U | 20 | Â | 28 |
| F | 5 | N | 13 | V | 21 | Ș | 29 |
| G | 6 | O | 14 | W | 22 | Ț | 30 |
| H | 7 | P | 15 | X | 23 | □ | 31 |

Să considerăm un alfabet $\mathcal{A}$ cu 32 de caractere, începând cu A, B, –, Z și continuând cu Ă, Î, Â, Ș, Ț, □. Fie $k \in \mathcal{A}^5$ o cheie pentru OTP modulo 32 a.î.

$$E_k(\text{ELENA}) = \text{MARIA}$$

a) Găsiți $E_k(\text{MARIA})$

b) Calculați $E_k(k)$

c) Calculați cheia $k$.

Codul lui Vernam (OTP)

$\mathcal{A} = \{0,1\}$, $\#K = \#M = \#C = 2^n$ și $c = m \oplus k$

unde $\oplus$ este adunarea peste $\mathbb{F}_2$ care se face literă cu literă.

Dem

Știm că $c = m \oplus k$. Deci $k = c - m$.

Prima dată calculăm cheia $k$.

$k = \text{MARIA} - \text{ELENA} = (12,0,17,8,0) - (4,11,4,13,0) \bmod 32$

$= (8,-11,13,-5,0) \bmod 32 =$

$= (8,21,13,27,0) \bmod 32$

Adică $k = $ IVNÎA

Calculăm

$E_k(\text{MARIA}) = (12,0,17,8,0) + (8,21,13,27,0) =$

$= (20,21,30,35,0) \bmod 32$

$= (20,21,30,3,0) \bmod 32$

Deci $E_k(\text{MARIA}) = $ UVȚDA

Acum $E_k(k) = k \oplus k = (16,42,26,54,0) \bmod 32 =$

$= (16,10,26,22,0) \bmod 32$

și deci $E_k(k) = $ QKĂWA

□

**Ex #8** Considerăm un alfabet $A$ cu 32 de caractere ca în problema anterioară. Alfabetul este codat folosind șiruri binare 00000, 00001, —, 11111 (adică vom folosi reprezentarea binară de lungime 5 a asocierii anterioare). Fie $k \in \{0,1\}^{25}$ o cheie pentru OTP modulo 2 ai.

$$E_k(ELENA) = MARIA$$

a) Găsiți $E_k(MARIA)$

b) Calculați $E_k(k)$

c) Calculați $k$.

Dem: $E_k(ELENA) = MARIA \Leftrightarrow ELENA \oplus k = MARIA$

Pentru că facem calculele modulo 2, putem aduna $k$ la egalitatea anterioară și avem

$$ELENA \oplus k \oplus k = MARIA \oplus k \Leftrightarrow$$
$$ELENA = MARIA \oplus k$$

Deci $E_k(MARIA) = ELENA$.

Acum $E_k(k) = k \oplus k = 2k = 0 = AAAAA$

Calculăm $k$.

Știm că $c = m \oplus k \Leftrightarrow k = c - m$, dar, pentru că lucrăm mod 2 și $-1 = 1$ avem $k = c \oplus m$. Deci $k = MARIA \oplus ELENA$.

$$M = 12 = 2^3 + 2^2 = 0\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0 = 01100_{(2)}$$

$$R = 17 = 2^4 + 2^0 = 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = 10001_{(2)}$$

$$I = 8 = 2^3 = 01000_{(2)}$$
$$E = 4 = 2^2 = 00100_{(2)}$$
$$L = 11 = 2^3 + 2^1 + 2^0 = 01011_{(2)}$$
$$N = 13 = 2^3 + 2^2 + 2^0 = 01101_{(2)}$$

| | | | | | |
|---|---|---|---|---|---|
| $k =$ | 01100 | 00000 | 10001 | 01000 | 00000 $\oplus$ |
| | 00100 | 01011 | 00100 | 01101 | 00000 |
| | 01000 | 01011 | 10101 | 00101 | 00000 |
| | I | L | V | F | A |

$10101_{(2)} = 2^4 + 2^2 + 2^0 = 16 + 4 + 1 = 21_{(10)} = V$

$00101_{(2)} = 2^2 + 2^0 = 4 + 1 = 5_{(10)} = F$

Prin urmare $k = ILVFA$

$\square$

$\boxed{Ex\#9}$ Folosind algoritmul de exponențiere rapidă, calculați $9^{-1} \bmod 26$.

Teorema lui Euler

Dacă $m \geq 1$ și $gcd(a, m) = 1$, atunci $a^{\varphi(m)} \equiv 1 \pmod m$

Funcția lui Euler

Notăm cu $\varphi(n)$ numărul numerelor naturale prime cu $n$ care nu-l depășesc pe $n$

$$\varphi(n) = \#\{m \mid m \leq n, gcd(m, n) = 1\}$$

Teoremă

Dacă $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ atunci

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right) \Leftrightarrow$$

$$\Leftrightarrow \varphi(n) = n \prod_{i=1,k} \left(1 - \frac{1}{p_i}\right)$$

SAU $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

Formulare echivalentă

$$\varphi(n) = p_1^{k_1 - 1}(p_1 - 1)\, p_2^{k_2 - 1}(p_2 - 1) \ldots p_r^{k_r - 1}(p_r - 1)$$

Dem Din Teorema lui Euler avem că, în general,

$$a^{\varphi(n)} = 1 \pmod n \Leftrightarrow$$

$$a \cdot a^{\varphi(n) - 1} = 1 \pmod n \Leftrightarrow$$

$$a^{-1} = a^{\varphi(n) - 1} \pmod n$$

În cazul nostru $9^{-1} = 9^{\varphi(26)-1} \pmod{26}$.

Calculăm $\varphi(26) = \varphi(2 \cdot 13) = \varphi(2)\varphi(13) = (2-1)(13-1)$

$\varphi(26) = 12$

Deci $9^{-1} = 9^{12-1} = 9^{11} \bmod 26$. Acum putem aplica algoritmul de exponențiere rapidă:

$$11 = 2^3 + 2^1 + 2^0$$

$9^{11} = 9^8 \cdot 9^2 \cdot 9 \bmod 26$

- $9^2 = 81 \bmod 26 = 3 \bmod 26$
- $9^8 = 9^4 \cdot 9^4 \bmod 26$

$9^4 = 9^2 \cdot 9^2 = 3 \cdot 3 = 9 \bmod 26$

$9^8 = 9 \cdot 9 \bmod 26 = 81 \bmod 26 = 3 \bmod 26$

Deci $9^{11} = 3 \cdot 3 \cdot 9 \bmod 26 =$

$= 9 \cdot 9 \bmod 26 =$

$= 81 \bmod 26 =$

$= 3 \bmod 26$

Prin urmare $9^{-1} = 3 \bmod 26$.

$\square$

<u>Algoritmul lui Euclid</u>

Fie $a, b \in \mathbb{Z}$ cu $a \geq b > 0$. Notăm $a = r_{-1}$, $b = r_0$. Aplicând, în mod repetat, Teorema împărțirii cu rest, obținem

$$r_{i-1} = r_i q_{i+1} + r_{i+1}$$

cu $0 < r_{i+1} < r_i$, unde $n$ este ultimul număr neunul ai $r_{i+1} = 0$. În acest caz $\gcd(a,b) = r_n$.

<u>Algoritmul extins al lui Euclid</u>

Fie $a, b \in \mathbb{N}$ și $q_i, i = \overline{1, n+1}$ coeficienții obținuți prin aplicarea algoritmului lui Euclid pentru aflarea lui $d = \gcd(a,b)$, unde $n \in \mathbb{Z}_+$ ai $r_{n+1} = 0$. Dacă

$$t_{-1} = 1, \; t_0 = 0 \text{ și } t_i = t_{i-2} - q_{n-i+2} t_{i-1}$$

pentru $i = \overline{1, n+1}$, atunci $d = t_{n+1} a + t_n b$.

Ex#10 Aflați gcd pentru fiecare din următoarele perechi folosind Alg lui Euclid și scrieți $d = \gcd(a,b)$ ca o combinație liniară de a și b:

a) $a=22, b=55$
b) $a=15, b=113$
c) $a=1224, b=567$
d) $a=687, b=24$

Dem

a) $a=22, b=55$

$55 = 22\cdot 2 + 11$
$22 = 11\cdot 2 + 0$
$\Rightarrow \gcd(22,55)=11$

$11 = 55 - 22\cdot 2 \Leftrightarrow 11 = 1\cdot 55 + (-2)\cdot 22$ ok

b) $a=15, b=113$

$113 = 15\cdot 7 + 8$
$15 = 8\cdot 1 + 7$
$8 = 7\cdot 1 + 1$
$7 = 1\cdot 7 + 0$
$\Rightarrow \gcd(15,113)=1.$

$1 = 8 - 7\cdot 1 = 8 - (15 - 8\cdot 1) = 2\cdot 8 - 15 =$
$= 2\cdot(113 - 15\cdot 7) - 15 = 2\cdot 113 - 15\cdot 15$

$\Leftrightarrow 1 = 2\cdot 113 + (-15)\cdot 15$

Care este inversul lui 113 mod 15?

Facem $2\cdot 113 + (-15)\cdot 15 = 1 \pmod{15}$
$2\cdot 113 = 1 \pmod{15}$

Deci $113^{-1} = 2 \pmod{15}$

c) $a=1224, b=567$

$1224 = 567\cdot 2 + 90$
$567 = 90\cdot 6 + 27$
$90 = 27\cdot 3 + 9$
$27 = 9\cdot 3 + 0$
$\Rightarrow \gcd(1224,567)=9.$

$$9 = 90 - 27\cdot 3 =$$
$$= 90 - (567 - 90\cdot 6)\cdot 3 =$$
$$= 90\cdot 19 - 567\cdot 3 =$$
$$= (1224 - 567\cdot 2)\cdot 19 - 567\cdot 3 =$$
$$= 1224\cdot 19 - 567\cdot 41$$

Deci $9 = 1224\cdot 19 + 567\cdot(-41)$.

d) $a = 687$, $b = 24$

$$687 = 24\cdot 28 + 15$$
$$24 = 15\cdot 1 + 9$$
$$15 = 9\cdot 1 + 6 \quad \Rightarrow \gcd(687, 24) = 3$$
$$9 = 6\cdot 1 + 3$$
$$6 = 3\cdot 2 + 0$$

Vrem $s, t$ a.î. $3 = 687s + 24t$.

$$3 = 9 - 6 =$$
$$= 9 - (15 - 9) = 9\cdot 2 - 15 =$$
$$= (24 - 15)\cdot 2 - 15 = 24\cdot 2 - 15\cdot 3 =$$
$$= 24\cdot 2 - (687 - 24\cdot 28)\cdot 3 =$$
$$= 24\cdot 86 - 687\cdot 3 \Leftrightarrow$$
$$\Leftrightarrow 3 = 24\cdot 86 + (-3)\cdot 687$$

Deci $s = -3$ şi $t = 86$. $\square$

$\boxed{\text{EX\#11}}$ Similar pentru: a) $a = 254$, $b = 32$

b) $a = 74$, $b = 383$

c) $a = 7544$, $b = 115$

Care este inversul lui 74 modulo 383?