DIDACTICA MATHEMATICA, Vol. 41 (2023) , pp. 57–66

INELUL $\mathbf{Z}_{31}$ ŞI CODIFICAREA FIDELĂ A TEXTELOR SCRISE ÎN LIMBA ROMÂNĂ

Mihai IVAN

Abstract. In this paper, an elementary method for encoding and decoding texts written in Romanian is presented. This method is based on the ring of residual classes modulo 31. The theme presented is at the interference between mathematics, the Romanian language and cryptography.
AMS classification 2000. 97D40.
Key words. Encryption alphabet, fidel codification, the ring of residual classes.

1. INTRODUCERE

Obiectivul principal al învățării matematicii în liceu este conștientizarea naturii matematicii ca disciplină dinamică strâns legată de viața reală prin relevanţa ei în viaţa de zi cu zi şi prin rolul ei în ştiinţe şi tehnologii.

În lucrarea [3], alfabetul limbii române este extins la un alfabet special, notat cu $\mathbf{A}$ şi numit alfabet de codificare/criptare. Alfabetul $\mathbf{A}$ conţine 31 litere mici ale alfabetului limbii române şi 18 caractere care permit codificarea fidelă a textelor scrise în limba română (de exemplu, fraze, strofe din poezii, citate celebre etc.).

În acest articol prezentăm o metodă elementară (sistem de criptare) pentru codificarea şi decodificarea textelor, care se bazează pe alfabetul $\bar{\mathbf{A}}$ (asociat alfabetului $\mathbf{A}$) şi pe o funcţie bijectivă (numită funcţie de codificare). Funcţia de codificare este definită cu ajutorul inelului $\mathbf{Z}_{31}$.

2. NOŢIUNI ELEMENTARE DE CRIPTOGRAFIE

Criptografia este ştiinţa comunicării informaţiei sub o formă securizată. În sens restrâns, termenul de **criptografie** desemnează numai operaţia de cifrare şi descifrare legală ([1, 5]).

Un **mesaj** $\mathcal{M}$ (numit *text în clar*), scris în limba română, este mesajul ce urmează a fi secretizat. Un **mesaj cifrat**, notat cu $\mathcal{C}$, este mesajul secretizat.

Criptarea/cifrarea, notată cu $\mathcal{E}$, este procesul de codificare ("ascundere") a unui mesaj în clar în mesajul secretizat. Avem: $\mathcal{E}(\mathcal{M}) = \mathcal{C}$. Procesul de secretizare a unui text este realizat de către expeditor.

Decriptarea/descifrarea, notată cu $\mathcal{D}$, este acţiunea de a descifra ("regăsi") mesajul în clar din mesajul cifrat. Avem: $\mathcal{D}(\mathcal{C}) = \mathcal{D}(\mathcal{E}(\mathcal{M})) = \mathcal{M}$. Desecretizarea unui text criptat este realizată de către destinatar.

Prin **algoritm de criptare** se desemnează o mulţime de transformări inversabile prin care mulţimea mesajelor se transformă în mulţimea mesajelor cifrate şi invers. Cifrul este construit cu ajutorul a două funcţii (funcţia de criptare $\mathcal{E}$ şi funcţia de decriptare $\mathcal{D}$).

Cheia de criptare (*key*) $\mathcal{K}$ este mărimea (secretă) necesară realizării criptării şi decriptării. Cheia de criptare este reprezentată printr-un număr, cuvânt etc. şi reglementează operaţia de criptare. Algoritmul care realizează operaţiile de criptare şi decriptare se numeşte **sistem de criptare**.

Pentru aplicarea unui sistem de criptare se procedează astfel:

– un mesaj în forma sa originală este un text în clar;
– expeditorul rescrie mesajul $\mathcal{M}$, folosind un algoritm cunoscut numai de el (şi de destinatar). Se spune că el criptează mesajul $\mathcal{M}$, obţinând un text criptat $\mathcal{C}$;
– destinatarul primeşte textul criptat $\mathcal{C}$ şi îl decriptează, cunoscând algoritmul folosit pentru criptare.

3. ALFABETUL CRIPTAT $\bar{\mathbf{A}}$ ASOCIAT ALFABETULUI $\mathbf{A}$

Considerăm un alfabet $\mathbf{A} = \mathbf{A}_1 \cup \mathbf{A}_2$ format din 49 caractere, unde:
$\mathbf{A}_1 =$
$\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z,$ ă, î, â, ş, ţ $\}$
este *mulţimea formată din 31 litere* (litere mici ale alfabetului limbii române);
$\mathbf{A}_2$ este *mulţimea formată din 18 caractere* (simboluri sau semne grafice de punctuaţie) care au semnificaţiile date în tabelul următor:

Nr.	**Simbol**	**Semnificaţie**
1	$\mathcal{L}$	*litera mică care urmează devine literă mare*
2	⊔	*un spaţiu liber*
3	/	*rând nou*
4	,	*virgulă*
5	-	*cratimă*
6	?	*semnul întrebării*
7	!	*semnul exclamării*
8	”	*ghilimele pentru scrierea unui text*
9	”	*ghilimele pentru încheierea unui text*
10	;	*punct şi virgulă*
11	–	*linia de pauză sau linia de dialog*
12	.	*punct*
13	:	*două puncte*
14	’	*apostrof*
15	(	*paranteză deschisă*
16	)	*paranteză închisă*
17	&	*şi*
18	@	*simbol pentru e-mail*

OBSERVAŢIA 1. *Fiecare din simbolurile* $\mathcal{L}, \sqcup, /$ *ne indică executarea unei acţiuni asupra unei litere mici, cuvânt sau rând (mai precis, transformarea unei litere mici a alfabetului* $\mathbf{A}_1$ *în litera mare corespunzătoare, lăsarea unui spaţiu liber după un cuvânt scris sau trecerea la un rând nou după un rând scris).*

Notăm cu $c_i, i = \overline{1,49}$ caracterul din alfabetul $\mathbf{A}$ care se află în poziţia i (ordinea literelor mici şi a simbolurilor alfabetului este fixată). Deci:

$$\mathbf{A} = \{c_i | i = \overline{1,49}\}.$$

De exemplu: $c_1 = a$; $c_7 = g$; $c_{20} = t$; $c_{32} = \mathcal{L}$.

Avem: $\mathbf{A}_1 = \{c_i | i = \overline{1,31}\}$ şi $\mathbf{A}_2 = \{c_{31+j} | j = \overline{1,18}\}$.

Notăm cu $\bar{\mathbf{A}}$, mulţimea numerelor naturale mai mici sau egale cu 48.

Mulţimea $\bar{\mathbf{A}} = \{m | m \in \mathbf{N}, m \leq 48\}$, este numită *alfabetul criptat* asociat alfabetului $\mathbf{A}$. Între alfabetul $\mathbf{A}$ şi alfabetul criptat $\bar{\mathbf{A}}$, există o funcţie bijectivă definită prin:

$$f : \mathbf{A} \to \bar{\mathbf{A}}, \quad f(c_i) = i - 1.$$

De exemplu, avem corespondenţele următoare:

$p \leftrightarrow 15$; $z \leftrightarrow 25$; $\mathcal{L} \leftrightarrow 31$; $\sqcup \leftrightarrow 32$; $f \leftrightarrow 5$; $\hat{a} \leftrightarrow 28$.

Altfel spus, $\mathbf{A}$ şi $\bar{\mathbf{A}}$, se "identifică" prin intermediul funcţiei f.

4. UTILIZAREA ALFABETULUI CRIPTAT $\bar{\mathbf{A}}$ ŞI A INELULUI $\mathbf{Z}_{31}$ ÎN CODIFICAREA TEXTELOR SCRISE ÎN LIMBA ROMÂNĂ

În acest paragraf prezentăm o metodă de codificare a textelor care permite redarea exactă în textele criptate a valorilor stilistice ale frazelor scrise în limba română. Această metodă se bazează pe alfabetul criptat $\bar{\mathbf{A}}$ şi pe o funcţie bijectivă $\bar{e}_k : \bar{\mathbf{A}} \to \bar{\mathbf{A}}$, numită funcţie de codificare cu cheia k. Funcţia $\bar{e}_k$ este definită cu ajutorul unei permutări a elementelor inelului $\mathbf{Z}_{31}$ (care se identifică cu mulţimea $\bar{\mathbf{A}}_1$) şi permutarea identică a mulţimii $\bar{\mathbf{A}}_2 = \{31, 32, \ldots, 47, 48\}$.

Pentru a secretiza un text scris în limba română se vor respecta următoarele *convenţii*:

– *textul în clar este format din cuvinte, propoziţii sau fraze* care conţin litere mici şi litere mari ale alfabetului limbii române, semne de punctuaţie şi spaţii libere între cuvinte;

– *textul este interpretat ca un singur cuvânt* (spaţiul liber este un caracter distinct).

Pentru a aplica metoda de codificare bazată pe alfabetul criptat $\bar{\mathbf{A}}$ şi utilizarea unei funcţii de codificare cu cheie dată, se vor aplica următoarele **reguli**:

• **fiecărui caracter** (care intră în componenţa unui cuvânt) i se asociază prin intermediul unei funcţii bijective o literă mică sau un număr format din două cifre. Mai precis:

– *unei litere mici* i se asociază o altă literă mică;

– *fiecărui simbol* (care reprezintă un semn de punctuaţie sau o acţiune) i se asociază un număr de două cifre (cuprins între numerele 31 şi 48);
– *unei litere mari* i se asociază o succesiune formată din numărul 31 şi litera mică corespunzătoare;

• **textul codificat** (criptat) este format dintr-o succesiune de litere mici şi numere naturale de două cifre din mulţimea $\bar{\mathbf{A}}_2$.

Scriem alfabetul criptat $\bar{\mathbf{A}}$ ca o reuniune între $\bar{\mathbf{A}}_1$ (format din numerele din $\bar{\mathbf{A}}$ care corespund literelor mici ale alfabetului limbii române) şi $\bar{\mathbf{A}}_2$ (format din numerele din $\bar{\mathbf{A}}$ care corespund ultimelor 18 caractere). Deci:

$$\bar{\mathbf{A}} = \bar{\mathbf{A}}_1 \cup \bar{\mathbf{A}}_2,$$

unde: $\bar{\mathbf{A}}_1 = \{0, 1, 2, 3, \ldots, 29, 30\}$ şi $\bar{\mathbf{A}}_2 = \{31, 32, 33, \ldots, 47, 48\}$.

Avem următoarele corespondenţe:

$$\mathbf{A}_1 = \{c_i | i = \overline{1, 31}\} \quad \leftrightarrow \quad \bar{\mathbf{A}}_1 = \{0, 1, 2, 3, \ldots, 29, 30\};$$

$$\mathbf{A}_2 = \{c_{31+j} | j = \overline{1, 18}\} \quad \leftrightarrow \quad \bar{\mathbf{A}}_2 = \{31, 32, 33, \ldots, 47, 48\}.$$

Interpretăm numerele din alfabetul $\bar{\mathbf{A}}_\mathbf{1}$ ca fiind elemente din inelul $\mathbf{Z}_{31}$ al claselor de resturi modulo 31. Deci:

$$\bar{\mathbf{A}}_1 \equiv \mathbf{Z}_{31} = \{0, 1, 2, \ldots, 29, 30\}.$$

Fie k un număr natural astfel încât $0 \leq k \leq 30$, numit *cheie de criptare*.

Matematic, procedăm în modul următor:

• Cu ajutorul cheii de criptare k, definim permutarea
$e_k : \bar{\mathbf{A}}_1 \to \bar{\mathbf{A}}_1,\ \alpha \mapsto e_k(\alpha)$.

• Extindem e_k la funcţia bijectivă $\bar{e}_k : \bar{\mathbf{A}} \to \bar{\mathbf{A}}$, definită astfel:

$$\bar{e}_k(\alpha) := \begin{cases} e_k(\alpha) & \text{pentru} \quad \alpha \in \bar{\mathbf{A}}_1, \\ \alpha & \text{pentru} \quad \alpha \in \bar{\mathbf{A}}_2. \end{cases} \tag{1}$$

Observăm că $\bar{e}_k(\overline{3j}) = \overline{3j},\ j \in \{1, 2, 3, \ldots, 9\}$ şi $\bar{e}_k(\overline{4m}) = \overline{4m},\ m \in \{0, 1, 2, \ldots, 8\}$.

Notăm $\bar{e}_k(\mathbf{A}) = \bar{\mathbf{A}}_\mathbf{k}$. În acest mod,$\bar{\mathbf{A}}_k$ este un nou alfabet criptat, numit *alfabet criptat cu cheia k*, definit cu ajutorul inelului $\mathbf{Z}_{31}$. Funcţia $\bar{e}_k : \bar{\mathbf{A}} \to \bar{\mathbf{A}}$, este numită *funcţie de codificare cu cheia k*.

Într-un tabel, alfabetul $\bar{\mathbf{A}}_k$ se scrie sub alfabetul $\bar{\mathbf{A}}$, pentru a pune în evidenţă corespondenţa bijectivă între numere. Observăm că alfabetele $\bar{\mathbf{A}}$ şi $\bar{\mathbf{A}}_k$ au aceleaşi numere pe poziţiile $31, 32, 33, \ldots, 47, 48$.

Alfabetul criptat $\bar{\mathbf{A}}_k$ se poate scrie sub forma:

$$\bar{\mathbf{A}}_k = \bar{\mathbf{A}}_{k,1} \cup \mathbf{A}_2, \qquad \textit{unde} \quad \bar{\mathbf{A}}_{k,1} = \{\bar{e}_k(\alpha) | \forall \alpha \in \bar{\mathbf{A}}_1\}.$$

Funcţia de codificare $\bar{e}_k : \bar{\mathbf{A}} \to \bar{\mathbf{A}}$, se descrie cu ajutorul tabelului:

$\bar{\mathbf{A}}$	0	1	2	...	α	...	31	32	...	48
$\bar{\mathbf{A}}_k$	$\bar{e}_k(0)$	$\bar{e}_1(1)$	$\bar{e}_k(2)$	...	$\bar{e}_k(\alpha)$	...	31	32	...	48

Pentru codificarea mesajului $\mathcal{M}$ folosim funcţia $e_k : \bar{\mathbf{A}}_1 \to \bar{\mathbf{A}}_1$, definită prin:

$$e_k(\alpha) := (\alpha + k)\ mod\ 31, \tag{2}$$

unde k este cheia de criptare, iar α reprezintă numărul corespunzător literei din mesajul care va fi codificat.

Pentru codificarea unui text în clar (interpretat ca un singur cuvânt c) se foloseşte următorul **algoritm de codificare**. Acest algoritm constă în efectuarea etapelor următoare care se aplică fiecărui caracter component al mesajului dat:

Etapa 1. Unui caracter (literă mică sau simbol) $c_i \in \bar{\mathbf{A}}$ (care intră în componenţa cuvântului c) *i se asociază numărul corespunzător* $\alpha_i \in \bar{\mathbf{A}}$;

Etapa 2. Numărului $\alpha_i \in \bar{\mathbf{A}}$ *i se asociază numărul* $e_k(\alpha_i) = \beta_j \in \bar{\mathbf{A}}_k$;

Etapa 3. Numărului $\beta_j \in \bar{\mathbf{A}}_k$, *i se asociază* $d_j \in \mathbf{A}_1 \cup \mathbf{A}_2$ (literă mică sau număr de două cifre care compun cuvântul d);

Etapa 4. Unei litere mari care corespunde literei mici $c_m \in \mathbf{A}_1$ *i se asociază secvenţa* $31d_m$, unde d_m este litera obţinută prin aplicarea Etapelor $1, 2, 3$, pornind de la $c_m \in \mathbf{A}_1$.

În final se obţine textul codificat $\mathcal{C}$.

Mesajul codificat $\mathcal{C}$ este interpretat ca un singur cuvânt care se scrie ca o succesiune de litere mici şi numere din mulţimea $\{31, 32, 33, \ldots, 47, 48\}$.

În cele ce urmează vom "identifica" alfabetul $\mathbf{A}$ cu alfabetul $\bar{\mathbf{A}}$. Pentru exemplificare, considerăm cheia $k = 9$. Deoarece:
$e_9(29) = (29 + 9)\ mod\ 31 = 7$; $e_9(8) = (8 + 9)\ mod\ 31 = 17$;
$e_9(17) = (17 + 9)\ mod\ 31 = 26$; $e_9(20) = (20 + 9)\ mod\ 31 = 29$,
rezultă corespondenţele următoare:
ş$\in \mathbf{A}_1 \leftrightarrow \bar{e}_9(29) = 7 \in \bar{\mathbf{A}}_9 \leftrightarrow h \in \mathbf{A}_1$;
$i \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(8) = 17 \in \bar{\mathbf{A}}_9 \leftrightarrow r \in \mathbf{A}_1$;
$r \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(17) = 26 \in \bar{\mathbf{A}}_9 \leftrightarrow$ ă$\in \mathbf{A}_1$;
$u \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(20) = 29 \in \bar{\mathbf{A}}_9 \leftrightarrow$ ş$\in \mathbf{A}_1$;
$\mathcal{L} \in \mathbf{A}_2 \leftrightarrow \bar{e}_9(31) = 31 \in \bar{\mathbf{A}}_9 \leftrightarrow 31 \in \mathbf{A}_2$.

Literei mari "R" îi corespunde secvenţa $31ă$. Deci, "R" $\leftrightarrow$ $31ă$.

Exemplul 1. *(***model de codificare a unui mesaj pentru** $k = 9$*)*
Codificăm mesajul: "Şirul lui Rolle".

Soluţie. Cuvântul $c =$ "Şirul lui Rolle" este format din 15 caractere.

Aplicând algoritmul de codificare pentru cheia $k = 9$, obţinem corespondenţele următoare:
$l \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(11) = 20 \in \bar{\mathbf{A}}_9 \leftrightarrow u \in \mathbf{A}_1$;
$o \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(14) = 23 \in \bar{\mathbf{A}}_9 \leftrightarrow x \in \mathbf{A}_1$;
$e \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(4) = 13 \in \bar{\mathbf{A}}_9 \leftrightarrow n \in \mathbf{A}_1$.

Folosind rezultatele anterioare, obţinem tabelul următor:

M	Ş	i	r	u	l		l	u	i		R	o	l	l	e
$\bar{\mathbf{A}}$	29	8	17	20	11	32	11	20	8	32	17	14	11	11	4
$\bar{\mathbf{A}}_9$	7	17	26	29	20	32	20	29	17	32	26	23	20	20	13
C	$31h$	r	ă	ş	u	32	u	ş	r	32	$31ă$	x	u	u	n

Mesajul codificat **C** este: "*31hrăşu32uşr32 31ăxuun*". □

Exemplul 2. *Codificaţi următoarea strofă din poezia "Liniştе", de Lucian Blaga (1895-1961):*
"Atâta linişte-i în jur de-mi pare că aud
cum se izbesc de geamuri, razele de lună."

Soluţie. Cele două versuri formează un text compus din 82 caractere.

Pentru codificare procedăm în acelaşi mod ca la Exemplul 1. Aplicând algoritmul de codificare cu cheia $k = 9$, obţinem corespondenţele următoare:
$a \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(0) = 9 \in \bar{\mathbf{A}}_9 \leftrightarrow j \in \mathbf{A}_1$;
â$\in \mathbf{A}_1 \leftrightarrow \bar{e}_9(28) = 6 \in \bar{\mathbf{A}}_9 \leftrightarrow g \in \mathbf{A}_1$;
$t \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(19) = 28 \in \bar{\mathbf{A}}_9 \leftrightarrow$ â$\in \mathbf{A}_1$;
$n \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(13) = 22 \in \bar{\mathbf{A}}_9 \leftrightarrow w \in \mathbf{A}_1$;
î$\in \mathbf{A}_1 \leftrightarrow \bar{e}_9(27) = 5 \in \bar{\mathbf{A}}_9 \leftrightarrow f \in \mathbf{A}_1$;
$j \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(9) = 18 \in \bar{\mathbf{A}}_9 \leftrightarrow s \in \mathbf{A}_1$;
$d \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(3) = 12 \in \bar{\mathbf{A}}_9 \leftrightarrow m \in \mathbf{A}_1$;
$m \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(12) = 21 \in \bar{\mathbf{A}}_9 \leftrightarrow v \in \mathbf{A}_1$;
$p \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(15) = 24 \in \bar{\mathbf{A}}_9 \leftrightarrow y \in \mathbf{A}_1$;
$c \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(2) = 11 \in \bar{\mathbf{A}}_9 \leftrightarrow l \in \mathbf{A}_1$;
ă$\in \mathbf{A}_1 \leftrightarrow \bar{e}_9(26) = 4 \in \bar{\mathbf{A}}_9 \leftrightarrow e \in \mathbf{A}_1$;
$s \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(18) = 27 \in \bar{\mathbf{A}}_9 \leftrightarrow$ î$\in \mathbf{A}_1$;
$z \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(25) = 3 \in \bar{\mathbf{A}}_9 \leftrightarrow d \in \mathbf{A}_1$;
$b \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(1) = 10 \in \bar{\mathbf{A}}_9 \leftrightarrow k \in \mathbf{A}_1$;
$g \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(6) = 15 \in \bar{\mathbf{A}}_9 \leftrightarrow p \in \mathbf{A}_1$;
$/ \in \mathbf{A}_1 \leftrightarrow \bar{e}_9(33) = 33 \in \bar{\mathbf{A}}_9 \leftrightarrow 33 \in \mathbf{A}_1$.

Ţinând seama de corespondenţele anterioare şi de relaţia
$\bar{\mathbf{e}}_k(\alpha) = \alpha \ (\forall) \ \alpha \in \bar{\mathbf{A}}_2$, obţinem următorul mesaj codificat:

C : " 31jâgâj32urwrhân35r32fw32sşă32mn35vr32yjăn32le32jşn33lşv32în32 rdknîl32mn32pnjvşăr34 32ăjdnun32mn32uşwe42". □

Propoziţia 1. *Dacă se aplică algoritmul de codificare pentru toate elementele alfabetului* **A**, *atunci rezultă următorul* **tabel de codificare cu cheia** $k = 9$*:*

A	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*
$\bar{\mathbf{A}}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\bar{\mathbf{A}}_9$	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*

A	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*	*ă*	*î*	*â*	*ş*	*ţ*	$\mathcal{L}$	⊔
$\bar{\mathbf{A}}$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\bar{\mathbf{A}}_9$	*ă*	*î*	*â*	*ş*	*ţ*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	31	32

A	/	,	-	?	!	”	”	;	–	.	:	’	(	)	&	@
$\bar{\mathbf{A}}$	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$\bar{\mathbf{A}}_9$	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

Demonstraţie. Se completează mai întâi literele şi simbolurile din tabel, folosind rezultatele obţinute în exemplele date. Pentru literele şi simbolurile rămase se procedează în acelaşi mod ca în Exemplul 1. □

EXEMPLUL 3. *Codificaţi mesajul: "Implicaţi-ne şi vom învăţa !".*

Soluţie. Pentru mesajul dat, aplicăm tabelul de codificare cu cheia $k = 9$ din Propoziţia 1. De exemplu, avem următoarele corespondenţe:
$I \to \mathcal{L}i \to 31r$; $m \to v$; $p \to y$; $l \to u$; $\ldots \Longrightarrow$ "*31rvyu....*".
În final obţinem mesajul codificat:
"$C:\ \ 31rvyurljir35wn32hr32\c{t}xv32fw\c{t}eij37$". □

5. UTILIZAREA ALFABETULUI CRIPTAT $\bar{\mathbf{A}}$ ŞI A INELULUI $\mathbf{Z}_{31}$ ÎN DECODIFICAREA TEXTELOR SCRISE ÎN LIMBA ROMÂNĂ

Decodificarea unui text criptat se realizează, utilizând inversa funcţiei de codificare $\bar{e}_k : \bar{\mathbf{A}} \to \bar{\mathbf{A}}$.

Matematic, procedăm în modul următor:

- cu ajutorul cheii de decriptare k (are aceeaşi valoare cu cheia de criptare), definim o permutare $d_k : \bar{\mathbf{A}}_{k,1} \to \bar{\mathbf{A}}_{k,1},\ \beta \mapsto d_k(\beta)$ (d_k este inversa permutării e_k);
- extindem d_k la funcţia bijectivă $\bar{d}_k : \bar{\mathbf{A}}_{\mathbf{k}} \to \bar{\mathbf{A}}_{\mathbf{k}}$, definită astfel:

$$\bar{d}_k(\beta) := \begin{cases} d_k(\beta) & \text{pentru} \quad \beta \in \bar{\mathbf{A}}_{k,1}, \\ \beta & \text{pentru} \quad \beta \in \bar{\mathbf{A}}_2. \end{cases} \tag{3}$$

Observăm că $\bar{d}_k(\overline{3j}) = \overline{3j},\ j \in \{1, 2, 3, \ldots, 9\}$ şi $\bar{d}_k(\overline{4m}) = \overline{4m},\ m \in \{0, 1, 2, \ldots, 8\}$.

Funcţia $\bar{d}_k : \bar{\mathbf{A}}_k \to \bar{\mathbf{A}}_k$, este numită *funcţie de decodificare cu cheia k.*

Funcţia $\bar{d}_k : \bar{\mathbf{A}}_k \to \bar{\mathbf{A}}_k$ se poate descrie cu ajutorul unui *tabel cu două linii* care se obţine prin *inversarea liniilor tabelului asociat* funcţiei $\bar{e}_k : \bar{\mathbf{A}} \to \bar{\mathbf{A}}$.

Pentru decodificarea mesajului criptat $\mathcal{C}$ este folosită funcţia bijectivă $d_k : \bar{\mathbf{A}}_{k,1} \to \bar{\mathbf{A}}_{k,1}$, definită prin:

$$d_k(\beta) := (\beta - k)\ mod\ 31, \tag{4}$$

unde k este cheia de decriptare, iar β reprezintă numărul corespunzător literei mici din mesajul care va fi decodificat.

Pentru decodificarea unui text criptat $\mathcal{C}$ (interpretat ca un singur cuvânt d) se foloseşte următorul **algoritm de decodificare**. Acest algoritm constă în efectuarea etapelor următoare care se aplică fiecărui caracter component al mesajului dat:

Etapa 1. Unui caracter (literă mică sau simbol) $d_i \in \bar{\mathbf{A}}$ (care intră în componenţa cuvântului d) *i se asociază* numărul corespunzător $\beta_i \in \bar{\mathbf{A}}_k$;

Etapa 2. Numărului $\beta_i \in \bar{\mathbf{A}}_k$ *i se asociază* numărul $\bar{d}_k(\beta_i) = \alpha_j \in \bar{\mathbf{A}}$;

Etapa 3. Numărului $\alpha_j \in \bar{\mathbf{A}}$, *i se asociază* $c_j \in \mathbf{A}_1 \cup \bar{\mathbf{A}}_2$ (literă mică sau număr de două cifre care compun cuvântul c);

Etapa 4. Unei secvenţe de forma $31d_m$, unde d_m este o literă mică, *i se asociază* litera mare care corespunde literei mici $c_m \in \mathbf{A}_1$, obţinută prin aplicarea Etapelor $1, 2, 3$, pornind de la $d_m \in \mathbf{A}_1$.

În final se obţine textul decodificat $\mathcal{M}$.

Pentru exemplificare, considerăm cheia $k = 9$. Deoarece:
$d_9(14) = (14 - 9)\ mod\ 31 = 5$; $d_9(23) = (23 - 9)\ mod\ 31 = 14$;
$d_9(26) = (26 - 9)\ mod\ 31 = 17$; $d_9(1) = (1 - 9)\ mod\ 31 = 23$,
rezultă corespondenţele următoare:
$o \in \mathbf{A}_1 \leftrightarrow 14 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(14) = 5 \in \bar{\mathbf{A}}_1 \leftrightarrow f \in \mathbf{A}_1$;
$x \in \mathbf{A}_1 \leftrightarrow 23 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(23) = 14 \in \bar{\mathbf{A}} \leftrightarrow o \in \mathbf{A}_1$;
ă$\in \mathbf{A}_1 \leftrightarrow 26 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(26) = 17 \in \bar{\mathbf{A}}_1 \leftrightarrow r \in \mathbf{A}_1$;
$b \in \mathbf{A}_1 \leftrightarrow 1 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(1) = 23 \in \bar{\mathbf{A}}_1 \leftrightarrow x \in \mathbf{A}_1$.

Pentru numărul $33 \in \bar{\mathbf{A}}_2$, obţinem corespondenţa următoare:
$33 \in \bar{\mathbf{A}}_2 \leftrightarrow 33 \in \bar{\mathbf{A}}_2 \leftrightarrow \bar{d}_9(33) = 33 \in \bar{\mathbf{A}}_2 \leftrightarrow / \in \mathbf{A}_2$.

Secvenţei $31n$ îi corespunde litera mare "E", deoarece $31 \leftrightarrow \mathcal{L}$ şi $n \in \mathbf{A}_1 \leftrightarrow 13 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(13) = 4 \in \bar{\mathbf{A}}_1 \leftrightarrow e \in \mathbf{A}_1$. Deci, $31n \leftrightarrow$ "E".

Exemplul 4. *(***model de decodificare a unui mesaj criptat pentru** $k = 9$*) Decodificăm mesajul:* (C) *"31oxăvşuj32uşr32 31nşună".*

Soluţie. Cuvântul criptat C este format din 19 caractere.

Aplicând algoritmul de decodificare obţinem următoarele corespondenţe:
$v \in \mathbf{A}_1 \leftrightarrow 21 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(21) = 12 \in \bar{\mathbf{A}}_1 \leftrightarrow m \in \mathbf{A}_1$;
ş$\in \mathbf{A}_1 \leftrightarrow 29 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(29) = 20 \in \bar{\mathbf{A}}_1 \leftrightarrow u \in \mathbf{A}_1$;
$u \in \mathbf{A}_1 \leftrightarrow 20 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(20) = 11 \in \bar{\mathbf{A}}_1 \leftrightarrow l \in \mathbf{A}_1$;
$j \in \mathbf{A}_1 \leftrightarrow 9 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(9) = 0 \in \bar{\mathbf{A}}_1 \leftrightarrow a \in \mathbf{A}_1$;
$r \in \mathbf{A}_1 \leftrightarrow 17 \in \bar{\mathbf{A}}_{9,1} \leftrightarrow \bar{d}_9(17) = 8 \in \bar{\mathbf{A}}_1 \leftrightarrow i \in \mathbf{A}_1$.

Folosind rezultatele anterioare, obţinem tabelul următor:

C	$31o$	x	$ă$	v	ş	u	j	32	u	ş	r	32	$31n$	ş	u	n	$ă$
$\bar{\mathbf{A}}_9$	14	23	26	21	29	20	9	32	20	29	17	32	13	29	20	13	26
$\bar{\mathbf{A}}$	5	14	17	12	20	11	0	32	11	20	8	32	4	20	11	4	17
M	F	o	r	m	u	l	a		l	u	i		E	u	l	e	r

Mesajul decodificat **M** este: "*Formula lui Euler*".

Formula lui Euler " $e^{i\pi} + 1 = 0$ ", prezintă relaţia dintre cele cinci constante matematice fundamentale: $0, 1, \pi, e, i$. Această formulă a fost scrisă în anul 1748 de Euler (1707-1783). □

Exemplul 5. *Decodificaţi mesajul* **C** : *"31luşs3531wjyxlj ".*

Soluţie. Mesajul criptat C este compus din 13 caractere.

Pentru decodificare procedăm în acelaşi mod ca la Exemplul 4. Aplicând algoritmul de codificare cu cheia $k = 9$, obţinem corespondenţele următoare:
$l \in \mathbf{A}_1 \leftrightarrow \bar{d}_9(11) = 2 \in \bar{\mathbf{A}}_1 \leftrightarrow c \in \mathbf{A}_1$;
$s \in \mathbf{A}_1 \leftrightarrow \bar{d}_9(18) = 9 \in \bar{\mathbf{A}}_1 \leftrightarrow j \in \mathbf{A}_1$;
$w \in \mathbf{A}_1 \leftrightarrow \bar{d}_9(22) = 13 \in \bar{\mathbf{A}}_1 \leftrightarrow n \in \mathbf{A}_1$;
$y \in \mathbf{A}_1 \leftrightarrow \bar{d}_9(24) = 15 \in \bar{\mathbf{A}}_1 \leftrightarrow p \in \mathbf{A}_1$.

Ţinând seama de corespondenţele anterioare şi de relaţia $\bar{\mathbf{d}}_k(\beta) = \beta,\ (\forall)\ \beta \in \bar{\mathbf{A}}_2$, obţinem mesajul **M**: " Cluj-Napoca ". □

PROPOZIŢIA 2. *Dacă se aplică algoritmul de decodificare pentru toate elementele alfabetului* **A**, *atunci rezultă următorul* **tabel de decodificare cu cheia** $k = 9$*:*

A	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*
$\bar{\mathbf{A}}_9$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\bar{\mathbf{A}}$	*w*	*x*	*y*	*z*	*ă*	*î*	*â*	*ş*	*ţ*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*

A	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*	*ă*	*î*	*â*	*ş*	*ţ*	$\mathcal{L}$	⊔
$\bar{\mathbf{A}}_9$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\bar{\mathbf{A}}$	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	31	32

A	/	,	-	?	!	”	”	;	–	.	:	’	(	)	*&*	@
$\bar{\mathbf{A}}_9$	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$\bar{\mathbf{A}}$	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

Demonstraţie. Se completează mai întâi literele şi simbolurile din tabel, folosind rezultatele obţinute în exemplele date. Pentru literele şi simbolurile rămase se procedează în acelaşi mod ca în Exemplul 4. □

EXEMPLUL 6. *Decodificaţi mesajul criptat* "**C** : *31wş35wâănkj32wrîryşu32lrwn32yxjăâe32ţjuşu33 31le32jă32or32fw32îâjăn 32îe35ir32ăeîyşwme43 32 41 32 31nş37“, cu cheia* $k = 9$.

Soluţie. Pentru mesajul criptat dat, aplicăm tabelul de decodificare cu cheia $k = 9$ din Propoziţia 2. De exemplu, avem următoarele corespondenţe:
31w $\to \mathcal{L}n \to N$; ş $\to u$; 35 $\to -$; $w \to n$; â $\to t$; ... $\Longrightarrow$ "*Nu-nt....*".
În final, descoperim mesajul decodificat care constă din două versuri ale poeziei "Un gând", de Elena Farago (1878-1954):
"*Nu-ntreba nisipul cine poartă valul*
Că ar fi în stare să-ţi răspundă: - Eu!" □

EXEMPLUL 7. *Decodificaţi mesajul ciptat*
"**C** : *31leăirun32îşwâ32jukrwnun32ljăn32mşl32yxunwşu32fwîşounirâxă32mn 32uj32x32vrwân32uj32juâj42", cu cheia* $k = 9$.

Soluţie. Se procedează la fel ca la Exemplul 6. În final, descoperim un citat de James Russell Lowell(1819-1891): " *Cărţile sunt albinele care duc polenul însufleţitor de la o minte la alta.*". □

6. IMPORTANŢA STUDIERII ACESTUI SUBIECT ÎN LICEU

Teoria inteligenţelor multiple se bazează pe existenţa a opt tipuri de inteligenţă (pentru detalii, vezi articolul [2]). Dintre aceste tipuri de inteligenţă menţionăm inteligenţa logico-matematică. În totalitatea activităţilor didactice în care se dezvoltă acest tip de inteligenţă se remarcă şi activităţile de criptografie.

Studierea acestui subiect contribuie la formarea şi dezvoltarea de aptitudini şi competenţe matematice. În acest scop, acest articol propune un material ştiinţifico-didactic pentru proiectarea şi organizarea unor activităţi de învăţare în cadrul unor lecţii de matematică.

Proiectarea şi organizarea unei activităţi didactice bazată pe elementele de conţinut ale acestei lucrări este benefică din următoarele motive:
− se prezintă într-un mod elementar utilitatea conceptelor matematice (de exemplu: corespondenţe între cuvinte şi secvenţe de numere şi simboluri, funcţie bijectivă, inversa unei funcţii, operaţii cu clase de resturi);
− contribuie la familiarizarea elevilor cu unele aplicaţii simple ale criptografiei. Prin descifrarea mesajului trimis, elevii au satisfacţia reuşitei;
− prin dobândirea abilităţilor de criptare, elevii învaţă ceva atractiv.

Conţinutul ştiinţific al acestei lucrări se poate folosi la alcătuirea listei de teme cu statut opţional la disciplina de matematică. În aceeaşi listă se poate include şi tema: *Rime şi Permutări* ([4], pp. 319-324).

REFERENCES

[1] A. Atanasiu, *Securitatea Informaţiei, vol. 1 (Criptografie)*. Ed. InfoData, Cluj, 2007.
[2] C.-A. Bercovici, *Teoria inteligenţelor multiple şi Matematica*. Didactica Mathematica, 32(2014), 25-38.
[3] M. Ivan, *An elementary method for the fidel codification of texts written in Romanian language*. ArXiv: 1803.00523v1 [math. HO], 2018, 1-9.
[4] M. Ivan, *Didactica matematicii aplicată în procesul de predare, învăţare şi evaluare din gimnaziu şi liceu*. Editura Mirton, Timişoara, 2022.
[5] C, Popescu, *Introducere în criptografie*. Editura Universităţii din Oradea, Oradea, 2001.

Teacher Training Department
West University of Timişoara
Str. V. Pârvan, no. 4
300223 Timişoara, Romania
e-mail: mihai.ivan@e-uvt.ro