ITINERARII ÎN CERCETARE

A tacit rite of passage for the mathematician is the first sleepless night caused by an unsolved problem.

B. Reznick

Everything should be made as simple as possible but not simpler.

A. Einstein

Mathematics is the study of mental objects with reproducible properties.

R. Davis, R. Hersh

Prof. univ. dr. Ioan TOFAN

Zilele Universității „Alexandru Ioan Cuza” din Iași

octombrie 2016

PREMISE

- 1. Platon – teoria ideilor numere (Theaitetos, Timaios)
- Aristotel – abstracție idealizantă (Metafizica)
- 2.

M, $\in$

ax. Z-F

alg. Boole

t. categ.

relații
funcții

algebre Heyting

Ex. 1 T. Pitagora $a^2 + b^2 = c^2$

- înlocuirea pătratelor (reprezentare geometrică) cu figuri similare (între ele)
- t. cosinusului
- plan și spațiu (tetraedru)
- geometrie Riemann $a^2 + b^2 + O\left(\frac{1}{r^2}\right) = c^2$
- geometrie Lobacevski
- ? T. Pitagora $\Leftrightarrow$ ax. paralelelor

- Triplete pitagoreice (x, y, z) (din $\mathbb{Z}$)

  $x^2 + y^2 = z^2$ (ec. diofantică)

  Proprietăți - y par $\Rightarrow$ 4/y

  - 5/x sau z
  - etc.
- Triplet primitiv = pitagoreic și $(x, y) = 1$

  (rezultă și $(x, z) = 1 = (y, z)$)
- Problemă (reprezentări de numere):

  $$k = x^2 + y^2$$

  $$k^2 = x^2 + y^2$$
- T. $p > 2$, prim este sumă de pătrate $\Leftrightarrow p = 4k + 1$
- T. (Sierpinski) $z > 0$ satisf. $\exists x, y: z^2 = x^2 + y^2 \Leftrightarrow z$ are un factor prim de forma $4k + 1$.
- Probleme: - Nr. de reprezentări (pentru un p sau z).

  - Reprezentări: $x_1^2 + \ldots + x_k^2$

$$x^2 + y^2 = z^2 \Rightarrow \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \text{ (t. primitiv)}$$

- →coresp. bijectivă între $\{t.p\}$ și {puncte de coord. raționale de pe cercul unitar aflate în primul cadran (fără axe)}.
- ! Diofant – metodă de determinare a pct. de coordonate raționale de pe conice.

Probleme: - triplete de nr. raționale, „pitagoreice”

$$\left(\frac{x_1}{x_2}, \frac{y_1}{y_2}, \frac{z_1}{z_2}\right) \ \left(\frac{z_1}{z_2}\right)^2 = \left(\frac{x_1}{x_2}\right)^2 + \left(\frac{y_1}{y_2}\right)^2$$

Obs. $\Leftrightarrow (x_1 y_2 z_2, x_2 y_1 z_2, x_2 y_2 z_1)$ t. pitagoreic.

- legătura cu $E(\mathbb{Q})$ grupul abelian al pct. de coord. raționale de pe curbe eliptice.

  (T. Mordell: $E(\mathbb{Q})$ este finit generat)

- studiul proprietăților unor mărimi atașate t. p. (de ex. aria triunghiului dreptunghic asociat).

- Notăm $\mathrm{A}(p,q,r)$ aria tr. dreptunghic coresp. $(p,q,r \in \mathbb{Q})$.
- Obținem: $1,2,3 \neq \mathrm{A}(p,q,r)\ \ \forall t.p.$

$$\mathrm{A}(p,q,r) \neq k^2$$

(consecințe pentru ec. diofantice $x^4 - y^4 = z^2$, $x^4 + y^4 = z^4$).

! Fie E_n curba eliptică dată de $y^2 = x^3 - n^2x$.

T. n liber de pătrate este de forma $\mathrm{A}(p,q,r) \Leftrightarrow E_n(\mathbb{Q})$ are un element de ordin infinit.

Ex. 2. Fie $R_0 \subseteq R_1$ inele com., unitare $P \in R.[X]$. Se cer rădăcinile din R_1.

- cazuri: $R_0 = R_1 = \mathbb{Z}$, etc.; nr. răd.; intervale.
- soluțiile – numere algebrice.

1. $P \in R_0[X, Y]$

   $\text{Zero}(P) = \{(\alpha, \beta) \in R_1^2 / P(\alpha, \beta) = 0\}$

   $R_1 = \mathbb{R}$, $\text{Zero}(P)$ - curbă plană (curbă algebrică)

2. $P \in R_0[X, Y, Z]$ - suprafețe algebrice
3. $P \in R_0[X_1, \dots, X_d]$ - hipersuprafețe algebrice

- $(*)\begin{cases} P_1 = 0 \\ \quad\vdots \\ P_m = 0 \end{cases}$ $\qquad P_i \in R_0[X_1, \dots, X_d]$.

Zero$(P_1, \dots, P_m)$! Zero$(P_1, \dots, P_m)$=Zero$(\langle P_1, \dots, P_m \rangle)$

Pentru $J \subseteq R_0[X_1, \dots, X_d]$, Zero$(J)$

(pt. R_1 corp - Zero(J) - **mulțime algebrică**)

! $R_1 = \mathbb{C}$ (algebraic închis).

Wu Wen-tsun: *Mechanical Theorem Proving in Geometries*, Springer, 1994

(rezolvare pentru $(*)$)

! Sisteme de forma $\begin{cases} P_1 = 0, \dots, P_k = 0 \\ P_{k+1} > 0, \dots, P_l > 0 \\ P_{l+1} \geq 0, \dots, P_m \geq 0 \end{cases}$

sau cu tipuri particulare de polinoame.

- $R_0[X_1, \dots, X_d]$; R_1^d ($\mathbb{A}^d(R_1)$), top. Zariski.
- $J \subseteq R_0[X_1, \dots, X_d]$ $\rightsquigarrow$Zero(J)$\subseteq R_1^d$

întoarcere la algebră

- $U \subseteq R_1^d \rightsquigarrow$ Ideal$(U) = \{P \in R_0[X_1, \dots, X_d]\ a.i. P(\alpha_1, \dots, \alpha_d) = 0$ $\forall(\alpha_1, \dots, \alpha_d) \in U\}$ (! este ideal)
- - $\begin{cases} \text{Ideal}(\text{Zero}(J)) \\ \text{Zero}(\text{Ideal}(U)) \end{cases}$
- $J \subseteq \text{Ideal}\big(\text{Zero}(J)\big)$
- Zero(Ideal(Zero(J)))=Zero(J)
- $U \subseteq$ Zero(Ideal(U))
- Ideal(Zero(Ideal(U)))=Ideal(U)

Probleme:

- Restricţia: J ideal; R_1 corp alg. închis ($\mathbb{C}$) (U mulț. alg.)

- idealele inelului $R_0[X_1, \dots, X_d]$ - finit/infinit generate; privite în $R_1[X_1, \dots, X_d]$

- (T. bazei Hilbert: R_0 noetherian $\Rightarrow R_0[X_1, \dots, X_d]$ noetherian)

- Date $P_0, P_1, \dots, P_m \in R_0[X_1, \dots, X_d]$, avem $P_0 \in \langle P_1, \dots, P_m \rangle$? (baze Gröbner)

- (T. zerourilor, Hilbert) (bijecție: mulț. alg - radicali)
- J = Ideal(Zero(J))$\Leftrightarrow$J este radical

- ! Idealele – mai multe informații decât mulț. alg.

Ex. 3 Geom. pct. laticeale (coord. $\in \mathbb{Z}$)

- l-dreapta ($\equiv$ dreaptă ce conține 2 puncte laticeale distincte)

- l-segment ($\equiv$ segment cu extremități – p. laticeale)

- l- poligon ($\equiv$ cu vf. în p. laticeale).

Obs. i) $s =$ lungimea unui l -segment $\Rightarrow s^2 \in \mathbb{N}$

- ii) $\alpha = \sphericalangle\, l$ -drepte, $\alpha \neq \frac{\pi}{2}, 3\frac{\pi}{2} \Rightarrow \text{tg}\alpha \in \mathbb{Q}$
- iii) $\nexists\ l$ -triunghiuri echilaterale.

Problemă

- l-poligoane regulate (! doar pătrate)

- l – poligon primitiv (singurele p. laticeale din interior sau de pe laturi: vârfurile)

- baze în $\mathbb{Z}^2$ (ca $\mathbb{Z}$-modul) (laturi pentru l –triunghiuri primitive)

- ! Paralelogramul pe elem. unei baze este l – paralelogram (și are aria =1).

Problemă

– aria unui l –poligon

- T. Pick: $A = \frac{1}{2}B(P) + I(P) - 1$
- $B(P)$ = nr. p. laticeale de pe laturile poligonului)
- $I(P)$ = nr. p. laticeale interioare poligonului
- T. $n =$ aria unui l – pătrat $\Leftrightarrow$ $n =$sumă de pătrate de întregi nenegativi

Probleme: - pct laticeale $p = (a, b)$ cu a, b relativ prime.

- ! pe l dreapta ce conține $(0,0)$ și (a, b) avem că (a, b) este cel mai apropiat de origine.
- Fie P un l-pătrat de latură t (centrul în origine) și $N(t)$-p. laticeale, $V(t)$-p. laticeale cu (a, b) relativ prime (din P).

$$\lim_{t\to\infty} \frac{V(t)}{N(t)} = \frac{6}{\pi^2}$$

- Fie $C(\sqrt{n})$ cerc centrat în origine de rază $\sqrt{n}$ și $L(n) =$ nr. pct. laticeale din și de pe cerc

$$\lim_{n\to\infty} \frac{L(n)}{n} = \pi$$

– l triunghiuri T cu $I(T) = 0$ sau 1.

– legătură p. laticeale $p = (a, b)$, unde a, b-prime între ele cu șirurile Farey.

– legătura cu T. Minkowski (pt. $\mathbb{R}^2$: s mărg., convexă, simetrică față de origine ⇒ s conține p. laticeale ≠ $(0,0)$ și are aria > 4; similar pt $\mathbb{R}^k$).

– polinoamele Ehrhart

Ex. 4 Aproximări diofantice

- Obs. $\left|\frac{a}{b}-\frac{p}{q}\right|<\frac{1}{bq}\Rightarrow\frac{a}{b}=\frac{p}{q}$

- $0<\left|\frac{a}{b}-\frac{p}{q}\right|<\frac{1}{mb}\Rightarrow q>m$

- $\alpha\in\mathbb{R}, \delta, \eta\in\mathbb{R}_+\Rightarrow\exists$ nr finit de $\frac{p}{q}\in Q$ cu $q\leq n$ a.i.

  $\left|\alpha-\frac{p}{q}\right|\leq\delta$.

- ! Nr. raționale „apropiate” de numere reale
- T. Dirichlet $\alpha \in \mathbb{R}$, $n \in \mathbb{N}^*$. $\exists \frac{p}{q} \in \mathbb{Q}$ cu $0 < q \leq n$ a.î. $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(n+1)q}$
- Obs. Ineg. nu poate fi îmbunătățită (n fixat, $\exists\alpha$, cu „=”)
- Consec. i) $\forall\alpha \in \mathbb{R}\ \exists \frac{p}{q} \in \mathbb{Q}$: $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$
- ii) α irațional $\Rightarrow\exists$ o infinitate de nr. $\frac{p}{q} \in \mathbb{Q}$ a.i. $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Problemă: $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ poate fi îmbunătățită?

- De ex. $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$?
- T. Hurwitz Fie α irațional. ∃ o infinitate de nr. raționale $\frac{p}{q}$ a.î. $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$
- (și constanta $\sqrt{5}$ este cea mai bună posibilă).

Problemă: determinarea lui $\frac{p}{q}$ din T. Dirichlet

- \- algoritm (v. teoria fracțiilor continue)

Alte probleme: - legătura cu Alg. Euclid

- \- unicitatea dezvoltării în fr. continue (raționale/iraționale)

- Obs. Ineg. Dirichlet $\Rightarrow |\alpha q - P| \leq \frac{1}{n+1} \Rightarrow$ reformulare
- $\exists q \in \mathbb{Z}: 1 \leq q \leq n$ și $\|aq\| \leq (n+q)^{-1}$ $(\|x\| = min\{x - n/n \in \mathbb{Z}\})$
- $\longrightarrow$ T. Lagrange, T. Legendre („cea mai bună aproximație”)
- \- T. Liouville

I ask circumspect questions to avoid circumspect answers.

Stanislav Jerzy Lec