

Az aritmetika és a számelmélet története az ókortól Hilbert VII. problémája megoldásáig.

Bevezető gondolatok.

Klukovits Lajos

TTIK Bolyai Intézet

2016. február 4.

A két fő témakör.

1. Aritmetika.

- ➊ Mit értettek számon az egyes történelmi korokban, pontosabban a mai számfogalom terminusait használva, milyen típusú számokat ismertek, használtak.
- ➋ Az adott korban ismert számokkal hogyan számoltak.
- ➌ Az igényeknek megfelelően hogyan definiáltak, használtak újabb típusú számokat.

A két fő témakör.

2. Számelmélet.

- ➊ A számelmélet alapvetően az egész számokkal kapcsolatos kérdésekkel foglalkozik.
- ➋ Módszereit, problémafölvetéseit figyelembe véve 4 fő irányzata van.
 - ➊ Klasszikus számelmélet: a problémák megfogalmazásában és azok kezelésében, valamint a bizonyításokban használt fogalmak és módszerek nem terjednek túl az egész számokon.
 - ➋ Analitikus számelmélet: a bizonyításokban, sőt olykor a problémák megfogalmazásában analitikus/függvénytan fogalmakat és módszereket alkalmaznak.
 - ➌ Algebrai számelmélet: az egész számok alkotta gyűrű általánosításait vizsgálja absztrakt algebrai módszerekkel.
 - ➍ Kombinatorikus számelmélet: kombinatorikai módszereket (is) használ. (E területre eső kérdéseket nem fogunk érinteni.)

Példák az egyes számelméleti irányzatokra.

Klasszikus számelmélet.

- Pithagoraszai számhármások.
- Tökéletes számok, barátságos számpárok.
- Speciális alakú prímek, pl. Mersenne prímek, Fermat számok.
- Lineáris kongruencia rendszerek.
- Határozatlan egyenletek az egész számok fölött.
- Hatványösszegekre bontás.

Analitikus számelmélet.

- Becslések a prímszámokkal kapcsolatban, a prímszámok eloszlása.
- Diofantikus approximáció.
- Transzcendens számok.

Példák az egyes számelméleti irányzatokra.

Algebrai számelmélet

- A Fermat probléma. (A megoldás az $n = 3$ esetben.)
- Kvadratikus testek (a racionális számtest másodfokú bővítései), ezek egészeinek gyűréje.
- Prímfaktorizációs testek (meddig általánosítható a számelmélet alaptétele).

I.e. XX-XIX. század: az Egyiptomi Középbirodalom kora.

Rhind 40. probléma, egy határozatlan egyenletre vezető.

100 cipót úgy kell elosztani 5 ember között, hogy a két legkisebb összege egy hetede legyen a 3 legnagyobb összegének. Mennyi a differencia?

Kommentár.

A megoldásból kiolvasható, hogy az egyes emberek között kiosztandó mennyiségek számtani sorozatot alkotnak, és a kérdés ennek a differenciájára utal.

A megoldást mai, nem a korabeli szimbolikával adjuk meg.

I.e. XX-XIX. század: az egyiptomi középbirodalom kora.

A megoldás.

1. Ha a differencia $5\frac{1}{2}$ lenne, akkor egy lehetséges elosztás

$$1, \quad 6\frac{1}{2}, \quad 12, \quad 17\frac{1}{2}, \quad 23.$$

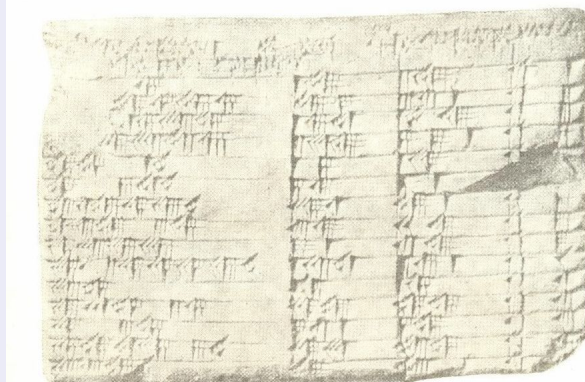
2. Ez kielégíti a föltételt, de
3. a tagok összege csak 60, azaz csak 60 cipót osztottunk el 100 helyett.
4. A 100-hoz még 40 kell, ami a 60 kétharmada.
5. Az előbbi sorozatot „arányosítani” kell: azaz megszorozni $1\frac{2}{3}$ -dal,
6. így a megoldás

$$1\frac{2}{3}, \quad 10\frac{2}{3} + \frac{1}{6}, \quad 20, \quad 29\frac{1}{6}, \quad 38\frac{1}{3}.$$

7. A végleges differencia: $9\frac{1}{6}$.

I.e. XVIII. század: az Óbabiloni Birodalom.

A Plimpton 322. agyagtábla.



A Plimpton 322. agyagtábla, Neugebauer átírásában.

[1, 59, 0,]15	1, 59	2, 49	1
[1, 56, 56,]58, 14, 50, 6, 15	56, 7	3, 12, 1	2
[1, 55, 7,]41, 15, 33, 45	1, 16, 41	1, 50, 49	3
[1,]5[3, 1,]0, 29, 32, 52, 16	3, 31, 49	5, 9, 1	4
[1,]48, 54, 1, 40	1, 5	1, 37	5
[1,]47, 6, 41, 40	5, 19	8, 1	6
[1,]43, 11, 56, 28, 26, 40	38, 11	59, 1	7
[1,]41, 33, 59, 3, 45	13, 19	20, 49	8
[1,]38, 33, 36, 36	9, 1	12, 49	9
1, 35, 10, 2, 28, 27, 24, 26, 40	1, 22, 41	2, 16, 1	10
1, 33, 45	45	1, 15	11
1, 29, 21, 54, 2, 15	27, 59	48, 49	12
[1,]27, 0, 3, 45	7, 12, 1	4, 49	13
1, 25, 48, 51, 35, 6, 40	29, 31	53, 49	14
[1,]23, 13, 46, 40	56	53	15

I.e. XVIII. század: az Óbabiloni Birodalom.

Mit rejt ezen agyagtábla?

- A mezopotámiaiak 60-as helyiértékes számírást alkalmaztak, amely mindössze két jelet használt.
- Ezt Neugebauer ügyesen írta át decimális jegyekkel.
- A töredékes táblán 4 oszlopban és 15 sorban állnak számok.
- Ha az első oszlopbeli számok négyzetét rendre kivonjuk a harmadik oszlopbeli számok négyzetéből, akkor a második oszlopbeli számok négyzeteit kapjuk. **(Megjegyzés. A számok nem föltétlenül egészek.)**
- Mit rejt ez?
- Nyilván az ismert Pithagorasz tételt, pontosabban ún. **pithagorasz számhármassokat**, DE
- **közel 1500 évvel Pithagorasz előtt.**
- Ez tekinthető a jelenleg ismert legkorábbi tisztán számelméleti eredménynek.

A legkorábbi szigorúan bebizonyított számelméleti eredmények.

Definíciók Euklidesz Elemek c. művéből.

- **VII.1.D** Az **egység** az, ami szerint minden létezőt egynek mondunk.
- **VII.2.D** A **szám** az egységekből összetevődő sokaság.
- **VII.3.D** Egy kisebb szám egy nagyobbban **hányada** (része), ha osztja a nagyobbat.
- **VII.12.D** **Prímszám**, amelyik csak az egységgel osztható.
- **VII.23.D** Egy szám **tökéletes**, ha egyenlő osztói (részei) összegével.

Két tétel a IX. könyvből.

- **IX.20.** Prímszámok bármely adott sokaságánál van több.
- **IX.36.** Ha az egységtől indulva kétszeres arányban mértani sorozatot alkotunk addig, amíg az összeg prímszám nem lesz, és ezt megszorozzuk az utolsó taggal, akkor tökéletes számot kapunk.

Ókori görög eredetű, maig nyitott kérdések.

- Euklidesz IX.36. Tételének megfordítását a XVIII. században igazolta Euler.
- A két tételt egybe fogalmazva:
 - ▶ Egy páros szám pontosan akkor tökéletes szám, ha $2^{p-1}(2^p - 1)$ alakú, ahol p és $2^p - 1$ prím.
 - ▶ Például $6 = 2(2^2 - 1)$, $28 = 2^2(2^3 - 1)$,...
- **Van-e végtelen sok páros tökéletes szám? Van-e páratlan tökéletes szám?**
- Azt mondjuk, hogy (m, n) **barátságos számpár**, ha mindkettő egyenlő a másik osztói (kivéve magát a számot) összegével.
 - ▶ Például a 220 és a 284 ilyen. (Már a Bibliában is szerepel.)
- **Létezik-e végtelen sok barátságos számpár?**
- **Létezik-e olyan barátságos számpár, amelyiknek tagjai különböző paritásúak?**
- Tabit ben Qurra (IX. sz.) eredménye pontosítva: Ha p, q, r speciális alakú prímek, akkor $m = 2^k pq$ és $n = 2^k r$ barátságos számpár.

Határozatlan egyenletek és egyenletrendszerek 1.

Diophantos I.sz. 250 körül

- 1. Keressünk három olyan számot, hogy közülük bármely kettőnek a szorzatát egy adott számmal növelve négyzetszámot kapunk. (Aritmetika Γ 10. probléma)
- 2. Keressünk két olyan négyzetszámot, amelyek összege köbszám. (Aritmetika 4. 3. probléma)

Aryabhata és Brahmagupta, I.sz. VI.-VII. sz.

Keressünk olyan y számot, amelyre b_1y -t a_1 -gyel osztva c_1 , és b_2y -t a_2 -vel osztva c_2 maradékot kapunk. Másképpen, megoldandó az

$$a_1x_1 + c_1 = b_1y$$

$$a_2x_2 + c_2 = b_2y$$

egyenletrendszer.

Határozatlan egyenletek és egyenletrendszerek 2.

Aryabhata és Brahmagupta, I.sz. VI.-VII. sz.

- Egy példa (a hinduk CSAK konkrét számokkal dolgoztak).

$$29x_1 + 4 = 8y$$

$$25x_2 + 7 = 17y$$

- Egy megoldás: $y = 1001$, $x_1 = 276$, $x_2 = 378$.

Kína: A matematika művészete 9 könyvben.

- 576 pénzért 78 bambuszrudat veszünk, hosszút és rövidet. Mennyit veszünk az egyes fajtákból, és mennyi az áruk.
- A megoldás, 48 rövidet egyenként 7 pénzért és 30 hosszút egyenként 8 pénzért.

A „kínai maradéktétel”.

1. probléma.

- Van egy csomó tárgyunk, de nem tudjuk mennyi. Ha hármasával számoljuk le, kettő kimarad. Ha ötösével számolunk három, míg ha hetesével számolunk kettő marad ki.
- A tárgyak száma 23.

2. probléma.

17 kalóz zsákmányolt egy láda aranyat. Egyenlő arányban akarták elosztani, de 3 arany kimaradt. Ezen összevesztek, és egy társukat megölték. Újra kezdték az elosztást ugyanúgy, de most 10 arany maradt ki. Ezen ismét összevesztek, és ismét megölték egy társukat. Most már el tudták osztani úgy az aranyat, hogy mindenkinek ugyanannyi jutott. Hány arany volt a ládában?

A ládában 3930 arany volt.

Az európai kezdet, a pisai Leonardo.

A Liber abaci egy feladata.

- Egy ember 30 madarat vásárol: foglyokat, galambokat és verebeket. A fogoly ára darabonként 3 ezüst, a galamboké 2, míg a verebeké $\frac{1}{2}$. Összesen 30 ezüstöt fizet. Hány madarat vett az egyes fajtákból?
- Az egyetlen pozitív megoldás a 3, 5, 22.
- **Megjegyzés.** E probléma számos ókori kultúrában is szerepel.

Palermoi János egy problémája a Liber quadratorumból.

- Melyik az a négyzetszám, amelyhez 5-öt adva is és 5-öt kivonva is négyzetszámok kapunk.
- A megoldandó egyenletrendszer

$$x^2 + 5 = y^2$$

$$x^2 - 5 = z^2$$

Leonardo megoldása.

$$x = 3 + \frac{5}{12}, \quad y = 4 + \frac{1}{12}, \quad z = 2 + \frac{7}{12}.$$

Megjegyzés. Abban a korban — részben ókori mintára — nem ragaszkodtak az egész megoldáshoz, megelégedtek racionálissal.

Elemek X. Könyv (az irracionálisok ókori elmélete).

- **X.1.D** Mennyiségeket *összemérhető*eknek mondunk, ha ugyanazon mértékkel mérhetők, *összemérhetetlenek*nek pedig, ha nem található hozzájuk közös mérték.
- **X.4.D** És nevezzük az adott szakasz négyzetét *racionális*nak, és az azzal összemérhető felületeket racionálisnak, az azzal összemérhetetleneket pedig *irracionálisok*nak, az őket előállító szakaszokat — ti. ha a felületek négyzetek, magukat az oldalakat, ha pedig valamely más sokszögek, a velük egyenlő négyzeteket fölrajzoló szakaszokat — irracionálisoknak.
- **X.2.T** Ha adva van két nem egyenlő mennyiség, a kisebbet váltakozva mindig kivonjuk a nagyobbból, és a maradék sohasem méri az előzőt, akkor a mennyiségek összemérhetetlenek.

Irracionális számok 1.

Hinduk a VII.-X. században.

- Korrekt módon számoltak gyökmennyiségekkel, de semmit sem bizonyítottak.
- Szabályokat fogalmaztak meg, amelyeket számpéldákkal illusztráltak.
- Egy illusztráló példa

$$\sqrt{3} + \sqrt{12} = \sqrt{(3+12) + 2\sqrt{3 \cdot 12}} = \sqrt{27} = 3\sqrt{3}.$$

- Tulajdonképpen a

$$\sqrt{a} + \sqrt{b} = \sqrt{(a+b) + 2\sqrt{ab}}$$

azonosságot alkalmazták. Természetesen $a, b > 0$.

Irracionális számok 2.

Hinduk a VII.-X. században.

- Látható, hogy az irracionálisokkal ugyanúgy bántak, mint az egészekkel, a

$$c + d = \sqrt{(c+d)^2} = \sqrt{c^2 + d^2 + 2cd}$$

azonosságot írták át.

- Bhaskara egy szabálya két irracionális összegére: *A nagyobbik és a kisebbik hányadosának négyzetgyökét növelj eggyel, vedd ezen összeg négyzetét, majd szorozd meg a kisebbel, és ennek négyzetgyöke a két négyzetgyök összege.*
- Illusztráló példája:

$$\sqrt{3} + \sqrt{12} = \sqrt{\left(\sqrt{\frac{12}{3}} + 1\right)^2 \cdot 3} = 3\sqrt{3}.$$

Irracionálisok a XVI.-XVII. században

Rövid áttekintés.

- 1500 körül az európai matematikusok, elsősorban az iszlám tradíciók alapján, már egyre kiterjedtebben számoltak gyökmennyiségekkel,
- speciális típusokat definiáltak és kalkulusokat adtak meg, pl. a $\sqrt[n]{a + \sqrt[n]{b}}$ alakúakra (Stevin).
- Az a kérdés, hogy az irracionálisok, a gyökmennyiségek, számok, vagy nem még jó ideig élénk vita tárgya volt.
- De tisztázatlan a 0 státusza, valamint az, hogy mik is a negatív számok (pl. a hiányt jelző mennyiségek), számok e egyáltalán.

Irracionálisok a XVI.-XVII. században

Stiefel, Arithmetica integra, 1544.

Mivel az olyan geometriai bizonyításokban, ahol a racionális számok nem megfelelőek alkalmazhatók az irracionális számok, és velük elvégezhetjük a bizonyításokat; az irányba kényszerülünk haladni, hogy kijelentsük: az irracionálisok igenis számok, mivel a velük kapott eredmények reálisok (valóságosak). Másrészt azonban más megfontolások arra készítetnek bennünket, hogy tagadjuk azt, hogy az irracionálisok egyáltalán számok. Ugyanis, amikor számolunk velük (tizedestört alakban) azt tapasztaljuk, hogy nem lehet őket pontosan meghatározni. Így nem nevezhetjük őket igazi számoknak, mivel természetüknél fogva hiányzik belőlük a precizitás. Ezért, ugyanúgy mint ahogy a végtelen nem szám, egy irracionális szám sem igazi szám, hanem éppúgy valami ködös végtelen.

Irracionálisok a XVI.-XVII. században

B. Pascal.

Úgy vélte, hogy az olyan mennyiségek, mint például a $\sqrt{3}$ csak geometriai mennyiségként fogható föl. Az irracionálisok pusztán szimbólumok, amelyek nem léteznek az általuk reprezentált folytonos geometriai mennyiségtől függetlenül. A velük való számolásokra tehát nem aritmetikai szabályok vonatkoznak, hanem az Eudoxos-féle arányelméletet (Euklidesz V. könyve) kell alkalmazni.

Lényegében ugyanezen véleményt olvashatjuk Newton *Arithmetica Universalis* c. könyvében, amely 1707-ben jelent meg, de kb. 30 évvel korábbi eredményeinek összefoglalása.

Irracionálisok a XVI.-XVII. században

Néhány érdekesség.

- J. Wallis
$$\frac{4}{\pi} = \frac{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \dots}{2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdot 8 \dots}$$
- F. Viete formulája π -re, amelyet körbe írt 4, 8, 16, ... oldalú sokszögek segítségével nyert:

$$\begin{aligned} \frac{2}{\pi} &= \cos \frac{90^\circ}{2} \cos \frac{90^\circ}{4} \cos \frac{90^\circ}{8} \dots \\ &= \sqrt{\frac{1}{2}} \sqrt{\frac{1}{2} + \frac{1}{2} \sqrt{\frac{1}{2}}} \sqrt{\frac{1}{2} + \frac{1}{2} \sqrt{\frac{1}{2} + \frac{1}{2} \sqrt{\frac{1}{2}}}} \dots \end{aligned}$$

- Bombelli láncörtöje: $\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \dots}}$

A negatív számok és a nulla.

Egy XVI. századi feladat.

- Az apa most 56, a fia 29 éves. Hány év múlva lesz az apa kétszer annyi idős, mint a fia?

- Az

$$56 + x = 2(29 + x)$$

egyenlet megoldása: $x = -2$.

- Hogyan lehet ezt értelmezni?

- A

$$(-1) : 1 = 1 : (-1)$$

arány kérdése.

Komplex számok.

Egy integrálási probléma.

- John Bernoulli és Leibniz az

$$\frac{a^2}{a^2 - x^2} = \frac{a}{2} \left(\frac{1}{a+x} + \frac{1}{a-x} \right)$$

fölbontást használta.

- De ezt általánosították az $\int \frac{dx}{ax^2+bx+c}$ esetre is, ahol már negatív (esetleg komplex) szám logaritmus is előkerül, mivel a másodfokú polinomnak negatív (komplex) gyöke is lehetett.

Euler.

Inkorrekt úton korrekt megoldás a negatív (komplex) számok logaritmusára.

Transzcendens számok 1.

Euler egy fölvetése.

- Lehetnek olyan számok, amelyek **meghaladják az algebrai módszerek erejét**.
- Ezek azok a számok, amelyek nem lehetnek gyökei racionális (egész) együtthatós egyenleteknek.

Euler sejtése.

- Ebbe a kategóriába tartozik a két neves konstans az

$$e \text{ és } \pi$$

valamint a logaritmus- és a trigonometrikus függvények értékeinek zöme.

- Bizonyítani csak azt tudta, hogy az e irracionális.
- Tanítványa Lambert megmutatta, hogy π is irracionális.

Transzcendens számok 2.

Egy súlyos probléma.

- A matematika, különösen az analízis (a függvénytan) súlyos válságba került a XIX. század fordulóján.
- Elkerülhetetlennek látszott a visszatérés a deduktív tárgyalásmódhoz.
- Számos bizonyítási kísérlet sikertelen lett még alapvető tételeknél is.
- A fő ok a **valós szám fogalmának tisztázatlansága**.

Liouville 1844.

- Algebrai szám: az olyan komplex szám, amely lehet egész együtthatós polinom gyöke. Az összes algebrai számok halmaza: $\mathbb{A}$.
- Az algebrai számok általában **rosszul approximálhatók** racionális számokkal.

Transzcendens számok 3.

Liouville példája 1844.

A

$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

végtelen sor konvergens, és összege transzcendens szám.

Néhány további eredmény

- 1873. Hermite: e transzcendens.
- 1874. Cantor: Kontinuum sok transzcendens szám van.
- 1882. Lindemann: A π transzcendens.

Egy meglepő eredmény.

A mai napig nem ismert, hogy $e + \pi$ milyen szám, míg az, hogy $e + i\pi$ transzcendens egyetlen sorban igazolható.

Transzcendens számok 4. David Hilbert 1900. Párizs.

Hermite és Lindemann eredményeit — amelyek az exponenciális függvényekre vonatkoznak — minden matematikus nagyra értékeli. Ezen az úton tovább kell haladni, s az elkövetkező időben az alábbi problémát kellene megoldani. Bizonyos — az analízisben fontos — transzcendens függvények egyes algebrai szám helyeken algebrai szám értékeket vesznek föl. Úgy tűnik, hogy ezt érdemes alaposan megvizsgálni. Ugyanis általában azt képzeljük, hogy a transzcendens függvények mindenütt transzcendens értékeket vesznek föl. Tesszük ezt annak ellenére, hogy ismerünk olyan transzcendens függvényeket, amelyek algebrai számokhoz algebrai számot, sőt racionálisat rendelnek.

Transzcendens számok 5. D. Hilbert 1900. Párizs (folytatás)

Például az $e^{i\pi z}$ exponenciális függvény értéke minden $z \in \mathbb{Q}$ -ra algebrai, míg minden $z \in \mathbb{A} \setminus \mathbb{Q}$ -ra transzcendens. Ezen állítás geometriailag is megfogalmazható. Ha egy egyenlőszárú háromszögben az alapon fekvő szög és a száraz által alkotott szög aránya transzcendens, akkor az alap és a szár aránya is transzcendens. Bár ez egy igen egyszerűen hangzó állítás, ekvivalens Hermite és Lindemann eredményével, s a bizonyítása is igen nehéz, sőt meglehetősen bonyolult. Hasonlóan nehéz lehet a bizonyítása a következő állításnak is.

Hilbert 1900-as előadása VII. problémája.

Ha $\alpha \in \mathbb{A}$ és $\beta \in \mathbb{A} \setminus \mathbb{Q}$, akkor az α^β alakú számok, például $2^{\sqrt{2}}$, $e^\pi = i^{-2i}$ mindig transzcendens számok, vagy legalább irracionálisok.

Vizsgarend

- A kollokvium írásbeli,
 - ▶ amely egy feleletválogatós tesztből,
 - ▶ és ezt követően röviden megválaszolandó kérdésekből áll.
- A teszten legalább 50%-s eredményt el nem érő vizsgázók esetén a további kérdéseket nem javítjuk, a vizsga elégtelen.

FONTOS!

Az írásbeli vizsgán előzetesen mindenkinek fényképes igazolvánnyal kell magát azonosítani, amely lehet az index, a diákigazolvány, a személyi igazolvány, vagy más — a vonatkozó jogszabályok szerinti — fényképes igazolvány.

IRODALOM

JAVASOLT IRODALOM 1.

- B. L. van der Waerden, **Egy tudomány ébredése**, *Gondolat*, 1977.
- A. P. Juskevics, **A középkori matematika története**, *Gondolat*, 1982.
- Euklidész, **Elemek**, *Gondolat*, 1983.
- Freud Róbert (szerk.) **Nagy pillanatok a matematika történetében**, *Gondolat*, 1981.
- Szénássy Barna, **A magyarországi matematika története**, *Polygon Könyvtár*, 2008.
- O. Neugebauer, **Egzakt tudományok az ókorban**, *Gondolat*, 1984.
- Szabó Árpád matematika történeti tárgyú írásai.

IRODALOM

JAVASOLT IRODALOM 2.

- M. Kline, **Mathematical Thought from ancient to modern Times**, *Oxford University Press* 1972, 1990.
- C. B. Boyer, **A History of Mathematics**, *Wiley & Sons*, 1968,
- U. C. Merzbach - C. B. Boyer, **A History of Mathematics**, *Wiley & Sons*, 2010.
- G. Flegg, **Numbers Through the Ages**, *Machmillan*, 1989
- J. Sesiano, **Books IV to VII of Diophantus' Arithmetica**, *Spriger*, 1982.

IRODALOM

NEM JAVASOLT MŰVEK

- Sain Márton könyvei,
- A tanárképző főiskolák matematika történeti tárgyú jegyzetei,
- Filep László könyvei,
- Ribnyikov, **A matematika története**, Tankönyvkiadó.