Már az Ókorban is tudták

BSc Szakdolgozat

Készítette: Berekszászi Gergő

Matematika BSc, Matematikai elemző szakirány

Témavezető: Dr. Munkácsy Katalin
Eötvös Loránd Tudományegyetem, Természettudományi Kar
Matematikatanítási és Módszertani Központ

Belső konzulens: Dr. Wintsche Gergely
Eötvös Loránd Tudományegyetem, Természettudományi Kar
Matematikatanítási és Módszertani Központ

Eötvös Lóránd Tudományegyetem
Természettudományi kar
2022

NYILATKOZAT

Név: Berekszászi Gergő

ELTE Természettudományi Kar, szak: Matematika Bsc

NEPTUN azonosító: ENPM5I

Szakdolgozat címe:

Már az Ókorban is tudták

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022.05.06.

Berekszászi Gergő

a hallgató aláírása

KÖSZÖNETNYÍLVÁNÍTÁS

Szeretném megköszönni Munkácsy Katalin Tanárnőnek, aki javaslataival, meglátásaival sokat segített a szakdolgozat készülése közben.

Továbbá szeretném megköszönni Wintsche Gergely Tanár Úrnak, aki nélkül ez a munka nem jöhetett volna létre.

Tartalomjegyzék

1. Bevezetés

Azért választottam az ókori görög matematikát témámnak, mert mindig is érdekeltek a kezdetek, a matematika fejlődésének története. Hogyan lehetséges az, hogy a több mint 2000 évvel ezelőtt élő görögök olyan nagy mértékben járultak hozzá a matematika jelenlegi állapotához, mint talán senki más. Példaként említhetnénk, hogy a matematikaoktatás általános iskolás szintjétől kezdve találkozunk eljárásaikkal, tételeikkel.

Szakdolgozatomban azt mutatom meg, hogy az ókori matematika néhány fontos eredménye milyen kapcsolatban áll a modern matematikával. Külön fejezetet szenteltem a prímszámoknak, és azok egyik alkalmazásának.

2. Egy új kultúra létrejötte

A matematikatörténettel sokan foglalkoztak, ebben a témában írt könyvet Ropolyi László és Szegedi Péter [1]. Ennek alapján a következőket mondhatjuk az antik görög kultúráról.

2.1. a „görög csoda”

Amikor az ókori görög világot és kultúrát vizsgáljuk, elkerülhetetlenül is találkozunk a következő fogalommal: „görög csoda”. A „csoda” kifejezés arra utal, hogy a korábbi kultúrákhoz képest meglepően új jött létre, amely már a modern európai szellem alapját képezheti. Ennek megfelelően szokás, az ókori Görögországot az európai kultúra bölcsőjeként emlegetni.

2.2. ismeretük forrása

Az ókori görögök ismereteik jelentős részét korábbi kultúrák (főként Egyiptom és Mezopotámia) képviselőitől sajátították el. Ugyanakkor azt figyelhetjük meg, hogy ezeket az ismereteket más összefüggésbe ágyazva, más világszemlélettel kezelték, s a tudásnak egészen más szerepet tulajdonítottak.
Erről árulkodik a következő idézet Platóntól a [2] könyvből:

„Bármit is vettek át a hellének a barbároktól, azt mindig magasabb tökélyre fejlesztették.”

2.3. gondolkodásmódjuk

A tudás felhasználásának módjában különbséget tehetünk a korábbi kultúrák képviselői és a görögök között. Amíg az előbbiek a tudásukat elsősorban konkrét problémák, ill. szituációk megértésére és kezelésére használták, addig a görögök túlléptek ezen, s a konkrét ismeretekből valamiféle általánosított tudás létrehozására törekedtek.
Az ismereteket nem pusztán egyes konkrét feladatok megoldásában alkalmazták, hanem összehasonlítva, egymáshoz kapcsolva, egymásra vonatkoztatva valamilyen összefüggő nézetrendszer, más szóval világnézet kiépítésében is. Az antik görög világnézet képviselői által kialakított ismeretszerző és ismeretrendszerező eljárásokon és módszereken alapultak a később kifejlődő tudományok eljárásai és módszerei.

Az új tipusú tudományos világnézet kibontakozása, s ezzel a korábban uralkodó mitologikus világkép meghaladása mindenekelőtt abban állt, hogy a különféle ismereteket kritikusan kezelték s valamiféle összefüggő egésszé, ésszerű rendszerré próbálták kiépíteni.

Ebben a vonatkozásban legfontosabb fejleményként már a kezdeteknél felmerül az ismeretek bizonyításának igénye. Bizonyítások segítségével, pusztán gondolati úton szükségszerűen érvényes ismeretekhez juthatunk. Ez annyit jelent, mint a tradicionális tudáshoz kritikusan viszonyulni, s igazságukat önállóan, független értelmünkre támaszkodva belátni.
A görög gondolkodást áthatja ez a kritikus megközelítési mód, s vele szorosan összefonódva a bizonyított igazságok keresése: az a hozzáállás, mely szerint nem elég pusztán „rálelni” a tudásra, vagy átvenni azt a megbízható ősöktől, hanem annak igazságát értelmünk segítségével be is kell látnunk.

„ Ami a görög matematikára jellemző, s ami benne teljesen új, az éppen a lépésről lépésre, tételről tételre való előrehaladás bizonyítások útján. Úgy hiszem, hogy a görög matematikának ez volt a jellege a kezdettől fogva, és hogy Thálész volt, aki ezt a jelleget adta neki."

Az előző idézet szintén a [2] könyvből származik és jól összefoglalja az antik görögök hozzáállását a matematikához. Könnyen kiolvasható belőle, hogy Thálész volt az első, aki kimondott és be is bizonyított tételeket és így a matematika legfontosabb fordulatában döntő szerepet játszott.

Amellet, hogy az antik görögök más irányból közelítették meg az egyes próblémák megoldását és azok eredményeinek felhasználását, milyen más tényező hatása vezetett oda, hogy ilyen sok új tudást halmoztak fel?
Mindenképpen szerepet játszott eme folyamat lezajlásában az, hogy ki férhetett hozzá a tudáshoz. A korábbi társadalmakban csak egy szűk rétegnek volt lehetősége az akkori tudás összességéhez hozzáférni, tanulni és bőviteni azt. Ellenben a helléneket egy úgynevezett „nyílt tudás" jellemezte, mely lényegében azt jelenti, hogy bárki hozzáférhet a tárolt tudáshoz.
([1]: 33-37.o., [2]: 137,150.o.)

3. Az ókori görög matematika legfontosabb műve: Elemek

A görög matematika nagy mértékben való fejlődése, kezdve Thalésszal, azt eredményezte, hogy szükségszerűvé vált egy, az addigi tudást tartalmazó, összefoglaló alkotás elkészítése. Eukleidész fő műve, az Elemek(eredeti nyelven Sztoikheia), olyan 13 könyvből álló precíz munka, amely mindmáig a matematika egyik alapköve.

Azonban azt is meg kell jegyezni, hogy az Elemek nem tartalmaz minden akkori görög matematikai eredményt vagy tudást. Csak geometriai, aritmetikai és arányokkal kapcsolatos témajú ismeretek lelhetők fel benne, a geometriai részek kapnak nagyobb hangsúlyt. Eukleidészhez hasonlóan mások is készítettek összefoglaló művet még e mű megszületése előtt, melyeken mind érzékelhető, hogy forrásmunkák alapján íródtak. Ám az Eukleidész féle Elemekkel ellentétben a többi ilyen célű alkotás, vagy nem maradt fenn, vagy feledésbe merült az Eukleidészi mű megjelenése után.
([3]: 148.o.)

Eukleidész elsősorban nem mint alkotó matematikus volt kiemelkedő, de ez nem azt jelenti, hogy az Elemekben ne jelenne meg önálló gondolata. Példaként említhetnénk a róla elnevezett Eukleidészi algoritmust, ami talán a legismertebb a saját felfedezései közül. A [8] könyv alapján részletesebben is ismertetem.

Eukleidészi algoritmus

A számelméleti általánosítás egyik formai megjelenése, hogy nem pontok, hanem a folytonos alakzatok, a szakaszok ábrázolják az egész számokat, így Eukleidész algoritmusát tetszőleges szakaszokra írta le – azaz Eukleidész tetszőleges pozitív egész számokra definiálta és határozta meg algoritmikusan a legnagyobb közös osztót.

3.1. Algoritmus. $lnko(a,b)$

Adott a, $b \in Z$ számokra ismételten alkalmazzuk a maradékos osztás tételét: ha $|a| \geq |b|$ akkor osszuk el az a számot b-vel, majd b-t a maradékkal, stb. mindig az osztót a maradékkal.
Azaz legyen

$$\begin{aligned}
a &= b \cdot q_1 + r_1, \quad 0 < r_1 < |b|,\\
b &= r_1 \cdot q_2 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, \quad 0 < r_3 < r_2,\\
r_2 &= r_3 \cdot q_4 + r_4, \quad 0 < r_4 < r_3,\\
&\vdots\\
r_{i-2} &= r_{i-1} \cdot q_i + r_i, \quad 0 < r_i < r_{i-1},\\
&\vdots\\
r_{m-2} &= r_{m-1} \cdot q_m + r_m, \quad 0 < r_m < r_{m-1},\\
r_{m-1} &= r_m \cdot q_{m+1}.
\end{aligned}$$

Az algoritmus akkor áll meg, ha 0 maradékot kapunk, azaz $r_{m+1} = 0$. Ekkor

$$lnko(a,b) = r_m$$

vagyis a „legutolsó nemnulla maradék”.

Kérdés: Megáll-e egyáltalán az algoritmus minden input esetében?

Az eljárás természetesen véges sok lépésben véget ér mert

$$|b| > r_1 > r-2 > \ldots > r_i > r_{i+1} > \ldots > 0$$

és pozitív egész számok csökkenő sorozata nem lehet végtelen. Ezt az „elvet" hívják *descente infinie* (végtelen leszállás) *elv*nek.

Alkalmazásai:relatív prímek ellenőrzésénél és keresésénél, törtműveleteknél (törtek egyszerűsítésekor), lineáris Diophantikus egyenleteknél, lineáris kongruenciáknál és kongruenciarendszereknél (Kínai Maradéktétel), számok (*mod m*) multiplikatív inverzének kiszámításakor...
([8]: 33-35.o)

3.2. Példa. $lnko(3\,462\,246, 7\,457\,224)$ meghatározása:

$$\begin{aligned}
7\,457\,224 &= 3\,462\,246 \cdot 2 + 532\,732 \\
3\,462\,246 &= 532\,732 \cdot 6 + 265\,854 \\
532\,732 &= 265\,854 \cdot 2 + 1\,024 \\
265\,854 &= 1\,024 \cdot 259 + 638 \\
1\,024 &= 638 \cdot 1 + 386 \\
638 &= 386 \cdot 1 + 252 \\
386 &= 252 \cdot 1 + 134 \\
252 &= 134 \cdot 1 + 118 \\
134 &= 118 \cdot 1 + 16 \\
118 &= 16 \cdot 7 + 6 \\
16 &= 6 \cdot 2 + 4 \\
6 &= 4 \cdot 1 + 2 \\
4 &= 2 \cdot 2 + 0
\end{aligned}$$

tehát

$$lnko(3\,462\,246, 7\,457\,224) = 2.$$

3.3. Tétel. *A $\sqrt{2}$ nem racionális.*

Ahogy azt látni fogjuk, az elméleti beállítottságú görög matematikusokat, akiknek a pontosság mindennél előrevalóbb, fő szempont volt, nem hagyta nyugodni, hogy például a négyzet oldalhosszából az átló hosszát nem tudták sem számmal (egész számmal), sem aránnyal kifejezni, amikor ugyanennek a feladatnak a geometriai megoldására a szerkesztés elvileg teljesen pontos eredményt szolgáltatott. Tehát a két szakasz összemérhetetlen, ezt onnan tudjuk, hogy az az állítás, hogy mindkét szakasz hossza szám (egész, racionális) ellentmondásra vezet. Vagyis a kor matematikájának az egyik legnagyobb felfedezése, hogy az egységnyi oldalhosszúságú négyzet átlójának hossza, ami $\sqrt{2}$ valószínűleg az első ismert nem racionális szám.
([3]: 153.o)

Bizonyítás. Indirekt

1. Tegyük fel, hogy a $\sqrt{2}$ egy racionális szám, tehát léteznek a és b egészek, hogy $\frac{a}{b} = \sqrt{2}$.

2. Akkor lehet felírni $\sqrt{2}$-t tovább nem egyszerűsíthető törtként, ha a és b relatív prímek, valamint $\left(\frac{a}{b}\right)^2 = 2$.
3. Ebből következik, hogy $\frac{a^2}{b^2} = 2$ és $a^2 = 2 \cdot b^2$.
4. Tehát a^2 páros, mert egyenlő $2 \cdot b^2$-tel.
5. Ebből következik, hogy a is páros, mert csak a páros számoknak páros a négyzetük.
6. Mivel a páros, létezik k egész szám, ami teljesíti, hogy $a = 2 \cdot k$.
7. Behelyettesítve $2 \cdot k$-t a (6). lépésből a (3). lépés második egyenlőségébe: $2 \cdot b^2 = (2 \cdot k)^2$, ami megegyezik $2 \cdot b^2 = 4 \cdot k^2$, ami megegyezik $b^2 = 2 \cdot k^2$.
8. Mivel $2 \cdot k^2$ osztható 2-vel, és $2 \cdot k^2 = b^2$, ezért b^2 szintén osztható 2-vel, tehát b is.
9. Az (5). és (8). lépésből tudjuk, hogy a és b is párosak, ami ellentmond annak, hogy relatív prímek, ahogy azt megállapítottuk a (2). lépésben.

Mivel van ellentmondás, az (1)-es feltétel, hogy a $\sqrt{2}$ racionális szám, hamis. Az állítás be van bizonyítva: $\sqrt{2}$ irracionális. □

([5])

Az irracionális számok felfedezése után, minden algebrai jellegű feladatot átfogalmaztak geometriaivá, hiszen míg szakaszokkal tudták ezeket ábrázol, addig „számokkal" nem tudták kifejezni őket. így a számok közötti műveleteket, a négyzetgyökvonásig bezárólag, a számoknak megfeleltetett szakaszok segítségével mindig el tudták végezni: a számok összeadását, illetve kivonását a szakaszok összeadásával, illetve kivonásával helyettesítették; a szorzást és az osztást a párhuzamos szelők tételével hajtották végre, a négyzetgyökvonást pedig mértaniközép-szerkesztéssel.
([3]: 153.o.)

Eddig az antik görögök **Számelmélet** témakörébe tartozó felfedezéseik közül ismertünk meg párat, a következőkben a **Geometria**i ismereteik bemutatása következik.

Ami az Elemeket igazán kiemelkedővé teszi az a korát meghaladóan kifinomult állításokra, axiómákra és definíciókra alapozott bizonyítás, vagyis az úgynevezett deduktív módszer, a geometria axiomatikus feldolgozása.

Ha már bizonyítunk, akkor szükség van olyan állításokra, melyekre a bizonyítás során hivatkozhatunk, ezért műve az alapozással, azaz a bizonyítás nélkül elfogadott állítások felsorolásával kezdődik. Eukleidész fontosnak tartotta, hogy a geometriában is szükségképpen előforduló legegyszerűbb alapfogalmakat szemléltesse, amelyek nem definiálhatók. Ilyen a pont, az egyenes és a sík. Amikor Eukleidész megkísérli ezek meghatározását, akkor egyszerűbb fogalmakat bonyolultabbakkal definiál.
([3]: 149)

A következő definíciók, axiómák, posztulátumok az Elemekből valók:
A huszonhárom definíció (melyek feladata tehát, hogy rögzítsék a fogalmak jelentését, azokat szemléltessék):

1. „ Pont az, aminek nincs része.

2. A vonal szélesség nélküli hosszúság.

3. A vonal végei pontok.

4. Egyenes vonal* az, amelyik a rajta levő pontokhoz viszonyítva egyenlően fekszik.

5. Felület az, aminek csak hosszúsága és szélessége van.

6. A felület végei (=szélei) vonalak.

7. Síkfelület az, amelyik a rajta levő egyenesekhez viszonyítva egyenlően fekszik.

8. A síkszög két olyan egysíkbeli vonal egymáshoz való hajlása, amelyek metszik egymást, és nem fekszenek egy egyenesen.

9. Ha a szöget közrefogó vonalak egyenesek, egyenes vonalúnak nevezzük a szöget.

10. Ha valamely egyenesre egyenest állítunk úgy, hogy egyenlő mellékszögek keletkeznek, akkor a két egyenlő szög derékszög, és az álló egyenest merőlegesnek mondjuk arra, amelyen áll.

11. Tompaszög az, amelyik nagyobb a derékszögnél.

12. Hegyesszög pedig, amelyik kisebb a derékszögnél.

13. Határ az, ami vége valaminek.

14. Alakzat az, amit egy vagy több határ vesz körül.

15. A kör síkbeli alakzat, amelyet egy vonal vesz körül [ezt nevezzük körvonalnak] úgy, hogy az e vonal és egy, az alakzat belsejében fekvő pont közé eső szakaszok egyenlők egymással.

16. Ezt a pontot a kör középpontjának nevezzük.

17. A körnek átmérője bármely, a középponton át haladó egyenes vonal, amely mindkétoldalt a kör kerületén végződik. Az ilyen egyenes félbevágja a kört.

18. A félkör olyan alakzat, amelyet egy átmérő és az általa kimetszett körív vesz körül. (A félkör középpontja ugyanaz a pont, mint amelyik a köré is.)

19. Egyenes vonalú alakzatok (azaz sokszögek)* azok, amelyeket egyenes vonalak vesznek körül, háromoldalúak, amelyeket három, négyoldalúak, amelyeket négy, sokoldalúak pedig, amelyeket négynél több egyenes vesz körül.

20. A háromoldalú alakzatok közül egyenlő oldalú háromszög az, amelynek három egyenlő oldala van, egyenlő szárú, amelynek csak két egyenlő oldala van, ferde pedig, amelynek három nem egyenlő oldala van.

21. Továbbá a háromoldalú alakzatok közül derékszögű háromszög az, amelynek van derékszöge, tompaszögű, amelynek van tompaszöge, hegyesszögű pedig, amelynek három hegyesszöge van.

22. A négyoldalú alakzatok közül négyzet az, amelyik egyenlő oldalú és derékszögű, téglalap, amelyik derékszögű, de nem egyenlő oldalú, rombusz, amelyik egyenlő oldalú, de nem derékszögű, romboid, amelynek a szemközti oldalai és szögei egyenlők egymással, de sem nem egyenlő oldalú, sem nem derékszögű. A többi négyoldalú neve legyen trapéz.

23. Párhuzamosak azok az egyenesek, amelyek ugyanabban a síkban vannak és mindkétoldalt végtelenül meghosszabbítva egyiken sem találkoznak. ”

A kilenc axióma (ezek olyan igazságok, amelyeket a logikus gondolkozás érdekében kényszerülünk elfogadni, tehát kényszerítő erejűek):

1. „ Amik ugyanazzal egyenlők, egymással is egyenlők.
2. Ha egyenlőkhöz egyenlőket adunk hozzá, az összegek egyenlők.
3. Ha egyenlőkből egyenlőket veszünk el, a maradékok egyenlők.
4. Ha nem egyenlőkhöz egyenlőket adunk hozzá, az összegek nem egyenlők.
5. Ugyanannak a kétszeresei egyenlők egymással.
6. Ugyanannak a fele részei egyenlők egymással.
7. Az egymásra illeszkedők egyenlők egymással.
8. Az egész nagyobb a résznél.
9. Két egyenes vonal nem fog közre területet."

Az öt posztulátum (ezek olyan állítások, amelyek nem a gondolkozásunk alappillérei, de az adott elmélet keretében el kell fogadnunk. Nem mint általános igazságot, hanem mint az adott elmélet sajátosságait.):

1. „ Követeltessék meg, hogy minden pontból minden ponthoz legyen egyenes húzható.
2. És hogy véges egyenes vonal egyenesben folytatólag meghoszszabbítható legyen.
3. És hogy minden középponttal és távolsággal legyen kör rajzolható.
4. És hogy minden derékszög egymással egyenlő legyen.
5. És hogy ha két egyenest úgy metsz egy egyenes, hogy az egyik oldalon keletkező belső szögek (összegben) két derékszögnél kisebbek, akkor a két egyenes végtelenül meghosszabbítva találkozzék azon az oldalon, amerre az (összegben) két derékszögnél kisebb szögek vannak."

([4]: első könyv)

Ezzel egy olyan nagyszerű axiómarendszert hozott létre, melynél egészen a XIX. század végéig nem sikerült tökéletesebbet készíteni. Az Elemek jelentősége, hogy követésre méltóvá tette mind a mai napig a matematikát, sőt más tudományok számára is az axiomatikus feldolgozást. ([3]: 150.o.)

Az Eukleidész által ránk hagyott axiomatikus rendszerhez két kiegészítés tartozik. Az egyik, hogy miként lehet felfedezni ezeket a tételeket, melyek ebben a szigorú rendben bizonyítottak. A másik pedig az elmélet alkalmazása.

3.1. Antik heurisztika

„Az antik matematikai tárgyú értekezésekben általában szigorú rendben sorakoznak egymás után a tételek és bizonyításaik, de vajon hogyan fedezték fel ezeket a tételeket? Hogyan készült a matematika, és hogyan nyerte el azt az egzaktságot, melyet a kész műben tapasztalunk?
Ezek a kérdések már az ókorban felmerültek, amikor a matematika tanulmányozása a mester és tanítvány közötti párbeszéd helyett a klasszikus szövegek olvasását, újragondolását, továbbvitelét jelentette.

Papposz a régi nagy matematikusokat (Euklidész, Apollóniosz, Ptolemaiosz, . . .) olvasva gyakran fűzött szövegeikhez kommentárokat. Mint az igazán figyelmes olvasó, részletezte a bizonyítást, ahol nem minden részlet volt leírva, kiegészítette az esetszétválasztást, ha hiányos volt, vagy éppen megfogalmazta az implicit lemmákat.
Papposz az általa összeállított gyűjteményes munka (Collectio) VII. könyvében a a heurisztikát (azaz a felfedezés művészetét) olyan tudományágként definiálja, mely a matematika elemeinek ismerőit hozzásegítheti feladatok megoldásához.

A heurisztikának két módszerét különbözteti meg: az analízist és a szintézist.

- Az analízis során abból indulunk ki, amit bizonyítani akarunk. Következményeinek vizsgálata során szerencsés esetben eljutunk egy olyan ponthoz, amit már valóban biztosan tudunk, és ami az elkövetkező szintézis kiindulópontja lehet. (Tekinthetjük e leírás alapján az analízist ellenőrzésnek is, melyben, ha szükséges és elégséges következtetések mentén haladunk, akkor elindulhatunk visszafelé.) Fordított irányú munkának is nevezi, mert a kérdés, amit a vizsgálódás folyamán újra meg újra felteszünk:
  Mi kellene ahhoz, hogy ez a tétel igaz legyen?
  Ebben a megfogalmazásban nem a következmények, hanem inkább a feltételek vizsgálata jellemzi az analízist. Összefoglalóan tehát azt mondhatnánk, a tétel logikai-matematikai környezetének bejárásáról van szó, amíg egy már ismert részhez nem jutunk.

  Kétféle analízist is megkülönböztet. Az egyik a bizonyítási feladatokhoz tartozik: célja az előre megfogalmazott tétel igazságának alátámasztása vagy cáfolata. A meghatározó feladatokban pedig egy ismeretlent keresünk, mely világosan rögzített feltételeknek felel meg, s ekkor az analízis célja ezen ismeretlen megtalálása.
- A szintézis ezzel szemben az ismertből indul ki, és innen építi fel a bizonyítás révén a tételt. Ezt Papposz konstruktív megoldásnak vagy egyenes irányú munkának is nevezi.

([1]: 55-56.o.)

3.2. Alkalmazott matematika a hellenisztikus korban

A mindennapok során is találkozhatunk olyan problémákkal, melyeket a matematika segítségével lehet megoldani. Az Ókori Görögországban Arkhimédész foglalkozott a legtöbbet ezen problémák megoldásán. Noha maga Arkhimédész igen kevés írásos munkát hagyott hátra ez irányú munkásságáról – lévén maga is a tiszta matematika elkötelezett híve –, saját korában híressé és elismertté mégis e tevékenysége tette.
Nos valóban elméleti tudására alapozva szerkesztette meg híres hajítógépeit, melyek hatalmas köveket dobtak az ellenség hajóira, daruit, melyek felborították, víz alá nyomták, vagy épp kövekkel, ólomdarabokkal terhelve elsüllyesztették azokat. Erre utalnak Az úszó testekről, ill. a Síkidomok egyensúlyáról szóló elméleti értekezései.

Nem Arkhimédész az egyetlen azonban, aki a geometriai összefüggéseket más területeken alkalmazta. Pszeudo-Arisztotelész és Héron Mechanikái, Eukleidész és Ptolemaiosz Optikái, Heron Katoprtikája (A tükrözésről), Dioklész munkája a (paraboloid alakú) Gyújtótükrökről is ily módon vitte át egy nem matematikai területre a geometria eredményeit.
A térképészetben a gömbi geometria, illetve a sztereografikus projekció és a perspektíva geometriai tanulmányozása segített, ahogy az kiderül Ptolemaiosz Geográfiájában leírt képekből és eljárásokból.

Végül talán a legismertebb alkalmazott matematikai terület a hellenisztikus korban a csillagászat lett, melynek betetőzése Ptolemaiosz Almagesztje."
([1]: 56.o.)

3.3. Prímszámok az Elemekben

A továbbiakban az Elemek prímszámokkal kapcsolatos egyes megfigyeléseit ismertetem, mivel a szakdolgozatom későbbi részeiben részletesebben is foglalkozok a prímszámokkal.

Mindenekelőtt az Elemekben szereplő definíció:

3.4. Defníció. „Prímszám, amelyik csak az egységgel osztható." ([4]: hetedik könyv)

3.5. Tétel. *„Prímszámból prímszámok bármely adott sokaságánál több van." (vagyis végtelen sok prímszám létezik)*

A tétel bizonyítása Eukleidésztől származik:

Bizonyítás. „Legyenek az adott prímszámok a, b és c. Azt állítom, hogy több prímszám van, mint a, b és c. Vegyük ugyanis a, b és c legkisebb közös többszörösét, legyen ez DE, és adjuk hozzá DE-hez a DF egységet. Ekkor EF vagy prím, vagy nem.

- Legyen először prím. Találtunk tehát az a, b, c számoknál több prímet, a-t, b-t, c-t és EF-et.
- Ne legyen most EF prím. Ekkor osztja valamely prímszám. Ossza a g prím. Azt állítom, hogy g az a, b és c egyikével sem azonos. Tegyük föl ugyanis, hogy az a, b és c osztják DE-t, tehát g is osztja DE-t. Viszont EF-et is osztja, tehát a maradék DF egységet is osztja g, noha szám, ami ellentmondás, g tehát nem azonos az a, b, c számok egyikével sem. S feltétel szerint prím, tehát találtunk az adott a, b, c prímeknél több prímet, a-t, b-t, c-t és g-t.

Éppen ezt kellett megmutatni." □

([4]: kilencedik könyv)

Mai szemlélettel ez a bizonyítás igen nehezen érthető, könnyen felfedezhető benne az antik görög stílus, hiszen a már említett módszert alkalmazza. A geometriát segítségül hívva, a számokat szakaszoknak felelteti meg és azokkal végzi el a szükséges lépéseket.
Éppen ezért a tétel bizonyítását egy modern átírásban is bemutatom.

Bizonyítás. Indirekt.

Tételezzük fel az ellenkezőjét, azaz tételezzük fel, hogy van legnagyobb prímszám, azaz a prímszámok száma véges. Tegyük fel, hogy k darab prímszám van: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ és a feltételezett utolsó prímszám a k-ik p_k.
Szorozzuk össze a feltételezett összes prímszámot: $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$, majd adjunk hozzá 1-t! Az így kapott $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$ szám vagy prím, vagy összetett.

- Ha az így képzett N szám prím, akkor különbözik mindegyiktől, amit összeszoroztunk, tehát nem igaz, hogy az összes prímszám szerepel az N szám képzésében.

- Ha pedig N összetett szám, akkor a számelmélet alaptételéből következik, hogy van prímosztója. De az oszthatóság szabályai szerint ez nem lehet egyik sem a p_k-ig terjedő prímszámok között.

Van tehát az általunk gondolt összes (k db) prímszámon kívül más prímszám is. Ez ellentmond annak a feltételezésnek, hogy k db prímszám van, ebből következik hogy végtelen sok prímszám van. □

([6])

A bizonyításban felhasznált tételek:

3.6. Tétel. *A számelmélet alaptétele*

Bármely összetett szám, a tényezők sorrendjétől eltekintve, egyértelműen felírható prímszámok szorzataként.

([7])

Ezt a tételt most nem bizonyítom, mert nem kapcsolódik lényegesen a szakdolgozatom témájához.

3.7. Tétel. *„Bármely összetett számot oszt valamely prímszám."*

Bizonyítás. „Legyen a egy összetett szám. Azt állítom, hogy a-t osztja valamely prímszám.

Minthogy a összetett szám, osztja valamely szám. Ossza egy b szám. Ha b prím, készen vagyunk a tétellel. Ha összetett, osztja valamely szám. Ossza egy c szám. Minthogy c osztja b-t, b pedig a-t, c is osztja a-t. Ha c prím, kész vagyunk a tétellel. Ha összetett, osztja valamely szám. Folytatva ezt a vizsgálatot találni fogunk egy prímszámot, mely osztja [a megelőző számot, így a-t is osztja].
Ha ugyanis nem találnánk, akkor végtelen sok szám osztaná az a számot, melyek közül a következő mindig kisebb az előzőnél, ami a számok körében lehetetlen. Találni fogunk tehát egy prímszámot, mely osztja a megelőző számot, így a-t is osztja. Tehát bármely összetett számot oszt valamely prímszám. Éppen ezt kellett megmutatni." □

([4]: hetedik könyv)

4. Néhány érdekes probléma

A kritikus és elvont görög matematikai gondolkodásra különösen jellemző, hogy már az i.e. 5. század végén olyan feladatokkal is foglalkoztak, amelyeknek nem volt gyakorlati jelentőségük, elméletileg azonban csak a 19. századi késői utódok tudták azokat megoldani. Az ókori görög geometria az utókorra hagyott részben megoldatlanul négy szerkesztési feladatot, de már a görögök is sejtették, hogy nem lehetséges pusztán eukleidészi szerkesztéssel végrehajtani, de bizonyítani még nem tudták. Néhány esetben találtak olyan nemeukleidészi megoldást, melyhez a körzőn és a vonalzón kívül más görbé(ke)t és/vagy eszköz(öke)t használtak. Tehát nem arról van szó, hogy nem tudták megszerkeszteni, hanem nem tudták bebizonyítani, hogy nem szerkeszthető meg eukleidészi módon. Az utódok csak sokára tudtak felelni a kihívásra, s kimutatták, hogy a keresett megoldások nem is léteznek. A négy megoldatlan – megoldhatatlan ókori szerkesztési feladat a szabályos sokszög szerkesztése, a szögharmadolás, a kockakettőzés (az ún. déloszi probléma) és a kör négyszögesítése.
([15]: 9.o., [9])

4.1. Eukleidészi szerkesztés

4.1. Defníció. A síkgeometria szerkesztési feladatainak olyan kivitelezését nevezzük eukleidészi szerkesztésnek, amelynek során csak egyélű vonalzót és körzőt használunk, és ezeket is csak meghatározott módon.

„Egy szerkesztési feladatot akkor mondunk eukleidészi szerkesztéssel megoldhatónak, ha a következő hat alapművelet véges számú ismétlésével elvégezhető:

1. A vonalzót két adott ponton átmenő egyenes megrajzolására használhatjuk.
2. A körzővel adott pont körül adott hosszú sugárral kört rajzolhatunk.
3. Két egyenes metszéspontját megjelölhetjük.
4. Egyenes és kör metszéspontját megjelölhetjük.
5. Két kör metszéspontját megjelölhetjük.
6. Két pont távolságát körzőnyílásba vehetjük.

Az 1. és 2. művelet Eukleidész posztulátumainak felel meg. Az első szerint „. . . minden pontból minden ponthoz legyen egyenes húzható”, a második pedig megköveteli, hogy „. . . minden középponttal és távolsággal legyen kör rajzolható”. Ezért nevezzük e szerkesztési módott eukleidészinek.
A következő három alapművelet megfogalmazásában a „megjelölhetjük” azt fejezi ki, hogy ha az említett két vonalat az $1-2$. művelettel megrajzoltuk (vagy adott volt valamelyik), akkor a vonalak metszését a szerkesztés következő lépéseiben mint adott pontot tekinthetjük. Hangsúlyozni kell, hogy csak metszéspontról van szó. Az egyenes és kör, vagy két kör érintési pontja nem jelölhető meg, az érintési pontot szabályosan szerkeszteni kell Thálész tétellel.
Végül a 6. szerint önkényesen felvehetünk pontokat az adott és megszerkesztett pontokon kívül, ha ezek helyzete közömbös a feladat megoldása szempontjából.”
([10])

4.2. szabályos sokszögek szerkesztése

„Az antik görögöknél ez a feladat úgy szerepelt, mint adott körbe írható tetszőleges oldalszámú szabályos sokszög szerkesztése. Néhány szabályos sokszöget könnyedén megszerkeszthetünk körző és vonalzó felhasználásával; másokat nem. Eukleidésznél több szabályos sokszög szerkesztése szerepel (3, 4, 5, 6, 10, 15), de a görögök nem tudták a szabályos 7-szöget megszerkeszteni.
Mivel ismerjük hogyan kell szöget felezni, ezért Eukleidész bátran állíthatta, hogy ezen szabályos sokszögek kettő hatványaival való szorzatait is könnyen meg tudjuk szerkeszteni az oldalfelező merőlegesek segítségével. Tehát szerkeszthető szabályos n-szög, ahol $n = 2^k$, $2^k \cdot 3$, $2^k \cdot 5$ és $2^k \cdot 3 \cdot 5$."
Ez vezetett a következő kérdéshez: Lehetséges-e minden szabályos n-szög megszerkesztése körző és vonalzó használatával? Ha nem, akkor mely n-szögek szerkeszthetők és melyek nem? A választ már a görögök nem találták meg és hosszú idő elteltével Gaussnak sikerült rájönnie egy elméletre, mely lehetővé teszi egy elégséges feltétel megfogalmazását:
([12], [9])

4.2. Állítás. *Minden m-szög, ahol m Fermat-prím, körzővel és vonalzóval megszerkeszthető.*

Egyben az állítás megfordítása is igaz. ([16])

A Fermat-prímek definíciója:

4.3. Defníció. Legyen $n \in N$ tetszőleges természetes szám. Az

$$F_n := 2^{2^n} + 1$$

alakú számokat Fermat-számoknak nevezzük, és Fermat-prímnek ha F_n prímszám.

([8])

4.3. Szögharmadolás

Trisectio, azaz tetszőleges szög harmadrészének megszerkesztése. Először Arkhimédész adott rá megoldást neuszisz szerkesztéssel, (mivel már ő is tudta, hogy nem lehet Eukleidészi szerkesztéssel végrehajtani,) ami a következő:

4.4. Defníció. A neuszisz szerkesztés feladata: egy adott hosszúságú szakaszt két vonal közé beilleszteni úgy, hogy a szakasz egyenese egy adott ponton menjen át.

Az, hogy tényleg nem lehet Eukleidészi módon megszerkeszteni látszik abból is, hogy azok a szerkesztési feladatok, amelyek analitikusan harmadfokú egyenlethez vezetnek, nem oldhatók meg eukleidészi szerkesztéssel. Márpedig a szögharmadolás ilyen, ugyanis a $2\cos\frac{\alpha}{3}$ ismeretlenre felírt egyenlet: $x^3 - 3x - 2\cos\alpha = 0$ valós gyökét kellene megszerkeszteni.
([9], [13], [14])

Vagyis ahhoz hogy meg tudjuk szerkeszteni egy szög harmadát, az eukleidészi szerkesztésen felül még szükségünk van egy vonalzóra kijelölt szakaszra. Most Nikomédész módszerét és

bizonyítását mutatom be a [2] könyből, amely két egyenes közötti neusziszt használ, míg Arkhimédész kör és egyenes közötti neusziszt vett igénybe.

Szerkesztés menete:
Legyen ABT az adott szög, AT merőleges BT-re. Legyen továbbá $AE \parallel BT$. Fektessük most az AT és AE egyenes közé olyan EC szakaszt, amely kétszer hosszabb AB-nál, s melynek meghosszabbítása áthalad B-n. Akkor a CBT szög éppen az adott ABT szög harmadrésze.

Bizonyítás. Kössük össze A-t a CE szakasz H felezőpontjával. Akkor (mivel az ACE derékszögű háromszög félkörbe írható) a HC, HA és HE szakaszok mindegyike CE fele, vagyis mindhárom egyenlő AB-vel. Mármost az ABH egyenlőszárú háromszögben

$$ABC\sphericalangle = AHC\sphericalangle,$$

s mivel az AHC szög az úgyszintén egyenlőszárú AHE háromstög külső szöge, érvényes

$$AHC\sphericalangle = 2E\sphericalangle.$$

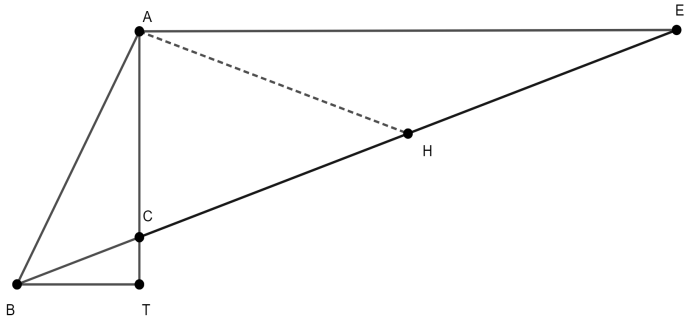
Mivel továbbá $AE \parallel BT$, azért

$$TBC\sphericalangle = E\sphericalangle,$$

tehát végeredményben

$$ABT\sphericalangle = TBA\sphericalangle + ABC\sphericalangle = E\sphericalangle + 2E\sphericalangle = 3E\sphericalangle.$$

□



4.4. Kockakettőzés

Olyan kocka élét kell megszerkeszteni, amelyik egy adott kocka térfogatának kétszerese.

Legkorábban a khioszi Hippokratész foglalkozik vele, de gyökerei régebbre nyúlnak vissza. „Ő volt az, aki megtette az alapozó lépéseket, amelyekre utódai számos szerkesztést építettek. Lényegében a négyzetkettőzés feladatát általánosította.
Ha ugyanis az adott a oldalú négyzethez szerkesztenünk kell $2 \cdot a^2$ területű négyzetet, akkor az

a és a $2 \cdot a$ mértani középarányosát kell megszerkesztenünk, vagy ami ugyanaz, keresnünk kell olyan x távolságot, amely kielégíti az $a : x = x : 2 \cdot a$ aránypárt. Hippokratész úgy okoskodott, hogy a hasonló térbeli feladat esetén nem egy, hanem két mértani középarányost kell az a és a $2 \cdot a$ közé beilleszteni, és ezek kisebbiké a keresett megoldás, azaz a $2a^3$ térfogatú kocka éle. Ezt úgy kell értenünk, hogy az a-hoz és a $2 \cdot a$-hoz keresünk olyan x és y szakaszt, amelyek kielégítik az $a : x = x : y = y : 2 \cdot a$ folytonos aránypárláncolatot.
Ekkor valóban: $x^2 = a \cdot y$ és $x \cdot y = 2 \cdot a^2$. Az első egyenlőségből $y = \frac{x^2}{a}$. Ezt beírva a másodikba: $x^3 = 2 \cdot a^3$, tehát az x élű kocka térfogata csakugyan kétszerese az a élű kockáénak. Magával a szerkesztéssel azonban Hippokratész már nem boldogult."
A szögharmadoláshoz hasonlóan ez a feladat is egy harmadfokú egyenlethez vezet.
([3]: 105-106.o., [9])

4.5. Kör négyszögesítése

Adott sugarú körrel egyező területű négyzet oldalának megszerkesztése (vagy a kör kerületével megegyező szakasz szerkesztése, a körvonal kiegyenesítése).

„A kockakettőzéshez hasonlóan a kezdeti sikereket Hippokratész érte el. Ha nem is tudott egy adott körhöz azzal egyenlő területű négyzetet szerkeszteni, de elsőként alakított át körívekkel határolt síkidomokat (holdacskákat) azokkal egyenlő területű négyszögekké, négyzetekké. Bizonyításaihoz felhasználta a hasonlóságot. Tudta, hogy a hasonló síkidomok területei úgy aránylanak, mint megfelelő lineáris méreteik négyzetei. Speciálisan arra épített, hogy hasonló körszeletek területének aránya egyenlő a hozzájuk tartozó alapok négyzeteinek arányával."
Az előző feladatokhoz hasonlóan nemeukleidészi szerkesztéssel már az antik görögök is meg tudták oldani ezt a feladatot. De annak bizonyítása, hogy nem lehet eukleidészi módon megszerkeszteni az utókorra maradt.
([9], [3]: 102.o.)

5. Prímek

A korábbiakban már találkozhattunk a prímszámok görög, Elemekben szereplő definíciójával. Azonban nem árthat újból felidézni egy kissé „modernebb” megfogalmazásban.

5.1. Defníció. Egy $p \geq 2$ természetes számot prímnek nevezzük, ha abból, hogy osztója egy szorzatnak, következik, hogy osztója a szorzat valamelyik tényezőjének. Ez a természetes számok halmazán azt jelenti, hogy egy szám prím, ha pontosan két osztója van, 1 és önmaga.

5.1. Prímkeresés

A legegyszerűbb prímtesztet úgy nevezték el, hogy próbaosztás. Legyen a bemenetként megadott szám n, és azt kell eldöntenünk, hogy vajon n prímszám-e. A próbaosztás során $d = 2,3,4,\ldots\sqrt{n}$ számokra megnézzük, hogy d osztója-e n-nek. Amennyiben találunk osztót, n összetett szám. Ha semelyik ilyen d nem osztója n-nek, akkor n prímszám.
A fenti okoskodásnak alapja az, hogy minden összetett n számnak van $\sqrt{n}$-nél nem nagyobb osztója, ugyanis $n = a \cdot b$ esetén a vagy b kisebb egyenlő mint $\sqrt{n}$. Ennek a módszernek az az előnye, hogy biztosan kiderül a vizsgált számról, hogy összetett-e. Továbbá e módszer végén azt is megtudjuk, hogy mi a vizsgált szám pontos felbontása.
([18]: 83.o.)

Az ókori görögök idejében is volt olyan, aki másfajta prímkeresési módszer megtalálásán dolgozott és előállt egy új módszerrel. Nevezetesen Eratoszthenész, kinek módszerét Eratoszthenészi szitaként ismerjük. E módszer algoritmusának lépései a következők:

1. Írjuk fel egymás után az egész számokat 2-től (az első prímszámtól) addig, ameddig a prímtesztet csinálni szeretnénk.
2. Az első át nem húzott szám lesz a következő prím. Írjuk fel a prímek közé, és húzzuk le listáról az összes többszörösével együtt.
3. Ismételjük az előző lépést addig, amíg vannak át nem húzott számok a listán.

([22])

De gyakran elég nagy(akár több száz jegyű) prímszámokra van szükség, melyeknél a próbaosztás beláthatatlanul sokáig tartana, mivel nem polinomiális algoritmus, melynek futási ideje $\sqrt{n} \cdot (\log n)^2$. Ilyenkor más prímteszteket kell használnunk, melyek lényegesen gyorsabbak. Két fajta prímteszt létezik, melyekre mind igaz, hogy nem adnak felbontást.
([18]: 83.o.)

Valószínűségelméleti prímtesztek: Olyan véletlenített algoritmusok, amelyek a prímszámokat minden esetben elfogadják, az összetett számokat pedig nagy valószínűséggel elutasítják. Előnyük, hogy a determinisztikus prímteszteknél jelentősen kisebb műveletigénnyel rendelkeznek.

Determinisztikus prímtesztek: Melyek biztosan megmondják egy számról, hogy prím-e. Azonban ezek már nagyon bonyolult algoritmusok, amik már kézzel nem is számolhatók és a leírásuk is sok időt venne igénybe.
([20])

A következőben az egyik legismertebb teszt kerül bemutatásra, melyet gyors futási ideje és

egyszerűbbsége miatt használják oly gyakran.

5.1.1. Fermat prímteszt

Ami a kis-Fermat tételen alapül, csakúgy, mint a legtöbb prímteszt:

5.2. Tétel. *Ha p prím és az a egész számra (a,p) = 1, akkor*

$$a^{p-1} \equiv 1 \pmod{p}$$

A prímteszt a következőképpen működik:

Veszünk egy tetszőleges a-t, melyre n nem osztja a-t. Megnézzük teljesül-e, hogy $a^{n-1} \equiv 1 \pmod{n}$

Ha $a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n$ összetett.

Ha $a^{n-1} \equiv 1 \pmod{n}$ választunk egy másik a-t és újra elvégezzük a tesztet. Sok ilyen próba után n valószínűleg prím.

Ha azt kapjuk a teszt végén, hogy a vizsgált szám összetett akkor az a szám biztosan összetett. Fontos kérdés, hogy igaz-e ez más eredménynél is, vagyis, hogy ha eredményként a teszt alapján a vizsgált szám prím, akkor tényleg prím-e?
NEM, és ezért itt meg kell jegyeznünk egy fontos különbséget a Fermat prímteszt eredményével kapcsolatban. Ha a teszt alapján a vizsgált számra azt kapjuk, hogy prím, akkor sem állítjuk teljes bizonyossággal, hogy tényleg prímszám. Ezeket a különleges számokat vizsgálom meg a következőkben.
([18]: 83-84.o.)

5.2. Carmichael-számok

Érdemes megvizsgálni azokat az összetett számokat, amelyek átmennek a Fermat prímteszten. Ezt Carmichael tette meg. Ezeket a Fermat-álprímeket hívjuk Carmichael-számoknak. A szakdolgozatomban [18] könyv segítségével mutatom be őket. A pontos definíciójuk a következő:

5.3. Defníció. Egy n pozitív egész számot **Carmichael-szám**nak nevezünk, ha n összetett szám, és minden $(a,n) = 1$ esetén

$$a^{n-1} \equiv 1 \pmod{n}.$$

Vizsgálta az 561 számot. Figyeljük meg, hogyan viselkedik. Bebizonyítjuk, hogy az $561 = 3 \cdot 11 \cdot 17$ összetett szám egy Carmichael-szám.

Bizonyítás. Belátjuk, hogy minden $(a,561) = 1$-re $a^{560} \equiv 1 \pmod{561}$. Legyen $(a,561) = 1$. Ekkor $561 = 3 \cdot 11 \cdot 17$ miatt $(a,3) = (a,11) = (a,17)$.

Írjuk fel a kis-Fermat tételt $p = 3$-ra:

$$a^2 \equiv 1 \pmod{3}.$$

A fenti kongruenciát a 280. hatványra emelve

$$a^{560} \equiv 1 \pmod{3}.$$

Azaz $3|a^{560}-1$.

Írjuk fel a kis-Fermat tételt $p = 11$-ra:

$$a^{10} \equiv 1 \pmod{11}.$$

A fenti kongruenciát a 56. hatványra emelve

$$a^{560} \equiv 1 \pmod{11}.$$

Azaz $11|a^{560}-1$.

Írjuk fel a kis-Fermat tételt $p = 17$-ra:

$$a^{16} \equiv 1 \pmod{17}.$$

A fenti kongruenciát a 35. hatványra emelve

$$a^{560} \equiv 1 \pmod{17}.$$

Azaz $17|a^{560}-1$. Vagyis $3 \cdot 11 \cdot 17 = 561|a^{560}-1$, ezt kellett bebizonyítanunk. □

Történetesen ez a legkisebb Carmichael-szám. A következő 6 konkrétan: $1105, 1729, 2465, 2821, 6601$, 8911, ([19]), melyekről könnyen belátható, hogy Carmicheal-számok a következő tétel segítségével:

5.4. Tétel. *(A. Korselt, 1899) Egy n pozitív egész szám, akkor és csak akkor Carmichael-szám, ha n négyzetmentes, és n minden p prímosztójára teljesül, hogy* $p-1|n-1$.

Bizonyítás. Először azt látjuk be, hogy ha n négyzetmentes szám, és n minden p prímosztójára $p-1|n-1$, akkor n Carmicheal-szám. Valóban, legyen n prímtényezős felbontása

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r,$$

ahol $p_1, p_2, \ldots, p_r$ prímek különbözőek. Legyen

$$(a,n) = 1.$$

Ekkor

$$(a,p_1) = (a.p_2) = \ldots = (a,p_r) = 1$$

Mivel $(a,p_i) = 1$ a kis-Fermat tétel miatt

$$a^{p_i-1} \equiv 1 \pmod{p_i}. \tag{5.1}$$

Mivel $p_i - 1|n-1$, ezért létezik k_i pozitív egész szám, hogy

$$n-1 = k_i \cdot (p_i - 1)$$

Így az (5.1) kongruenciát a k_i-edik hatványra emelve kapjuk, hogy

$$\begin{aligned} a^{k_i\cdot(p_i-1)} &\equiv 1 \pmod{p_i} \\ a^{n-1} &\equiv 1 \pmod{p_i} \\ p_i \;&\mid\; a^{n-1}-1. \end{aligned} \tag{5.2}$$

Mivel (5.2) fennáll $i = 1,2,\ldots,r$-re, ezért

$$\begin{aligned} p_1\cdot p_2\cdot\ldots\cdot p_r &| a^{n-1}-1 \\ n &| a^{n-1}-1 \\ a^{n-1} &\equiv 1 \ (mod\ n). \end{aligned} \tag{5.3}$$

Ekkor (5.3) kongruencia minden $(a,n) = 1$ egész számra fennáll, tehát n Carmichael-szám.

Ezután rátérünk a tétel bizonyításának második részére, nevezetesen ha n Carmichael-szám, akkor egyrészt n négyzetmentes, másrészt n minden p prímosztójára $p-1 \mid n-1$. Először azt látjuk be, hogy n négyzetmentes. Indirekten bizonyítunk, azaz feltesszük, hogy létezik p prím, amelyre

$$n = p^k \cdot m$$

alakú, ahol $k \geq 2$ alakú egész szám és az m egész számra $(m,p) = 1$. Tekintsük azt az a egész számot, amelyre

$$a \equiv 1 + p \ (mod\ p^2) \quad \text{és} \quad a \equiv 1 \ (mod\ m).$$

A Kínai-maradéktétel miatt ilyen a egész szám létezik. A binomiális tétel alapján

$$\begin{aligned} a^{n-1} &\equiv (1+p)^{n-1} \pmod{p^2} \\ a^{n-1} &\equiv 1 + \binom{n-1}{1}\cdot p + \binom{n-1}{2}\cdot p^2 + \ldots + \binom{n-1}{n-1}\cdot p^{n-1} \pmod{p^2} \\ a^{n-1} &\equiv 1 + (n-1)\cdot p \pmod{p^2}. \end{aligned} \tag{5.4}$$

Másrészt n Carmichael-szám, így

$$\begin{aligned} a^{n-1} &\equiv 1 \ (mod\ n) \\ n &\mid a^{n-1}-1 \\ p^2 &\mid a^{n-1}-1 \\ a^{n-1} &\equiv 1 \ (mod\ p^2). \end{aligned}$$

Ezt (5.4)-gyel összevetve kapjuk, hogy

$$\begin{aligned} 1 &\equiv 1 + (n-1)\cdot p \ (mod\ p^2) \\ p^2 &\mid (n-1)\cdot p \\ p &\mid n-1, \end{aligned}$$

ami ellentmond $p \mid n$-nek. Ezzel beláttuk, hogy n-nek nincs prímnégyzet osztója, azaz n valóban négyzetmentes.

Ezután rátérhetünk annak bizonyítására, hogy n minden p prímosztójára teljesül, hogy $p-1 \mid n-1$.

Írjuk fel n-et $n = p \cdot m$ alakban. Mivel n négyzetmentes, feltehetjük, hogy $(m, p) = 1$. Tekintsünk egy g primitív gyököt modulo p. Ekkor $g, g^2, g^3, \ldots, g^{p-2} \not\equiv 1 \ (mod\ p)$, de $g^{p-1} \equiv 1 \ (mod\ p)$, mivel g rendje $p-1$ Azaz az $1, g, g^2 \ldots$ végtelen sorozat periodikus lesz modulo p, és a periódushossz $p-1$, vagyis

$$g^k \equiv 1 \quad (mod\ p) \leftrightarrow p-1 \quad | \quad k. \tag{5.5}$$

Tegyük fel, hogy minden $(a, n) = 1$ esetén

$$a^{n-1} \equiv 1 \ (mod\ n).$$

A kínai maradéktétel szerint létezik olyan a egész szám amelyre

$$a \equiv g \ (mod\ p) \qquad \text{és} \qquad a \equiv 1 \ (mod\ m).$$

Mivel g primitív gyök $(g, p) = 1$, és így $(a = g + t \cdot p, p) = 1$ is teljesül. Továbbá $a \equiv 1 \ (mod\ m)$ miatt $(a, m) = 1$ is teljesül. Azaz $(a.n) = (a, p \cdot m) = 1$. Tehát

$$\begin{aligned} a^{n-1} &\equiv 1 \quad (mod\ n) \\ n \quad &| \quad a^{n-1} - 1 \\ p \cdot m \quad &| \quad a^{n-1} - 1 \\ n \quad &| \quad a^{n-1} - 1 \\ a^{n-1} &\equiv 1 \quad (mod\ p) \\ g^{n-1} &\equiv 1 \quad (mod\ p). \end{aligned}$$

Ekkor (5.5)-öt használva kapjuk, hogy $p-1 \mid n-1$, ami a bizonyítandó állítás volt. □

([18]: 84-85.,88-91.o.)

Ahogy az egész számok növekszenek, a Carmichael-számok egyre ritkásabban helyezkednek el a számegyenesen. Általában, jelölje $C(x)$ az 1 és x közé eső Carmichael-számok számát. Alford, Granville és Pomerance bebizonyította, hogy $C(x) > x^{2/7}$. Ebből az is látható, hogy végtelen sok Carmichael-szám létezik. Azért fontosak ezek a számok, mert ha nem léteznének, akkor a Fermat-prímtesztet lehetne használni mindig egy szám összetettségének eldöntéséről. Így ezek a számok teszik a Fermat-prímtesztet kevésbé hatákonnyá más prímtesztekkel szemben.
([18]: 88.o., [21])

6. Prímszámok gyakorlati alkalmazása

Visszagondolva a prímkereséssel foglalkozó alfejezetre, miért is jó nekünk, hogy meg tudunk találni nagy prímszámokat?
Az egyik leggyakoribb terület, ahol a prímszámok igen hasznosnak bizonyúlnak, az a **nyilvános(asszimetrikus) kulcsú titkosítás**ok algoritmusa. „A nyilvános kulcsú kriptográfia(rejtjelezéssel, titkosírással és kódolással foglalkozó tudományág) alapja, hogy a kódoló és a dekódoló transzformáció, illetve az azokat paraméterező nyilvános és titkos kulcsok nem azonosak, sőt egyiket a másikból kiszámítani nagy komplexitású feladat, azaz praktikusan lehetetlen. Ezért a két kulcs közül az egyiket, általában a kódoló kulcsot, nyilvánosságra lehet hozni.
Ez azért hasznos, mert ezáltal leegyszerűsödni látszik a kulcscsere probléma, ugyanis a titkos kommunikáció megvalósításához nincsen szükség egy titkos (szimmetrikus) kapcsolatkulcs létrehozására a küldő és a vevő között; elegendő a rejteni kívánt üzenetet a vevő nyilvános kódoló kulcsával rejtjelezni. Megjegyezve azonban azt, hogy gondoskodni kell a nyilvános kulcsok hitelességéről. Más szavakkal, a küldőnek meg kell tudnia győződni arról, hogy a használni kívánt nyilvános kulcs valóban a vevő nyilvános kulcsa, és nem egy harmadik, feltehetően rosszszándékú félé.
A nyilvános kulcsú kriptográfia tehát oly módon egyszerűsíti a kulcscsere problémát, hogy titkos csatorna helyett hiteles csatornalétezését követeli meg a vevő és a küldő között, melyen a vevő eljuttathatja a nyilvános kulcsát a küldőnek.”
Az alábbiakban ismertetésre kerül, az egyik leggyakrabban használt nyilvános kulcsú rejtjelező módszert, az RSA algoritmus, [23] című könyv alapján.

6.1. RSA algoritmus

Az RSA algoritmus három algoritmusból, a kulcsválasztás, a kódolás és a dekódolás algoritmusából áll. A kulcsválasztást a rendszer minden felhasználója elvégzi:

1. Véletlenszerűen választunk két nagy, p és q prímszámot($p \neq q$). Jelenleg „nagynak” a legalább 500 bit bináris méretű számokat tekintik.
2. Kiszámítjuk az $N = pq$ modulust és a $\varphi(N) = (p-1)(q-1)$ szorzatot. Választunk továbbá egy e számot, amelyik mind $(p-1)$-hez, mind $(q-1)$-hez, tehát $\varphi(N)$-hez relatív prím.
3. Kiszámítjuk az e inverzét modulo $\varphi(N)$, azaz keresünk egy d számot, amelyre $1 < d < \varphi N)$ és $ed \equiv 1 \pmod{\varphi(N)}$.

A kulcsválasztás a 3. lépéssel be is fejeződik. A rendszerszerű üzemeltetés során azonban egy központi, minden felhasználó által hozzáférhető nyilvántartásra van szükség. Ennek érdekében a kulcs nyilvános részét, esetünkben az (N,e) számpárt nyilvánosságra hozzuk, a kulcs titkos részét, a (d,p,q) számhármast s ezzel együtt a $\varphi(N)$ számot titokban tartjuk.
Ha A felhasználó B felhasználónak akar üzenni, akkor A felhasználó kikeresi a B nyilvános kulcsát, az $e = e_B$ és $N = N_B$ számokat.A felhasználó előkódolja az üzenetet. A nyílt szöveg valamilyen karakterkészlet elemeiből áll. A rejtjelezéshez ezt a karaktersorozatot olyan nemnegatív egészek sorozatává kell átalakítani, amelyek mindegyike kisebb, mint N_B. Ez egy kölcsönösen egyértelmű transzformáció, amelyet minden felhasználó ismer. A rejtjelezést az előkódolt üzenet egymás utáni számain A felhasználó egyenként hajtja végre. Ha az előkódolt szöveg

következő száma x, akkor a megfelelő rejtjeles szám:

$$y \equiv E_B(x) = x^{e_B} \pmod{N_B}.$$

A B felhasználó megkap egy rejtjeles üzenetet. Ez az üzenet szükségszerűen a 0 és $N_B - 1$ közti egész számok egy $y_1, y_2, \ldots$ sorozata. A dekódolást a számsorozat elemein külön-külön hajtja végre. Legyen a rejtjeles szöveg a következő szám: y. Ekkor az „előkódolt" üzenet megfelelő száma

$$x \equiv D_B(y) = y^{d_B} \pmod{N_B}.$$

A visszaállított, „előkódolt" $x_1, x_2, \ldots$ sorozatból az előkódolás inverzét alkalmazva adódik a valódi nyílt szöveg.
Egy konkrét példán keresztül megnézzük, hogyan is kell ezt az algoritmust a gyakorlatban használni.

6.1. Példa. Legyen $p = 73$, $q = 151$, így $N = 73 \cdot 151 = 11\,023$, $\varphi(N) = (73-1)(151-1) = 10\,800$. Az e paramétert $e = 11$-re választhatjuk, mivel $(10\,800, 11) = 1$, hiszen $10\,800 = 2^4 \cdot 3 \cdot 5^2 \cdot 9$. Az e inverzét $\bmod \varphi(N)$ az $e \cdot s + \varphi(N) \cdot t = 1$ előállításból kaphatjuk ($d \equiv s \pmod{\varphi(N)}$), amelyhez az euklidészi algoritmussal juthatunk:

$$\begin{aligned} 10\,800 &= 11 \cdot 981 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0, \end{aligned}$$

ahonnan

$$\begin{aligned} 9 &= 10\,800 - 981 \cdot 11 \\ 2 &= 11 - 9 = 11 - (10\,800 - 981 \cdot 11) = -10\,800 + 982 \cdot 11 \\ 1 &= 9 - 2 \cdot 4 = 10\,800 - 981 \cdot 11 - 4(-10\,800 + 982 \cdot 11) = \\ &= 5 \cdot 10\,800 - 4\,909 \cdot 11, \end{aligned}$$

így

$$-4\,909 \cdot 11 \equiv 1 \pmod{10\,800},$$

ezért

$$d \equiv 10\,800 - 4\,909 = 5\,891 \pmod{10\,800}.$$

Nyilvánosságra hozzuk az $e = 11$, $N = 11\,023$ egészeket, s titokban tartjuk a $p = 73$, $q = 151$, $d = 5\,891$ egészeket.
Tegyük fel, hogy az $x = 17$ nyílt üzenetet kívánjuk kódolni, ekkor

$$y \equiv 17^{11} \pmod{11\,023},$$

ahonnan $y = 1\,782$. A dekódolás az

$$x \equiv 1\,782^{5\,891} \pmod{11\,023}, \tag{6.1}$$

művelettel történik. Ezen modulo hatvány kiszámítását egyszerűsíti a „négyzetreemelés és szorzás" módszere. A kitevőt az

$$5\,891 = 2^0 + 2^1 + 2^8 + 2^9 + 2^{10} + 2^{12}$$

összegre bonthatjuk a bináris ábrázolása alapján. Ennek alapján a (6.1) hatványt az alábbi alakba célszerű átírni:

$$1\,782^{2^{12}} \cdot 1\,782^{2^{10}} \cdot 1\,782^{2^9} \cdot 1\,782^{2^8} \cdot 1\,782^{2^1} \cdot 1\,782$$
$$= ((\ldots(1\,782)^2)^2 \cdot 1\,782)^2 \cdot 1\,782)^2)^2)^2)^2)^2)^2 \cdot 1\,782)^2 \cdot 1\,782.$$

A kiértékelést a legbelső moduláris négyzetre emeléssel kezdjük, azaz az első néhány lépés:

$$\begin{aligned} 17\,822 &\equiv 900 \quad (mod \quad 11\,023) \\ 9\,002 &\equiv 5\,321 \quad (mod \quad 11\,023) \\ 5\,321 \cdot 1\,782 \equiv 2\,242^2 &\equiv 76 \quad (mod \quad 11\,023), \\ &\ldots \end{aligned}$$

amely lépéseket követve, végül 17-et kapjuk vissza.

([23]: 79-83.o)

7. Összegzés

Manapság talán már fel sem tűnik az eredmények vizsgálása közben, hogy a megértésükhöz milyen nagy mértékben járulnak hozzá az ókori görög korból származó fogalmak és összefüggések. Nélkülönözhetetlenné váltak az idő során és így a tudásunk alapjait képezik.

Hivatkozások

[1] Ropolyi László, Szegedi Péter: A tudományos gondolkodás története

[2] Van Der Waerden: Egy tudomány ébredése

[3] Sain Márton: Nincs királyi út!

[4] Eukleidész: Elemek (Mayer Gyula fordításában)

[5] https://hu.wikipedia.org/wiki/Négyzetgyök_2

[6] https://matekarcok.hu/primszamok-szama-vegtelen/

[7] https://matekarcok.hu/szamelmelet-alaptetele/

[8] Szalkai István, Dósa György: Algoritmikus számelmélet

[9] https://hu.wikipedia.org/wiki/Geometriai_szerkesztések

[10] https://hu.wikipedia.org/wiki/Euklideszi_szerkesztés

[11] https://hu.wikipedia.org/wiki/Szerkeszthet%C5%91_soksz%C3%B6gek

[12] Kiss Laura: A szabályos 17-szög szerkesztése

[13] https://hu.wikipedia.org/wiki/Neuszisz_szerkesztés

[14] https://hu.wikipedia.org/wiki/Szögharmadolás

[15] Simonovits András: Matematikatörténeti vázlat

[16] https://hu.wikipedia.org/wiki/Fermat-pr%C3%ADmek

[17] https://hu.wikipedia.org/wiki/Kriptográfia

[18] Gyarmati Katalin: Számítógépés Számelmélet

[19] https://en.wikipedia.org/wiki/Carmichael_number

[20] https://people.inf.elte.hu/nebsabi/2013-2014-2/Crypto/primality.pdf

[21] https://academickids.com/encyclopedia/index.php/Carmichael_number

[22] https://lexiq.hu/eratoszthenesz-szitaja

[23] Buttyán Levente, Vajda István: Kriptográfia és alkalmazásai