Teoria nr cu apl. în criptografie

24-02-2024

Curs 1

- Examen scris $p \in [1,10]$
- Nota se obține prin o rotunjire standard din $p + 0{,}15 \cdot s$.
- s e nota de la seminar ($s \in [0,10]$)

Bibliografia :
1) Cursul și seminarul
2) L. Panaitopol, A. Gica - O introducere în aritmetica și teoria nr., EUB 199
3) Simon Singh - The code book., Fourth Estate 1999

Aritmetică în $\mathbb{N}$

$\boxed{T1}$ (Teorema împărțirii cu rest pentru numerele naturale)

Fie $a, b \in \mathbb{N}$ cu $b \neq 0$.
Atunci există $q, r \in \mathbb{N}$ a.î. :
i) $a = bq + r$ și
ii) $r < b$.
În plus, q și r sunt unic determinate de a, de b și de condițiile (i) și (ii).

Dem.: Considerăm mulțimea
$M \overset{not}{=} \{ u \in \mathbb{N} : \exists k \in \mathbb{N} \quad u = a - bk \}$
Avem $M \subset \mathbb{N}$ și $a \in M$, deci $M \neq \emptyset$
Ca urmare, M admite un cel mai mic element, fie el r.
Atunci există $q \in \mathbb{N}$ cu $\underbrace{r = a - bq}_{\Updownarrow}$
$a = bq + r$.

Presupunem că $r \geq b$
Atunci. $a = bq + r = b(q+1) + r - b \Rightarrow \mathbb{N} \ni r - b = a - b\underbrace{(q+1)}_{\in \mathbb{N}}$, deci $r - b \in M$ sau $r - b < r$ $\Big\}$ ⊛

Rămâne, deci, că $r < b$.
Pt. a dem. unicitatea, fie $q', r' \in \mathbb{N}$ astfel ca $a = bq' + r'$ și $r' < b$.
Atunci $bq' + r' = a = bq + r$ (1)
Presupunem că $r \neq r'$, pentru a fixa ideile, să facem $r < r'$. Atunci

$(1) \Rightarrow \mathbb{N}^* \ni \underbrace{r' - r}_{\substack{r \in \mathbb{N} \\ b - r \leq b}} = b(q - q')$ (2), deci $q > q'$

Dar $q > q' \Rightarrow q - q' \geq 1 \Rightarrow b(q-q') \geq b$

Ca urmare relația (2) e contradictorie.

Rămâne, așadar, că $\left.\begin{matrix} r = r' \\ (1) \end{matrix}\right\} \Rightarrow bq' = bq \Rightarrow b(q'-q) = 0 \xRightarrow{b \neq 0} q' = q$ ■

Def. 2 Fie $a, b \in \mathbb{N}$. Spunem că a îl divide pe b sau că a e divizor al lui b sau că b se divide prin a sau că b e multiplu a lui a dacă $\exists c \in \mathbb{N}$ $b = a \cdot c$.

Prop. 3: (Proprietăți ale relației de divizibilitate de pe $\mathbb{N}$).

(i) $\forall a \in \mathbb{N}$ $a | a$

(ii) $\forall a, b \in \mathbb{N}$ $((a | b \wedge b | a) \Rightarrow a = b)$

(iii) $\forall a, b, c \in \mathbb{N}$ $((a | b \wedge b | c) \Rightarrow a | c)$

(iv) $\forall a \in \mathbb{N}$ $a | 0$; $\forall a \in \mathbb{N}$ $(0 | a \Rightarrow a = 0)$

(v) $\forall a \in \mathbb{N}$ $1 | a$; $\forall a \in \mathbb{N}$ $(a | 1 \Rightarrow a = 1)$

(vi) $\forall a, b, k \in \mathbb{N}$ $(a | b \Rightarrow a | kb)$

(vii) $\forall a, b, c \in \mathbb{N}$ $((a | b \wedge a | c) \Rightarrow a | b + c)$

(viii) $\forall a, b, c \in \mathbb{N}$ $((a | b \wedge a | c \wedge b \geq c) \Rightarrow a | b - c)$

■

Obs 4: Proprietățile (i), (ii) și (iii) din prop. 3 spun că relația de divizibilitate este o relație de ordine pe $\mathbb{N}$.

Pentru fiecare $a \in \mathbb{N}$ vom nota $D_a = \{b \in \mathbb{N} : b | a\}$

Exemple: $D_2 = \{1, 2\}$

$D_3 = \{1, 3\}$

$D_4 = \{1, 2, 4\}$.

$D_5 = \{1, 5\}$

$D_6 = \{1, 2, 3, 6\}$.

$D_1 = \{1\}$

Obs. 5: $\forall a \in \mathbb{N}$ $(|D_a| = 1 \Leftrightarrow a = 1)$

$D_0 = \mathbb{N}$

Obs. 6: $\forall a \in \mathbb{N}$ $(|D_a| = \infty \Leftrightarrow a = 0)$

În cuvinte, D_a e mulțimea divizorilor lui a iar $D_a \cap D_b$ e mulțimea divizorilor comuni lui a și b

$D_4 \cap D_6 = \{1, 2, 4\} \cap \{1, 2, 3, 6\} = \{1, 2\}$

$D_{12} \cap D_{18} = \{1, 2, 3, 4, 6, 12\} \cap \{1, 2, 3, 6, 9, 18\} = \{1, 2, 3, 6\}$.

Fie $a, b \in \mathbb{N}^*$

Dacă $a \neq b$, să zicem, pentru a fixa ideile $a > b$, atunci:

(0): • $\exists\, q_0, r_0 \in \mathbb{N}$ $\left(a = bq_0 + r_0 \wedge r_0 < b\right)$ — $r_0 = 0$: cmmdc (a, b)

(1): • $\exists\, q_1, r_1 \in \mathbb{N}$ $\left(b = r_0 q_1 + r_1 \wedge r_1 < r_0\right)$ — $r_0 \neq 0$, $r_1 = 0$, $r_1 \neq 0$.

Scanned with CamScanner

(2): $\exists q_2, r_2 \in \mathbb{N}$ $\quad (r_0 = r_1 q_2 + r_2 \wedge r_2 < r_1)$

- - - - - -

$(m+1)$: $\exists q_{m+1}, r_{m+1} \in \mathbb{N}$ $\quad (r_{m-1} = r_m q_{m+1} + r_{m+1} \wedge r_{m+1} < r_m)$

$(m+2)$: $\exists q_{m+2} \in \mathbb{N}$ $\quad r_m = r_{m+1} q_{m+2}$

$(m+2) \Rightarrow r_{m+1} \mid r_m \overset{(m+1)}{\Longrightarrow} r_{m+1} \mid r_{m-1} \overset{(m)}{\Longrightarrow} r_{m+1} \mid r_{m-2}$.

Inductiv, $r_{m+1} \mid r_j \quad \forall j \in \{0, 1, \dots, m\} \overset{(1)}{\Longrightarrow} r_{m+1} \mid 1 \overset{(0)}{\Longrightarrow} r_{m+1} \mid a$.

Deci, $r_{m+1} \mid a$ și $r_{m+1} \mid b$. (deci r_{m+1} e divizor comun pt. a și b). (*)

În plus, fie $d \in \mathbb{N}$ un divizor comun a lui a și b

Atunci (0) $\left\{ \Rightarrow \underset{(1)}{d \mid r_0} \right\} \Rightarrow \underset{(2)}{d \mid r_1} \Big\} \Rightarrow d \mid r_2$.

Inductiv, $d \mid r_j$, $\forall j \in \{0, 1, \dots, m+1\}$, deci $d \mid r_{m+1}$, de unde $d \leq r_{m+1}$.

De aici și din (*), r_{m+1} e c.m.m.d.c. a lui a și b.

(Am folosit:

Prop. 2.5: $\forall a, b \in \mathbb{N} \quad ((a \mid b \wedge b \neq 0) \Rightarrow a \leq b)$)

Def. 7 Procedeul de mai sus, care ne furnizează cmmdc al nr. nat. nenule a și b s.n. ALGORITMUL LUI EUCLID.

Prop. 8: Date fiind $a, b \in \mathbb{N}^*$ cu $a \neq b$, cmmdc al lui a și b este ultimul rest nenul din algoritmul lui Euclid.

Obs 9: Prop. 8 e completată de următoarele prop evidente:

(i) $\forall a \in \mathbb{N}^*$ cmmdc $\{a, 0\} = a$.

(ii) $\forall a \in \mathbb{N}^*$ cmmdc $\{a, a\} = a$.

Din considerațiile din dem. afirmației algoritmului lui Euclid rezultă:

Prop. 10: Date fiind $a, b \in \mathbb{N}^*$ și $d \in \mathbb{N}$.

d e cmmdc $\{a, b\} \Leftrightarrow$ sunt îndeplinite condițiile:

(i) $d \mid a$ și $d \mid b$

(ii) $\forall d' \in \mathbb{N} \quad ((d' \mid a \wedge d' \mid b) \Rightarrow d' \mid d)$

Din aceste motive, vom folosi pt. cmmdc a 2 nr. nat urm. def.:

Def. 11 Fie $a, b \in \mathbb{N}$. Un nr. $d \in \mathbb{N}$ s.n. cel mai mare div com. a lui a și b dacă:

(i) $d \mid a \wedge b \mid b$

(ii) $\forall d' \in \mathbb{N} \quad ((d' \mid a \wedge d' \mid b) \Rightarrow d' \mid d)$

Obs 12 Cu această def. cmmdc$(0, 0) = 0$.

Prop. 13: $\forall$ 2 nr. nat. admit un unic cmmdc.

Scanned with CamScanner

Teoria numerelor cu
apl. în criptografie

12-03-2024

Curs 3

Def. 1 Partea întreagă a nr. real x = cel mai mare nr. întreg care nu-l întrece pe x

Notație: $[x]$ (în România, în engleză $\lfloor x \rfloor$)

Obs 2: $\forall x \in \mathbb{R}$, $[x] \leq x \leq [x]+1$.

Def 3: Partea fracționară a nr. real x = numărul $\{x\} \overset{not.}{=} x-[x]$.

Obs. 4: $\forall x \in \mathbb{R}$ $\{x\} \in [0,1)$

Prop. 5 (Proprietățile părții întregi):

(i) $\forall x \in \mathbb{R}$ $\forall m \in \mathbb{Z}$ $[x+m] = [x]+m$

(ii) $\forall x, y \in \mathbb{R}$ $[x+y] \in \{[x]+[y], [x]+[y]+1\}$.

(iii) $\forall x \in \mathbb{R}$ $\forall m \in \mathbb{N}^*$ $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$.

Prop. 6: Fie $a, x \in \mathbb{R}$. Atunci:

$$a = [x] \Leftrightarrow (a \in \mathbb{Z} \wedge a \leq x < a+1)$$
$$\Leftrightarrow (a \in \mathbb{Z} \wedge x-1 < a \leq x)$$

Dem. prop. 6: E evidentă din definiția def. părții întregi $\square$

Dem. prop. 5: (i) Fie $x \in \mathbb{R}$, fie $m \in \mathbb{Z}$

Atunci $[x] \leq x < [x]+1$, de unde $[x]+m \leq x+m < ([x]+m)+1$.

Ca urmare, $[x+m] = [x]+m$.

(ii) Fie $x, y \in \mathbb{R}$. Atunci $\{x\}+\{y\} \in [0,2)$

Dacă $\{x\}+\{y\} \in [0,1)$, $[x+y] = [[x]+\{x\}+[y]+\{y\}] = [x]+[y]+[\underbrace{\{x\}+\{y\}}_{\in[0,1)}] =$
$= [x]+[y]$.

Dacă $\{x\}+\{y\} \in [1,2)$, $[x+y] = [[x]+\{x\}+[y]+\{y\}] = [x]+[y]+[\underbrace{\{x\}+\{y\}}_{\in[1,2)}] = [x]+[y]+1$.

(iii) Fie $x \in \mathbb{R}$, $m \in \mathbb{N}^*$.

Atunci $\frac{x}{m} = \frac{[x]+\{x\}}{m} \in \left[\frac{[x]}{m}, \frac{[x]+1}{m}\right) = (1)$

Punând $\lambda = \frac{[x]}{m}$, $\frac{[x]}{m} = \lambda + \frac{[x]}{m} - \lambda = \lambda + \frac{[x]-m\lambda}{m} \in [0,1)$ $\left(\Leftrightarrow \frac{[x]-m\lambda}{m} \leq \frac{m-1}{m}\right)$

Deci, $(1) = \left[\lambda + \frac{[x]-m\lambda}{m}, \lambda + \underbrace{\frac{[x]-m\lambda+1}{m}}_{\leq 1}\right) \subset [\lambda, \lambda+1)$

Ca urmare, $\left[\frac{x}{m}\right] = \lambda = \left[\frac{[x]}{m}\right]$ $\square$.

Scanned with CamScanner

T7 (Teorema împărțirii cu rest pentru numere întregi)

Pentru orice $a, b \in \mathbb{Z}$ cu $b \neq 0$ există $q, r \in \mathbb{Z}$ a.î.:

(i) $a = bq + r$

și (ii) $0 \leq r < |b|$

Mai mult, q și r sunt unic determinate de a, de b și de condițiile (i) și (ii).

Dem.: Fie $a, b \in \mathbb{Z}$ cu $b \neq 0$.

Conform TIR pentru numere naturale, există $q', r' \in \mathbb{N}$ a.î. $|a| = |b|q' + r'$ și $r' < |b|$.

1. Dacă $a \geq 0$, $b > 0$:

Luăm $q = q'$ și $r = r'$.

Atunci $a = |a| = |b|q' + r' = bq + r$. (iar $r = r'$, deci $0 \leq r < |b|$)

2. Dacă $a \geq 0$, $b < 0$:

Luăm $q = -q'$, $r = r'$

Atunci $a = |a| = |b|q' + r' = bq + r$, iar $r = r'$ deci $0 \leq r < |b|$.

3. Dacă $a < 0$, $b > 0$:

3.1. Dacă $r' \neq 0$.

Luăm $q = -q' - 1$ și $r = b - r'$ $\in (0, b)$, avem $r \in (0, b) \Rightarrow 0 \leq r \leq b$.

Atunci $a = -|a| = -|b|q' - r' = -bq' - r' = b \cdot (-q') - r' = b(-q-1) + b - r' = bq + r$

3.2. Dacă $r' = 0$

Luăm $q = -q'$, $r = 0 \in [0, b) = [0, |b|)$

Atunci $a = -|a| = -|b|q' = b \cdot (-q')$

4. Dacă $a < b$ și $b < 0$:

4.1. Dacă $r' \neq 0$

Luăm $q = q' + 1$ și $r = -b - r'$ $\in (-|b|, 0)$ $\in [0, |b|)$

Atunci $a = -|a| = -|b|q' - r' = b \cdot q' - r' = b(q'+1) - b - r' = bq + r$

4.2. Dacă $r' = 0$

Luăm $q = q'$, $r = 0 \in [0, |b|)$

și avem $a = -|a| = -|b|q' = bq' = bq + r$.

Unicitatea: Fie $q_{1,2} \in \mathbb{Z}$ și $r_1, r_2 \in \mathbb{Z} \cap [0, |b|)$ cu $bq_1 + r_1 = a = bq_2 + r_2$

Atunci $b(q_1 - q_2) = r_2 - r_1 \in (-|b|, |b|)$

Dacă, prin absurd, $q_1 \neq q_2$, atunci $|b(q_1 - q_2)| = |b| \underbrace{|q_1 - q_2|}_{\geq 1} \geq |b|$, ceea ce contrazice (2)

Rămâne, deci, că $q_1 = q_2$ și din (2) obținem și $r_1 = r_2$. □.

Uneori ne e utilă o variantă a TIR și anume

T7' (Varianta a TIR pt. nr. întregi)

Pt. $\forall$ $a, b \in \mathbb{Z}$ cu $b \neq 0$, există $c, d \in \mathbb{Z}$ a.î.:

(i) $a = b \cdot c + d$

și (ii) $-\frac{|b|}{2} < d \leq \frac{|b|}{2}$

Scanned with CamScanner

În plus, c și r sunt unic determinate de a, de b și de relațiile (i) și (ii).

Dem.: Fie a, b ca în enunț.

Potrivit TIR pt. nr. întregi, există $q, r \in \mathbb{Z}$ a.î. $a = bq + r$ și $0 \le r < |b|$.

Dacă $r \le \frac{|b|}{2}$, punem $c = q$ și $d = r$ și gata.

Dacă $r > \frac{|b|}{2}$, atunci punem $c = q + \frac{|b|}{b}$ și $d = r - |b| \in \left(\frac{|b|}{2} - |b|, |b| - |b|\right) = \left(-\frac{|b|}{2}, 0\right)$

și avem $a = bq + r = bq + |b| + r - |b| = b\left(q + \frac{|b|}{b}\right) + r - |b| = bc + d$

Unicitatea se probează similar ca cea de la T7. □.

Divizibilitate în $\mathbb{Z}$

Def. 8: Fie $a, b \in \mathbb{Z}$. Spunem că a îl divide pe b
sau că
a e divizor al lui b
sau că
b se divide prin a
sau că
b e multiplu al lui a

dacă există $c \in \mathbb{Z}$ a.î. $b = ac$.

Notăm faptul că a divide b cu $a|b$ (sau cu $b \vdots a$, citit. cel mai adesea "b se divide prin a")

Prop 9: Fie $a, b \in \mathbb{Z}$. Atunci $a|_{\mathbb{Z}} b \iff |a| \,|_{\mathbb{N}}\, |b|$.

Dem.: "$\Rightarrow$" Cum $a|_{\mathbb{Z}} b$, $\exists c \in \mathbb{Z}$ $b = ac$. Atunci $|b| = |a|\underbrace{|c|}_{\in \mathbb{N}}$, deci $|a| \,|_{\mathbb{N}}\, |b|$.

"$\Leftarrow$" Din ipoteză, $\exists \gamma \in \mathbb{N}$ $|b| = |a| \cdot \gamma$. Atunci $b = a\gamma$ sau $b = -a\gamma = a \cdot (-\gamma)$,

?? $\pm\gamma \in \mathbb{Z}$. La urmare, $a|_{\mathbb{Z}} b$ □

Prop. 10: Proprietăți ale divizibilității din $\mathbb{Z}$.

(i) $\forall a \in \mathbb{Z}$ $a|_{\mathbb{Z}} a$

(ii) $\forall a, b \in \mathbb{Z}$ $(a|b \wedge b|a \Rightarrow |a| = |b|)$

(Prop. 9: $a|_{\mathbb{Z}} b \wedge b|_{\mathbb{Z}} a \Rightarrow (|a| \,|_{\mathbb{N}}\, |b| \wedge |b| \,|_{\mathbb{N}}\, |a|) \Rightarrow |a| = |b|$)

(iii) $\forall a, b, c \in \mathbb{Z}$ $((a|b \wedge b|c) \Rightarrow a|c)$

(iii') $\forall a, b, k \in \mathbb{Z}$ $(a|b \Rightarrow a|bk)$

(iv) $\forall a \in \mathbb{Z}$ $a|0$; $\forall a \in \mathbb{Z}$ $(0|a \Rightarrow a = 0)$

(v) $\forall a \in \mathbb{Z}$ $a|a$; $\forall a \in \mathbb{Z}$ $(a|1 \Rightarrow |a| = 1)$

(vi) $\forall a \in \mathbb{Z}$ $\forall b, c, \beta, \gamma \in \mathbb{Z}$
$((a|b \wedge a|c) \Rightarrow a|\beta b + \gamma c)$

Obs 11: Proprietatea (ii) ne arată că, spre deosebire de divizibilitatea de pe $\mathbb{N}$, cea de pe $\mathbb{Z}$ NU este antisimetrică.

Scanned with CamScanner

Def. 12 Fie $a, b \in \mathbb{Z}$. Spunem că a și b sunt <u>asociate în divizibilitate</u> dacă $a|b \wedge b|a$.

Prop. 13: Fie $a, b \in \mathbb{Z}$. Atunci a e asociat în divizibilitate cu b ddacă $|a| = |b|$.

<u>Notație</u>: $a \sim b$ pt. $a|b \wedge b|a$.

<u>Dem. prop. 13</u>: "$\Rightarrow$" rezultă din prop. 10, (ii)

"$\Leftarrow$" cf. prop. 9 $\square$

Obs 14: Relația de asociere în divizibilitate pe $\mathbb{Z}$ e o relație de echivalență.

Obs. 15: $\frac{\mathbb{Z}}{\sim}$ "este perfect reprezentată" de $\mathbb{N}$.

Observația 15 și prop. 9 sunt afirmații tehnice care susțin afirmația "intuitivă dar foarte sugestivă":

Divizibilitatea din $\mathbb{Z}$ e esențialmente ace din $\mathbb{N}$.

Def. 16: Fie $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Spunem că m e <u>ireductibil</u> dacă $\forall a, b \in \mathbb{Z}$ $m = ab \Rightarrow$
$\Rightarrow (|a| = 1 \vee |b| = 1)$

Prop. 17: Fie $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Atunci m e ireductibil ddacă $|m|$ e ireductibil în $\mathbb{N}$.

<u>Dem.</u>: "$\Rightarrow$": Fie $a, b \in \mathbb{N}$ cu $|m| = ab$

Atunci $m = \pm a \cdot b$, deci $|a| = |\pm a| = 1$ sau $|b| = 1$. De unde $a = 1$ sau $b = 1$

La urmare, $|m|$ e ireductibil (în $\mathbb{N}$).

"$\Leftarrow$". Fie $a, b \in \mathbb{Z}$ cu $m = ab$.

Atunci $|m| = |a| \cdot |b|$, deci $|a| = 1$ sau $|b| = 1$.

La urmare, m e ireductibil (în $\mathbb{Z}$) $\square$.

Def. 18: Fie $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Spunem că m e prim dacă $\forall a, b \in \mathbb{Z}$ $(m | ab \Rightarrow (m | a \vee m | b))$.

Prop. 19: Fie $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Atunci m e prim ddacă $|m|$ e prim în $\mathbb{N}$.

(Dem: la prop. 17).

Drept consecință a acestor

Prop. 20: Fie $m \in \mathbb{Z}$. Atunci: m e prim ddacă m e ireductibil.

Dem. m e prim (în $\mathbb{Z}$) ddacă $|m|$ e prim în $\mathbb{N}$
ddacă $|m|$ e ired. în $\mathbb{N}$
ddacă m e ired. (în $\mathbb{Z}$).

Aplicând aceste și t. fundam. a

T21: Pt. $\forall m \in \mathbb{Z} \setminus \{-1, 0, 1\}$ există și sunt unic det. de m, un nr. $\varepsilon \in \{-1, 1\}$, un nr. $n \in \mathbb{N}^*$, numerele prime naturale distincte $p_1, p_2, \dots, p_n$ și nr. nat. nenule $\alpha_1, \alpha_2, \dots \alpha_n$ a.î.:

$$m = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

Scanned with CamScanner

Teoria numerelor cu apl. în criptografie

19-03-2024

Cursul 4

Din Teorema Fundamentală a Aritmeticii pt. $\mathbb{Z}$ rezultă imediat și:

$\boxed{T1}$: Pentru orice $n \in \mathbb{Z}^* \setminus \{-1,1\}$ există $\varepsilon \in \{-1,1\}$, $k \in \mathbb{N}^*$, $p_1, \dots, p_k \in \mathbb{Z}$ numere prime distincte și $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ astfel că

$$n = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

În plus, k și $\alpha_1, \dots, \alpha_k$ sunt unic determinați de n, iar $p_1, \dots, p_k$ sunt determinate de n până la o asociere în divizibilitate.

Rezultatul nu e, însă, "le fel de precis", ca teoremele din cursul 3, din cauză că "se pierde unicitatea pentru o parte din elementele componente ale scrierii".

Def. 2 Fie $a, b \in \mathbb{Z}$. Un element d al lui $\mathbb{Z}$ s.n. cel mai mare divizor comun pentru a și b dacă (i) $d|a \wedge d|b$

și (ii) $\forall \delta \in \mathbb{Z}$ $((\delta|a \wedge \delta|b) \Rightarrow \delta|d)$

Prop. 3: Fie $a, b \in \mathbb{Z}$; fie $d \in \mathbb{Z}$. Sunt echivalente:

(i) d e cel mai mare divizor comun pt. a și b.

(ii) $|d|$ ——— " ——— în $\mathbb{N}$ pentru $|a|$ și $|b|$.

Dem.: $\underline{(i) \Rightarrow (ii)}$: Știm $d|_{\mathbb{Z}} a$ și $d|_{\mathbb{Z}} b$

Atunci $|d|\,|_{\mathbb{N}}\,|a|$ și $|d|\,|_{\mathbb{N}}\,|b|$.

Fie $\delta \in \mathbb{N}$ cu $\delta|_{\mathbb{N}}|a|$ și $\delta|_{\mathbb{N}}|b|$.

Atunci $\delta|_{\mathbb{Z}}|a|\,|_{\mathbb{Z}}\,a$ și $\delta|_{\mathbb{Z}}|b|\,|_{\mathbb{Z}}\,b$.

Din ipoteză: $\delta|_{\mathbb{Z}} d$ deci $\delta = |\delta|\,|_{\mathbb{N}}|d|$.

$(ii) \Rightarrow (i)$ Cum $|d|\,|_{\mathbb{N}}\,|a|$ și $|d|\,|_{\mathbb{N}}\,|b|$ obținem $d|_{\mathbb{Z}} a$ și $d|_{\mathbb{Z}} b$.

Fie $\delta \in \mathbb{Z}$ astfel ca $\delta|_{\mathbb{Z}} a$ și $\delta|_{\mathbb{Z}} b$.

Atunci $|\delta|\,|_{\mathbb{N}}\,|a|$ și $|\delta|\,|_{\mathbb{N}}\,|b|$; cum $|d|$ e cmmdc în $\mathbb{N}$ pt. $|a|$ și $|b|$, obținem $|\delta|\,|_{\mathbb{N}}\,|d|$ de unde $\delta|_{\mathbb{Z}} d$. $\square$

De aici obținem:

$\boxed{T4}$: Orice două nr. întregi admit c.m.m.d.c.

Dem: Un c.m.m.d.c$_{\mathbb{Z}}$ (a,b) = c.m.m.d.c$_{\mathbb{N}}$ $(|a|, |b|)$ $\square$

Prop. 5: Fie $a, b \in \mathbb{Z}$ și fie d', d'' c.m.m.d.c pt. a și b. Atunci $d' \sim d''$.

Dem: $\left.\begin{array}{l} \text{Cum } d' \text{ e c.m.m.d.c pt. } a \text{ și } b,\ d''|d' \\ \text{Cum } d'' \text{ e c.m.m.d.c pt. } a \text{ și } b,\ d'|d'' \end{array}\right\} \Rightarrow d' \sim d''$ $\square$

Prop. 6: Date fiind două nr. întregi a și b, ele admit drept c.m.m.d.c exact numerele:

$$-(|a|, |b|)_{\mathbb{N}} \text{ și } (|a|, |b|)_{\mathbb{N}}.$$

Notație: Vom nota cu (a,b) oricare din numerele din prop. 6.

Scanned with CamScanner

$\boxed{T7}$: $\forall a,b \in \mathbb{Z}$ $\exists \alpha, \beta \in \mathbb{Z}$. $(a,b) = \alpha a + \beta b$.

Dem.: Dacă $a=0$, luăm $\alpha=1$, $\beta=1$.

I am considerat, tacit, că $(a,b)=b$.

Dacă, cumva, doresc într-o anumită situație să consider $(a,b)=-b$, iau pt. $\alpha=1$, $\beta=-1$.)

Dacă $b=0$, luăm $\alpha=1$, $\beta=1$.

Dacă $|a|=|b|\neq 0$, luăm $\alpha=\pm 1$, $\beta=0$.

Dacă $a,b \in \mathbb{Z}^*$ și $|a|\neq|b|$, aplicăm algoritmul lui Euclid pt. $|a|$ și $|b|$.

$|a| = |b|\cdot q_0 + r_0 \iff r_0 = |a| - q_0|b|$. Punem: $\alpha_0 = 1$; $\beta_0 = -q_0$.

$|b| = r_0 q_1 + r_1 \iff r_1 = |b| - r_0 q_1 = -q_1|a| + (1+q_0q_1)|b|$. $\alpha_1 = -q_1$; $\beta_1 = 1+q_0q_1$.

$r_0 = r_1 q_2 + r_2$

. . . . .

$r_{j-2} = r_{j-1} q_j + r_j$

. . . . .

$r_{m-1} = r_m q_{m+1} + r_{m+1}$

$r_m = r_{m+1} q_{m+2}$

și avem $r_0 = \alpha_0|a| + \beta_0|b|$

și $r_1 = \alpha_1|a| + \beta_1|b|$

Presupunem că, pt. fiecare $k \in \{0,1,\dots,j-1\}$ $(j \leq m+1)$ am găsit α_k și β_k cu $r_k = \alpha_k|a| + \beta_k|b|$.

Atunci $r_j = r_{j-2} - q_j r_{j-1} \iff r_j = (\alpha_{j-2}|a| + \beta_{j-2}|b|) - q_j(\alpha_{j-1}|a| + \beta_{j-1}|b|) =$

$= (\alpha_{j-2} - q_j\alpha_{j-1})|a| + (\beta_{j-2} - q_j\beta_{j-1})|b|$.

Definim $\alpha_j = \alpha_{j-2} - q_j\alpha_{j-1}$ și $\beta_j = \beta_{j-2} - q_j\beta_{j-1}$ și obținem $r_j = \alpha_j|a| + \beta_j|b|$.

Ca urmare, existența de constante α_k, β_k cu $r_k = \alpha_k|a| + \beta_k|b|$ e probată pt. orice $k \in \{0,1,\dots,m+1\}$, deci, în particular, pt. $k=m+1$.

Pentru a obține $(a,b) = r_{m+1} = \alpha_{m+1}a + \beta_{m+1}b$ nu mai trebuie decât să "mutăm" eventualele semne "−" de la a la α_{m+1} și/sau de la b la β_{m+1}. □

Def. 8: Fie $a,b,m \in \mathbb{Z}$. Spunem că m e cel mai mic multiplu comun pt. a și b dacă

(i) $a|m \wedge b|m$

și (ii) $\forall \mu \in \mathbb{Z}$ $((a|\mu \wedge b|\mu) \Rightarrow m|\mu)$.

Prop. 9: Fie $a,b,m \in \mathbb{Z}$. Sunt echivalente:

(i) m e cmmmc (în $\mathbb{Z}$) pt. a și b

(ii) $|m|$ e —— " —— în $\mathbb{N}$ pt. $|a|$ și $|b|$.

Dem: Similară cu cea a Prop. 3. □.

$\boxed{T10}$: Orice 2 nr. întregi admit cmmmc.

Dem.: Un cmmmc pt. a și b e cmmmc$_{\mathbb{N}}(|a|,|b|)$.

Prop. 11: Fie $a,b \in \mathbb{Z}$ și $m', m'' \in \mathbb{Z}$ doi cmmmc pt. a și b. Atunci $m' \sim m''$.

Dem: Ca la prop. 5. □.

Prop. 12: Date fiind nr. întregi a și b, ele admit drept cmmmc exact nr.

$-[|a|,|b|]_{\mathbb{N}}$, și $[|a|,|b|]_{\mathbb{N}}$

Vom nota cu $[a,b]$ oricare din nr. din Prop. 12.

Scanned with CamScanner

Prop. 13: $\forall a, b \in \mathbb{Z}$, $(a,b)\cdot[a,b] \sim ab$.

Readucem în discuție valorile v_p. Ele se pot extinde după cum urmează.

Fie $p \in \mathbb{N}$ un nr. prim.

Definim $\bar{v}_p : \mathbb{Z}^* \to \mathbb{Z}$, $\bar{v}_p(n) = v_p(|n|) = \max\{k \in \mathbb{N} : p^k \mid n\}$

Obs 14: Pt. orice $p \in \mathbb{N}$ prim și orice $n \in \mathbb{Z}^*$ $\bar{v}_p(-n) = \bar{v}_p(n)$

Prop. 15: Fie $p \in \mathbb{N}$ prim. Atunci:

(i) $\forall m, n \in \mathbb{Z}^*$ $(m+n \neq 0 \Rightarrow \bar{v}_p(m+n) \geq \min\{\bar{v}_p(m), \bar{v}_p(n)\}$.

(i') $\forall m, n \in \mathbb{Z}^*$ $(m-n \neq 0 \Rightarrow \bar{v}_p(m-n) \geq \min\{\bar{v}_p(m), \bar{v}_p(n)\}$.

(ii) $\forall m, n \in \mathbb{Z}^*$ $((m+n \neq 0 \wedge \bar{v}_p(m) \neq \bar{v}_p(n)) \Rightarrow \bar{v}_p(m+n) = \min\{\bar{v}_p(m), \bar{v}_p(n)\}$.

(ii') $\forall m, n \in \mathbb{Z}^*$ $((m-n \neq 0 \wedge \bar{v}_p(m) \neq \bar{v}_p(n)) \Rightarrow \bar{v}_p(m-n) = \min\{\bar{v}_p(m), \bar{v}_p(n)\}$

(iii) $\forall m, n \in \mathbb{Z}^*$ $\bar{v}_p(mn) = \bar{v}_p(m) + \bar{v}_p(n)$.

Dem: Similară cu/ce reduce la cea a prop. similare de la v_p..

$\mathcal{P} \overset{not.}{=} \{p \in \mathbb{N} : p \text{ e prim}\}$.

Prop. 16: (i) $\forall m, n \in \mathbb{Z}^*$ $m \mid n \Leftrightarrow (\forall p \in \mathcal{P}\ \bar{v}_p(m) \leq \bar{v}_p(n))$

(ii) $\forall n \in \mathbb{Z}^*$ $n = 1 \Leftrightarrow (\forall p \in \mathcal{P}\ \bar{v}_p(n) = 0)$

"Cu $\bar{v}_p$" obținem și următoarea reformulare a teoremei fundamentale a aritmeticii:

$\boxed{T17}$: $\forall n \in \mathbb{N}^*$ $n = \operatorname{sgn}(n) \prod_{p \in \mathcal{P}} p^{\bar{v}_p(n)}$.

De fapt, valorile v_p (și/sau $\bar{v}_p$) se pot extinde chiar la $\mathbb{Q}^*$, după cum urmează:

• Observăm următoarele:

Dacă, pt. $r \in \mathbb{Q}^*$, avem $\frac{a}{s} = r = \frac{b}{t}$, $a, b, s, t \in \mathbb{Z}$, atunci $at = bs$, deci pt. $p \in \mathcal{P}$

$\bar{v}_p(at) = \bar{v}_p(bs) \Rightarrow \bar{v}_p(a) + \bar{v}_p(t) = \bar{v}_p(b) + \bar{v}_p(s) \Rightarrow \bar{v}_p(a) - \bar{v}_p(s) = \bar{v}_p(b) - \bar{v}_p(t)$.

Aceste lucruri ne sugerează că funcția:

$\vartheta_p : \mathbb{Q}^* \to \mathbb{Z}$, $\vartheta_p\left(\frac{a}{b}\right) = \bar{v}_p(a) - \bar{v}_p(b)$ $\forall a, b \in \mathbb{Z}^*$ e corect definită.

Def. 18: Dat fiind $p \in \mathcal{P}$, funcția $\vartheta_p : \mathbb{Q}^* \to \mathbb{Z}$, $\vartheta_p\left(\frac{a}{b}\right) = \bar{v}_p\left(\frac{a}{b}\right) = \bar{v}_p(a) - \bar{v}_p(b)$ $\forall a, b \in \mathbb{Z}^*$.

s.n. valuarea pe $\mathbb{Q}^*$ asociată lui p.

Obs. 19: $\forall r \in \mathbb{Q}^*$ $\vartheta_p(-r) = \vartheta_p(r)$

Prop. 20: Se mențin proprietățile din Prop. 15 pt. orice $m, n \in \mathbb{Q}^*$.

(i): $\vartheta_p(m+n) \underset{a,b,s,t \in \mathbb{Z}^*}{\overset{m=\frac{a}{s},\ n=\frac{b}{t}}{=}} \vartheta_p\left(\frac{at+bs}{st}\right) = \bar{v}_p(at+bs) - \bar{v}_p(st) \geq \min\{\bar{v}_p(at) - \bar{v}_p(st), \bar{v}_p(bs) - \bar{v}_p(st)\} = \min\{\vartheta_p\left(\frac{a}{s}\right), \vartheta_p\left(\frac{b}{t}\right)\}$. $\square$

Scanned with CamScanner

Prop. 21: $\forall n \in \mathbb{Q}^*$ $\quad n \in \mathbb{Z}^* \Leftrightarrow (\forall p \in \mathcal{P}\ \ \nu_p(n) \geq 0)$. $\square$

$\boxed{T22}$: $\forall n \in \mathbb{Q}^*$ $\quad n = \operatorname{sgn}(n) \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$.

Congruențe

condiție "de comoditate" ca să evităm tratarea separată a anumitor în viitor!

Def. 23 Fie $a, b \in \mathbb{Z}$ și $m \in \mathbb{N}$, $m \geq 2$. Spunem că <u>a e congruent modulo m cu b</u> dacă $m \mid b-a$.

Prop. 24: (Proprietăți ale congruențelor)

Fie $m, n \in \mathbb{N}$, $m, n \geq 2$.

(i) $\forall a \in \mathbb{Z}$ $\quad a \equiv a \pmod m$ $\square$.

(ii) $\forall a, b \in \mathbb{Z}$ $\quad (a \equiv b \pmod m \Rightarrow b \equiv a \pmod m)$

(iii) $\forall a, b, c \in \mathbb{Z}$ $\quad ((a \equiv b \pmod m \wedge b \equiv c \pmod m) \Rightarrow a \equiv c \pmod m)$

Obs. 24,5: (i), (ii), (iii) zic că congruența $(\bmod m)$ e o rel. de echivalență. Ea este, de fapt, cea a cărei mulțime factor e $\mathbb{Z}_m$. Ca urmare

$$\boxed{a \equiv b \pmod m \Leftrightarrow \hat{a} = \hat{b} \quad (\text{în } \mathbb{Z}_m)}$$

Vom face uz de această echivalență în mod repetat pentru a "transporta" problema în zona în care dispunem de teoria mai eficientă pt. rezolvarea ei!

(iv) $\forall a, b, c, d \in \mathbb{Z}$ $\quad ((a \equiv b \pmod m \wedge c \equiv d \pmod m) \Rightarrow a + c \equiv b + d \pmod m)$ $\square$

(v) $\forall a, b, c, d \in \mathbb{Z}$ $\quad ((a \equiv b \pmod m \wedge c \equiv d \pmod m) \Rightarrow ac \equiv bd \pmod m)$

<u>Dem</u>: Știu $\left.\begin{array}{l} m \mid b-a \Rightarrow m \mid bc - ac \\ m \mid d-c \Rightarrow m \mid bd - bc \end{array}\right\} \Rightarrow m \mid bd - ac$ $\square$

(vi) $\forall a, b, k \in \mathbb{Z}$ $\quad (a \equiv b \pmod m \Rightarrow ak \equiv bk \pmod m)$ $\square$

(vii) $\forall a, b \in \mathbb{Z}$ $\quad \forall k \in \mathbb{N}^*$ $(a \equiv b \pmod m \Rightarrow a^k \equiv b^k \pmod m)$

((v) + inducție) $\square$

(viii) $\forall a, b \in \mathbb{Z}$, $s \in \mathbb{Z}$ $\quad (a \equiv b \pmod m \Leftrightarrow as \equiv bs \pmod{ms})$

(ix) $\forall a, b \in \mathbb{Z}$, $\quad ((a \equiv b \pmod m \wedge a \equiv b \pmod n) \Rightarrow a \equiv b \pmod{[m, n]})$ $\square$.

(x) $\forall a, b \in \mathbb{Z}$, $\forall k \in \mathbb{Z}$ $\quad ((ak \equiv bk \pmod m \wedge (m, k) = 1) \Rightarrow a \equiv b \pmod m)$.

Def. 25: Fie $m \geq 2$, $m \in \mathbb{N}$ și fie $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ s.n. invers modulo m pt. a dacă $ab \equiv 1 \pmod m$.

Def. 26: În contextul din Def 25, a s.n. inversabil modulo m dacă el admite măcar un invers modulo m.

Scanned with CamScanner

~~Teor~~

Prop-27: Fie $m \in \mathbb{N}$, $m \geq 2$ și $a \in \mathbb{Z}$ inversabil modulo m. Atunci, dacă b și c sunt inverși modulo m pt. a, avem $b \equiv c \pmod m$.

Dem.: Știu $ab \equiv 1 \pmod m$ și $ac \equiv 1 \pmod m$

Deci $ab \equiv ac \pmod m \overset{b}{\Rightarrow} \underbrace{bab}_{1} \equiv \overbrace{bac}^{1} \pmod m \Rightarrow b \equiv c \pmod m$ □.

T28: Fie $m \in \mathbb{N}$, $m \geq 2$ și $a \in \mathbb{Z}$. Atunci a e inversabil mod m dacă $(a, m) = 1$.

Dem.: "$\Rightarrow$" Știu că $\exists\, a'$ a.î. $aa' \equiv 1 \pmod m$

At. $m \mid aa' - 1$, deci $\exists\, k \in \mathbb{Z}$ $aa' - 1 = km \Leftrightarrow$

$\exists\, k \in \mathbb{Z}$ $aa' - km = 1$ (1)

Inv (a, m) MS. din (1) deci, $(a, m) = 1$.

"$\Leftarrow$" Știu $(a, m) = 1 \overset{T.10?}{\Rightarrow} \exists\, \alpha, \gamma \in \mathbb{Z}$ $\alpha a + \gamma m = 1$.

At. $\alpha a - 1 = \gamma m \mid m$, deci $\alpha a \equiv 1 \pmod m$.

(xi) $\forall a, b \in \mathbb{Z}$ $((a \equiv b \pmod m$ și $a \equiv b \pmod n \wedge (m, n) = 1) \Rightarrow a \equiv b \pmod{mn})$.

Scanned with CamScanner

Cursul 5

Reprezentarea numerelor în baze de numerație

$37485 = 3\cdot 10^4 + 7\cdot 10^3 + 4\cdot 10^2 + 8\cdot 10 + 5$

Pe tot parcursul acestei discuții, b va desemna un nr. natural mai mare decât 1.

Fie $n \in \mathbb{N}$.

Cf. TÎR, $\exists q, r \in \mathbb{N}$ $(n = bq + r \wedge r \in \{0, 1, \dots, b-1\})$.

Notăm $a_0 = r$.

(Notăm $\beta = b-1$)

Dacă $n = a_0$, $q = 0$ și ne oprim.

Dacă $n \neq a_0$, $q \neq 0$ și cf. TÎR, $\exists q_1, r_1$ $q = q_1 b + r_1$.

(Atunci $n = (q_1 b + r_1) b + a_0 = q_1 b^2 + r_1 b + a_0$)

Punem $a_1 = r_1$, obținem $n = q_1 b^2 + a_1 b + a_0$.

Dacă $q_1 = 0$ ne oprim

Dacă $q_1 \neq 0$, presupunem $a_0, a_1, \dots, a_k, q_k$ așa încât $a_0, a_1, \dots, a_k \in \{0, 1, \dots, \beta\}$. $q_k \in \mathbb{N}$ și $n = q_k b^{k+1} + a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$.

Dacă $q_k = 0$, $n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$.

Dacă $q_k \neq 0$, cf. TÎR $\exists q_{k+1}, r_{k+1} \in \mathbb{N}$ $(r_{k+1} \in \{0, 1, \dots, \beta\} \wedge q_k = b q_{k+1} + r_{k+1})$

Punem $a_{k+1} = r_{k+1}$ și obținem $n = q_{k+1} b^{k+2} + a_{k+1} b^{k+1} + \dots + a_1 b + a_0$.

Pe de altă parte, $q_{k+1} \leq \frac{q_k}{2}$, deci $n \geq 2q \geq 4q_1 \geq 8q_2 \geq \dots \geq 2^{k+1} q_k$.

Deci va apărea o valoare k cu $q_k = 0$.

Pentru respectiva valoare k, $n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$.

Să considerăm acum $n = a_k b^k + \dots + a_1 b + a_0$ (1) cu $k \in \mathbb{N}$, $a_0, \dots, a_k \in \{0, 1, \dots, \beta\}$ și $a_k \neq 0$.

Presupunem că există $s \in \mathbb{N}$, $\alpha_0, \dots, \alpha_s \in \{0, 1, \dots, \beta\}$ și $\alpha_0 \neq 0$ astfel ca

$n = \alpha_s b^s + \dots + \alpha_1 b + \alpha_0$ (2)

Atunci, din (1) avem

$$b^k \leq n \leq \beta(b^k + b^{k-1} + \dots + b + 1) = \cancel{\beta} \cdot \frac{b^{k+1} - 1}{\cancel{b - \beta}} < b^{k+1}$$

din (2) avem $b^s \leq n < b^{s+1}$:

Deci:
$$\left.\begin{array}{l} b^k \leq n < b^{s+1} \Rightarrow k < s+1 \\ b^s \leq n < b^{k+1} \Rightarrow s < k+1 \end{array}\right\} \xRightarrow{b, s \in \mathbb{N}} k = s.$$

Dacă $k (= s) = 0$, obținem $\alpha_0 = n = a_0$

Dacă $k (= s) > 0$,

$$b(a_k b^{k-1} + \dots + a_1) + a_0 = n = b(\alpha_k b^{k-1} + \dots + \alpha_1) + \alpha_0. \quad (3)$$

Observăm de aici că $a_0 \overset{b}{=} \alpha_0$, deci $\alpha_0 = a_0$.

Atunci din (3) obținem $a_k b^{k-1} + \dots + a_2 b + a_1 = \alpha_k b^{k-1} + \dots + \alpha_2 b + \alpha_1$.

și aplicând ipoteza de inducție: $\alpha_1 = a_1$, $\alpha_2 = a_2, \dots, \alpha_k = a_k$

Scanned with CamScanner

Am demonstrat, deci:

T1 Pentru orice $n \in \mathbb{N}^*$ există $k \in \mathbb{N}^*$ și $a_0, a_1, \dots, a_k \in \{0, 1, \dots, \beta\}$ astfel ca $a_k \neq 0$ și

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0. \quad (*)$$

În plus, k și $a_0, \dots, a_k$ sunt unic determinate de n, de b și de condițiile de mai sus.

Def. 2: Dat fiind $n \in \mathbb{N}$, scrierea din membrul drept al lui $(*)$ s.n. reprezentare a lui n în baza b.

Def. 3: Numerele $0, 1, \dots, \beta = b-1$ s.n. cifrele bazei b.

<u>NOTAȚIE</u>: Vom nota deseori expresia din MD al relației $(*)$ cu

$$\overline{a_k a_{k-1} \dots a_1 a_0}_{(b)}$$

Urmând de relația $n = sgn(n) \cdot |n|$ din cele de mai sus obținem:

T4 Orice nr. întreg nenul n admite o reprezentare unică în baza b

$$n = sgn(n)\, \overline{a_k a_{k-1} \dots a_1 a_0}_{(b)} \quad \text{cu } a_k \neq 0.$$

Fie $x \in [0,1)$

Notăm $x_1 = x$ și punem $a_1 \overset{not.}{=} [b x_1]$ și $x_2 = \{b x_1\}$

Obs: $x = x_1 = \frac{b x_1}{b} = \frac{[b x_1] + \{b x_1\}}{b} = \frac{a_1}{b} + \frac{x_2}{b}$

$a_2 \overset{not.}{=} [b x_2]$; $x_3 = \{b x_2\}$. Ca mai sus,

$$x = \frac{a_1}{b} + \frac{\frac{a_2}{b} + \frac{x_3}{b}}{b} = \frac{a_1}{b} + \frac{a_2}{b^2} + \frac{x_3}{b^2}$$

$x_1 = 0,7432$; $10x_1 = 7,432$

$[10x_1] = 7$; $x_2 = \{10x_1\} = 0,432$.

$[10x_2] = 4$; $x_3 = \{10x_2\} = 0,32$

$[10x_3] = 3$; $x_4 = \{10x_3\} = 0,2$.

$[10x_4] = 2$; $x_5 = \{10x_4\} = 0$.

În plus, $x_i \in [0,1) \Rightarrow b x_i \in [0, b) \Rightarrow a_i = [b x_i] \in \{0, 1, \dots, \beta\}$, $i = \overline{1,2}$.

Presupunem construite $a_1, a_2, \dots, a_m \in \{0, 1, \dots, \beta\}$ și $x_{m+1} \in [0,1)$ cu $x = \frac{a_1}{b} + \frac{a_2}{b^2} + \dots + \frac{a_m}{b^m} + \frac{x_{m+1}}{b^m}$

Punem $a_{m+1} = [b x_{m+1}] \in \{0, 1, \dots, \beta\}$ și $x_{m+1} = \{b x_m\} \in [0,1)$

Obținem $x = \frac{a_1}{b} + \dots + \frac{a_m}{b^m} + \frac{\frac{[b x_{m+1}] + \{b x_{m+1}\}}{b}}{b^m} = \frac{a_1}{b} + \frac{a_m}{b^m} + \frac{a_{m+1}}{b^{m+1}} + \frac{x_{m+2}}{b^{m+1}}$.

Ca urmare, $\forall m \in \mathbb{N}^*$ $\exists a_1, \dots, a_m \in \{0, 1, \dots, \beta\}$

$\exists x_{m+1} \in [0,1)$ $\quad x = \frac{a_1}{b} + \dots + \frac{a_m}{b^m} + \frac{x_{m+1}}{b^m}$ (1)

Dar $\quad 0 \leq \frac{x_{m+1}}{b^m} < \frac{1}{b^m}$ (2)

$$\frac{x_{m+1}}{b^m} \to 0, \quad \frac{1}{b^m} \to 0$$

(1) & (2) $\Rightarrow \lim_{m \to \infty} \left(\frac{a_1}{b} + \frac{a_2}{b^2} + \dots + \frac{a_m}{b^m} \right) = x$

$$\overset{\shortparallel}{\sum_{m \geq 1} \frac{a_m}{b^m}}.$$

Scanned with CamScanner

Def. 5 O scriere de forma $\sum_{n\geq 1} \frac{a_n}{b^n}$ cu $a_n \in \{0, 1, \dots, \beta\}$ pt. orice $n \in \mathbb{N}^*$ s.n. reprezentare a lui $x \in [0,1)$ în baza b dacă $\sum_{n\geq 1} \frac{a_n}{b^n} = x$.

Din cele de mai sus obținem:

Prop. 6: Orice număr $x \in [0,1)$ admite o reprezentare în baza b.

Obs 7: Din T4 și Prop. 6 obținem:
Orice nr. real admite reprezentare în baza b.

Propoziție: Notație: Vom folosi frecvent, în loc de $\sum_{n\geq 1} \frac{a_n}{b^n}$, notația $\overline{0, a_1 a_2 a_3 \dots}_{(b)}$

Prop. 8: $\overline{0, \beta\beta\beta\dots}_{(b)} = 1$

Dem.: $\overline{0, \beta\beta\beta\dots}_{(b)} = \frac{\beta}{b} + \frac{\beta}{b^2} + \frac{\beta}{b^3} + \dots = \beta \lim_{n\to\infty} \left(\frac{1}{b} + \frac{1}{b^2} + \dots + \frac{1}{b^n}\right) = \frac{\beta}{\beta} \lim_{n\to\infty} \frac{1 - \frac{1}{b^n}}{1 - \frac{1}{b}} =$

$= \frac{\beta}{\cancel{b}} \cdot \frac{1}{\frac{b-1}{\cancel{b}}} = \frac{\beta}{b-1} = 1.$ $\square$.

Datorită Obs 7, orice nr. real admite o reprezentare în baza b; cf. T4 și Prop 6, aceasta e de forma

$$a_{-r} b^r \dots + a_{-2} b^2 + a_{-1} b + a_0 + \frac{a_1}{b} + \frac{a_2}{b^2} + \frac{a_3}{b^3} + \dots = \sum_{n\geq -r} \frac{a_n}{b^n} \quad \text{cu } r \in \mathbb{N} \text{ și } a_{-r} \neq 0.$$

Să presupunem că pt. un anumit $x \in \mathbb{R}$, avem două reprezentări în baza b:

$$\sum_{n\geq -r} \frac{\alpha_n}{b^n} = x = \sum_{n\geq -r} \frac{a_n}{b^n} \qquad \alpha_{-r} \neq 0 \neq a_{-r}$$

Fie j cel mai mic indice pt. care $\alpha_j \neq a_j$. Pt. a fixa ideile, vom considera $\alpha_j < a_j$ ($\Rightarrow \alpha_j < \beta$).

Atunci $x = \sum_{n\geq -\max\{r,0\}} \frac{\alpha_n}{b^n} = \sum_{n\geq -\max\{r,0\}}^{j} \frac{\alpha_n}{b^n} + \sum_{n\geq j+1} \frac{\alpha_n}{b^n} \leq \sum_{n\geq -\max\{r,0\}}^{j} \frac{\alpha_n}{b^n} + \beta \sum_{n\geq j+1} \frac{1}{b^n} =$

$= \sum_{n\geq -\max\{r,0\}}^{j} \frac{\alpha_n}{b^n} + \frac{\beta}{b^{j+1}} \sum_{n\geq 0} \frac{1}{b^n} = \sum_{n\geq -\max\{r,0\}}^{j} \frac{\alpha_n}{b^n} + \frac{\cancel{\beta}}{b^{j+1}} \cdot \frac{b}{\cancel{b-1}} = \sum_{n\geq -\max\{r,0\}}^{j+1} \frac{a_n}{b^n} + \frac{\alpha_j}{b^j} + \frac{1}{b^j} =$

din def. lui j !!

$a'_n = \begin{cases} a_n + j \\ 1 + \alpha_j \end{cases}$ $= \sum_{n\geq -\max\{r,0\}}^{j} \frac{a'_n}{b^n} \leq \sum_{n\geq -r} \frac{a_n}{b^n} = x.$

Deci toate "$\leq$" din acest raționament calculatoriu sunt de fapt "$=$".

Ca urmare:
- $\alpha_n = \beta \quad \forall n \geq j+1$
- $a_n = 0 \quad \forall n \geq j+1$
- $a_j = 1 + \alpha_j$
- $\alpha_k = a_k \quad \forall k < j.$

Scanned with CamScanner

În concluzie:

$\boxed{T9}$: Singura abatere de la unicitate pentru reprezentările nr. reale în baza b este cea în care una din reprezentări admite "perioada β", iar cealaltă se obține din ea înlocuind "perioada β" cu o "0" creșcând cu o unitate cifra imediat anterioară perioadei β (acceptând "trecerea peste virgulă").

$\boxed{T10}$: Orice nr. real admite reprezentare în baza b; aceasta e unică dacă nr. dat nu admite reprezentare cu "perioada β" sau "completata" cu încă una, descrisă în T9, dacă nr. admite reprezentări cu "perioade β".

Def. 11: O reprezentare de forma $\sum_{n\geq 1} \frac{a_n}{b^n}$ cu $a_n \in \{0, 1, \dots, \beta\}$ se mai numește "fracție în baza b".

Def. 12: O fracție $\overline{0, a_1 a_2 a_3 \dots}_{(b)}$ s.n. periodică dacă $\exists\, k \in \mathbb{N}^*$, $\exists\, n_0 \in \mathbb{N}$, $\forall\, n \geq n_0$, $a_{n-k} = a_n$.

Scanned with CamScanner

Teoria nr. cu apl în criptografie

02-04-2024

Cursul 6

vreau să scriu un mesaj.

v r e a u s ă s c r i u u n m e s a j.

VEUS CI NMSJRA ĂSRUU EA.

se cristalizează ideea permutării simbolurilor din mesaj.

SCYTALLE

CIFRU = Algoritm (depinzând de anumiți parametri) de prelucrare a unui text în scopul de a-i da o formă care să nu fie inteligibilă decât pentru expeditorul de destinatarul de drept al mesajului.

CHEIE = sistem concret de valori pentru parametrii unui cifru.

Cifruri → de transpoziție (ele păstrează simbolurile din mesaj, dar le schimbă poziția)
→ de substituție (ele substituie simbolurile din mesaj cu alte simboluri, dar le conservă pozițiile).

Cifruri de substituție:

SUETENIUS - Julius Caesar folosea un cifru în care înlocuia fiecare literă a alfabetului cu cea aflată la 3 poziții după ea.

ex: e l e m e n t e d e t e o r i a n u m e r e l o r
H O H P H Q V H G H V H R T K B Q X P H T H O R T

(De fapt, e atestat documentar că a existat un tratat al lui Valerius Probus în care acesta descria și multe alte cifruri folosite de Caesar. Tratatul lui Probus nu s-a păstrat însă.)

Kama-Sutra: Tinerele din înalte societate din India trebuia să cunoască "arta transmiterii de mesaje secrete" în care foloseau un alfabet de "grupare în perechi a literelor alfabetului.

ex:
a b c d e n i j k l m n o
m f h s q g w z p t r y x

m a i t r e y i d e v i
D N W L G Q U W S Q X W

Atât cifrurile de tip Caesar, cât și cele de "dispunere a literelor în perechi" menționate în Kama-Sutra sunt exemple de cifruri ce constau în permutarea literelor unui alfabet. De aceea, o generalizare a lor e cea reprezentată de cifrul ce utilizează permutarea literelor unui anumit alfabet (ale cărui chei sunt permutările propriu-zise).

Scanned with CamScanner

Teoria numerelor cu apl. în cripto

23-04-2024

Cursul 9

$\boxed{89 \qquad 7}$

$A \xrightarrow{76} B$

$A \xleftarrow{87} B$

Alice știe și exponentul ei, adică 3
Bob îl știe pe al lui, adică 4.

$B: 76^4 \equiv \boxed{81} \pmod{89}$

$A: 87^3 \equiv \boxed{81} \pmod{89}$

Def. 1 Fie $m \in \mathbb{N}^*$ și fie $a \in \mathbb{Z}$ cu $(a, m) = 1$. Numim GAUSSIANUL (sau ORDINUL) lui $a \pmod m$ ordinul lui $\hat{a}$ în $U(\mathbb{Z}_m)$

Notăm: gaussianul lui $a \pmod m$ cu $\gamma_m(a)$.

Prop. 2: Fie $m \in \mathbb{N}^*$ și fie $a \in \mathbb{Z}$ cu $(a, m) = 1$. Atunci:

(i) $\forall k \in \mathbb{Z}$ $(a^k \equiv 1 \pmod m \Rightarrow \gamma_m(a) \mid k)$.

(ii) $\gamma_m(a) \mid \varphi(m)$.

(iii) $\forall k, l \in \mathbb{Z}$ $(a^k \equiv a^l \pmod m \Leftrightarrow k \equiv l \pmod{\gamma_m(a)})$

Exemplu: Determinați $\gamma_{23}(2)$.

Sol.:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	2	4	6	8	10	12	14	16	18	20	22	1	3	5	7	9	11	13	15	17	19	21
$2^\wedge$	2	4	8	16	9	18	13	3	6	12	1											

Conform tabelului $\gamma_{23}(2) = 11$

Def. 3: Fie $m \in \mathbb{N}^* \setminus \{1\}$ și fie $a \in \mathbb{Z}$ și $k \in \mathbb{N}^*$ cu $(a, m) = 1$. (i) Spunem că a e RĂDĂCINĂ DE ORDIN k A LUI 1 $\pmod m$ adică $a^k \equiv 1 \pmod m$

(ii) Dacă, în plus, $k \mid \varphi(m)$, spunem că a e RĂDĂCINĂ PRIMITIVĂ DE ORDIN $k \pmod m$ dacă $\gamma_m(a) = k$.

(iii) Spunem că a e RĂDĂCINĂ PRIMITIVĂ modulo m dacă $\gamma_m(a) = \varphi(m)$.

ex.: De mai sus, $\gamma_{23}(2) = 11$, deci 2 nu e rădăcină primitivă $\pmod{23}$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
3	3	6	9	12	15	18	21	1	4	7	10	13	16	19	22	2	5	8	11	14	17	20
$3^\wedge$	3	9	4	12	13	16	2	6	18	8	1											
5	5	10	15	20	2	7	12	17	22	4	9	14	19	1	6	11	16	21	3	8	13	18
$5^\wedge$	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1

Scanned with CamScanner

conform tabelului, $\gamma_{23}(3)=11$, deci 3 nu e rădăcină primitivă (mod 23), iar $\gamma_{23}(5)=22$, deci 5 e rădăcină primitivă (mod 23).

Def. 4 Fie $m \in \mathbb{N}^*$. Presupunem că există rădăcini primitive (mod m) și fie b una dintre ele. Fie $a \in \mathbb{Z}$ cu $(a,m)=1$. Numim **INDICELE LUI a ÎN BAZA b** acel exponent k cu proprietatea $b^k \equiv a \pmod m$.

Prop. 5: Fie m și b ca în def. 4. Atunci:

(i) Dacă $a_1, a_2, \dots, a_s \in \mathbb{Z}$ și $(a_i, m)=1$, atunci $ind_b(a_1 a_2 \dots a_s) \equiv ind_b a_1 + ind_b a_2 + \dots + ind_b a_s \pmod{\varphi(m)}$.

(ii) Dacă $a \in \mathbb{Z}$, $(a,m)=1$ și $k \in \mathbb{Z}$,
$ind_b a^k \equiv k\, ind_b a \pmod{\varphi(m)}$.

(iii) Dacă b' e altă rădăcină primitivă (mod m), iar $a \in \mathbb{Z}$, $(a,m)=1$, atunci
$ind_{b'} a \cdot ind_b b' = ind_b a \pmod{\varphi(m)}$.

Observăm că modulo 8 nu există rădăcini primitive. Se pune deci, întrebarea "pentru ce numere m există rădăcini primitive?"

Fie $m \in \mathbb{N}^* \setminus \{1\}$. Pp. că există rădăcină primitivă (mod m); fie b una din ele. Atunci, descompunând m în factori primi, avem $U(\mathbb{Z}_m) \overset{\varphi}{\cong} U(\mathbb{Z}_{p_1^{\alpha_1}}) \times U(\mathbb{Z}_{p_2^{\alpha_2}}) \times \dots \times U(\mathbb{Z}_{p_r^{\alpha_r}})$.

Atunci $\varphi(m) = ord\, \varphi(b) = [ord_{\mathbb{Z}_{p_1^{\alpha_1}}} \beta_1, ord_{\mathbb{Z}_{p_2^{\alpha_2}}} \beta_2, \dots, ord_{\mathbb{Z}_{p_r^{\alpha_r}}} \beta_r]$.

(β_j fiind componenta j a lui $\varphi(m)$).

Dar $|U(\mathbb{Z}_{p_j^{\alpha_j}})| = p_j^{\alpha_j - 1}(p_j - 1)$;