

CAIET TUTORIAT

Lista 2: ⑦)

$$\mathbb{Z}_{31} : 2019^{2018}, 2020^{2029}, 2021^{2021}$$

$$\mathbb{Z}_{100} \rightarrow$$

$\varphi(n) =$ numărul de numere mai mici sau egale cu n și prime cu n

$$\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$$

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \text{ unde } n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

descompunerea în factori primi
a lui n

i) dacă $(a, b) = 1$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

(ii) $\varphi(p) = p-1$, unde p este prim

(iii) $\varphi(p^k) = p^k - p^{k-1}$

Teorema lui Euler:

$$\boxed{\text{dacă } (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}}$$

sau în \mathbb{Z}_n : $\widehat{a}^{\varphi(n)} = \widehat{a}^{\varphi(n)} = \widehat{1}$

Dacă $p = \text{prim} \Rightarrow$ Th. Fermat:

$$\text{dacă } p \nmid a: a^{p-1} \equiv 1 \pmod{p}$$

sau în \mathbb{Z}_p : $\widehat{a}^{p-1} = \widehat{a}^{p-1} = \widehat{1}$

Folosim Th. Euler: $\varphi(31) = 30 \Rightarrow (a, 31) = 1$ at. $a^{30} \equiv 1 \pmod{31}$

$$2019 : 31 = 65 \text{ rest } 9 \Rightarrow \mathbb{Z}_{31}: \widehat{2019} = \widehat{9}$$

$$2019 : 30 = 6 \text{ rest } 9$$

$$\mathbb{Z}_{31}: \widehat{2019}^{2019} = \widehat{9}^{2019} = \widehat{9}^{30 \cdot 67 + 9} = (\widehat{9}^{30})^{67} + \widehat{9}^9 \text{ Euler } (\widehat{9})^{67} \cdot (\widehat{9}^3)^3 = \\ = \widehat{1} \cdot (\widehat{64})^3 = \widehat{1} \cdot (\widehat{2})^3 = \widehat{1} \cdot \widehat{8} \quad (1, 31) = 1$$

$$\mathbb{Z}_{31}: \widehat{2020}^{2020} = \widehat{5}^{2020} = \widehat{5}^{67 \cdot 30 + 10} = (\widehat{5}^{30})^{67} \cdot \widehat{5}^{10} = \\ = (\widehat{5}^3)^{67} \cdot \widehat{5}^5 =$$

$$= \widehat{5} \cdot \widehat{5}^{3 \cdot 3+1} = (\widehat{5}^3)^3 \cdot \widehat{5} = (\widehat{125})^3 \cdot \widehat{5} = (\widehat{1})^3 \cdot \widehat{5} = \widehat{5}$$

$$\widehat{2020}^{2021} = \widehat{6}^{67 \cdot 30 + 11} = (\widehat{6}^{30})^{67} \cdot \widehat{6}^{11} \stackrel{\text{cuburi}}{=} (\widehat{1})^{67} \cdot \widehat{6}^{2 \cdot 5+1}$$

$$= (\widehat{6}^2)^5 \cdot \widehat{6} = (\widehat{36})^5 \cdot \widehat{6} = \widehat{5}^5 \cdot \widehat{6} =$$

$$= \cancel{\widehat{6}^3 \cdot \widehat{6}^2} \cdot \widehat{5}^4 \cdot \widehat{5} \cdot \widehat{6} = \widehat{625} \cdot \widehat{36} = \widehat{-5} = \widehat{35} \stackrel{11}{\widehat{-5}} = \widehat{31} \widehat{-5} = \widehat{26}$$

$$\varphi(100) = \varphi(4) \varphi(25) = \cancel{2} \cdot 2 \cdot 20 = 40$$

91

$$\widehat{\sum}_{100} : \widehat{2019}^{2019} = \widehat{19}^{19+10 \cdot 50} = (\widehat{19}^{100})^{11} = (\widehat{19}^{50}) \cdot \widehat{19}^{19} =$$

cuburi

$$= (\widehat{19}^2)^9 \cdot \widehat{19} = \widehat{361}^9 \cdot \widehat{19} = \widehat{61}^9 \cdot \widehat{19} = (\widehat{61}^3)^3 \cdot \widehat{19} =$$

$$= \cancel{226981}^3 \cdot \widehat{19} = \cancel{81} \widehat{19}^3 = \widehat{531351} \cdot \widehat{19} = \widehat{51} \cdot \widehat{19} = \widehat{29} = \widehat{29}$$

$$\text{patr. c.c. } (\widehat{31} = \widehat{30} + 1 \Leftrightarrow \widehat{3} = \widehat{30} + 1)$$

$\Leftrightarrow \widehat{30} = \widehat{3}$

$$\widehat{2020}^{2020} = \widehat{20}^{2020}$$

dacă $(20, 100) \neq 1 \Rightarrow$ nu putem folosi cuburi, dacă

$$\widehat{20}^{2020} = \widehat{20}^{2 \cdot 1010} = (\widehat{20}^2)^{1010} = (\widehat{400})^{1010} = \widehat{0}^{1010} = \widehat{0}$$

(asta a fost ușor patr. c.c. $100 = 2^2 \cdot 5^2$)

și $20 = 2^2 \cdot 5$

și deci $20^2 = (2^2 \cdot 5)^2 = (2^2)^2 \cdot 5^2 : 2^2 \cdot 5^2$

i.e. $20 \text{ și } 100$ au un același factor prim
mai mult pătrat care se împarte și la numărul de mai multe

$$a = 7 \quad b = 8$$

$$\therefore 7 / 06.06.2022 : 8^{7^8 7^7} \pmod{31}$$

a.s. $20 \wedge 100$

$8^{7^8 7^7} \pmod{31} \rightarrow$ ca în exercițiul trecut trebuie să se impună ca restul exponentului să fie $\varphi(31) = 30$ și, în fel
 \Rightarrow rezulta că ca în exercițiul trecut, o parte

ne ducem $\varphi(\text{dim Euler})$ și ne interesează restul
 Dacă vom să calculăm $7^{8^7} \pmod{30}$. $\varphi(30) = \varphi(5) \varphi(6)$

$$\text{Deci } \mathbb{Z}_{30}: 7^{8^7} = \left(7^8\right)^{8^6} = \left(\varphi(30)\right)^{8^6} = 7^{8^6} = 7^4 = 49 = 7 \cdot 2 = 8$$

$$\Rightarrow 7^{8^7} \equiv 1 \pmod{30}$$

Ne interesează de $8^{8+8^7} \pmod{30}$ și stim că $7^{8^7} = 30 \cdot \text{cote} + 1$

$$\mathbb{Z}_{30}: 8^{8^7} = 8^{(30 \cdot \text{cote} + 1)} = (8^{30})^{\text{cote}} \cdot 8^1 = (8^{30})^{\text{cote}} \cdot 8 = 8$$

$$(8^{30})^{\text{cote}} = \varphi(30) = 8$$

Euler/Fermat

$$a=6 \quad b=11$$

$$11^{6^6} \pmod{31} \rightarrow 11^{6^6} \pmod{30} \rightarrow 6^6 \pmod{8}$$

$$\varphi(31)=30 \quad (11, 30)=1 \quad \vdots \quad 6^6 = 2^6 \cdot 3^6 : 2^3 = 8$$

$$\varphi(30)=8 \quad \text{nu e divizor} \quad \text{Euler} \quad \Rightarrow 8|6^6$$

$$\cancel{6^6} \equiv 0 \pmod{8}$$

$$\hookrightarrow 11^{6^6} \stackrel{30}{\equiv} 11^{8 \cdot \text{cote}} \stackrel{30}{=} (11^8)^{\text{cote}} \stackrel{\text{Euler}}{=} 1, \text{ cote} = 1$$

$$\hookrightarrow 11^{6^6} = 11^{30 \cdot \text{altcote} + 1} = (11^{30})^{\text{altcote}} \cdot 11^1 \stackrel{\text{Euler}}{=} 1, \text{ altcote} = 11$$

ALGORITMUL LUI EUCLID

Input: $a, b \in \mathbb{Z}$

Output: $\gcd(a, b)$

Teoreme imp. cirest în mod repetat:

$$\begin{aligned}
 & \text{cireste} \quad a = b \cdot q_1 + r_1 \quad r_1 < |b| \quad r_1 = r_{m+1} \cdot q_{m+1} + r_{m+2} \\
 & r_2 < |r_1| = r_1 \quad \leftarrow b = r_1 \cdot q_2 + r_2 \quad r_{m+2} = r_{m+1} \cdot q_{m+2} + 0 \\
 & r_3 < r_2 \quad \leftarrow r_2 = r_3 \cdot q_3 + r_3 \quad \Rightarrow \text{cireste} \\
 & r_4 < r_3 \quad \leftarrow r_3 = r_4 \cdot q_4 + r_4 \quad \Rightarrow \gcd(a, b) = r_{m+2}
 \end{aligned}$$

Obs.: $|b| > r_1 > r_2 > r_3 \dots > r_m > r_{m+1} = 0$

Algoritmul se termină într-un mtr. finit de pasi pînă cînd rezultatul este un sir descrescător de nr. nat., care e deci finit.

Ex. $\text{gcd}(48672, 16848)$

$$(1) 48672 = 2 \cdot 16848 + 14976$$

$$(2) 16848 = 1 \cdot 14976 + 1872 \Rightarrow \text{gcd} = 1872$$

$$(3) 14976 = 8 \cdot 1872 + 0$$

Intervadă, $48672 = 2^5 \cdot 3^2 \cdot 13$

$$16848 = 2^4 \cdot 3^3 \cdot 13$$

$$\Rightarrow \text{gcd} = 2^4 \cdot 3^2 \cdot 13$$

$$= 16 \cdot 9 \cdot 13 = 1872$$

Mai mult, din (2) avem

$$\cancel{a = 2b + 14976} \quad \cancel{1872}$$

$$1872 = 16848 - 1 \cdot \underbrace{14976}_{(1)} = 16848 - 1 \cdot (48672 - 2 \cdot 16848)$$

$$= 16848 - 48672 + 2 \cdot 16848 = 3 \cdot 16848 - 48672$$

$$\Rightarrow \text{gcd}(a, b) = 3b - a$$

Așa că $\text{gcd}(a, b)$ are forma unei combinații liniare de a și b .

Nă interesează în special cazul când $(a, b) = 1$ atunci căpătăm

Algoritmului lui Euclid, avem $m, n \in \mathbb{Z}$ s.t. $am + nb = 1$.

Când trecem în \mathbb{Z}_p : $\overbrace{am + nb}^{\infty} = \overbrace{1}^{\infty}$
 $\Leftrightarrow \widehat{am} + \widehat{nb} = \widehat{1} \Leftrightarrow \widehat{a} \cdot \widehat{m} + \widehat{n} \cdot \widehat{b} = \widehat{1}$

$$\widehat{a} \widehat{m} = \widehat{1} \Rightarrow \widehat{m} = \widehat{a}^{-1}$$

\Rightarrow Metoda de calcul a inversului modular ca algoritm

Euclid

(Obs.): A fost măsură că $(a, b) = 1$ (a și inversabil în $\mathbb{Z}_b \Rightarrow (a, b) = 1$, altfel, nu există invocație a în \mathbb{Z}_b)

Ex.: inversul lui 31 în \mathbb{Z}_{100} : 31^{-1} . Obs. că $(100, 31) = 1$

$$(1) 100 = 3 \cdot 31 + 7$$

$$(2) 31 = 4 \cdot 7 + 3$$

$$(3) 7 = 2 \cdot 3 + 1$$

$3 = 1 \cdot 3 + 0 \Rightarrow$ obținem că și asta este $(100, 31) = 1$

Mai mult,

$$\begin{aligned} (3): 0 &= 7 - 3 \cdot 2 \stackrel{(2)}{=} 7 - 2 \cdot (31 - 4 \cdot 7) = 7 - 2 \cdot 31 + 8 \cdot 7 \\ &\stackrel{\text{L.I.}}{=} 9 \cdot 7 - 2 \cdot 31 \stackrel{(1)}{=} 9 \cdot (100 - 3 \cdot 31) = 2 \cdot 31 = \\ &= 9 \cdot 100 - 27 \cdot 31 - 2 \cdot 31 = 9 \cdot 100 - 29 \cdot 31 \end{aligned}$$

$$\Rightarrow 9 \cdot 100 - 29 \cdot 31 = 1 \Rightarrow \widehat{29} \cdot \widehat{31} = 1$$

$$\Rightarrow \widehat{31}^{-1} = -\widehat{29} = \cancel{-29} = \widehat{71}$$

$$\begin{matrix} \text{Z.} \\ \mathbb{Z}_{100} \end{matrix} : \widehat{0} - \widehat{29} = \widehat{100} - \widehat{29} = \widehat{100 - 29} = \widehat{71}$$

Într-o altă ordine, $\widehat{71} \cdot \widehat{31} = \widehat{2201} = 1$.

LEMA CHINEZĂ A RESTURILOR

~~Un nr. m împărțit la m_1 dă restul a_1 , la m_2 dă restul a_2 , ... la m_n dă restul a_n , iar m_1, m_2, \dots, m_n sunt oricare două prime între ele. Aflați un astfel de nr. mai mic decât k și mai mare decât q .~~

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_m \pmod{m_m} \quad (\text{Astfel apoi, } \exists \text{ unică soluție minimă } \stackrel{x_0}{\text{dată produsul }} m_1 \cdot m_2 \cdot \dots \cdot m_m)$$

$$(m_i, m_j) = 1 \quad \forall i, j \in \{1, \dots, m\}$$

LCR: Soluție și modul

$$m_1 \cdot m_2 \cdot \dots \cdot m_m$$

$$x_0$$

(Astfel apoi, \exists unică soluție minimă

dată produsul $m_1 \cdot m_2 \cdot \dots \cdot m_m$)

În plus, orice altă soluție $x \equiv x_0 \pmod{m_1, \dots, m_n}$
 adică $\hat{x} = \hat{x}_0$, sau $x = x_0 + k(m_1, \dots, m_n)$, $k \in \mathbb{Z}$

pentru orice k , numărul definit este
 o soluție.

$$M := m_1 \cdot m_2 \cdots m_n$$

$$M_i := \frac{M}{m_i} \quad (M_i = m_2 \cdot m_3 \cdots m_n)$$

$$M_1 = m_1 \cdot m_2 \cdot m_3 \cdots m_n$$

$$\rightarrow M_i = m_1 \cdot m_2 \cdot m_3 \cdots m_{i-1} \cdot m_{i+1} \cdots m_n$$

Abs.: Cînd toate m_i -urile sunt prime între ele, avem că

$$(M_i, m_i) = 1 \text{ deci putem calcula } y_i = M_i^{-1} \pmod{m_i}$$

il calculăm cu Edd.

numărul care e inversul lui M_i în \mathbb{Z}_{m_i}

$$\Rightarrow \hat{y}_2 = 5$$

$$\cdot \hat{35}^{-1} \text{ în } \mathbb{Z}$$

Observație

$$\Rightarrow \hat{35}^{-1}$$

=>

$$x_0 = 63 \cdot$$

$$= 2$$

Soluție

mat. core

Obs

$$\left\{ \begin{array}{l} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{array} \right.$$

$$\left\{ \begin{array}{l} x \equiv 8 \pmod{9} \end{array} \right.$$

o soluție x_0 e date de formula de mai sus

*

$$M_1 = 7 \cdot 9 = 63 \quad M_2 = 5 \cdot 9 = 45 \quad M_3 = 5 \cdot 7 = 35$$

$$\cdot \hat{63}^{-1} \text{ în } \mathbb{Z}_5$$

Reminder: Nu de fapt contăm o comb. liniare

$$a \cdot 63 + b \cdot 5 = 1 \Rightarrow a \cdot \hat{63} = 1 \text{ în } \mathbb{Z}_5$$

Este OK dacă o vedem „din ochi”.

$$63 \cdot 3 = 189$$

$$38 \cdot 5 = 190$$

$$38 \cdot 5 - 63 \cdot 3 = 1$$

$$\Rightarrow \hat{63} \cdot (-3) = 1$$

$$75: \hat{63}^{-1} = \hat{-3} = \hat{5-3} = \hat{2}$$

(SAU, apărut)

$$\Rightarrow y = 2$$

$$\cdot \hat{45}^{-1} \text{ în } \mathbb{Z}_7$$

$$45 = 7 \cdot 6 + 3$$

$$7 = 3 \cdot 2 + 1$$

$$3 = 3 \cdot 1 + 0$$

=>

$$x_0 = 63 \cdot$$

Soluție

mat. core

Obs

Răsp

$$D5: \widehat{63}^{-1} = \widehat{-3} = \widehat{5-3} = \widehat{2}$$

(SAU, aparent, mai simplu $63 \cdot 2 = 126$, $5 \cdot 25 = 125$)

$$63 \cdot 2 - 25 \cdot 5 = 1 \Rightarrow \widehat{63} \cdot 2 = \widehat{1} \text{ în } \mathbb{Z}_5$$

se poate că sunt cu numărători 1

$$\Rightarrow y_1 = 2$$

$$\cdot \widehat{45}^{-1} \text{ în } \mathbb{Z}_7$$

$$45 = 7 \cdot 6 + 3$$

$$7 = 3 \cdot 2 + 1 \Rightarrow 1 = 7 - 3 \cdot 2 \Rightarrow 1 = 7 - 2 \cdot 45 + 12 \cdot 7$$

$$= 13 \cdot 7 - 2 \cdot 45$$

$$\widehat{45}^{-1} = \widehat{2} \Rightarrow \widehat{45}^{-1} = \widehat{-2} = \widehat{5}$$

$$\Rightarrow y_2 = 5$$

$$\cdot \widehat{35}^{-1} \text{ în } \mathbb{Z}_9$$

~~Observăm că~~ $\widehat{35} = \widehat{36-1} = \widehat{36} \widehat{-1} = \widehat{8-1} = \widehat{7} = \widehat{9-1} = \widehat{8}$

$$\Rightarrow \widehat{35}^{-1} = \widehat{8}^{-1} \quad (\text{putem face asta și ca celelalte, nu stiu de ce m-am complicate})$$

~~Observăm că~~ $9 \cdot 1 - 1 \cdot 8 = 1 \Rightarrow \widehat{-1} \cdot \widehat{8} = \widehat{1} \text{ în } \mathbb{Z}_9$

$$\Rightarrow \widehat{8} \cdot \widehat{8} = \widehat{1} \Rightarrow \widehat{8}^{-1} = \widehat{8} \quad (\text{ab. } \widehat{8} \cdot \widehat{8} = \widehat{64} = \widehat{63} + \widehat{1} = \widehat{1})$$

$$x_0 = 63 \cdot 2 \cdot 3 + 45 \cdot 5 \cdot 2 + 35 \cdot 8 \cdot 8 =$$

$$= \cancel{2798} \quad 3068$$

Soluție e unică mod $5 \cdot 7 \cdot 9 = 315$, deci cel mai mic nr. nat. care e sol. e de formă $3068 - k \cdot 315$

OBS. că $k=9$ conține: $3068 - 9 \cdot 315 = 3068 - 2835 = \boxed{233}$

Răspunsul e 233.

815

$(R, +, \cdot)$ este multime cu 2 operații, unde pot aduna și înmultiri, iar înmulțirea este distributivă față de adunare.

- Există un element neutru la adunare numit 0_R și orice element $r \in R$ are o inversă $-r \in R$ în raport cu adunarea.

Altfel spus: $(R, +)$ este grup

(R, \cdot) este monoid

- înmulțirea este distributivă față de adunare:

$$\forall r, a, b \in R \quad r \cdot (a+b) = r \cdot a + r \cdot b$$

$$\forall r', a', b' \in R \quad (a'+b') \cdot r' = a' \cdot r' + b' \cdot r'$$

Numim înversabilele din R elementele înversabile în raport cu înmulțirea.

c.e. $x \in R$ c.a. $\exists y \in R$ a.i. $x \cdot y = 1_R$.

• Proprietăți rapide: $\forall r \in R \quad 0_R \cdot r = 0_R$

• Zero-divizori: elementele din inel pentru care există alte elemente din inel care înmulțite cu primele să devină 0_R .

Evident 0_R este zero-divizor.

Alte exemple: $(\mathbb{Z}_6, +, \cdot)$: $\hat{2} \cdot \hat{3} = \hat{6} = 0$

$(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$: $(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$

$$(\mathcal{M}(R), +, \cdot): \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

inel necomutativ (înmulțirea nu e comutativă - nu vom lucra doar peste inele comutative).

- orice inversabil este non-zero-divizor (NVD) este zero divisor).

Denum.: R.p.c. $\exists x \in U(R)$ și $\exists y \neq 0 \in R$ a.i. $xy = 0$

$$x^{-1} \mid xy = 0 \Rightarrow xx^{-1}y = x^{-1} \cdot 0 \Rightarrow 1 \cdot y = 0 \Leftrightarrow y = 0 \text{ și } y \neq 0.$$

• Un inel comun
s.m. domeniu
elem. diferență de

formă
nu e)

Dacă toate
(adice pot se

Ex.:

①

$y =$
(1)

este e
făc

Notărie

$a \in R$, (a
fiecărat

• Într-un inel finit, totii non-zero din inel sunt inversabili.

~~E. Z.~~

- Un inel comutativ în care ~~nu~~ singurul zero-dinor e cel trivial (0_R) și n. domeniu. Altfel spus, un domeniu e un inel în care înmulțirea două elem. diferite de zero, și rezultatul e diferit de 0.

Ex. de domeniu: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Amenajat că $\mathbb{Z} \times \mathbb{Z}$ nu e domeniu (să, de fapt, niciun inel produs direct nu e) și nici \mathbb{Z}_m cănd nu e număr compus. Dar \mathbb{Z}_p e domeniu.

Dacă toate elementele diferite de 0 sunt inversabile

(adică pot să "import" lecile diferite de 0) atunci inelul se numește corp.

Ex.: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sunt coruri. \mathbb{Z} nu e corp (pt. $\frac{1}{2} \notin \mathbb{Z}$)

\mathbb{Z}_p e corp. (pentru calculul împădurii reia algebră Euclid)

$$\textcircled{1} \quad J = (2, X^2 - 1) \text{ ideal în } \mathbb{Z}[X]$$

(i) Arătă că J nu e ideal principal

care e un ideal?

Ce submultime J a unui inel R și $J \subseteq R$ cu urm. prop.

$$(i) \quad \forall i, j \in I : i - j \in I \quad || \quad I - I \subseteq I$$

$$(ii) \quad \forall r \in R, \forall i \in I : r \cdot i \in I \quad || \quad R \cdot I \subseteq I$$

Notă: $J \trianglelefteq R$.

Oricare inel are: $\{0\} \trianglelefteq R, R \trianglelefteq R$

Există o rețetă pentru a crea ideale anume?

$a \in R$,
 foarte

(a) -idealul generat de a

$$(a) = \{r \cdot a \mid r \in R\} \leftarrow \text{toti "multiplii" de } a.$$

Obs. că ~~acestea~~ (i) și (ii) se verifică

$$\begin{array}{c|c} \frac{r \cdot a - r' \cdot a}{R} = (r - r') \cdot a \in I & \frac{r' \cdot r \cdot a}{R} = (r' \cdot r) \cdot a \in I \\ \hline \end{array}$$

idealul e
subgrup aditiv
din inel

(a, b) - idealul generat de a și b

$$\{(r \cdot a + r' \cdot b) / r, r' \in \mathbb{R}\} \leftarrow \text{sume de "multipli" de } a \text{ și } b$$

Abs.: Dacă $I \subseteq R$ și $1 \in I$, atunci $I = R$.

de ce? conform (i) dacă un $r \in R$ arbitrar, cum $1 \in I$

evidență $\boxed{I \subseteq R}$

atunci $r \cdot 1 \in I$, adică $r \in I$, adică $R \subseteq I$

mai: $a \in I$ (R)

$$\stackrel{r}{\Rightarrow} R = I$$

Mai general, dacă $u \in R$ inversabil, $u \in I$, atunci $I = R$.

De fel $\forall r \in R, r \in I$ (i.e. $R \subseteq I$) de ce?

ptr. cu $r \in R$, conform (i), $(r \cdot u^{-1}) \cdot u \in I$

$$(r \cdot u^{-1}) \cdot u = r \cdot (u^{-1} \cdot u) = r \cdot 1 = r \in I$$

Deci dacă un ideal conține un inversibil, atunci este la fel în I .

Un ideal $I \subseteq R$

s.m. principal dacă este de formă $I = (a)$, $a \in R$.

Un inel s.m. Principal dacă toate idealele sale sunt principale.

Idealele lui \mathbb{Z} sunt toate de formă (m) , $m \in \mathbb{Z}$

multiplici întregi de m \rightarrow

$$\dots \{-m, 0, m, 2m, 3m, \dots\}$$

\mathbb{Z} e inel principal.

Idealele lui \mathbb{Z}_m sunt de formă (d) unde $d|m$.

$(R, +, \cdot)$ inel

$\bullet R[X]$ inelul de polinoame cu coef. în inelul R

\downarrow $a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0$ - elementele sunt expresii de forma asta cu $a_0, a_1, \dots, a_m \in R$.

$\nexists \text{ grad}(f) = \text{cel mai mare putere de } X \text{ în } f$

$f(x) = g(x) \Leftrightarrow \text{grad}(f) = \text{grad}(g)$ ($m = n$) și

$$a_m = b_m, a_{m-1} = b_{m-1}, \dots, a_0 = b_0$$

$$a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0 \quad b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$$

$$(f+g)(x)$$

$$f(x) = a_p x^p + \dots + a_1 x + a_0$$

$$g(x) = b_p x^p + \dots + b_1 x + b_0$$

(pot p.p. că sunt sume de termeni
pentru puterea p numărul eventual cunoscute
se joacă $a_p = b_p$).

$$(f+g)(x) = (a_p + b_p)x^p + (a_{p-1} + b_{p-1})x^{p-1} + \dots + (a_1 + b_1)x + (a_0 + b_0)$$

~~$$(f \cdot g)(x) =$$~~

$$f(x) = a_m x^m + \dots + a_1 x + a_0 \quad g(x) = b_m x^m + \dots + b_1 x + b_0$$

$$(f \cdot g)(x) = (a_m b_m) x^{m+m} + (a_m b_{m-1} + a_{m-1} b_m) x^{m+m-1} +$$

$$+ (a_m b_{m-2} + a_{m-1} b_{m-1} + a_{m-2} b_m) x^{m+m-2} + \dots + (a_0 b_1 + a_1 b_0) x + (a_0 b_0)$$

atât după, se înmulțesc fiecare cu fiecare și se adună termenii asemenea.

- dacă coeficienții dominanti (coeficienții termenilor care au gradul) a_m și b_m nu sunt zero divizori (adică $a_m \cdot b_m \neq 0$) atunci

$$\text{grad}(fg) = \text{grad } f + \text{grad } g$$

deci este adăugarea produselor ~~termenii~~ a celor două coeficienți

care e inversabil și deci nu e
zero divizor.

$$(\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x])$$

$$(\mathbb{Z}_p[x])$$

Revenind la exercițiu, presupunem prin absurd că g este principal adică $\exists f \in \mathbb{Z}[x]$ a.s. $g = (f)$.

$$(\mathbb{Z}, x^2 - 1)$$

$$2 \in (\mathbb{Z}, x^2 - 1) \Rightarrow 2 \in (f) \Rightarrow \exists g \in \mathbb{Z}[x] \text{ polinom a.s.}$$

$$1 \cdot 2 + 0 \cdot x^2 = 2$$

$$x^2 - 1 = 0 \cdot 2 + 1(x^2 - 1) \in (\mathbb{Z}, x^2 - 1)$$

$$2 = f \cdot g \quad | \text{ grad}(\cdot)$$

$$\text{grad}(2) = \text{grad}(f) + \text{grad}(g)$$

$$0 = \text{grad}(f) + \text{grad}(g)$$

Polinoamele de grad 0 din $\mathbb{R}[x]$

sunt tot unei cu elementele \mathbb{R} din \mathbb{R} , inelul de coeficienți. Se consideră că

$$\text{grad}(a_R) = -\infty.$$

$$\Rightarrow \text{grad}(f) = \text{grad}(g) = 0.$$

$$\text{grad}(f)=0 \Rightarrow f \in \mathbb{Z} \Rightarrow f = m \in \mathbb{Z}$$

$$\text{grad}(g)=0 \Rightarrow g = m \in \mathbb{Z} \Rightarrow 2 = m \cdot m \Rightarrow m/2 \leftarrow \begin{array}{l} \text{if } m \neq 0 \\ \text{and } 2 \mid m \end{array}$$

$\exists x^2 - 1 \in (f) = (m) \Rightarrow \exists h(x) \in \mathbb{Z}[x] \text{ a.s. } x^2 - 1 = m \cdot h(x)$
 $\text{grad}(x^2 - 1) = \text{grad}(m) + \text{grad}(h(x)) =$
 $\Rightarrow 2 = 0 + \text{grad}(h) \Rightarrow \text{grad}(h) = 2 \Rightarrow h(x) = ax^2 + bx + c$
 $a, b, c \in \mathbb{Z}$

$$\Rightarrow x^2 - 1 = m \cdot (ax^2 + bx + c) = amx^2 + bm \cdot x + cm$$

$$\Rightarrow \begin{cases} 1 = am \Rightarrow m = \pm 1 \\ 0 = bm \\ -1 = cm \Rightarrow m = \pm 1 \end{cases}$$

$$\text{Atunci } (f) = (m) = (\pm 1) \subset U(\mathbb{Z})$$

$$\Rightarrow \mathbb{J} = (\pm 1) = \mathbb{Z}$$

Dacă $R = \mathbb{Z}$ domeniul atunci $U(R) = U(R[x])$

$$U(\mathbb{Z}) = \{-1, 1\}$$

înversibile din inel sunt înversibile și în inelul de pol. și toate inv. din inelul de pol. sunt inv. în inelul de coef.

$$\Rightarrow (2, x^2 - 1) = \mathbb{Z}$$

$$1 \in \mathbb{Z} \Rightarrow 1 \in (2, x^2 - 1) \Rightarrow \exists g, h \in \mathbb{Z}[x]$$

$$1 = 2g(x) + h(x)(x^2 - 1)$$

Puteam evalua polinoamele în diferite valori din R sau din inele mai mari și il continu pe R ca subinel.

$$\text{ptz. } x = 0 \Rightarrow 1 = 2g(0) + h(0)(0^2 - 1)$$

$$\Rightarrow 1 = 2 \cdot g(0)$$

$$\Rightarrow 1 = \text{prod. ab}$$

$$\begin{array}{l} f(x) \in R[x], a \in R \\ \Rightarrow f(a) \in R \end{array}$$

$\Rightarrow \mathbb{J}$ este principal.

(2) elementele nilpotente din $R[x]/\mathbb{J}$.

Revenim la "mai"

Așa cum le spune Th. imp. care spune că ptz. $a \neq 0$ și $b \neq 0$

$$\exists 2^k \in \mathbb{Z} \text{ cu } k < \deg(f)$$

$$\text{a.s. } a = b \cdot g + r, \text{ unde există } g \in R[x]$$

Rm. f $\in \text{ig}(R[X])$ cu $\text{LC}(g) \in U(R)$ $\exists g_2(x), h_2(x) \in R[X]$
 coeficientul dominant imparabil în R
 cu $\text{grad}(r(x)) < \text{grad}(g)$, ^{alung} d. a. i. $f(x) = g(x) \cdot g_2(x) + r(x)$.

Algebra - am info 2022.pdf

(Examen veria 13)
2022

Lecția IV

$$P = 5 \quad Q = 6$$

(1) cîntul și restul împ. lui $x^4 + x^2 + 5$ la $x^3 + x + 6$ în $\underline{\underline{Q[x]}}$

pot împărti atât numărăt

coef. dominant (care evident e nenul) e irr. în $\underline{\underline{Q}}$

care e coprime, deci orice nenul e irr. în $\underline{\underline{Q}}$

\Rightarrow pot împ. orice le orice $\neq 0$.

$$\begin{array}{c|cc} x^4 + x^2 + 5 & x^3 + x + 6 \\ -x^4 - x^2 - 6x & \hline -6x + 5 & \end{array}$$

rest $-6x + 5$

$$\begin{aligned} \text{Ob. că } \text{grad}(-6x+5) &= \\ &= 1 < 3 = \text{grad} \\ &\underline{(x^3 + x + 6)} \end{aligned}$$

$$\Rightarrow x^4 + x^2 + 5 = (x^3 + x + 6) \cdot x + (-6x + 5)$$

cântul = x restul = $-6x + 5$

$$(2) \quad \text{gcd} (x^5 + x^2 + 5, x^5 + 6x + 9) \text{ în } \mathbb{Z}_2[X]$$

Când $R[X] = K[X]$ K corp, atunci $K[X]$ are o strucție similară cu \mathbb{Z} i.e. orice proprietate de divizibilitate din \mathbb{Z} există și în $K[X]$.

Atfel pus, se poate calcula comodă, al doilea polinom cu Alg. lui Euclid, zintă restul în loc să se scadă în modul, se scadă împărțit.

$\mathbb{Z}_2[X]$: coeficienți sunt close în $\mathbb{Z}_2 = \{0, 1\}$.

$$x^5 + x^2 + 5 = x^5 + x^2 + 1; \quad x^5 + 6x + 9 = x^5 + 1$$

$$\begin{array}{r} x^5 + x^2 + i \\ -x^5 - x^2 \\ \hline = i \end{array} \quad \left| \begin{array}{l} x^3 + i \\ x^2 \text{ rest } i \end{array} \right.$$

$$x^5 + x^2 + i = (x^3 + i) \cdot x^2 + i$$

$$x^3 + i = i \cdot (x^3 + i) + 0$$

$$\Rightarrow \text{cmmdc} = i$$

Analog prozedur

$$(4) \quad I = (x)$$

Pp. e2

$$P=7 \quad Q=7$$

$$\begin{array}{r} x^5 + x^3 + i \\ -x^5 - x^3 - x^2 \\ \hline = -x^2 + i \end{array} \quad \left| \begin{array}{l} x^3 + x + i \\ x^2 - i \text{ rest } x \end{array} \right.$$

Alg. Euclid:

$$\begin{array}{r} x^5 + x^2 + i \\ -x^5 - x^3 - x^2 \\ \hline = -x^3 + i \\ + x^3 + x + i \\ \hline x + i = X \end{array} \quad \left| \begin{array}{l} x^3 + x + i \\ x^2 - i \text{ rest } x \end{array} \right.$$

$$x^5 + x^2 + i = (x^3 + x + i) \cdot (x^2 - i) + X$$

$$x^3 + x + i = X(x^2 - i) + i$$

$$X = i \cdot x + 0$$

$$\Rightarrow \text{cmmdc} = i$$

$$a \cdot e \cdot 1 = ($$

pqr. $x=5$

$$\begin{array}{r} x^3 + x + i \\ -x^3 \\ \hline x + i \end{array} \quad \left| \begin{array}{l} X \\ x^2 - i \text{ rest } i \end{array} \right.$$

$$\frac{x}{i}$$

$$x^5 + x^2, x^3 + x + i \quad \begin{array}{r} x^5 + x^2 \\ -x^5 - x^3 - x^2 \\ \hline -x^3 \\ + x^3 + x + i \\ \hline x + i \end{array} \quad \left| \begin{array}{l} x^3 + x + i \\ x^2 - i \text{ rest } (x + i) \end{array} \right.$$

$$x^5 + x^2 = (x^3 + x + i)(x^2 - i) + (x + i)$$

$$x^3 + x + i = (x + i)(x^2 - i) + 1$$

$$1 = i \cdot (x + i) + 1$$

$$\Rightarrow \text{cmmdc} = 1$$

$$\frac{a+b}{2}$$

$$2m+1$$

$$2m+1$$

$$= \underline{2m+1}$$

$$= \underline{m+m}$$

$$= m-m+$$

Analog se procedeet in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_p[x]$.
pprim.

(i) $I = (x - 5, 6)$ in $\mathbb{Z}[x]$. Zeige, dass $I \neq \mathbb{Z}[x]$.

Pr. es. $(x - 5, 6) = \mathbb{Z}[x]$

$$i \in \mathbb{Z}[x] \Rightarrow i \in (x - 5, 6) \Rightarrow \exists g(x), h(x) \in \mathbb{Z}[x]$$

d.h. $i = (x - 5)g(x) + 6h(x)$.

ptr. $x = 5 \Rightarrow i = 0 \cdot g(5) + 6h(5)$
+ 1
 $i = 6h(5) \Rightarrow 6 | i$ ab

$$(2 \ 4 \ 7 \ 8 \ 6) \quad \mathbb{Z}_5 \cdot \widehat{2011} = \overline{1}$$

$$\overline{1} + \sqrt{-1}$$