

## Seminar 2

Ex#1 Pentru operația

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

găsiți regula de decifrare / cheia de decriptare.

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

Dacă

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

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  $2 \times 2$  de tipul

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

ce avem de făcut este să învețăm pozitile elementelor de pe diagonala principală, semnele elementelor de pe diagonala secundară, iar noua matrice astfel obținută să o înmulțim cu inversul determinantei

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

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  $M^{-1}$ .

□

**Ex#2** Fie un alfabet  $\#A=26$  litere și blocuri de lungime 2 deci criptarea va fi de tipul  $x_1 x_2 \rightarrow y_1 y_2$ . Identificăm at că  $\mathbb{Z}_{26}$ : Operația  $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \text{ mod } 26$

Acei este binește deținută realiză o criptare liniară pentru că  $\text{gcd}(26, \det M) = 2$  deci  $M$  nu este inversabilă. Dacă două blocuri  $x_1 x_2$  și  $x'_1 x'_2$  care se duc în același loc  $y_1 y_2$ .

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

Dacă nu putem riguri că  $M$  nu este inversabilă, verificăm  $\det M = 12 - 10 = 2$

Observăm că  ~~$\det M = 26, 2$~~   $\det M = 26, 2 \neq 1$ , deci  $M$  nu aduce că  $M$  este inversabilă.

Exemplu de doară blocuri care se duc în același loc sunt,  $\begin{bmatrix} * \\ 0 \end{bmatrix} \text{ și } \begin{bmatrix} * \\ 13 \end{bmatrix}$ . Ar e?

$$\text{Verificăm } \begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} * \\ 0 \end{bmatrix} = \begin{bmatrix} 6* \\ 5* \end{bmatrix} \text{ și }$$

$$\begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} * \\ 13 \end{bmatrix} = \begin{bmatrix} 6* + 26 \\ 5* + 26 \end{bmatrix} = \begin{bmatrix} 6* \\ 5* \end{bmatrix} \text{ mod } 26.$$

□

### Lemma Chineză a Resturilor

Fie  $p \geq 2$ ,  $a_i, i = \overline{1, p}$  întregi pozitivi cu  $\text{gcd}(a_i, n_j) = 1$ ,  $\forall i, j = \overline{1, p}, i \neq j$

Atunci oricare ar fi  $a_1, \dots, a_p$  numere întregi, există un singur și unică soluție a următoarei sisteme

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_p \pmod{n_p} \end{cases}$$

În plus, toate soluțiile ale sistemului sunt congruente mod  $N = n_1 \cdots n_p$

**Ex#3** Nihai avea să fie învățătore de la 1000. Piereții lui știau că

- Acea zilnic, mărula lui Nihai era divizibilă cu 3
- În doi ani, mărula lui va fi multiplă de 5
- În patru ani, va fi multiplă de 7

Câtă ană avea Nihai?

Dacă  $x \equiv a \pmod{m}$  și  $x \equiv b \pmod{n}$

rezolvarea condiției:

$$\begin{cases} x - a \equiv 0 \pmod{m} \\ x - b \equiv 0 \pmod{n} \end{cases}$$

sau, adică, avem

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \Leftrightarrow \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

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

OBS Nă mai facem demonstrația LCR, doar să vedem reiese forma lui  $x$ . Mai exact:  $\rightarrow$  Definim  $b_i = N/n_i$  (produsul celorlalți  $n_j$ ,  $j \neq i$ )

$\rightarrow$  Definim  $b_i^{-1} = b_i^{-1} \pmod{n_i}$

$\rightarrow$  Găsim  $x = \sum_{i=1, n} a_i b_i b_i^{-1} \pmod{N}$  soluție unică.

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

$$3 \cdot 3 \cdot 7 \cdot ((3 \cdot 7)^{-1} \pmod{5}) +$$

$$3 \cdot 3 \cdot 5 \cdot ((3 \cdot 5)^{-1} \pmod{7})) \pmod{(3 \cdot 5 \cdot 7)} \iff$$

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

Avem separat

$$35^{-1} \pmod{3} = 2^{-1} \pmod{3} = 2$$

$$21^{-1} \pmod{5} = 1^{-1} \pmod{5} = 1$$

$$15^{-1} \pmod{7} = 1^{-1} \pmod{7} = 1$$

$$\text{Revenind în avem } x = (35 \cdot 2 + 63 + 45) \pmod{105}$$

$$x = (70 + 108) \pmod{105}$$

$$x = (70 + 3) \pmod{105}$$

$$x = 73 \pmod{105}.$$

□

**Ex #4** Afloți  $x$  astfel încât

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases}$$

$$\text{Dacă } N = 5 \cdot 7 \cdot 11 = 385$$

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

$$77^{-1} \pmod{5} = 2^{-1} \pmod{5} = 3 \pmod{5}$$

$$55^{-1} \pmod{7} = 6^{-1} \pmod{7} = 6 \pmod{7}$$

$$35^{-1} \pmod{11} = 2^{-1} \pmod{11} = 6 \pmod{11}$$

$$x = (154 \cdot 3 + 165 \cdot 6 + 350 \cdot 6) \pmod{385}$$

$$x = 3552 \pmod{385} = (385 \cdot 9 + 87) \pmod{385}. \quad \square$$

## Algoritmo de exponente rápido

- Calcularea  $b^x$  mod  $m$  peste b,  $x_1, m \in \mathbb{N}$ . Prin urmare pe calea il face cu este să decompunem  $x$  în baza elor.

$$g_k = \sum_{j=0,1} a_j 2^j$$

Anvendes også calculonne  $c \equiv b^x \pmod{n}$ . Facit:

PAS INICIAL: Fix  $b_0 = b$  in  $C = \begin{cases} 1, & \text{dado } a_0 = 0 \\ 0, & \text{dado } a_0 = 1 \end{cases}$

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

PAS j: Calculăm restul pozitiv bj pentru  $bj-1 \text{ mod } n$ . Dacă  $a_j = 1$ , atunci înlocuim c cu  $c b_j$  și reducem rezultatul mod n. Dacă  $a_j = 0$ , lăsăm c ne modificat. Așadar, la pasul j, avem

$$c_j = b^{q_j} \pmod{u}$$

Znaleźć rekt. wstępu pozitiv neutru bij' wadu i rą

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

Az ador, la pasul k, am calculat  $c = b^k \pmod{n}$ .

EX #5 Folosind algoritmul de exponentiere rapidă, calculați  $5^{17} \bmod 19$ .

Dew  
me PAS 1 Series 117 im box 2.

$$\begin{array}{r}
 117 \overline{)58} \\
 10 \overline{)17} \\
 16 \overline{)1} \\
 = \boxed{1}
 \end{array}
 \quad
 \begin{array}{r}
 2 \\
 \overline{)58} \\
 29 \\
 \overline{)29} \\
 2 \\
 \overline{)14} \\
 14 \\
 \overline{)0} \\
 = \boxed{0}
 \end{array}
 \quad
 \begin{array}{r}
 2 \\
 \overline{)14} \\
 7 \\
 \overline{)7} \\
 6 \\
 \overline{)1} \\
 = \boxed{1}
 \end{array}
 \quad
 \begin{array}{r}
 2 \\
 \overline{)3} \\
 2 \\
 \overline{)1} \\
 = \boxed{1}
 \end{array}$$

Dacă  $M_{(10)} = 1110101_{(2)}$ , de unde, ca semnul de paritate al

avenue

$$\mu_7 = 2^0 + 2^2 + 2^4 + 2^5 + 2^6$$

$$\text{从} 7 = 1 + 4 + 16 + 32 + 64$$

$$\text{Así como } 5^{17} \bmod 19 \equiv 5^{(1+4+16+32+64)} \bmod 19$$

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

## PAS 2 : Calculus

$$5^1 \bmod 19 = 5$$

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

EEx #8 Considerăm un alfabet A cu 32 de caractere ca în problema  
+ + + + + și re biuore 00000, 00001, -

$$5^2 \text{ mod } 19 = 25 \text{ mod } 19 = 6$$

$$5^4 \text{ mod } 19 = 6 \cdot 6 \text{ mod } 19 = 36 \text{ mod } 19 = 17$$

$$\bullet 5^{16} \text{ mod } 19 = 5^8 \cdot 5^8 \text{ mod } 19$$

$$5^8 \text{ mod } 19 = 5^4 \cdot 5^4 \text{ mod } 19 = 17 \cdot 17 \text{ mod } 19 = 289 \text{ mod } 19 = 4$$

$$5^{16} \text{ mod } 19 = 4 \cdot 4 \text{ mod } 19 = 16$$

$$\bullet 5^{32} \text{ mod } 19 = 5^{16} \cdot 5^{16} \text{ mod } 19 = 16 \cdot 16 \text{ mod } 19 = 256 \text{ mod } 19 = 9$$

$$\bullet 5^{64} \text{ mod } 19 = 5^{32} \cdot 5^{32} \text{ mod } 19 = 9 \cdot 9 \text{ mod } 19 = 81 \text{ mod } 19 = 5$$

Pas 3: Faceem calculul final

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

$$= 5 \cdot 17 \cdot 16 \cdot 9 \cdot 5 \text{ mod } 19 =$$

$$= 17 \cdot 80 \cdot 45 \text{ mod } 19 =$$

$$= 17 \cdot 4 \cdot 4 \text{ mod } 19 =$$

$$= 68 \cdot 7 \text{ mod } 19 =$$

$$= 11 \cdot 7 \text{ mod } 19 =$$

$$= 77 \text{ mod } 19 =$$

$$= 1 \text{ mod } 19,$$

□

EEx #6 Calculați  $7^{256} \text{ mod } 13$ .

Din

$$\text{Deci } 256 = 2^8.$$

În acest caz, calculăm:

256	2
128	2
64	23
8	23
1	

$$1) 7^2 = 49 \text{ mod } 13 = 10$$

$$2) 7^4 = 7^2 \cdot 7^2 = 10 \cdot 10 = 100 \text{ mod } 13 = 9$$

$$3) 7^8 = 7^4 \cdot 7^4 = 9 \cdot 9 = 81 = 3 \text{ mod } 13$$

$$4) 7^{16} = 7^8 \cdot 7^8 = 3 \cdot 3 = 9 \text{ mod } 13$$

$$5) 7^{32} = 7^{16} \cdot 7^{16} = 9 \cdot 9 = 3 \text{ mod } 13$$

$$6) 7^{64} = 7^{32} \cdot 7^{32} = 3 \cdot 3 = 9 \text{ mod } 13$$

$$7) 7^{128} = 7^{64} \cdot 7^{64} = 9 \cdot 9 = 3 \text{ mod } 13$$

$$8) 7^{256} = 7^{128} \cdot 7^{128} = 3 \cdot 3 = 9 \text{ mod } 13.$$

$$\text{Deci } 7^{256} \text{ mod } 13 = 9$$

□

Ex#

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

Se consideră un alfabet cu 32 de caractere, începând cu A, B, ..., Z și continuând cu Ă, Ğ, Ą, Ĥ, Į, Ĳ. Fie  $k \in \mathbb{Z}^5$  o cheie pentru OTP modulo 32 astfel

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

- Goști  $E_k(\text{MARIA})$
- Calculezi  $E_k(k)$
- Calculezi cheia  $k$ .

### Codul lui Vernam (OTP)

$$\mathcal{A} = \{0, 1\}, \#K = \#M = \#C = 2^{32} \text{ și } C = m \oplus k$$

unde  $\oplus$  este adunarea pe trunchiuri care se face literă cu literă.

Deci

$$\text{Stiu că } c = m \oplus k. \text{ Deci } k = c - m.$$

Pentru dată calculăm cheia  $k$ .

$$\begin{aligned} k &= \text{MARIA} - \text{ELENA} = (12, 0, 17, 8, 0) - (4, 11, 4, 13, 0) \bmod 32 \\ &= (8, -11, 13, -5, 0) \bmod 32 = \\ &= (8, 21, 13, 27, 0) \bmod 32 \end{aligned}$$

Adică  $k = \text{IVNTA}$

Calculăm

$$\begin{aligned} E_k(\text{MARIA}) &= (12, 0, 17, 8, 0) + (8, 21, 13, 27, 0) = \\ &= (20, 21, 30, 35, 0) \bmod 32 \\ &= (20, 21, 30, 3, 0) \bmod 32 \end{aligned}$$

Deci  $E_k(\text{MARIA}) = \text{UVJDA}$

$$\text{Acum } E_k(k) = k \oplus k = (16, 42, 26, 54, 0) \bmod 32 = \\ = (16, 10, 26, 22, 0) \bmod 32$$

și deci  $E_k(k) = \text{QKAWA}$

□

**Ex #8** Considerăm un alfabet A cu 32 de caractere ca în problema anterioră. Alfabetul este codat folosind siruri binare 00000, 00001, ... → 11111 (adică oron folosi reprezentarea binară de lungime 5 a caracterei anterioare). Tie  $E_K(ELENA) = MARIA$

$E_K(ELENA) = MARIA$

a) Găsiți  $E_K(MARIA)$

b) Calculați  $E_K(k)$

c) Calculați  $k$ .

Dacă  $E_K(ELENA) = MARIA \Leftrightarrow ELENA \oplus k = MARIA$

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

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

Dacă  $E_K(MARIA) = ELENA$ .

Acum  $E_K(k) = k \oplus k = 2k = 0 = AAAAAA$

Calculem k.

Stim că  $e = m \oplus k \Leftrightarrow k = e - m$ , deci că lucram mod 2

și  $-1 = 1$  avem  $k = c \oplus m$ . Deci  $k = MARIA \oplus ELENA$ .

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

$$R = 14 = 2^4 + 2^0 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = \\ = 10001_{(2)}$$

$$I = 8 = 2^3 = 01000_{(2)}$$

$$E = 4 = 2^2 = 00100_{(2)}$$

$$L = 11 = 2^3 + 2^1 + 2^0 = 01011_{(2)}$$

$$N = 13 = 2^3 + 2^2 + 2^0 = 01101_{(2)}$$

$$\begin{array}{c} k = 01100 | 00000 | 10001 | 01000 | 00000 \oplus \\ 00100 | 01011 | 00100 | 01101 | 00000 \\ \hline 01000 | 01011 | 10101 | 00101 | 00000 \\ I \quad L \quad V \quad F \quad A \end{array}$$

Ex#8

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

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

Prin urmare  $R = ILVFA$   $\square$

Ex#9 Folosind algoritmul de exponentiere rapidă, calculați  $g^{-1} \pmod{26}$ .

Teorema lui Euler

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

Funcția lui Euler

Notăm cu  $\varphi(n)$  numărul numerelor naturale prime cu  $n$  care sunt deosebite pe  $n$ .

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

Teorema

Dacă  $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$  atunci

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

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

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

Formulare echivalentă

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

Deoarece Teorema lui Euler are cōști, în general,

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

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

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

Ex#10 Afălați gcd pentru fiecăreia din următoarele perechi folosind Algoritm lui Euclidian 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)  $a = 687, b = 24$

Dacă  
avem

a)  $a = 22, b = 55$

$$55 = 22 \cdot 2 + 11$$

$$22 = 11 \cdot 2 + 0$$

$$\Rightarrow \gcd(22, 55) = 11$$

$$11 = 55 - 22 \cdot 2 \Leftrightarrow 11 = 1 \cdot 55 + (-2) \cdot 22 \quad \text{OK}$$

b)  $a = 15, b = 113$

$$113 = 15 \cdot 7 + 8$$

$$15 = 8 \cdot 1 + 7$$

$$8 = 7 \cdot 1 + 1$$

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

$$\Rightarrow \gcd(15, 113) = 1.$$

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

Care este inversul lui  $113 \pmod{15}$ ?

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

$$2 \cdot 113 \equiv 1 \pmod{15}$$

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

c)  $a = 1224, b = 567$

$$1224 = 567 \cdot 2 + 90$$

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

$$90 = 27 \cdot 3 + 9$$

$$27 = 9 \cdot 3 + 0$$

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

Calculăm  $\varphi(26) = \varphi(2 \cdot 13) = \varphi(2)\varphi(13) = (2-1)(13-1)$   
 $\varphi(26) = 12$

Deci  $g^{-1} = g^{12-1} = g^{11} \pmod{26}$ . Atunci putem aplica algoritmul de exponentiere rapidă:

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

$$g^{11} = g^8 \cdot g^2 \cdot g \pmod{26}$$

$$\cdot g^2 = 81 \pmod{26} = 3 \pmod{26}$$

$$\cdot g^8 = g^4 \cdot g^4 \pmod{26}$$

$$g^4 = g^2 \cdot g^2 = 3 \cdot 3 = 9 \pmod{26}$$

$$g^8 = g \cdot g \pmod{26} = 81 \pmod{26} = 3 \pmod{26}$$

$$\text{Deci } g^{11} = 3 \cdot 3 \cdot 9 \pmod{26} =$$

$$= g \cdot g \pmod{26} =$$

$$= 81 \pmod{26} =$$

$$= 3 \pmod{26}$$

Prin urmare  $g^{-1} = 3 \pmod{26}$ .

□

### Algoritmul lui Euclid

Fie  $a, b \in \mathbb{N}$  cu  $a \geq b > 0$ . Notăm  $a = q_{-1}r_0$ ,  $b = q_0r_1$ . Aplicând, în mod repetat, teorema împărțirii cu rest, obținem

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

cu  $0 < r_{i+1} < r_i$ , unde avem este ultimul număr nenul al  $r_{i+1} = 0$ .  
În acest caz  $\gcd(a, b) = q_m$ .

### Algoritmul extins al lui Euclid

Fie  $a, b \in \mathbb{N}$  și  $g_i, i = \overline{1, n+1}$  coeficienți obținuți prin aplicarea algoritmului lui Euclid pentru aflarea lui  $d = \gcd(a, b)$ , unde

$\forall i \in \mathbb{Z}_+$  al  $q_{n+1} = 0$ . 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  $d = t_{n+1}a + t_n b$ .

$$\begin{aligned}
 g &= 90 - 27 \cdot 3 = \\
 &= 90 - (567 - 90 \cdot 6) \cdot 3 = \\
 &= 90 \cdot 19 - 567 \cdot 3 = \\
 &= (1224 - 567 \cdot 2) \cdot 19 - 567 \cdot 3 = \\
 &= 1224 \cdot 19 - 567 \cdot 41
 \end{aligned}$$

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

d)  $a = 687, b = 24$

$$\begin{aligned}
 687 &= 24 \cdot 28 + 15 \\
 24 &= 15 \cdot 1 + 9 \\
 15 &= 9 \cdot 1 + 6 \quad \Rightarrow \gcd(687, 24) = 3 \\
 9 &= 6 \cdot 1 + 3 \\
 6 &= 3 \cdot 2 + 0
 \end{aligned}$$

Vom căuta  $r_0, t$  cu  $3 = 687r_0 + 24t$ .

$$\begin{aligned}
 3 &= 9 - 6 = \\
 &= 9 - (15 - 9) = 9 \cdot 2 - 15 = \\
 &= (24 - 15) \cdot 2 - 15 = 24 \cdot 2 - 15 \cdot 3 = \\
 &= 24 \cdot 2 - (687 - 24 \cdot 28) \cdot 3 = \\
 &= 24 \cdot 86 - 687 \cdot 3 \Leftrightarrow \\
 &\Leftrightarrow 3 = 24 \cdot 86 + (-3) \cdot 687
 \end{aligned}$$

Deci  $r_0 = -3$  și  $t = 86$ .  $\square$

- 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?