Carl Friedrich Gauss élete és matematikája

Szakdolgozat

Készítette: Egri Zoltán

Matematika BSc, Matematikai elemző szakirány

Témavezető: Károlyi Gyula, Egyetemi docens

Algebra és Számelmélet Tanszék

Budapest, 2009

Eötvös Loránd Tudományegyetem
Természettudományi Kar

Tartalom

1. Bevezetés **3**

1.1. A dolgozat felépítése 3

2. Élettörténeti betekintés **4**

3. Gaussról algebrai tanulmányaimból **7**

3.1. A Gauss-eliminációról 7

3.2. Gauss-egészekről 10

4. Szabályos, prímoldalú sokszögek szerkeszthetősége **14**

4.1. Bevezetés 14

4.2. A szabályos 5-szög és 17-szög szerkeszthetősége 16

5. Kvadratikus maradékok, a kvadratikus reciprocitás tétele **23**

5.1. Bevezetés 23

5.2. Kvadratikus maradékok, Legendre-szimbólum 24

5.3. Kvadratikus reciprocitási tétel bizonyítása a Gauss-lemmával 26

5.4. Kvadratikus reciprocitás Gauss-összegekkel történő bizonyítása 31

6. Összefoglalás **39**

1. Bevezetés

Gauss kíváló tehetségű tudós volt, aki a tudományok számos területének fejlődéséhez járult hozzá, így a *számelmélet*hez, az *analízis*hez, a *differenciálgeometriá*hoz, a *geodéziá*hoz, a *mágnesesség*hez, az *asztronómiá*hoz és az *optiká*hoz. A gyakran „matematika fejedelmé"-nek is nevezett Gaussnak olyan komoly hatása volt a matematika és a tudomány több területén, hogy Euler, Newton és Arkhimédesz mellett minden idők egyik legnagyobb matematikusaként tartják számon. Gauss csodagyerek volt, akinek kisgyermekkori, meghökkentő koraérettségéről anekdoták keringenek, s még csak tinédzser volt, mikor első áttörő matematikai felfedezéseit elérte. 24 évesen fejezte be fő művét, a **Disquisitiones Arithmeticae**-t, amely döntő szerepet játszott a számelmélet tudományágként való megszilárdulásában, és ezt a területet a mai napig formálja.

1.1. A dolgozat felépítése

Carl Friedrich Gauss munkássága példaértékű minden matematikával foglalkozó ember számára. A matematika szinte minden területén alkotott. Jómagam is a 3 év tanulmányai alatt számtalanszor találkoztam a nevével. Ezen tapasztalatok sarkalltak arra, hogy szakdolgozatomnak az ő munkásságát válasszam. Természetesen lehetetlen volna ezen dolgozat terjedelmén belül, akárcsak említés szintjén az általa megalkotott, kidolgozott összes elmélettel foglalkozni, így erre kísérletet sem próbálok tenni. A számomra legérdekesebb és leghasznosabb eredményeit próbáltam mikroszkóp alá venni.

Dolgozatomat úgy szerkesztettem, hogy a bevezető fejezeteken (Bevezetés, Élettörténeti betekintés) kívüli fejezetek, így a harmadik fejezet foglalakozik az általam tanult, Gausstól származó algebrai eredményekkel, úgymint a *Gauss-elimináció* és a *Gauss-egészek*. A negyedik fejezet foglalkozik a szabályos, prímoldalú sokszögek, így a 17-szög szerkeszthetőségével, melyben le is írom, hogy az ifjú lángész hogy jött rá ennek a 2000 éves problémának a megoldására. Az utolsó fejezetben megvizsgálom

a *kvadratikus reciprocitási tétel*t és mutatok rá 2 bizonyítást is. Mindkettő Gauss nevéhez köthető.

2. Élettörténeti betekintés

Gauss 1777. április 30-án Braunschweigben született, a németországi Braunschweig-Lüneburgi hercegségben, alacsonyabb osztálybeli szülők gyermekeként. Tehetsége már nagyon korán kezdett kibontakozni. Négy éves korában már ismerte a számokat ezerig és kavicsok segítségével ismerkedett a csoportosítással. Hét éves korában megkezdte tanulmányait a Katalin népiskolában, ahol harmadik évben számtant is oktattak. Ekkor hívta fel magára először a figyelmet. Feladatuknak kapták, hogy adják össze a számokat 1-től 100-ig. A 10 éves Gauss pár másodpercen belül megoldotta a feladatot (ugyanis ekkor már tisztában volt a *számtani sorozat* összegképletével), és csak az ő megoldása bizonyult helyesnek. Ezután gyorsan kezdett elterjedni a kis csodagyerek híre. Bartels segédtanítóval ismerkedett a végtelen sorokkal és a Newton-féle binomiális együtthatókkal. Braunschweig hercege ösztöndíjat adományozott az ifjúnak a Collegium Carolinumba, ahova 1792 és 1795 között járt. Innen pedig a göttingeni egyetemre ment, ahol 1795 és 1798 között folytatta tanulmányait. Itt bámulatos szorgalommal veti bele magát a számokkal való műveletekbe. *Induktív módszer*ekkel jön rá az általános összefüggésekre.

1796-ban történt az első igazi áttörés Gauss életében. Sikerült bebizonyítania, hogy a szabályos 17-szög megszerkeszthető geometriai szerkesztéssel. Általánosságban megmutatta azt is, miszerint bármely szabályos sokszög, melynek oldalainak száma *Fermat-prím*, megszerkeszthető. Ezen eredményét *március 30*-án publikálta. E nappal datálva kezdődik a napló, melybe az ifjú a felfedezéseit, áttöréseit írja le. Az iromány ból kiderül, hogy a tudóspalánta szinte naponta gazdagította a matematika legtöbb területét egy-egy tétel bizonyításával. *Április 8*-án bebizonyította az általa arany-nak nevezett tételt, s mint kiderült ez Euler általános sejtésének bizonyítása volt a *kvadratikus reciprocitási tétel*-re. *Május 30*-án megsejti a *prím-*

*számtétel*t és használható képet ad a prímszámok egész számok közti eloszlásáról. 1799-es disszertációjában Gauss bizonyítást adott az algebra alaptételére. Ez a tétel azt állítja, hogy minden legalább elsőfokú, valós vagy általában komplex együtthatós polinomnak van komplex gyöke. Gauss életében még három bizonyítást adott ezen tételre.

1801-ben 4 év megfeszített munkája eredményeként megjelent leghíresebb munkája, a **Disquisitiones Arithmeticae**. Ez a hatalmas munka tartalmazza Gauss alapvető eredményeit. A hét részből álló műben olvashatjuk a *kvadratikus reciprocitás tétel*ének első két bizonyítását, a a körvonal egyenlő részekre bontásának problémáját, a *számelmélet alaptétel*ének bizonyítását. A nyolcadik rész, mely a reciprocitási tétel kettőnél magasabb, legfeljebb negyedfokú hatványokra való kiterjesztését (*bikvadratikus reciprocitási tétel*) tartalmazza, pénz hiányában nem került kiadásra. A mű óriási hatást gyakorolt a számelmélet és az algebra további fejlődésére. Galois a könyv hatására jutott el annak a kérdésnek a megválaszolására, hogy mely egyenletek oldhatóak meg gyökvonás segítségével.

A tudósnak a matematikán kívül volt egy másik szenvedélye is: a csillagászat. 1801. január 1-én Giuseppe Piazzi olasz csillagász felfedezett egy addig ismeretlen csillagot. Piazzi negyven napig figyelte a csillagot, (melyről utólag kiderült, hogy az egy a Mars és a Jupiter között elhelyezkedő kisbolygó, melynek a Ceres nevet adták), kilenc fokon át követve az égen, amikor az átmenetileg eltűnt a Nap ragyogása mögé. További hónapokkal később, amikor a Ceresnek ismét meg kellett volna jelennie, Piazzinak nem sikerült megtalálnia. Gauss két hónapi munka után kiszámította a bolygó pályáját, melynek alapján (egy évvel a bolygó felfedezése után) újra megtalálták a Ceres-t. Ez a esemény sarkallta Gausst arra, hogy megírja munkáját a kisbolygók nagybolygók által megzavart mozgásának elméletéről, amelyet végül 1809-ben publikált *Theoria motus corporum coelestium in sectionibus conicis solem ambientum* (a Nap körül kúpmetszetekben mozgó égitestek mozgásának elmélete) címen. Gauss számára megjön az elismerés: a Pétervári Tudományos Akadémia levelező tagjává választja. Megírja az *Égitestek mozgásának elmélete* című művét, mely-

ben bevezeti a legkisebb négyzetek módszerét. 1807-ben a göttingeni csillagászati obszervatórium csillagászprofesszora és igazgatója lett, amely posztokat élete végéig megtartotta.

Az 1810-es évek végén Gausst megkérték arra, hogy hajtson végre egy geodéziai vizsgálatot Hannover államban, hogy összekapcsolódjon a meglévő dán térképhálózattal. A hannoveri vizsgálat később a Gauss-eloszlás (amelyet normál eloszlásként is ismernek) kidolgozásához vezetett, a mérési hibák leírására. Sőt, ez felkeltette a tudós érdeklődését a differenciálgeometria iránt. Ezen a területen egy fontos tétellel állt elő: a theorema egregiummal (latinul nevezetes tétel), amely a görbület fogalmának egy fontos tulajdonságát állapítja meg. Hétköznapi nyelven a tétel azt állítja, hogy a felület görbülete teljes egészében meghatározható szögek és távolságok mérésével a felületen.

A fizika terén is maradandót alkotott a „matematikusok fejedelme". Wilhelm Weber fizikaprofesszorral 1833-ban elkészítették az első elektromos távírót. Kifejlesztett egy módszert a mágneses mező horizontális intenzitásának mérésére, amely egészen a XX. század második feléig használatban volt és elősegítette a Föld mégneses mezője belső (mag és kéreg), valamint külső részének (magnetoszféra) elkülönítésének matematikai elméletét.

Gauss a németországi Göttingenben hunyt el 1855. február 23-án. Braunschweigben a tiszteletére emelt emlékmű alapzata szabályos 17-szög. Életéről könyvek mesélnek és a matematika is számtalan fogalomban megőrizte a nevét, például: *Gauss-összeg, Gauss-lemma, Gauss-elimináció, Gauss-Seidel módszer, Gauss-Osztrogradszkij tétel, Gauss-görbe, Gauss-Bonnet tétel.* Fizikai mértékegységben is megemlékszünk róla. A mágneses térerősség mértékére bevezették a *Gauss*-t, melynek nagysága 10^{-4} Tesla.

3. Gaussról algebrai tanulmányaimból

3.1. A Gauss-eliminációról

Matematikai számításaink során gyakran felmerül a lineáris egyenletrendszerek megoldása. A matematika történelme során sokan, sokféle megoldást adtak erre a problémára. Lényegében kétféle módszertípus alakult ki: az egyik, amikor megpróbáljuk az egyenletekből a pontos megoldást kinyerni, a másik, amikor csupán csak meg akarjuk közelíteni a megoldást, viszont minden lépéssel közelebb és közelebb szándékozunk kerülni a megoldáshoz. Ez előbbi elv alapján működő algoritmusokat *direkt módszerek*nek, míg az utóbbiakat *iterációs módszerek*nek hívjuk. A direkt módszerek közé sorolható a Carl Friedrich Gaussról elnevezett *Gauss-elimináció* vagy más néven *Gauss-Jordan-elimináció*.

Tekintsük a következő, speciális esetet, amikor n ismeretlent tartalmazó, n egyenletből álló lineáris algebrai egyenletrendszerünk van:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= f_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= f_2 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &= f_n \,. \end{aligned}$$

Itt $a_{i,j}$ és f_i $(i = 1 \ldots n, j = 1 \ldots n)$ értékek adott, általában valós számok, míg x_i ismeretlen értékek. Jelölje M a fenti egyenletrendszer együtthatómátrixát:

$$M := \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

továbbá

$$x := \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \qquad f := \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix}$$

az oszlopvektorokat. Ekkkor a fenti egyenletrenszer átírható a következőképpen:

$$Mx = f\,.$$

Az $Mx = f$ rendszer esetén a Gauss-elimináció a következőképpen jár el. (Megjegyezzük, hogy ez egy speciális eset, a valóságban legtöbbször az ismeretlenek és az egyenletek száma nem eggyezik meg.) Legyen $a_{11} \neq 0$. Kivonjuk az első egyenlet $c_{i1} = \frac{a_{i1}}{a_{11}}$-szeresét az i-edik egyenletből, $(i > 1)$. Ha az M mátrix elemeit $a_{ij} := a_{ij}^{(1)}$-vel jelöljük, továbbá a kivonás által $(i > 1)$ megalkotott új elemeket pedig $a_{ij}^{(2)}$-vel, akkor a műveleteket a következőképpen írhatjuk fel:

$$a_{ij}^{(2)} := a_{ij}^{(1)} - c_{i1} a_{ij}^{(1)}, \qquad j = 1 \ldots n \tag{3.1}$$

$$b_i^{(2)} := b_i^{(1)} - c_{i1} b_1^{(1)}, \qquad i = 2 \ldots n\,. \tag{3.2}$$

Az első lépés után az egyenletrendszer a következőképpen módosul:

$$\begin{aligned} a_{11}^{(1)} x_1 + a_{12}^{(1)} x_2 + \ldots + a_{1n}^{(1)} x_n &= f_1^{(1)} \\ a_{22}^{(2)} x_2 + \ldots + a_{2n}^{(2)} x_n &= f_2^{(2)} \\ &\vdots \\ a_{n2}^{(2)} x_2 + \ldots + a_{nn}^{(2)} x_n &= f_n^{(2)}\,. \end{aligned}$$

A második lépésben, feltéve, hogy $a_{22}^{(2)} \neq 0$, hasonlóképpen járunk el az első sor alatti $(n-1) \times (n-1)$-es egyenletrendszerrel. Folytatva az eliminációt, feltéve, hogy nem történik fennakadás $(a_{kk}^{(k)} \neq 0,\ k = 3, \ldots, n-1)$, a következő egyenletrendszert

kapjuk:

$$\begin{aligned} a_{11}^{(1)}x_1 + a_{12}^{(1)}x_2 + a_{13}^{(1)}x_3 + \ldots + a_{1n}^{(1)}x_n &= f_1^{(1)} \\ a_{22}^{(2)}x_2 + a_{23}^{(2)}x_3 + \ldots + a_{2n}^{(2)}x_n &= f_2^{(2)} \\ a_{33}^{(3)}x_3 + \ldots + a_{3n}^{(3)}x_n &= f_3^{(3)} \\ \vdots & \\ a_{nn}^{(n)}x_n &= f_n^{(n)}\,. \end{aligned}$$

Ha az utolsó egyenletben az $a_{nn}^{(n)} \neq 0$ feltétel is teljesül, akkor x_n értékét könnyen megkaphatjuk, majd fordított sorrendben haladva az $x_{n-1}, \ldots, x_1$ értékek is kiszámolhatóak.

Hogyan tudjuk ellenőrizni, hogy a Gauss-elimináció megakad-e vagy sem? Az alábbi tétel adja meg erre a választ.

3.1.1. Tétel. A Gauss-elimináció pontosan akkor végezhető el, ha az összes bal felső főminor nemzérus:

$$det \begin{pmatrix} a_{11} & \ldots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \ldots & a_{kk} \end{pmatrix} \neq 0, \qquad k = 1, \ldots, n \tag{3.3}$$

A Gauss-elimináció alkalmazása a matematika számos területén megfigyelhető. Az algebrai egyenletrendszerek egyik leggyorsabb megoldási módszere, az operációkutatásban a szimplex módszerek elengedhetetlen eszköze. A numerikus analízisben az LU– és a *Cholesky*– felbontás is erre épül.

3.2. Gauss-egészekről

Diofantikus egyenletnek általában olyan egész együtthatós algebrai egyenletet nevezünk, melynek a megoldásait is az egész, esetenként a racionális számok körében keressük.

Ezen egyenletek megoldása igen változatos eljárásokat követel, mivel univerzális megoldási algoritmus nem ismeretes, sőt annak a kérdésnek az eldöntése is nehéz, hogy egy ilyen egyenlet megoldható-e vagy sem. A Gauss-egészek jól használhatóak bizonyos diofantikus egyenletek megoldásánál. Vizsgáljuk meg közelebbről ezen számok gyűrűjét.

3.2.1. Definíció. Azokat az $\alpha = a + bi$ komplex számokat, ahol $a, b \in \mathbb{Z}$, *Gauss-egészek*nek nevezzük.

3.2.2. Definíció. $\alpha = a+bi$ Gauss-egész *normá*jának nevezzük és $N(\alpha)$-val jelöljük az α abszolút értékének négyzetét:

$$N(\alpha) = |\alpha|^2 = \alpha\bar{\alpha} = a^2 + b^2 \,. \tag{3.4}$$

3.2.3. Tétel. Tetszőleges α és β Gauss-egészekre

1. $N(\alpha)$ nemnegatív egész szám.
2. $N(\alpha) = 0 \Longleftrightarrow \alpha = 0$.
3. $N(\alpha\beta) = N(\alpha)N(\beta)$
4. $\alpha|_{\mathbb{G}}\beta \Longrightarrow N(\alpha)|_{\mathbb{Z}}N(\beta)$

4.-ben $|_{\mathbb{G}}$ a Gauss-egészek-beli, $|_{\mathbb{Z}}$ az egész számok-beli oszthatóságot jelöli.

3.2.4. Tétel. A Gauss-egészek gyűrűjében az egységek ± 1, $\pm i$ számok. Ezek pontosan azok a Gauss-egészek, amelyeknek normája 1.

A következő tétel ad lehetőséget a maradékos osztás elvégzésére, és az arra alapuló Euklideszi-algoritmusra, aminek alapján levezethető a Gauss-egészek körében a számelmélet alaptétele.

3.2.5. Tétel. Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, amelyekre $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Mivel a számelmélet alaptétele fennáll a Gauss-egészek körében is, a prím és a felbonthatatlan fogalma itt is egybeesik.

3.2.6. Tétel. A Gauss-egészek között a prímek az alább felsorolt számok, illetve egységszereseik:

1. $1 + i$.
2. Minden pozitív, $\mathbb{Z}$-beli $4k + 3$ alakú prímszám.
3. Minden pozitív, $\mathbb{Z}$-beli $4k+1$ alakú p prímszám esetén a $p = \pi_1\pi_2$ felbontásból származó p normájú π_1 és π_2.

Példák:
$2 = (1 + i)(1 - i) = (-i)(1 + i^2)$ a 2 kanonikus alakja $\mathbb{G}$-ben.
$3, -3, 3i, -3i$ mind prímek a Gauss egészek között.
$5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$.

A következő két állítás elégséges feltételt biztosít arra, hogy vajon egy α Gauss-egész prím-e $\mathbb{G}$-ben.

3.2.7. Állítás. Ha $N(\alpha)$ prím $\mathbb{Z}$-ben, akkor α prím $\mathbb{G}$-ben.

3.2.8. Állítás. Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím $\mathbb{Z}$-ben, akkor α prím $\mathbb{G}$-ben.

Kanyarodjunk vissza a diofantikus egyenletekhez. Arra a kérdésre keressük a választ, vajon mely számok állnak elő két négyzetszám összegeként. Az $x^2+y^2=n$ egyenlet bal oldalát az egész (vagy akár a valós) számok keretén belül nem tudjuk szorzattá alakítani, viszont a Gauss-egészek körében már igen. Az $(x+iy)(x-iy)=n$ egyenlet vizsgálata ezzel visszavezethető n kanonikus alakjának vizsgálatára.

3.2.9. Tétel (Két-ngyzetszám-tétel). Legyen az n pozitív egész kanonikus alakja

$$n = 2^{\alpha} p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s} , \tag{3.5}$$

ahol a p_μ prímek $4k+1$, a q_υ prímek $4k-1$ alakúak, és az $\alpha, \beta_\mu, \gamma_\upsilon$ kitevők nemnegatív egészek. Az

$$x^2 + y^2 = n \tag{3.6}$$

diofantikus egyenlet akkor és csak akkor oldható meg, ha minden γ_υ páros, és ebben az esetben a megoldásszám

$$4 \prod_{\mu=1}^{r} (\beta_\mu + 1) .$$

Példa: Legyen $n = 4050$. A 4050 kanonikus alakja $2 \cdot 3^4 \cdot 5^2$. Itt 3 az egyetlen $4k-1$ alakú szám, és ennek kitevője páros, tehát van megoldás. A megoldásszám az 5 (az egyetlen $4k+1$ alakú prímtényező) kitevőjéből: $4(2+1)$. A megoldások

$$4050 = (\pm 45)^2 + (\pm 45)^2 = (\pm 9)^2 + (\pm 63)^2 = (\pm 63)^2 + (\pm 9)^2 .$$

Most nézzünk egy konkrét feladatot a Gauss-egészek felhasználására.

Feladat: Oldjuk meg az $x^2 + 1 = y^3$ diofantikus egyenletet!

Megoldás: Bontsuk az egyenlet bal oldalát szorzattá: $(x+i)(x-i) = y^3$. Legyen $x+i$ és $x-i$ legnagyobb közös osztója δ. Ekkor

$$\delta | (x+i) - (x-i) = 2i = (1+i)^2 .$$

Ebből az következik, hogy $\delta = (1+i)^r$, ahol $0 \leq r \leq 2$. A konjugálás műveletartó tulajdonságból ($\overline{zv} = \overline{z}\overline{v}$) adódik, hogy

$$(1+i)^s \,|\, x+i \Longleftrightarrow (1-i)^s \,|\, x-i\,. \tag{3.7}$$

Az $1+i$ és $1-i$ egymás egységszeresei, ezért (3.7)-ből következik, hogy az $1+i$ kitevője az $x+i$ és $x-i$ kanonikus alakjában egyaránt r. Az $(x+i)(x-i)$ szorzat a Gauss-egészek körében is köbszám, így kanonikus alakjában minden Gauss-prím így $1+i$ kitevője is osztható 3-mal. Innen következik, hogy $3 \,|\, 2r$, ahonnan $r = 3t$. Mivel tudjuk, hogy $0 \leq r \leq 2$, így csupán $r = 0$ lehetséges. Innen következik, hogy $\delta = 1$ vagyis $x+i$ és $x-i$ relatív prímek. Az előző gondolatmenetből pedig kiderül, hogy mindkettő köbszám a Gauss-egészek körében, ugyanis az egységek: $1 = 1^3$, $(-1) = (-1)^3$, $i = (-i)^3$, $-i = i^3$ is köbszámok. Így

$$x + i = (c+di)^3 = c^3 - 3cd^2 + (3c^2d - d^3)i\,. \tag{3.8}$$

Összehasonlítva a képzetes részeket $1 = d(3c^2 - d^2)$ adódik. Innen $d = \pm 1$ lehetséges, amiket visszahelyettesítva csupán $d = -1$ esetén kapunk c-re egész értéket. Ekkor $c = 0$. (3.8)-ból kapjuk, hogy $x = c^3 - 3cd^2$, ahonnan $x = 0$, így $y = 1$.

4. Szabályos, prímoldalú sokszögek szerkeszthetősége

4.1. Bevezetés

A geometriai szerkeszthetőségi problémák évezredekre nyúlnak vissza. Az ókori Görögországból származnak a híres szerkesztési problémák. Ezek a következők: **szögharmadolás, kockakettőzés, körnégyszögesítés**. Ezek Euklideszi-szerkesztéssel nem kivitelezhetőek, vagyis az alábbi 5 alaplépés segítségével nem megoldhatóak.

1. Két adott vagy megszerkesztett ponton át egyenes húzása.
2. Két megszerkesztett egyenes metszéspontjának kijelölése.
3. Két adott vagy megszerkesztett pont körzőnyílásba vétele, és ezzel a sugárral egy adott vagy megszerkesztett pont körüli kör rajzolása.
4. Megszerkesztett kör és egyenes metszéspontjainak kijelölése.
5. Két megszerkesztett kör metszéspontjainak kijelölése.

Ezek a szerkesztések a négy algebrai alapművelet és a gyökvonás felhasználásával is megoldhatóak. Az 1. és 2. lépésben az alapműveletek elegendőek a megoldáshoz, a 3. és 4. lépésben a kör sugarának kiszámításához a gyökvonás műveletét is használnunk kell. Az 5. lépésben a két kör metszéspontjának kijelölését visszavezetjük egy kör és egy egyenes mesztéspontjainak kijelölésére, így ez egy 4. típusú lépés megoldása. Mivel körző és vonalzó segítségévelegyszerűen meg tudjuk adott szakaszok hosszának összegét, különbségét, szorzatát, hányadosát és adott szakasz gyökhosszát is, ez lehetőséget nyújt a szerkeszthetőség problémájának pontos, algebrai megfogalmazására.

Tegyük fel hogy már meghúztunk egy szakaszt, melyet egységhosszúnak definiáltunk. Ekkor körzővel és vonalzóval újabb szakaszokat tudunk szerkeszteni, melynek

hosszai a meglévőből összeadás, szorzás, kivonás, osztás és négyzetgyökvonás műveletével adódnak.

4.1.1. Definíció. Az olyan számokat, (szakaszok hosszát) amelyek az egységből véges számú összeadás, szorzás, kivonás, osztás és gyökvonás műveletével megkaphatóak, *kvadratikusan irracionális szám*oknak nevezzük.

Érthető, hogy a szabályos n-szög szerkesztése ekvivalens az egységsugarú kör n részre osztásával. A körvonalnak az n részre osztott íveinek a szomszédos végpontjait összekötő szakaszok (a kör húrjai) lesznek a szabályos n-szög oldalai, melyeknek hossza $2\sin(\frac{\pi}{n})$. Következésképpen olyan n-ekre amelyekre $\sin\frac{\pi}{n}$ kvadratikusan irracionális szám, szerkeszthető körzővel és vonalzóval szabályos n-szög.

Két egyszerű állítás szabályos sokszögek szerkesztéséről:

- Ha a körvonal n egyenlő részre osztható, akkor természetesen $2^k n$ részre is felosztható, bármely k pozitív egész esetén. Ez abból adódik, hogy bármely szög felezhető körzővel és vonalzóval.

- Ha a körvonalat fel tudjuk osztani p_1 és p_2 egyenlő részekre, amelyekre $(p_1, p_2) = 1$, vagyis relatív prímek, akkor a körvonal felosztható $p_1 p_2$ egyenlő részre is. Vagyis ha megszerkeszthetőek a $\frac{2\pi}{p_1}$ és a $\frac{2\pi}{p_2}$ szögek, akkor megszerkeszthető a $\frac{2\pi}{p_1 p_2}$ szög is körzővel és vonalzóval.
  Itt felhasználtuk azt a számelméleti tényt, hogy ha $(p_1, p_2) = 1$ akkor léteznek olyan A és B egész számok (egyik pozitív, másik negatív), hogy $Ap_1 + Bp_2 = 1$.

A szabályos sokszögek szerkeszthetőségénél egyszerűbb dolgunk van, ha a komplex számok halmazán vizsgáljuk a szerkeszthetőséget. Az egységsugarú, origóközéppontú körbe rajzolt szabályos n-szög megszerkeszthető, ha az n-edik *egységgyökök* megszerkeszthetőek. Az n-edik *egységgyökök*

$$\epsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}; \qquad k = 0, 1, \ldots, n-1\,. \tag{4.1}$$

Könnyű megmutatni, hogy az ϵ_k vektorok végpontjai egy szabályos n-szög csúcsai. Ha meg tudjuk mutatni hogy az ϵ_k számok kvadratikusan irracionálisak (valós és képzetes részük is), akkor ezzel azt is megmutatjuk, hogy körzővel és vonalzóval szerkeszthető szabályos n-szög.

Tekintsünk most olyan a, b számokat, melyek kvadratikusan irracionálisak. Képezzük belőlük a következő két komplex számot:

$$a + bi = x \qquad \text{és} \qquad a - bi = y\,.$$

A két szám szorzata és összege is kvadratikusan irracionális ($xy = a^2 + b^2$, $x + y = 2a$). Ezek egy másodfokú egyenletnek, a $z^2 - 2az + (a^2 + b^2)$ gyökei. Továbbá ha megoldjuk az egyenletet, visszakapjuk az eredeti x és y számokat. Tehát az olyan komplex számok, melyeknek valós és képzetes része is kvadratikusan irracionális, szintén kvadratikusan irracionálisak. Ennek az észrevételnek a megfordítását legegyszerűbben az algebrai bővítések elméletén keresztül lehet igazolni.

Fontos ismernünk a következő két egyszerű műveletet az egységgyökökről:

$$\epsilon_k \epsilon_l = \epsilon_{k+l} \qquad \text{és} \qquad \epsilon_k = (\epsilon_1)^k\,.$$

Az *n-edik egységgyökök* pont a $z^n = 1$ egyenlet gyökei. Alakítsuk át az egyenletet.

$$z^n - 1 = (z-1)(z^{n-1} + z^{n-2} + \cdots + z + 1) = 0\,. \tag{4.2}$$

Most már elegendő információnk van, hogy megmutassuk, hogy a szabályos 17-szög megszerkeszthető. Előtte azonban egy egyszerűebb, de nagyon hasonló feladat megoldását mutatom be, nevezetesen az ötszög megszerkeszthetőségét.

4.2. A szabályos 5-szög és 17-szög szerkeszthetősége

Először az ötszög ($n = 5$) megoldhatóságát mutatom be. A (4.2) egyenlőséget felhasználva két egyenletet kapunk: $z = 1$ és

$$z^4 + z^3 + z^2 + z + 1 = 0 \tag{4.3}$$

amelynek négy gyöke van. Ezek ϵ_1, ϵ_2, ϵ_3 és ϵ_4. Átalakítva a (4.3) egyenletet (leosztva z^2-tel és rendezve) kapjuk a következő egyenletet:

$$\left(z+\frac{1}{z}\right)^2+\left(z+\frac{1}{z}\right)-1=0\,.$$

Vezessük be a következő helyettesítést: $y=z+\frac{1}{z}$. Ekkor egy másodfokú egyenletet kapunk, melynek gyökei

$$y_{1,2}=\frac{-1\pm\sqrt{5}}{2}\,.$$

Vagyis $z+\frac{1}{z}=y_1$ és $z+\frac{1}{z}=y_2$ egyenleteket kellene megoldani, melyekből már meghatározhatóak a (4.3) egyenlet gyökei, melyek másodfokú egyenletek gyökei. A továbbiakhoz viszont érdemes meggondolni a következőt. Vegyük észre, hogy

$$\epsilon_1+\epsilon_4=\epsilon_1+\frac{1}{\epsilon_1}=y_1=\frac{-1+\sqrt{5}}{2}\,. \tag{4.4}$$

Hasonlóan

$$\epsilon_3+\epsilon_2=\epsilon_3+\frac{1}{\epsilon_3}=y_2=\frac{-1-\sqrt{5}}{2}\,. \tag{4.5}$$

Vagyis a gyökök alkalmas csoportosításával kapjuk, hogy

$$(\epsilon_1+\epsilon_4)(\epsilon_2+\epsilon_3)=\epsilon_3+\epsilon_4+\epsilon_6+\epsilon_7=\epsilon_3+\epsilon_4+\epsilon_1+\epsilon_2\,.$$

Kibővítve a jobb oldalon álló összeget $(-1+1)$ -gyel

$$-1+1+\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4$$

ahol a második tagtól kezdve egy mértani sorozat összegét láthatjuk, melyet átalakítva

$$-1+\frac{\epsilon^5-1}{\epsilon-1}=-1$$

ahol $\epsilon^5=1$, mivel 5-dik egységgyök.

Tehát azt kaptuk, hogy $\epsilon_1+\epsilon_4$ és $\epsilon_2+\epsilon_3$ szorzata és összege is egyenlő -1-gyel, ami

szerkeszthető, így ez a két szám is. Továbbá $\epsilon_1 \cdot \epsilon_4 = \epsilon_2 \cdot \epsilon_3 = \epsilon_5 = 1$, így ϵ_1, ϵ_2, ϵ_3 és ϵ_4 is mind megszerkeszthető. Tehát a szabályos ötszöget is meg tudjuk szerkeszteni.

Gaussnak pontosan ilyen módszerekkel sikerült megvalósítania a 17-szög szerkesztését. A gyökök olyan csoportosítását választotta, amelyek összegei meghatározhatóak másodfokú egyenletek egymás utáni megoldásával. Mielőtt azonban a pontos számolásokra térnénk rá, be kell vezetnünk a primitív gyök definícióját.

4.2.1. Definíció. Legyen p tetszőleges prímszám és $q \in \mathbb{Z}$. Azt mondjuk, hogy a q *primitív gyök* modulo p, ha $p \nmid q$ és az $1 = q^0, q, q^2, \ldots, q^{p-2}$ számok mind különböző maradékot adnak p-vel osztva; vagy másképpen: e számok maradékai – sorrendtől eltekintve – éppen az 1, 2, ..., $p-1$ számok.

Nem nehéz bebizonyítani, hogy minden p prímszámhoz létezik legalább egy primitív gyök modulo p.

Vizsgáljuk most a $p = 17$ prímszámhoz tartozó legkisebb primitív gyököt: $q = 3$. Ezek hatványai kiadják az összes maradékot modulo 17. Ezen maradékok tanulmányozásával találta meg Gauss a

$$z^{16} + z^{15} + z^{14} + \cdots + z + 1 = 0 \tag{4.6}$$

egyenlet gyökeinek alkalmas csoportosítását, melyeket visszavezetett másodfokú egyenletek láncolatainak megoldására.

A (4.6)-os egyenlet gyökeinek az indexelését úgy változtatta meg (ϵ_k -ről $\epsilon_{(m)}$ -re, ahol $0 \leq m \leq 15$), hogy tekintette mikor ad a 3^m 17-tel való osztásakor k maradékot, vagyis az $k = 1, 2, \ldots, 16$ számok 3 alapú indexét vizsgálta (jelölése: $ind_{3,17}(m)$). A következő táblázat első sorában a m értékei vannak feltüntetve, az alatta lévő sorban pedig a 3^m 17-tel való osztásának maradékai olvashatóak le, vagyis k értékei.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

1. táblázat. $k = ind_{3,17}(m)$ értékei

Ez az új indexelés lehetővé tette Gauss számára, hogy a (4.6)-os egyenlet gyökeit csoportokra ossza. Mostmár elegendő információnk van a 17-szög szerkesztésének részletes levezetéséhez.

$$\epsilon_1 + \epsilon_2 + \cdots + \epsilon_{16} = \epsilon_{(0)} + \epsilon_{(1)} + \cdots + \epsilon_{(15)}$$

$$\epsilon_{(0)} + \epsilon_{(1)} + \cdots + \epsilon_{(15)} = -1\,.$$

A továbbiakban jelölje $\eta_{l,r}$ az $\epsilon_{(m)}$ számok olyan összegét m indexre, amelyeket l-lel osztva r maradékot kapunk. Ekkor a következőt kapjuk (a táblázat segít):

$$\eta_{2,0} = \epsilon_{(0)} + \epsilon_{(2)} + \cdots + \epsilon_{(14)} = \epsilon_1 + \epsilon_9 + \cdots + \epsilon_2$$

$$\eta_{2,1} = \epsilon_{(1)} + \epsilon_{(3)} + \cdots + \epsilon_{(15)} = \epsilon_3 + \epsilon_{10} + \cdots + \epsilon_6\,.$$

Nyilvánvaló, hogy

$$\eta_{2,0} + \eta_{2,1} = \epsilon_{(0)} + \epsilon_{(1)} + \cdots + \epsilon_{(15)} = -1\,. \tag{4.7}$$

Közvetlen számolásokkal és az $\epsilon_k\epsilon_l = \epsilon_{k+l}$ felhasználásával könnyen megmutatható, hogy

$$\eta_{2,0} \cdot \eta_{2,1} = 4(\epsilon_{(0)} + \epsilon_{(1)} + \cdots + \epsilon_{(15)})\,. \tag{4.8}$$

A (4.7) és a (4.8) egyenleteket felhasználva a Viète-formula segítségével kapunk egy másodfokú egyenletet melynek gyökei $\eta_{2,0}$ és $\eta_{2,1}$:

$$x^2 + x - 4 = 0\,,$$

melynek megoldásai

$$x_{1,2} = \frac{-1 \pm \sqrt{17}}{2}\,.$$

Egyszerű számolások útján (mivel a $\eta_{2,0}$ és $\eta_{2,1}$ összegekben inverz párok, vagyis a konjugált gyökpárok szerepelnek) megmutatható, hogy $\eta_{2,0} > \eta_{2,1}$. Mivel inverz párokról van szó, a valós részeik kétszeresét kell venni. Így

$$\eta_{2,0} = \frac{-1+\sqrt{17}}{2} \quad \text{és} \quad \eta_{2,1} = \frac{-1-\sqrt{17}}{2}\,. \tag{4.9}$$

Most bontsuk két-két részösszegre az $\eta_{2,0}$ és az $\eta_{2,1}$ összegeket úgy, hogy minden második tag kerül ugyanabba a részösszegbe. Így kapjuk a következőket:

$$\eta_{4,0} = \epsilon_{(0)} + \epsilon_{(4)} + \epsilon_{(8)} + \epsilon_{(12)}$$

$$\eta_{4,1} = \epsilon_{(1)} + \epsilon_{(5)} + \epsilon_{(9)} + \epsilon_{(13)}$$

$$\eta_{4,2} = \epsilon_{(2)} + \epsilon_{(6)} + \epsilon_{(10)} + \epsilon_{(14)}$$

$$\eta_{4,3} = \epsilon_{(3)} + \epsilon_{(7)} + \epsilon_{(11)} + \epsilon_{(15)}\,.$$

Ismét másodfokú egyenletek gyökeire próbálva visszavezetni a részösszegeket, felhasználjuk, hogy

$$\eta_{4,0} + \eta_{4,2} = \eta_{2,0} = \frac{\sqrt{17}-1}{2}\,. \tag{4.10}$$

Továbbá megmutatható, hogy

$$\eta_{4,0} \cdot \eta_{4,2} = \eta_{2,0} + \eta_{2,1} = -1\,. \tag{4.11}$$

A (4.10) és (4.11) egyenlőségek felhasználásával ismét kapunk egy másodfokú egyenletet melyeknek gyökei $\eta_{4,0}$ és $\eta_{4,2}$:

$$x^2 - \left(\frac{\sqrt{17}-1}{2}\right) x - 1 = 0\,.$$

Megoldva az egyenletet , s felhasználva, hogy $\eta_{4,0} > \eta_{4,2}$ kapjuk, hogy

$$\eta_{4,0} = \frac{1}{4}\left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}\right)$$

$$\eta_{4,2} = \frac{1}{4}\left(\sqrt{17} - 1 - \sqrt{34 - 2\sqrt{17}}\right).$$

Hasonlóan $\eta_{4,1}$-re és $\eta_{4,3}$-ra

$$\eta_{4,1} + \eta_{4,3} = \eta_{2,1} = \frac{-\sqrt{17} - 1}{2}.$$

Továbbá

$$\eta_{4,1} \cdot \eta_{4,3} = \eta_{2,0} + \eta_{2,1} = -1.$$

Tehát $\eta_{4,1}$ és $\eta_{4,3}$ az

$$x^2 - \left(\frac{-\sqrt{17} - 1}{2}\right)x - 1 = 0 \quad \text{egyenlet gyökei}.$$

Így

$$\eta_{4,1} = \frac{1}{4}\left(-\sqrt{17} - 1 + \sqrt{34 + 2\sqrt{17}}\right)$$
$$\eta_{4,3} = \frac{1}{4}\left(-\sqrt{17} - 1 - \sqrt{34 + 2\sqrt{17}}\right).$$

Ismét bontsuk fel az összegeket az előző módon részösszegekre, így kapunk nyolc különálló összeget, melynek mindegyike kéttagú. Ezek közül vizsgáljuk az $\eta_{8,0}$-t és az $\eta_{8,4}$-t, melyeknek felhasználása elegendő a szerkeszthetőséghez. Elég bebizonyítanunk, hogy az $\eta_{8,4} = 2\cos\frac{8\pi}{17}$ kvadratikusan irracionális szám.

Tudjuk, hogy $\eta_{8,0} + \eta_{8,4} = \eta_{4,0}$ és $\eta_{8,0} \cdot \eta_{8,4} = \eta_{4,1}$. Továbbá megállapítható, hogy $\eta_{8,0} > \eta_{8,4}$, ezért $\eta_{8,4}$ az $x^2 - \eta_{4,0}x + \eta_{4,1} = 0$ egyenlet kisebbik gyöke, tehát

$$\eta_{8,4} = 2\cos\frac{8\pi}{17} = \frac{1}{2}\left(\eta_{4,0} - \sqrt{\eta_{4,0}^2 - 4\eta_{4,1}}\right).$$

Elvégezve a szorzásokat és helyettesítéseket kapjuk a következő kifejezést:

$$\frac{1}{8}\left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}\right) - \frac{1}{4}\left(\sqrt{17 + \sqrt{17} - \sqrt{170 + 38\sqrt{17}}}\right). \qquad (4.12)$$

Továbbá a $2\cos\frac{8\pi}{17}$ átírható elemi trigonometrikus összefüggések felhasználásával. Így

$$2\cos\frac{8\pi}{17} = 2\sin\left(\frac{\pi}{2} - \frac{8\pi}{17}\right) = 2\sin\frac{\pi}{34}$$

ami nem más mint az egységsugarú körbe írt szabályos 34-szög oldalhossza. Ennek segítségével nyilván az egységsugarú körben vett szabályos 17-szög is megszerkeszthető.

Gauss a 17-szög szerkeszthetőségénél sokkal többet bizonyított be. Tőle származik az alábbi tétel:

4.2.2. Tétel. Szabályos n-szög ($n > 2$) akkor és csak akkor szerkeszthető meg, ha n prímtényezős felbontása

$$n = 2^m p_1 \cdots p_r \qquad m, r \geq 0$$

ahol $p_1, \ldots p_r$ páronként különböző *Fermat-prímek* (vagyis $2^{2^k} + 1$ alakú prímek).

Gauss tételéből tehát következik, hogy azok a szabályos sokszögek, melyeknek oldalai olyan prímszámok, melyek Fermat-prímek, megszerkeszthetőek. Ezt a tételt az algebrai testek véges, másodfokú, normális bővítésével lehetne igazolni, felhasználva a körosztási-test definícióját.

Az első 5 Fermat szám valóban prím, ezek: 3, 5, 17, 257, 65537, és ilyen oldalú szabályos sokszögeket valóban meg lehet szerkeszteni. A 6. Fermat szám nem prím, mivel osztható 641-gyel. Elvi akadálya nincsen ezen sokszögek szerkesztésének, viszont a gyökök alkalmas csoportosítását megtalálni, és a gyököket meghatározni hatalmas feladat, de teljesen gépies munkát igényel. A 257-oldalú szabályos sokszögre való bizonyítást adta Richelot, melynek terjedelme közel 80 oldal. A 65537-oldalúra J.Hermes mutatott levezetést, mely több mint 20 évi munkának a gyümölcse.

5. Kvadratikus maradékok, a kvadratikus reciprocitás tétele

5.1. Bevezetés

A kvadratikus reciprocitási tételnek ma már több mint 200 különböző bizonyítása létezik. Ezen bizonyításoknak majdnem a fele támaszkodik a Gauss által megalkotott lemmára és a Gauss összegekre. Az általa csak *arany tétel*nek nevezett tételre életében 8 különböző bizonyítást adott, melyből 6-ot ő maga publikált, a maradék kettőt a halála után nyilvánosságra került jegyzeteiből ismeri a világ.

Az első bizonyítása indukción alapul, megjegyzendő, hogy ebben a bizonyításban neki is – hasonlóan Legendre-hoz – szüksége volt egy bizonyos segédprímre. Második bizonyítása a bináris kvadratikus formulák elméletén alapszik, a negyedik és hatodik igazolás során a Gauss összegeket használja fel. Mint ennek a tételnek a legtöbb bizonyítása, a 3. és 5. igazolás az ún. Gauss-lemmán alapul. Hogy miért bizonyította nyolcféleképpen a német zseni ezt a tételt, arról a legtöbb matematikus hasonlóképpen vélekedik: „A bizonyítás olyan út, melynek során a matematikai területek új tulajdonságait és új mezőit fedezzünk fel”[1].

Most lássuk a már sokat említett tételt.

5.1.1. Tétel (Kvadratikus reciprocitás tétele). Legyen p és q különböző páratlan prím. Ha legalább az egyikük az 1 maradékot adja 4-gyel osztva, akkor az

$$x^2 \equiv p \pmod{q} \quad \text{és az} \quad y^2 \equiv q \pmod{p} \tag{5.1}$$

kongruenciák egyszerre megoldhatóak vagy megoldhatatlanok (az x és y megoldások nem szükségképp azonosak) ha viszont mindkét prím a 3 maradékot adja 4-gyel osztva, a fenti kongruenciáknak pontosan egyike oldható meg.

A tétel jobb megértéséhez szükségünk van a kvadratikus maradékok és a Legendre-szimbólum alapvető ismeretére.

[1] Yuri I. Manin, orosz matematikussal történő interjú során adott válaszából.

5.2. Kvadratikus maradékok, Legendre-szimbólum

Ebben a szakaszban a p végig 2-nél nagyobb prímet jelöl.

5.2.1. Definíció. Tegyük fel, hogy $(a, p) = 1$. Az a számot aszerint nevezzük *kvadratikus maradék*nak, illetve *kvadratikus nemmaradék*nak modulo p, hogy az $x^2 \equiv a \pmod{p}$ kongruencia megoldható-e vagy sem.

Az $a \equiv 0 \pmod{p}$ számokat nem soroljuk sem a kvadratikus maradékok, sem a kvadratikus nemmaradékok közé. Az elsőéves számelméleti tanulmányaink során megismerkedtünk az alábbi tétellel:

5.2.2. Tétel.

1. Az a szám akkor és csak akkor kvadratikus maradék modulo p ha $a^{(p-1)/2} \equiv 1 \pmod{p}$.
2. Az a szám akkor és csak akkor kvadratikus nemmaradék modulo p ha $a^{(p-1)/2} \equiv -1 \pmod{p}$.
3. A páronként inkongruen kvadratikus maradékok száma illetve kvadratikus nemmaradékok száma egyaránt $(p-1)/2$.
4. Ha a kvadratikus maradék, akkor az $x^2 \equiv a \pmod{p}$ kongruenciának két (páronként inkongruens) megoldása van.

A fenti tétel 1. állítását szokás *Euler-kritérium*nak is nevezni.

5.2.3. Definíció (Legendre-szimbólum). Legyen $p > 2$ prím. A *Legendre-szimbólum*ot tetszőleges a egész számra a következőképpen definiáljuk:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ kvadratikus maradék modulo } p \\ 0, & \text{ha } p \text{ osztója } a\text{-nek} \\ -1, & \text{ha } a \text{ kvadratikus nemmaradék modulo } p\,. \end{cases}$$

Példa: $\left(\frac{3}{11}\right) = 1$, mert az $x^2 \equiv 3 \pmod{11}$ kongruencia megoldható, és az egyik megoldása az $x \equiv 6 \pmod{11}$.

A (5.2.2) Tétel és a Legendre-szimbólum összevetésével kapjuk az alábbi összefüggést:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}. \tag{5.2}$$

A Legendre-szimbólummal kapcsolatos műveleteket a következő tétel segíti.

5.2.4. Tétel.

1. $a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4} \\ -1, & \text{ha } p \equiv -1 \pmod{4} \end{cases}$

Bizonyítás: A fent említett állításokat könnyű bizonyítani, mivel szinte azonnal adódnak (5.2)-ből. A 4. állítást bizonyítom, amely két részből tevődik össze: ha (A) $p = 4k+1$ alakú illetve ha (B) $p = 4k-1$ alakú.

(A)
$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1 \pmod{p}$$

(B)
$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k-2}{2}} = (-1)^{2k-1} = -1 \pmod{p}$$

amit állítottunk. ■

A kvadratikus reciprocitási tétel a Legendre-szimbólummal megfogalmazva a következőképpen írható:

5.2.5. Tétel. Ha p, $q > 2$ két különböző prím, akkor

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}} \tag{5.3}$$

Ehhez a tételhez szoktak még csatolni egy úgynevezett kiegészítő lemmát:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}. \tag{5.4}$$

A (5.3), a (5.4) és a 5.2.4 Tétel alapján egyszerű algoritmussal minden Legendre-szimbólum értéke kiszámolható.

Ellenőrizhető, hogy a korábbi megfogalmazása valóban ugyanazt mondja, ugyanis ha p, q valamelyike 1-gyel kongruens modulo 4 (mondjuk $p = 4u + 1$, azaz $p - 1 = 4u$), a jobb oldal kitevője páros (felhasználva, hogy a prímek páratlanok, azaz $q = 2v+1$ alakú),

$$\frac{(p-1)(q-1)}{4} = \frac{[(4u+1)-1][(2v+1)-1]}{4} = \frac{4u \cdot 2v}{4} = 2uv.$$

Így a jobb oldal értéke 1, tehát vagy mindkét bal oldali Legendre-szimbólum pozitív, vagy mindkettő negatív, azaz egyszerre kvadratikus maradékok vagy kvadratikus nemmaradékok a prímek egymásra nézve. Ha viszont mindkét prím 3-at ad néggyel osztva, akkor $p = 4u + 3$ és $q = 4v + 3$, azaz a jobb oldali kitevő

$$\frac{(4u+2)(4v+2)}{4} = 4\frac{(2u+1)(2v+1)}{4} = (2u+1)(2v+1)$$

páratlan, így a jobb oldal értéke -1, és így a bal oldai Legendre-szimbólumok értéke különböző: ha az egyik 1, a másik -1, emiatt ha az egyik prím a másikra nézve kvadratikus maradék, akkor a másik az egyikre nézve kvadratikus nemmaradék.

5.3. Kvadratikus reciprocitási tétel bizonyítása a Gauss-lemmával

A kvadratikus recioprocitási tétel elemi szintű bizonyításainak fő összetevője a Gauss-lemma, melyet a német matematikus fedezett fel, és a harmadik bizonyításá-

nak magját alkotta.

5.3.1. Tétel (Gauss-lemma). Legyen $p > 2$ prím és $(a, p) = 1$. Tekintsük az

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

számok modulo p vett legkisebb abszolút értékű maradékait a $(-\frac{p}{2}, \frac{p}{2})$ intervallumon. Jelölje ν az előbb említett intervallumba képzett negatív maradékok számát. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^{\nu}$$

Bizonyítás: A ν definiálásához meghatároztuk a

$$S = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

számok maradékait a

$$K = \left\{1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\right\}$$

halmazból. Az előjelre való tekintet nélkül egyik szám $(1, 2, 3, \ldots, \frac{p-1}{2})$ se jelenik meg egynél többször, mert ha így lenne, akkor bármely két elem az S-ből kongruens lenne modulo p, vagy összegük 0 lenne. Egyik eset sem lehetséges. Ezért a K halmaz elemeit felírhatjuk a következőképpen:

$$T = \left\{\lambda_1 \cdot 1, \lambda_2 \cdot 2, \ldots, \lambda_{(p-1)/2} \cdot \frac{p-1}{2}\right\},$$

ahol λ_i értéke 1 vagy -1. Összeszorozva az S -beli elemeket és a T elemeit:

$$(1a) \cdot (2a) \cdot (3a) \cdots \left(\frac{p-1}{2}a\right) \equiv (\lambda_1 \cdot 1) \cdot (\lambda_2 \cdot 2) \cdots \left(\lambda_{(p-1)/2} \cdot \frac{p-1}{2}\right) \pmod{p}.$$

Így

$$a^{\frac{p-1}{2}} \equiv \lambda_1 \cdot \lambda_2 \cdots \lambda_{(p-1)/2} \pmod{p}.$$

Felhasználva a (5.2) összefüggést és azt hogy a $\lambda_1 \cdot \lambda_2 \cdots \lambda_{(p-1)/2}$ szorzat értéke attól függ, hogy a T halmaz elemei között hány negatív elem szerepel (ν értéke), a következőt kapjuk:

$$\left(\frac{a}{p}\right) = (-1)^{\nu},$$

amit bizonyítani akartunk. ■

A Gauss-lemma segítségével könnyen bizonyíthatjuk a kvadratikus reciprocitási tétel kiegészítő lemmáját (5.4).

Bizonyítás: $a = 2$ paraméterre alkalmazzuk az előbbi lemmát. Megnézzük, hogy az

$$S = \{2, 4, 6, \ldots, p-1\}$$

számok közül hány darab negatív előjelű legkisebb abszolút értékű maradék van modulo p. Összesen $\frac{p-1}{2}$ számról van szó, s ezek közül a pozitív előjelű számok száma $\left\lfloor \frac{p-1}{4} \right\rfloor$. Vagyis a negatív előjelűek száma

$$\nu = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$$

$p = 8k+1$ esetén $\nu = 2k$, tehát $\left(\frac{2}{p}\right) = 1$.

Ha $p = 8k+3$, akkor $\nu = 2k+1$, így $\left(\frac{2}{p}\right) = -1$.

$p = 8k-1$ esetén $\nu = 2k$, tehát $\left(\frac{2}{p}\right) = 1$.

Ha $p = 8k-3$, akkor $\nu = 2k-1$, így $\left(\frac{2}{p}\right) = -1$. ■

Ezt az eredményt egyszerűbben összefoglalva:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv \pm 1 \pmod 8 \\ -1, & \text{ha } p \equiv \pm 3 \pmod 8 . \end{cases} \tag{5.5}$$

Könnyen ellenőrizható, hogy (5.4) és (5.5) ekvivalensek egymással.

Most már elegendő ismeretünk van ahhoz, hogy bizonyítsuk a 5.2.5 Tételt.

Bizonyítás: A bizonyítás során r_1, r_2, …, r_μ jelöli a legkisebb abszolút értékű maradékok közül a pozitívakat, s_1, s_2, …, s_ν pedig a negatívakat. A ta számok

jelölik a Gauss-lemma igazolásánál használt S halmaz elemeit, így

$$ta \equiv \begin{cases} r_i \\ p - s_j \end{cases} \pmod{p}\,.$$

Két állítást bizonyítunk:

(A) $(a,p)=1$, továbbá a páratlan, akkor

$$\left(\frac{a}{p}\right) = (-1)^k, \qquad \text{ahol} \qquad k = \sum_{t=1}^{\frac{p-1}{2}} \left\lfloor \frac{ta}{p} \right\rfloor . \tag{5.6}$$

(B) Ha b és c páratlan, 1-nél nagyobb, relatív prím számok, akkor

$$\sum_{\omega=1}^{\frac{c-1}{2}} \left\lfloor \frac{\omega b}{c} \right\rfloor + \sum_{\tau=1}^{\frac{b-1}{2}} \left\lfloor \frac{\tau c}{b} \right\rfloor = \frac{b-1}{2} \cdot \frac{c-1}{2}\,. \tag{5.7}$$

Ezekből a kvadratikus reciprocitás képlete már könnyen következik, ha b és c paramétereknek p és q prímszámokat választjuk, vagyis

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^l, \qquad \text{ahol} \qquad l = \sum_{\omega=1}^{\frac{p-1}{2}} \left\lfloor \frac{\omega q}{p} \right\rfloor + \sum_{\tau=1}^{\frac{q-1}{2}} \left\lfloor \frac{\tau p}{q} \right\rfloor$$

ami a (B) állítás szerint

$$l = \frac{p-1}{2} \cdot \frac{q-1}{2}\,.$$

(A) bizonyításánál, a Gauss-lemmára támaszkodva, elég megmutatnunk, hogy

$$k = \sum_{t=1}^{\frac{p-1}{2}} \left\lfloor \frac{ta}{p} \right\rfloor \equiv \nu \pmod{2}\,. \tag{5.8}$$

Tekintsük a ta számok p-vel történő maradékos osztását. Ekkor

$$ta = \left\lfloor \frac{ta}{p} \right\rfloor p + \begin{cases} \text{vagy} & r_i \\ \text{vagy} & p - s_j\,. \end{cases} \tag{5.9}$$

A (5.9) egyenlőséget összegezve $t = 1, 2, \ldots, \frac{p-1}{2}$-re

$$\left(1 + 2 + 3 + \cdots + \frac{p-1}{2}\right) a = p \sum_{t=1}^{(p-1)/2} \left\lfloor \frac{ta}{p} \right\rfloor + \sum_{i=1}^{\mu} r_i + \sum_{j=1}^{\nu} (p - s_j) \,.$$

A fenti egyenletet átalakítjuk a következőképpen: mindkét oldalhoz hozzáadunk $2\sum s_j$-t. Ekkor a bal oldal bővülni fog a kétszeres szummával, a jobb oldalon pedig $\sum_{j=1}^{\nu}(p - s_j)$-ből $\sum_{j=1}^{\nu}(p + s_j)$ lesz. Mint a Gauss-lemma bizonyításánál beláttuk, az r_1, r_2, …, r_μ, s_1, s_2, …, s_ν számok az $1, 2, \ldots, \frac{p-1}{2}$ számok egy permutációját alkotják, vagyis

$$\sum r_i + \sum s_j = 1 + 2 + \cdots + \frac{p-1}{2} \,.$$

Mindkét oldalból kivonva egy ilyen összeget, a következő összefüggést kapjuk:

$$\left(1 + 2 + 3 + \cdots + \frac{p-1}{2}\right)(a-1) + 2\sum_{j=1}^{\nu} s_j = p\left(\sum_{t=1}^{(p-1)/2} \left\lfloor \frac{ta}{p} \right\rfloor + \nu\right) . \qquad (5.10)$$

Mivel feltettük, hogy a páratlan, így az egyenlőség bal oldala páros szám, továbbá p páratlan prím volta miatt (5.8) valóban teljesül.

(B) belátásához tekintsük a következő csúcsok által meghatározott téglalapot:

$$A = (0,0), \qquad B = \left(\frac{b}{2}, 0\right), \qquad C = \left(\frac{b}{2}, \frac{c}{2}\right), \quad \text{és} \quad D = \left(0, \frac{c}{2}\right)$$

Megmutatjuk, hogy (5.7) mindkét oldalán a fenti csúcsok által meghatározott téglalap egész koordinátájú rácspontjainak száma áll. (5.7) jobb oldalára ez nyilván igaz. Vizsgáljuk meg a bal oldalt.

A téglalapot két részre osztva, az A és C csúcsokat összekötő, $y = \frac{c}{b}x$ egyenletű átlóval, külön megszámoljuk a két háromszögbe eső rácspontokat. Mivel b és c számok relatív prímek, így az átlóra nem esik rácspont. Az alsó háromszögbe eső pontok számát n-nel jelöljük. Nézzük meg, hogy ebben a háromszögben hány rácspont helyezkedik el az $x = \tau$ egyenes mentén. A rácspontok y koordinátáira az $1 \le y < \frac{c}{b}\tau$ egyenlőtlenségnek kell teljesülnie. Az ilyen y koordináták száma

$\left\lfloor \frac{\tau c}{b} \right\rfloor$. Ezen érték $\tau = 1, 2, \ldots, \frac{b-1}{2}$ összegzésére megkapjuk az ABC háromszögbe eső pontok számát. Tehát

$$n = \sum_{\tau=1}^{\frac{b-1}{2}} \left\lfloor \frac{\tau c}{b} \right\rfloor .$$

Hasonlóképpen járunk el az ACD háromszöget illetően. Az $y = \omega$ egyenes mentén számoljuk a felső háromszög rácspontjai, melynek számát jelöljük m-mel. Ezen pontok x koordinátáira $1 \leq x < \frac{b}{c}\omega$ egyenlőtlenség teljesül. Az ilyen x-ek száma $\left\lfloor \frac{\omega b}{c} \right\rfloor$. Összegezve ezt $\omega = 1, 2, \ldots, \frac{c-1}{2}$-re megkapjuk a felső háromszögbe eső rácspontok számát. Tehát a téglalap rácspontjainak száma

$$n + m = \sum_{\tau=1}^{\frac{b-1}{2}} \left\lfloor \frac{\tau c}{b} \right\rfloor + \sum_{\omega=1}^{\frac{c-1}{2}} \left\lfloor \frac{\omega b}{c} \right\rfloor ,$$

ami a (5.7)-es bal oldala. Ezzel a (B) állítást beláttuk, és a 5.2.5 Tételt bebizonyítottuk. ■

5.4. Kvadratikus reciprocitás Gauss-összegekkel történő bizonyítása

A Gauss-összegek alkalmazásával sokkal algebraibb bizonyítást adunk a 5.2.5 Tételre.

A 17-szög szerkeszthetőségéről szóló szakaszban megismerkedtünk az *egységgyökök* fogalmával. A továbbiakban szükségünk van a *primitív egységgyök* definíciójára. A korábban alkalmazott jelölésekkel:

5.4.1. Definíció. Az ϵ egységgyök *primitív n-dik egységgyök,* ha n a legkisebb pozitív egész, amelyre $\epsilon^n = 1$.

5.4.2. Definíció. Legyen p páratlan prímszám. Ekkor az a egész számhoz tartozó *Gauss-összeg*

$$g_a = \sum_{n=0}^{p-1} \left(\frac{n}{p} \right) \epsilon^{an} , \tag{5.11}$$

ahol $\epsilon = \epsilon_p = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)$ *p-edik primitív egységgyök.*

Példa: A g_2 összeg $p = 5$-re a következő

$$\begin{aligned} g_2 &= \left(\frac{0}{5}\right) + \left(\frac{1}{5}\right)\epsilon^2 + \left(\frac{2}{5}\right)\epsilon^4 + \left(\frac{3}{5}\right)\epsilon + \left(\frac{4}{5}\right)\epsilon^3 \\ &= \epsilon^2 - \epsilon^4 - \epsilon + \epsilon^3 \,. \end{aligned}$$

Az előző fejezetben, az 5-szög szerkeszthetőségénél már kiszámoltuk ezen összeg tagjait. Ezt a (4.4) és (4.5) egyenletek mutatják. Ez a példa sugallja a következő tételt:

5.4.3. Tétel. Bármely a pozitív, egész számra, mely nem osztható p-vel

$$g_a^2 = (-1)^{(p-1)/2} p \,. \tag{5.12}$$

Ennek bizonyításához bevezetünk néhány lemmát.

5.4.4. Lemma. Bármely a egész számra

$$\sum_{n=0}^{p-1} \epsilon^{an} = \begin{cases} p & \text{ha } a \equiv 0 \pmod{p} \\ 0 & \text{egyébként} \,. \end{cases}$$

Bizonyítás: Ha $a \equiv 0 \pmod{p}$, akkor az összeg minden tagja 1-gyel egyenlő, így az összeg egyenlő p-vel. Egyébként pedig felhasználva az előző fejezetben megismert azonosságot, $x^p - 1 = (x-1)(x^{p-1} + \ldots + x + 1)$, x helyére $x = \epsilon^a$ helyettesítéssel,

$$\sum_{n=0}^{p-1} \epsilon^{an} = \frac{\epsilon^{ap} - 1}{\epsilon^a - 1} = \frac{1-1}{\epsilon^a - 1} = 0$$

amit állítottunk. ■

5.4.5. Lemma. Ha x és y tetszőleges egész számok, akkor

$$\sum_{n=0}^{p-1} \epsilon^{(x-y)n} = \begin{cases} p & \text{ha } x \equiv y \pmod{p} \\ 0 & \text{egyébként} \,. \end{cases}$$

Bizonyítás: Ennek bizonyítása a 5.4.4 lemmából következik az $a = x - y$ behelyettesítéssel. ■

5.4.6. Lemma. $g_0 = 0$

Bizonyítás: A definícióból tudjuk, hogy

$$g_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) .$$

A 5.2.2 Tétel 3. állításából tudjuk, hogy a kvadratikus maradékok és a kvadratikus nemmaradékok száma egyenlő, továbbá $\left(\frac{0}{p}\right) = 0$. Így az összeg valóban nullával egyenlő. ■

5.4.7. Lemma. Bármely a egész számra

$$g_a = \left(\frac{a}{p}\right) g_1 .$$

Bizonyítás: Ha $a \equiv 0 \pmod{p}$ akkor a 5.4.6 Lemma eredményét kapjuk, tehát tegyük fel, hogy $a \not\equiv 0 \pmod{p}$. Ekkor felhasználva a Legendre-szimbólum multiplikativitását, valamint, hogy az an $(n = 0, 1, \ldots, p-1)$ számok teljes maradékrendszert alkotnak modulo p, így

$$\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \epsilon^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \epsilon^{an} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \epsilon^{m} = g_1 .$$

Mindkét oldalt beszorozva $\left(\frac{a}{p}\right)$-vel és felhasználva, hogy $\left(\frac{a}{p}\right)^2 = 1$, megkapjuk a lemma állítását. ■

Elegendő lemmánk van a 5.4.3 Tétel bizonyítására.

Bizonyítás: A bizonyíás során kétféle módon számoljuk ki a $\sum_{a=0}^{p-1} g_a g_{-a}$ összeget. Felhasználva a 5.4.7 lemmát, továbbá feltéve, hogy $a \not\equiv 0 \pmod{p}$,

$$g_a g_{-a} = \left(\frac{a}{p}\right) g_1 \left(\frac{-a}{p}\right) g_1 = \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right)^2 g_1^2 = (-1)^{\frac{p-1}{2}} g_1^2 .$$

Mindkét oldalt $a = 0$-tól $(p-1)$-ig összegezve

$$\sum_{a=0}^{p-1} g_a g_{-a} = (p-1)(-1)^{\frac{p-1}{2}} g_1^2 \,. \tag{5.13}$$

Másrészt a definícióból kiindulva

$$\begin{aligned} g_a g_{-a} &= \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \epsilon^{an} \cdot \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \epsilon^{-am} \\ &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \epsilon^{an} \epsilon^{-am} \\ &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \epsilon^{a(n-m)} \,. \end{aligned}$$

Az egyenlőség mindkét oldalát összegezve az előzőhöz hasonló módon

$$\begin{aligned} \sum_{a=0}^{p-1} g_a g_{-a} &= \sum_{a=0}^{p-1} \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \epsilon^{a(n-m)} \\ &= \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \sum_{a=0}^{p-1} \epsilon^{a(n-m)} \,. \end{aligned}$$

A fenti egyenlőségre alkalmazva a 5.4.5 lemmát, ahol

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \sum_{a=0}^{p-1} \epsilon^{a(n-m)}$$

Ebben az összegben csak $n = m$ esetén kapunk 0-tól különböző tagot, ezért elég erre az esetre elvégezni az összegzést és így az összeg értéke:

$$\sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^2 p = p(p-1) \,.$$

Összevetve ezt és a (5.13) egyenletet

$$(p-1)(-1)^{\frac{p-1}{2}} g_1^2 = p(p-1) \,,$$

majd $(p-1)$-gyel egyszerűsítve, és átrendezve

$$g_1^2 = (-1)^{\frac{p-1}{2}} p\,.$$

Mivel $a \not\equiv 0 \pmod{p}$, továbbá $\left(\frac{a}{p}\right)^2 = 1$, a 5.4.7 lemma értelmében

$$g_a^2 = \left(\frac{a}{p}\right)^2 g_1^2 = g_1^2\,.$$

Tehát

$$g_a^2 = (-1)^{\frac{p-1}{2}} p\,.$$

A 5.4.3 tételt ezzel bebizonyítottuk. ■

Elegendő ismeretünk van ahhoz, hogy a kvadratikus reciprocitás tételét bebizonyítsuk a Gauss-összegek segítségével.

Bizonyítás: Legyen q páratlan prím és $q \neq p$. Legyen $p^* = (-1)^{(p-1)/2} p$. A 5.4.3 Tétel jelölésének megfelelően $p^* = g^2$ ahol $g = g_1 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \epsilon^n$. Alkalmazva a (5.2) összefüggést

$$(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod{q}\,.$$

Felhasználva, hogy $g^{q-1} = (g^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}}$, majd behelyettesítve a fenti kongruenciába és g-vel szorozva mindkét oldalt

$$g^q \equiv g \left(\frac{p^*}{q}\right) \pmod{q} \tag{5.14}$$

adódik.

Ez a kongrencia azt jelenti, hogy a $g^q - g\left(\frac{p^*}{q}\right)$ különbség a (q) ideálnak az eleme, a $\mathbb{Z}[\epsilon]$ gyűrűben. Ennek a gyűrűnek az elemei ϵ egész együtthatós „polinomjai". A $\mathbb{Z}[\epsilon]/(q)$ gyűrű karakterisztikája q, tehát ha $x, y \in \mathbb{Z}[\epsilon]$, akkor $(x+y)^q \equiv x^q + y^q \pmod{q}$. Alkalmazzuk ezt a fenti (5.14) egyenletre

$$g^q = \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \epsilon^n\right)^q \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^q \epsilon^{nq} \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \epsilon^{nq} \equiv g_q \pmod{q}\,.$$

A 5.4.7 lemmából

$$g^q \equiv g_q \equiv \left(\frac{q}{p}\right) p \pmod{q},$$

kombinálva ezt a (5.14)-gyel

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q}.$$

Mivel $g^2 = p^* = \pm p$, továbbá $p \neq q$, vagyis g és q relatív prímek $\mathbb{Z}[\epsilon]/(q)$-ban, g-t törölhetjük mindkét oldalról. Lásd későbbi megjegyzést. Ekkor $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right)$ (mod q). Mindkét szimbólum értéke ± 1, a különbségük így legfeljebb 2, továbbá q páratlan volta miatt $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$ Az Euler-kritériumot felhasználva

$$\begin{aligned}\left(\frac{p^*}{q}\right) &= \left(\frac{(-1)^{(p-1)/2}p}{q}\right) \\ &= \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) \\ &= (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)\end{aligned}$$

A kvadratikus reciprocitás tételét ezzel bebizonyítottuk. ■

Megjegyzés: A g-vel történő osztás korántsem olyan triviális, mint először gondolnánk. $g \in \mathbb{Z}[\epsilon]$. Ilyen gyűrűben sajnos általában nem érvényes a számelmélet alaptétele. Vizsgáljuk meg közelebbről!

Tudjuk, hogy $g^2 = \pm p$, továbbá $(p, q) = 1$ $\mathbb{Z}$-ben. Azt állítjuk, hogy $(g, p) = 1$ $\mathbb{Z}[\epsilon]$-ban, és $\exists u, v \in \mathbb{Z}[\epsilon]$, amelyre

$$ug + vp = 1.$$

Hasonlóképpen nézzük p, q-ra. Ezek relatív prímek $\mathbb{Z}$-ben. Ekkor létezik $a, b \in \mathbb{Z}$,

amelyre

$$\begin{aligned} ap + bq &= 1 \\ a(\pm g^2) + bq &= 1 \\ \underbrace{(\pm ag)}_{u \notin \mathbb{Z}} g + \underbrace{b}_{v} q &= 1\,. \end{aligned}$$

Ekkor $\mathbb{Z}[\epsilon]$-ban minden c-re igaz, hogy cg és cq-nak is van kitüntetett közös osztója és c-vel egyenlő, ugyanis

$$u(cg) + v(cq) = c(ug + vq) = c\,.$$

Vagyis, ha

$$\alpha \in \mathbb{Z}[\epsilon] \mid cg, cq \Longrightarrow \alpha | c\,,$$

továbbá

$$c \mid cg, cq\,.$$

Így tehát, ha $Ag \equiv Bg \pmod{q}$, vagyis $q \mid (A-B)g = cg$, akkor

$$q \mid (cg, cq) = c = A - B \Longrightarrow A \equiv B \pmod{q}\,,$$

tehát leoszthatunk g-vel.

Most nézzük meg egy feladaton keresztül, hogyan használhatjuk a kvadratikus reciprocitás tételét és a Legendre-szimbólum tulajdonságait.

Feladat: Megoldható-e az $x^2 \equiv 66 \pmod{191}$ kongruencia? (A 191 prímszám.)

A 66 kanonikus alakja $66 = 2 \cdot 3 \cdot 11$ így

$$\left(\frac{66}{191}\right) = \left(\frac{2}{191}\right)\left(\frac{3}{191}\right)\left(\frac{11}{191}\right)$$

A kvadratikus reciprocitás kiegészítő-lemmája alapján, mivel $191 \equiv -1 \pmod{8}$, így

$$\left(\frac{2}{191}\right) = 1\,.$$

A 5.2.5 Tételt alkalmazva, majd a Legendre szimbólum tulajdonságait és a kiegészítő lemmát felhasználva

$$\left(\frac{3}{191}\right) = -\left(\frac{191}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

Hasonlóképpen járunk el $\left(\frac{11}{191}\right)$-gyel.

$$\left(\frac{11}{191}\right) = -\left(\frac{191}{11}\right) = -\left(\frac{4}{11}\right) = -\left(\frac{2}{11}\right)^2 = -1$$

Tehát

$$\left(\frac{66}{191}\right) = 1 \cdot 1 \cdot (-1) = -1,$$

vagyis a 66 kvadratikus nemmaradék modulo 191, így a kongruencia nem oldható meg.

6. Összefoglalás

Szakdolgozatom célja az volt, hogy szélesebb képet alkothassak a XIX. század legnagyobb matematikusáról, s bepillantást nyerhessünk matematikai elgondolásaiba.

A harmadik fejezetben bemutattam, hogyan alkalmazzuk az általa kifejlesztett kiküszöbölési eljárást, s bepillantást nyertünk a Gauss-egészekbe. Példát mutattam rá, hogy alkalmazhatjuk e számok gyűrűjét diofantikus egyenletek megoldásában.

A negyedik fejezetben megmutattam, hogyan oldotta fel azt a 2000 éves problémát, (minössze 18 évesen) mellyel sok neves matematikus elődje próbálkozott. Sőt bizonyítását sikerült általánosítania további prímoldalú sokszegekre.

Az ötödik fejezetben ismertettem a kvadratikus maradékok és a kvadratikus reciprocitási tétel elméletét. Ezen elméletet többek között a kódelméletben és a kriptográfiában széleskörben alkalmazzák.

Táblázatok jegyzéke

1. $k = ind_{3,17}(m)$ értékei 19

Hivatkozások

[1] M. B. W. Tent, *The Prince of Mathematics: Carl Friedrich Gauss*, A K Peters, Ltd, 2006.

[2] Stoyan Gisbert - Takó Galina, *Numerikus módszerek I.*, Typotex kiadó, 2002

[3] Czédli Gábor - Szendrei Ágnes, *Geometriai szerkeszthetőség*, Polygon kiadó, 1997

[4] Szemjon Grigorjevics Gingyikin, *Történetek fizikusokról és matematikusokról*, Második kiadás, Typotex kiadó, 2004

[5] William Stein, *Elementary Number Theory*, Springer , 2008

[6] Freud Róbert - Gyarmati Edit, *Számelmélet*, Nemzeti Tankönyvkiadó, 2006

[7] Franz Lemmermeyer, *Numbers and Curves*, Springer, 2001

[8] Franz Lemmermeyer, *Reciprocity Laws: From Eulet to Einstein*, Springer, 2000

Köszönet

Hálás köszönettel tartozom témavezetőmnek, Károlyi Gyulának, aki időt és energiát nem sajnálva segítette ezen dolgozat létrejöttét. Hasznos tanácsai a szakdolgozat emészthetőségét segítették elő.