1. rész

Gauss egyik legnevezetesebb tétele a szabályos sokszög megszerkeszthetőségére mond ki szükséges és elégséges feltételt. Ez a tétel, amelyet a nagy német matematikus 1796 márciusában fedezett fel, a következőképpen szól: a kör kerületét pontosan akkor lehet körzővel és vonalzóval n egyenlő részre osztani, ha az n prímtényezős felbontásában 2-hatványon és egymástól különböző Fermat-prímszámok első hatványán kívül más nem fordul elő.[2] A feltételből már gondolhatjuk, hogy itt legfeljebb látszólag van szó geometriai problémáról. Valóban, a geometriai szerkeszthetőséggel kapcsolatos kérdések eddig mindig algebrai eszközök segítségével tisztázódtak. Ez nem meglepő, hiszen a feladat általában az, hogy egy szakaszból annak valahányszorosát (x) akarjuk megszerkeszteni, ennek megoldhatósága pedig láthatóan azon múlik, hogy a kérdéses x arányszám kifejezhető-e racionális számokkal, a valós számok közti négy alapművelettel és véges sok négyzetgyökvonással.

Amint ez a címből sejthető, ebben a cikkben a szabályos n-szög megszerkeszthetőségére adott feltétel elégségességét fogom bizonyítani, viszonylag elemi számelméleti eszközök felhasználásával. A bizonyítás itt is abból áll, hogy egy arányszám a fenti alakban előállítható. Mielőtt a bizonyításhoz hozzáfognánk, sok mindennel meg kell ismerkednünk. Először a szükséges számelméleti és algebrai alapfogalmakat vezetjük be, majd foglalkozunk a számelmélet egy igen nevezetes tételével, amelynek első bizonyítását szintén Gauss adta, épp egy-két héttel a „sokszög szerkeszthetőségi" tétel bizonyítása után. Ezt az ún. négyzetes (kvadratikus) reciprocitási tételt azután tudjuk kimondani, miután a számelméleti segédeszközöket már ismertettük.

Kezdjük el tehát a szükséges alapfogalmak bevezetését. Fermat-számoknak a $2^{2^k}+1$ alakú egészeket nevezzük, ezek közül a törzsszámokat Fermat-prímeknek mondjuk. Az elnevezést indokolja, hogy Fermat[3], meggyőződve arról, hogy az említett alakú számok közül a $k=0,1,2,3,4$ kitevőkhöz tartozóak (vagyis a $3,5,17,257,65537$) mind prímek, megfogalmazta azt a sejtését, hogy a $(2^{2^k}+1)$ $k=0,1,2,\ldots$ sorozat minden eleme prím. Ezt elsőként Euler cáfolta meg, igazolva azt,[4] hogy $641|2^{32}+1$. Ma sem ismeretes, hogy létezik-e végtelen sok Fermat-prím, és az sem, hogy van-e végtelen sok nem prím a Fermat-számok között. Sőt, az említett öt prímszámon kívül jelenleg egyetlen egy Fermat-prímről sem tudunk.

A $2^{2^k}+1$ Fermat-számot F_k-val szokás jelölni, tehát $F_0=3$, $F_1=5$, stb. E jelölés segítségével egyszerű megfogalmazni azt, amit majd bizonyítani akarunk:

1. Tétel. *Ha az n prímhatványtényezős előállítása $n=2^\alpha\cdot\prod_{k=1}^{\gamma}F_{i_k}$, akkor a kör kerületének n egyenlő részre való felosztása körzővel és vonalzóval megoldható.*

Legyen m egy adott pozitív egész. Az $[a]=\{a+km \mid k\in\mathbf{Z}\}$ halmazt az *a elem által reprezentált* mod m *maradékosztálynak* nevezzük. Ha $a\equiv b \bmod m$, akkor $(a,m)=(b,m)$ s ezért értelmes a következő definíció: az $[a]$ ún. *redukált maradékosztály,* ha $(a,m)=1$. Itt hívjuk fel a figyelmet, hogy ezentúl $a\equiv b \bmod m$ helyett általában a rövidebb $a\equiv b\ (m)$ jelölést használjuk. A most következő fogalomnak a későbbiekben alapvető szerepe lesz. Mod m *redukált maradékrendszernek* nevezzük egész számoknak olyan halmazát, amelyet úgy kapunk, hogy minden redukált maradékosztályból pontosan egy elemet választunk. A „redukált maradékrendszert" ezentúl RMR-rel rövidítjük. Mod m RMR-t alkotnak például az $[1,m]$ intervallumba eső, m-hez relatív prímek is. Itt vezetjük be az Euler-féle φ függvényt, amely az elemi számelméletben alapvető szerepet játszik. Euler-féle φ függvénynek nevezzük azt a függvényt, amelyre $\varphi(m)$ egyenlő a mod m redukált maradékosztályok számával. Természetesen $\varphi(m)$ megadható úgy is, mint a mod m RMR-ek elemszáma, vagy mint az $[1,m]$-be eső m-hez relatív prímek száma.

Könnyen látható, hogy $\{t_1,t_2,\ldots,t_k\}$ pontosan akkor RMR mod m, ha egyszerre teljesül az alábbi három követelmény. (A továbbiakban egy számhalmaz ilyen, felsorolásszerűen történő megadásakor a kapcsos zárójelet elhagyjuk.)

a) Ha $1\le i\le k$, akkor $(t_i,m)=1$
b) $i\not\equiv j$ esetén $t_i\not\equiv t_j(m)$
c) $k=\varphi(m)$

---

[1] Fermat-prím a gyűjtőneve a $2^{2^k}+1$ alakú prímeknek.

[2] E tétel megfogalmazása a későbbiekben bevezetésre kerülő Euler-féle φ függvény segítségével lényegesen egyszerűbbé válik, ugyanis a fenti feltétel azzal ekvivalens, hogy $\varphi(n)$ 2-hatvány. Ez a $\varphi(n)$ explicit alakjának (lásd [5] alatt) felhasználásával könnyen belátható. Mi azonban a bizonyítás során nem ebből, hanem a fenti megfogalmazásból fogunk kiindulni.

[3] Pierre Fermat (1601. aug. 20.–1665. jan. 12.). Francia matematikus és fizikus. Elsősorban számelmélettel, geometriával és analízissel foglalkozott.

[4] Bizonyára sokan tudják, hogy $a\equiv b \bmod m$ és $c\equiv d \bmod m$ esetén $a+c\equiv b+d \bmod m$ és $ac\equiv bd \bmod m$. (Ez azonnal látható, ha a kongruenciákat átírjuk a megfelelő oszthatósági formulákba.) A kongruenciáknak ezt a tulajdonságát lépten-nyomon fel fogjuk használni.

Leonhard Euler (1707. ápr. 15.–1783. szept. 18.), a világon az egyik legtermékenyebb matematikus ötletességére jellemző a következő gondolatmenet. Vegyük észre, hogy $641=2^4+5^4=5\cdot 2^7+1$. Ebből $5\cdot 2^7=-1 \bmod 641$, így tehát $5^4\cdot 2^{28}\equiv 1 \bmod 641$. Ugyanakkor $5^4\equiv -2^4 \bmod 641$, ahonnan $2^{32}\equiv -1 \bmod 641$ következik, amit látni akartunk. (Persze azért Euler sem azt csinálta, hogy ránézett a $2^{32}+1$-re és rávágta, hogy osztható 641-gyel. Rendre megnézte a $64k+1$ alakú prímeket, hogy melyik osztja $2^{32}+1$-et, és amikor a 641 sorra került, akkor jöhetett ez az ötlete. Egy későbbi feladat: Miért csak a $64k+1$ alakú prímeket kellett néznie?)

Ennek segítségével azonnal ellenőrizhető, hogy ha $t_1, \dots, t_{\varphi(m)}$ RMR, és $(a,m)=1$, akkor $at_1, \dots, at_{\varphi(m)}$ is RMR mod m. Erre az észrevételre a későbbiekben *„Euler–Fermat-ötlet"* néven fogunk utalni. Rögtön kiderül, mi indokolja ezt az elnevezést. Ennek felhasználásával igazolható ugyanis legegyszerűbben az alábbi, *Euler–Fermat-tétel* néven ismeretes állítás: Ha $(a,m)=1$, akkor $a^{\varphi(m)} \equiv 1\ (m)$. Valóban, ha $t_1, \dots, t_{\varphi(m)}$ és $at_1, \dots, at_{\varphi(m)}$ mindketten RMR-ek, akkor

$$t_1 \equiv at_{\mu(1)}\ (m) \qquad t_2 \equiv at_{\mu(2)}\ (m) \quad \dots \quad t_{\varphi(m)} \equiv at_{\mu\left(\varphi(m)\right)}\ (m) \tag{1}$$

ahol μ az $1, 2, \dots, \varphi(m)$ egy permutációja. Az (1) kongruenciákat összeszorozva, majd az m-hez relatív prím $\prod_{i=1}^{\phi(m)} t_i$ szorzattal egyszerűsítve adódik a bizonyítandó $a^{\varphi(m)} \equiv 1(m)$. Ezt a tételt felhasználva egy fontos tételt fogunk bevezetni. $(a,m)=1$ esetén legyen k az a legkisebb pozitív egész, amelyre $a^k \equiv 1\ (m)$. Ezt a k kitevőt az a *rendjének nevezzük* mod m és $o_m(a)$-val (vagy, ha nem okoz félreértést $o(a)$-val) jelöljük (olvasd: ordo a). Könnyen látható, hogy $a^n \equiv 1\ (m)$ pontosan akkor teljesül, ha $o(a) \mid n$.

Most pedig — a szokásosnál általánosabban — definiáljuk az indexeket. Rögzítsünk egy m-hez relatív prím g-t és legyen a olyan, hogy $g^k \equiv a\ (m)$ egy alkalmas nemnegatív egész k-ra. Ezt a modulo $o(g)$ egyértelműen meghatározott k-t az *a szám g alapú indexének* nevezzük mod m és ${}^g\mathrm{ind}\, a$-val jelöljük.

Egy újabb alapvető definíció: *g primitív gyök* mod m, ha $o(g) = \varphi(m)$. Ezzel kapcsolatban bebizonyítjuk a következőt.

Lemma. *Minden prímszámhoz létezik primitív gyök.*

Először az alábbiakat látjuk be.

1. Állítás. *Az $f(x) \equiv 0\ (p)$ n-edfokú prímmodulusú kongruenciának legfeljebb n (páronként inkongruens) megoldása van.*

2. Állítás. *Ha valamely m-re n és k olyan, hogy $\big(o_m(n), o_m(k)\big) = 1$, akkor $o_m(n \cdot k) = o_m(n) \cdot o_m(k)$.*

Az 1. Állítás bizonyítása: Teljes indukciót alkalmazunk az $f(x)$ fokszáma szerint. $n=0$-ra az állítás nyilvánvalóan igaz. Tegyük fel, hogy minden $(n-1)$-edfokú kongruenciának maximálisan $n-1$ megoldása lehet, és legyen $\mathrm{gr}\, f(x) = n$, (ahol $\mathrm{gr}\, f(x)$ jelöli $f(x)$ fokszámát). Feltehetjük, hogy $f(x) \equiv 0\ (p)$-nek létezik megoldása, legyen az egyik megoldás x_1. Ekkor $f(x) \equiv 0\ (p)$ pontosan akkor igaz, ha $f(x) - f(x_1) \equiv 0\ (p)$, ámde $f(x) - f(x_1) = \sum_{i=1}^{n} a_i\big(x^i - x_1^i\big) = (x - x_1)g(x)$, ahol $\mathrm{gr}\, g(x) = n-1$. Mivel p prím, ezért ha $x \not\equiv x_1\ (p)$, akkor szükségképpen $g(x) \equiv 0\ (p)$. Ez utóbbinak az indukciós feltétel miatt legfeljebb $n-1$ megoldása van, tehát az $f(x) \equiv 0\ (p)$ megoldásszáma valóban soha nem nagyobb, mint n.

A 2. Állítás bizonyítása: Ha valamely pozitív egész t kitevőre $(nk)^t \equiv 1\ (m)$, akkor $n^{t \cdot o(n)} \cdot k^{t \cdot o(n)} \equiv 1\ (m)$, amiért $k^{t \cdot o(n)} \equiv 1\ (m)$. Ennélfogva $o(k) \mid t \cdot o(n)$, ugyanilyen meggondolás szerint $o(n) \mid t \cdot o(k)$ is igaz. Innen $\big(o(n), o(k)\big) = 1$ miatt $o(n) \cdot o(k) \mid t$, amiből kapjuk, hogy $o(n) \cdot o(k) \mid o(nk)$. Viszont $o(nk) \mid o(n) \cdot o(k)$ is igaz, hiszen $(nk)^{o(n) \cdot o(k)} \equiv 1\ (m)$, amivel beláttuk a 2. Állítást is.

Ezek után igazoljuk a Lemmát. Tekintsük az $o_p(1), \dots, o_p(p-1)$ legkisebb közös többszörösét. Ennek prímfelbontása $u = \prod_{i=1}^{r} q_i^{\alpha_i}$. Mivel u a rendek legkisebb közös többszöröse, ezért minden i-hez van olyan x_i, aminek a rendje $a_i q_i^{\alpha_i}$ alakú. Világos, hogy ekkor $o\big(x_i^{a_i}\big) = q_i^{\alpha_i}$. A 2. Állításból következik, hogy $o\left(\prod_{i=1}^{r} x_i^{a_i}\right) = u$. Ebből a „kis"-Fermat-tétel felhasználásával $u \mid (p-1)$ adódik. Nyilván $x^u \equiv 1\ (p)$ minden $1 \le x \le p-1$ esetén. Innen az 1. Állítást figyelembe véve kapjuk, hogy $u \ge p-1$, így tehát $u = p-1$, vagyis $\prod_{i=1}^{r} x_i^{a_i}$ primitív gyök mod p.

Gyakran lesz szükség a következőre. Könnyű észrevenni, hogy ha g primitív gyök, akkor az $\big\{1, g, g^2, \dots, g^{\varphi(m)-1}\big\}$ éppen egy mod m RMR. Ellenkező esetben ugyanis lenne olyan i és j, amelyre $0 \le i < j \le \varphi(m) - 1$ és $g^i \equiv g^j\ (m)$, ekkor viszont $g^{j-i} \equiv 1\ (m)$ állna fenn, ami g primitív gyök volta miatt lehetetlen.

A továbbiakban kizárólag prímmodulusú kongruenciákat szerepeltetünk, és p-vel – úgy, mint eddig – csak prímszámot fogunk jelölni.

Legyen $p > 2$ és $(a,p) = 1$. Ekkor a „kis"-Fermat-tételből és p prím voltából következik, hogy $a^{\frac{p-1}{2}} \equiv \pm 1\ (p)$; $a^{\frac{p-1}{2}} \equiv 1\ (p)$ esetén a-ról azt mondjuk, hogy *kvadratikus maradék*, ellenkező esetben pedig *a kvadratikus nemmaradék* mod p. Definiáljuk az $\left(\frac{a}{p}\right)$ ún. *Legendre-szimbólumot* tetszőleges a egészre a következőképpen:

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

Nyilván $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$, s ebből minden a és b-re $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ adódik; ezzel kapcsolatos a következő definíció. Az $f\colon \mathbf{Z}\to\mathbf{R}$, ill. $\mathbf{N}\to\mathbf{R}$ függvényt *multiplikatívnak* mondjuk, ha $(a,b)=1$-ből következik, hogy $f(a)\cdot f(b) = f(ab)$, és *teljesen multiplikatívnak*, ha $f(a)\cdot f(b) = f(ab)$ tetszőleges a,b egész számpárra fennáll. Előbbiek szerint tehát az $\left(\frac{a}{p}\right)$ Legendre-szimbólum bármely $p>2$ esetén teljesen multiplikatív.[5] E tulajdonság felhasználásával azonnal belátható, hogy (egy RMR-en belül) a mod p kvadratikus maradékok és nemmaradékok száma megegyezik. Ha ugyanis g primitív gyök mod p, akkor $\left(\frac{g}{p}\right) = -1$, amiből $\left(\frac{g^k}{p}\right) = (-1)^k$, s így állításunk valóban igaz. A teljes multiplikativitás és a most következő – már korábban szóba hozott – tétel teszi lehetővé konkrét esetben a Legendre-szimbólum gyors kiszámolását.

2. Tétel. (Négyzetes reciprocitási tétel.) *Legyenek p és q különböző páratlan prímek. Ekkor* $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Más szóval, ha p és q között van $4k+1$ alakú, akkor p pont akkor kvadratikus maradék mod q, ha q is az mod p; és ha p is és q is $4k-1$ alakú, akkor közülük pontosan az egyik kvadratikus maradéka a másiknak. A prímszámoknak ezt a törvényszerűségét a XVIII. század matematikusai közül már jónéhányan ismerték. Első hiánytalan bizonyítása Gausstól származik, akinek ez a tétel annyira kedvence volt, hogy élete folyamán még további hétféleképpen igazolta. A reciprocitási tételnek ma már kb. 100 bizonyítása ismeretes.

Az 1. Tétel bizonyítása egy olyan tételen – helyesebben szólva annak hátterén – nyugszik, amely a 2. Tétel – egy lehetséges – belátásához is igen jó kiindulásul szolgál. E harmadik tétel felírása előtt azonban bevezetjük a komplex számok és ezen belül a komplex egységgyökök fogalmát. Ezek felhasználásával fogjuk bizonyítani az 1. és a 2. Tételt.

Következik tehát a *komplex számok bevezetése*, amelyet azért nyújtottam olyan hosszúra, mert bizonyára sokan vannak, akik ezeket idáig még nem ismerték. Most a pontos leírás elolvasása után ők is a megfelelő eszközök birtokában tanulmányozhatják a bizonyításokat.

A komplex számok bevezetése

A valós számok összessége az idők folyamán több szempontból is elégtelennek bizonyult. A legnagyobb hiány az volt, hogy a négyzetgyökvonás nem mindig végezhető el a valós számok ($\mathbf{R}$) körében. A XVI. század olasz matematikusai megtalálták a harmadfokú egyenlet megoldóképletét. Alkalmazása azonban gyakran nehézségekbe ütközött. Amikor ugyanis a vizsgált harmadfokú egyenletnek 3 valós gyöke volt, a képlet használatakor negatív számból kellett négyzetgyököt vonni. Ez inspirációt adott arra, hogy a $\sqrt{x}(x<0)$ alakú „értelmetlen kifejezéseket" is tekintsék számoknak, és úgy számoljanak velük, mint ahogy azt addig a valós számokkal tették.

A komplex számok bevezetésének célja lényegében az $\mathbf{R}$-nek egy olyan kibővítése, amelyben (a 0-val való osztást kivéve) elvégezhető a „négy alapművelet", érvényesek a műveleti azonosságok (az összeadás és a szorzás kommutativitása, asszociativitása és a disztributivitás), és van olyan szám, amelynek a négyzete -1.

Nézzük most meg, hogyan lenne célszerű a komplex számokat megkonstruálni. Elsődleges követelmény, hogy legyen olyan i elem, amelyre $i^2=-1$. Könnyen látható, hogy ha ezek között a számok között valóban a megkívánt műveleti azonosságok mellett tudunk összeadni és szorozni, akkor az $a+b\cdot i$ $(a,b\in\mathbf{R})$ alakú számok halmaza zárt lesz a két műveletre nézve. A kivonást és az osztást is nyilván el tudjuk végezni, hiszen $(a+bi)=(a-c)+(b-d)i+c+di$, valamint $a+bi = \left(\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i\right)\cdot(c+di)$, hacsak $c\neq 0$ vagy $d\neq 0$. Mindezek alapján úgy tűnik, elég a komplex számok körébe az $a+bi$ alakú „számokat" bevenni, és ezeken értelmezni a szükséges műveleteket. (Meg fogjuk látni, hogy ez tényleg így van.) A definíciók előtt nézzük még meg, mikor lehet egyenlő két komplex szám a támasztott követelmények teljesülése mellett. Tegyük fel, hogy $a+bi=c+di$. Ha $b\neq d$, akkor $i=\frac{a-c}{d-b}$, ami képtelenség, ugyanis egy valós számnak nem lehet -1 a négyzete. Így csak $b=d$ lehet, amiből egyúttal $a=c$ is következik. Eredményeink alapján megfogalmazzuk a pontos definíciót.

Definíció. *Komplex számoknak* nevezzük azokat a valós számokból álló (a,b) párokat, amelyekre

(i) $(a,b)=(c,d)$ pontosan akkor, ha $a=c$ és $b=d$

(ii) $(a,b)+(c,d)=(a+c,b+d)$ és $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$.

A komplex számok halmazát $\mathbf{C}$-vel jelöljük. Az (ii)-ben megadott két művelet közül az első a komplex számok összeadása, a második pedig a komplex számok szorzása. Felhasználva az $\mathbf{R}$-beli összeadás és szorzás kommutativitását

[5] Nem túl nehéz igazolni az Euler-függvény multiplikativitását sem. 1-től ab-ig $\big((a,b)=1\big)$ felírva a számokat a oszlopban és b sorban úgy, hogy az 1. sorban 1-től a-ig, a 2. sorban $a+1$-től $2a$-ig stb. legyenek, akkor felhasználva azt, hogy egy szám pontosan akkor relatív prím ab-hez, ha a-hoz és b-hez is relatív prím, már könnyen belátható, hogy $\varphi(a)\cdot\varphi(b)=\varphi(ab)$. Mivel $\alpha\geq 1$ esetén $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$, azért ha az n prímtényezős előállítása $\prod_{i=1}^{r} q_i^{\alpha_i}$, akkor $\varphi(n)=\prod_{i=1}^{r} q_i^{\alpha_i-1}(p_i-1)$.

és asszociativitását, valamint a disztributivitást – némi kis számolással – könnyen beláthatók az (ii) alatt definiált műveletekhez tartozó azonosságok is. A következő – szintén lényeges – állítások bizonyítását is az Olvasóra hagyom, ezeket azonban nem nehéz igazolni az $\mathbf{R}$ és a $\mathbf{C}$-beli összeadás és szorzás tulajdonságainak figyelembevételével.

a) Létezik egy és csak egy úgynevezett *nullelem* (jelölje 0), ami olyan (x, y)-t jelent, amelyre tetszőleges (a, b) esetén $(a, b) + (x, y) = (a, b)$. (Ez az (x, y) nyilván a $(0, 0)$ lesz.)

b) Minden komplex számnak létezik pontosan egy *ellentettje,* amin azt a számot értjük, amit az eredeti számhoz hozzáadva 0-t kapunk. Az (a, b) szám ellentettjét $-(a, b)$-vel jelöljük.

Az a) és b) pontok alapján a komplex számok körében elvégezhető a *kivonás,* azaz minden (a, b) és $(c, d) \in \mathbf{C}$-hez van olyan egyértelműen meghatározott $(x, y) \in \mathbf{C}$, amelyre $(c, d) + (x, y) = (a, b)$.

c) Létezik $\mathbf{C}$-nek *egységeleme,* azaz olyan elem, amellyel tetszőleges számot szorozva az eredmény maga az eredeti szám lesz. Az egységelemet a valós esetből megszokott módon itt is 1-gyel jelöljük. Az egységelem $1 = 1 \cdot 1' = 1'$ miatt egyértelmű (feltettük, hogy $1'$ is egységelem), és nyilván az $(1, 0)$ lesz az.

d) Minden 0-tól különböző $(a, b) \in \mathbf{C}$-nek létezik egyértelműen megadott *reciproka* (más szóval *multiplikatív inverze*).

A c) és d) pontokból következik, hogy a komplex számok körében bármely 0-tól különböző számmal lehet osztani is.

Itt érdemes megemlíteni a következő definíciót, amely az algebrában alapvető szerepet játszik. Egy $\mathbf{K}$ halmaz a rajta értelmezett $+$ és $\cdot$ műveletekkel *testet* alkot, ha a fentebb írt műveleti azonosságok teljesülnek, továbbá $+$ és $\cdot$ rendelkezik az előbbi a) és b), illetve c) és d) tulajdonságokkal.

A komplex számtestet az $\mathbf{R}$ egy alkalmas kibővítésének szántuk. Ezt nem sikerült tökéletesen megvalósítani, hiszen $\mathbf{C}$ elemei mind valós számpárok. A konstrukció alapján látszik, hogy $\mathbf{C}$-nek azon elemei, amelyek $(a, 0)$ alakúak, „éppen úgy viselkednek", mint a valós számok. Így hát feleltessük meg minden $(a, 0) \in \mathbf{C}$ számnak az $a \in \mathbf{R}$ számot. Ez a leképzés kölcsönösen egyértelmű (más szóval bijektív), ugyanis (i) szerint $a = b$ pontosan akkor igaz, ha $(a, 0) = (b, 0)$. Megfeleltetésünk művelettartó is, ami azt jelenti, hogy bármely összeg képe egyenlő a tagok képének összegével, és bármely szorzat képe a tényezők képének szorzata. Ezt az $(a, 0) + (b, 0) = (a + b, 0)$ és az $(a, 0) \cdot (b, 0) = (a \cdot b, 0)$ összefüggések igazolják. Mindezek alapján az $(a, 0)$ alakú komplex számokat azonosíthatjuk a valós számokkal, és ennek jegyében $(a, 0)$ helyett ezentúl a-t fogunk írni.

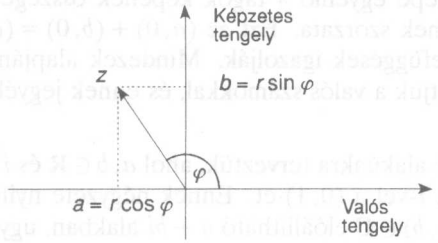
A komplex számokat eredetileg $a + bi$ alakúakra terveztük, ahol $a, b \in \mathbf{R}$ és $i^2 = -1$. Ez lényegében sikerült is. Jelöljük i-vel a $(0, 1)$-et. Ennek négyzete nyilván -1, és ezen i elem segítségével minden $(a, b) \in \mathbf{C}$ előállítható $a + bi$ alakban, ugyanis: $a + bi = (a, 0) + (b, 0) \cdot (0, 1) = (a, b)$. Ennélfogva a továbbiakban – eredeti elképzelésünkhöz hűen – az (a, b) komplex számot $a + bi$ formában tüntetjük fel.

A következőkben jónéhány, a komplex számok alapvető tulajdonságaival kapcsolatos definíció fog sorra kerülni. Kezdjük az egyik leglényegesebbel. A $z = a + bi$ *konjugáltjának* nevezzük az $a - bi$ komplex számot, amelynek jelölése $\overline{z}$. Azonnal látható, hogy az a függvény, amely minden egyes komplex számnak a konjugáltját felelteti meg, bijektív és művelettartó, amellett involutórikus, azaz $\overline{(\overline{z})} = z$. Az $s(z) = z + \overline{z}$ számot a z *nyomának,* az $N(z) = z \cdot \overline{z}$-t pedig a z *normájának* nevezzük. Nyilván, ha $z = a + bi$, akkor $s(z) = 2a$ és $N(z) = a^2 + b^2$, így minden komplex szám nyoma is és normája is valós. Az is látszik, hogy a nyom összegtartó, a norma pedig szorzattartó függvény. Egy komplex szám *abszolút értékének* nevezzük normájának négyzetgyökét. Ez az elnevezés azért lehetséges, mert bármely valós szám ez új értelemben vett abszolút értéke megegyezik „eredeti" abszolút értékével.

A valós számoknál baj volt, hogy nem lehetett minden elemből négyzetgyököt vonni. Kérdés, hogy nem maradt-e meg ez a gond a komplex számok körében is. Az világos, hogy az összes $\mathbf{R}$-beli elemnek van négyzetgyöke $\mathbf{C}$-ben. Megmutatjuk azonban, hogy tetszőleges $z = a + bi$ komplex számhoz mindig van olyan $w = x + iy$, amelyre $w^2 = z$. A feltételezett $(x + yi)^2 = x^2 - y^2 + 2xyi = a + bi$ egyenlőségből adódóan az $x^2 - y^2 = a$; $2xy = b$ egyenletrendszer megoldásait kell meghatározni. Érdemes észrevenni, hogy $a^2 + b^2 = N(z) = \big(N(w)\big)^2 = \big(x^2 + y^2\big)^2$. Ebből ugyanis $x^2 + y^2 = \sqrt{a^2 + b^2}$, innen pedig már rögtön adódik, hogy $x^2 = \dfrac{a + \sqrt{a^2 + b^2}}{2}$ és $y^2 = \dfrac{-a + \sqrt{a^2 + b^2}}{2}$. Mivel $a^2 \le a^2 + b^2$, ezért ilyen x és y létezik is. A $2xy = b$ feltétel miatt x és y csak azonos, illetve csak különböző előjelű lehet, attól függően, hogy b pozitív-e vagy negatív. (Ha $b = 0$, akkor $x^2 = a$ és $y^2 = 0$, illetve $x^2 = 0$ és $y^2 = |a|$, attól függően, hogy a pozitív-e vagy sem.) Számolással ellenőrizhető, hogy a w-re kapott két lehetséges érték közül tényleg mindkettőnek z a négyzete.

A valós esethez hasonlóan itt is célszerű egyértelműsíteni egy szám négyzetgyökét. Ezt a következő definícióval érhetjük el. $\sqrt{a + bi}$ jelölje azt az $x + iy$ komplex számot, amelynek a négyzete $a + bi$, emellett vagy $x > 0$, vagy $x = 0$ és $y \ge 0$. Az így értelmezett négyzetgyökről már valóban látszik, hogy minden komplex számhoz pontosan egy komplex számot rendel.

A komplex számokat mint valós számokból álló (rendezett) párokat definiáltuk. Ennek alapján fölmerül annak a gondolata, hogy $\mathbf{C}$ elemeit valamilyen módon a sík pontjaival, ill. síkvektorokkal azonosítsuk.



Ez legtermészetesebben úgy történhet, hogy felveszünk egy Descartes-féle koordináta-rendszert, és az $a+bi$ számnak megfeleltetjük az (a,b) pontot, illetve azt a vektort, ami a $(0,0)$-ból az (a,b) pontba mutat. Azt a síkot, amin a komplex számokat ábrázoljuk, *Gauss-féle számsíknak* nevezzük. Ezt az indokolja, hogy Gauss vezette be a komplex számok geometriai értelmezését. Neki köszönhető az is, hogy a komplex számok elvesztették a XVI. században kialakult misztikus jellegüket, és használatuk meghonosodott a matematikában.

Annak, hogy $\mathbf{C}$ elemeit a sík vektoraival azonosítsuk, akkor van értelme, ha a vektorok komplex számként való összeadása „ugyanúgy megy", mint az eredeti vektorösszeadás, vagyis ha $\mathbf{C}$ és a síkvektorok közötti, előbb megadott bijekció összegtartó. Ez az összegtartás viszont nagyon könnyen belátható.

A komplex számok geometriai értelmezésének valódi haszna a szorzás (és ebből adódóan a hatványozás, gyökvonás) elvégzésének megkönnyítéséből ered. A Gauss-féle számsík tetszőleges pontját polárkoordinátákkal is megadhatjuk. (r,φ) annak a z komplex számnak felel meg, amihez tartozó síkvektor hossza r, és az 1-et jelentő egységvektort φ szöggel pozitív (az óramutató járásával ellentétes) irányba elforgatva z-vel egyállású vektort kapunk. Ezt a $z \neq 0$ esetén mod 2π egyértelműen meghatározott φ szöget a z szám arkuszának (vagy argumentumának, irányszögének) nevezzük, és $\arc z$-vel jelöljük. A 0 argumentumát nem definiáljuk.

Legyen a $z = a + bi$ számot jelentő vektor hossza továbbra is r, amely nyilván megegyezik z abszolút értékével. Ha $\varphi = \arc z$, akkor a szögfüggvények definíciójából adódik, hogy $a = r \cdot \cos\varphi$ és $b = r \cdot \sin\varphi$, amiből azt kapjuk, hogy $z = r(\cos\varphi + i\sin\varphi)$. A z komplex számnak ezt a formáját a szám *trigonometrikus alakjának* nevezzük. Ez a trigonometrikus alak az, ami a szorzást olyan kényelmessé teszi. Lássuk csak:

$$z_1 \cdot z_2 = r_1 \cdot r_2 \cdot (\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) =$$
$$= r_1 \cdot r_2 \cdot \big(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)\big)$$

a közismert addíciós tétel alapján.

Vagyis két komplex szám szorzatának abszolút értéke megegyezik a két szám abszolút értékének szorzatával (ezt már eddig is tudtuk a norma szorzattartásából), és két nem nulla komplex szám szorzatának arkusza mindig a két arkusz összege. Ez a tétel *Abraham de Moivre* (1667–1754) Londonban élt francia matematikustól származik, aki a valószínűségszámítás megalapozásában alkotott jelentőset. A Moivre-tétellel kitűnően hatványozhatunk is. Teljes indukcióval rögtön látható, hogy minden természetes n-re $z^n = r^n(\cos n\varphi + i\sin n\varphi)$. Az is nyilvánvaló, hogy $\frac{1}{z} = \frac{1}{r}\big(\cos(-\varphi)+i\sin(-\varphi)\big)$, hiszen ezt kell z-vel szorozni ahhoz, hogy 1-et kapjunk. Így az előző, hatványozásra vonatkozó összefüggést a negatív egész n-ekre is megkaptuk.

Hátra van még a gyökvonás. Legyen n pozitív egész, $z \neq 0$, $z = r(\cos\varphi + i\sin\varphi)$. Azt állítjuk, hogy az $x^n = z$ egyenletet pont azok az $x \in \mathbf{C}$ számok elégítik ki, amelyek trigonometrikus alakja $x = \sqrt[n]{r}\left(\cos\left(\frac{\varphi+2k\pi}{n}\right) + i\sin\left(\frac{\varphi+2k\pi}{n}\right)\right)$ valamilyen k egész számmal. Hogy ezek az x-ek tényleg megfelelnek, az magától értetődő az előbb z^n-re adott képlet alapján. Az állítás másik felét pedig bizonyítja a komplex számtestben is – mint minden testben – érvényes fokszámtétel[6], ugyanis az x lehetséges értékeit feltételező iménti formula éppen n különböző számot ad.

A gyökvonással kapcsolatban elérkeztünk a bevezető legvégső részéhez, a komplex egységgyökhöz. Legyen $n \in \mathbf{N}^+$. Az $x^n = 1$ egyenlet megoldásait *n-edik komplex egységgyököknek* nevezzük. A korábbiakból kitűnik, hogy az n-edik egységgyökök az $\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ sorozatnak az elemei, amelyek a 0 középpontú egységkörön helyezkednek el

[6] A fokszámtételt tulajdonképpen már a számelméleti bevezető részben az 1. Állítás címszó alatt bebizonyítottuk, az ott alkalmazott gondolatmenet ugyanis tetszőleges test esetére szóról szóra átvihető. Vegyük észre, hogy az 1. Állítás igazolásakor is lényegében egy testben számoltunk. Tudjuk, bárhogy választunk ki két maradékosztályból egy-egy elemet, azok összege mindig egyazon maradékosztályba esik, és ugyanez igaz a két elem szorzatára is. Ennek alapján a $\mathbf{Z}$-beli műveletek indukálnak egy összeadást és egy szorzást a mod m maradékosztályok között (pl. az $[a]$ és $[b]$ maradékosztályok szorzata nyilván az $[ab]$ maradékosztály lesz). A mod m maradékosztályok a most megadott műveletekkel az ún. mod m maradékosztálygyűrűt alkotják, amelyet $\mathbf{Z}_m$-mel, illetve mod m-mel jelölünk. (A maradékosztálygyűrű helyett az algebrában a faktorgyűrű elnevezést is használják.) A gyűrűk a testektől annyiban különböznek, hogy az előbbieknél nem teszünk fel mást a szorzásról, csak az asszociativitást, valamint az így már megkülönböztetendő bal- és jobboldali disztributivitást. Könnyen belátható, hogy $\mathbf{Z}_m$ pontosan akkor test, ha m prím.

Itt szeretném felhívni a figyelmet egy később előforduló pontatlanságra. Azon például, hogy „írjuk $\mathbf{Z}_q$ elemeit egy g primitív gyök hatványaiként" azt kell érteni, hogy írjuk az $1, 2, \ldots, q-1$ RMR elemeit olyan sorrendben, hogy a k-adik elem g^{k-1}-nel legyen kongruens mod q.

annak a szabályos n-szögnek a csúcsaiban, amelynek egyik csúcsa az 1-et jelentő pont. A kongruenciánál tárgyaltakkal analóg módon, az egységgyökök körében is definiálható a rend és a primitív (n-edik) egységgyök fogalma. *Primitív n-edik egységgyököknek* nevezzük azokat az ε_k n-edik egységgyököket, amelyekre $o(\varepsilon_k) = n$. Ezekkel kapcsolatban három olyan ekvivalens állítást fogalmazunk meg, amelyek megkönnyítik az n-edik egységgyökök kezelését.

1. ε_k primitív n-edik egységgyök,
2. ε_k első n hatványa kiadja az összes n-edik egységgyököt,
3. $(k, n) = 1$.

Könnyen látható, hogy ezek valóban ekvivalensek egymással.