Teorema împărțirii cu rest

$\forall a, b \in \mathbb{Z}$, $b \neq 0$

$\exists! q, r$ a.î. $a = b \cdot q + r$, $0 \leq r < |b|$

~~$r < 0$~~

$a = 35 \quad b = -13$

$35 = -13 \cdot (-2) + 9$

Alg. Euclid $(a,b) = (b, a \bmod b)$ .... rest 0 comb. liniară după a, și b

$a > b$

$a = b \cdot q_1 + r_1$

$b = r_1 \cdot q_2 + r_2$

$a : b = q_1$ rest r_1

$r_1 = a - q_1 \cdot b$

$42 : 12 = 3$ ....

$42 - 3 \cdot 12 =$ rest

$V_a = (1,0) \quad V_b = (0,1)$

? $\cdot a +$? $b =$

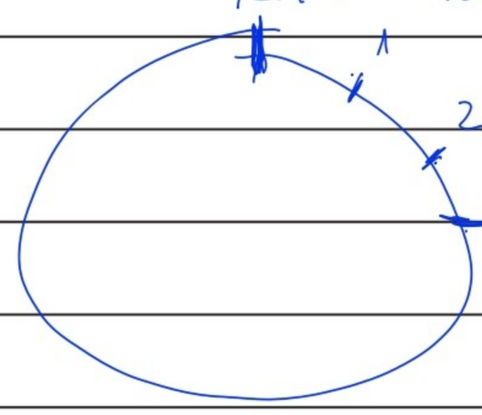
$V_{r_1} = V_a - q_1 V_b = (\ ,\ )$

$V_{r_2} = V_b - q_2 \cdot V_{r_1} = (\ ,\ )$

$12 + 30 = 42$ mod 12, 24, 36

$42 - 12 \cdot 3$

36 = 6



15 − 12 / 3

ex 1 $a = 11 \quad b = 5$

$11 = 5 \cdot 2 + 1$

$5 = 1 \cdot 5 + 0$

ult. rest nenul

$V_{11} = (1,0) \quad V_5 = (0,1)$

$V_1 = V_{11} - 2 \cdot V_5 = (1,0) - 2 \cdot (0,1) = (1-2 \cdot 0, 0 - 2 \cdot 1) = (1, -2)$

$\alpha \quad \beta$

Vf. $1 \cdot 11 + (-2) \cdot 5 = 1$

$11 + (-10) = 1$ ✓

ex 2 $a = 4 \quad b = 19$

(*) $V_4 = (0,1) \quad V_{19} = (1,0)$

$V_3 = V_{19} - 4 \cdot V_4 = (1,0) - 4 \cdot (0,1) = (1, -4)$

$19 = 4 \cdot 4 + 3$

$4 = 3 \cdot 1 + 1$ cmmdc $(a,b) = (4, 19) = 1$

$3 = 1 \cdot 3 + 0$

$V_1 = V_4 - 1 \cdot V_3 = (0,1) - (1,-4) = (-1, 5)$

$\beta \quad \alpha$

$5 \cdot 4 + (-1) \cdot 19 = 1$

$V_4 = (1,0) \quad V_{19} = (0,1)$

$4 = 19 \cdot 0 + 4$

$19 = 4 \cdot 4 + 3$

$\vdots$

$+1$

$V_1 = (\alpha, \beta)$

inv. modular al lui a mod b $\Leftrightarrow \alpha \bmod b$

$a \cdot a^{-1} \equiv_b 1 \equiv 1 \bmod b$

$(11 \bmod 5) \cdot (1 \bmod 5) = 1$

$a \equiv b \bmod m \Rightarrow m \mid a - b$; $19 \mid 20 - 1$

Inversul lui 4 mod 19

$4 \cdot 5 \equiv 1 \bmod 19$ $\quad 20 - 19 = 1$ ✓

$4 \in \mathbb{Z}_{19}^* \quad 4^{-1} \in \mathbb{Z}_{19}^*$

$\alpha \bmod 19 = 5 \bmod 19 = 5$

– Alg. Euclid (extins)

$\square \cdot a + \square \cdot b = \bigcirc$

$a > b$ $\quad a = 19,\ b = 4$ $\quad 0 \le rest < b$

$V_a = (1,0) \quad V_b = (0,1)$

$19 = 4 \cdot 4 + 3$ $\quad 3 = 19 - 4 \cdot 4$ $\quad V_3 = V_{19} - 4 \cdot V_4 = (1,0) - 4(0,1) = (1,-4)$

$4 = 3 \cdot 1 + \boxed{1}$ $\quad 1 = 4 - 1 \cdot 3$ $\quad V_1 = V_4 - 1 \cdot V_3 = (0,1) - 1 \cdot (1,-4) = (-1,5)$

$3 = 1 \cdot 3 + 0$ $\quad\quad \alpha\ \beta$

$\boxed{-1} \cdot 19 + \boxed{5} \cdot 4 = 1$

$\alpha \quad\quad \beta$

- Ecuatii diofantice liniare

$a x + b y = c$ $\quad \exists$ sol. $(a,b) \mid c$

Calc. 1) Alg. Ext. Euclid $\quad (a,b) = \alpha \cdot a + \beta \cdot b$

2) $c' = \frac{c}{(a,b)}$

3) $x = \alpha \cdot c'$ $\quad\quad x = \alpha \cdot \frac{c}{(a,b)}$

$y = \beta \cdot c'$ $\quad\quad y = \beta \cdot \frac{c}{(a,b)}$

- TCR teor. chin. rest.

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \dots \\ x \equiv b_k \mod m_k \end{cases}$$

$c_i = \frac{m}{m_i}$ $\quad c_i x_i \equiv b_i \mod m_i$ $\quad$ obs. $(c_i, m_i) = 1$

$x_0 = \left(\sum_{i=1}^{k} c_i x_i\right) \mod m$

$m = m_1 \cdot \ldots \cdot m_k$; $m_1, \ldots, m_k \ge 1$ si co-prime 2 câte 2, $b_i \in \mathbb{Z}$

$\exists!$ sol. în $\mathbb{Z}_m$

$a x \equiv 1 \mod m \Rightarrow m \mid ax - 1 \Rightarrow \exists y \in \mathbb{Z},\ ax - 1 = my \iff$

$ax - my = 1 \quad (a,m) \mid 1$

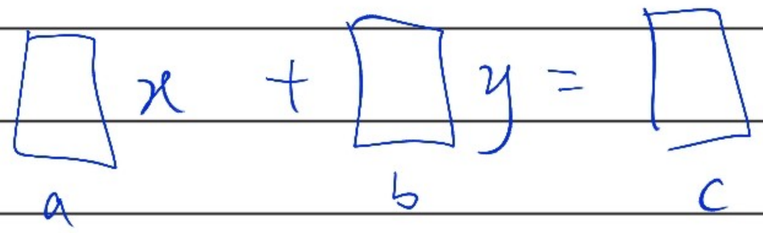
Inversul modular $\quad a \in \mathbb{Z}_m^*, \quad a \cdot a^{-1} \equiv_m 1$

$\rightarrow$ alg. ext. Euclid $\quad (a,m) \rightsquigarrow \alpha, \beta, \quad a^{-1} \mod m = \alpha \mod m$

Ex 1 $a=27 \quad b=21 \qquad (a,b) \mid c$

$ax+by=c \qquad 3 \mid 9 \;\; V \;\; \exists x,y \in \mathbb{Z}$

$27x+21y=9$



① Alg. Euclid

$27 = 21 \cdot 1 + 6$

$21 = 6 \cdot 3 + 3$

$6 = 3 \cdot 2 + 0$

$(27,21) = 3$

$27 - 21 \cdot 1 = 6$

$V_{27} \quad V_{21}$

② Alg. Extins al lui Euclid $V_{27}=(1,0)$ $V_{21}=(0,1)$

$V_6 = V_{27} - 1 \cdot V_{21} = (1,0) - 1 \cdot (0,1) = (1,-1)$

$V_3 = V_{21} - 3 \cdot V_6 = (0,1) - 3 \cdot (1,-1)$

$(0,1) - (3,-3)$

$(0-3, 1-(-3))$

$(-3, 4)$

$\alpha \quad \beta$

$\underline{\underline{(a,b) = \alpha \cdot a + \beta \cdot b}}$

③ $c' = \dfrac{c}{(a,b)}$; $c' = \dfrac{9}{(27,21)} = \dfrac{9}{3} = 3$

④ $x = \alpha \cdot c' = \alpha \cdot \dfrac{c}{(a,b)}$; $x = (-3) \cdot 3 = -9$

$y = \beta \cdot c' = \beta \cdot \dfrac{c}{(a,b)}$; $y = 4 \cdot 3 = 12$

Vf. $27 \cdot (-9) + 21 \cdot 12 = 9$

$-243 \quad +252 \quad = 9 \; V$

$1287x - 4y = 1$

① $\exists$ sol $(1287,4) \mid 1$

② A.E.

$1287 = 4 \cdot 321 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 1 \cdot 3 + 0$

③ A.E.E. $V_{1287}=(1,0)$ $V_4=(0,1)$

$V_3 = V_{1287} - 321 \cdot V_4 = (1,0) - 321\,(0,1) = (1,-321)$

$V_1 = V_4 - 1 \cdot V_3 = (0,1) - 1 \cdot (1,-321) = (-1, 322)$

$\alpha \quad \beta$

④ $c' = \dfrac{c}{(a,b)} = \dfrac{1}{1}$

⑤ $x_1 = \alpha \cdot c' = \alpha = -1 \bmod 4 = 3$

(c) Verificaţi dacă congruenţele $2x^2 + 3x - 2 \equiv 0 \bmod 7$ şi $2x^2 + 3x - 2 \equiv 0 \bmod 3$ admit soluţii în $\mathbf{Z}_7$ şi, respectiv, $\mathbf{Z}_3$, iar în cazul în care admit, determinaţile.

$ax^2 + bx + c \equiv 0 \bmod p$

→ 2 rădăcini în $\mathbb{Z}_p$ dacă $\Delta \equiv y^2 \bmod p$; $y \in \mathbb{Z}$, $p \nmid y$

→ 1 rădăcină în $\mathbb{Z}_p$ dacă $\Delta \equiv 0 \bmod p$

→ 0 altfel

unde $\Delta = b^2 - 4ac$ iar $x = \frac{-b \pm \sqrt{\Delta}}{2a} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

$2x^2 + 3x - 2 \equiv 0 \bmod 7$

$\Delta = b^2 - 4ac$,

$\Delta = 9 - 4 \cdot 2 \cdot (-2) = 9 + 16 = 25$

$\Delta = 5^2$, $7 \nmid 5$ $\Rightarrow$ 2 rad. $x_1 = \frac{-b \pm \sqrt{\Delta}}{2a} \Rightarrow x_1 = \frac{-3+5}{2 \cdot 2} = \frac{2}{4} = 2 \cdot (4^{-1}) \bmod 7$

$x_1 = 2 \cdot 2 = 4 \bmod 7$ $\boxed{x_1 = 7}$

Vf. $2 \cdot 4^2 + 3 \cdot 4 - 2 \equiv_7 32 + 12 - 2 \equiv_7 42 \equiv_7 0$ V

$x_2 = \frac{-3-5}{2 \cdot 2} = -8 \cdot (4^{-1}) = -8 \cdot 2 = -16 \bmod 7 = 5$

Vf. $2 \cdot 5^2 + 3 \cdot 5 - 2 \equiv_7 50 + 15 - 2 \equiv_7 63 \equiv_7 0$ V

$ax \equiv b \bmod m \Rightarrow m \mid ax-b \Rightarrow \exists y \in \mathbb{Z},\ ax-b = my \Leftrightarrow$

$\Leftrightarrow \boxed{ax - my = b}$

$a \equiv b \bmod m \overset{def}{\Rightarrow} m \mid a-b$ pe $a-b$ îl scriu în funcție de m

$\overset{def}{\Rightarrow} \exists q \in \mathbb{Z},\ a-b = m \cdot q$

$ax - my = b$ Alg. Euclid $(a,m) = d = \alpha \cdot a + \beta \cdot m$

$(ax + by = c)$

$m \quad b$

$c' = \frac{b}{(a,m)}$

$x_0 = \alpha \cdot c' = \alpha \cdot \frac{b}{(a,m)}$

$\boxed{\left(x_0 + i \frac{m}{(a,m)}\right) \bmod m}$

#sol (a,m) toate sol. din $\mathbb{Z}_m$

Ex 1. $14x \equiv 6 \bmod 18 \Rightarrow 18 \mid 14x-6 \Rightarrow \exists y \in \mathbb{Z},\ 14x-6 = 18y \Leftrightarrow$

$14x - 18y = 6$

$\exists$ sol? $14x - 18y = 6$ $\exists$ sol $\Leftrightarrow (14,18) \mid 6$

#sol $= (14,18) = 2$ sol în $\mathbb{Z}_m$

Verif.

$x_0 = 12 \in \mathbb{Z}_8$ ✓

$14 \cdot 12 \equiv 6 \bmod 18$ ✓ (Vf.)

$\boxed{\alpha \cdot a + \beta \cdot m} = (a,m)$ $4 \cdot 14 + (-3) \cdot 18 = 2$ ✓

$\alpha = 4,\ \beta = -3$ ✓

$(14,18) = 2$

$x_1 = x_0 + 1 \cdot \frac{18}{(14,18)} = (12+9) \bmod 18 = 3$

Vf $14 \cdot 3 \equiv 6 \bmod 18$ ✓

$\boxed{x_0 = 12,\ x_1 = 3}$ 2 sol în $\mathbb{Z}_{18}$

$c_i x_i \equiv b_i \bmod m_i$

$m_i \mid c_i x_i - b_i \Rightarrow \exists y \in \mathbb{Z}$, a.î.

$c_i x_i - b_i = m_i \cdot y \Leftrightarrow c_i x_i - m_i \cdot y = b_i$

$\exists$ sol. $\Leftrightarrow (c_i, m_i) \mid b_i$ $\quad 1 \mid b_i$

$$\begin{cases} x \equiv & \bmod 2 \\ x \equiv & 3 \\ x \equiv & 7 \end{cases}$$

$m = 2 \cdot 3 \cdot 7$; $c_1 = \frac{2 \cdot 3 \cdot 7}{2}$

$c_2 = \frac{2 \cdot 3 \cdot 7}{3}$

$c_3 = \frac{2 \cdot 3 \cdot 7}{7}$

c_i co-prim cu m_i

$c_i x_i - m_i y = b_i$

① Alg. Euclid $\quad (-2,-6) = (2,6) = (-2,6) = (2,-6)$

$(c_i, m_i) \quad 2 \quad 2 \quad 2 \quad 2$

② Alg. Ext. Euclid

$\alpha \cdot a + \beta \cdot b = (a,b)$

③ $c' = \frac{c}{(a,b)}$

④ $x = \alpha \cdot c' = \frac{\alpha \cdot c}{(a,b)}$

$y = \beta \cdot c' = \frac{\beta \cdot c}{(a,b)}$

$ax \equiv b \bmod m$

ec. congruențiale

$\Rightarrow m \mid ax - b \Rightarrow \exists y \in \mathbb{Z}$ a.î.

$ax - b = m \cdot y$

$ax + (-my) = b$

$a \equiv b \bmod m$

$\Downarrow$

$m \mid a - b$

$\Downarrow$

$\exists q \in \mathbb{Z}$, a.î. $a - b = m \cdot q$

$6 \mid 30$

$4 \mid 16$

$4 \mid 16 \Rightarrow 16 = 4 \cdot q$

$\Downarrow$

$\exists q \in \mathbb{Z}$, a.î. $16 = 4 \cdot q$ + rest 0

$6 \mid 30 \quad 30 = 6 \cdot 5$

$\Downarrow$

$\exists q \in \mathbb{Z}$, a.î. $30 = 6 \cdot q$ + rest 0

$c_i x_i \equiv b_i \bmod m_i$

$x_i \quad i = \overline{1,k}$

$x_0 = \left(\sum_{i=1}^{k} c_i x_i \right) \bmod m$

$$\begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 2 \bmod 9 \\ x \equiv 3 \bmod 11 \\ x \equiv 11 \bmod 13 \end{cases}$$

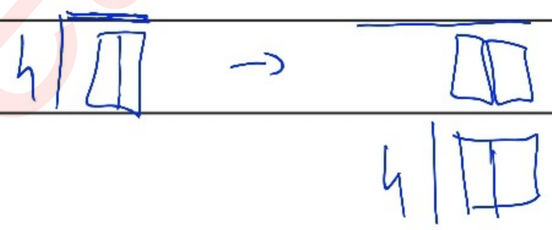
$c_1 = 9 \cdot 11 \cdot 13 = 1287$ $\quad 1287 x_1 \equiv 1 \bmod 4$ $\quad x_1 = 3$

$c_2 = 4 \cdot 11 \cdot 13 = 572$ $\quad 572 x_2 \equiv 2 \bmod 9$ $\quad x_2 = 4$

$c_3 = 4 \cdot 9 \cdot 13 = 468$ $\quad 468 x_3 \equiv 3 \bmod 11$ $\quad x_3 = 6$

$c_4 = 4 \cdot 9 \cdot 11 = 396$ $\quad 396 x_4 \equiv 11 \bmod 13$ $\quad x_4 = 4$

$x = 245$



~~TCR~~

$$\begin{cases} x \equiv 9 \bmod 12 \\ x \equiv 3 \bmod 18 \\ x \equiv 1 \bmod 10 \end{cases}$$

$12 = 2^2 \cdot 3$, $18 = 2 \cdot 3^2$, $10 = 2 \cdot 5$ — toate numerele prime la puterea lor cea mai mare ⇝

nu sunt coprimi 2-2

TCR ✓

$$\begin{cases} x \equiv 9 \bmod 4 \\ x \equiv 3 \bmod 9 \\ x \equiv 1 \bmod 5 \end{cases}$$

sunt coprimi 2-2

$|\mathbb{Z}_m^*| = \phi(m)$

Resturi pătratice

modul prim → p, $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right)$ → simbolul Legendre

$\exists x,\ x^2 \equiv a \bmod m$ — a este rezidiu pătratic, $\left(\frac{a}{p}\right) = 1$ ⟸

$\left(\frac{a}{p}\right) = -1$, a non-rez. pătratic

modul compus → simb. Jacobi $\left(\frac{a}{m}\right)$ — 1 ?⟸ a rez; -1 ⇒ a non-rez.; 0, $p \mid a$

$$\left(\frac{41}{163}\right) = \left(\frac{163 \bmod 41}{41}\right) \overset{F2}{=} \left(\frac{40}{41}\right) \overset{B}{=} \overset{E1}{\left(\frac{2^3}{41}\right)} \cdot \left(\frac{5}{41}\right) = 1 \cdot \left(\frac{41}{5}\right) \overset{F2}{=} 1 \cdot 1 = 1.$$

$\left(\frac{5}{41}\right)$

$5 \bmod 4 = 1$

~~$41 \bmod 4 = 1$~~

$163 \equiv_4 3$

$163 : 4 = 40$ rest 3

$163 \bmod 41 = 40$

$41 \equiv_4 1$

$40 \bmod 4 ? 0$

$2^3 \cdot 5$

41 prim?

$$\left(\frac{2}{p}\right) \overset{F}{=} \begin{cases} (1) & -\left(\frac{p}{2}\right), \ p \equiv_8 \pm 3 \\ (2) & \left(\frac{p}{2}\right), \ p \equiv_8 \pm 1 \end{cases}$$

$p \equiv_8 \pm 3 \Rightarrow p \equiv_4 3$

$p \vee 2$

$$\left(\frac{2}{p}\right) \overset{E(4)}{=} \begin{cases} 1, & p \equiv_8 \pm 1 \\ -1, & p \equiv_8 \pm 3 \end{cases}$$

$$\left(\frac{a \cdot b}{p}\right) \overset{B}{=} \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Alg. Sardinas - Patterson

$C = \{ [c], [c][x] \ldots \}$ → C_1

$C = \{aa, aab, baa, baab\} = \{a^2, a^2b, ba^2, ba^2b\}$

$C_1 = \{x \in \Sigma^+ \mid \exists c \in C, cx \in C\}$ → cuv. din C

C → C_i → C_{i+1}

$C_1 = \{b\} \cap C = \phi$

$C_i = \quad \neq \phi \Rightarrow$ C nu e cod $\Rightarrow$ STOP

$C_{i+1} = \{x \in \Sigma^+ \mid \exists c \in C, cx \in C_i \lor \exists c \in C_i, cx \in C\}$

$C_2 = \{aa, aab\} \cap C = \{aa, aab\} \neq \phi \Rightarrow$ C nu e cod

$C_t = \{ \ldots \} \cap C = \phi$

$C_s = C_t \Rightarrow$ C cod

ab^m ; $n, m \geq 1$

$C = \{ab, ab^m, b^n a\}$

$C_1 = \{b^{m-1}\}$

- Codificarea Huffman clasic

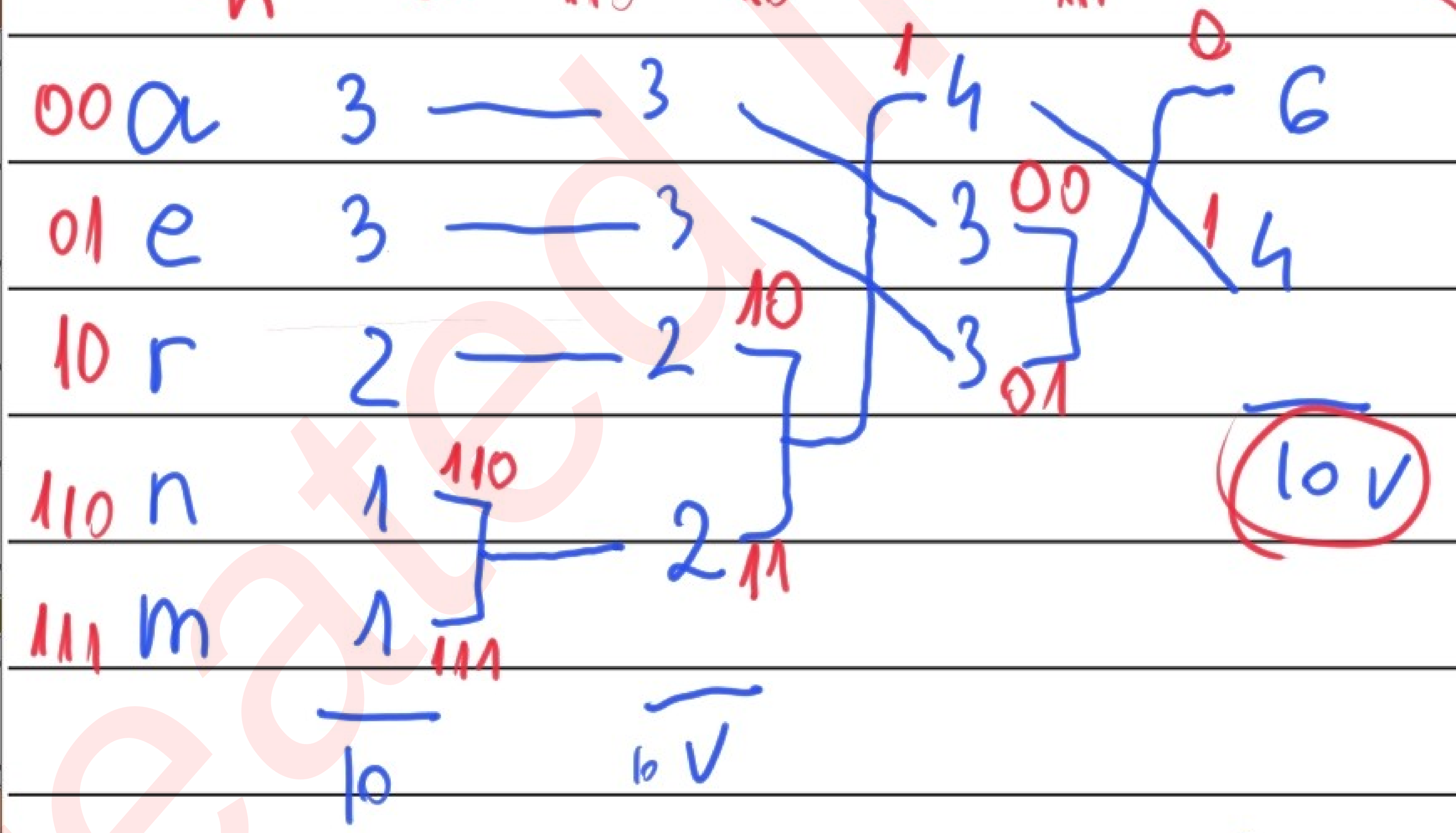
anaaremere

$is = (A, \pi)$ → 00 110 00 00 10 01 111 ...
a n a a r e m

→ ordinea car. în text

→ π 0 sus, 1 jos

is: A	a	n	r	e	m
π	$\frac{3}{10}$	$\frac{1}{10}$	$\frac{2}{10}$	$\frac{3}{10}$	$\frac{1}{10}$
h	00	110	10	01	111



2 parcurgeri (clasic)

$$L_h(is) = \frac{3}{10} \cdot 2 + \frac{3}{10} \cdot 2 + \frac{2}{10} \cdot 2 + \frac{1}{10} \cdot 3 + \frac{1}{10} \cdot 3 = \frac{22}{10} = 2,2$$

2,2

$C_{cod} = \{ \square_{c_1}, \square_{c_2}, \square_{c_3} \}$

$c_1 \| c_2$ $\quad$ $c_1 \| c_1 \| c_3$ $\quad$ 

$c_i \in C$ UNICĂ ⇓ C_{cod}

Sardinas-Patterson

$C = \{ \ldots, \underline{c}, \ldots, \boxed{cx}, \ldots \}$

$C_1 = \{ x \in \Sigma^+ \mid \exists c \in C, cx \in C \} = \{x\}$ sufixul

$C_i = \{ \underline{cx}, \ldots, \boxed{c}, \ldots \}$

$C_{i+1} = \{ x \in \Sigma^+ \mid \exists c \in C, cx \in C_i \ \vee \ \exists c \in C_i, cx \in C \}$

$C_j = \{ \ldots \}$

$C_i \cap C = \emptyset$; $C_t = C_j$, $j < t$ $\Rightarrow$ C este cod

$C_i \cap C \neq \emptyset \Rightarrow C$ nu e cod

C_{t-1}

$C_t = \{ \ldots \} \cap C = \emptyset$ $\quad$ $C_t = C_j$

ex $C = \{aa, aab, baa, baabb\}$

$C_1 = \{b, bb\} \cap C = \emptyset$

$C_2 = \{aa, \ldots\} \cap C = \{aa, \ldots\}$ $\Rightarrow$ $C_{nu\ e\ cod}$

$C = \{ \underbrace{aba^2}_{c_1}, ba^2, (ab)^2, \underbrace{aba^2bab}_{c_1} \}$

$C_1 = \{bab\} \cap C = \emptyset$

$C_2 = \emptyset \cap C = \emptyset$

$C_3 = \emptyset \cap C = \emptyset$ $\quad$ $C_3 = C_2 \Rightarrow C_{cod}$

$C = \{ab, ab^2, b^3a\}$

$C_1 = \{b\} \cap C = \emptyset$

$C_2 = \{b^2a\} \cap C = \emptyset$

$C_3 = \emptyset$

$C_4 = \emptyset$ $\quad$ $C_4 = C_3 \Rightarrow C_{cod}$ $\quad$ $\forall i, C_i \cap C = \emptyset$

$C_1 = \{a, b\}$

$C_2 = \{ab, a\}$

$C_1C_2 = \{aab, aa, bab, ba\}$

aababa

$C_1' = \{b\} \cap C_1C_2 = \emptyset$

$C_2' = \{ab, a\} \cap C_1C_2 = \emptyset$

$C_3' = \{ab, a\} \cap C_1C_2 = \emptyset$ $\Rightarrow$ C cod

$C_1 = \{a, ba\}$ → cod

$C_2 = \{a, ab\}$ → cod

$C_1C_2 = \{aa, aab, baa, baab\}$ ⊛

$c_1 \quad c_2 \quad c_3 \quad c_4$

$C_1' = \{b\} \cap C_1C_2 = \emptyset$

$C_2' = \{aa, aab\} \cap C = \{aab, aa\} = C_2'$ $\Rightarrow$ C nu e cod

Ex2 Produsul a 2 coduri nu este întotdeauna cod.

$C_1 = \{w_1, w_2\}$

$C_2 = \{x_1, x_2\}$

$\in C_1$	$\in C_2$

$C_1C_2 = C_1 \| C_2 = \{w_1x_1, w_1x_2, w_2x_1, w_2x_2\}$

$w_1x_1 w_2x_2$

$w_1x_1 + w_2x_2$

$w_2x_1 + w_1x_2$ $\Rightarrow C_1C_2$ nu e cod

Concatenare de cuvinte din C_1C_2

⊛ baabaa

$c_3 + c_3$

$c_4 + c_1$ $\Rightarrow C_1C_2$ nu e cod

⊛ aabaa

$c_1 + c_3$

$c_2 + c_1$ $\Rightarrow C_1C_2$ nu e cod

$C_2 = \{a, ab\}$ → $C_1' = \{b\} \cap C_2 = \emptyset$

$C_2' = \emptyset$ $C_3' = \emptyset$ $C_3' = C_2'$ $\Rightarrow$ C cod

Ex3 C^k cod când C cod

$u_1 \cdots u_m = v_1 \cdots v_n \Rightarrow m = n \wedge (\forall i)\ u_i = v_i$

$\forall u_i, v_i \in C^k$

$u_i = u_{i_1} \cdots u_{i_k}, u_{i_j} \in C$

$\in C^k$ $\quad \in C \quad \in C$

$v_i = v_{i_1} \cdots v_{i_k}, v_{i_j} \in C$

$\forall$ concatenare de cuvinte din C are descompunere unică

$\forall u_i$, $\forall v_i$ sunt concatenări de cuvinte din C $\Rightarrow u_{i_1} \cdots u_{i_k}$, $v_{i_1} \cdots v_{i_k}$ $\exists! u_{i_j} = v_{i_j}$

$u_{1_1} \cdots u_{1_k} u_{2_1} \cdots u_{2_k} \cdots u_{m_1} \cdots u_{m_k} = v_{1_1} \cdots v_{1_k} v_{2_1} \cdots v_{2_k} \cdots v_{m_1} \cdots v_{m_k}$

C cod $\Rightarrow m = n$ și $(\forall i_j)\ u_{i_j} = v_{i_j}$ $\Rightarrow C^k$ cod

Codif. H. adaptiv — 1 parcurgere

a b a c a c d

cod: cod ASCII a 0 cod ASCII b 1 00 cod ASCII c 1 001

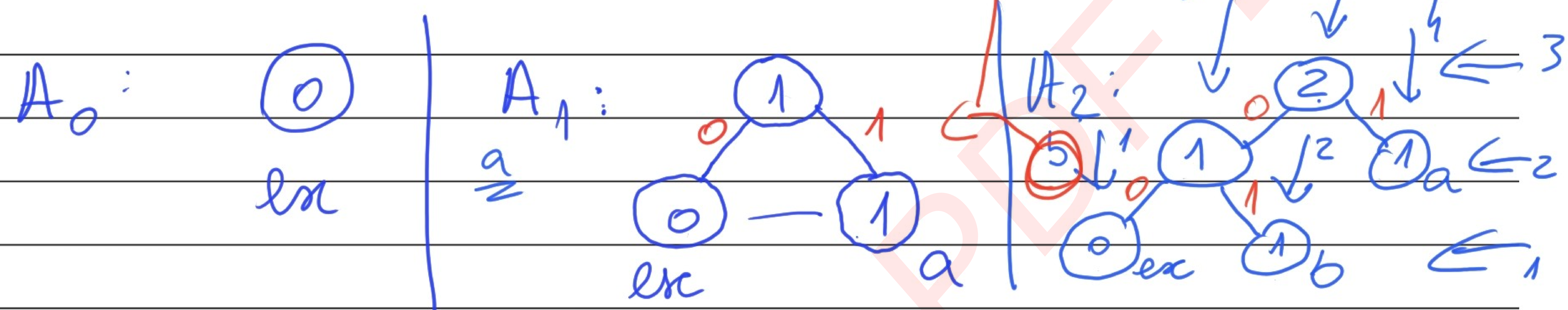
cod ex din arb. anterior

cod ex A3

cod a A4

cod c A5

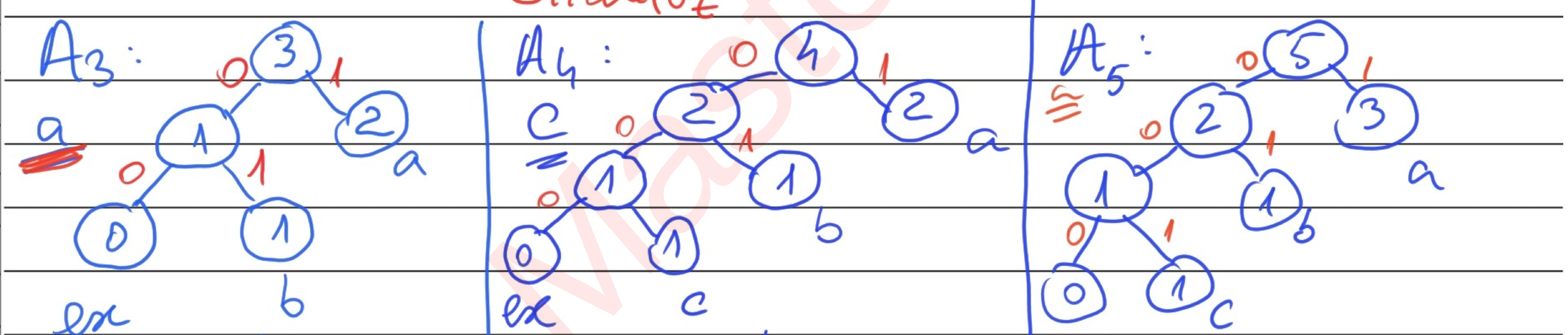
de la nod → frunză



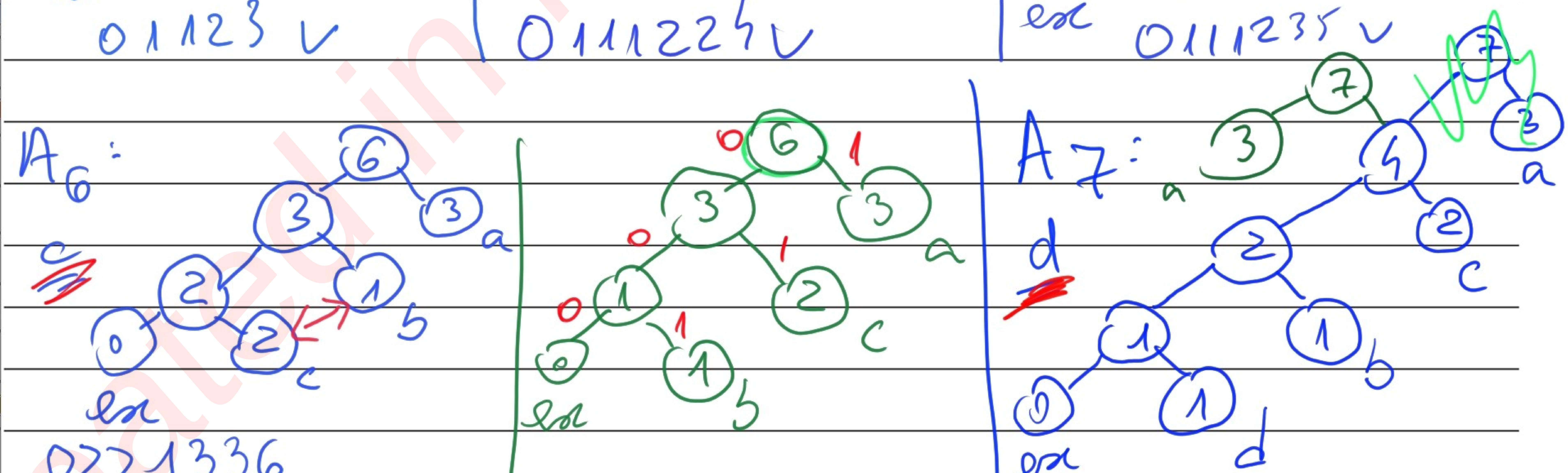
✓ Sibling jos-sus, stg, dr. → cresc.

011 ✓ 01112 ✓

Etichetez



01123 ✓ 0111224 ✓ 0111235 ✓



0221336

0112336

011122437

Cod += 000 cod ASCII d

Grupuri

Noțiuni:
- grup
- grup ciclic
- $\phi(m)$
- ordinul unui el. într-un grup ciclic
- propr. ord. unui el. în cazul $\mathbb{Z}_m^*$
- rădăcini primitive

$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$

$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$

$(\mathbb{Z}_m^*, \cdot, ^{-1}, 1)$ grup abelian ← op. asoc. și comut., elementele inversabile, element neutru

$a \in \mathbb{Z}_m^*$

$\exists a^{-1} \in \mathbb{Z}_m^*, \; a \cdot a^{-1} \equiv_m 1$ (inv. mod.)

- $ord_{\mathbb{Z}_m^*}(a) = ord_m(a) = \min\{k \mid a^k \equiv 1 \bmod m, \; k \geq 1\}$

- **Funcția lui Euler** $\phi(m) = |\mathbb{Z}_m^*|$
  - câte numere $< m$ sunt coprime cu m
  - $\phi(m)$ reprezintă ordinul grupului $\mathbb{Z}_m^*$

1) $\phi(1) = 1$
2) $\phi(p) = p - 1$, p prim
3) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, $(a, b) = 1$
4) $\phi(p^e) = p^e - p^{e-1}$, p prim
5) $\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1}) \cdot \dots \cdot (p_k^{e_k} - p_k^{e_k - 1})$, unde $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$

Dacă $ord_m(a) = t$, atunci $ord_m(a^k) = t$ ddacă $(k, t) = 1$

Ordinul unui element divide ordinul grupului

- **Rădăcini primitive**

Dacă $ord_m(a) = \phi(m)$, atunci a este rād. primitivă mod m

Câte rād. primitive există în $\mathbb{Z}_m^*$? $\phi(\phi(m))$

Grupuri - aplicații

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ $\quad \phi(7) = 7 - 1 = 6$ $\quad$ # generatori $\mathbb{Z}_m^* = \phi(\phi(m))$

$4^1 \equiv_7 4$
$4^2 \equiv_7 16 \equiv_7 2$
$4^3 \equiv_7 64 \equiv_7 1$
$4^4 \equiv_7 4$
$4^5 \equiv_7 2$
$4^6 \equiv_7 1$
$\vdots$ 4, 2, 1, ...

$ord_7(4) = 3$

$\{1, 2, 4\}$

$3^1 \equiv_7 3$
$3^2 \equiv_7 9 \equiv_7 2$
$3^3 \equiv_7 6$
$3^4 \equiv_7 4$
$3^5 \equiv_7 5$
$3^6 \equiv_7 729 \equiv_7 1$

3 rād. primitivă mod 7

$\phi(7) = 6$
$\phi(6) = \phi(2) \cdot \phi(3)$
$= 1 \cdot 2$
$= 2$

generatori $\mathbb{Z}_7^*$

$ax \equiv b \bmod m \Rightarrow m \mid ax-b \Rightarrow ax-b = m \cdot y \Leftrightarrow ax - my = b$

$ax + by = c$

$x = \alpha \cdot \frac{c}{(a,b)}$

$A \mid B \Rightarrow \exists y \in \mathbb{Z},\ B = A \cdot y$

$\Downarrow$

$x = \alpha \cdot \frac{b}{(a,m)}$

$a^{-1} \bmod m$

$a \cdot a^{-1} \bmod m = 1$

$\exists \#sol = (a,m)$ $\left(x_0 + i \cdot \frac{m}{(a,m)} \right) \bmod m$ $\quad i = \overline{1,(a,m)}$

$|\mathbb{Z}_m| = m$ $\quad \mathbb{Z}_m = \{0,1,\dots,m-1\}$

$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$

$|\mathbb{Z}_m^*| = \phi(m)$ $\quad \mathbb{Z}_m^* = \{x \in \mathbb{Z}_m \mid (x,m) = 1\}$

$ord_m(a^k) = \frac{ord_m(a)}{(k, ord_m(a))}$

a^k este rād. primitivă $\Leftrightarrow$ ordinul lui e $\phi(m)$

$\prod \left(p_i^k - p_i^{k-1} \right)$

$\mathbb{Z}_6^* = \{1, 5\}$

$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

$\phi(6) = \phi(2) \cdot \phi(3) = (2^1 - 2^0)(3^1 - 3^0) = 1 \cdot 2 = 2$

$\phi(7) = 7 - 1 = 6 = (2 \cdot 3)$

#rād. primitive $= \phi(\phi(m))$

$\phi(\phi(7)) = \phi(6) = 2$

$2^1 \equiv_7 2$

$2^2 \equiv_7 4$

$2^3 \equiv_7 1$

$\langle 2 \rangle = \{1,2,4\}$

3^1

$\vdots$

$3^{\phi(m)}$

$\frac{6}{2}$? $\quad \frac{6}{3}$

$2 \equiv_7 1 \equiv_7 2^3$ ✓

$2^{\frac{6}{3}} \not\equiv_7 1 \not\equiv_7 2^2$ ✓

2 n.p.?

$3^3 \equiv_7 27 - 21 \equiv_7 6 \not\equiv_7 1$ ✓

$3^2 \equiv_7 9 - 7 \equiv 2 \not\equiv_7 1$ ✓

$\Rightarrow$ 3 e rād. primitivă

α - este rād. primitivă $\Leftrightarrow$ $\alpha^{\frac{\phi(m)}{q}} \not\equiv 1 \bmod m,\ \forall q$

q factori ai lui $\phi(m)$

$x^m \equiv 1 \mod m$ $\quad\quad$ $\mathbb{Z}_m^* \rightarrow$ rād. pr.

$\alpha^{in} \equiv \alpha^0 \mod m$ $\quad\quad$ $in \equiv 0 \mod \phi(m)$

α este rād. pr.

$\alpha^i \mod m$, $i \in \left\{ k \cdot \frac{\phi(m)}{(m, \phi(m))} \mid 0 \leq k < (m, \phi(m)) \right\}$

x

$x^m \equiv -1 \mod p$, p prim impar

$\exists$ sol. $\Leftrightarrow (m, p-1) \mid \frac{p-1}{2}$, $\#sol = (m, p-1)$

Rescriem: $\alpha^{im} \equiv \alpha^{\frac{p-1}{2}} \mod p$, unde α e rădăcină primitivă modulo p

$in \equiv \frac{p-1}{2} \mod (p-1)$

Soluțiile: $\alpha^i \mod p$, unde $i \in \left\{ \frac{p-1}{2 \times (m, p-1)} + k \times \frac{\phi(p)}{(m, p-1)} \mid 0 \leq k < (m, p-1) \right\}$

3. Considerăm grupul multiplicativ $\mathbf{Z}_{11}^*$.

(a) Arătaţi că $\mathbf{Z}_{11}^*$ este ciclic.

(b) Câte subgrupuri are $\mathbf{Z}_{11}^*$ şi care sunt ordinele lor?

(c) Câte din subgrupurile de la punctul anterior sunt ciclice?

(d) Specificaţi câte un generator pentru fiecare dintre subgrupurile ciclice ale lui $\mathbf{Z}_{11}^*$.

(a) - def. grup ciclic

(b) $\langle x \rangle$, $x \in \mathbb{Z}_{11}^*$

(c) toate

(d) $\langle x \rangle$

(a) căutăm o rădăcină primitivă în $\mathbb{Z}_{11}^* = \{1, 2, 3, \dots, 10\}$ $\quad |\mathbb{Z}_{11}^*| = 11-1 = 10$

$\phi(11) = 10 = 2 \cdot 5$

$x^{\frac{\phi(11)}{2}}$, $x^{\frac{\phi(11)}{5}}$ unde $x \in \mathbb{Z}_{11}^*$

fie $x = 2$: $2^5 \equiv_{11} 10 \neq_{11} 1$ ✓ $\Rightarrow$ 2 este rād. pr.

$2^2 \equiv_{11} 4 \neq_{11} 1$ ✓

$\Rightarrow 2^i \bmod 11$, $i = \overline{1, \phi(11)}$ va genera tot grupul $\mathbb{Z}_{11}^*$

$2^1 \equiv_{11} 2$

$2^3 \equiv_{11} 8$

$2^7 \equiv_{11} 7$

$2^9 \equiv_{11} 6$

(b) $\phi(10) = 4 \Rightarrow$ 34 rād. primitive $\quad 2^k$, $(k, \phi(11)) \Rightarrow k \in \{1, 3, 7, 9\}$ ($\phi(11) = 10$)

$\text{ord}_{11}(2^k) = 10 \Rightarrow \langle 2^k \rangle = \mathbb{Z}_{11}^*$

$\mathbb{Z}_{11}^* - \{2, 6, 7, 8\} = \{1, 3, 4, 5, 9, 10\}$

$\text{ord}_{11}(1) = 1$ $\quad \langle 1 \rangle = \{1\}$

$\text{ord}_{11}(3) = 5$ $\quad \langle 3 \rangle = \{1, 3, 4, 5, 9\}$ $\quad 3^1 \equiv_{11} 3$ $\quad 3^2 \equiv_{11} 9$ $\quad 3^3 \equiv_{11} 5$ $\quad 3^4 \equiv_{11} 4$ $\quad 3^5 \equiv_{11} 1$

$\text{ord}_{11}(4) = 5$ $\quad \langle 4 \rangle = \{1, 3, 4, 5, 9\}$ $\quad 4^1 \equiv_{11} 4$ $\quad 4^2 \equiv_{11} 5$ $\quad 4^3 \equiv_{11} 9$ $\quad 4^4 \equiv_{11} 3$ $\quad 4^5 \equiv_{11} 1$

$\text{ord}_{11}(5) = 5$ $\quad \langle 5 \rangle = \{1, 3, 4, 5, 9\}$ $\quad 5^1 \equiv_{11} 5$ $\quad 5^2 \equiv_{11} 3$ $\quad 5^3 \equiv_{11} 4$ $\quad 5^4 \equiv_{11} 9$ $\quad 5^5 \equiv_{11} 1$

$\text{ord}_{11}(9) = 5$ $\quad \langle 9 \rangle = \{1, 3, 4, 5, 9\}$ $\quad 9^1 \equiv_{11} 9$ $\quad 9^2 \equiv_{11} 4$ $\quad 9^3 \equiv_{11} 3$ $\quad 9^4 \equiv_{11} 5$ $\quad 9^5 \equiv_{11} 1$

$\text{ord}_{11}(10) = 2$ $\quad \langle 10 \rangle = \{1, 10\}$ $\quad 10^1 \equiv_{11} 10$ $\quad 10^2 \equiv_{11} 1$

Subgrupuri ciclice: $\underset{=1}{|\{1\}|}$, $|\{1, 3, 4, 5, 9\}|$, $|\{1, 10\}|$, $|\mathbb{Z}_{11}^*| = 10$

1 $\quad$ 5 $\quad$ 2 $\quad$ 10

(c) Toate subgrupurile de la (b) sunt ciclice

(d) gen. pt $\langle 1 \rangle$ este 1. ; pt. $\{1, 3, 4, 5, 9\}$ avem generatori 3, 4, 5, 9 ; pt $\{1, 10\}$ avem 10 ca generator

iar pt. $\mathbb{Z}_{11}^*$ avem 2, 6, 7, 8 ca generatori

$\begin{cases} x \equiv 31 \bmod 50 \\ x \equiv 16 \bmod 35 \end{cases}$ $\Leftrightarrow 50 \mid (x-31) \Rightarrow \exists y,\ x-31 = 50y \Rightarrow \boxed{x = 50y+31}$

$x = 50 \cdot 27 + 31$

$31 + 50y \equiv 16 \bmod 35$

$50y \equiv 16 - 31 \bmod 35$

$50y \underset{35}{\equiv} -15 \equiv 20 \bmod 35$

$50y \equiv 20 \bmod 35 \Rightarrow 35 \mid (50y-20) \Rightarrow \exists q \in \mathbb{Z},$

$50y - 20 = 35q \Leftrightarrow 50y - 35q = 20$

Are sol $\Leftrightarrow (50, 35) \mid 20$

$5 \mid 20$ V DA.

$[50, 35] = 2 \cdot 5^2 \cdot 7 = \boxed{350}$ $\qquad \boxed{x = 331}$

$31 + 50y \equiv 16 \bmod 35 \Rightarrow$

$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \end{cases} \Leftrightarrow m_1 \mid (x - b_1) \Leftrightarrow \exists y,\ x - b_1 = m_1 y,$

$x = b_1 + m_1 y$

$b_1 + m_1 y \equiv b_2 \bmod m_2$

$m_1 y \equiv b_2 - b_1 \bmod m_2$

Are sol $\Leftrightarrow (m_1, m_2) \mid b_2 - b_1 \Leftrightarrow \boxed{b_1 \equiv b_2 \bmod (m_1, m_2)}$

ax $\qquad (m_1, m_2) \neq 1$

Dacă are sol, ea este unică mod $[m_1, m_2]$, cel mai mic multiplu comun

R.A. α_1, α_2 - 2 sol. distincte

$$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \end{cases}$$ Are soluție $\Leftrightarrow b_1 \equiv b_2 \bmod (m_1, m_2)$

$(m_1, m_2) \neq 1$

Dacă are sol., ea e unică $\bmod [m_1, m_2]$

R.A. α_1, α_2 – două sol. incongruente

$$\begin{cases} \alpha_1 \equiv b_1 \bmod m_1 \\ \alpha_1 \equiv b_2 \bmod m_2 \\ \alpha_2 \equiv b_1 \bmod m_1 \\ \alpha_2 \equiv b_2 \bmod m_2 \end{cases} \Rightarrow \begin{cases} \alpha_1 \equiv \alpha_2 \bmod m_1 \\ \alpha_1 \equiv \alpha_2 \bmod m_2 \end{cases} \Rightarrow$$

$\Rightarrow \alpha_1 \equiv \alpha_2 \bmod [m_1, m_2]$