SZÁMELMÉLET

KÉSZÍTETTE: MÜLLER ISTVÁN 12.E

MI IS AZ A SZÁMELMÉLET?

- A **számelmélet** a matematika egyik ága, mely eredetileg a természetes számok oszthatósági tulajdonságait vizsgálta.
- Az ez irányú vizsgálatok elnevezésére még ma is alkalmazzák a számelmélet eredeti latinos elnevezését **(aritmetika)**. Utóbbi szót maga a latin is a görögből vette át („arithmosz": „szám", a görög szó az „összeácsolni, összetenni, összeilleszteni" igéből eredt).
- A természetes számok számelméleti tulajdonságai vizsgálhatóak egészen elemi eszközökkel is (elemi számelmélet), de a felsőbb matematika eszköztára (komplex analízis) segítségével is (analitikus számelmélet).
- A természetes számok körében felvetődő bizonyos kérdések tanulmányozása vezetett a számelmélet problémáinak és fogalmainak gyűrűkre vonatkozó kiterjesztéséhez, a gyűrűk (szám)elméletét **algebrai számelmélet**nek nevezzük.
- A számelmélet területén számos egyszerű, laikusok számára is könnyen érthető problémával találkozhatunk, amelyek megoldása azonban még a legnagyobb elméknek is komoly, sokszor megoldhatatlan kihívást jelent (lásd a Nagy Fermat-tételt vagy az ikerprím-sejtést).

MATEMATIKATÖRTÉNETI VONATKOZÁSOK

- Az első számelméleti jellegű felfedezés - természetesen maguknak a számoknak és a velük végzett alapműveleteknek a felfedezése után - a helyiértékes számábrázolásmód fokozatos kialakulása volt. E folyamat az őskor végén és az ókor elején indult, Európában csak a középkorra teljesedett ki. Ez még minden bizonnyal induktív alapokon és nem módszeres, elméleti vizsgálatok eredményeképp történt.
- Az **görög püthagoreusok** színre lépése több szempontból is nagyon fontos eredményeket hozott a számelmélet szempontjából. Először is, filozófiai és misztikus spekulációkkal tarkítva, és részben ezek által hajtva, igen érdekes és fontos tudományos felfedezéseket tettek, pl. a természetes számokat összegalakban próbálván előállítani, felfedezték a háromszögszámokat, valamint hasonló fogalmakat és az ezekkel kapcsolatos törvényeket.
- Rájöttek többek közt, hogy a páratlan számok sorozatának valamely tagig bezárólag történő összegzésével négyzetszám adódik.

MATEMATIKATÖRTÉNETI VONATKOZÁSOK

- Hirdették, hogy minden dolgok lényege a szám, hogy a természetes számokra építkezve a világ minden jelensége megmagyarázható. De saját maguk mérték filozófiájukra a legnagyobb csapást az összemérhetetlenség - mai szóval, az irracionális számok felfedezésével.
- Rájöttek ugyanis, hogy vannak olyan mértani alakzatok, pl. egy négyzet és átlója, melyek hosszúságviszonya nem írhatóak le egész számok arányaival, azaz hogy az általuk ismert algebra eszközei korlátozottabbak, mint a geometriai szemlélet.
- Ez a felfedezés meglepte az elméleti problémákat szerető és a tudományok iránt érdeklődő görögöket. Természetesen adódó válasz volt, hogy mértanként alakították ki matematikájukat (geometrizálás).
- Így a természetes számok, különösen tudományos szempontból, elvesztették kiemelt jelentőségüket, és sem velük nem foglalkoztak többé évszázadokig kiemelt módon, sem összeadásukkal. Ha összeadni kellett, az általában mértani alakzatként (egyenesszakasz) adódó valós számok összeadását jelentette, és konkrét esetben ezt a görög geométerek könnyedén elvégezhették körzővel.

MATEMATIKATÖRTÉNETI VONATKOZÁSOK

- A **görögök** után már aritmetikáról sem igen beszélhetünk mint tudományról: a rómaiak korától kezdve teljesen elvesztette minden elméleti jelentőségét. Bár **Proklosz** az *Elemek*hez írott ún. második előszóban leszögezi: a matematika két résztudományból áll, aritmetikából és geometriából, és az aritmetikát elvontsága miatt elsődleges figyelem illeti meg; ez valószínűleg egy tradicionális alapokon elfogadott, de a gyakorlatot illetően fokozatosan kiüresedett kijelentés volt, pont az *Elemek* főképp geometriával foglalkozik, és a püthagoreusok utáni időből sokáig nem maradt fenn olyan írott munka, ami az aritmetikával részletesen foglalkozna.
- Az aritmetika vizsgálatok az újkorban indultak meg újra, ebben kiemelt szerepe van **Carl Friedrich Gaussnak**. A huszadik században a számelmélet kettéosztható az ősibb multiplikatív számelméletre (ez főképp a prímek tanulmányozása, részben absztrakt algebrai, részben analitikus eszközök segítségével) és az additív számelméletre (ez leginkább lineáris algebrát és csoportelméletet igényel).
- A huszadik század egyik legnagyobb közfigyelmet kiváltó matematikai felfedezése számelméleti jellegű volt: megoldódott a **Fermat-sejtés** kérdése. További fontos változás, hogy a hatvanas években még szinte lenézett, alkalmazhatatlan elmetornának gondolt diszkrét matematika és különösen a számelmélet az alkalmazott matematika egyik nagyon fontos területévé vált.

MATEMATIKATÖRTÉNETI VONATKOZÁSOK

- Az egyiptomi **Rhind-**papiruszon (Kr.e. 2000–1700) a „törzstörtek” felsorolásában csak a páratlan nevezőjű törtek szerepeltek, tehát az egyiptomiak különbséget tettek a páros és a páratlan számok között.
- Az öttel való oszthatóságot az ókori hinduk is ismerték.
- A hárommal való oszthatóság szabályát először a pizai **Leonardo** (1200 körül) írta le.
- A tizeneggyel való oszthatóság szabályát a XI. századi arab matematikusok ismerték, viszont szabatosan csak **Lagrange** (1736–1813) francia matematikus fogalmazta meg: a pároshelyiértéken álló számjegyeinek összege megegyezik a páratlan helyiértéken álló számjegyek összegével, vagy a kettő különbsége 11-nek a többszöröse.
- **Pascal** (1623–1662) francia matematikus teljes általánosságban vizsgálta az oszthatóságot a természetes számok körében.

MATEMATIKATÖRTÉNETI VONATKOZÁSOK

- Prímszámok meghatározás az eratoszthenészi (K.r.e. III. század) szitával: Felírjuk 2-tõlkezdõdõen az egész számokat (õ 100-ig csinálta). A 2-t bekeretezzük, ez az első prímszám, majd kihúzzuk az összes olyan számot, ami 2 többszöröse (minden másodikat). Bekeretezzük az első át nem húzott számot, a 3-at, ez a következő prímszám. Innen kezdve áthúzzuk a 3 többszöröseit (minden harmadikat). Ezt az eljárást folytatva megkapjuk a prímszámokat(bekeretezett számok).
- A **sumérok** (Kr.e. 2000 előtt) a 10-es, 12-és és 60-as alapú számrendszer kombinációját használták az asztronómiai és egyéb számításaiknál. Ezt a rendszer átvették a **görögök**, a **rómaiak** és az **egyiptomiak**. A 60-as számrendszer maradványait felismerhetjük a mai idő- (órák, percek) és a szögmérésben (szögpercek).
- A 12-es számrendszer nagyon népszerű volt, mert a 12 maradék nélkül osztható 2-vel(felezhető), 3-mal (harmadolható), 4-gyel (negyedelhető), 6-tal (hatodolható). A ma használtnaptárban az év 12 hónapra oszlik, 12 óra a nappal és 12 óra az éjszaka az év mind a 365 nap-ján. Csaknem minden nyelvben külön szó van a 12 dologból álló csoportra, például a magyar„tucat”, az angol „dozen”, a német „das Dutzend”, az orosz „djuzsina” stb.
- Nyelvészeti kutatások szerint az ősmagyarok a hetes számrendszert ismerték, használták: mesék hétfejű sárkánya, hetedhét ország, hétmérföldes csizma, hétpecsétes titok, hétszerteszebb lett, stb.
- A 2-es alapú bináris számrendszert már a 17. században **Leibniz** ismertette, aki Kínában hallott róla, de általános használata a 20. században, a számítógépek megjelenésével terjedt el.
- **Neumann János** (1903–1957) magyar származású matematikus a róla elnevezett elvben megfogalmazta a számítógépek működési elvét. Ebben a számítógépek használjanak kettesszámrendszert, az összes művelet kettes számrendszerbeli logikai műveletre redukálható.

A SZÁMELMÉLET ALÁGAI

- **Elemi számelmélet :** Ide tartoznak a minden alágban közös fogalmak és tételek, úgymint

- oszthatóság
- prímek
- maradékos osztás, az euklideszi algoritmus
- a számelmélet alaptétele
- moduláris aritmetika (maradékosztályok és kongruenciák),
- egyszerű diofantoszi egyenletek

- **Analitikus számelmélet :**A számelméleti problémákat a függvényanalízis eszközeivel vizsgálja: a diszkrét matematika területéhez sorolt számelmélet megközelítése a folytonosság vizsgálatára létrejött szemlélettel és módszerekkel.

- a prímszámtétel, Riemann-sejtés,

Az első jelentősebb analitikus számelméleti eredmény Dirichlet nevéhez fűződik, aki függvénytani módszerekkel bizonyította azt az állítást, miszerint ha a és d relatív prímek, akkor az a, a+d, a+2d, ... , a+*n*d számtani sorozat végtelen sok eleme prímszám.

A SZÁMELMÉLET ALÁGAI

- **Algebrai számelmélet :** A számelméleti problémákat az absztrakt algebra módszereivel vizsgálja.
  - algebrai számok
  - algebrai egészek
  - Galois-elmélet
  - véges testek számelmélete
  - p-adikus számok
  - ideálok elmélete
- **Kombinatorikus számelmélet :** Ez a nagyrészt Erdős Pál által létrehozott terület a természetes számok kombinatorikusan megfogalmazható tulajdonságaival foglalkozik. Gyakorta használ lineáris algebrai eszközöket is.
- **Prímszámelmélet :** A prímszámok eloszlásával, tulajdonságaikkal foglalkozik

A SZÁMELMÉLET ALÁGAI

- **Additív számelmélet :** Goldbach-sejtés, Waring-probléma
- **Diofantoszi egyenletek :** pitagoraszi számhármasok, Pell-egyenlet, Catalan-sejtés, kétnégyzetszám-tétel, Nagy Fermat-tétel, abc-sejtés
- **Geometriai számelmélet**
- Rácsgeometria
- Minkowski-tétel
- pakolási problémák
- algebrai geometriai problémák
- Nagy Fermat-tétel
- **Számításelméleti számelmélet**
- Prímteszt
- Prímfaktorizáció
- Kriptográfia

SZÁMELMÉLET ALKALMAZÁSAI

- Oszthatóság,
- Oszthatósági szabályok és tételek.
- Prímszámok.
- Számrendszerek.
- Legnagyobb közös osztó: törtek egyszerűsítése
- Legkisebb közös többszörös: törtek közös nevezőre hozása
- Kétismeretlenes egyenlet megoldása a természetes számok halmazán (oszthatóság felhasználásával)
- Számítógépekben a 2-es számrendszer a két jegyével jól használható: folyik áram = 1, nem folyik áram = 0 (Neumann-elv). Ma már inkább a 16-os, hexadecimális számrendszert használják, ami felépíthető a kettesből.

OSZTHATÓSÁG

- Az oszthatóság fogalmánál alaphalmaznak az egész számok halmazát tekintjük. Két egész számhányadosa nem mindig egész szám, az oszthatóságnál azt vizsgáljuk, hogy egész számok osztása-kor mikor lesz a hányados is egész szám, vagyis a maradék 0.
- Oszthatósági szabályok :
- Egy n egész szám osztható
  - 2-vel, ha n páros, vagyis utolsó jegye Œ{0; 2; 4; 6; 8}.
  - 3-mal, ha a számjegyek összege osztható 3-mal.
  - 4-gyel, ha a két utolsó jegyből képzett szám osztható 4-gyel.
  - 5-tel, ha utolsó jegye Œ{0; 5}.
  - 6-tal, ha 2-vel és 3-mal osztható.
  - 8-cal, ha a három utolsó jegyből képzett szám osztható 8-cal.
  - 9-cel, ha számjegyek összege osztható 9-cel.
  - 10-zel, ha utolsó jegye 0.

HÍRES SZÁMELMÉLETI PROBLÉMÁK

- **A nagy Fermat sejtés:**

- Ez a probléma már régóta izgatta a matematikusokat.
- Az $x^2+y^2=z^2$ egyenlet Pitagorasz tételét jelenti, ahol **x, y** egy derékszögű háromszög befogóinak oldalhosszúságait, **z** pedig az átfogó hosszúságát jelenti, tehát pozitív valós számok. Az olyan pozitív egész számokat, amelyek kielégítik a Pitagorasz tételt, pitagoraszi számhármasoknak nevezzük. Ilyen számhármasból végtelen sok van.
- Ezek után a matematikusokat elkezdte izgatni, hogy **van-e megoldása az egész számok körében az $x^3+y^3=z^3$ egyenletnek, sőt általában az $x^n+y^n=z^n$ egyenletnek.**
- Fermat miután elolvasta Diophantosz *"Arithmetica"* című művében azt a részt, amely az $x^2+y^2=z^2$ egyenlet megoldásairól szól az egész számok körében (Pitagoraszi számhármasok), a következő tartalmú feljegyzést írta ennek a kiadványnak a margójára

- **Azaz nincs megoldása az $x^n+y^n=z^n$ x,y,z,n ∈ ,n>2 *diophantoszi egyenlet*nek az egész számok körében n>2 természetes szám esetén.**
- Ezzel a széljegyzetével azonban Fermat egy évszázadokon átnyúló versengést indított el a matematikusok között.
- Fermat **n=4** esetére szóló bizonyítását később megtalálták, és az itt használt módszert átvéve sikerült Euler-nek bizonyítani **n=3** esetére is. (az un. végtelen leszállás módszerével)

HÍRES SZÁMELMÉLETI PROBLÉMÁK

- A Fermat állítása szerint létező eredeti bizonyítást máig nem sikerült megtalálni. Az utókor rendre igazolni tudta Fermat minden más tételét, ám ez a kijelentés makacsul tartotta magát – így vált ez **Fermat utolsó tétel**évé, a **nagy Fermat-sejtés**sé, melyet csak 1994-ben sikerült bizonyítani.
- Andrew Wiles bizonyítása óta **nagy Fermat-tétel**en (vagy **Fermat–Wiles-tétel**en) azt a kijelentést értjük, hogy a Fermat-sejtés állítása bizonyított.
- **Wiles megoldása és tétele:**
- A Fermat-tétel az egyik leghosszabb ideig bizonyítatlanul maradó sejtés volt. A ma ismert bizonyítás Andrew Wiles, princetoni professzor érdeme, hétévnyi titokban végzett munkával sikerült belátnia az állítást 1995-ben. Noha korunkban egyre inkább az a jellemző, hogy a bizonyításokon és egyéb tudományos felfedezéseken többfős kutatócsapatok dolgoznak, Wiles majdnem végig önállóan dolgozott. A bizonyítás első, 1993-as prezentálása után egy látszólag fatális hibát fedeztek fel, ám Wilesnak egy tanítványa segítségével 1994 őszére sikerült kijavítania a bizonyítást, amelyet végül 1995-ben fogadtak el. A bizonyítás olyan összetett, hogy a számelméleti matematikusok közül is csak néhányan képesek megérteni.

A SZÁMELMÉLET ALAPTÉTELE

A számelmélet alaptétele

Bármely összetett szám, a tényezők sorrendjétől eltekintve egyértelműen bontható fel prímszámok szorzatára.

$$N = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdot \ldots \cdot p_k^{r_k}$$

$$252000 = 2^5 \cdot 3^2 \cdot 5^3 \cdot 7$$