1. Komplex szám rendje

A hatványok periódikusan ismétlődnek.

Tétel
Legyen $0 \neq z \in \mathbb{C}$. Ha z egységgyök, akkor hatványai periódikusan ismétlődnek. Ha z nem egységgyök, akkor bármely két, egész kitevőjű hatványa különböző.

Bizonyítás
Tegyük föl, hogy $z^k = z^\ell$, de $k \neq \ell$. Ekkor $z^{k-\ell} = z^{\ell-k} = 1$. Így:

Definíció
Az n egész szám *jó kitevője* a z komplex számnak, ha $z^n = 1$.

Mivel a $k - \ell$ és $\ell - k$ jó kitevők egyike pozitív, ezért z-nek van pozitív jó kitevője.

A jó kitevők tulajdonságai.

Lemma
Legyen d a z *legkisebb pozitív* jó kitevője. Ekkor a jó kitevők pontosan a d többszörösei.

Bizonyítás
Legyen n jó kitevő. Osszuk el n-et maradékosan d-vel: $n = dq + r$, ahol $0 \leq r < d$. Ekkor $1 = z^n = z^{dq+r} = (z^d)^q z^r = 1^q z^r = z^r$. Tehát r is jó kitevő. A d a *legkisebb pozitív* jó kitevő. Mivel $r < d$, ezért r nem lehet pozitív. Tehát $r = 0$. De akkor $n = dq + r = dq$, azaz n többszöröse d-nek. Megfordítva, ha n többszöröse d-nek, azaz $n = dq$, akkor $z^n = z^{dq} = (z^d)^q = 1^q = 1$, azaz n jó kitevő. □

mert n jó kitevő
a hatványozás azonosságai miatt
$z^d = 1$, mert d jó kitevő

A tétel bizonyításának vége.

Beláttuk:
Legyen d a z *legkisebb pozitív* jó kitevője. Ekkor a jó kitevők pontosan a d többszörösei.

Következmények:
$z^k = z^\ell \iff z^{k-\ell} = 1 \iff d \mid k - \ell$. Ezért $1 = z^0 = z^d, z^1, \ldots, z^{d-1}$ páronként különböző. Ezek z összes hatványai, mert ha n tetszőleges egész, akkor $n = dq + r$, ahol $0 \leq r < d$, és $d \mid n - r$ miatt $z^n = z^r$. (Így z^n csak az n-nek a d-vel való osztási maradékától függ.) Tehát z különböző hatványainak a száma d. Azaz z rendje d, és a hatványok periódikusan ismétlődnek. Ezzel a tételt beláttuk. □

A rend tulajdonságainak összefoglalása.

Összefoglalás
Legyen z nem nulla komplex szám.

- A z *egységgyök*, ha $z^m = 1$ alkalmas $m > 0$ egészre.
- A z pontosan akkor egységgyök, ha hossza 1, szöge 2π-nek racionális többszöröse.
- Ha z nem egységgyök, akkor bármely két egész kitevőjű hatványa különböző. Ilyenkor z rendje ∞.
- Ha z egységgyök, akkor a hatványai periódikusan ismétlődnek. A periódus hossza z *rendje*, jele $o(z)$.
- $z^k = z^\ell \iff o(z) \mid k - \ell$. Így $z^n = 1 \iff o(z) \mid n$.
- A z *jó kitevői* azok az n egészek, melyekre $z^n = 1$.
- A z rendje a legkisebb pozitív jó kitevője. A jó kitevők pontosan a rend többszörösei.

2. Hatvány rendjének képlete

A bolhás feladat.

Egy bolha ugrál körbe egy szabályos n-szög csúcsain úgy, hogy minden ugrásnál k csúcsnyit jut előre. Hány ugrás után jut vissza a kiindulóponthoz? Hány kört tesz meg ezalatt? Hány csúcsot érint összesen?

Legyen $n = 6$, a csúcsokat számozzuk így: 0, 1, 2, 3, 4, 5.

k	bejárás	ugrásszám	körszám	csúcsszám
1	0-1-2-3-4-5-0	6	1	6
2	0-2-4-0	3	1	3
3	0-3-0	2	1	2
4	0-4-2-0	3	2	3
5	0-5-4-3-2-1-0	6	5	6
k		$n/(n,k)$	$k/(n,k)$	$n/(n,k)$

A bolhás feladat megoldása.
Az (n,k) legnagyobb közös osztót jelöl.

A bolha k-asával ugrál: m ugrás után a km-edik csúcson lesz. Ez akkor a kiindulópont, ha $n \mid km$. A legkisebb ilyen m kell.

$$n \mid km \iff \frac{n}{(n,k)} \,\Big|\, \frac{k}{(n,k)} m$$

Mivel $n/(n,k)$ és $k/(n,k)$ relatív prímek, ez akkor igaz, ha:

$$\frac{n}{(n,k)} \,\Big|\, m.$$

A *legkisebb* ilyen m maga az $n/(n,k)$. Így a bolha $n/(n,k)$ ugrást tesz meg, amikor először visszaér. HF: ennyi csúcsot is érint. Ezalatt k-szor ennyi „távolságot” tesz meg, ami $kn/(n,k)$. A kör hossza n, ezért a megtett körök száma a megtett távolság n-edrésze, vagyis $k/(n,k)$.

Hatvány rendjének képlete.

Tétel
Ha z rendje véges és k egész, akkor $o(z^k) = \dfrac{o(z)}{(o(z),k)}$.

Bizonyítás
Legyen z rendje n, írjuk z hatványait egy n-szög csúcsaira. Amikor z^k-t hatványozzuk, akkor k-asával ugrálunk körbe a csúcsokon, a $z^0 = 1$-ből kiindulva. A bolhás feladat miatt először az $n/(n,k)$-adik lépésben kapunk 1-et. Vagyis z^k-nak az $n/(n,k)$-adik hatványa lesz először 1. □

Példa
$o(i) = 4$. Ezért $o(i^3) = \dfrac{4}{(4,3)} = 4$.

A rend meghatározása.

Állítás
Ha $(n,k) = 1$, akkor $\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n)$ rendje n.

Bizonyítás
Láttuk, hogy $\varepsilon_1 = \cos(2\pi/n) + i\sin(2\pi/n)$-nek a k-adik hatványa ε_k, ezért ε_1 hatványai pontosan az n-edik egységgyökök. Így ε_1-nek n darab hatványa van, azaz rendje $o(\varepsilon_1) = n$. A hatvány rendjének képlete miatt $o(\varepsilon_k) = o(\varepsilon_1^k) = n/(n,k)$. Mivel $(n,k) = 1$, ezért $o(\varepsilon_k) = n$.

Megjegyzés
Ha n és k nem relatív prímek, akkor ε_k rendje kisebb, mint n (az n-nek valódi osztója).

Példa a rend meghatározására.

Állítás
Ha $(n,k) = 1$, akkor $\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n)$ rendje n.

Példa
Mennyi lesz $z = \cos 336° + i\sin 336°$ rendje?

Megoldás
$\cos 336^\circ + i \sin 336^\circ$ hossza 1, szöge $336 \cdot 1^\circ$, ami $336/360 \cdot 2\pi$. Mivel $336/360$ racionális szám, z egységgyök. Egyszerűsítve:

$$\frac{336}{360} = \frac{14}{15}.$$

Tehát $z = \cos(14 \cdot 2\pi/15) + i \sin(14 \cdot 2\pi/15)$. Mivel $(14, 15) = 1$, ezért z rendje a fenti állítás miatt 15.

3. Primitív egységgyökök

Primitív n-edik egységgyökök.

Definíció
Az ε szám *primitív n-edik egységgyök*, ha hatványai pontosan az n-edik egységgyökök.

Tétel
Az $\varepsilon \neq 0$ számra az alábbi három állítás ekvivalens.

(1) Az ε primitív n-edik egységgyök.

(2) Az ε rendje n.

(3) $\varepsilon = \cos(2k\pi/n) + i \sin(2k\pi/n)$, ahol $(k, n) = 1$.

Emlékeztető
Ha $(n, k) = 1$, akkor $\varepsilon_k = \cos(2k\pi/n) + i \sin(2k\pi/n)$ rendje n. Ha $(n, k) \neq 1$, akkor ε_k rendje n-nél kisebb. Így (2) $\iff$ (3).

A primitív n-edik egységgyökök jellemzése.

Emlékeztető
Az ε szám *primitív n-edik egységgyök*, ha hatványai pontosan az n-edik egységgyökök.

Bizonyítandó: Az $\varepsilon \neq 0$ számra ekvivalens:

(1) Az ε primitív n-edik egységgyök.

(2) Az ε rendje n.

Bizonyítás
(1) $\implies$ (2) Ha ε hatványai pontosan az n-edik egységgyökök, akkor n darab hatványa van, így rendje n. (2) $\implies$ (1) Ha ε rendje n, akkor n-edik hatványa 1, és ezért n-edik egységgyök. Így minden hatványa is az. Rendje n, tehát n hatványa van. Így minden n-edik egységgyököt megkapunk.

$$\varepsilon^n = 1 \implies (\varepsilon^k)^n = (\varepsilon^n)^k = 1^k = 1.$$

A primitív n-edik egységgyökök száma.

Legyen n pozitív egész. Ekkor a $\varphi(n)$ *Euler-függvény* a $0, 1, \ldots, n-1$ számok közül az n-hez relatív prímek száma.

Számelméleti tétel
Ha n kanonikus alakja $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, ahol $\alpha_i \neq 0$, akkor

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \ldots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

Állítás
A primitív n-edik egységgyökök száma $\varphi(n)$.

Bizonyítás
A primitív n-edik egységgyökök: $\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n)$, ahol $(k, n) = 1$. Láttuk: $\varepsilon_k = \varepsilon_\ell \iff n \mid k - \ell$.

Példák primitív n-edik egységgyökökre.

Példa
A *negyedik* primitív egységgyökök $i^1 = i$ és $i^3 = -i$, mert 1 és 3 relatív prímek 4-hez, de 0 és 2 nem. $\varphi(4) = 2$.

Példa
A *hatodik* primitív egységgyökök

$$\cos(2\pi/6) + i\sin(2\pi/6) = \frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{és}$$
$$\cos(5 \cdot 2\pi/6) + i\sin(5 \cdot 2\pi/6) = \frac{1}{2} - i\frac{\sqrt{3}}{2},$$

mert 1 és 5 relatív prímek 6-hoz, de 0, 2, 3, 4 nem. $\varphi(6) = 2$.

Ezzel elvégeztük a Kiss-jegyzet 1.4. Szakaszát.

4. A binomiális tétel

Binomiális együtthatók.

Ismétlés
Ha van n tárgyunk, akkor ezeket $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$ különböző módon tudjuk sorba rakni. Az itt szereplő $n!$ szám neve: *n faktoriális*. Megállapodás szerint $0! = 1$.

Ismétlés
Ha van n tárgyunk, és ebből k darabot akarunk kiválasztani (a sorrendre való tekintet nélkül), akkor ezt

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!}$$

különböző módon tehetjük meg. Az itt szereplő kifejezés az „n alatt a k” *binomiális együttható*. Megállapodás szerint ennek értéke nulla, ha $k > n$, vagy ha $k < 0$.

A binomiális tétel.

Fejtsük ki az $(a+b)^3$ szorzatot.

Az $(a+b)(a+b)(a+b)$ szorzatot kifejtve egy összeget kapunk. A tagok $u_1 \cdot u_2 \cdot u_3$ szorzatok, ahol $u_1, u_2, u_3 \in \{a, b\}$, az összes lehetséges kombinációban (összesen $2^3 = 8$ tag).
a^3 csak egyféleképpen keletkezhet: ha $u_1 = u_2 = u_3 = a$.
$a^2 b$ úgy keletkezhet, hogy u_1, u_2, u_3 közül kettő a-val egyenlő.
Ezt a kettőt $\binom{3}{2} = 3$-féleképpen választhatjuk ki.
Hasonlóan ab^2-ből is három darab lesz, b^3-ből pedig egy.

A binomiális tétel (Kiss-jegyzet, 2.2.42. Gyakorlat)

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + b^n\,.$$

(Lásd a 2.1.4. és 2.1.10. Gyakorlatokat is.)