

Algebra és számelmélet 4. jegyzet

Farkas Norbert Levente

2019. június 3.

Tartalomjegyzék

| | |
|--|-----------|
| Előszó | 1 |
| 1. Gyűrűk | 2 |
| 1.1. Gyűrű fogalma | 2 |
| 1.2. Gyűrűk számelmélete | 5 |
| 1.3. Gauss-lemmák | 8 |
| 2. Irreducibilitás | 11 |
| 2.1. Prímek, felbonthatatlanok | 11 |
| 2.2. Számelmélet alaptétele | 14 |
| 2.3. Trükkök $\mathbb{Z}[x]$ -ben | 15 |
| 2.4. Karakterisztika | 17 |
| 2.5. Algebrai, transzcendens, minimálpolinom | 20 |
| 3. Test és vektortér | 23 |
| 3.1. Testbővítés | 23 |
| 3.2. Algebrai bővítés | 26 |
| 3.3. Mátrixok és egyenletrendszerek | 28 |
| 4. Szerkesztés | 31 |
| 4.1. Algebrai zártság | 31 |
| 4.2. Euklideszi szerkesztés | 34 |
| 4.3. Törtek | 40 |
| 5. Törtek általánosítása | 41 |
| 5.1. Hányadostest | 41 |

TARTALOMJEGYZÉK

| | |
|--|-----------|
| 5.2. Nevezetes szerkesztési problémák | 46 |
| 6. Primitív gyök | 50 |
| 6.1. Kongruencia emlékek | 50 |
| 6.2. Primitív gyök | 52 |
| 6.3. Binom kongruenciák | 56 |
| 7. Kvadratikus maradékok | 60 |
| 7.1. Két négyzetszám tétel | 60 |
| 7.2. Legendre-szimbólum | 63 |
| 7.3. π féleképpen | 67 |
| 8. Fermat, Wiles, Rivest, Shamir, Adleman | 70 |
| 8.1. Pitagorasz számhármak (emlék) | 70 |
| 8.2. Fermat-sejtés, Wiles-tétel | 70 |
| 8.3. Titkosítás (RSA) | 70 |
| 9. Egészen új egészek | 71 |
| 9.1. Gauss-egészek | 71 |
| 9.2. Gauss-prímek | 75 |
| 9.3. Alkalmazások | 79 |
| 10. Színes becslések | 82 |
| 10.1. Körosztási polinomok | 82 |
| 10.2. Faktoriálisok számelmélete | 84 |
| 10.3. Csebisev-tétel | 89 |
| 11. Számelméleti függvények | 92 |
| 11.1. Hegy- és völgytétel | 92 |
| 11.2. Tökéletes | 93 |
| 11.3. Melyik fákat látom? | 95 |
| Végtelen sok prím | 98 |

| | |
|--|------------|
| 12.1. $\sum_{n=1}^{\infty} \frac{1}{n}$ divergenssel | 98 |
| 12.2. $\sum_{p \text{ prím}} \frac{1}{p}$ divergenssel | 99 |
| 12.3. $4k + 1$ alakúak | 101 |
| 12.4. $8k + 1$ alakúak | 101 |
| 12.5. $8k - 1$ alakúak | 102 |
| 12.6. $8k + 3$ alakúak | 103 |
| 12.7. Mersenne-számokkal: $q \mid 2^p - 1$ | 104 |
| 12.8. Csebisev-tétellel | 105 |
| 12.9. Alsó becslés $\pi(n)$ -re | 105 |
| 12.10. Körosztási polinomokkal: $nk + 1$ alakúak | 107 |
| Mi várható? | 109 |
| Mellékletek | 110 |
| 13.1. Miért a bővítése? | 110 |
| 13.2. Klasszikus bizonyítás | 111 |
| 13.3. Csebisev-tétel vége | 111 |

Előszó

Kedves Olvasó!

Igyekeztem összefoglalni ami 2019 tavaszi félévének Algebra és számelmélet 4. előadásán elhangzott. Ez a dokumentum elég sok mindenből tevődött össze. Nagyrészt az előadáson készült hanganyagra támaszkodtam és saját jegyzeteimre. Nagy hatással vannak a jegyzetre Dr. Freud Róbert: Számelmélet és Dr. Kiss Emil: Bevezetés az algebrába című könyvei, valamint Hermann Péter 2019 tavaszi félévi gyakorlatán elhangzott információk.

Jelölés rendszerét tekintve Dr. Freud Róbert könyveihez hasonlóan én is ♣ szimbólummal jelzem a definíciók és a tételek végét, valamint minden bizonyítást ■ zár.

Sok esetben elég vegyes felvágott lett a jegyzet. Van amit az előadás alapján definiálok, de rá vonatkozó tételeket már a szakirodalom szerint, vagy bár az előadáshoz igazodva, de magam fogalmazom meg. A bizonyítások gyakran tartalmazznak saját ötleteket, gondolatokat, lépéseket, ezért kérnék mindenkit, hogy figyelmesen olvassa a jegyzetet! Igyekeztem nem butaságokat írni, de **a leírt információk helyességét illetően felelősséget nem vállalok!**

Hibák tehát előfordulhatnak a jegyzetben. Ha bárki bármilyen féle gondolati hibát, elírást, egyéb javítási ötletet talál és azt jelzi nekem, nagyon hálás leszek érte és mindenképpen figyelmet fordítok rá. Észrevételt jelezni (például) ebben a google táblázatban lehetséges: [visszajelzés](#).

Már csak az maradt hátra, hogy ezúton is köszönetet mondjak mindazoknak, akik segítettek valamilyen módon a munkámat a félév során. A teljesség igénye nélkül csak néhány fontosabb név: Antal Kamilla, Fábián Terézia, Nagy Zsófia, Ongai Erik, Palánkai Gabriella, Veszely Orsolya.

Köszönöm mindenkinek! Sok sikert a tanuláshoz!

Farkas Norbert Levente

1. előadás

Gyűrűk

1.1. Gyűrű fogalma

1.1.1. Definíció. Legyen adott egy R halmaz¹ és rajta értelmezett egy $(+): R^2 \rightarrow R$ és egy $(\cdot): R^2 \rightarrow R$ műveletek. Azt mondjuk hogy az R halmaz **gyűrű** az adott $+$ és \cdot műveletekre nézve (jel: $(R, +, \cdot)$), amennyiben teljesülnek a gyűrű axiómák:

- Összeadás kommutatív: $\forall a, b \in R: a + b = b + a$
- Összeadás asszociatív: $\forall a, b, c \in R: (a + b) + c = a + (b + c)$
- Létezik nullelem: $\exists 0 \forall a \in R: a + 0 = 0 + a = a$
- Minden elemnek van additív inverze (ellentettje): $\forall a \in R \exists a' \in R: a + a' = a' + a = 0$

Eddig azt mondtuk, hogy a gyűrű az összeadásra nézve egy kommutatív csoport. Mondunk még egy állítást a szorzásról és az összeadás-szorzás kapcsolatáról is:

- Szorzás asszociatív: $\forall a, b, c \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Disztributivitási tulajdonságok: $\forall a, b, c \in R:$
 - Bal oldali: $a \cdot (b + c) = a \cdot b + a \cdot c$
 - Jobb oldali: $(b + c) \cdot a = b \cdot a + c \cdot a$



Megjegyzés. Azért kellett külön bal és jobboldali disztributivitásról beszélnünk, mert a szorzás kommutativitásáról nem esett szó.

1.1.2. Definíció. Ha R gyűrű és $\exists 1 \in R: 1 \cdot a = a \cdot 1 = a$, akkor azt mondjuk, hogy R **egységelemes** gyűrű, az 1 szimbólumot pedig **egységelemnek** nevezzük.



¹Az R jelölés az angol „ring” szóból származik, nem összekeverendő a valós számok halmazával: \mathbb{R}

1.1.3. Definíció. Ha R egységelemes gyűrű és minden (nemnulla) elemnek létezik multiplikatív inverze, vagyis $\forall a \in R \setminus \{0\} \exists a'' \in R: a \cdot a'' = a'' \cdot a = 1$, akkor azt mondjuk, hogy R **ferdetest**. ♣

1.1.4. Definíció. Ha R ferdetest és R -ben a szorzás is kommutatív, akkor **testnek** nevezzük.² ♣

Az egységelem és az egység szavak nem összekeverendőek. Utóbbi az oszthatóság témaköréhez kapcsolódik.

1.1.5. Definíció. Egy egységelemes gyűrű $u \in R$ elemét **egységnek** nevezzük, amennyiben „osztja”³ a gyűrű egységelemét, vagyis $\exists v \in R: u \cdot v = 1 = v \cdot u$. ♣

1.1.6. Definíció. Egy R gyűrűt **nullosztómentesnek** nevezünk, ha $\forall a, b \in R$ esetén $a \cdot b = 0 \Rightarrow a = 0$ vagy $b = 0$. ♣

Láttuk már, hogy két elem szorzata anélkül is lehet 0, hogy bármelyikük is 0 volna. Ilyen mondjuk \mathbb{Z}_6 -ban a 2 és a 3, melyek szorzata $2 \cdot 3 = 6 \equiv 0$.

1.1.7. Definíció. Ha R gyűrűben $a \neq 0$ elemhez $\exists b \neq 0$ úgy, hogy $a \cdot b = 0$, akkor azt mondjuk, hogy a **baloldali nullosztó**, b pedig **jobboldali nullosztó**. ♣

1.1.8. Definíció. Ha R gyűrűben $a \neq 0$ elemhez $\exists n \in \mathbb{Z}$ úgy, hogy $a^n = 0$, akkor azt mondjuk, hogy a **nilpotens**. ♣

Példa: $\mathbb{Z}, 2 \cdot \mathbb{Z}$ és \mathbb{R} halmazok gyűrűk – ahol $2 \cdot \mathbb{Z}$ alatt azt értjük, hogy a \mathbb{Z} halmaz minden elemét megszorozzuk 2-vel balról, tehát ezek a páros egész számok –, de \mathbb{N} nem (mert mondjuk nincs ellentettje az $1 \in \mathbb{N}$ számnak). Ráadásul ezek mind kommutatív gyűrűk is, hasonlóan \mathbb{C} -hez. Gyűrűt alkotnak még a T test feletti polinomok, vagyis $T[x]$, sőt valamely gyűrű feletti polinomok is.

Általánosan is igaz, hogy minden test gyűrű is, hiszen a test definíció szerint egy egységelemes kommutatív gyűrű, melyben minden elemnek van inverze (ha nem mondjuk, hogy milyen inverz, akkor multiplikatívról gondoljunk).

Tudunk mondani olyan gyűrűket is, melyek nem testek. Már az első példánk, \mathbb{Z} is ilyen volt. Ilyen például \mathbb{Z}_4 és még $\mathbb{Z}_4[x]$ is. Utóbbi azért nem test, mert például az x polinomnak nincs inverze, hiszen ha megszorozzuk őt egy polinommal, az eredmény:

$$x \cdot (a_n \cdot x^n + \dots + a_1 \cdot x + a_0) = a_n \cdot x^{n+1} + \dots + a_1 \cdot x^2 + a_0 \cdot x \neq 1$$

Vigyázzunk viszont, mert hasonló érvelés nem működne a $2x + 1$ polinomra, neki ugyanis van inverze, mivel egység: például önmagával megszorozva 1-et kapunk:

$$(2x + 1)^2 = 4x^2 + 4x + 1 \equiv 1$$

1.1.1. Tétel. $\forall a \in R: 0 \cdot a = 0$ ♣

²Jelölés tekintetében néha az Algebra2-ben megismert T betűt használjuk testekre, máskor pedig a szélesebb körben használt K betűt, mely a német Körper (=test) szóból származik.

³Gyűrűben oszthatóságot még nem definiáltunk, de később esik róla szó speciális gyűrűben.

Bizonyítás.

$$0 + 0 = 0$$

Szorozzuk meg mindkét oldalt jobbról a -val:

$$(0 + 0) \cdot a = 0 \cdot a$$

Bal oldalt disztributivitást használva:

$$0 \cdot a + 0 \cdot a = 0 \cdot a$$

Legyen $(0 \cdot a)'$ az additív inverze (ellentettje) az a számnak, ekkor (jobbról) hozzáadva:

$$(0 \cdot a + 0 \cdot a) + (0 \cdot a)' = 0 \cdot a + (0 \cdot a)'$$

Bal oldalt átzárójelezve:

$$0 \cdot a + (0 \cdot a + (0 \cdot a)') = 0 \cdot a + (0 \cdot a)'$$

Használva az ellentett tulajdonságot:

$$0 \cdot a + 0 = 0$$

Végül a nullelem tulajdonságot:

$$0 \cdot a = 0$$

■

Az axiómák kimondják, hogy minden számnak létezik ellentettje, a továbbiakban egy gyűrű egységelemének ellentettjét $-1 = 1'$ jelölje. Ekkor igaz, hogy minden szám ellentettjét megkaphatjuk, ha a számot megszorozzuk az 1 ellentettjével, -1-gyel.

1.1.2. Tétel. $\forall a \in R: a' = (-1) \cdot a$

♣

Bizonyítás. Hasonlóan az előzőhöz, itt most onnan érdemes indulni, hogy $1 + (-1) = 0$ és ezt szorozni a -val, majd disztributivitást használni. Ekkor kapjuk, hogy

$$1 \cdot a + (-1) \cdot a = 0 \cdot a$$

Bal oldalon az egységelem definíciója szerint $1 \cdot a = a$, jobb oldalon az előző tétel alapján 0 áll, vagyis

$$a + (-1) \cdot a = 0$$

ami alapján a $(-1) \cdot a$ ellentettje az a -nak és mivel láttuk, hogy az ellentett egyértelmű, így ez az egyetlen ellentettje a -nak. ■

Felmerülhet a kérdés, hogy mi az, hogy „mivel láttuk”. Hol láttuk mi ezt? Nos idén sehol, tavaly Algebra3-ból annál inkább, hiszen a gyűrű első 4 (összeadásra vonatkozó) axiómája a csoport axiómáknak felel meg és bizonyítottuk, hogy csoportban az inverz egyértelmű.

Tegyünk meg egy hasznos észrevételt a továbbiakra való tekintettel: Egy $a \in R$ elem **pontosan akkor egység, ha van inverze**. Mindkettő megnevezés azt jelenti, hogy van olyan $b \in R$ szám, amellyel akármelyik oldalról is szorozzuk meg 1-et kapunk.

1.1.3. Tétel. Nullosztónak nincs inverze. (Vagyis nullosztó nem lehet egység.)



Bizonyítás. Azt fogjuk belátni, hogy a nem lehet jobboldali nullosztó (a baloldali ugyanígy kellene). Indirekt tegyük fel, hogy egy $a \in R$ elem jobboldali nullosztó és van inverze is. A nullosztó definíciója szerint ekkor $\exists b \neq 0$, melyre

$$b \cdot a = 0$$

Az inverz definíciója szerint pedig $\exists a' \in R$:

$$a \cdot a' = 1$$

Számoljuk ki a $b \cdot a \cdot a'$ szorzatot kétféle zárójelezéssel:

- $(b \cdot a) \cdot a' = 0 \cdot a = 0$
- $b \cdot (a \cdot a') = b \cdot 1 = b$

Mivel az asszociativitás miatt mindegy hogyan zárójelezek, ugyanazt az eredményt kell kapnom. Ezért $b = 0$, ami ellentmondás, hiszen feltettük, hogy $b \neq 0$. ■

1.2. Gyűrűk számelmélete

Láttuk, hogy gyűrű esetén az egység definiálásához két egyenlőségre is szükségünk volt. Egyszerűsítés kedvéért csak speciális gyűrűk esetében beszéljünk oszthatóság fogalomról.

1.2.1. Definíció. A kommutatív és nullosztómentes gyűrűket **integritási tartománynak** nevezzük.

1.2.2. Definíció. Az egységelemes integritási tartományokat **szokásos gyűrűnek** nevezzük.

Például $\mathbb{Z}[x]$ és $\mathbb{Q}[x]$ és \mathbb{Z}_2 és $\mathbb{Z}_2[x]$ szokásos, de \mathbb{Z}_6 és $\mathbb{Z}_6[x]$ már nem azok. Mindkettőnek elemei például a 2 és a 3, és mivel $2 \cdot 3 = 6 \equiv 0 \pmod{6}$, így egyik sem nullosztó mentes.

Emlék: $\mathbb{Z}[x]$ -ben az egységek az 1 és a -1 , $\mathbb{Z}_2[x]$ -ben az 1, valamint $\mathbb{Q}[x]$ -ben a racionális számok, kivéve a nulla: $\mathbb{Q} \setminus \{0\}$. Hiszen gondoljuk meg, hogy ezek mindhárman nullosztómentesek, vagyis ha például két $\mathbb{Q}[x]$ -beli polinomot összeszorozok, a fő tagok kitevői összeadódnak. Tehát csakis akkor kaphatom az 1 polinomot (ami nulladfokú), ha konstansokat szoroztam össze (kitevőben $0 + 0 = 0$), melyek \mathbb{Q} -ban egységek voltak. Ezek pedig \mathbb{Q} esetén a racionális számok, kivéve a 0.

A számelmélet alapfogalmai korábbi tapasztalatainkhoz hasonlóan kerülnek definiálásra gyűrűben, az egységgel már találkoztunk is (kommutatív gyűrű esetén elég az egyik egyenlőség).

1.2.3. Definíció. Legyen R szokásos gyűrű. Ekkor $a, b \in R$ esetén a **osztja** b -t, amennyiben $\exists c \in R$, hogy $a \cdot c = b$. Jelölés: $a \mid b$.

Ugyebár ha nem lenne kommutatív a gyűrűm, akkor vitatkozhatnánk, hogy mikor beszéljünk oszthatóságról. Írjuk le, hogy $ac = b$ és $ca = b$ is teljesüljön? Vagy beszéljünk bal- és jobb-oldali oszthatóságról? Éppen ennek a problémának az elnapolása miatt beszéljünk most csak kommutatív gyűrűkben oszthatóságról.

A szokásos tulajdonság magába foglalja, hogy van egységelem a gyűrűben. Ez azért jó, mert teljesül egy „szokásos” állítás: Tetszőleges $r \in R$ esetén $r \mid r$, hiszen $r \cdot 1 = r$. Nézzünk további fogalmakat.

1.2.4. Definíció. Legyen R szokásos gyűrű. Ekkor $t \in R$ **felbonthatatlan**, – más megnevezéssel **irreducibilis** – amennyiben t nem egység és $t = t_1 \cdot t_2 \Rightarrow t_1$ vagy t_2 egység. ♣

1.2.5. Definíció. Az $a, b \in R$ számok **kitüntetett közös osztója** δ , amennyiben osztója mindkét számnak és a számok összes közös osztójának többszöröse:

- $\delta \mid a$ és $\delta \mid b$
- $c \mid a$ és $c \mid b \Rightarrow c \mid \delta$



Ugorjunk egy nagyot, kiterjeszthetnénk a számelmélet alaptételét is gyűrűkre (más kérdés, hogy igaz-e ez minden gyűrűben vagy sem). Fogalmazzuk meg mit várnánk el a tételtől.

1.2.1. Tétel (Számelmélet alaptétele). Minden $r \in R$ nullelemtől és egységtől különböző számhoz $\exists!$ t_1, t_2, \dots, t_k , melyekre

$$r = t_1 \cdot t_2 \cdot \dots \cdot t_k$$

ahol $\forall t_i$ felbonthatatlan. Vagyis minden ami nem nullelem és nem egység, az felbontható felbonthatatlanok szorzatára, méghozzá ez a felbontás t_i -k sorrendjétől és egységszeresektől eltekintve egyértelmű. ♣

Ezek után szeretnénk általánosítani a maradékos osztás fogalmát. Emlékezzünk vissza, hogy az volt az alapja az euklideszi algoritmusnak, ami a számelmélet alaptételének (továbbiakban SZAT) bizonyításához kellett. Hogyan tanultuk Algebra1-ből a maradékos osztást egész számok körében?

1.2.2. Tétel. Minden $a, b \in \mathbb{Z}$, $b \neq 0$ esetén $\exists!$ $r, q \in \mathbb{Z}$, melyekre

$$a = b \cdot q + r \quad \text{és} \quad 0 < r < b \quad \text{vagy} \quad r = 0$$



Nos ez szép és jó, de gyűrű esetében mi az, hogy $r < b$? Rendezést nem definiáltunk gyűrű elemekre! Rögtön ott vannak a komplex számok, hogyan értelmeznénk ezt két komplex szám között? Emlékezzünk vissza mi volt a helyzet T test feletti polinomokkal. Ez a tétel polinomokra úgy teljesült, hogy a fokszámuk között állt fenn reláció, ami egy természetes szám. Éppen ezért azt tesszük, hogy definiálunk egy leképezést ami gyűrű elemekhez természetes számokat rendel, és azok között vizsgáljuk ezt a bizonyos relációt.

1.2.6. Definíció. Egy R szokásos gyűrűre azt mondjuk, hogy **euklideszi**, amennyiben $\exists \varphi: R \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ és $\forall a, b \in R, b \neq 0$ esetén $\exists r, q \in R$, melyekre

$$a = b \cdot q + r \quad \text{és} \quad 0 < \varphi(r) < \varphi(b) \quad \text{vagy} \quad r = 0$$



A zöld részek azért kerültek ide, mert mi a fogalmat velük együtt értelmezzük, de lehetne nélkülük is, és akkor is egy ekvivalens definíciót kapnánk.

Euklideszi gyűrű például $\mathbb{Z}, T[x]$ vagy \mathbb{R} . A maradékos osztást \mathbb{Z} -ben Algebra1-ből, $T[x]$ -ben Algebra2-ből láttuk be. \mathbb{R} pedig azért euklideszi, mert $r = 0$ és $q = \frac{a}{b}$ választással

$$a = q \cdot b + r = \frac{a}{b} \cdot b + 0$$

valóban teljesül. Az ilyen gyűrűket szeretjük, hiszen esetükben igaz az euklideszi algoritmus, és az abból következő SZAT. Idézzük fel, hogyan is működött az euklideszi algoritmus \mathbb{Z} -ben!

1.2.3. Tétel (Euklideszi algoritmus). Legyen $a, b \in \mathbb{Z}$, valamint a két szám kitüntetett közös osztója δ . Az esetben, ha $b = 0$, akkor $(a, b) = \delta = a$. Ellenkező esetben, ha $b \neq 0$, akkor a maradékos osztás tétele szerint $\exists! q, r \in \mathbb{Z}$

$$a = b \cdot q + r \quad \text{és} \quad 0 < r < b \quad \text{vagy} \quad r = 0$$

Ha $r \neq 0$, akkor ez tovább folytatható, $\exists! q_1, r_1 \in \mathbb{Z}$

$$b = r \cdot q_1 + r_1 \quad \text{és} \quad 0 < r_1 < r \quad \text{vagy} \quad r_1 = 0$$

Hasonlóan tovább folytatva⁴:

- $r = r_1 \cdot q_2 + r_2$ és $0 < r_2 < r_1$ vagy $r_2 = 0$
- \vdots
- $r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$ és $0 < r_{k+1} < r_k$ vagy $r_{k+1} = 0$
- $r_k = r_{k+1} \cdot q_{k+2} + 0$

Ekkor $(a, b) = \delta = r_{k+1}$



Bizonyítás. Először is egy apró észrevétel: értelmes az algoritmus amit felírtunk, vagyis véges sok lépés után valóban egyszer $r_{k+2} = 0$ lesz. Hiszen $b > r > r_1 > r_2 > \dots > r_k > \dots$, vagyis az r_i egész számok szigorú monoton csökkenő sorozatot alkotnak, mely minden lépésben legalább 1-et csökken, egyszer tehát már nem lesz hová csökkennie, eléri a 0 alsó korlátot.

⁴A színezéseket én más módon használtam, mint Szabó Csaba. Nekem ez a maradékos osztások megjegyzésében szokott segíteni, hogy melyik lépésben mit mivel osztok. Minden lépésben odébb csúsztatok egyel a számokat: Először a -t osztom b -vel a maradék r , aztán b -t r -rel a maradék...

A kitüntetett közös osztó definíciója szerint 2 dolgot kell belátnunk: osztja mindkét számot r_{k+1} , valamint hogy minden közös osztója a -nak és b -nek osztója r_{k+1} -nek is.

Az utolsó sorból indulva látszik, hogy $r_{k+1} \mid r_k$. Előtte levő sor jobb oldalát tekintve akkor nyilván $r_{k+1} \mid r_{k+1}$ és $r_{k+1} \mid r_k \cdot q_{k+1}$, tehát ezek összegét is, ami azt jelenti, hogy a bal oldalt osztja: $r_{k+1} \mid r_{k-1}$. Ezt folytathatnánk még így tovább soronként, a végén oda jutnánk el, hogy második sor jobboldalát osztja, tehát a balt is: $r_{k+1} \mid b$. Majd első sorban is eljátszva: $r_{k+1} \mid r$ és $r_{k+1} \mid b$ miatt a teljes jobb oldalt osztja, tehát $r_{k+1} \mid a$. Ezzel az első feltételt be is láttuk.

A másikat pont fordítva fogjuk belátni. Tegyük fel, hogy az ellenség azt mondja egy $c \in \mathbb{Z}$ számról, hogy $c \mid a$ és $c \mid b$. Ekkor mi azt mondjuk az első sort átrendezve, hogy $c \mid a - b \cdot q$ is teljesül, tehát $c \mid r$. Hasonlóan a második egyenletben $c \mid b - r \cdot q_1$, tehát $c \mid r_1$. Végighaladva a sorokon adódik, hogy $c \mid r_{k+1}$. Ezzel be is láttuk a kitüntetett osztó tulajdonságát r_{k+1} -nek. ■

Innen már belátható a számelmélet alaptétele is euklideszi gyűrűkben (ugyanúgy ahogy Algebra1-ből egészekre, Algebra2-ből T test feletti polinomokra csináltuk). De nem csak ezekben teljesül a SZAT! Már Algebra2-ből is említésre került, hogy $\mathbb{Z}[x]$ -ben nincs maradékos osztás, mégis igaz marad az alaptétel.

1.2.7. Definíció. Azt mondjuk, hogy R gyűrű **alaptételes**, ha teljesül benne a számelmélet alaptétele. ♣

Alaptételes például minden euklideszi gyűrű ($\mathbb{Z}, T[x], \mathbb{R}, \dots$), de alaptételes $\mathbb{Z}[x]$ is. Azt, hogy a SZAT miért igaz $\mathbb{Z}[x]$ -ben, a következő fejezetben vizsgáljuk.

1.3. Gauss-lemmák

Míg $\mathbb{R}[x]$ vagy $\mathbb{C}[x]$ esetén pontosan meg tudjuk mondani melyek az irreducibilis polinomok, $\mathbb{Q}[x]$ vagy $\mathbb{Z}[x]$ esetében már nehezebb dolgunk van. Ismerünk bizonyos trükköket, de ezekkel csak a következő fejezetben foglalkozunk. Most azt vizsgáljuk, hogy milyen tekintetben viselkedik hasonlóan $\mathbb{Z}[x]$ és $\mathbb{Q}[x]$.

Először is ide írnék egy emlékeztető tételt Algebra2-ből amely általánosságban testek fölötti polinomokról szól.

1.3.1. Tétel. Legyen T test, ekkor

- $T[x]$ -ben az egységek pontosan a nemnulla konstans polinomok
- ha $f \in T[x]$ 1-fokú \Rightarrow irreducibilis T fölött
- ha $f \in T[x]$ 2- vagy 3-fokú és nincs gyöke T -ben \Rightarrow irreducibilis T fölött
- ha $f \in T[x]$ legalább 2-fokú és irreducibilis T -ben $\Rightarrow f$ -nek nincs gyöke T -ben.



Ebből speciálisan következik, hogy $\mathbb{C}[x]$ -ben az irreducibilis polinomok pontosan az 1-fokúak, $\mathbb{R}[x]$ -ben pedig az 1-fokúak és azok a 2-fokúak melyeknek nincs valós gyöke.

\mathbb{Q} -ról tudjuk, hogy test, \mathbb{Z} -ről pedig, hogy nem. Ezért is lehet meglepő, hogy ha azt mondom, \mathbb{Q} és \mathbb{Z} fölött „majdnem ugyanazok” az irreducibilis polinomok. Na persze azért nem teljesen, például ott van a $2x + 4$ polinom. Az előző tétel alapján mivel \mathbb{Q} test, ez pedig egy 1-fokú polinom, ezért irred.⁵ \mathbb{Q} fölött. Ugyanakkor $2x + 4 = 2 \cdot (x + 2)$, ahol sem a 2, sem pedig az $x + 2$ nem egység $\mathbb{Z}[x]$ -ben (hiszen ott az egységek csak az 1 és -1).

Na jó, de mondhatjuk erre, hogy ez nem izgalmas eset, könnyen elintéztük egy kiemeléssel a kérdést. Foglalkozzunk olyan polinomokkal inkább, amelyek esetén nem tehető meg, hogy kiemelünk egységtől különböző tényezőt minden tagból.

1.3.1. Definíció. Legyen $f \in \mathbb{Z}[x]$. Azt mondjuk, hogy f **primitív polinom**, amennyiben az együtthatók összességében relatív prímek, vagyis $(a_1, a_2, \dots, a_n) = 1$. ♣

Például a $2x + 4$ polinom nem primitív, de a $2x + 3$ már igen. És furcsa módon a $2x + 3$ már \mathbb{Q} és \mathbb{Z} fölött is irreducibilis. Mivel nincs pontos megegyezés arról, mely tételeket nevezzük Gauss-lemmáknak, ezért az előadáson kimondott mind a 4 tételt egyben, ilyen néven sorolom fel.

1.3.2. Tétel. (Gauss-lemmák.)

1. Ha $f \in \mathbb{Z}[x]$ primitív, akkor: f irred. \mathbb{Z} fölött $\Leftrightarrow f$ irred. \mathbb{Q} fölött.
2. Ha $f, g \in \mathbb{Z}[x]$ primitívek, akkor: $f \mid g$ -t \mathbb{Z} fölött $\Leftrightarrow f \mid g$ -t \mathbb{Q} fölött.
3. Ha $f \in \mathbb{Z}[x]$ primitív és $g, h \in \mathbb{Q}[x]$ és $f = g \cdot h \Rightarrow \exists G, H \in \mathbb{Z}[x]$, melyre $f = G \cdot H$ és $G = \frac{A}{B} \cdot g$ és $H = \frac{C}{D} \cdot h$
4. Ha $f, g \in \mathbb{Z}[x]$ primitívek $\Rightarrow f \cdot g$ is primitív.

♣

Az első 3 bizonyítást egyelőre elhagyjuk, de a 4. esetet nézzük meg.

Bizonyítás. Legyen $f = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x + a_0$ és $g = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + \dots + b_1 \cdot x + b_0$, szorzatuk

$$f \cdot g = c_k \cdot x^k + \dots + c_1 \cdot x + c_0$$

Indirekt tegyük fel, hogy $f \cdot g$ nem primitív. Ez azt jelenti, hogy $\exists p$ prímszám, ami osztja $f \cdot g$ -t, vagyis annak minden együtthatóját: $\forall k$ -ra $p \mid c_k$. Mivel f és g primitívek, ezért ez a p prímszám nem oszthatja f minden együtthatóját. Legyen i a legkisebb olyan szám, amire $p \nmid a_i$, hasonlóan j , melyre $p \nmid b_j$. Tekintsük az $f \cdot g$ polinomban x^{i+j} tagot:

$$c_{i+j} \cdot x^{i+j} = \sum_{k+l=i+j} (a_k \cdot x^k) \cdot (b_l \cdot x^l) = \left(\sum_{k+l=i+j} a_k \cdot b_l \right) \cdot x^{i+j}$$

Hogyan néznek ki a jobboldali szumma tagjai? Hát az egyik éppen $a_i \cdot b_i$, melyről tudjuk, hogy $p \nmid a_i \cdot b_i$, mert ha osztaná, akkor a prím tulajdonság miatt az egyiküket is osztaná, amiről feltettük, hogy nem így van.

⁵Az irreducibilis szót mostantól néha így rövidítem, már unalmas volt ennyiszer kiírni.

A többi tag mindegyikében vagy a_k alsó indexe kisebb mint i , ekkor $p \mid a_k$, vagy b_l alsó indexe kisebb mint j , ekkor $p \mid b_l$. Tehát az összes többi tagra igaz, hogy $p \mid a_k \cdot b_l$.

Összeségében $c_{i+j} = p \cdot \text{valami} + a_i b_i$ alakú, vagyis $p \nmid c_{i+j}$, ami ellentmondás, hiszen feltettük, hogy $f \cdot g$ minden együtthatóját osztja. ■

Foglaljuk össze egy tételben a kapcsolatot \mathbb{Z} és \mathbb{Q} fölött irreducibilis polinomok között. (ez is valójában Algebra2-ből elhangzott már, ott sem bizonyított, de a Gauss-lemmából már következik).

1.3.3. Tétel. Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor felbonthatatlan \mathbb{Z} felett, ha $f = p \in \mathbb{Z}$ prímszám vagy f nem konstans felbonthatatlan \mathbb{Q} felett. ♣


Innentől tehát elegendő lesz az irreducibilitást egyik fölött vizsgálnunk és a másiktól is kapunk információt.

2. előadás

Irreducibilitás

2.1. Prímek, felbonthatatlanok

Az 1.2.3 tételből következik, hogy bármely 2 elemnek kitüntetett közös osztója előáll az elemek lineáris kombinációjaként. Bár az euklideszi algoritmust csak egészekre láttuk be, de bármely euklideszi gyűrűben hasonlóan működött volna a bizonyítás (nagyjából annyit változik, hogy \mathbb{Z} helyett R -et kell írni). Innentől kezdve egészek helyett általánosabban gondolkodjunk.

2.1.1. Tétel. Legyen R egy euklideszi gyűrű. Tetszőleges $a, b \in R$ esetén $\exists x, y \in R$ melyekre $(a, b) = x \cdot a + y \cdot b$ 

Bizonyítás. Tekintsük az euklideszi algoritmus során kapott maradékos osztásokat. Azt fogjuk belátni, hogy minden r_i kifejezhető a és b lineáris kombinációjaként, így tehát $r_{k+1} = (a, b)$ is.

Teljes indukciót csinálunk. Nézzük $i = 1$ -re. Az első maradékos osztás sorát átrendezve

$$r = a - b \cdot q$$

ahonnan r -t helyettesítve a második maradékos osztásba

$$b = (a - b \cdot q) \cdot q_1 + r_1$$

majd r_1 -et kifejezve

$$r_1 = -q_1 \cdot a + (1 + q \cdot q_1) \cdot b$$

vagyis $x_1 = -q_1$ és $y_1 = 1 + q \cdot q_1$ választással kifejeztük r_1 -et.

Hasonlóan látható $i = 2$ -re is:

$$r_2 = r - r_1 \cdot q_2$$

beírva r és r_1 helyére amiket előzőleg kaptunk:

$$r_2 = (a - b \cdot q) - (x_1 \cdot a + y_1 \cdot b) \cdot q_2$$

Átrendezve a jobboldalt:

$$r_2 = (1 - x_1 \cdot q_2) \cdot a + (-q - y_1 \cdot q_2) \cdot b$$

vagyis $x_2 = 1 - x_1 \cdot q_2$ és $y_2 = -q - y_1 \cdot q_2$ választással kifejeztük r_2 -t.

Hasonlóan belátható az indukciós lépés, vagyis ha feltesszük, hogy r_{k-1} és r_k kifejezhető, akkor r_{k+1} is. ■

A felbonthatatlanság fogalma után definiáljuk gyűrűben is a prím fogalmát, hasonlóan Algebra1-hez, ahol mindezt az egészek körében tettük.

2.1.1. Definíció. Egy $p \in R$ nemnulla és nem egység elemet **prímnek** nevezünk, ha $\forall a, b \in R$ esetén $p \mid a \cdot b \Rightarrow p \mid a$ vagy $p \mid b$. ♣

Sokszor hajlamosak vagyunk ezt a két fogalmat összekeverni, mert bizonyos számkörökben valóban meg is egyeznek. Nézzünk 2 példát, melyek arra figyelmeztetnek minket, hogy általában ezek különböző fogalmak.

2.1.1. Példa. Tekintsük a páros számok gyűrűjét: $2 \cdot \mathbb{Z}$. Itt a 6 felbonthatatlan, hiszen a 6 sehogys íráható fel két páros szám szorzataként, vagyis igaz, hogy bárhogyan is írtuk fel a 6-ot két páros szorzataként, azok között van egység: $6 = a \cdot b \Rightarrow a$ egység vagy b egység. Ugyanakkor nem prím, hiszen $6 \mid 6 \cdot 2$, de $6 \nmid 6$ és $6 \nmid 2$.

A második példa némi előkészületet is igényel. Eddig használtuk a $\mathbb{Z}[x]$ jelölést a \mathbb{Z} fölötti polinomok halmazára, melyek így néztek ki:

$$a_n \cdot x^n + \dots + a_1 \cdot x + a_0$$

és $a_n, \dots, a_1, a_0 \in \mathbb{Z}$. Ha behelyettesítjük ebbe a polinomba például 2-t az úgy néz ki, hogy minden x -et 2-re cseréljük:

$$a_n \cdot 2^n + \dots + a_1 \cdot 2 + a_0$$

Az ilyen alakú számok halmazát jelölhetnénk $\mathbb{Z}[2]$ -vel, jelképezve azt, hogy ott is csupán le-cseréltük az x -et 2-re. Persze ez nem annyira lenne izgalmas, hiszen ezzel az egész számok halmazát definiálnánk csupán. Izgalmasabb lenne, ha például $\sqrt{-5}$ -öt írnánk x helyére:

$$a_n \cdot (\sqrt{-5})^n + \dots + a_1 \cdot \sqrt{-5} + a_0$$

de mivel páros kitevő esetén $(\sqrt{-5})^n$ valós, páratlan esetén pedig felírható egy valós és $\sqrt{-5}$ szorzataként, ezért ez a halmaz valójában

$$\mathbb{Z}[\sqrt{-5}] = \{a + b \cdot \sqrt{-5} \mid a, b \in \mathbb{Z}\} = \{a + \sqrt{5}b \cdot i \mid a, b \in \mathbb{Z}\}$$

Mivel ezek komplex számok, így értelmezhetjük rájuk a norma fogalmát¹: Egy ilyen $a + \sqrt{5}b \cdot i$ alakú szám normája $a^2 + 5b^2$ ahol a és b továbbra is ugyebár egészek. Na most ezek tudatában nézzük meg a másik példát.

2.1.2. Példa. Tekintsük $\mathbb{Z}[\sqrt{-5}]$ gyűrűt. Mivel

$$6 = 2 \cdot 3 = (1 + \sqrt{5} \cdot i) \cdot (1 - \sqrt{5} \cdot i)$$

ezért $2 \mid (1 + \sqrt{5} \cdot i) \cdot (1 - \sqrt{5} \cdot i)$, de $2 \nmid (1 + \sqrt{5} \cdot i)$ és $2 \nmid (1 - \sqrt{5} \cdot i)$, vagyis a 2 nem prím.

¹komplex szám normája az abszolútértékének négyzete

Ugyanakkor a 2 felbonthatatlan, mert tegyük fel, hogy $2 = \alpha \cdot \beta$. Nyilván a 2 oldal normája is megegyezik és felhasználva, hogy komplex számok esetén szorzat normája a normák szorzata (hiszen ha ez abszolútértékre igaz, akkor annak négyzetére is):

$$N(2) = 4 = N(\alpha) \cdot N(\beta)$$

Mivel ezek már egész számok, így a következő esetek lehetségesek.

1. $N(\alpha) = a^2 + 5b^2 = 1 \Rightarrow b = 0 \Rightarrow a = \pm 1 \Rightarrow \alpha = \pm 1$, vagyis egység az α
2. $N(\alpha) = 4 \Rightarrow N(\beta) = c^2 + 5d^2 = 1 \Rightarrow \beta = \pm 1$, vagyis β egység
3. $N(\alpha) = a^2 + 5b^2 = 2 \Rightarrow a^2 = 2$, ami nem lehetséges, hiszen $a \in \mathbb{Z}$

Látjuk tehát, hogy a 2 csakis úgy bomlik két szám szorzatára, hogy az egyikük egység kell legyen, tehát a 2 felbonthatatlan, de nem prím.

Most pedig be fogjuk látni, hogy euklideszi gyűrűben a prímekek és felbonthatatlanok ugyanazok, és ez a kitüntetett közös osztó azon tulajdonságán fog múlni, hogy előáll a számok lineáris kombinációjaként.

2.1.2. Tétel. Euklideszi gyűrűben p akkor és csak akkor prím, ha felbonthatatlan. ♣

Bizonyítás. Két lépésben bizonyítunk, először a prím tulajdonságból az irreducibilitást, majd fordítva.

Ha p prím, akkor felbonthatatlan biz.:

Azt kell belátnunk, hogy ha $p = a \cdot b$, akkor a vagy b egység. Nos amennyiben $p = a \cdot b$, akkor $p \mid a \cdot b$ is teljesül, amiből a prímtulajdonság miatt $p \mid a$ vagy $p \mid b$. Amennyiben $p \mid a$, akkor $\exists c$, melyre $a = p \cdot c$, tehát ott tartunk, hogy

$$\begin{cases} p = a \cdot b \\ a = p \cdot c \end{cases}$$

Az elsőbe helyettesítve a helyére a másodikat $p = p \cdot c \cdot b$ adódik, amit p -vel egyszerűsítve $1 = c \cdot b$, vagyis van olyan szám, amivel megszorozva a b -t 1-et kapunk. Ez éppen annak a definíciója, hogy $b \mid 1$, vagyis hogy b egység. Hasonlóan látható be a másik eset: $p \mid b \Rightarrow a$ egység.

Ha f felbonthatatlan, akkor prím biz.:

Azt kellene belátnunk, hogy ha $f \mid a \cdot b \Rightarrow f \mid a$ vagy $f \mid b$. Tekintsük a és f kitüntetett közös osztóját. Mivel f -et csupán egység és önmaga osztja, így csak 2 esetet kell megvizsgálnunk. Az első eset, hogy $(a, f) = f$, ekkor nyilván $f \mid a$. A másik eset, hogy $(a, f) = 1$, ekkor viszont mivel a kitüntetett közös osztó felírható az elemek lineáris kombinációjaként: $\exists x, y \in R$ melyekre

$$1 = x \cdot a + y \cdot f$$

Beszorozva az egészet b -vel:

$$b = (ba) \cdot x + (by) \cdot f$$

ahonnan látható, hogy $f \mid f \Rightarrow f \mid (by) \cdot f$ és $f \mid ba \Rightarrow f \mid (ba) \cdot x$, tehát a teljes jobboldalt osztja f . Ekkor viszont a vele egyenlő balt is, vagyis $f \mid b$. ■

2.2. Számelmélet alaptétele

2.2.1. Tétel. Minden euklideszi gyűrű alaptételes (vagyis teljesül benne az 1.2.1 tétel). ♣

Bizonyítás. Két dolgot kell bizonyítanunk: Minden felbontható és a felbontás egyértelmű.

Egyértelműség biz.:

Tegyük fel, hogy egy $r \in R$ elemnek ismerjük kétféle felbontását is:

$$r = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

ahol minden p és q felbonthatatlan (tehát prím is, mivel euklideszi gyűrűben vagyunk). Látható, hogy $p_1 \mid q_1 \cdot q_2 \cdot \dots \cdot q_t$. Mivel p_1 prím tulajdonságú, ezért a szorzat egyik tényezőjét osztania kell: $\exists i$ melyre $p_1 \mid q_i$. Ez az oszthatóság azt jelenti, hogy $\exists c$ melyre

$$q_i = p_1 \cdot c$$

de mivel q_i felbonthatatlan, ezért p_1 vagy c egység kell legyen. Mivel p_1 prím, ő már nem lehet egység, tehát c valójában egy e egység. Helyettesítsünk q_i helyére $p_1 \cdot e$ -t:

$$p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_{i-1} \cdot (p_1 \cdot e) \cdot q_{i+1} \cdot \dots \cdot q_t$$

majd egyszerűsítsünk p_1 -gyel:

$$p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_{i-1} \cdot e \cdot q_{i+1} \cdot \dots \cdot q_t$$

Ezt folytassuk tovább p_2, \dots, p_k esetén is, mindegyikre hasonlóan kapjuk, hogy valamilyen q_i egységszerese, így tehát ez a két felbontás lényegében ugyanaz.

Felbonthatóság biz.:

Úgy definiáltuk az euklideszi gyűrűt, hogy van benne „maradékos osztás”, amihez szükségünk volt egy φ függvényre, hogy azt mondhassuk folyamatosan „csökken” valamilyen értelemben a maradék. A felbonthatóság bizonyításához szükségünk lesz egy segédállításra ezzel kapcsolatban, amit most nem bizonyítottunk:

$$\text{Ha } a \mid b \text{ és } a \neq e \cdot b \Rightarrow \varphi(a) < \varphi(b).$$

Legyen adott $a \in R$ elem. Az egyik eset, hogy a felbonthatatlan, ekkor kész vagyunk. Ha nem, akkor felbontható két elem szorzatára úgy, hogy azok egyike sem egység: $a = a_1 \cdot a_2$. Innentől elegendő a_1 -ről mondanom dolgokat, miután vele végeztünk, utána a_2 -vel is mindezt meg tudjuk csinálni.

Az egyik eset, hogy a_1 felbonthatatlan, ekkor vele nincs több dolgunk. A másik, hogy bontható:

$$a = a_1 \cdot a_2 = b_1 \cdot b_2 \cdot a_2$$

ahol b_1 és b_2 sem egység. És innentől ezt a folyamatot ismételtessük amíg nem lesz minden szám felbonthatatlan. Ha odáig elértünk nincs több dolgunk, elkészült a felbontás.

Vegyük észre, hogy a segédállítás garantálja, hogy véges sok lépésben elkészülünk a felbontással. Hiszen például az első lépésben $a = a_1 \cdot a_2$ esetén a_1 és a_2 egyike sem egység, ezért bár $a_1 \mid a$, de $a_1 \neq e \cdot a$, vagyis a segédállítás szerint $\varphi(a_1) < \varphi(a)$. Hasonlóan látható, hogy

$$\varphi(a) > \varphi(a_1) > \varphi(b_1) > \dots > 0$$

hiszen a φ függvény képhalmaza $\mathbb{N} \setminus \{0\}$. Ha pedig ez folyamatosan csökken és végig pozitív egész, akkor egy idő után be kell fejeződnie a folyamatnak. ■

2.3. Trükkök $\mathbb{Z}[x]$ -ben

Az 1.3.2 tétel 4. pontjára adjunk egy másik, elegánsabb bizonyítást, mely más szempontból is tanulságos lesz.

Bizonyítás. Indirekt tegyük fel, hogy $f \cdot g$ nem primitív. Ez azt jelenti, hogy $\exists p \in \mathbb{Z}$ prímszám, melyre $p \mid f \cdot g$. Tekintsük az $f \cdot g$ polinomot modulo p , ekkor $f \cdot g = 0$ teljesül $\mathbb{Z}_p[x]$ -ben.

Algebra2-ből tudjuk, hogy $\mathbb{Z}_p[x]$ nullosztómentes gyűrű. Ez azt jelenti, hogy ha $\mathbb{Z}_p[x]$ -ben $f \cdot g = 0$, akkor $f = 0$ vagy $g = 0$. Ha $f = 0$, akkor $p \mid f$, ami ellentmondás, mert ekkor f nem lenne primitív. Ha pedig $g = 0$, akkor $p \mid g$, ismét ellentmondás. Tehát $f \cdot g$ is primitív. ■

Hogyan segíthet ez az ötlet eldönteni egy polinomról $\mathbb{Z}[x]$ -ben, hogy irreducibilis-e? Ez a „vegyük modulo p ” lesz számos trükk alapja, köztük a Schönemann-Eisenstein kritériumnak is, de mielőtt azt tárgyalnánk, nézzünk néhány példát.

1. Igaz-e, hogy $5x^3 - 28x^2 + 2$ irreducibilis $\mathbb{Z}[x]$ -ben?

Habár \mathbb{Z} nem test, a 1.3.1 tétel 3. pontja itt is hasznunkra lesz, mert a polinomunk primitív, így a Gauss-lemma miatt \mathbb{Z} helyett \mathbb{Q} fölötti felbonthatatlanságot is vizsgálhatunk. Azt kell megnéznünk, hogy van-e racionális gyöke a polinomnak, amit **racionális gyökteszt** segítségével végzünk.

A lehetséges gyökök jelen esetben $1, -1, 2, -2, \frac{1}{5}, -\frac{1}{5}, \frac{2}{5}, -\frac{2}{5}$. Látható, hogy ezek egyike sem gyöke a polinomnak, tehát nincs racionális gyöke, irreducibilis. Ez a módszer **2- és 3-fokú** polinomokra működik.

2. Igaz-e, hogy $7x^{111} - 11$ irreducibilis $\mathbb{Z}[x]$ -ben?

Tegyük fel, hogy felbontható, vagyis $7x^{111} - 11 = f \cdot g$ ahol f és g egyike sem egység.

Ötlet: tekintsük ezt az egyenlőséget \mathbb{Z}_{11} , ekkor² $7x^{111} = \overline{f} \cdot \overline{g} = \overline{f} \cdot \overline{g}$. Mivel \mathbb{Z}_{11} test, ezért igaz benne a számelmélet alaptétele, a bal oldal egyértelműen bomlik fel irreducibilis polinomok szorzatára: $7x^{111} = 7 \cdot \underbrace{x \cdot x \cdot \dots \cdot x}_{111 \text{ darab}}$.

Vagyis $\overline{f} = ax^k$ és $\overline{g} = b \cdot x^{111-k}$ alakú lehet csak. Ez azt jelenti, hogy amikor f -et modulo 11 vettük, akkor megmaradt belőle egy ax^k rész, a többi „elveszett”, mert osztható volt minden egyéb együttható 11-el. Vagyis $f = a' \cdot x^k + 11 \cdot f_1$ és $g = b' \cdot x^{111-k} + 11 \cdot g_1$ alakú. Mi lesz akkor $f \cdot g$?

$$7x^{111} - 11 = f \cdot g = a'b' \cdot x^{111} + 11a' \cdot g_1 \cdot x^k + 11b' \cdot f_1 \cdot x^{111-k} + 11^2 \cdot f_1 \cdot g_1$$

²felülvonással jelölve azt, hogy modulo 11 vesszük az együtthatókat

Azt látjuk tehát, hogy a jobboldali polinom konstans tagja osztható 11^2 -el, de a bal oldali nem, ami ellentmondás, tehát a polinom felbonthatatlan.

Megjegyzés. Meggondolandó, hogy mi lenne $k = 0$ vagy $k = 111$ esetén. Ezzel szerencsére nem kellett most foglalkozunk, hiszen akkor f vagy g konstans lenne, de mivel láthatóan $7x^{111} - 11$ primitív, ezért biztosan nem emelhető ki belőle konstans. Általában inkább primitív polinomokkal foglalkozunk, hiszen feltehető, hogy ha valami kiemelhető azt észrevesszük, és már csak a maradék részből kell eldöntenünk, hogy bontható vagy sem.

Megjegyzés. Vegyük észre, hogy $p = 7$ prím választásával is hasonlóan mondhattunk volna el mindent. Akkor $\bar{f} \cdot \bar{g} = 3$ lett volna és $f = a' + 7f_1$, $g = b' + 7g_1$ alakú. Innen $7x^{111} - 11 = f \cdot g = 7^2 \cdot f_1 \cdot g_1 + \dots$ miatt a főegyüttható osztható kellene legyen 7^2 -el, ami ellentmondás lenne. (Ezt nevezik egyes szakirodalmak fordított Schönemann-Eisenstein kritériumnak.)

3. Igaz-e, hogy $13x^{126} + 8x + 49$ irreducibilis $\mathbb{Z}[x]$ -ben?

Most fogjuk összegyűjteni az előző 2 technikát. Tegyük fel, hogy felbomlik $13x^{126} + 8x + 49 = f \cdot g$ -re, ahol egyik sem egység. Először szabaduljunk meg a nagy fokú tagtól, tekintsük \mathbb{Z}_{13} az egészet: $8x + 10 = \bar{f} \cdot \bar{g}$.

Mit tudunk itt a jobboldali tényezők fokszámairól? Valahogy ki kell adják a bal oldali 1-et. Nullosztómentes gyűrű esetén polinomok szorzásakor a fokok összeadódnak, tehát az egyik 0-fokú, a másik 1 kell legyen. Legyen mondjuk \bar{f} konstans, \bar{g} pedig elsőfokú. Ekkor $f = c + 13 \cdot f_1$, valamint $g = ax + b + 13 \cdot g_1$ alakú.

Na most ha ezeket összeszorozzuk, akkor a legmagasabb fokú tag $13x^{126}$ kellene legyen, hiszen $f \cdot g$ adja éppen a vizsgált polinomunkat. Viszont ha itt g_1 foka legalább 2 lenne, akkor g főegyütthatója osztható lenne 13-al, f főegyütthatója szintén osztható 13-al (feltehető, hogy f nem konstans, mert primitív a vizsgált polinomunk, konstans nem emelhető ki), és polinomok szorzatakor a főegyüttható éppen a tényezők főegyütthatóinak szorzata lesz, vagyis 13^2 osztaná a vizsgált polinomunk főegyütthatóját, de $13^2 \nmid 13$.

Tehát feltehető, hogy g_1 foka legfeljebb 1, vagy esetleg $g_1 = 0$. Ekkor $g = Ax + B$ alakú, ami azt jelenti, hogy a vizsgált polinomnak kell legyen gyöke, innentől úgy vizsgáljuk mint az 1. trükk tárgyalásakor: racionális gyöktesztet alkalmazunk, jelenleg a szóba jöhető gyökök:

$$1, -1, 7, -7, 49, -49, \frac{1}{13}, -\frac{1}{13}, \frac{7}{13}, -\frac{7}{13}, \frac{49}{13}, -\frac{49}{13}$$

Tehát a tanulság itt az volt, hogy könnyen tudunk nyilatkozni 1-, 2-, vagy 3-fokú polinomokról. Fölötte pedig amennyire csak tudjuk próbáljuk **csökkenteni a fokszámot vagy a tagok számát** és úgy mondani valamit a polinomról.

Ezen fejezet zárásaként mondjuk ki a Schönemann-Eisenstein kritériumot, mely az előadás utolsó perceiben hangzott el, de alapvetően ehhez a témakörhöz tartozik. Bizonyítását egyelőre elhagyom, nem is biztos hogy szükséges visszatérni hozzá: ugyan úgy zajlik, mint 2. trükk, tulajdonképpen már ott is ezt alkalmaztuk.

2.3.1. Tétel. (Schönemann-Eisenstein kritérium).

Legyen $f = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x + a_0$ egész együtthatós polinom. Ha

$\exists p$, melyre $p \nmid a_n$ és $\forall i \neq n$ -re $p \mid a_i$ és $p^2 \nmid a_0$ **vagy** $p \nmid a_0$ és $\forall i \neq 0$ -ra $p \mid a_i$ és $p^2 \nmid a_n$

akkor f irreducibilis \mathbb{Q} fölött.



Például $x^6 + 6x^5 + 3x^3 + 9x + 12$ polinom esetében $p = 3$ választással alkalmazható a Schönemann-Eisenstein kritérium, hiszen a főegyütthatón kívül mindegyiket osztja, de $3^2 = 9$ már nem osztja a konstans.

2.4. Karakterisztika

Egy ideig most testekkel fogunk foglalkozni. Minden testről tudjuk, hogy legalább két elemű, hiszen biztosan benne van a 0 nullelem és a tőle különböző 1 egységelem.

Zárt az összeadásra, tehát ha benne van az 1, akkor $1 + 1$ is, továbbá $1 + 1 + 1$ is, stb... Azért, hogy könnyebb legyen ezekről is beszélni, adjunk nekik nevet, definiáljuk a $2, 3, \dots$ számokat:

$$\begin{aligned} 2 &= 1 + 1 \\ 3 &= 1 + 1 + 1 \\ 4 &= 1 + 1 + 1 + 1 \\ &\vdots \\ n &= \underbrace{1 + 1 + \dots + 1}_{n \text{ darab}} \end{aligned}$$

Bizonyos esetekben találkoztunk már olyannal, hogy egy idő után ha kellően sok 1-est adtunk össze, 0-t kaptunk. Például \mathbb{Z}_3 esetén: $1 + 1 + 1 = 0$. Ennek jellemzésére vezetjük be a karakterisztika fogalmát.

2.4.1. Definíció. Egy T test **karakterisztikája** a legkisebb olyan p pozitív egész szám, ahányszor az egységelemet összeadva nullelemet kapunk. Ha ez sosem fordulhat elő, akkor 0. Jelölés:

$$\text{char}(T) = \begin{cases} \min\{p > 0, p \in \mathbb{Z} \mid \underbrace{1 + 1 + \dots + 1}_{p \text{ darab}} = 0\} & \text{ha } \exists p > 0, p \in \mathbb{Z}: \underbrace{1 + 1 + \dots + 1}_{p \text{ darab}} = 0 \\ 0 & \text{különben} \end{cases}$$



Például $\text{char}(\mathbb{Z}_3) = 3$, illetve $\text{char}(\mathbb{R}) = 0$.

2.4.1. Tétel. Ha egy test karakterisztikája egy p pozitív egész szám, akkor p prím.



Bizonyítás. Valójában a felbonthatatlan tulajdonságot bizonyítjuk, de egészek körében beláttuk, hogy ugyanazok a prímek mint a felbonthatatlanok. Indirekt tegyük fel, hogy $p = a \cdot b$, továbbá a és b sem egység. Ekkor nyilván $a, b < p$ és mivel p a karakterisztika, ezért

$$\underbrace{1 + 1 + \dots + 1}_{p=a \cdot b \text{ darab}} = 0$$

Legyen $x = \underbrace{1 + 1 + \dots + 1}_{a \text{ darab}}$ és $y = \underbrace{1 + 1 + \dots + 1}_{b \text{ darab}}$. Mi lesz $x \cdot y$?

$$x \cdot y = \underbrace{(1 + 1 + \dots + 1)}_{a \text{ darab}} \cdot \underbrace{(1 + 1 + \dots + 1)}_{b \text{ darab}} = \underbrace{1 \cdot 1 + 1 \cdot 1 + \dots + 1 \cdot 1}_{a \cdot b \text{ darab}} = \underbrace{1 + 1 + \dots + 1}_{a \cdot b \text{ darab}} = 0$$

Azt kaptuk tehát, hogy $x \cdot y = 0$, de mivel T test, és testről Algebra2-ben láttuk, hogy nullosztómentes, ezért $x = 0$ vagy $y = 0$ kell teljesüljön. Viszont akkor $x = 0$ esetén már a elemet elég lenne összeadnunk, hogy 0-t kapjunk, p nem lenne minimális. Hasonlóan ellentmondás $y = 0$ is. Kaptuk tehát, hogy p prím. ■

Vegyük észre, hogy nem muszáj nekünk feltétlenül mindig egységelemekkel gondolkoznunk, hiszen ha p darabot összeadva egységelemekből nullelemet kapunk, akkor tetszőleges elemre is igaz ez: $\underbrace{a + a + \dots + a}_{p \text{ darab}} = a \cdot \underbrace{(1 + 1 + \dots + 1)}_{p \text{ darab}} = a \cdot 0 = 0$

Az is könnyen látható, hogy pontosan akkor pozitív a karakterisztika, ha különböző számú 1-eket összeadva ugyanazt kapjuk:

$$\underbrace{1 + 1 + \dots + 1}_{i \text{ darab}} = \underbrace{1 + 1 + \dots + 1}_{j \text{ darab}}$$

akkor átrendezve (azt feltételezve, hogy $i > j$)

$$\underbrace{1 + 1 + \dots + 1}_{i-j \text{ darab}} = 0$$

ami éppen azt jelenti, hogy van olyan szám, ahányszor 1-eket összeadva 0-t kapunk, akkor ezek között legkisebb is van, tehát pozitív a karakterisztika.

Ennek megfordítása, hogy ha 0 a karakterisztikája egy testnek, akkor az $0, 1, 2, 3, 4, \dots$ számok mind különbözőek. Akkor viszont már ott tartunk, hogy ebben a testben egész sok elem benne van: az összes természetes szám!

Gondolkozzunk tovább ezzel a 0 karakterisztikájú testtel: minden elemnek van ellentettje, vagyis minden $i \in T$ esetén $\exists -i \in T$.

2.4.1. Állítás. Az ellentettek mind különbözőek és ha $i \in \{1, 2, 3, \dots\}$, akkor $-i \notin \{1, 2, 3, \dots\}$ ♣

Bizonyítás. Az, hogy az ellentettek mind különbözőek egyszerűen azért van, mert minden elem ellentettje egyértelmű, tehát ha x az ellentettje a -nak és y a b -nek és $x = y$, akkor nyilván $a = b$ is igaz kell legyen.

Indirekt tegyük fel, hogy $\exists j \in \{1, 2, 3, \dots\}$, melyre $-i = j$, másképpen $i + j = 0$, azaz

$$\underbrace{1 + 1 + \dots + 1}_{i \text{ darab}} + \underbrace{1 + 1 + \dots + 1}_{j \text{ darab}} = \underbrace{1 + 1 + \dots + 1}_{i+j \text{ darab}} = 0$$

ami ellentmond annak, hogy a test 0 karakterisztikájú volna. ■

Ezzel most már látjuk, hogy benne van a testben az összes egész szám. De tudjuk azt is, hogy minden nemnulla elemnek van inverze, tehát $0 \neq b \in T \Rightarrow \frac{1}{b} \in T$. Zárt a szorzásra is, tehát: $a, b \in R, b \neq 0 \Rightarrow \frac{a}{b} \in T$.

Ezzel kaptunk egy halmazt, az $\frac{a}{b}$ alakú számok halmazát, melyről egyből a racionális számtest juthat eszünkbe. Valóban van kapcsolat a kettő között, de ezt csak később bizonyítjuk be.

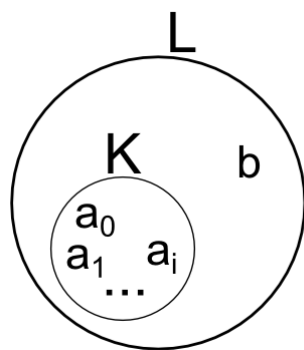
2.4.2. Tétel. Az $\frac{a}{b}$ alakú számok teste izomorf³ a racionális számokéval: $\left\{\frac{a}{b}\right\} \cong \mathbb{Q}$. ♣

2.4.2. Definíció. Legyen T test. Ha $S \subseteq T$ és S is test a T -beli műveletekre nézve, akkor azt mondjuk, hogy S **részteste** T -nek. Jelölés: $S \leq T$. Hasonlóan gyűrű esetén a részgyűrű. ♣

A 2.4.2 tétel és az elmúlt két oldal gondolatmenete bizonyítja a következő állítást.

2.4.3. Tétel. Bármely T test esetén $\mathbb{Z}_p \leq T$ vagy $\mathbb{Q} \leq T$. Első esetben $\text{char}(T) = p$, második esetben $\text{char}(T) = 0$. ♣

Képzeljük el most a következőt: Legyen L test és $K \leq L$ részteste. Tegyük fel, hogy L -nek van olyan eleme, ami K -ban nincs benne: $b \in L \setminus K$, továbbá a_0, a_1, \dots, a_i jelöljenek K résztest belüli elemeket.



Tudjuk a testaxiómákat, tudjuk mi mindent tehetünk K testben. Most tegyük fel, hogy csalni akarunk és úgy szeretnénk tenni, mintha b is K eleme lenne. Hogyan nézne ki akkor a K , ha továbbra is szeretnénk, hogy test maradjon?

Ha bevinnénk b -t, akkor már b^2 -et is kellene, sőt az összes b hatványt, hogy zártak maradjunk a szorzásra. Sőt, nem csak önmagával, de K belüli elemekkel is meg kell tudjuk szorozni a b hatványokat. Tehát biztosan benne kellene lennie a testünkben minden $a_n \cdot b^n + \dots + a_2 \cdot b^2 + a_1 \cdot b + a_0$ alakú számnak (bárhogyan is választjuk az a_i elemeket, a fenti ábra esetén tehát annyi pontosítás, hogy minden a_i tetszőleges K -beli elem lehet, nem rögzítettek). Ilyen kifejezéssel találkoztunk már, ezek a polinomok. Vagyis ha minden ilyen polinom halmazát tekintem, akkor megkapom a teljes K fölötti polinomgyűrűt a b változóban:

$$K[b] = \{a_n \cdot b^n + \dots + a_2 \cdot b^2 + a_1 \cdot b + a_0\}$$

Viszont ha továbbra is testet szeretnénk kapni, akkor ezeknek (kivéve a 0 polinomot) inverzére is szükségünk lenne. Tehát szükségünk van a racionális törtfüggvényekre is.

³ugyanúgy értelmezzük az izomorfizmust testekre, mint csoportokra: izomorf két test, ha elemeik között művelettartó bijekció létesíthető

2.4.3. Definíció. Legyen K gyűrű és $f(x), g(x) \in K[x]$ és $g(b) \neq 0$. Ekkor az $\frac{f(b)}{g(b)}$ elemek halmazát a K gyűrű fölötti **racionális törtfüggvényeknek** nevezzük. Jelölés:

$$K(b) = \left\{ \frac{f(b)}{g(b)} \mid f(x), g(x) \in K[x], g(b) \neq 0 \right\}$$



2.5. Algebrai, transzcendens, minimálpolinom

2.5.1. Definíció. Legyen L test és $K \leq L$. Ekkor azt mondjuk, hogy $a \in L$ a K fölött **algebrai**, ha $\exists f(x) \in K[x], f(x) \neq 0$, melyre $f(a) = 0$. Egy $a \in \mathbb{C}$ komplex számra ha nem mondjuk mi fölött algebrai, akkor \mathbb{Q} fölött értendő. Ha $a \in L$ nem algebrai, akkor **transzcendens**.



Például a $\sqrt{2}$ algebrai, mert az $x^2 - 2$ racionális együtthatós polinomnak gyöke.

2.5.1. Tétel. A π és az e számok transzcendensek.



Nem bizonyítjuk.

Tegyük fel, hogy α egy algebrai szám K fölött. Ez azt jelenti, hogy $\exists n$, melyre

$$f(x) = x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x + a_0$$

polinomnak gyöke az α . Ez annyit tesz, hogy helyettesítve

$$f(\alpha) = \alpha^n + a_{n-1} \cdot \alpha^{n-1} + \dots + a_1 \cdot \alpha + a_0 = 0$$

ahonnan α^n kifejezhető az α kisebb hatványaival. Akkor viszont minden $f(\alpha)$ átírható a magasfokú tagok kisebbekre visszavezetésével legfeljebb $n-1$ fokúra.

Ekkor az α változós racionális törtfüggvények halmaza is picit változik, ugyanis feltehető, hogy a számláló és a nevező foka is kisebb mint n :

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in K[x], \deg f, \deg g < n \right\}$$

Sőt belátható, hogy nem csak magas fokú polinomjai fejezhetők ki α -nak kis fokúakkal, de a racionális törtfüggvényei is polinomokkal.

2.5.2. Tétel. Ha α algebrai K fölött, akkor $K(\alpha) = K[\alpha]$.



Az állítás a gyöktelenítésen múlik, ahogy például az a tény, hogy az $a + b \cdot \sqrt{2}$ alakú számok testet alkotnak. Ott is, illetve még Algebra2-ből a komplexek esetében is az inverz létezésének kérdését gyöktelenítéssel oldottuk meg.

Például miért $a + b \cdot \sqrt{2}$ alakú a $\frac{3 + \sqrt{2}}{2 - \sqrt{2}}$ szám? A nevezőt gyöktelenítve:

$$\frac{3 + \sqrt{2}}{2 - \sqrt{2}} \cdot \frac{2 + \sqrt{2}}{2 + \sqrt{2}} = \frac{(2 + \sqrt{2}) \cdot (3 + \sqrt{2})}{2} = \frac{6 + 2 + 3\sqrt{2} + 2\sqrt{2}}{2} = \frac{8 + 5\sqrt{2}}{2} = 4 + \frac{5}{2} \cdot \sqrt{2}$$

Magát a tételt már nem igazoljuk ebben a fejezetben, de még bevezetünk egy hasznos fogalmat és annak néhány tulajdonságát belátjuk.

2.5.2. Definíció. Legyen α algebrai K fölött. Az α **minimálpolinomjának** nevezzük azt a legkisebb fokú, 1 főegyütthatós polinomot, aminek gyöke az α . Jelölés: $m(x) = m_\alpha(x)$. ♣

2.5.3. Tétel. Minimálpolinom tulajdonságai:

1. Egyértelműen létezik minimálpolinomja α -nak.
2. $m_\alpha(x)$ irreducibilis K fölött
3. Minden polinomot oszt, aminek gyöke az α : $f(\alpha) = 0 \Rightarrow m_\alpha(x) \mid f(x)$



Bizonyítás. Az elsőt bizonyítjuk utoljára, mert 2. és 3. felhasználásával egyszerűbb.

2. *biz.:*

Indirekt tegyük fel, hogy $m_\alpha = f(x) \cdot g(x)$, és $f(x)$ és $g(x)$ sem egység. Mivel test fölött vagyunk, egységek a numnulla konstansok, vagyis f és g foka is legalább 1 kell legyen. De mivel fokszámaik összege $m_\alpha(x)$ foka, ezért mindkettő kisebb fokú $m_\alpha(x)$ -nél. Helyettesítsünk α -t:

$$0 = m_\alpha(\alpha) = f(\alpha) \cdot g(\alpha)$$

ezért $f(\alpha) = 0$ vagy $g(\alpha) = 0$. Amennyiben $f(\alpha) = 0$, akkor találtunk egy polinomot aminek gyöke az α és foka kisebb mint $m_\alpha(x)$ -nek, ez ellentmondás (különben $m_\alpha(x)$ nem lenne minimálpolinom). Hasonlóan $g(\alpha) = 0$ is ellentmondást ad.

3. *biz.:*

Test fölött van maradékos osztás, osszuk el $f(x)$ -et maradékosan $m_\alpha(x)$ -el és lássuk be, hogy 0 a maradék: $\exists! r(x), q(x) \in K[x]$, melyre

$$f(x) = m_\alpha(x) \cdot q(x) + r(x) \quad \text{és} \quad \deg r < \deg m_\alpha \quad \text{vagy} \quad r = 0$$

helyettesítve α -t:

$$0 = f(\alpha) = \underbrace{m_\alpha(\alpha) \cdot q(\alpha)}_0 + r(\alpha) = r(\alpha)$$

Amennyiben $r(x) \neq 0$, akkor találtunk egy m_α -nál kisebb fokú polinomot aminek gyöke az α , ez ellentmondás lenne ismét. Tehát csakis az lehet, hogy a maradék, $r(x) = 0$.

1. *biz.:*

A létezést nem szükséges bizonyítani, hiszen algebrai K fölött az α , vagyis van olyan K fölötti polinom, aminek gyöke. Nyilván ezek között minimális fokszámú is van, és ha azt leosztjuk a főegyütthatójával (ezzel a gyökein nem változtatva), akkor megkapjuk a megkívánt 1 főegyütthatónkat is. Nézzük az egyértelműség igazolását.

Legyen $m_1(x)$ és $m_2(x)$ is az α minimálpolinomja. Lássuk be, hogy ők valójában ugyanazok. Nyilván ekkor $m_1(\alpha) = m_2(\alpha) = 0$, vagyis a 3. állítás miatt $m_1 \mid m_2$, de hasonlóan $m_2 \mid m_1$. Ez csakis úgy lehetséges, ha $m_1 = e \cdot m_2$, ahol e egység. Ráadásul mivel mindkettő minimálpolinom, főegyütthatójuk 1, tehát egészen konkrétan $e = 1$ lehetséges csak, azaz $m_1 = m_2$. ■

Például a $\sqrt{2}$ minimálpolinomja \mathbb{R} és \mathbb{C} fölött is $m_{\sqrt{2}}(x) = x - \sqrt{2}$. Mi a helyzet \mathbb{Q} fölött? Ott $m_{\sqrt{2}}(x) = x^2 - 2$. Ehhez 2 dolgot kell látni:

- Ennek valóban gyöke a $\sqrt{2}$, hiszen $(\sqrt{2})^2 - 2 = 0$
- Előző pont miatt a minimálpolinomja $\sqrt{2}$ -nek osztja az $x^2 - 2$ polinomot a bizonyított 3. tulajdonság miatt. Ugyanakkor \mathbb{Q} fölött $x^2 - 2$ felbonthatatlan (például Schönemann-Eisenstein kritérium $p = 2$ -vel azonnal látszik).

Hasonlóan $\sqrt[5]{2}$ minimálpolinomja \mathbb{R} fölött $x - \sqrt[5]{2}$, de \mathbb{Q} fölött $x^5 - 2$, melynek gyöke $\sqrt[5]{2}$, és $p = 2$ választással látszik, hogy felbonthatatlan.

3. előadás

Test és vektortér

3.1. Testbővítés

3.1.1. Definíció. Az L testet a K **test bővítésének** nevezzük, ha K részteste L -nek: $K \leq L$.
Jelölés: $L \mid K$. ♣

Például $\mathbb{R} \mid \mathbb{Q}$ és $\mathbb{C} \mid \mathbb{R}$, hiszen $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

3.1.1. Példa. $\mathbb{R} \mid \{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}$. Az világos, hogy a jobboldali halmaz részhalmaza \mathbb{R} -nek. Azt kellene még belátni, hogy testet is alkot, és akkor igaz volna, hogy \mathbb{R} az ő bővítése:

- Összeadásra zárt: $a + b\sqrt{2} + c + d\sqrt{2} = (a + c) + (b + d)\sqrt{2}$
- Szorzásra zárt: $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$ és $ac + 2bd \in \mathbb{Q}$ és $ad + bc \in \mathbb{Q}$
- Kommutativitás, asszociativitás, disztributivitás nyilván teljesül.
- Nullelem: $0 = 0 + 0\sqrt{2}$
- Egységelem: $1 = 1 + 0\sqrt{2}$
- Van ellentettje minden elemnek: $a + b\sqrt{2}$ ellentettje $-a - b\sqrt{2}$ is halmazbeli
- Van inverze minden nemnulla elemnek: Ha $a + b\sqrt{2} \neq 0$, akkor $a - b\sqrt{2} \neq 0$. Különben ha $a - b\sqrt{2} = 0$ volna, akkor két eset lenne lehetséges. Az egyik, hogy $b = 0$, ekkor viszont $a = 0$ is teljesül, ami ellentmond annak, hogy $a + b\sqrt{2} \neq 0$. A másik, hogy $b \neq 0$, ekkor $\sqrt{2} = \frac{a}{b}$ racionális volna, ami szintén nem lehetséges. Tehát biztosan bővíthetünk konjugálttal:

$$\frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2} \cdot \sqrt{2}$$

ahol $\frac{a}{a^2 - 2b^2} \in \mathbb{Q}$ és $\frac{-b}{a^2 - 2b^2} \in \mathbb{Q}$, tehát nemnulla elemeknek létezik inverze.

Ezt az előbb vizsgált furcsa halmazt jelöljük mostantól $\mathbb{Q}(\sqrt{2})$ -vel. Belátható, hogy ez a jelölés összhangban van a múlt órai $K(\alpha)$ racionális törtfüggvényekre bevezetett jelöléssel. A racionális törtfüggvények fogalmáig is úgy jutottunk el múlt előadáson, hogy bővíteni szerettünk volna egy testet egy rajta kívüli elemmel és meg akartuk találni a legszűkebb, testaxiómáknak eleget tevő halmazt. Megtehetjük ezt egyszerre több elemmel is. Korábbi tanulmányoknak megfelelően a generálás fogalmát vezetjük be most testelemekre is.

3.1.2. Definíció. Legyen $L | K$ testbővítés és $\alpha, \beta, \dots \in L$. Ekkor a K és az α, β, \dots elemek által **generált résztest** az L test legszűkebb olyan részteste, mely K -t és az α, β, \dots elemeket is tartalmazza. Jelölés: $K(\alpha, \beta, \dots)$. Ha csupán egy elemmel bővítünk, azt **egyszerű** bővítésnek nevezzük¹. Ennek a jelölése $K(\alpha)$. ♣

Átfogalmazva a generált résztest az adott K testet és α, β, \dots elemeket tartalmazó testek metszete. Persze ellenőrizendő most is a definíció értelmessége: A tavalyiakhoz (generált altér, részcsoport) hasonlóan látható be a következő tétel.

3.1.1. Tétel. Testek metszete is test. ♣

3.1.1. Állítás. Ha $L | K$ testbővítés, akkor L tekinthető egy vektortérnek K felett. ♣

Az állítás igazolásához ellenőrizni kellene a 8 vektortér axiómát, melyek nyilván teljesülnek.

3.1.3. Definíció. Az $L | K$ testbővítés **foka** az K fölötti L vektortér dimenziója: $\dim_K L$. Az $L | K$ bővítés **véges**, ha a foka véges. ♣

Például $\dim_{\mathbb{R}} \mathbb{C} = 2$, hiszen ahogy tavaly is tanultuk az 1 és az i komplex számok bázist alkotnak. Hasonlóan gondolható végig, hogy $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$ (az 1 és a $\sqrt{2}$ bázist alkotnak). Azt is kimondtuk (bizonyítás nélkül) tavaly, hogy \mathbb{R} vektortér \mathbb{Q} fölött végtelen dimenziós. Most analóg módon azt mondhatjuk, hogy $\dim_{\mathbb{Q}} \mathbb{R} = \infty$, vagyis az $\mathbb{R} | \mathbb{Q}$ testbővítés végtelen fokú.

3.1.2. Tétel (Testbővítések fokszámtétele). Legyen $K \leq L \leq M$ testbővítések sorozata. Ekkor $\dim_K M = \dim_K L \cdot \dim_L M$, azaz a bővítések foka szorozódik. ♣

Bizonyítás. Először külön vizsgáljuk ha a jobboldal valamelyike végtelen.

I. eset: $\dim_K L = \infty$ vagy $\dim_L M = \infty$

Ha $\dim_K L = \infty$, akkor L -ben kiválasztható végtelen sok független vektor. De $L \subseteq M$, vagyis ezek mind benne vannak M -ben is, tehát M -ben kiválasztható végtelen sok független vektor: $\dim_K M = \infty$

Ha $\dim_L M = \infty$, akkor M -ben kiválasztható végtelen sok független vektor. Ez azt jelenti, hogy azokat akármilyen L beli együtthatóval látom el, csakis úgy lehet a lineáris kombinációjuk 0, ha mindegyik együttható 0. De akkor ha L helyett annak részalmazából, K -ból választhatok csak együtthatókat, akkor továbbra is csak 0 együtthatókkal érhetem el, hogy a lineáris kombináció 0 legyen. Tehát függetlenek maradnak L helyett K felett is a vektorok: M -et K felett tekintve van egy végtelen független rendszerem: $\dim_K M = \infty$

¹Az egy elemmel bővítés úgy értendő, hogy $\exists \alpha$ melyre $L | K$ bővítésből $L = K(\alpha)$, vagyis a nagyobb test megadható a kisebb egy elemmel való bővítésével. Hiszen mondhatnánk, hogy $\mathbb{Q}(\sqrt{2}) | \mathbb{Q}$ bővítés esetén például a $\sqrt{2}$ és az $1 + \sqrt{2}$ is bekerült a halmazba (utóbbi az összeadásra való zártság miatt), de jobb szeretnénk mi ezt 1 elemmel való bővítésnek nevezni: $\mathbb{Q}(\sqrt{2}, 1 + \sqrt{2}) = \mathbb{Q}(\sqrt{2})$.

II. eset: $\dim_K L = s < \infty$ és $\dim_L M = t < \infty$

Legyen b_1, \dots, b_s bázisa L -nek K felett és c_1, \dots, c_t bázisa M -nek L felett. Ekkor azt állítom, hogy

$$\{b_i \cdot c_j \mid 1 \leq i \leq s, 1 \leq j \leq t\}$$

bázisa M -nek K felett. Azt kell belátnunk, hogy független és generátorrendszer. Ha ez megvan, onnan a tétel automatikusan következik, hiszen ez $s \cdot t$ darab vektor, melyek bázist alkotnak, tehát a dimenzió $s \cdot t$.

- Függetlenség:

Legyen

$$\sum_{i,j} k_{ij} \cdot b_i c_j = 0$$

Azt kell belátnunk, hogy ekkor minden $k_{ij} = 0$. Írjuk ki a szummát, hogy lássuk is miről van szó:

$$k_{11} \cdot b_1 c_1 + k_{12} \cdot b_1 c_2 + \dots + k_{1t} \cdot b_1 c_t + k_{21} \cdot b_2 c_1 + \dots + k_{st} \cdot b_s c_t = 0$$

Csoportosítunk bal oldalon c_j -k szerint:

$$\underbrace{(k_{11}b_1 + k_{21}b_2 + \dots + k_{s1}b_s)}_0 \cdot c_1 + \underbrace{(\dots)}_0 \cdot c_2 + \dots + \underbrace{(k_{1t}b_1 + k_{2t}b_2 + \dots + k_{st}b_s)}_0 \cdot c_t = 0$$

Mivel c_j -k bázist alkotnak, lineáris kombinációjuk csak akkor lehet 0, amennyiben minden együttható 0. Viszont b_i -k is bázist alkotnak, ez rájuk is igaz.

$$\Rightarrow k_{11} \cdot b_1 + k_{21} \cdot b_2 + \dots + k_{s1} \cdot b_s = 0 \Rightarrow k_{11} = k_{21} = \dots = k_{s1} = 0$$

Hasonlóan a többi c_j együttható esetében is. Megkaptuk tehát, hogy $\forall k_{ij} = 0$.

- Generálás:

Legyen $m \in M$ tetszőleges. Azt kellene megmutatnunk, hogy léteznek olyan k_{ij} együtthatók, melyekre

$$k_{11} \cdot b_1 c_1 + k_{12} \cdot b_1 c_2 + \dots + k_{st} \cdot b_s c_t = m$$

Hát ha nem is tudunk ilyen k_{ij} együtthatókat azonnal, azt tudjuk, hogy c_1, \dots, c_t generátorrendszer M -ben (mert bázis), tehát léteznek olyan $l_1, \dots, l_t \in L$ elemek, melyekre

$$l_1 \cdot c_1 + \dots + l_t \cdot c_t = m \quad (3.1.1)$$

előáll. Továbbá b_1, \dots, b_s generátorrendszer L -ben, tehát bármelyik $l_i \in L$ elem esetén kifejezhető azok lineáris kombinációjával, vagyis léteznek olyan $k_{1i}, \dots, k_{si} \in K$ elemek, melyekre

$$l_i = k_{1i} \cdot b_1 + k_{2i} \cdot b_2 + \dots + k_{si} \cdot b_s$$

Helyettesítve (3.1.1) egyenletbe minden l_i helyére a most kapott kifejezést és elvégezve a szorzásokat, végül $b_i c_j$ elemek lineáris kombinációját kapjuk K -beli együtthatókkal. Pont ezt szerettük volna.



3.2. Algebrai bővítés

Bevezettük előző órán a K test feletti algebrai szám fogalmát. Egy apró észrevétel, hogy K összes eleme algebrai K felett, hiszen $\forall \alpha \in K$ esetén tudunk mutatni olyan $f \neq 0$ polinomot K fölött, melynek gyöke az α , például: $x - \alpha$ ilyen. Ezért vizsgálni valamiről, hogy algebrai vagy sem K fölött akkor izgalmas, ha maga az elem nincs benne a K -ban.

3.2.1. Tétel. Ha $L \mid K$ egy véges bővítés $\Rightarrow \forall l \in L$ algebrai K felett. ♣

Bizonyítás. Legyen a bővítés foka $\dim_K L = d < \infty$. Tekintsük az $1, l, l^2, \dots, l^d \in L$ elemeket. Ez $d + 1$ darab elem, tehát L -beli vektorként tekintve rájuk összefüggő rendszert alkotnak (hiszen d dimenziós L , vagyis annál több vektor már biztosan összefüggő). Ekkor viszont $\exists k_0, k_1, \dots, k_d \in K$ nem mindannyian 0 skalárok, melyekre

$$k_0 \cdot 1 + k_1 \cdot l + k_2 \cdot l^2 + \dots + k_d \cdot l^d = 0$$

ez viszont éppen azt jelenti, hogy a

$$k_0 + k_1 \cdot x + k_2 \cdot x^2 + \dots + k_d \cdot x^d \in K[x]$$

polinomnak gyöke az l , vagyis l algebrai K felett. ■

Az előző előadáson kimondtunk egy tételt, hogyan lehet leírni egy test egyetlen algebrai elemmel való bővítését. Az 2.5.2. tételt mondjuk ki újra, és most lássuk is be.

3.2.2. Tétel. Ha α algebrai K fölött, akkor $K(\alpha) = K[\alpha]$. ♣

Bizonyítás. Mivel α algebrai, ezért létezik neki minimálpolinomja, jelölje ezt m_α . Annak foka legyen $d = \deg m_\alpha$. Tekintsük a következő halmazt:

$$T = \{a_0 + a_1 \alpha + \dots + a_{d-1} \alpha^{d-1} \mid a_0, a_1, \dots, a_{d-1} \in K\}$$

Azt fogjuk belátni, hogy $T = K(\alpha)$. Azt mondtuk, hogy $K(\alpha)$ a K test elemeit és az α elemet tartalmazó testek metszete. Ha egy L test tartalmazza K elemeit és α -t is, akkor a most definiált halmaz összes elemét is. Tehát a metszet minden egyes tagja tartalmazza T -t, akkor végül $K(\alpha)$ is, ezzel beláttuk, hogy $T \subseteq K(\alpha)$.

Elég lesz azt belátnunk, hogy T egy test, hiszen mivel $K(\alpha)$ metszete a K elemeit és az α elemet tartalmazó testeknek, a metszendő elemek egyike T , és a metszet mindig részhalmaza a metszendő elemek mindegyikének, így: $K(\alpha) \subseteq T$ teljesülne.

A testaxiómák közül az világos, hogy zárt az összeadásra, van egységelem, ellentett. Szorzat esetén miért lehetünk benne biztosak, hogy $f, g \in T$ esetén $f \cdot g \in T$? A problémát egy dolog jelenthetné, ha megjelenne a szorzatban egy $d - 1$ -nél magasabb fokú tag is. Mint azonban korábban már láttuk, ekkor α^d kifejezhető volna kisebb hatványok segítségével, hiszen:

$$m_\alpha = m_0 + m_1 x + \dots + m_d x^d$$

minimálpolinomba helyettesítve α -t

$$0 = m_\alpha(\alpha) = m_0 + m_1 \alpha + \dots + m_d \alpha^d$$

egyenletből kifejezhető α^d . Hasonlóan magasabb hatványai is az α -nak visszavezethetők legfeljebb $d - 1$ fokúakra. Ez az oka annak is, hogy $T = K[\alpha]$.

Az igazi kérdés a test tulajdonságok közül tehát a reciprokok maradt. Azt kell belátnunk, hogy ha az ellenség ad egy $p(\alpha) \in T$ elemet ($p \neq 0$), akkor mi tudunk neki mutatni egy $q(\alpha) \in T$ elemet, amelyre $p(\alpha) \cdot q(\alpha) = 1$.

Mivel $p(\alpha) \in T$, ezért $\deg p \leq d - 1$. Ugyanakkor azt is tudjuk, hogy m_α felbonthatatlan K fölött. Ez azt jelenti, hogy csupán 2 osztója van: 1 és önmaga. Mi lehet akkor (p, m_α) ? Nem lehet m_α , hiszen $\deg p \leq d - 1 < d = \deg m_\alpha$. Akkor ez csak az 1 lehet. Az euklideszi algoritmus következménye miatt a legnagyobb közös osztó felírható a polinomok lineáris kombinációjaként: $\exists q_1, q_2 \in K[x]$ melyekre

$$p \cdot q_1 + m_\alpha \cdot q_2 = 1$$

Ahonnán α -t helyettesítve kapjuk, hogy

$$p(\alpha) \cdot q_1(\alpha) + \underbrace{m_\alpha(\alpha) \cdot q_2(\alpha)}_0 = 1$$

vagyis

$$p(\alpha) \cdot q_1(\alpha) = 1$$

ami éppen azt jelenti, hogy $q = q_1$ választással megkaptuk $p(\alpha)$ reciprokat.

Rakjuk össze tehát mi mindenünk van: $T = K[\alpha]$, $T \subseteq K(\alpha)$ és $K(\alpha) \subseteq T$. Ezekből láthatóan következik, hogy $K(\alpha) = K[\alpha]$. ■

3.2.3. Tétel. Ha $L \mid K$ testbővítés és $\alpha \in L$ algebrai K fölött \Rightarrow a $K(\alpha) \mid K$ bővítés véges, és foka: $\dim_K K(\alpha) = \deg m_\alpha$. ♣

Bizonyítás. Az előző bizonyításhoz hasonlóan legyen $d = \deg m_\alpha$. Elegendő azt belátnunk, hogy az

$$1, \alpha, \alpha^2, \dots, \alpha^{d-1}$$

egy bázisa $K(\alpha)$ -nak és mivel ez d darab elem, így igazolnánk is ezt a tételt. A bázis tulajdonság ekvivalens azzal, hogy segítségével minden egyértelműen áll elő. Ebből az előző bizonyításban már láttuk, hogy K test α -val bővített testének minden eleme előáll ezek lineáris kombinációjaként. Elegendő volna az egyértelműséget igazolni.

Tegyük fel, hogy valami kétféleképpen előáll lineáris kombinációként:

$$a_0 + a_1 \alpha + \dots + a_{d-1} \alpha^{d-1} = b_0 + b_1 \alpha + \dots + b_{d-1} \alpha^{d-1}$$

átrendezve

$$(a_0 - b_0) + (a_1 - b_1) \cdot \alpha + \dots + (a_{d-1} - b_{d-1}) \cdot \alpha^{d-1} = 0$$

ahonnán következik, hogy $\forall a_i = b_i$. Hiszen azt látjuk, hogy egy $d - 1$ fokú polinom helyettesítési értéke α helyen 0. Ez akkor csakis a 0 polinom lehet, különben ellentmondanánk azzal, hogy a minimálpolinom d -fokú (találnánk nála kisebb fokút, aminek gyöke az α). ■

3.2.1. Definíció. Az $L \mid K$ algebrai bővítés, ha $\forall \alpha \in L$ algebrai K felett. Ha egy bővítés nem algebrai, akkor **transzcendensnek** nevezzük. ♣

3.2.4. Tétel. Ha α algebrai K felett \Rightarrow a $K(\alpha) \mid K$ algebrai bővítés. ♣

Bizonyítás. Ez közvetlen következménye a 3.2.3 és 3.2.1 tételeknek. Ha α algebrai K felett, akkor $K(\alpha) \mid K$ bővítés véges, márpedig véges bővítés esetén $L = K(\alpha)$ speciális esettel a bővebb $K(\alpha)$ test minden eleme algebrai a szűkebb K fölött. ■

3.2.5. Tétel. Minden transzcendens bővítés végtelen dimenziós. ♣

Bizonyítás. Ha az $L \mid K$ bővítés transzcendens, akkor $\exists \alpha \in L$ elem, amely transzcendens K fölött. Ez azt jelenti, hogy nincs olyan nemnulla polinom, melynek gyöke lenne az α .

Ekkor viszont α hatványaiból bármilyen véges sokat véve azok független rendszert alkotnak. Hiszen ha $1, \alpha, \alpha^2, \dots, \alpha^n$ összefüggő volna, akkor $\exists a_0, a_1, \dots, a_n \in K$ nem mind nulla számok, melyre

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$$

volna, vagyis az

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$$

nemnulla polinomnak gyöke volna az α , ami ellentmondás, hiszen feltettük, hogy α transzcendens K fölött.

Viszont ha α hatványaiból akárhányat is véve azok független rendszert alkotnak, akkor találtunk egy végtelen sok elemű független rendszert, a dimenzió végtelen. ■

Transzcendens bővítés esetén tehát nem elegendő a polinomokkal foglalkoznunk, hanem a racionális törtfüggvények is szerepet kapnak. Előző előadáson láttuk alapján azok segítségével írható le egy transzcendens elemmel való bővítés: Például ha a racionális számok halmazát szeretnénk bővíteni a π transzcendens elemmel, akkor a

$$\mathbb{Q}(\pi) = \left\{ \frac{p(\pi)}{q(\pi)} \mid p, q \in \mathbb{Q}[x], q(\pi) \neq 0 \right\}$$

halmaz írja ezt le.

3.3. Mátrixok és egyenletrendszerek

Ez a fejezet főleg emlékekről fog szólni, de néhány új fogalommal, állítással is találkoztunk még az óra végén. Átismételtük a mátrix rangjának a fogalmát: oszloprang = maximális független oszlopvektorok száma, sorrang hasonlóan a sorokra. Visszaemlékeztünk, hogy ezek egyenlőek és ráadásul a determinánsranggal is megegyeznek. Ez volt az első új fogalom, mely nem pontosan az általam leírt formában hangzott el, de Freud Róbert: Lineáris algebra című könyvében hasonlóan található meg.

3.3.1. Definíció. Egy $n \times n$ -es mátrix **aldeterminánsának** nevezzük egy rész mátrixának a determinánsát. Vagyis amit úgy kapunk, hogy az eredeti mátrixból választunk valahány oszlopot és ugyanennyi sort, majd a közös részükből képzett mátrix determinánsát vesszük. A választott oszlopok száma az **aldetermináns rendje**. ♣

3.3.2. Definíció (Freud R. 3.4.1.). Egy A mátrix **determinánsrangja** r , ha van olyan $r \times r$ -es aldeterminánsa, ami nem nulla, de bármely r -nél nagyobb rendű aldeterminánsa (ha egyáltalán van ilyen) már nulla. ♣

Ezután egy szintén tavaly tanult és bizonyított állításról volt szó. A most következő részt a tavalyi jegyzetből másolom.

3.3.1. Tétel (Ismétlés). Ha van egy $A \in T^{k \times n}$ mátrix, akkor $r(A) = \dim \operatorname{Im}(A)$, vagyis mátrix rangja megegyezik a hozzátartozó lineáris leképezés képterének dimenziójával. ♣

Bizonyítás. Hogyan szorzunk meg egy mátrixot egy oszlopvektorral jobbról?

$$[\mathbf{a}_1 \quad \mathbf{a}_2 \quad \dots \quad \mathbf{a}_n] \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha_1 \cdot \mathbf{a}_1 + \alpha_2 \cdot \mathbf{a}_2 + \dots + \alpha_n \cdot \mathbf{a}_n$$

Azt látjuk tehát, hogy a szorzat az eredeti mátrix oszlopvektorainak lineáris kombinációja lesz.

Tekintsük a következő leképezést: Legyen A mátrix rögzített, oszlopvektorai $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ és tetszőleges \mathbf{x} vektor képe legyen $\varphi(\mathbf{x}) = A \cdot \mathbf{x}$. Könnyen látható, hogy ez egy lineáris leképezés. Az kell, hogy összeg képe a képek összege

$$\varphi(\mathbf{x}_1 + \mathbf{x}_2) = A \cdot (\mathbf{x}_1 + \mathbf{x}_2) = A \cdot \mathbf{x}_1 + A \cdot \mathbf{x}_2 = \varphi(\mathbf{x}_1) + \varphi(\mathbf{x}_2)$$

és skalárszoros képe a kép skalárszorosa

$$\varphi(\lambda \cdot \mathbf{x}) = A \cdot (\lambda \cdot \mathbf{x}) = \lambda \cdot (A \cdot \mathbf{x}) = \lambda \cdot \varphi(\mathbf{x})$$

Márpedig, ha ez egy lineáris leképezés, akkor van neki képtere. Az micsoda?

A képtér azon vektorok halmaza, melyek előállnak képként, vagyis azon \mathbf{b} vektorok amelyekre $\exists \mathbf{x}$ vektor, hogy $A \cdot \mathbf{x} = \mathbf{b}$, vagyis melyek esetén az $A \cdot \mathbf{x} = \mathbf{b}$ lineáris egyenletrendszer megoldható. Másképpen fogalmazva a képtér azon vektorok halmaza, melyek előállnak lineáris kombinációjaként az $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ vektoroknak, ez pedig éppen az általuk generált altér: $\operatorname{Im}(\varphi) = \langle \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \rangle$.

Ha pedig ezek megegyeznek, akkor dimenziójuk is:

$$\dim \operatorname{Im}(\varphi) = \overbrace{\dim \langle \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \rangle}^{\text{def}} = r(A)$$

■

3.3.2. Tétel. Az $A \cdot \mathbf{x} = \mathbf{b}$ lineáris egyenletrendszernek pontosan akkor létezik megoldása T -ben, ha $r(A) = r(A|\mathbf{b})$, ahol $[A|\mathbf{b}]$ mátrix alatt az A mátrix \mathbf{b} oszlopvektorral való kiegészítését értjük. ♣

Bizonyítás. Pontosán akkor van megoldás, ha $\mathbf{b} \in \operatorname{Im}(A)$, ami azzal ekvivalens, hogy \mathbf{b} függ A oszlopvektoraitól. Tehát őt is hozzájuk véve az $\operatorname{Im}(A)$ nem változik, vagyis annak dimenziója (ami a rang) sem változik. ■

Szintén ismétlés, hogy ha adott egy lineáris egyenletrendszernek az egyik megoldása és a homogenizált változat megoldásai, abból hogyan kaphatjuk meg az eredeti összes megoldását.

3.3.1. Állítás. Legyen $A \cdot \mathbf{x} = \mathbf{b}$ egyenletrendszer egyik megoldása \mathbf{x}_0 , továbbá az $A \cdot \mathbf{x} = \mathbf{0}$ egyik megoldása \mathbf{h} . Ekkor $\mathbf{x}_0 + \mathbf{h}$ is megoldása az eredeti egyenletrendszernek. ♣

Bizonyítás. Azt kell belátnunk, hogy $A \cdot (\mathbf{x}_0 + \mathbf{h}) = \mathbf{b}$. Bal oldalt felbontva a zárójelet majd kihasználva, hogy \mathbf{x}_0 partikuláris megoldás, \mathbf{h} pedig megoldása a homogénnek:

$$A \cdot (\mathbf{x}_0 + \mathbf{h}) = A \cdot \mathbf{x}_0 + A \cdot \mathbf{h} = \mathbf{b} + \mathbf{0} = \mathbf{b}$$

ami éppen azt jelenti, hogy $\mathbf{x}_0 + \mathbf{h}$ megoldása az eredeti egyenletrendszernek. ■

Fontos szerepet játszanak tehát a homogén lineáris egyenletrendszerek is. Visszatérve oda, hogy ha $A \in T^{k \times n}$ mátrixot egy lineáris leképezésnek feleltetjük meg, akkor $A: T^n \rightarrow T^k$ képez. Azt már láttuk, hogy a leképezés képtere azon vektorok halmaza, melyek esetén $A \cdot \mathbf{x} = \mathbf{b}$ -nek van megoldása, de mi a magtér?

A magtér azon vektorok halmaza, melyek $\mathbf{0}$ -ba képződnek, vagyis megoldásai az $A \cdot \mathbf{x} = \mathbf{0}$ homogén LER²-nek. A mag dimenziója és a rang között is kaphatunk összefüggést.

3.3.3. Tétel. Legyen $A \in T^{k \times n}$, azaz A mátrix egy $T^n \rightarrow T^k$ lineáris leképezésnek felel meg. Ekkor $\dim \text{Ker}(A) = n - r(A)$. ♣

Bizonyítás. Írjuk fel a tavalyi félévben, lineáris leképezések magtere és képtere közti kapcsolatra tanult dimenziótételt. $A: V_1 \rightarrow V_2$ lineáris leképezés esetén

$$\dim \text{Ker}(A) + \dim \text{Im}(A) = \dim V_1$$

ahol most $V_1 = T^n$, vagyis n dimenziós. A 3.3.1 tétel miatt $\dim \text{Im}(A) = r(A)$, ezeket helyettesítve

$$\dim \text{Ker}(A) + r(A) = n$$

ami éppen a bizonyítandó állítás. ■

²A továbbiakban a „lineáris egyenletrendszer” kifejezést LER rövidítéssel illetem

4. előadás

Szerkesztés

4.1. Algebrai zártság

4.1.1. Definíció. A \mathbb{Q} és a \mathbb{Z}_p testeket **prímtestek**nek nevezzük.



A 2.4.3. tétel szerint minden testben van tehát egy prímtest. Tehát innentől fogva, ha van egy K testünk, akkor az mindig bővítése egyiknek: $K \mid \mathbb{Q}$ vagy $K \mid \mathbb{Z}_p$. Továbbiakban ha mást nem mondunk, akkor \mathbb{Q} bővítéseiről beszélünk.

Egy $L \mid K$ testbővítés fokát az előző előadáson $\dim_K L$ jelöléssel illettük, a továbbiakban ugyanerre a fogalomra vonatkoznak az $[L : K]$ és a $\dim(L \mid K)$ jelölések is.¹

Múlt órán tárgyaltuk az algebrai elemmel való bővítés leírását is:

$$K(\alpha) = \{a_0 + a_1 \cdot \alpha + \dots + a_{n-1} \cdot \alpha^{n-1} \mid n = \deg m_\alpha, a_i \in K\}$$

4.1.2. Definíció. Egy K testet **algebrailag zárt**nak nevezünk, ha $\forall f \in K[x], \deg f \neq 0$ polinomnak van gyöke K -ban.



4.1.1. Tétel. Ha K algebrailag zárt és $f \in K[x]$, akkor ekvivalensek a következő állítások:

1. $\deg f \geq 1 \Rightarrow \exists$ gyöke
2. $\deg f = n \Rightarrow n$ gyöke van
3. $f(x) = a_n \cdot (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$
4. Az irreducibilis polinomok pont az 1-fokúak



Bizonyítás. Amennyiben $\deg f = 1$, akkor látható, hogy az állítások ekvivalensek. Hiszen ha $f = ax + b$, akkor nyilván van gyöke: $-\frac{b}{a}$, pontosan 1 gyöke van, felírható a gyöktényezőss alakja: $f(x) = a \cdot (x - \frac{b}{a})$, és irreducibilis, hiszen bármely test fölötti 1-fokú polinomok irreducibilisek.

¹Testbővítések fokszámtételét például nekem könnyebb volt a második jelöléssel megjegyezni. Olyan mintha egy egyszerűsítés miatt esne ki egy osztásból a középső test: $[M : K] = [M : L] \cdot [L : K]$.

Ha pedig $\deg f > 1$ és algebrailag zárt (tehát teljesül az 1. állítás), abból következik a másik három is.

Hiszen ha a foka legalább 1 és van gyöke, akkor emeljük ki gyöktényezőként, ezzel kaptunk egy $\deg f - 1$ fokú polinomot, aminek foka még mindig ≥ 1 . Addig ismételgessük ezt a kiemelgetést, amíg 1-fokút nem kapunk. Értelem szerűen ha kezdetben a fok n volt, akkor $n - 1$ -szer kell ezt megtennünk és végül a maradék tényezőnek is lesz még egy gyöke, tehát összesen n gyöke van f -nek.

A kiemelgetések folyamatával előállítottuk a gyöktényező alakot, és azt is láttuk, hogy ha f foka nagyobb mint 1, akkor mindig kiemelhető elsőfokú tag, tehát f nem irreducibilis. Vagyis pontosan az 1-fokúak irreducibilisek (konstans azért nem lehet irreducibilis, mert test fölött a konstansok egységek vagy a 0 polinom). ■

4.1.1. Lemma. α algebrai K fölött $\Leftrightarrow |K(\alpha) : K| < \infty$. ♣

Bizonyítás. Mindkét irányt láttuk már egy korábbi tételben.

\Leftarrow

Indirekt tegyük fel, hogy α transzcendens. De a 3.2.5. tétel miatt ekkor a $K(\alpha) | K$ bővítés végtelen dimenziós lenne, amiről feltettük, hogy véges.

\Rightarrow

A 3.2.3. tétel éppen azt mondja hogy ha α algebrai, akkor a $K(\alpha) | K$ bővítés véges. ■

A továbbiakra való tekintettel jegyezzük meg, hogy $K(\alpha, \beta) = K(\alpha)(\beta) = K(\beta)(\alpha)$, hiszen mindegy, hogy egyszerre bővítek α és β elemekkel, vagy először α , utána β elemmel, vagy először β majd α elemekkel.

4.1.2. Tétel. Ha α és β algebraiak K fölött, akkor $|K(\alpha, \beta) : K| \leq |K(\alpha) : K| \cdot |K(\beta) : K|$. ♣

Bizonyítás. Az, hogy egyszerre bővítek két algebrai elemmel ugyanaz, mintha külön-külön lépésenként bővítenék velük. Van a K testem és azt először α , majd β elemmel bővítem: $K(\alpha) | K$ majd $K(\alpha)(\beta) | K(\alpha)$.

Legyen K fölött az α minimálpolinomja m_α , valamint β minimálpolinomja m_β . Ekkor az első $K(\alpha) | K$ bővitésem foka $\deg m_\alpha$. A második $K(\alpha)(\beta) | K(\alpha)$ bővítés esetén pedig felső korlát $\deg m_\beta$. Hiszen mivel $K \leq K(\alpha)$, ezért ha K együtthatókkal találtunk egy m_β polinomot aminek gyöke a β , akkor annak együtthatói benne vannak $K(\alpha)$ -ban is, a minimálpolinom $K(\alpha)$ fölött biztosan nem nagyobb fokú (kisebb lehet, hiszen m_β nem biztos hogy irreducibilis $K(\alpha)$ fölött).

Ezzel azt láttuk, hogy $|K(\alpha, \beta) : K(\alpha)| \leq |K(\beta) : K|$. Használva a testbővítések fokszámtételét már meg is van a bizonyítandó:

$$|K(\alpha, \beta) : K| = |K(\alpha, \beta) : K(\alpha)| \cdot |K(\alpha) : K| \leq |K(\beta) : K| \cdot |K(\alpha) : K|$$

■

Például hogyan mondanánk meg mennyi $d = |\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}|$? Mivel $m_{\sqrt{2}} = x^2 - 2$ és $m_{\sqrt[3]{2}} = x^3 - 2$, ezért az előző tétel miatt a bővítés foka $d \leq 2 \cdot 3 = 6$.

Közelítsük meg a problémát 2 oldalról. Először képzeljük el, hogy $\sqrt{2}$ -vel bővítettük a \mathbb{Q} -t, utána hogy azt tovább $\sqrt[3]{2}$ -vel. Itt az első bővítés dimenzióját tudjuk: $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$. A másodikról most nem tudunk semmit, legyen egyszerűen

$$d_1 = |\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})|$$

Ekkor a testbővítések fokszámtétele miatt

$$d = |\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = d_1 \cdot 2$$

Hasonlóan végiggondolható, hogy mi történik, ha először $\sqrt[3]{2}$ -vel bővítünk:

$$d = |\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})| \cdot |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = d_2 \cdot 3$$

Rakjuk össze mit tudunk d -ről:

$$d \leq 6 \quad d = 2 \cdot d_1 \quad d = 3 \cdot d_2$$

Mivel $2 \mid d$ és $3 \mid d$, ezért $6 \mid d$, ugyanakkor d legfeljebb 6, tehát $d = 6$.

4.1.3. Definíció. Jelölés: \mathbb{A} jelöli az **algebrai számok halmazát**, vagyis

$$\mathbb{A} = \{\alpha \in \mathbb{C} \mid \exists f \in \mathbb{Q}[x], f \neq 0, f(\alpha) = 0\}$$



4.1.3. Tétel. Az algebrai számok algebrailag zárt testet alkotnak.



Bizonyítás. Két lépésben bizonyítunk, először a test tulajdonságot, majd az algebrai zárttságot.

Test biz.:

Mivel $\mathbb{A} \subseteq \mathbb{C}$, ezért a testaxiómák közül csomó automatikusan teljesül. Hiszen nyilván ha a komplex számok halmazán teljesül, hogy a szorzás asszociatív, akkor ebben a részhalmazban is teljesülni fog. Azt kell tehát csak belátnunk, hogy zárt az összeadásra, szorzásra, ellentett- és reciprokképzésre, vagyis $\alpha, \beta \in \mathbb{A}$ esetén $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$ és $\alpha \neq 0$ esetén $\frac{1}{\alpha}$ is algebrai.

Legyenek α és β algebrai elemek. A 4.1.1. lemma szerint ez pontosan azt jelenti, hogy

$$|K(\alpha) : K| = m < \infty \quad |K(\beta) : K| = n < \infty$$

Ekkor az előző 4.1.2. tétel szerint

$$|K(\alpha, \beta) : K| \leq n \cdot m < \infty$$

ami azt jelenti, hogy $K(\alpha, \beta) \mid K$ egy véges bővítés. Véges bővítés esetén a bővebb test minden eleme algebrai a szűkebb fölött a 3.2.1. tétel miatt.

Tehát azt kaptuk, hogy $K(\alpha, \beta)$ minden eleme algebrai K fölött. Ezzel kész is vagyunk, hiszen $K(\alpha, \beta)$ test, ami tartalmazza α és β számokat, tehát benne van $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$, és $\alpha \neq 0$ esetén $\frac{1}{\alpha}$ is.

Algebrai zártság biz.:

Azt kell belátnunk, hogy minden $f(x) \in \mathbb{A}[x]$, $\deg f \geq 1$ polinomnak van \mathbb{A} -beli gyöke.

Legyen $f(x) = x^n + \beta_{n-1} \cdot x^{n-1} + \dots + \beta_1 \cdot x + \beta_0$, ahol $\forall \beta_i \in \mathbb{A}$. Mivel $\mathbb{A} \subseteq \mathbb{C}$, ezért ez egyben egy komplex együtthatós polinom is. Neki tudjuk, hogy van gyöke \mathbb{C} -ben, legyen ez α . Azt kellene belátnunk, hogy α algebrai.

Fogjuk meg a \mathbb{Q} -t és kezdjük el bővíteni a polinom együtthatóival szépen sorban, ekkor végül kapunk egy K testet

$$K = \mathbb{Q}(\beta_0)(\beta_1) \dots (\beta_{n-1})$$

amiről a 4.1.2. tétel miatt tudjuk, hogy

$$|K : \mathbb{Q}| \leq \prod |\mathbb{Q}(\beta_i) : \mathbb{Q}| = |\mathbb{Q}(\beta_0) : \mathbb{Q}| \cdot |\mathbb{Q}(\beta_1) : \mathbb{Q}| \cdot \dots \cdot |\mathbb{Q}(\beta_{n-1}) : \mathbb{Q}|$$

Ezt egy picit magyarázom, mert ez a nehezebb gondolat. Ahogy folyamatosan bővítettünk úgy becsülgethetünk is, mindig leválasztunk jobboldalról 1-1 újabb tényezőt:

$$\overbrace{|\mathbb{Q}(\beta_0)(\beta_1) \dots (\beta_{n-2})(\beta_{n-1}) : \mathbb{Q}|}^K \stackrel{4.1.2. \text{ tétel}}{\leq} |\mathbb{Q}(\beta_0)(\beta_1) \dots (\beta_{n-2}) : \mathbb{Q}| \cdot |\mathbb{Q}(\beta_{n-1}) : \mathbb{Q}| \leq \dots$$

Innen már nem olyan nehéz a bizonyítás. Tudjuk, hogy minden β_i algebrai, tehát az összes $|\mathbb{Q}(\beta_i) : \mathbb{Q}|$ véges, vagyis a szorzatuk is, tehát $|K : \mathbb{Q}| < \infty$.

Másrészt $|K(\alpha) : K| < \infty$, hiszen α algebrai K fölött, mert gyöke az $f \in K[x]$ polinomnak.

A fokszámtételt használva innen következik, hogy

$$|K(\alpha) : \mathbb{Q}| = |K(\alpha) : K| \cdot |K : \mathbb{Q}| < \infty$$

azaz $|K(\alpha) : \mathbb{Q}|$ véges, a 3.2.1. tétel szerint ekkor $K(\alpha)$ minden eleme algebrai \mathbb{Q} fölött, tehát $\alpha \in \mathbb{A}$. ■

4.1.4. Tétel. Ha α algebrai β transzcendens, akkor $\alpha + \beta$ transzcendens és $\alpha \neq 0$ esetén $\alpha \cdot \beta$ is transzcendens. ♣

Bizonyítás. Indirekt tegyük fel, hogy $\alpha + \beta$ algebrai. Ekkor ebből kivonva az α algebrai számot azt kapnánk, hogy β . Viszont algebrai számok különbsége is algebrai kellene legyen, β ugyanakkor transzcendens, ami ellentmondás.

Hasonlóan $\alpha \cdot \beta = \gamma \in \mathbb{A}$ indirekt feltétellel indulva $\beta = \frac{\gamma}{\alpha}$ adódna, vagyis hogy β algebrai. ■

4.2. Euklideszi szerkesztés

Ebben a fejezetben az euklideszi-szerkesztést fogjuk algebrai szempontból vizsgálni.

Ismételjük át a lépéseit az euklideszi-szerkesztésnek:

- két ponton húzhatok egy egyenest

- két egyenes metszéspontját meg tudom határozni
- adott pont körül adott sugárral tudok kört rajzolni
- kör és egyenes metszéspontját meg tudom határozni
- két kör metszéspontját meg tudom határozni

Mikor tekintünk egy objektumot megszerkesztettnek? Geometriában úgy csináltuk, hogy **adott volt néhány pont és meg kellett szerkeszteni néhány új pontot**. De mondhatjuk, hogy egy háromszög már igazából megszerkesztett, ha ismerjük a 3 oldalát, hiszen ha azokat tudjuk, abból meg tudjuk szerkeszteni a háromszöget. Algebrailag tehát a szerkesztést számokkal fogjuk vizsgálni.

Fontos észrevétel: Nincs olyan euklideszi szerkesztési lépés, hogy "húzzunk egy egyenest" csak úgy random! Ahhoz szükséges legalább 2 pont, hogy azt az egyenest meg tudjuk szerkeszteni. Tehát valójában ha kezdetben csak 1 pont adott, akkor azzal semmit nem tudunk csinálni, innentől kezdve feltehető, hogy legalább 2 pontunk kezdetben is van.

Kössünk össze az adott pontok közül 2-t és egyiket 0-nak nevezzük $((0,0)$ koordinátákkal látjuk el), másikat 1-nek nevezzük $((1,0)$ koordinátákkal látjuk el). A 0-ból tudunk szerkeszteni a meglévő egyenesre merőleges egyenest, ezzel kaptunk egy koordináta-rendszert. Innentől kezdve gondolkozhatunk végig úgy, hogy minden alakzatunk egy koordináta-rendszerben adott, vagyis jellemezhetjük őket számokkal.

Minden pontot megadhatunk 2 számmal, a koordinátaival. Ha van egy egyenesem: $y = mx + b$, azt is megadhatjuk 2 számmal: meredekség és y tengelymetszet. Kört: $(x - u)^2 + (y - v)^2 = r^2$ megadhatunk 3 számmal: a K középpontjának 2 koordinátájával és az r sugarával. Vagyis az euklideszi szerkesztés lépéseiben szereplő összes objektum jellemezhető számokkal. Ha távolságot akarunk megadni, azt sem úgy tesszük, hogy 2 pontot adunk meg, hanem egy számot, ami az origótól való távolságot jelenti.

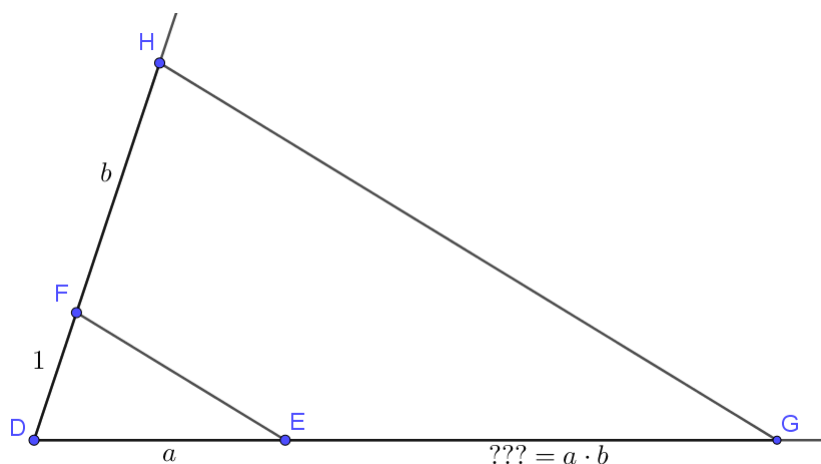
A szerkesztési feladat innentől kezdve úgy néz ki, hogy **vannak számok, és azokból új számokat kell szerkeszteni**.

4.2.1. Tétel. A számokkal lehet testműveleteket végezni és gyököt vonni, vagyis ha adott a és b számok megszerkesztettek, akkor meg tudjuk szerkeszteni az $a \pm b$, $a \cdot b$, $b \neq 0$ esetén $\frac{a}{b}$ és \sqrt{a} számokat is. ♣

Bizonyítás. Az összeg szerkesztése könnyű, az a után felmérem a b -t (különbség hasonlóan):



Szorzat szerkesztés a párhuzamos szelők tételén alapszik:

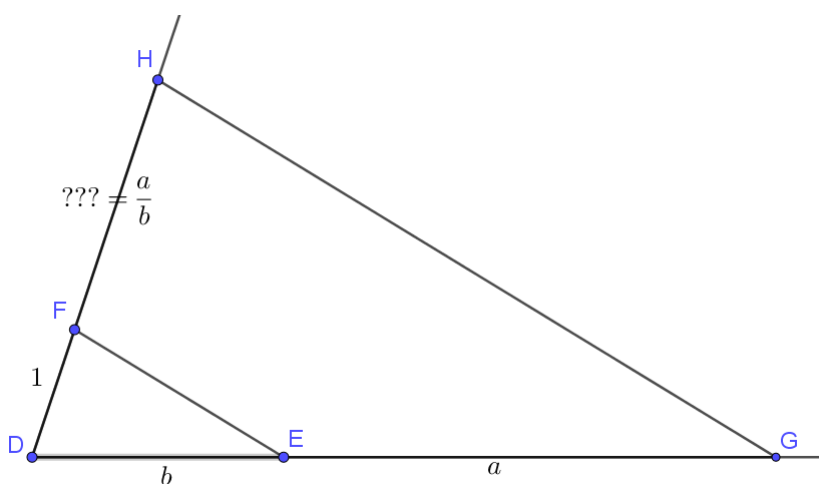


Hiszen ha

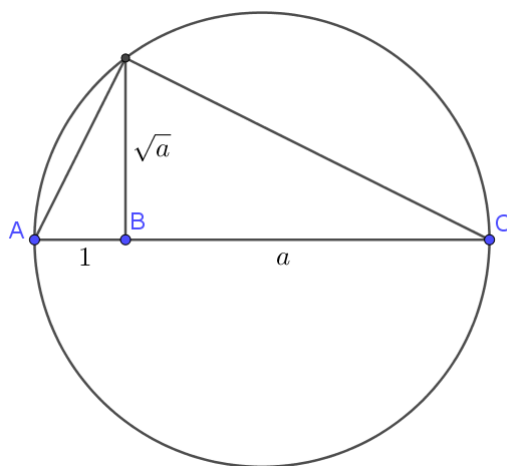
$$b = \frac{b}{1} = \frac{FH}{DF} = \frac{EG}{DE} = \frac{EG}{a}$$

akkor innen $EG = a \cdot b$ következik. Vagyis ha adott a és b (és persze az 1 távolság is adott, mert van origónk és $(1,0)$ pontunk, aminek segítségével vettük fel a koordináta-rendszert), akkor szorzatuk megszerkeszthető, ha EF egyenessel párhuzamost húzunk H ponton keresztül.

Hányados hasonlóan csak más szereposztással:



Végül \sqrt{a} megszerkesztése a magasságtétel miatt lehetséges:



Megszerkesztjük $1 + a$ szakaszt, majd köré Thalész-kört (AC szakasz felezőpontja a kör középpontja). Merőlegest állítunk B pontban és tekintjük a körrel az egyik metszéspontot. Ha összekötjük A és C pontokkal is, akkor olyan derékszögű háromszöget kapunk, aminek magassága éppen $m = \sqrt{1 \cdot a} = \sqrt{a}$. ■

Az előző állítás azt mondta, hogy ha meg tudjuk szerkeszteni egy K test minden elemét, és egy további γ számot is, akkor a $K(\gamma)$ bővebb test összes elemét meg tudjuk szerkeszteni biztosan (tudunk összeadni, kivonni, szorozni, osztani).

4.2.2. Tétel. Ha megszerkesztettük K test elemeit, akkor egyenesek metszéspontjaként, kör és egyenes metszéspontjaként és körök metszéspontjaként kapható új pont legfeljebb 2-fokú algebrai szám K fölött. ♣

Bizonyítás. Megvizsgáljuk mindhárom esetet egyesével.

Egyenesek metszéspontja:

Van 2 egyenesem (tegyük fel, hogy van metszéspontjuk), egyenleteik $(a, b, c, d \in K)$:

$$\begin{cases} y = ax + b \\ y = cx + d \end{cases}$$

akkor kivonva őket egymásból

$$0 = (a - c)x + b - d$$

és kifejezve x -et

$$x = \frac{d - b}{a - c} \in K$$

és $y = a \cdot \frac{d - b}{a - c} + b \in K$, tehát a keletkező metszéspont K testben van, a vele való bővítés 1-fokú.

Egyenes és kör:

Van egy egyenesem és egy köröm (megint csak feltéve, hogy kapunk új pontot, tehát van metszéspontjuk), egyenleteik $(a, b, c, m, t \in K)$:

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ y = mx + t \end{cases}$$

helyettesítve y -t az első egyenletbe

$$x^2 + (mx + t)^2 + ax + b(mx + t) + c = 0$$

rendezve

$$\underbrace{(m+1)}_A \cdot x^2 + \underbrace{(2mt + a + mb)}_B \cdot x + \underbrace{(t^2 + bt + c)}_C = 0$$

bevezetve A, B, C rövidítéseket

$$Ax^2 + Bx + C = 0$$

egyenlethez jutunk, ahonnan x -re kapható megoldás

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

ami egy legfeljebb 2-fokú algebrai szám K fölött, hiszen (a megoldóképletet fel se kellett volna írni) gyöke az $Ax^2 + Bx + C$ másodfokú polinomnak, aminek együtthatói K -beli elemek (tehát minimálpolinomja osztja ezt a másodfokú polinomot, vagyis legfeljebb 2-fokú).

Ha az $y = mx + t$ egyenletből x -et fejezzük ki és ugyanezt végigcsináljuk, akkor látszik, hogy y is legfeljebb 2-fokú algebrai szám.

Körök metszéspontja:

Van 2 körünk (metszik egymást), egyenleteik $(a, b, c, d, e, f \in K)$:

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases}$$

Kivonva az alsót a felsőből

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ (a-d)x + (b-e)y + c-f = 0 \end{cases}$$

adódik ahol a második egyenlet már egy egyenes egyenlete, tehát visszavezettük az előző esetre a kérdést, innen x és y már legfeljebb 2-fokú lehet. ■

A következőkben azon gondolkozzunk, hogy mi minden szerkeszthető meg, és mi az amiről biztosan meg tudjuk mondani, hogy nem lehetséges. Kezdetben biztosan van az 1 számunk (ahogy a koordináta-rendszert felvettük: a $(0,0)$ és az $(1,0)$ pontok távolságát neveztük el így). Ebből megszerkeszthető az összes racionális szám.

Vannak a szerkesztési feladatban adott alappontjaink, legyenek ezek $\alpha_1, \alpha_2, \dots, \alpha_n$. Nyilvánvalóan mivel ezek is adottak, így nem csak \mathbb{Q} elemeit tudjuk megszerkeszteni, hanem annak bővítéseit is az alappontokkal. Ezt nevezem **alaptestnek** és K -val jelölöm most:

$$K = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$$

4.2.3. Tétel. Ha δ megszerkeszthető, akkor m_δ foka K fölött 2 hatvány. ■

Bizonyítás. Ha δ megszerkeszthető, akkor $\exists \gamma_1, \gamma_2, \dots, \gamma_k$, amely pontokat közvetlenül euklideszi lépésként kapom (tehát előző tétel miatt mindegyik foka 1 vagy 2), melyekkel kibővítve a K testet, abban már benne lesz a δ :

$$\delta \in K(\gamma_1, \gamma_2, \dots, \gamma_k)$$

Ez azt is jelenti, hogy ehhez a kibővített testhez aminek eleme δ , ha hozzávénném δ elemet, nem kapnék bővebb testet, önmaga maradna.

De akkor a nála „szűkebb” $K \leq K(\gamma_1, \gamma_2, \dots, \gamma_k)$ testhez hozzávéve δ elemet sem kapnánk bővebb testet:

$$K(\delta) \leq K(\gamma_1, \gamma_2, \dots, \gamma_k)$$

A fokszámtétel miatt mivel $K \leq K(\delta) \leq K(\gamma_1, \gamma_2, \dots, \gamma_k)$:

$$|K(\gamma_1, \gamma_2, \dots, \gamma_k) : K| = |K(\gamma_1, \gamma_2, \dots, \gamma_k) : K(\delta)| \cdot |K(\delta) : K|$$

Viszont itt tudjuk a bal oldalról, hogy ha egyesével bővítjük γ_i -kel a K -t, akkor mindig vagy 1-fokú, vagy 2-fokú bővítésünk lesz. Tehát ha végrehajtjuk mind a k darab bővítést, ismét a fokszámtétel miatt ezek a fokszámok összeszorzódnak, vagyis 1-eket vagy 2-eseket szorzunk folyamatosan össze, a szorzat csakis 2-hatvány lehet:

$$|K(\gamma_1, \gamma_2, \dots, \gamma_k) : K| = 2^s$$

Innen viszont látszik, hogy $|K(\delta) : K|$ osztja 2^s -t, ami azt jelenti, hogy ő maga is 2-hatvány. ■

Ezzel az állítással kaptunk egy szükséges feltételt a megszerkeszthetőségre. Tehát csakis algebrai számokat tudunk megszerkeszteni, és közülük is csak aminek minimálpolinomja 2-hatvány fokú. Rögtön alkalmazzuk is, vizsgáljunk meg két nevezetes szerkesztési problémát.

4.2.1. Példa (Kockakettőzés). Adott egy kocka, a feladat megszerkeszteni egy olyan kockát, melynek térfogata az övének kétszerese. Mutassuk meg, hogy euklideszi szerkesztéssel ez nem lehetséges!

Legyen az eredeti kocka oldala a , ekkor térfogata $V = a^3$. Vagyis nekünk egy olyan kockát kellene szerkeszteni, aminek a térfogata $2 \cdot a^3$. Ez viszont azt jelentené, hogy oldala $\sqrt[3]{2} \cdot a$.

Indirekt feltéve, hogy ezt meg tudjuk tenni, azt kapnánk, hogy megszerkeszthető $\sqrt[3]{2} \cdot a$ és a is, akkor hányadosuk $\sqrt[3]{2}$ is. Ez ellentmondás, mert $\sqrt[3]{2}$ minimálpolinomja \mathbb{Q} fölött $x^3 - 2$, ami azt jelenti, hogy $m_{\sqrt[3]{2}}$ foka \mathbb{Q} fölött 3, ami nem kettőhatvány.

4.2.2. Példa (Körnégyesgögesítés). Adott egy kör, a feladat vele megegyező területű négyzet szerkesztése. Mutassuk meg, hogy euklideszi szerkesztéssel ez nem lehetséges!

Most adott egy kör, sugara legyen r . Területe ekkor $r^2 \cdot \pi$. A feladatunk olyan a oldalú négyzet szerkesztése, melyre $a^2 = r^2 \cdot \pi$, vagyis $a = r \cdot \sqrt{\pi}$.

Megint csak ha a megszerkeszthető volna, akkor (mivel r adott, így az is megszerkesztett) $\frac{a}{r} = \sqrt{\pi}$ is megszerkeszthető volna. Akkor viszont $\sqrt{\pi} \cdot \sqrt{\pi} = \pi$ is, ami ellentmondás, hiszen π még csak nem is algebrai (fel sem merül az a kérdés, hogy a foka 2-hatvány vagy sem).

4.3. Törtek

Az egész számokból úgy keletkeztek a racionális számok, hogy szükség volt az osztás műveletére is, ami az egészek köréből kivezet. Sok mindent általánosítottunk már az elmúlt félévekben, most ha mondhatni ilyet, a racionális számok konstrukcióját szeretnénk. Érdekes ebben a fejezetben leírtakat, mint racionális számok tulajdonságait végiggondolni, de általánosabban csinálunk most is dolgokat.

Legyen R egy kommutatív, nullosztómentes gyűrű (vagyis integritási tartomány). Könnyítés kedvéért egyelőre gondolhatunk \mathbb{Z} -re. Ennek az R gyűrűnek az elemeiből alkotunk (a, b) rendezett számpárokat, ahol $b \neq 0$. Definiálunk egy relációt is az elemek között.

4.3.1. Definíció. Az (a, b) és (c, d) rendezett párok akkor és csak akkor állnak relációban, ha $ad = bc$. Jelölés: $(a, b) \sim (c, d)$. ♣

4.3.1. Tétel. Ez egy ekvivalencia-reláció. ♣

Bizonyítás. A három szokásos dolgot kell belátni, végig feltesszük, hogy $b, d, f \neq 0$.

Reflexív: $(a, b) \sim (a, b)$

Persze, hiszen $ab = ba$, mert kommutatív a gyűrű.

Szimmetrikus: $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$

Persze, hiszen az első jelentése, hogy $ad = bc$, a másodikhoz pedig az kellene, hogy $cb = da$ ami igaz, mert a szorzás kommutatív és az $=$ reláció szimmetrikus.

Tranzitív: $(a, b) \sim (c, d)$ és $(c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f)$

Az első kettő jelentése, hogy

$$ad = bc \text{ és } cf = de \quad (4.3.1)$$

és kellene, hogy $af = be$.

I. eset: $c = 0$, ekkor $ad = bc = 0$, és mivel nullosztómentes a gyűrű és $d \neq 0$, ezért $a \cdot d = 0 \Rightarrow a = 0$. Hasonlóan $de = cf = 0$ és $d \neq 0$, ezért $e = 0$. Ekkor viszont kész vagyunk, $af = be = 0$ teljesül.

II. eset: $c \neq 0$. Szorozzuk össze a (4.3.1) egyenleteket:

$$adc f = bcde$$

rendezzük baloldalra és emeljünk ki cd -t:

$$cd \cdot (af - be) = 0$$

mivel itt $c, d \neq 0$, de a test nullosztómentes, ezért $af - be = 0$ következik, ami éppen a bizonyítandó $af = be$. ■

A tavalyiakhoz hasonlóan kapunk tehát ekvivalencia osztályokat, és az egy osztályba tartozó számpárokat tekintjük egyenlőnek. Például ha a gyűrűnk \mathbb{Z} , akkor az egyes osztályok képezik a racionális számokat, de ugyanabban az osztályban van a $\frac{2}{3} \rightarrow (2, 3)$ és $\frac{4}{6} \rightarrow (4, 6)$, hiszen $2 \cdot 6 = 3 \cdot 4$.

5. előadás

Törtek általánosítása

5.1. Hányadostest

5.1.1. Definíció. Legyen R egy kommutatív, nullosztómentes gyűrű. Ekkor értelmezzük az R elemeiből alkotott (a, b) rendezett párok halmazát ($b \neq 0$), továbbá:

- Egy relációt (beláttuk, hogy ekvivalencia-reláció): $(a, b) \sim (c, d) \Leftrightarrow ad = bc$.
- Egy szorzás műveletet: $(a, b) \cdot (c, d) = (ac, bd)$.
- Egy összeadás műveletet: $(a, b) + (c, d) = (ad + bc, bd)$.

és az ekvivalenciaosztályok halmazát R **hányadostestének** nevezzük. Jelölés: \mathbb{Q}_R .



5.1.1. Tétel. A szorzás és az összeadás műveletek jól definiáltak (reprezentáns választásától függetlenül), és \mathbb{Q}_R valóban testet alkot.



Bizonyítás.

Jól definiált a művelet: Azt kell megmutatnunk, hogy ha ekvivalens elemeket szorzunk vagy adunk össze, akkor az eredeti szorzattal/összeggel ekvivalens elemet kapunk.

Legyen

$$(a_1, b_1) \sim (a_2, b_2) \text{ azaz } a_1 b_2 = b_1 a_2$$

$$(c_1, d_1) \sim (c_2, d_2) \text{ azaz } c_1 d_2 = d_1 c_2$$

Kellene (összeadáshoz):

$$(a_1, b_1) + (c_1, d_1) \sim (a_2, b_2) + (c_2, d_2)$$

elvégezve az összeadást

$$(a_1 d_1 + b_1 c_1, b_1 d_1) \sim (a_2 d_2 + b_2 c_2, b_2 d_2)$$

felírva az ekvivalencia definícióját

$$(a_1 d_1 + b_1 c_1) \cdot b_2 d_2 = b_1 d_1 \cdot (a_2 d_2 + b_2 c_2)$$

használva a gyűrűben a disztributivitást

$$a_1 d_1 b_2 d_2 + b_1 c_1 b_2 d_2 = b_1 d_1 a_2 d_2 + b_1 d_1 b_2 c_2$$

használva a gyűrűbeli kommutativitást

$$a_1 b_2 d_1 d_2 + b_1 b_2 c_1 d_2 = b_1 a_2 d_1 d_2 + b_1 b_2 d_1 c_2$$

ami teljesül, hiszen $a_1 b_2 = b_1 a_2$ és $c_1 d_2 = d_1 c_2$.

Kellene (szorzáshoz):

$$(a_1, b_1) \cdot (c_1, d_1) \sim (a_2, b_2) \cdot (c_2, d_2)$$

elvégezve a szorzást

$$(a_1 c_1, b_1 d_1) \sim (a_2 c_2, b_2 d_2)$$

felírva az ekvivalencia definícióját

$$a_1 c_1 \cdot b_2 d_2 = b_1 d_1 \cdot a_2 c_2$$

használva a gyűrűben a kommutativitást

$$a_1 b_2 \cdot c_1 d_2 = b_1 a_2 \cdot d_1 c_2$$

ami igaz, hiszen $a_1 b_2 = b_1 a_2$ és $c_1 d_2 = d_1 c_2$.

Testaxiómák teljesülése:

Összeadáshoz:

- Kommutativitás: $(a, b) + (c, d) = (c, d) + (a, b)$ elvégezve az összeadást

$$(ad + bc, bd) = (cb + da, db)$$

ami nyilván igaz, mert $ad + bc = cb + da$ és $bd = db$, hiszen a gyűrűben a szorzás és összeadás kommutatív.

- Asszociativitás: $((a, b) + (c, d)) + (e, f) = (a, b) + ((c, d) + (e, f))$ elvégezve a „belső” összeadást

$$(ad + bc, bd) + (e, f) = (a, b) + (cf + de, df)$$

majd a „külső” összeadást

$$((ad + bc) \cdot f + bd \cdot e, bdf) = (a \cdot df + b \cdot (cf + de), bdf)$$

használva a gyűrű műveleteinek disztributivitás tulajdonságát

$$(adf + bcf + bde, bdf) = (adf + bcf + bde, bdf)$$

ami láthatóan megegyezik.

- Nullelem: Ez a $\{(0, a)\}$ ekvivalencia osztály lesz (ahol 0 a gyűrű nulleleme), hiszen

$$(c, d) \overset{\text{kellene}}{=} (0, a) + (c, d) = (0d + ac, ad) = (ac, ad)$$

teljesül, hiszen (c, d) és (ac, ad) ugyanabban az ekvivalenciaosztályban vannak, hiszen $(c, d) \sim (ac, ad)$, mivel $cad = dac$.

- **Ellentett:** Ha van egy (a, b) elemem, annak ellentettje $(-a, b)$, hiszen $(-a, b)$ értelmes (mert $b \neq 0$ itt is teljesül, valamint $-a \in R$, mert a gyűrűben van ellentett) és összege (a, b) elemmel a nullelem ekvivalencia osztályát adja:

$$(a, b) + (-a, b) = (ab + b \cdot (-a), b^2) = (0, b^2) \sim (0, a)$$

hiszen $0 \cdot a = b^2 \cdot 0 = 0$.

Szorzáshoz:

- **Kommutativitás:** $(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$ elvégezve a szorzást

$$(ac, bd) = (ca, db)$$

nyilván igaz, mert a gyűrűnkben a szorzás kommutatív.

- **Asszociativitás:** $((a, b) \cdot (c, d)) \cdot (e, f) = (a, b) \cdot ((c, d) \cdot (e, f))$ elvégezve az első szorzást

$$(ac, bd) \cdot (e, f) = (a, b) \cdot (ce, df)$$

majd a második szorzást

$$(ace, bdf) = (ace, bdf)$$

láthatóan megegyezik.

- **Egységelem:** Az $\{(e, e)\}$ ekvivalenciaosztály:

$$(a, b) \overset{\text{kellene}}{=} (e, e) \cdot (a, b) = (ea, eb)$$

teljesül, hiszen (a, b) és (ea, eb) ugyanabban az ekvivalenciaosztályban vannak, hiszen $(a, b) \sim (ea, eb)$, mivel $aeb = bea$.

- **Reciprok:** Adott $(a, b) \neq (0, b)$ elem reciproka (b, a) .

Először is (b, a) értelmes, hiszen ha $a = 0$ volna, akkor $(a, b) = (0, b)$ lenne. Továbbá

$$(e, e) \overset{\text{kellene}}{=} (a, b) \cdot (b, a) = (ab, ba)$$

ez valóban igaz, hiszen $(e, e) \sim (ab, ba)$, mivel $eba = eab$.

Disztributivitás: $((a, b) + (c, d)) \cdot (e, f) = (a, b) \cdot (e, f) + (c, d) \cdot (e, f)$ elvégezve a baloldali összeadást

$$(ad + bc, bd) \cdot (e, f) = (a, b) \cdot (e, f) + (c, d) \cdot (e, f)$$

majd a szorzásokat (használva a gyűrűbeli disztributivitást)

$$(ade + bce, bdf) = (ae, bf) + (ce, df)$$

majd a jobboldali összeadást

$$(ade + bce, bdf) = (aedf + bfce, bdfdf)$$

valóban megegyezik a két oldal, hiszen

$$(ade + bce) \cdot b f d f = b d f \cdot (a e d f + b f c e)$$

mert gyűrűben használva a disztributivitást a jobboldali f -ek kiemelésével + kommutativitás használatával látható, hogy a két oldalon ugyanaz áll.

Sehol nem használtuk fel, hogy a gyűrűnk nullosztómentes, akkor minek kötöttük ki? A műveletek értelmességéhez azt is kell látni, hogy nemcsak mindegy melyik elemet választom adott ekvivalencia osztályból, hanem egyáltalán **létezik** két elem összege, szorzata.

Itt jön képbe a nullosztómentesség, hiszen összeadásnál

$$(a, b) + (c, d) = (ad + bc, bd)$$

mivel $b, d \neq 0$, ezért $bd \neq 0$, különben nem lenne nullosztómentes a gyűrű. Hasonlóan a szorzás esetében

$$(a, b) \cdot (c, d) = (ac, bd)$$

eredmény létezik, mert $b, d \neq 0 \Rightarrow bd \neq 0$, különben lennének nullosztók.

Összességében láttuk tehát, hogy a definiált műveletek értelmesek és a halmaz testet alkot. ■

Például az egész (\mathbb{Z}) vagy a páros számok ($2\mathbb{Z}$) hányadosteste \mathbb{Q} , illetve az egész vagy racionális együtthatós polinomok ($\mathbb{Z}[x]$ és $\mathbb{Q}[x]$) hányadosteste a törtfüggvények ($\mathbb{Q}(x)$).

Az is könnyen látszik, hogy egy test hányadosteste önmaga, vagyis például \mathbb{Q} hányadosteste \mathbb{Q} , \mathbb{R} hányadosteste \mathbb{R} .

5.1.2. Tétel. Legyen R egy kommutatív, nullosztómentes gyűrű (vagyis integritási tartomány). Ha $\exists K$ test, melyre $R \leq K$, akkor $\exists L$ test is, melyre $R \leq L \leq K$ úgy, hogy $L \cong \mathbb{Q}_R$. ♣

Másképpen úgy is mondhatnánk, hogy van egy gyűrűnk (ami kommutatív, nullosztómentes) és abból akarunk testet csinálni valahogyan. A hányadostesttel lesz izomorf a legszűkebb olyan test, ami tartalmazza a gyűrűt. Hiszen ezen tétel szerint bármely, a gyűrűnél bővebb K testet veszünk, az R és a K között lesz olyan test, ami izomorf \mathbb{Q}_R -rel.

A bizonyítás sem így hangzott el előadáson, és a tétel sem (pl.: előadásról a füzetemben $R < L < K$ szerepel, de ha például $K \cong \mathbb{Q}_R$, akkor az utolsó nem lehet szigorú egyenlőtlenség), én végül némi gondolkodás után ennél a verziónál maradtam.

Bizonyítás. Találnunk kell izomorfizmust \mathbb{Q}_R és L között, vagyis kell egy $\varphi : \mathbb{Q}_R \rightarrow L$ művelettartó, bijektív leképezés. Ezek után még azt is meg kell mutatnunk, hogy $R \subseteq L$, valamint $L \subseteq K$. (Mivel mindhárman ugyanarra az összeadás és szorzás műveletre gyűrűt alkotnak, ezért csak a részhalmaz tulajdonságot kell bizonyítani.)

Tekintsük a

$$\varphi : \mathbb{Q}_R \rightarrow L \text{ leképezést, ahol } (a, b) \in \mathbb{Q}_R \text{ képe } \varphi((a, b)) = a \cdot b^{-1} = \frac{a}{b}$$

φ művelettartó:

- **Összegeztartás:** $\varphi((a,b) + (c,d)) = \varphi((a,b)) + \varphi((c,d))$ ugyanis baloldalt elvégezve az összeadást

$$\varphi((ad+bc, bd)) = \varphi((a,b)) + \varphi((c,d))$$

használva φ képzési szabályát

$$\frac{ad+bc}{bd} = \frac{a}{b} + \frac{c}{d}$$

valóban teljesül.

- **Szorzeztartás:** $\varphi((a,b) \cdot (c,d)) = \varphi((a,b)) \cdot \varphi((c,d))$ ugyanis baloldalt elvégezve a szorzást

$$\varphi((ac, bd)) = \varphi((a,b)) \cdot \varphi((c,d))$$

használva φ képzési szabályát

$$\frac{ac}{bd} = \frac{a}{b} \cdot \frac{c}{d}$$

valóban teljesül.

φ bijektív:

- **Injektív:** $(a,b) \approx (c,d) \Rightarrow \varphi((a,b)) \neq \varphi((c,d))$ hiszen átírva mindkét oldalát a következtetésnek:

$$ad \neq bc \Rightarrow \frac{a}{b} \neq \frac{c}{d}$$

egy igaz következtetés.

- **Szürjektív:** Adott $a, b \in R$, $b \neq 0$, akkor $\exists (c,d) \in \mathbb{Q}_R$, melyre $\varphi((c,d)) = \frac{a}{b}$. Nyilván, például $c = a$ és $d = b$ választások jók lesznek.

Mivel a függvény injektív és szürjektív, ezért bijektív is.

$R \subseteq L$:

Legyen $a \in R$ tetszőleges. Ekkor nyilván $a \in L$ is teljesül, hiszen a gyűrűben van egységelem, jelölje ezt 1. Ekkor viszont $(a, 1) \in \mathbb{Q}_R$, melynek képe pedig

$$\varphi((a, 1)) = \frac{a}{1} = a \cdot 1^{-1} = a \cdot 1 = a \in L$$

$L \subseteq K$:

Az L halmaz bármely eleme előáll $a \cdot b^{-1}$ alakban, ahol $a, b \in R$ és $b \neq 0$. Mivel feltettük, hogy $R \leq K$, ezért nyilván $a, b \in K$ és $b \neq 0$ továbbra sem. Ekkor viszont mivel K test, így $b^{-1} \in K$, sőt $a \cdot b^{-1} \in K$. Ezzel L bármely eleméről megkaphatjuk, hogy eleme K -nak is, vagyis L valóban részhalmaza K -nak. ■

5.2. Nevezetes szerkesztési problémák

Emlék: $\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha$.

Bizonyítás. Tekintsük a

$$z = \cos \alpha + i \cdot \sin \alpha$$

komplex számot. Mi lesz ennek a köbe? Kétféleképpen is hatványozhatunk, egyrészt tudjuk, hogy a szöget kell szorozni 3-mal, másrészt ténylegesen elvégezhetjük a hatványozást $(a+b)^3$ azonosság segítségével, ekkor:

$$z^3 = \cos 3\alpha + i \cdot \sin 3\alpha = \cos^3 \alpha + 3\cos^2 \alpha \cdot \sin \alpha \cdot i - 3\cos \alpha \cdot \sin^2 \alpha - \sin^3 \alpha \cdot i$$

ahonnan csak a valós részt véve

$$\operatorname{Re}(z^3) = \cos 3\alpha = \cos^3 \alpha - 3\cos \alpha \cdot \sin^2 \alpha$$

helyettesítve $\sin^2 \alpha = 1 - \cos^2 \alpha$ -t:

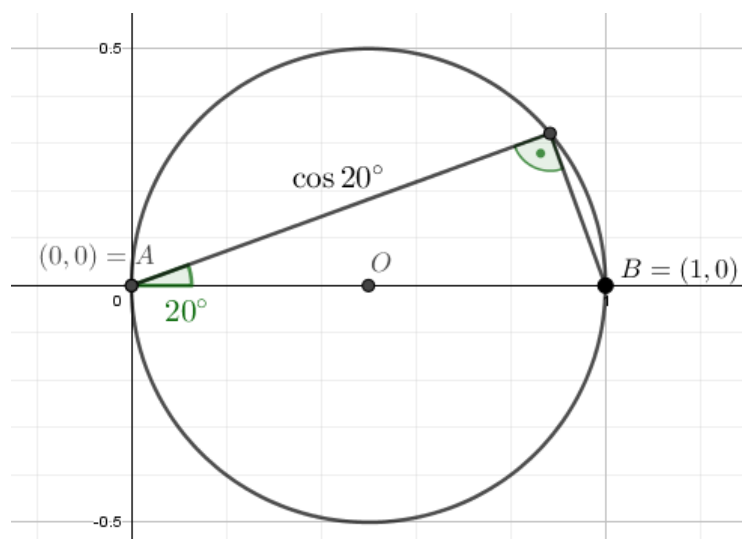
$$\cos 3\alpha = \cos^3 \alpha - 3\cos \alpha \cdot (1 - \cos^2 \alpha) = 4\cos^3 \alpha - 3\cos \alpha$$

adódik, ami éppen a bizonyítandó. ■

5.2.1. Tétel (Szögharmadolás). Nem szerkeszthető meg tetszőleges α szög harmada. ♣

Bizonyítás. A tétel azt mondja ki, hogy nem minden szög harmadát tudjuk megszerkeszteni. Egyeseket azért igen. Például a 180° harmadát pont meg tudjuk szerkeszteni, mert az 60° . Nekünk csak mutatnunk kell egy példát olyan szögre, melynek harmadát nem lehet megszerkeszteni. Jó példa erre a 60° , azt fogjuk belátni, hogy nem szerkeszthető meg a 20° .

Ha meg tudnánk szerkeszteni ezt a 20° -ot, akkor ott lenne nekünk a szokásos $A = (0,0)$ és $B = (1,0)$ pontunk, és át tudnánk másolni oda ezt a 20° -ot. Ezután szerkeszthetnénk a AB szakasz köré Thalész-kört. Innen a B ponttal szemközti befogó hossza éppen $\cos 20^\circ$ volna.



Tehát elegendő nekünk azt megmutatni, hogy $\cos 20^\circ$ nem szerkeszthető, innen már következik, hogy 20° sem. Tudjuk, hogy $\cos 60^\circ = \frac{1}{2} = \cos(3 \cdot 20^\circ)$. Felhasználva az emlék azonosságát:

$$\frac{1}{2} = 4 \cdot \cos^3 20^\circ - 3 \cdot \cos 20^\circ$$

Mit látnak szemeink? A $4x^3 - 3x - \frac{1}{2}$ polinomnak gyöke a $\cos 20^\circ$, tehát akkor a $8x^3 - 6x - 1$ egész együtthatós polinomnak is.

Mivel ez egy harmadfokú polinom, ezért pontosan akkor irreducibilis \mathbb{Q} fölött, ha nincs racionális gyöke. Márpedig mivel egész együtthatós(!), alkalmazhatjuk a racionális gyöktesztet, amiből pár próbálkozás után kiderül, hogy nincs racionális gyöke. Tehát az ő nyolcada a $\cos 20^\circ$ minimálpolinomja \mathbb{Q} fölött.

Viszont ekkor $|\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}| = 3$, ami nem 2 hatvány, vagyis 4.2.3 tétel szerint $\cos 20^\circ$ nem megszerkeszthető. ■

Emlék: Az Euler-féle φ -függvény adja meg 1-től n -ig az n -hez relatív prímek számát. Egyben ez határozta meg a primitív egységgyökök számát is, képlete (ha $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ kanonikus alakú):

$$\varphi(n) = \prod_{i=1}^k p_i^{\alpha_i} - p_i^{\alpha_i-1}$$

Emlék: Az n -edik körosztási polinom definíció szerint aminek gyökei az n -edik primitív egységgyökök (jelölje őket: $\xi_1, \xi_2, \dots, \xi_{\varphi(n)}$):

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \xi_i)$$

Tanultuk (bizonyítás nélkül) Algebra2-ből, hogy a körosztási polinomok 1 főegyütthatós, irreducibilis polinomok \mathbb{Q} fölött.

5.2.1. Lemma. Legyen ε egy primitív n -edik egységgyök. Ekkor $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n)$. ♣

Bizonyítás. Az előző emlékből máris következik, hiszen ε minimálpolinomja \mathbb{Q} fölött éppen $\Phi_n(x)$, mert ez éppen egy irreducibilis, 1 főegyütthatós polinom, melynek gyöke ε . A képletéből látható, hogy foka $\varphi(n)$. ■

5.2.2. Lemma. A $\cos\left(\frac{2\pi}{n}\right)$ algebrai \mathbb{Q} felett és foka $\frac{1}{2} \cdot \varphi(n)$, azaz

$$\left| \mathbb{Q}\left(\cos \frac{2\pi}{n}\right) : \mathbb{Q} \right| = \frac{\varphi(n)}{2}$$

♣

Bizonyítás. Tekintsük a $z = 1$ komplex számot. Az ő trigonometrikus alakja

$$z = 1 = \cos 2\pi + i \cdot \sin 2\pi$$

vegyük az n -edik gyökei közül az elsőt, vagyis az ε primitív egységgyököt.

$$\sqrt[n]{1} \rightarrow \varepsilon = \cos \frac{2\pi}{n} + i \cdot \sin \frac{2\pi}{n}$$

Az 5.2.1 lemmából tudjuk, hogy $|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n)$. Fokszámtétel segítségével bontsuk ezt 2 részre:

$$|\mathbb{Q}(\varepsilon) : \mathbb{Q}| = \varphi(n) = \left| \mathbb{Q}(\varepsilon) : \mathbb{Q} \left(\cos \frac{2\pi}{n} \right) \right| \cdot \left| \mathbb{Q} \left(\cos \frac{2\pi}{n} \right) : \mathbb{Q} \right|$$

Elegendő volna azt belátni, hogy

$$\left| \mathbb{Q}(\varepsilon) : \mathbb{Q} \left(\cos \frac{2\pi}{n} \right) \right| = 2$$

Ehhez tekintsük az

$$x^2 - 2 \cdot \cos \frac{2\pi}{n} \cdot x + 1$$

polinomot. Azt állítom, hogy ez ε minimálpolinomja $\mathbb{Q} \left(\cos \frac{2\pi}{n} \right)$ fölött. Amennyiben igazam van kész vagyunk, hiszen ennek 2 a foka. Mi kellene ehhez? Legyen ennek gyöke ε és legyen irreducibilis.

Mivel $\mathbb{Q} \left(\cos \frac{2\pi}{n} \right)$ egy olyan test, mely csak valós számokat tartalmaz, ezért elegendő volna ha belátnánk, hogy nincs valós gyöke a polinomnak, ettől már irreducibilis volna.

Nincs más hátra, nézzük meg a gyökeit! Ha minden jól megy ε az egyik gyöke, és a másik gyöke sem lesz valós:

$$x_{1,2} = \frac{2 \cdot \cos \left(\frac{2\pi}{n} \right) \pm \sqrt{4 \cdot \cos^2 \left(\frac{2\pi}{n} \right) - 4}}{2} = \cos \left(\frac{2\pi}{n} \right) \pm \sqrt{\cos^2 \left(\frac{2\pi}{n} \right) - 1}$$

használva, hogy $1 = \sin^2 \left(\frac{2\pi}{n} \right) + \cos^2 \left(\frac{2\pi}{n} \right)$:

$$= \cos \left(\frac{2\pi}{n} \right) \pm \sqrt{-\sin^2 \left(\frac{2\pi}{n} \right)} = \cos \left(\frac{2\pi}{n} \right) \pm i \cdot \sin \left(\frac{2\pi}{n} \right)$$

ahonnan azt látjuk, valóban ε és konjugáltja a gyökei a polinomnak, ezzel beláttuk a lemmát. ■

Emlék: Fermat-számoknak az $F_n = 2^{2^n} + 1$ alakú számokat nevezzük, ahol $n \geq 0$ egész. Értelem szerűen Fermat-prím egy olyan Fermat-szám, ami egyben prímszám is, ilyen például az első 5 Fermat-szám, de többről egyelőre nem is tudunk. Algebra1-ből láttuk, hogy ha $p = 2^k + 1$ alakú szám prím, akkor szükségképpen $k = 2^n$, vagyis p ekkor Fermat-prím is.

5.2.2. Tétel. Akkor és csak akkor szerkeszthető szabályos n -szög, amennyiben

$$n = 2^\alpha \cdot F_1 \cdot F_2 \cdot \dots \cdot F_t$$

kanonikus alakú, ahol minden F_i egy Fermat-prím. ♣

Bizonyítás. Csak a szükséges feltételt igazoljuk, vagyis hogy ha szerkeszthető n oldalú szabályos sokszög, akkor n a megadott alakú lehet csak (a másik irány nehéz).

A sokszög pontosan akkor szerkeszthető meg, ha megszerkeszthető egy „középponti szöge”, vagyis¹ $\cos \frac{2\pi}{n}$.

Mikor szerkeszthető meg $\cos \frac{2\pi}{n}$? Azt tudjuk, hogy foka $\frac{1}{2} \cdot \varphi(n)$ és a 4.2.3 tétel miatt csak 2-hatvány fokú számok szerkeszthetők meg, ezért szükségképpen²

$$\varphi(n) = \prod p_i^{\alpha_i} - p_i^{\alpha_i-1} = 2\text{-hatvány}$$

Látható, hogy a $p = 2$ prímtenyező itt nem sok vizet zavar, rá semmiféle megkötésünk nincs, a kanonikus alak maradék prímeiről kellene belátnunk, hogy csakis Fermat-prím lehet, és csakis az 1 kitevővel.

Tekintsük a többi p_i -t. Az ő esetükben $\alpha_i = 1$ kell legyen, különben $p_i^{\alpha_i} - p_i^{\alpha_i-1}$ tényezőből kiemelhetnénk p_i -t, ami azt jelentené, hogy összességében a szorzat (vagyis $\varphi(n)$) osztható volna $p_i \neq 2$ prímmel. Node 2-hatvány nem lehet osztható 2-től különböző prímeikkel.

Ha $\alpha_i = 1$, akkor minden p_i „szerepe” a szorzatban: $p_i - 1$. Ennek is 2-hatványnak kell lennie (mert ez továbbra is osztja $\varphi(n)$ -t, amiről tudjuk, hogy 2-hatvány kell legyen). Vagyis valójában p_i egy olyan prím, melyre valamilyen k -ra

$$p_i - 1 = 2^k \Rightarrow p_i = 2^k + 1$$

az ilyen alakú prímekek éppen a Fermat-prímekek, kész vagyunk a bizonyítással. ■

Előadás végén még volt szó háromszög szerkesztésről amennyiben adott 2 oldal és 1 szögfelező. Attól függően hogyan vannak megadva az adatok vagy meg lehet szerkeszteni vagy nem a háromszöget. Erre a példára visszatérek a későbbiekben, ha részletesebben tárgyalásra kerülne előadáson.

¹azt már megbeszéltük, hogy mindegy, hogy a szöget szerkesztjük meg vagy a koszinuszát

²bár a feltételünk $\frac{1}{2} \cdot \varphi(n)$ -re van, de ha az 2-hatvány, akkor $\varphi(n)$ is muszáj az legyen

6. előadás

Primitív gyök

6.1. Kongruencia emlékek

Ez a fejezet elsősorban emlékeztető néhány Algebra1-ben tanult fogalomról, tételről, ezért szerepel kevés bizonyítás: már elhangzottak régebbi tárgyon vagy nem kell tudni (Kínai maradéktétel).

6.1.1. Tétel. Adott a, b esetén az $ax \equiv b \pmod{m}$ lineáris kongruenciának pontosan akkor létezik megoldása (azaz olyan x maradékosztály, mely esetén a kongruencia teljesül), amennyiben $(a, m) \mid b$. Ekkor pedig a megoldások száma (a, m) . ♣

6.1.1. Állítás. Egy R gyűrű esetén az egységek¹ halmaza csoport (a szorzásra). Az egységek csoportjának jele mostantól R^* . ♣

Bizonyítás. Részcsoport tulajdonságot kell vizsgálni: $R^* \subseteq R$ zárt a szorzásra és az inverzképzésre. Először is vegyük észre, hogy ez nem egy üres halmaz, mert a gyűrű egységelemét 1 szimbólummal jelölve, az egyben egység is, tehát benne van a halmazban. Egységek szorzata is egység és minden egységnek van inverze, hiszen ha e egység, akkor mivel $1 \in R^*$, ezért $e \mid 1$, azaz $\exists f \in R$, melyre $e \cdot f = 1$, ami éppen azt jelenti, hogy az e -nek az f az inverze, ráadásul f is egység, tehát $f \in R^*$. ■

Például \mathbb{Z}_m esetén az egységek azok az $a \in \mathbb{Z}_m$ elemek, melyeknek van inverze, vagyis melyek esetén az $ax \equiv 1 \pmod{m}$ kongruencia megoldható. Ezek 6.1.1 tétel szerint éppen azok, melyekre $(a, m) \mid 1$, azaz $(a, m) = 1$, vagyis a modulushoz relatív prímelek halmaza. Ezeket neveztük Algebra1-ből redukált maradékosztályoknak. Tehát \mathbb{Z}_m^* a redukált maradékosztályok halmaza, mely csoportot alkot a szorzásra.²

Speciális esete ennek, amikor $m = p$ prím, ekkor $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, hiszen modulo p prím csak a 0 számnak nincs inverze, az összes többi relatív prím p -hez.

¹vagyis ahogy idén félév elején megállapítottuk: az invertálható elemek

²tavaly is előkerült ez a témakör: 85. oldal, Lagrange-tétel speciális esete az $a^{\varphi(m)} \equiv 1 \pmod{m}$ Euler-Fermat-tétel.

6.1.2. Tétel (Kínai maradéktétel). Az

$$\begin{cases} x \equiv a_1 \pmod{c_1} \\ x \equiv a_2 \pmod{c_2} \\ x \equiv a_2 \pmod{c_2} \\ \vdots \\ x \equiv a_k \pmod{c_k} \end{cases}$$

szimultán kongruenciarendszernek pontosan akkor létezik megoldása, ha bármelyik 2 kongruenciát kiválasztva az általuk alkotott szimultán kongruenciarendszernek van megoldása, azaz $\forall i, j: (c_i, c_j) \mid a_i - a_j$. A megoldás ekkor egyértelmű modulo $[c_1, c_2, \dots, c_k]$. ♣

Megjegyzés. Speciális eset: Amennyiben $\forall i, j: (c_i, c_j) = 1$, akkor egyértelműen létezik megoldás modulo $c_1 \cdot \dots \cdot c_k$.

Emlékezzünk vissza **rend** fogalmára is, mely azóta sok más kontextusban előkerült és hasonló dolgot jelentett mindig: modulo m egy a szám rendje (feltéve, hogy $(a, m) = 1$) a legkisebb olyan pozitív egész szám, amely hatványra emelve az a számot 1-et kapunk. Jelölése: $o_m(a)$.

Azért csak $(a, m) = 1$ esetén értelmezzük a rend fogalmát, mert akkor az Euler-Fermat-tétel garantálja, hogy lesz olyan hatványa a -nak amely 1 lesz modulo m , például $\varphi(m)$. Látható itt is, hogy jobban szeretünk egy $m = p$ prímszámmal dolgozni, hiszen ekkor $(a, p) = 1$ bármely $a \neq 0$ elemre, vagyis minden nemnulla elemnek van rendje.

Tudjuk, hogy osztja a „jó” kitevőket, vagyis $a^c \equiv 1 \pmod{m} \Leftrightarrow o_m(a) \mid c$. Mivel $\varphi(m)$ egy jó kitevő, ezért $o_m(a) \mid \varphi(m)$. További fontos tulajdonságai, hogy $a^b \equiv a^c \pmod{m} \Leftrightarrow b \equiv c \pmod{o_m(a)}$, és az a -nak $o_m(a)$ darab modulo m páronként inkongruens hatványa létezik.

6.1.1. Példa. Tudjuk, hogy $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 2 \cdot 20 = 40$ és $(7, 100) = 1$, ezért az Euler-Fermat-tétel miatt

$$7^{40} \equiv 1 \pmod{100}$$

De hasonlóan $\varphi(25) = 20$ és $\varphi(4) = 2$, ezért

$$7^{20} \equiv 1 \pmod{25} \quad \text{és} \quad 7^2 \equiv 1 \pmod{4}$$

ahonnan a második kongruenciát 10-edik hatványra emelve

$$\begin{cases} 7^{20} \equiv 1 \pmod{25} \\ 7^{20} \equiv 1 \pmod{4} \end{cases}$$

De mivel $(4, 25) = 1$, ezért az

$$\begin{cases} x \equiv 1 \pmod{25} \\ x \equiv 1 \pmod{4} \end{cases}$$

szimultán kongruenciarendszernek a kínai maradéktétel szerint egyértelműen létezik megoldása modulo $25 \cdot 4 = 100$, márpedig az 1 elem teljesíti ezt, vagyis $x \equiv 1 \pmod{100}$. Jelen esetben $7^{20} \equiv 1 \pmod{100}$. Ez egyben azt is jelenti, hogy $o_{100}(7) \neq 40$, mert találtunk nála kisebbet, de mivel osztja a „jó” kitevőket, ezért $o_{100}(7) \mid 20$.

Egyébként bármely $(a, 100) = 1$ esetén ugyanez elmondható lett volna, tehát modulo 100 egyetlen olyan elem sincs, aminek a rendje 40.

Emlékezzünk még meg a renddel kapcsolatban arról az összefüggésről, mely egy elem rendje és hatványai rendje között áll fenn, és mely szintén előkerült korábbi tanulmányok során:

6.1.3. Tétel. Egy g elem i -edik hatványának rendje az elem rendjének ismeretében:

$$o(g^i) = \frac{o(g)}{(i, o(g))}$$




6.2. Primitív gyök

Mivel $o_n(a) \mid \varphi(n)$, ezért nyilvánvaló, hogy a maximális elemrend $\varphi(n)$. A 6.1.1 példában láttuk, hogy ez bizony jóval kisebb is lehet. A kérdés, hogy van-e olyan elem, aminek a rendje éppen $\varphi(n)$.

6.2.1. Definíció. Egy a számot **primitív gyöknek** nevezünk modulo n , ha $o_n(a) = \varphi(n)$. 

Láttuk, hogy modulo 100 nem létezik primitív gyök, hiszen 7 helyett bármelyik másik, 100-hoz relatív prím esetén megállta volna helyét a gondolatmenetünk (nem relatív prímelek esetén pedig a rend értelmezve sincs).

6.2.1. Tétel. Modulo n pontosan akkor létezik primitív gyök, amennyiben $n = 2$ vagy $n = 4$ vagy $(\exists p > 2$ prím és $\alpha > 0$, melyre) $n = p^\alpha$ vagy $n = 2 \cdot p^\alpha$. 

A tétel $n = 2$ esetén nyilvánvaló, mert $\varphi(2) = 1 = o_2(1)$, hasonlóan $n = 4$ esetén $\varphi(4) = 2^2 - 2^1 = 2 = o_4(3)$, hiszen $3^2 \equiv 1 \pmod{4}$, de $3^1 \not\equiv 1 \pmod{4}$. Az állítást ezen kívül csak $n = p$ esetre fogjuk belátni, de először szükségünk lesz ehhez egy lemmára.

6.2.1. Lemma. $\sum_{d \mid n} \varphi(d) = n$. 

Vagyis ha veszem egy szám osztóit, mindegyiknél a φ helyettesítési értékét, majd összeadom, akkor megkapom az eredeti számot. Például 6 osztói: 1, 2, 3, 6, azaz a tétel szerint

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$$

Kétféle bizonyítást is mutatunk, az első bizonyos értelemben „elemibb” lesz.

Bizonyítás. Tekintsük a következő törtet:

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n}{n}$$

Kétféleképpen is meg fogjuk számolni, hogy hány darab tört ez. Egyrészt ez szemlátomást n darab tört. Hurrá! A feladat felével meg is vagyunk, már csak a 90%-a van hátra.

Egyszerűsítsük az összes törtet innen. Ha van egy $\frac{k}{n}$ törtünk, akkor hogyan egyszerűsítjük azt? Leosztjuk a számlálót és nevezőt is a legnagyobb közös osztójukkal. Vagyis

$$\frac{k}{n} = \frac{\frac{k}{(k,n)}}{\frac{n}{(k,n)}} = \frac{a}{d}$$

alakot kapunk, ahol $(a, d) = 1$ és $\frac{n}{(n,k)} = d \Leftrightarrow n = (n, k) \cdot d$ azaz $d \mid n$.

Adott d esetén hányféle lehet a értéke? Ahány relatív prím választható d -hez. Ez éppen $\varphi(d)$. Nincs más dolgunk, mint hogy végighaladjunk az n összes d osztóján és mindegyikre összegezzük $\varphi(d)$ értéket, ezzel megkapjuk a felírt törtek számát, amiről láttuk, hogy n darab. Éppen ezt mondja a lemma. ■

Bizonyítás. Tekintsünk egy n elemű ciklikus csoportot³, amelyet egy g elem generál: $G = \langle g \rangle$. Ekkor tudjuk, hogy g elemnek n különböző hatványa van, tehát $o(g) = n$.

Hány olyan eleme van a csoportnak⁴, aminek a rendje éppen d ? A csoport elemei g^i alakúak és most olyan i számot keresünk, amire $o(g^i) = d$. Hogyan néz ki az elemek rendje az előző fejezet végén lévő képlet alapján?

$$d = o(g^i) = \frac{o(g)}{(i, o(g))} = \frac{n}{(i, n)}$$

azt látjuk tehát, hogy

$$d = \frac{n}{(i, n)} \Leftrightarrow d \cdot (i, n) = n \Leftrightarrow (d \cdot i, d \cdot n) = n$$

Egyrészt a középső egyenlőségéből következik, hogy $d \mid n$, ezt mindjárt használni fogjuk.

Valamint látható, hogy $n \mid d \cdot i$, ami azt jelenti, hogy $\exists j$, melyre $n \cdot j = d \cdot i$. Mivel $d \mid n$, ezért leoszthatunk vele

$$\frac{n}{d} \cdot j = i$$

Azt kaptuk tehát, hogy ez csakis olyan hatványokra igaz, amelyek kitevője $\frac{n}{d} \cdot j$ alakú. Helyettesítve i helyére

$$(d \cdot \frac{n}{d} \cdot j, d \cdot n) = n$$

vagyis azt kaptuk, hogy

$$(n \cdot j, n \cdot d) = n \cdot (j, d) = n$$

egyszerűsítve n -nel: $(j, d) = 1$. Ez azt jelenti, hogy annyi féleképpen választható meg j (majd abból következően i is), ahány relatív prím létezik d -hez, ez éppen $\varphi(d)$.

Tehát a d rendű elemek száma $\varphi(d)$. A csoport elemeit megszámlálhatjuk úgy, hogy egyesével összegezzük, hogy a különböző rendű elemeiből hány van. Tehát képezve $\sum_{d \mid n} \varphi(d)$ összeget

megkapjuk a csoport elemszámát, amiről tudjuk, hogy n . ■

³egyetlen elemének n különböző hatványából áll, lásd: Algebra3 jegyzet, 7.4. fejezet

⁴feltesszük, hogy van egyáltalán ilyen rendű eleme, ha nincs akkor nyilván 0

Az előző bizonyítás vége egy picit be tud minket csapni: "Tehát a d rendű elemek száma $\varphi(d)$ ". Ne feledjük el, hogy itt ezt a d számot a csoport elemszámának különös módon történő megszámlálásához akartuk felhasználni, tehát feltehetjük, hogy csak olyan d számokkal foglalkozunk, amelyek tényleg előállnak valamely elem rendjeként! Láttuk például, hogy modulo 100 egyetlen elem sincs, aminek a rendje 40 lenne.

6.2.2. Tétel. Ha p prím, akkor modulo p létezik primitív gyök. ♣

Bizonyítás. A bizonyítás során tehát végig \mathbb{Z}_p -ben vagyunk. Mit tudunk elmondani, ha tudjuk 2 elemről, hogy rendjeik megegyeznek? Például legyen $o(a) = d$ és $o(b) = d$. Mik lesznek ekkor az $x^d - 1 \in \mathbb{Z}_p[x]$ polinom gyökei?

Láthatóan gyöke az 1. Aztán a is, hiszen $a^d \equiv 1 \pmod{p}$. Hasonlóan gyöke a^2 , mert

$$(a^2)^d - 1 = (a^d)^2 - 1 \equiv 1^2 - 1 \equiv 0 \pmod{p}$$

Hasonlóan látható, hogy a -nak az összes különböző hatványa gyöke. Mivel a rendje a páronként inkongruens hatványainak számával egyezik meg, ezért

$$1, a, a^2, \dots, a^{d-1}$$

d különböző hatványa a -nak, tehát ők biztosan gyökei a polinomnak.

Igen ám, de annak más gyöke nincs is rajtuk kívül, hiszen a polinomunk a \mathbb{Z}_p test fölötti polinom, tehát legfeljebb annyi gyöke lehet, amennyi a foka, ami jelen esetben d .

De vegyük észre, hogy mivel $o(b) = d$, ezért $b^d - 1 \equiv 0 \pmod{p}$, ami azt jelenti, hogy b is gyöke a polinomnak. Ez csak akkor lehetséges, ha $\exists i$, melyre $b = a^i$. Mi történne ha most akarnánk kiszámolni b rendjét?

$$d = o(a) = o(b) = o(a^i) = \frac{o(a)}{(i, o(a))} = \frac{d}{(i, d)}$$

összeolvasva az elejét és a végét: $d = \frac{d}{(i, d)}$ ahonnan $(i, d) = 1$.

Most is azt látjuk tehát, hogy ha van d rendű elem, akkor abból $\varphi(d)$ darab van. Vezessünk most be egy függvényt, hogy lekezeljük ezt a „ha van akkor” problémát:

$$\psi(d) = \begin{cases} \varphi(d) & \text{ha van } d \text{ rendű elem} \\ 0 & \text{különben} \end{cases}$$

Na most végre először legálisan mondhatom ki, hogy a d rendű elemek száma $\psi(d)$. Innen igazából annyit szeretnénk bizonyítani, hogy $\psi(p-1) > 0$, hiszen ekkor létezik $\varphi(p) = p-1$ rendű elem, vagyis primitív gyök modulo p .

Rögtön egy **fontos megállapítás**: $\varphi(d) \geq \psi(d)$, hiszen amilyen d -re van d rendű elem, ott közös az értékük, különben pedig $\varphi(d) \geq 0 = \psi(d)$ igaz.

Másik észrevétel: Minden elemnek van rendje! Pontosabban majdnem mindnek, a 0-nak nincs. De rajta kívül minden a -ra igaz, hogy $(a, p) = 1$, tehát értelmezzük rá a rend fogalmát. Azt is tudjuk, hogy mindegyik elem rendjére igaz, hogy $o(a) \mid \varphi(p) = p-1$. Vagyis ha végighaladnánk

$p - 1$ osztóin és megszámolnánk, hogy hány olyan elem van, aminek éppen az a rendje, akkor megszámolnánk \mathbb{Z}_p elemeit a 0 kivételével, vagyis $p - 1$ elemet számolnánk. Képletre fordítva a rízsát:

$$\sum_{d|p-1} \psi(d) = p - 1$$

Na most rakjunk össze mindent! Becsüljünk minden $\varphi(d)$ -t alulról $\psi(d)$ -vel:

$$\overbrace{p - 1 = \sum_{d|p-1} \varphi(d)}^{6.2.1 \text{ lemma}} \geq \sum_{d|p-1} \psi(d) = p - 1$$

Hiába becsültünk, nem lett kisebb ahonnan elindultunk. Ez csakis akkor lehetséges, ha valójában nem is történt becslés és $\forall d$ esetén $\psi(d) = \varphi(d)$. De akkor konkrétan $\psi(p - 1) = \varphi(p - 1) > 0$. Ezt akartuk. ■

6.2.1. Példa. Adjunk meg modulo 7 egy primitív gyököt!

Mivel a 7 prím, ezért meg tudjuk ezt tenni, például a 3 megfelelő lesz. Mivel $\varphi(7) = 6$, ezért 6 osztói jöhetnek szóba amikor 3 rendjét keressük, de $3^2 = 9 \equiv 2 \pmod{7}$, illetve $3^3 = 27 \equiv -1 \pmod{7}$. Tehát $o_7(3) = 6$, vagyis a 3 primitív gyök modulo 7.

Primitív gyök kereséskor segítségünkre lehet, ha ismerjük egy szám különböző hatványait. Ezeket a könnyebb átláthatóság kedvéért egy táblázatban rögzíthetjük, melynek felső sorába kerül a kitevő, alsóba pedig a hatvány.

Készítsünk a 2-höz modulo 23 egy ilyen táblázatot! Annyi oszlopunk lesz, ahány különböző hatvány, vagyis ami 2-nek a rendje. Tehát addig kell írjuk az oszlopokat, amíg az alsó sorban 1-est nem kapunk.

Számolás közben könnyíti a munkánkat, hogy elegendő modulo 23 számolni, tehát például $2^5 = 32 \equiv 9 \pmod{23}$. Ezután $2^6 = 2 \cdot 2^5 \equiv 2 \cdot 9 = 18 \pmod{23}$.

| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|----------------------|---|---|---|----|---|----|----|---|---|----|----|
| 2ⁿ | 2 | 4 | 8 | 16 | 9 | 18 | 13 | 3 | 6 | 12 | 1 |

A táblázatból közvetlenül leolvasható, hogy $o_{23}(2) = 11 \neq 22 = \varphi(23)$, tehát a 2 nem primitív gyök modulo 23. Ennél azonban sokkal több is látszik. A táblázat alsó sorában szereplő számok egyike sem lehet primitív gyök modulo 23.

Ugyanis ha veszek egy számot, ami előáll 2-nek egy hatványaként, akkor annak már a 11-edik hatványa biztosan 1 lesz, hiszen bármelyik a számot is venném ki az alsó sorból, létezne olyan i , melyre $a \equiv 2^i \pmod{23}$. Ekkor

$$a^{11} \equiv (2^i)^{11} = (2^{11})^i \equiv 1^i = 1 \pmod{23}$$

Ezzel kizártunk egy rakás számot, ami biztosan nem primitív gyök modulo 23. Persze ez a táblázat másra is használható. Tudjuk, hogy a 2-nek az összes különböző hatványa előfordul. Ezek után könnyen leolvasható, hogy például hanyadik hatványa lesz 2-nek 9: az 5. hatványa.

Ez az utóbbi kérdés a logaritmus fogalmára emlékeztet minket. Mintha egy olyan számot keresnénk, melyre $2^x = 9$. Ezt valós számokra úgy oldanánk meg, hogy $x = \log_2 9$. Ezen intuíció alapján definiálhatnánk maradékosztályokra is a logaritmus fogalmát. A gond itt az volna, hogy például mi a helyzet $\log_2 5$ értékével? Modulo 23 nem áll elő 2-hatványként az 5. Tehát itt nem csak a 0 maradékosztályt kellene kizárjuk. Ennek érdekében ezt a fogalmat⁵ primitív gyökökre szokás értelmezni, és csak amennyiben a modulus prímszám, a fogalom neve **diszkrét logaritmus** vagy **index**.

Ettől függetlenül a könnyebb áttekinthetőség kedvéért mi nyugodtan megfordíthatjuk a táblázat két sorát és „sorba rendezhetjük” a maradékosztályokat attól függetlenül, hogy a 2 nem primitív gyök modulo 23.

| | | | | | | | | | | | |
|----------|----|---|---|---|---|---|---|----|----|----|----|
| 2^n | 1 | 2 | 3 | 4 | 6 | 8 | 9 | 12 | 13 | 16 | 18 |
| n | 11 | 1 | 8 | 2 | 9 | 3 | 5 | 10 | 7 | 4 | 6 |

Hogyan tudnánk mondani egy primitív gyököt modulo 23? Láttuk, hogy a 2 nem volt jó, mert 11. hatványa már 1. De például jó lenne nekünk a -2 . Hiszen $o_{23}(-2) \in \{1, 2, 11, 22\}$, ahonnan az első 2 eset láthatóan nem igaz. Itt viszont már azt is láthatjuk, hogy a 11. hatványa sem lesz egy, hiszen

$$(-2)^{11} = (-1)^{11} \cdot 2^{11} \equiv -1 \cdot 1 \equiv -1 \pmod{23}$$

tehát a $-2 \equiv 21$ egy primitív gyök modulo 23.

Neki könnyű felírni ezt a fajta táblázatát is, hiszen hatványozása ugyanúgy zajlik ahogy 2 esetében, csak váltakozó előjellel jönnek a tagok:

| | | | | | | | | | | | |
|----------|----|---|----|----|----|----|-----|---|----|----|----|
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| $(-2)^n$ | -2 | 4 | -8 | 16 | -9 | 18 | -13 | 3 | -6 | 12 | -1 |

| | | | | | | | | | | | |
|----------|----|----|----|-----|----|-----|----|----|----|-----|----|
| n | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| $(-2)^n$ | 2 | -4 | 8 | -16 | 9 | -18 | 13 | -3 | 6 | -12 | 1 |

6.3. Binom kongruenciák

Ebben a fejezetben modulo p prímszám fogjuk keresni a megoldását az $x^n \equiv a \pmod{p}$ kongruenciának. Hogyan tudnánk ehhez felhasználni az előző fejezetben tárgyalt primitív gyök fogalmát?

6.3.1. Lemma. Legyen g primitív gyök modulo p prímszám. Ekkor $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ♣

Bizonyítás. Mivel g primitív gyök modulo p , ezért $o_p(g) = \varphi(p) = p - 1$, azaz g -nek $p - 1$ különböző hatványa létezik, ezek:

$$1, \quad g, \quad g^2, \quad \dots \quad g^{p-2}$$

⁵Freud: Számelmélet könyv 3.4.1 Definíció

Tudjuk, hogy a kis Fermat-tétel miatt

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

Mit tudunk egy x maradékosztályról, ha $x^2 \equiv 1 \pmod{p}$? Definíció szerint $p \mid x^2 - 1 = (x-1)(x+1)$. Használva p prímtulajdonságát ekkor

$$p \mid x-1 \Leftrightarrow x \equiv 1 \pmod{p} \quad \text{vagy} \quad p \mid x+1 \Leftrightarrow x \equiv -1 \pmod{p}$$

Azt kaptuk tehát, hogy

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{vagy} \quad g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

ahonnan az első eset nem lehetséges, mert akkor már g -nek $p-1$ -nél kisebb hatványa is 1 volna, pedig feltettük, hogy $p-1$ a rendje. ■

Jelölés: Egy H halmaz számosságára a $|H|$ mellett használatos a $\#H$ jelölés is.⁶

6.3.1. Definíció. Egy $x^n \equiv a \pmod{p}$ kongruenciát (ahol p prímszám) **binom kongruenciának** nevezzük. ♣

Mindjárt kimondunk egy hasznos tételt binom kongruenciák megoldhatóságáról, de előtte írunk ide egy lemmát, amit bizonyítás során használni fogok (ha valakinek ez triviális, akkor elnézést, de nekem meg kell gondolni ezt is).

6.3.2. Lemma. Ha $n, k, q \in \mathbb{Z}$ és $n \mid q$ és $k \mid q$, akkor $n \mid k \Leftrightarrow \frac{q}{k} \mid \frac{q}{n}$. ♣

Bizonyítás. A két irányt külön bizonyítom. Feltehető, hogy $q \neq 0$, különben triviális lenne az állítás.

\Rightarrow irány:

Ha $n \mid k$, akkor $\exists a$, melyre $n \cdot a = k$. Tudjuk, hogy $n \mid q$ és $k \mid q$, ezért $\frac{q}{n}, \frac{q}{k} \in \mathbb{Z}$. Az előző egyenletet $\frac{q}{n}$ egész számmal beszorozva

$$n \cdot a \cdot \frac{q}{n} = k \cdot \frac{q}{n}$$

azaz

$$a \cdot q = k \cdot \frac{q}{n}$$

Ezt beszorozva $\frac{q}{k}$ egész számmal

$$a \cdot q \cdot \frac{q}{k} = k \cdot \frac{q}{n} \cdot \frac{q}{k}$$

egyszerűsítve jobb oldalon k -val, illetve mindkét oldalt osztva $q \neq 0$ -val:

$$a \cdot \frac{q}{k} = \frac{q}{n}$$

⁶Nem tervezem használni a továbbiakban, de leírtam, hogy ha előadáson előfordulna, akkor értsük mit jelent.

ami éppen azt jelenti, hogy $\frac{q}{k} \mid \frac{q}{n}$.

\Leftarrow irány:

Tudjuk, hogy $\frac{q}{k} \mid \frac{q}{n}$, azaz $\exists b$, melyre

$$\frac{q}{k} \cdot b = \frac{q}{n}$$

szorozva $k \cdot n$ -el, majd osztva $q \neq 0$ -val:

$$n \cdot b = k$$

ami szerint éppen $n \mid k$. ■

6.3.1. Tétel. Legyen p prímszám és $(a, p) = 1$. Ekkor $x^n \equiv a \pmod{p}$ binom kongruencia pontosan akkor oldható meg, amennyiben

$$a^{\frac{p-1}{(n, p-1)}} \equiv 1 \pmod{p}$$

és a megoldások száma $(n, p-1)$ modulo p . ♣

Elméletileg ennek a tételnek a bizonyítása nem lesz számonkérve, de azért leírom ha már elhangzott előadáson.

Bizonyítás. Legyen g egy primitív gyök modulo p . Tudjuk a 6.2.2 tétel miatt, hogy mivel p prím, ezért létezik primitív gyök modulo p , tehát nem hülyeség a bizonyítás első mondata. Azaz a továbbiakban $o_p(g) = p-1$.

Tudjuk azt is, hogy $x \not\equiv 0 \pmod{p}$, hiszen különben $0 \equiv x^n \equiv a \not\equiv 0 \pmod{p}$ ellentmondást kapnánk. Ekkor viszont x egy redukált maradékosztály, márpedig tudjuk, hogy minden redukált maradékosztály előáll egy primitív gyök megfelelő hatványaként. Vagyis $\exists y$, melyre $x \equiv g^y \pmod{p}$.

Hasonlóan elmondható ez a maradékosztályról is (mivel $(a, p) = 1$, így a egy redukált maradékosztály), tehát $\exists k$, melyre $a \equiv g^k \pmod{p}$.

A megoldandó $x^n \equiv a \pmod{p}$ kongruencia ekkor

$$g^{n \cdot y} \equiv (g^y)^n \equiv g^k \pmod{p}$$

A rend egyik tulajdonsága szerint ekkor

$$n \cdot y \equiv k \pmod{o(g)}$$

mivel pedig $o(g) = p-1$, így az

$$n \cdot y \equiv k \pmod{p-1}$$

lineáris kongruenciához jutottunk. Ennek a 6.1.1 tétel alapján pontosan akkor van megoldása, amennyiben $(n, p-1) \mid k$, a megoldások száma modulo p pedig $(n, p-1)$. Ezzel a tétel egyik felét már be is láttuk, a megoldásszámot. A másikhoz kell még egy picit dolgozni.

Mikor teljesül $(n, p-1) \mid k$ oszthatóság? Hát tudjuk azt is, hogy $(n, p-1) \mid p-1$. Akkor viszont amit vizsgálunk azzal ekvivalens, hogy $(n, p-1) \mid (k, p-1)$. Most alkalmazva a 6.3.2 lemmát ez azzal ekvivalens, hogy

$$\frac{p-1}{(k, p-1)} \mid \frac{p-1}{(n, p-1)}$$

és mivel (6.1 fejezet végén lévő képlet alapján)

$$o(a) = o(g^k) = \frac{o(g)}{(k, o(g))} = \frac{p-1}{(k, p-1)}$$

ezért azt a feltételt kaptuk, hogy

$$(n, p-1) \mid k \Leftrightarrow o(a) = \frac{p-1}{(k, p-1)} \mid \frac{p-1}{(n, p-1)}$$

de mivel pontosan a rend többszörösei „jó kitevők”, ezért ez tovább ekvivalens azzal, hogy

$$a^{\frac{p-1}{(n, p-1)}} \equiv 1 \pmod{p}$$

ami éppen a bizonyítandó állítás. ■

Megjegyzés. Az $(a, p) = 1$ feltételre azért van szükség, hogy beszélhessünk a rendjéről. Amennyiben ez nem állna fenn, akkor mivel p prím, ezért $p \mid a$ esetet vizsgálnánk, vagyis $a \equiv 0 \pmod{p}$. De ez nem izgalmas eset, mert $x^n \equiv 0 \pmod{p}$ -nek láthatóan csak $x \equiv 0 \pmod{p}$ tesz eleget.

6.3.1. Példa. Oldjuk meg az $x^{17} \equiv 19 \pmod{23}$ binom kongruenciát!

Az előző tétel alapján mivel $(19, 23) = 1$, továbbá $19^{\frac{22}{(17, 22)}} = 19^{22} \equiv 1 \pmod{23}$ a kis Fermat-tétel miatt, így ez megoldható és a megoldások száma $(17, 22) = 1$ modulo 23.

Előző fejezet végén láttuk, hogy modulo 23 primitív gyök a -2 , és fel is írtuk a táblázatát a hatványainak. Tudjuk, hogy ekkor $\exists y$, melyre $x \equiv (-2)^y$, valamint leolvashatjuk a táblázatból, hogy $19 \equiv \underbrace{-4 \equiv (-2)^{13}}_{\text{táblázat}}$.

Tehát a binom kongruenciánkat átírhatjuk

$$((-2)^y)^{17} = (-2)^{17 \cdot y} \equiv (-2)^{13} \pmod{23}$$

alakba. A megoldandó kongruencia ekkor

$$17 \cdot y \equiv 13 \pmod{22}$$

Innen Algebra1-es a feladat. Átírva $17 \equiv 17 - 22 \equiv -5 \pmod{22}$ és $13 \equiv 13 + 22 \equiv 35 \pmod{22}$ kapjuk, hogy

$$-5 \cdot y \equiv 35 \pmod{22}$$

osztva (-5) -tel

$$y \equiv -7 \equiv 15 \pmod{22}$$

visszahelyettesítve $x \equiv \underbrace{(-2)^{15}}_{\text{táblázat}} \equiv -16 \equiv 7 \pmod{23}$.

7. előadás

Kvadratikus maradékok

7.1. Két négyzetszám tétel

Ebben a fejezetben azt fogjuk vizsgálni, mely számok írhatók fel 2 négyzetszám összegeként. Előtte viszont nézzünk meg néhány randomnak tűnő állítást. Először emlékezzünk vissza egy Algebra1-ben tanult tételre, melyre szükségünk lesz az egyik bizonyításhoz.

7.1.1. Tétel (Wilson-tétel). Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$. ♣

7.1.1. Állítás. Legyen $p > 2$ prímszám. Az $x^2 \equiv a \pmod{p}$ kongruencia ha megoldható, akkor pontosan 2 megoldása van modulo p . ♣

Bizonyítás. Tegyük fel, hogy a kongruencia megoldása b maradékosztály, azaz

$$x^2 \equiv b^2 \equiv a \pmod{p}$$

Ekkor $p \mid x^2 - b^2 = (x-b) \cdot (x+b)$, vagyis $x \equiv \pm b \pmod{p}$, tehát legfeljebb 2 megoldás lehet. Mivel ha b megoldás, akkor $-b$ is, ezért pontosan 2 megoldás van. ■

Megjegyzés. Következmenye a múlt órai 6.3.1 általános esetnek $n = 2$ -re, hogy a megoldások száma $(2, p-1)$ és mivel $p > 2$, így p páratlan, azaz $p-1$ páros, tehát a megoldások száma $(2, p-1) = 2$.

7.1.1. Lemma. Legyen $p > 2$ prímszám. Az $x^2 \equiv -1 \pmod{p}$ megoldható $\Leftrightarrow p = 4k+1$ alakú. ♣

Bizonyítás. Külön bizonyítjuk a 2 irányt.

\Rightarrow irány:

Tegyük fel, hogy $x^2 \equiv -1 \pmod{p}$ megoldható. Mivel $p > 2$ prím, ezért $p-1$ páros, azaz $\frac{p-1}{2}$ egész. Emeljük mindkét oldalt $\frac{p-1}{2}$ hatványra:

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

baloldalt hatványozási azonosságot alkalmazva

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

de mivel p prím, ezért kis Fermat-tétel miatt $x^{p-1} \equiv 1 \pmod{p}$, vagyis azt kaptuk, hogy

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

ami csakis úgy lehetséges, ha $\frac{p-1}{2}$ páros, azaz $2k$ alakú. Innen átrendezéssel:

$$\frac{p-1}{2} = 2k \quad \Leftrightarrow \quad p = 4k + 1$$

\Leftarrow *irány*:

Most tudjuk, hogy $p = 4k + 1$ alakú, azt kell megmutatnunk, hogy $x^2 \equiv -1 \pmod{p}$ kongruenciának van megoldása. Induljunk ki a Wilson-tételből:

$$(p-1)! \equiv -1 \pmod{p}$$

Írjuk ki a faktoriális definíció szerint:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-3) \cdot (p-2) \cdot (p-1) \equiv -1 \pmod{p}$$

Mivel p páratlan ezért $p-1$ páros, azaz kétfelé szedhetjük a baloldali szorzatot. Az első feléből a pozitív tagokat hagyjuk meg, a második feléből a negatívakat¹:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdot \dots \cdot (-3) \cdot (-2) \cdot (-1) \equiv -1 \pmod{p}$$

Itt kétszer látjuk összeszorozva 1-től $\frac{p-1}{2}$ -ig a számokat, aminek fele (tehát $\frac{p-1}{2}$ darab) negatív előjellel van. Hozzuk ki az elejére ezeket a negatív előjeleket, ekkor a megmaradó szorzat:

$$(-1)^{\frac{p-1}{2}} \cdot \left(1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2}\right)^2 \equiv -1 \pmod{p}$$

észrevesszük, hogy a négyzeten lévő tag éppen $\left(\frac{p-1}{2}\right)!$, így

$$(-1)^{\frac{p-1}{2}} \cdot \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$$

Most használjuk, hogy $p = 4k + 1$, mert ekkor $\frac{p-1}{2} = 2k$ páros, vagyis az elején a -1 -es tényező valójában ott sincs. Így módon

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$$

adódik, ami pontosan azt mutatja, hogy az $x^2 \equiv -1 \pmod{p}$ egyenletnek 2 megoldása

$$x \equiv \left(\frac{p-1}{2}\right)! \pmod{p} \quad \text{és} \quad x \equiv -\left(\frac{p-1}{2}\right)! \pmod{p}$$

■

¹szemléletesen mivel modulo p vagyunk, a piros színű p betűket el is hagyhatjuk

7.1.2. Lemma. Legyen $p = 4k - 1$ alakú prím. Ekkor ha $p \mid a^2 + b^2 \Rightarrow p \mid a$ és $p \mid b$. ♣

Bizonyítás. Indirekt tegyük fel, hogy $p \nmid b$ vagy $p \nmid a$. Csak az első esetet nézzük meg, a másikonál ugyanígy kaphatnánk ellentmondást.

Mivel p prím, ezért $(b, p) = 1$ (ez csak 1 vagy p lehetne, de utóbbi esetben $p \mid b$ állna fenn). Ekkor viszont

$$b \cdot x \equiv 1 \pmod{p}$$

kongruenciának létezik megoldása, jelölje ezt most \bar{b} . Feltettük, hogy $p \mid a^2 + b^2$, azaz

$$a^2 + b^2 \equiv 0 \pmod{p}$$

szorozva mindkét oldalt \bar{b}^2 -tel

$$(a^2 + b^2) \cdot \bar{b}^2 \equiv 0 \pmod{p}$$

rendezve

$$(a \cdot \bar{b})^2 + (b \cdot \bar{b}^2) \equiv 0 \pmod{p}$$

de úgy választottuk \bar{b} -t, hogy $b \cdot \bar{b} \equiv 1 \pmod{p}$, azaz

$$(a \cdot \bar{b})^2 + 1 \equiv 0 \pmod{p}$$

de ez azt jelentené, hogy az

$$x^2 \equiv -1 \pmod{p}$$

kongruenciának megoldása $a \cdot \bar{b}$, ami ellentmond a 7.1.1 lemmának, mert aszerint csak akkor lehetne megoldható ez a kongruencia, amennyiben $p = 4k + 1$ alakú, most viszont úgy indultunk, hogy ez nem teljesül. ■

7.1.2. Tétel (Két-négyzetszám-tétel). Legyen n egész szám kanonikus alakja

$$n = 2^\alpha \cdot (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s}) \cdot (q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_t^{\beta_t})$$

ahol $\forall p_i = 4k + 1$ és $\forall q_j = 4k - 1$ alakú. Az n szám pontosan akkor áll elő két négyzetszám összegeként ($\exists x, y: n = x^2 + y^2$), amennyiben $\forall \beta_j$ páros. ♣

Bizonyítás. Szokásosan külön látjuk be az állítás két irányát.

\Rightarrow *irány:* ha egy szám előáll, akkor $4k - 1$ alakú prímek páros hatványon vannak a kanonikus alakjában.

Tegyük fel, hogy $n = a^2 + b^2$ és $p = 4k - 1$ prímre $p \mid n$. Ekkor 7.1.2. lemma miatt $p \mid a$ és $p \mid b$. Vagyis $\exists a_1, b_1 \in \mathbb{Z}$, melyekre $a = p \cdot a_1$ és $b = p \cdot b_1$, azaz $n = (p \cdot a_1)^2 + (p \cdot b_1)^2$.

Láthatóan a jobboldalt osztja p^2 is, tehát $p^2 \mid n$, így $\exists n_1 \in \mathbb{Z}$, melyre $n = p^2 \cdot n_1$.

Amennyiben $p \nmid n_1$, akkor kész vagyunk, n kanonikus alakjában p kitevője 2, ami páros.

Amennyiben $p \mid n_1$, akkor az előző gondolatmenettel haladhatunk tovább és nemcsak p -t, hanem annak négyzetét is kiemelhetjük belőle. Majd újra feltehetjük a kérdést, hogy a megmaradt n_2 számot osztja-e a p . Bármeddig is folytatjuk ezt, n kanonikus alakjában p kitevője véges, tehát valamikor a végére kell jutnunk és addigi utunk során mindig 2. hatványait emelgettük ki a p -nek, így tehát ha k -szor ismételtük meg a kiemelést, akkor p kitevője $2k$, ami páros.

\Leftarrow *irány*: minden ilyen szám előáll két négyzetszám összegeként

A bizonyítás ezen része nem lesz teljes értékű, ugyanis feltesszük, hogy minden $4k + 1$ alakú prímszám előáll két négyzetszám összegeként. Erre később, a Gauss-egészeknél a 9.2.4. tételben visszatérünk, hogy miért igaz.

Tudjuk, hogy most a számunk alakja

$$n = 2^\alpha \cdot (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s}) \cdot (q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_t^{\beta_t})$$

ahol minden $\beta_i = 2 \cdot \gamma_i$, azaz $q_i^{\beta_i} = q_i^{2 \cdot \gamma_i} = (q_i^2)^{\gamma_i}$:

$$n = \overbrace{2 \cdot 2 \cdot \dots \cdot 2}^\alpha \cdot \overbrace{(p_1 \cdot p_1 \cdot \dots \cdot p_1)}^{\alpha_1} \cdot \dots \cdot \overbrace{(p_s \cdot p_s \cdot \dots \cdot p_s)}^{\alpha_s} \cdot \overbrace{(q_1^2 \cdot q_1^2 \cdot \dots \cdot q_1^2)}^{\gamma_1} \cdot \dots \cdot \overbrace{(q_t^2 \cdot q_t^2 \cdot \dots \cdot q_t^2)}^{\gamma_t}$$

vagyis n előáll olyan számok szorzataként, melyek mindegyike felírható két négyzetszám összegeként, hiszen $2 = 1^2 + 1^2$, p_i számokról feltettük, hogy igaz ez rájuk, $q_i^2 = q_i^2 + 0^2$. Elegendő volna tehát azt igazolnunk, hogy ha bizonyos számok felírhatók két négyzetszám összegeként, akkor a szorzatuk is!

Ebből is elegendő két számra igazolnunk, utána teljes indukcióval nyilvánvalóan továbbvihető az állítás. Kéne tehát, hogy ha adott $n, m \in \mathbb{Z}$ és $\exists a, b, c, d \in \mathbb{Z}$ melyekre

$$n = a^2 + b^2 \quad \text{és} \quad m = c^2 + d^2$$

akkor $n \cdot m$ is felírható két négyzetszám összegeként.

Tekintsük az $x = a + bi$ és $y = c + di$ komplex számokat. Ekkor² $n = N(x)$ és $m = N(y)$, továbbá $n \cdot m = N(x) \cdot N(y)$ és mivel komplex számok normáinak szorzata a szorzat normájával egyezik meg

$$n \cdot m = N(x \cdot y) = N((a + bi) \cdot (c + di)) = N((ac - bd) + (bc + ad)i) = (ac - bd)^2 + (bc + ad)^2$$

tehát $n \cdot m$ valóban előállt az $ac - bd$ és $bc + ad$ egész számok négyzeteinek összegeként. ■

7.1.3. Tétel (Négy-négyzetszám-tétel). Minden pozitív egész szám előáll 4 négyzetszám összegeként. ♣

Nem bizonyítjuk, de később gyakorlaton beláttuk az ekvivalens megfogalmazását: minden szám előáll két Gauss-egész négyzetösszegeként.

7.2. Legendre-szimbólum

Ebben a fejezetben az $x^2 \equiv a \pmod{p}$ kongruenciáról lesz szó ($p > 2$ prím). Itt feltehetjük, hogy $(a, p) = 1$, máskülönben az $x^2 \equiv 0 \pmod{p}$ kongruencia megoldásait keresnénk, amit pontosan tudunk, hogy csak a 0 maradékosztály elégíti ki.

Mit jelent szemléletesen, hogy a megoldása az $x^2 \equiv a \pmod{p}$ kongruenciának? Azt, hogy van olyan szám, melynek modulo p a négyzete a . Vagyis, hogy modulo p az a szám négyzetszám. Az ilyen számokat kvadratikuss (négyzetes) maradéknak nevezzük.

²Itt $N(z)$ szokásos módon a komplex szám normáját jelenti, vagyis abszolútértékének négyzetét.

7.2.1. Definíció. Legyen $p > 2$ prím és $(a, p) = 1$. Ha $x^2 \equiv a \pmod{p}$ kongruencia megoldható, akkor az a számot modulo p **kvadratikus maradék**nek nevezzük. Ha nem megoldható, akkor a nem kvadratikus maradék, vagy gyakoribb szóhasználatnál a **kvadratikus nemmaradék**. ♣

A binom kongruenciákról szóló 6.3.1. tétel szerint ennek pontosan akkor létezik megoldása, amennyiben $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Mivel $p > 2$ prím, ezért $p - 1$ páros, tehát $(2, p - 1) = 2$. A feltétel ekkor $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ alakot ölt.

7.2.1. Állítás. Ha $p > 2$ prím és $(a, p) = 1$, akkor $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ vagy $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ♣

Bizonyítás. A kis Fermat-tétel szerint

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

Mivel $p - 1$ páros, ezért $p - 1 = 2k$ alakú

$$a^{2k} \equiv 1 \pmod{p} \Leftrightarrow p \mid a^{2k} - 1 = (a^k - 1) \cdot (a^k + 1)$$

használva p prímtulajdonságát ekkor

$$p \mid a^k - 1 \quad \text{vagy} \quad p \mid a^k + 1$$

átírva kongruenciákra

$$a^k \equiv 1 \pmod{p} \quad \text{vagy} \quad a^k \equiv -1 \pmod{p}$$

ahonnan $k = \frac{p-1}{2}$ visszahelyettesítéssel éppen a bizonyítandót kapjuk

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{vagy} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

■

Következmény: a pontosan akkor kvadratikus maradék modulo p , amennyiben $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, és pontosan akkor kvadratikus nemmaradék, amennyiben $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Látjuk tehát, hogy a -nak ez a bizonyos hatványa különleges szereppel rendelkezik, érdemes rá bevezetnünk egy jelölést.

7.2.2. Definíció (Legendre-szimbólum). Legyen $p > 2$ prím és $(a, p) = 1$. Az $\left(\frac{a}{p}\right)$ (ejtsd: a per p) Legendre-szimbólum (ejtsd: lözsand szimbólum) értéke 1, amennyiben a kvadratikus maradék modulo p , és -1 , ha kvadratikus nemmaradék:

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

♣

Az előző állítás következményéből látjuk, hogy $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Nézzünk szabályokat arra, hogyan tudjuk kiszámolni a Legendre-szimbólum értékét.

7.2.1. Tétel. A Legendre-szimbólum számolási szabályai:

1. Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
3. $\left(\frac{a^2}{p}\right) = 1$
4. $\left(\frac{a^2 \cdot b}{p}\right) = \left(\frac{b}{p}\right)$
5. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4} \\ -1, & \text{ha } p \equiv -1 \pmod{4} \end{cases}$
6. $\left(\frac{1}{p}\right) = 1$



Bizonyítás. Mindegyiket igazolásához az segít, hogy $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Elegendő $\left(\frac{a}{p}\right)$ értékét modulo p vizsgálni, hiszen pontosan akkor lesz kongruens 1-gyel, amennyiben egyenlő is 1-gyel.

1. Ha $a \equiv b \pmod{p}$, akkor $\frac{p-1}{2}$ -edik hatványra emelve a kongruenciát $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod{p}$, ahonnan éppen azt kapjuk, hogy $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \pmod{p}$.
2. $\left(\frac{a \cdot b}{p}\right) \equiv (a \cdot b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
3. $\left(\frac{a^2}{p}\right) \stackrel{2.}{=} \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^2 = 1$, hiszen $\left(\frac{a}{p}\right)$ csak 1 vagy -1 lehet.
4. $\left(\frac{a^2 \cdot b}{p}\right) \stackrel{2.}{=} \left(\frac{a^2}{p}\right) \cdot \left(\frac{b}{p}\right) \stackrel{3.}{=} 1 \cdot \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)$
5. $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$. Ez utóbbi pontosan akkor 1, amennyiben $4 \mid p-1 \Leftrightarrow p \equiv 1 \pmod{4}$ és pontosan akkor -1 , amennyiben $4 \nmid p-1$. Mivel p páratlan, ekkor $p \equiv -1 \pmod{4}$.
6. $\left(\frac{1}{p}\right) \equiv 1^{\frac{p-1}{2}} = 1$



7.2.1. Példa. Számítsuk ki $\left(\frac{180}{31}\right)$ értékét!

Az 1. szabály alapján tekinthetem a 180-at modulo 31, ezzel a szimbólum értéke nem változik, majd 3. szabály alapján az érték 1:

$$\left(\frac{180}{31}\right) \stackrel{1.}{=} \left(\frac{25}{31}\right) = \left(\frac{5^2}{31}\right) \stackrel{3.}{=} 1$$

Ezek segítségével még nem tudunk biztosan kiszámolni egy Legendre-szimbólum értéket, szükségünk van további állításokra, ezeket viszont egyelőre az idei félévben nem bizonyítjuk.

7.2.2. Tétel.

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



7.2.3. Tétel (Kvadratikus reciprocitás).

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{ha } p \equiv 1 \pmod{4} \text{ vagy } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right), & \text{ha } p \equiv q \equiv -1 \pmod{4} \end{cases}$$



7.2.2. Példa. Számoljuk ki $\left(\frac{6}{13}\right)$ és $\left(\frac{501}{37}\right)$ értékét!

$$(a) \left(\frac{6}{13}\right) \stackrel{2.}{=} \left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) \stackrel{7.2.2}{=} -1 \cdot \left(\frac{3}{13}\right) \stackrel{7.2.3}{=} -\left(\frac{13}{3}\right) \stackrel{1.}{=} -\left(\frac{1}{3}\right) \stackrel{6.}{=} -1,$$

$$(b) \left(\frac{501}{37}\right) \stackrel{1.}{=} \left(\frac{20}{37}\right) = \left(\frac{2^2 \cdot 5}{37}\right) \stackrel{4.}{=} \left(\frac{5}{37}\right) \stackrel{7.2.3}{=} \left(\frac{37}{5}\right) \stackrel{1.}{=} \left(\frac{2}{5}\right) \stackrel{7.2.2}{=} -1$$

tehát a 6 kvadratikus nemmaradék modulo 13, vagyis az $x^2 \equiv 6 \pmod{13}$ kongruenciának nincs megoldása, hasonlóan $x^2 \equiv 501 \pmod{37}$ kongruenciának sem.

Nézzünk még néhány állítást, amik a primitív gyökök és a kvadratikus maradékok között teremtenek kapcsolatot.

7.2.2. Állítás. Legyen g primitív gyök modulo p . Ekkor g^i pontosan akkor primitív gyök modulo p , amennyiben $(i, p-1) = 1$.



Bizonyítás. A 6.1.3. tétel képletét használhatjuk:

$$o(g^i) = \frac{o(g)}{(i, o(g))}$$

mivel g primitív gyök: $o(g) = p-1$, és g^i is pontosan akkor primitív gyök, ha $o(g^i) = p-1$:

$$p-1 \stackrel{\text{kellene}}{=} o(g^i) = \frac{p-1}{(i, p-1)}$$

átrendezve adódik $(i, p-1) = 1$.



7.2.1. Lemma. Ha g primitív gyök modulo p , akkor g kvadratikus nemmaradék modulo p .



Bizonyítás. Azt kell belátnunk, hogy

$$o(g) = p - 1 \Rightarrow \left(\frac{g}{p}\right) = -1$$

Indirekt tegyük fel, hogy

$$1 = \left(\frac{g}{p}\right) \equiv a^{\frac{p-1}{2}} (p)$$

ez viszont ellentmondás, mivel azt látjuk, hogy $\frac{p-1}{2}$ egy „jó kitevő”, ami csak a rend többszöröse lehet, tehát

$$p - 1 = o(g) \mid \frac{p-1}{2}$$

ami lehetetlen. ■

7.2.4. Tétel. Legyen g primitív gyök modulo p . A g^i pontosan akkor kvadratikusan maradék modulo p , amennyiben i páros. ♣

Bizonyítás. Azt kell belátnunk, hogy

$$\left(\frac{g^i}{p}\right) = 1 \Leftrightarrow 2 \mid i$$

Először belátjuk, hogy a páros hatványok kvadratikusan maradékok, utána a páratlanokról, hogy azok kvadratikusan nemmaradékok.

Páros eset: $i = 2k$

$$\left(\frac{g^{2k}}{p}\right) = \left(\frac{(g^k)^2}{p}\right) \stackrel{3.}{=} 1$$

Páratlan eset: $i = 2k + 1$

$$\left(\frac{g^{2k+1}}{p}\right) = \left(\frac{g^{2k} \cdot g}{p}\right) \stackrel{2.}{=} \left(\frac{g^{2k}}{p}\right) \cdot \left(\frac{g}{p}\right) \stackrel{\text{páros eset}}{=} \left(\frac{g}{p}\right) \stackrel{7.2.1. \text{ lemma}}{=} -1$$
■

7.3. π féleképpen

7.3.1. Tétel. Egy szám átlagosan π féleképpen áll elő 2 négyzetszám összegeként. ♣

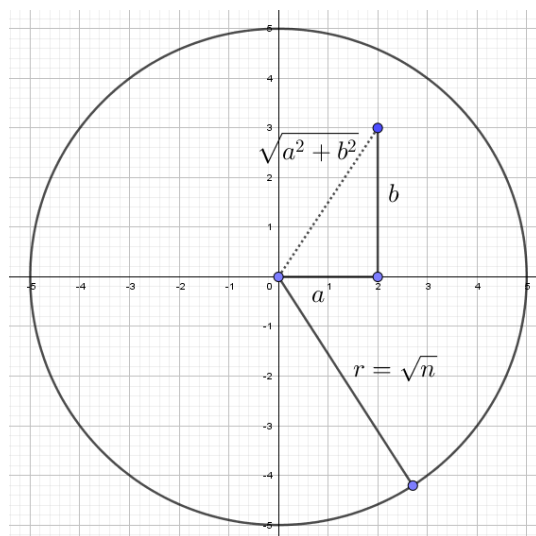
Tisztáznunk kell, hogy az átlag szó alatt itt mit értünk? Végtelen sok szám van, kiszámolhatjuk mindegyikre, hogy hányféleképpen áll elő két négyzetszám összegeként, de hogyan átlagoljuk a végtelen sok számot? Természetesen határértékkel. Az állítás tehát valójában azt mondja, hogy tekintsük a részátlagok sorozatának határértékét, ahol részátlag alatt azt értem, hogy n -ig átlagosan hányféleképpen áll elő egy szám két négyzetszám összegeként:

$$A_n = \frac{|(a, b) \text{ párok, melyekre } a^2 + b^2 \leq n|}{n}$$

Így a tétel a következőt mondja ki:

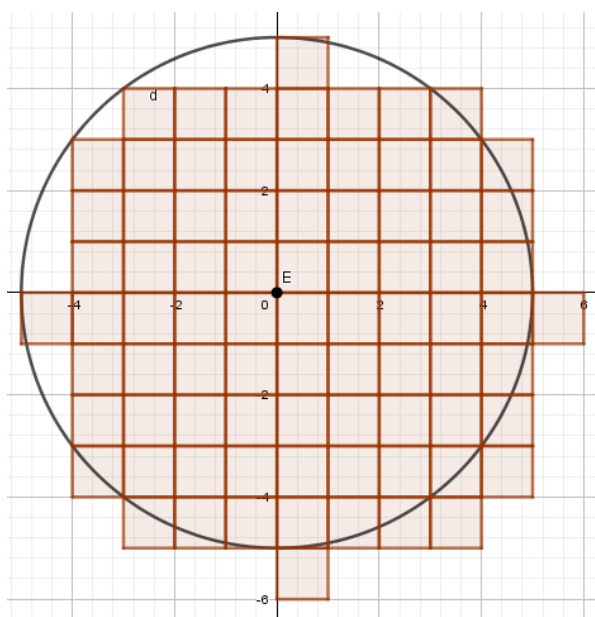
$$\lim_{n \rightarrow \infty} A_n = \pi$$

Bizonyítás. Tekintsük az $r = \sqrt{n}$ sugarú kört. Hány olyan (a, b) számpár van, melyre $a^2 + b^2 \leq n$? Másféleképpen fogalmazva ez azt jelenti, hogy hány olyan (a, b) egész koordinátájú pont van, melyre $\sqrt{a^2 + b^2} \leq \sqrt{n}$, vagyis melyek a kör belsejében vannak?



7.1. ábra. Pontok a körön belül

Ezeket a kör belsejébe eső egész koordinátájú pontokat szokás rácspontoknak is nevezni. Hogyan tudnánk megbecsülni adott n mellett a \sqrt{n} sugarú kör belsejébe eső rácspontok számát? Tegyük minden rácspontba egy egységoldalú négyzetet úgy, hogy a négyzet bal felső sarka legyen a rácspont:

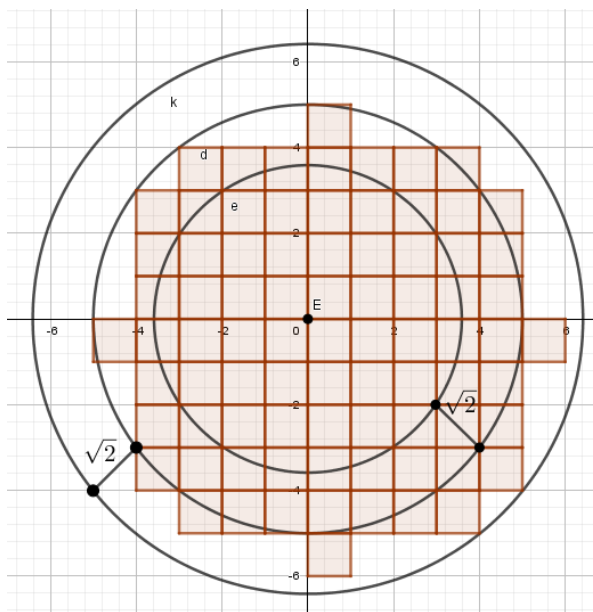


7.2. ábra. Négyzetek

Ha ezen négyzetek területét becsüljük meg, ugyanazt a számot kapjuk, mintha a pontok számát

becsülnénk. Látjuk, hogy a négyzetek „körülbelül kitöltik” a kört. Az a baj, hogy bizonyos pontok kilógnak, bizonyos pontjait pedig nem fedik le.

Vegyünk egy olyan kört, aminek sugara $\sqrt{n} - \sqrt{2}$ és egy olyat, melynek $\sqrt{n} + \sqrt{2}$.



7.3. ábra. Új körök

Mivel az egységoldalú négyzet két legtávolabbi pontja $\sqrt{2}$, így a kisebb körnek minden egyes pontját fedi valamely pontja valamely négyzetnek. Tehát a kisebb kör területe jó alsó becslés a négyzetek területére (azaz a pontok számára). Hasonlóan a külső kör területe jó felső becslés, tehát:

$$(\sqrt{n} - \sqrt{2})^2 \cdot \pi \leq T \leq (\sqrt{n} + \sqrt{2})^2 \cdot \pi$$

osztva n -nel:

$$\frac{(\sqrt{n} - \sqrt{2})^2 \cdot \pi}{n} \leq A_n \leq \frac{(\sqrt{n} + \sqrt{2})^2 \cdot \pi}{n}$$

Közrefogtuk A_n sorozatot két olyan sorozattal, melyek mindegyike π -hez tart (például):

$$\lim_{n \rightarrow \infty} \frac{(\sqrt{n} - \sqrt{2})^2 \cdot \pi}{n} = \lim_{n \rightarrow \infty} \frac{(n - 2\sqrt{2n} + 2) \cdot \pi}{n} = \pi \cdot \lim_{n \rightarrow \infty} \left(\frac{n}{n} - 2\sqrt{\frac{2n}{n^2}} + \frac{2}{n} \right) = \pi \cdot (1 - 0 + 0) = \pi$$

Így tehát a rendőrlv miatt $\lim_{n \rightarrow \infty} A_n = \pi$. ■

8. előadás

Fermat, Wiles, Rivest, Shamir, Adleman

8.1. Pitagoraszai számhármassok (emlék)

8.1.1. Lemma (Szorzat-hatvány lemma). Legyen R egy alaptételes gyűrű. Amennyiben $a, b \in R$, $(a, b) = 1$ és $\exists x \in R, n \in \mathbb{Z}$ melyre $a \cdot b = x^n$ akkor $\exists u, v \in R$ melyekre $a = \varepsilon u^n$ és $b = \varepsilon v^n$ ahol ε az R gyűrű (egyik) egysége. ♣

Röviden, a lényeget kiemelve, de pontatlanul leírva:

$$(a, b) = 1 \quad \text{és} \quad a \cdot b = x^n \quad \Rightarrow \quad a = u^n \quad \text{és} \quad b = v^n$$

Megjegyzés. Kellenek az egységszerekek, hiszen $R = \mathbb{Z}$ esetén $a = -1$, $b = -1$ és $n = 2$ szereposztással $\exists x \in \mathbb{Z}$, melyre $a \cdot b = (-1) \cdot (-1) = x^2$, ilyen például az $x = 1$. De az nem igaz, hogy $\exists u, v \in \mathbb{Z}$, melyekre $a = -1 = u^2$ és $b = -1 = v^2$.

8.1.1. Tétel. Az $x^2 + y^2 = z^2$ egyenlet alapmegoldásai (melyekre $(x, y, z) = 1$):

$$x = 2 \cdot r \cdot s \quad \text{és} \quad y = r^2 - s^2 \quad \text{és} \quad z = r^2 + s^2$$

ahol $(r, s) = 1$ és $r \not\equiv s \pmod{2}$. ♣

8.2. Fermat-sejtés, Wiles-tétel

8.2.1. Tétel (Fermat-sejtés, Wiles-tétel). Az $x^n + y^n = z^n$ egyenlet $n \geq 3$ esetén nem oldható meg a pozitív egész számok körében. ♣

8.2.2. Tétel. Az $x^4 + y^4 = z^2$ egyenlet nem oldható meg a pozitív egész számok körében. ♣

8.3. Titkosírás (RSA)

Ez a fejezet szolgált volna eredetileg az RSA titkosírás működésének leírására, ugyanakkor többek között időhiány miatt ez végül nem készül el. Elméletileg Algebra1-ből már volt szó róla, ott érdemes megnézni, meghallgatni a hanganyagot, illetve Freud: Számelmélet könyvében az 5.8.1 Tételt és „környezetét” megnézni.

9. előadás

Egészen új egészek

9.1. Gauss-egészek

9.1.1. Definíció. Azokat az komplex számokat, melyek valós és képzetes része is egész, **Gauss-egészeknek** nevezzük. A Gauss-egészek halmazát jelöli¹ $\mathcal{G} = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ ♣

A Gauss-egészeket gyakran görög abc betűivel fogjuk jelölni.

Algebra2-ből a komplex számoknak láttuk egy geometriai átfogalmazását, bevezettük a komplex számsíkot. Sokszor hasznos úgy gondolkodnunk, hogy a Gauss-egészek a komplex számsík rácspontjainak felelnek meg.

9.1.1. Tétel. A Gauss-egészek gyűrűt alkotnak a szokásos komplex számokra definiált összeadásra és szorzásra: $(\mathcal{G}, +, \cdot)$ gyűrű. ♣

Bizonyítás. Mivel $\mathcal{G} \subseteq \mathbb{C}$, ezért csak azt kell belátnunk, hogy zárt az összeadásra és szorzásra, van nullelem és ellentett.

- Összeadásra zártság: adott $\alpha = a + bi \in \mathcal{G}$ és $\beta = c + di \in \mathcal{G}$, kellene: $\alpha + \beta \in \mathcal{G}$. Ez nyilván teljesül, hiszen $\alpha + \beta = (a + c) + (b + d)i$ ahol $a + c \in \mathbb{Z}$ és $b + d \in \mathbb{Z}$ tehát $\alpha + \beta \in \mathcal{G}$
- Szorzásra zártság: adott $\alpha = a + bi \in \mathcal{G}$ és $\beta = c + di \in \mathcal{G}$, kellene: $\alpha \cdot \beta \in \mathcal{G}$. Ez nyilván teljesül, hiszen $\alpha \cdot \beta = (ac - bd) + (ad + bc)i$ ahol $ac - bd \in \mathbb{Z}$ és $ad + bc \in \mathbb{Z}$ tehát $\alpha \cdot \beta \in \mathcal{G}$
- Van nullelem: $0 = 0 + 0 \cdot i \in \mathcal{G}$
- Van ellentett: Adott $a + bi \in \mathcal{G}$ esetén $-a - bi \in \mathcal{G}$ teljesül.

■

¹sok helyen $\mathbb{Z}[i]$ jelöléssel is találkozhatunk

Sőt ennél többet is látunk, \mathcal{G} egy szokásos gyűrű. A szorzás kommutatív, nullosztómentes (hiszen ha lennének nullosztók, akkor a komplex számok testében is, ami nyilván nem lehet) és egységelemes, hiszen $1 = 1 + 0 \cdot i \in \mathcal{G}$.

Emlék: Szokásos gyűrűkre vezettünk be számelméleti fogalmakat és azt is láttuk (2.2.1. tétel), hogy ha egy gyűrű euklideszi, akkor alaptételes is (teljesül benne a számelmélet alaptétele). Jó lenne, ha be tudnánk látni, hogy \mathcal{G} euklideszi.

Emlék: Komplex számok normájáról beláttuk (Algebra2), hogy szorzat normája a normák szorzata ($N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$) és csakis a 0 komplex szám normája 0: $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.

9.1.2. Tétel. A Gauss-egészek gyűrűje euklideszi.



Bizonyítás. Azt kellene belátnunk, hogy létezik „maradékos osztás”, vagyis a 1.2.6. definíció szerint keresünk egy $\varphi: \mathcal{G} \setminus \{0\} \rightarrow \mathbb{Z}^+$ leképezést, melyre $\forall \alpha, \beta \in \mathcal{G} \setminus \{0\}$ esetén $\exists \gamma, \delta \in \mathcal{G}$ melyre

$$\alpha = \beta \cdot \gamma + \delta \quad \text{és} \quad \varphi(\delta) < \varphi(\beta) \quad \text{vagy} \quad \delta = 0$$

A norma éppenséggel nekünk egy jó φ leképezés lesz most. Az értelmezett 0 komplex számra is, de ez most nekünk nem baj, sőt előnyünkre is válik, mert nem kell a $\delta = 0$ esettel foglalkoznunk, hiszen akkor $N(\delta) = 0$, tehát $N(\delta) = 0 < N(\beta)$ automatikusan teljesül, hiszen $N(\beta) \neq 0$, mert csak a 0 szám normája lehet 0.

Hasznos továbbá ha Gauss-egészek helyett komplex számokban gondolkozunk és úgy fogalmazzuk át milyen γ és δ megtalálása a célunk. Komplex számokba átlépve a $\beta \neq 0$, tehát van neki inverze, oszthatunk vele:

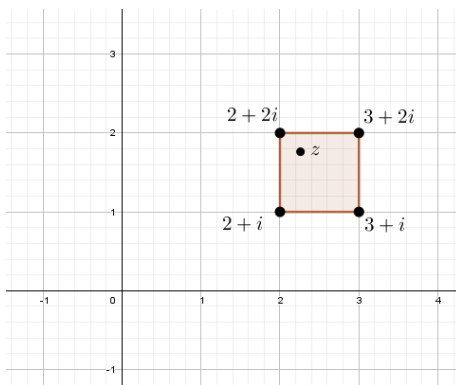
$$\frac{\alpha}{\beta} = \gamma + \frac{\delta}{\beta} \quad \text{és} \quad N(\delta) < N(\beta) \Leftrightarrow N\left(\frac{\delta}{\beta}\right) < 1$$

Az α és β adottak, tehát ki tudjuk számolni a hányadosukat, legyen ez $z = \frac{\alpha}{\beta} \in \mathbb{C}$ komplex szám a komplex síkon. Találunk kell olyan $\gamma \in \mathcal{G}$ Gauss-egészt, azaz rácspontot, melytől a z eltérése „kisebb” mint 1.

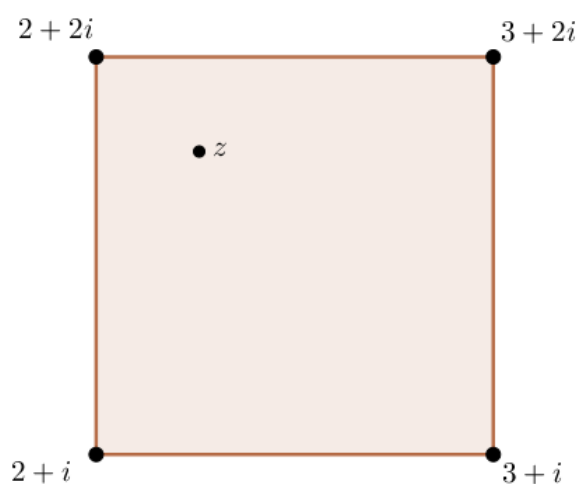
Ez az idézőjel azért van itt, mert komplex számokra nincs rendezésünk, de a norma már valós, arra van, tehát:

$$z - \gamma = \frac{\delta}{\beta} \Rightarrow N(z - \gamma) = N\left(\frac{\delta}{\beta}\right) < 1$$

Hogyan állítsunk elő ilyen γ Gauss-egészt? Keressük először is meg a z komplex számot a komplex síkon. Mondjuk megtaláltuk itt:

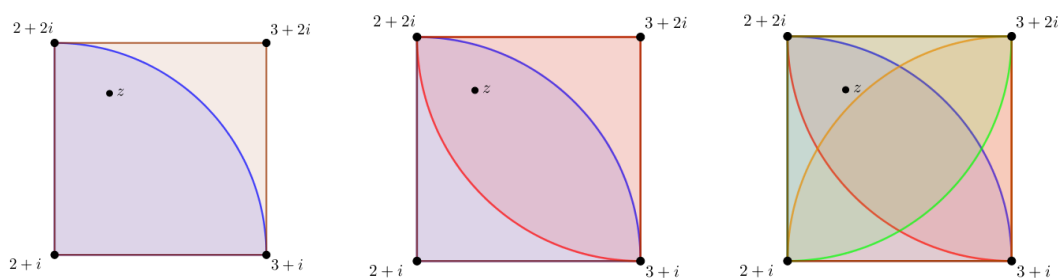


Innentől kezdve csak azzal az egységoldalú négyzettel fogunk foglalkozni, mely tartalmazza z -t és csúcsai rácspontok (ilyen nem feltétlenül 1 van, lehet 4 is, de akkor válasszunk egyet):



Elég volna megmutatnunk, hogy ennek a négyzetnek van olyan csúcsa, melytől z távolsága legfeljebb 1, az általa reprezentált Gauss-egész jó lesz γ választásnak, továbbá $\delta = \alpha - \beta \cdot \gamma$ választással δ is meglenne.

Nézzük meg mik azok a pontok, amelyek az egyes csúcsoktól legfeljebb 1 távolságra vannak, vagyis mely pontokhoz lennének jó választások az egyes csúcsok:



Látjuk, hogy már a bal alsó rácspont is jó választás lenne most számunkra, de általánosságban kell gondolkoznunk.

A bal alsó és a jobb felső rácspont valamelyike általánosságban is minden z esetén jó választás, ahogy az ábrán látható: nincs olyan pontja az egységnégyzetnek, mely távolsága mindkettőtől 1-nél több volna.

Bár a második kép is tanulságos olyan szempontból, hogy van ami kétszer is fedésbe került (tehát több jó rácspont is választható hozzá), a harmadik képen látszik igazán, hogy minden pont esetén legalább 2 rácspont választható volna, tehát ez a bizonyos „maradékos osztás” nem egyértelmű! (Nem is volt célunk, hogy az legyen, csak megmutatni, hogy van). ■

Innen tehát automatikusan következik, hogy teljesül a számelmélet alaptétele \mathcal{G} -ben. Ezért jó az euklideszi tulajdonsága egy gyűrűnek. Hamarabb beláttuk a SZAT-ot, minthogy megvizsgáltuk volna az egységeket vagy prímekeket a gyűrűben. Kerítsünk azért erre is sort.

9.1.1. Lemma. Minden Gauss-egész osztja a normáját: $\forall \alpha \in \mathcal{G}$ -re: $\alpha \mid N(\alpha)$ ♣

Bizonyítás. Azt kell belátnunk, hogy $\exists \beta \in \mathcal{G}$, melyre $\alpha \cdot \beta = N(\alpha)$.

Tudjuk, hogy $N(\alpha) = \alpha \cdot \bar{\alpha}$, és ha $\alpha = a + bi$ Gauss-egész, akkor $\bar{\alpha} = a - bi$ is Gauss-egész. Így $\beta = \bar{\alpha}$ választással máris látjuk, hogy $\alpha \mid N(\alpha)$. ■

9.1.2. Lemma. Legyenek $\alpha, \beta \in \mathcal{G}$ és $\alpha \mid \beta$. Ekkor $N(\alpha) \mid N(\beta)$ is teljesül. ♣

Bizonyítás. A feltétel szerint $\exists \gamma \in \mathcal{G}$, melyre $\beta = \alpha \cdot \gamma$. Ekkor mindkét oldal normáját véve

$$N(\beta) = N(\alpha \cdot \gamma) = N(\alpha) \cdot N(\gamma)$$

ami éppen azt jelenti, hogy $N(\alpha) \mid N(\beta)$. ■

9.1.3. Tétel. A Gauss-egészek között 4 egység létezik, ezek: $1, -1, i, -i$. ♣

Bizonyítás. Egységek azok, amelyek osztják a gyűrű egységelemét, tehát az 1-et: $\varepsilon \mid 1$. A 9.1.2. lemma alapján ekkor $N(\varepsilon) \mid N(1) = 1$.

Amennyiben $\varepsilon = a + bi$ alakú, akkor $N(\varepsilon) = a^2 + b^2$. Mivel egész számok körében az 1-nek csak 2 osztója van, ezért 2 lehetséges esetünk van:

$$a^2 + b^2 = 1 \quad \text{vagy} \quad a^2 + b^2 = -1$$

Utóbbi nyilvánvalóan nem lehetséges, mert baloldalon nemnegatív, jobboldalon pedig negatív szám áll. Mi a helyzet az elsővel? Hányféleképpen áll elő az 1 két négyzetszám összegeként? Négyféleképpen:

$$1 = 1^2 + 0^2 \quad \text{vagy} \quad 1 = (-1)^2 + 0^2 \quad \text{vagy} \quad 1 = 0^2 + 1^2 \quad \text{vagy} \quad 1 = 0^2 + (-1)^2$$

az egyes esetekben az ε komplex szám értéke:

$$\varepsilon = 1 + 0 \cdot i = 1 \quad \text{vagy} \quad \varepsilon = -1 + 0 \cdot i = -1 \quad \text{vagy} \quad \varepsilon = 0 + 1 \cdot i = i \quad \text{vagy} \quad \varepsilon = 0 - 1 \cdot i = -i$$

Tehát itt pontosan 4 egységünk van, úgy is mondhatnám a Gauss-egészek között 4-féle „előjele” létezik minden számnak.

Megjegyzés. Vannak olyan alaptételes gyűrűk is, amelyekben végtelen sok egység van. Ilyen például $\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Z}\}$. Itt egység a $\sqrt{2} + 1$, hiszen

$$(\sqrt{2} - 1) \cdot (\sqrt{2} + 1) = 1 \Rightarrow \sqrt{2} + 1 \mid 1$$

De ha valami egység, akkor annak négyzete, sőt akárhanyadik hatványa is, tehát $(\sqrt{2} + 1)^n$ mindannyian egységek és különböző n -ek esetén különböző számok az exponenciális függvény szigorú monotonitása miatt. Tehát itt máris mutattunk végtelen sok egységet.

9.2. Gauss-prímek

Ebben a fejezetben arra a kérdésre keressük a választ, hogy melyek a Gauss-prímek \mathcal{G} -ben. Ehhez jó néhány segédállításra szükségünk lesz. Jelzem, hogy ebben a fejezetben inkább a Freud: Számelmélet könyv szerint haladok, az alapján nekem könnyebb volt megérteni ezt a témakört.

A Gauss-prímeket általában π görög betűvel fogom jelölni.

9.2.1. Lemma. Egy $\pi \in \mathcal{G}$ Gauss-prím normája legalább 2: $N(\pi) \geq 2$



Bizonyítás. Legyen $\pi = a + bi$, ekkor azt kellene igazolnunk, hogy $N(\pi) = a^2 + b^2 \geq 2$. Tudjuk, hogy bármely komplex szám normája nemnegatív, tehát ha ez nem lenne igaz, akkor $a^2 + b^2 = 0$ vagy $a^2 + b^2 = 1$ lehetne. Mindkettő ellentmondás, mert első esetben $\pi = 0$, ami nem prím, másik esetben pedig π egység volna, ami szintén nem lehet prím (a prímtulajdonság definíciója úgy kezdődik, hogy olyan egységtől különböző szám, melyre...). ■

9.2.2. Lemma. Amennyiben $\pi \in \mathcal{G}$ prím, akkor $\exists p \in \mathbb{Z}$, melyre $\pi \mid p$.



Bizonyítás. A 9.1.1. lemma alapján $\pi \mid N(\pi)$. Mivel π prím 9.2.1. lemma miatt $N(\pi) \geq 2$, tehát nem 0 és nem egység. Ekkor a \mathbb{Z} -ben teljesülő számelmélet alaptétele miatt van neki prímtényező felbontása:

$$N(\pi) = p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n}$$

tehát visszatérve a Gauss-egészek körébe $\pi \mid p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n}$ használva π prímtulajdonságát ha egy szorzatot oszt, akkor annak valamely tényezőjét is, tehát $\exists p$ prím, melyre $\pi \mid p$. Ezt kellett igazolni. ■

Ez jó hír, ezek szerint úgy érdemes keresnünk a Gauss-prímeket, hogy a szokásos egész prímeink osztóit vizsgáljuk. Látni fogjuk, hogy megint érdemes különvenni a 2 -t, a $4k - 1$ alakú, és a $4k + 1$ alakú prímeiket. Lesz ezek közül amelyik megmarad Gauss-prímnak is, de olyan is ami felbomlik. Hasznos észrevétel, hogy igencsak korlátozottan tudnak a prímeink felbomlani Gauss-prímek szorzatára, legfeljebb 2 -re.

9.2.3. Lemma. Minden p pozitív prímszám vagy maga is Gauss-prím, vagy pedig pontosan két Gauss-prímnak a szorzata, amelyek normája p és amelyek egymás konjugáltjai.²



²Freud: Számelmélet, 7.4.14. Tétel (ii)

Bizonyítás. Azt kell belátnunk, hogy ha p nem Gauss-prím, akkor ő pontosan 2 Gauss-prím szorzata.

Mivel p nem Gauss-prím, a számelmélet alaptétele szerint \mathcal{G} -ben p felbomlik legalább 2 Gauss-prím szorzatára: $\exists \pi_1, \pi_2, \dots, \pi_r$

$$p = \pi_1 \cdot \pi_2 \cdot \dots \cdot \pi_r$$

Mindkét oldal normáját véve:

$$p^2 = N(p) = N(\pi_1 \cdot \pi_2 \cdot \dots \cdot \pi_r) = N(\pi_1) \cdot N(\pi_2) \cdot \dots \cdot N(\pi_r)$$

Mivel itt minden π_i Gauss-prím, ezért 9.2.1. lemma szerint $N(\pi_i) \geq 2$, tehát a jobboldali szorzat egyik tényezője sem egység.

Viszont p^2 csakis úgy bontható legalább 2 szám szorzatára (melyek egyike sem egység), hogy $p^2 = p \cdot p$. Tehát azt kaptuk, hogy jobboldalon pontosan 2 szám áll, azaz $p = \pi_1 \cdot \pi_2$.

De azt is tudjuk, hogy mindkét Gauss-prím normája p kell legyen, tehát speciálisan az első is $p = N(\pi_1) = \pi_1 \cdot \overline{\pi_1}$. Tehát valóban p két olyan Gauss-prím szorzataként áll elő, melyek egymás konjugáltjai. ■

9.2.1. Tétel. A 2 kanonikus alakja $2 = (-i) \cdot (1 + i)^2$ ♣

Bizonyítás. A 2 felbontható 2 Gauss-prím szorzatára, így ő nem Gauss-prím: $2 = (1 + i) \cdot (1 - i)$. A 9.2.3. lemma alapján mivel 2 nem Gauss-prím, ezért pontosan 2 Gauss-prím szorzataként áll elő, melyek egymás konjugáltjai: $1 + i$ és $1 - i$. De vigyázat! Ez nem 2 különböző Gauss-prím, ez csak 1, hiszen $1 - i = (-i) \cdot (1 + i)$, tehát ezek egységszeresei egymásnak.

Vagyis a 2-nek egységszerestől eltekintve egyetlen prímosztója van, az $1 + i$, melynek négyzetével is osztható. Mivel a 2 csupán egységszerese $(1 + i)^2$ -nek, ezért a 2 kanonikus alakja

$$2 = \varepsilon \cdot \pi_1^{\alpha_1} \cdot \dots \cdot \pi_r^{\alpha_r} = (-i) \cdot (1 + i)^2$$

■

9.2.2. Tétel. A $p = 4k - 1$ alakú prímek Gauss-prímek is. ♣

Bizonyítás. Indirekt tegyük fel, hogy egy $p = 4k - 1$ alakú prím nem Gauss-prím. Ekkor a 9.2.3. lemma szerint 2 olyan Gauss-prím szorzata, melyek normája p . Tehát van olyan Gauss-prím, legyen ez most $\pi = a + bi$, melynek normája: $N(\pi) = a^2 + b^2 = p$. De ez ellentmond a két-négyzetszám tételnek (7.1.2. tétel), hiszen p kanonikus alakjában (ami $p = p^1$) szerepel egy $4k - 1$ alakú prím páratlan hatványon. ■

9.2.3. Tétel. A $p = 4k + 1$ alakú prímek nem Gauss-prímek, egységszerestől eltekintve egyértelműen felbomlanak 2 Gauss-prím szorzatára, melyek egymás konjugáltjai, de nem egymás egységszeresei. ♣

Bizonyítás. Itt jó néhány dolgot be kell látnunk, haladjunk lépésekben.

Nem prímek:

Indirekt tegyük fel, hogy $p = 4k + 1$ Gauss-prím. Ekkor 7.1.1. lemma szerint $x^2 \equiv -1 \pmod{p}$ kongruencia megoldható, vagyis $\exists x$ melyre $p \mid x^2 + 1 = (x+i) \cdot (x-i)$. Feltettük, hogy p Gauss-prím és egy prím ha oszt egy szorzatot, akkor valamelyik tényezőt is, azaz

$$p \mid x+i \quad \text{vagy} \quad p \mid x-i$$

Az oszthatóság definíciója szerint $\exists \alpha = a + bi \in \mathcal{G}$, Gauss-egész, melyre

$$p \cdot (a + bi) = x + i \quad \text{vagy} \quad p \cdot (a + bi) = x - i$$

beszorozva

$$p \cdot a + p \cdot b \cdot i = x + 1 \cdot i \quad \text{vagy} \quad p \cdot a + p \cdot b \cdot i = x + (-1) \cdot i$$

komplex számok egyenlősége esetén a képzetes részük is megegyezik (ami jelen esetben egész)

$$p \cdot b = 1 \quad \text{vagy} \quad p \cdot b = -1$$

ami ellentmondás, mert sem az 1-nek, sem a -1 -nek nem lehet osztója egy p prímszám.

Egyértelműen felbomlanak:

Azt már nem kell igazolni, hogy felbomlanak pontosan 2 Gauss-prím szorzatára, melyek normája p és egymás konjugáltjai, hiszen 9.2.3. lemma szerint ez minden $p \in \mathbb{Z}$ prímre teljesül ami nem Gauss-prím.

Az egyértelműség rész van hátra. Tegyük fel, hogy többféleképpen is felbomlik:

$$p = \pi_1 \cdot \overline{\pi_1} = \pi_2 \cdot \overline{\pi_2}$$

ahol $p = N(\pi_1) = N(\overline{\pi_1}) = N(\pi_2) = N(\overline{\pi_2})$. Ekkor $\pi_2 \mid \pi_1 \cdot \overline{\pi_1}$, tehát a prímtulajdonság miatt a szorzat egyik tényezőjét is osztja:

$$\pi_2 \mid \pi_1 \quad \text{vagy} \quad \pi_2 \mid \overline{\pi_1}$$

Belátható, hogy első esetben $\pi_2 = \varepsilon \cdot \pi_1$, másodikban $\pi_2 = \varepsilon \cdot \overline{\pi_1}$. Mindkét esetben azt használjuk ki, hogy normájuk megegyezik. Például az első esetet én úgy csinálnám, hogy

$$\pi_2 \mid \pi_1 \quad \Rightarrow \quad \exists \gamma: \gamma \cdot \pi_2 = \pi_1$$

Mindkét oldal normáját véve

$$N(\gamma \cdot \pi_2) = N(\gamma) \cdot N(\pi_2) = N(\pi_1)$$

használva, hogy $N(\pi_1) = N(\pi_2) = p$

$$N(\gamma) \cdot p = p \quad \Rightarrow \quad N(\gamma) = 1$$

vagyis $\gamma = \varepsilon$ egység.

Nem egymás egységszeresei:

Itt csak végig kell próbálgatni, hogy mikor lehet egy Gauss-egész és konjugáltja egymás egységszerese. Meg kell nézni, hogyha az egyiket megszorozom egy egységgel, mikor kaphatom a másikat. A 4 egység szerint nézzük meg a 4 esetet: $\alpha = a + bi, \overline{\alpha} = a - bi, \varepsilon$ egység, milyen feltétel esetén lesz $\varepsilon \cdot \alpha = \overline{\alpha}$? (Tudjuk azt is, hogy $N(\alpha) = p$ prímszám.)

- $\varepsilon = 1$ esetén:

$$1 \cdot (a + bi) = a - bi \Rightarrow a = a \text{ és } b = -b \Rightarrow \alpha = a$$

vagyis $N(\alpha) = N(a) = a^2 \neq p$ prímszám.

- $\varepsilon = -1$ esetén:

$$-1 \cdot (a + bi) = a - bi \Rightarrow -a = a \text{ és } -b = -b \Rightarrow \alpha = b \cdot i$$

vagyis $N(\alpha) = N(b \cdot i) = b^2 \neq p$ prímszám.

- $\varepsilon = i$ esetén:

$$i \cdot (a + bi) = a - bi \Rightarrow -b = a \text{ és } a = -b \Rightarrow \alpha = a - ai$$

vagyis $N(\alpha) = N(a - ai) = 2 \cdot a^2 \neq p = 4k + 1$ alakú prímszám.

- $\varepsilon = -i$ esetén:

$$-i \cdot (a + bi) = a - bi \Rightarrow b = a \text{ és } -a = -b \Rightarrow \alpha = a + ai$$

vagyis $N(\alpha) = N(a + ai) = 2 \cdot a^2 \neq p = 4k + 1$ alakú prímszám.

■

Ezzel az előbbi tétellel egyben törlesztettük egy régi adósságunkat is, a két-négyzetszám tétellel kapcsolatban.

9.2.4. Tétel. Minden $4k + 1$ alakú prímszám előáll 2 négyzetszám összegeként.

♣

Bizonyítás. Az előző, 9.2.3. tétel szerint minden $p = 4k + 1$ alakú prímszámhoz egyértelműen léteznek π_1, π_2 Gauss-prímek, melyekre $p = \pi_1 \cdot \pi_2$ és ezek egymás konjugáltjai, valamint mindkettő normája $N(\pi_1) = N(\pi_2) = a^2 + b^2 = p$.

■

Megjegyzés. Ezzel nem csak azt láttuk be, hogy minden $p = 4k + 1$ alakú prímszám előáll két négyzetszám összegeként, de ráadásul ez az előállítás a és b sorrendjétől és egységszeresektől eltekintve egyértelmű.

Összefoglalva: A Gauss-prímek tehát a következők (és ezek egységszereseik):

- $1 + i$
- p , ahol $p = 4k - 1 \in \mathbb{Z}$ prím
- π és $\bar{\pi}$, ahol $\pi \cdot \bar{\pi} = p = 4k + 1 \in \mathbb{Z}$ prímszám

9.2.1. Példa. Adjuk meg a prímtényező felbontását az 5 és a $78 + 702i$ Gauss-egészeknek!

- (a) Az 5 egy $4k + 1$ alakú prím, tehát egyetlen dolgunk, hogy felírjuk két-négyzetszám összegeként:

$$5 = 1 + 4 = 1^2 + 2^2 = (1 + 2i) \cdot (1 - 2i)$$

Tudjuk, hogy a $4k + 1$ alakú prímek 2 olyan Gauss-prímre bomlanak fel, melyek egymás konjugáltjai, de nem egységszeresei, tehát az 5-nek ez a két prímosztója van, vagyis az 5 kanonikus alakja $5 = (1 + 2i)^1 \cdot (1 - 2i)^1$.

- (b) Most picit hosszadalmasabb dolgunk lesz, de mindenekelőtt bontsuk fel a valós és a képzetes részt prímtényezőkre és emeljük ki a legnagyobb közös osztót:

$$78 + 702i = (2 \cdot 3 \cdot 13) + (2 \cdot 3^3 \cdot 13)i$$

Kiemelhető a $2 \cdot 3 \cdot 13$ legnagyobb közös osztó:

$$78 + 702i = (2 \cdot 3 \cdot 13) \cdot (1 + 9i)$$

Innentől külön dolgozhatunk a $2 \cdot 3 \cdot 13$ -mal és az $1 + 9i$ -vel.

A $2 \cdot 3 \cdot 13$ esete könnyű lesz, hiszen a 2 felbontását tudjuk, hogy $2 = (-i) \cdot (1 + i)^2$, a $3 = 4k - 1$ alakú prím, tehát ő egyben Gauss-prím is, a 13 esete pedig az előző feladat 5 esetéhez hasonló, hiszen ez is $4k + 1$ alakú prím:

$$13 = 9 + 4 = 3^2 + 2^2 = (3 + 2i) \cdot (3 - 2i)$$

Tehát a feladat „felével” megvagyunk: $2 \cdot 3 \cdot 13 = (-i) \cdot 3 \cdot (1 + i)^2 \cdot (3 + 2i)^1 \cdot (3 - 2i)^1$

Mit kezdjünk az $1 + 9i$ -vel? A szokásos trükk, hogy láttuk a 9.1.1. lemmában, hogy minden Gauss-egész osztja a normáját, tehát

$$1 + 9i \mid N(1 + 9i) = 1^2 + 9^2 = 1 + 81 = 82 = 2 \cdot 41$$

Bontsuk a normáját Gauss-prímek szorzatára, hiszen $1 + 9i$ osztói csakis normájának osztói közül kerülhetnek ki ($41 = 25 + 16$):

$$1 + 9i \mid (-i) \cdot (1 + i)^2 \cdot (5 + 4i) \cdot (5 - 4i)$$

Nézzük meg innen melyik szám osztja $1 + 9i$ -t. Ezt egyszerűen úgy nézzük meg, hogy elosztjuk vele, és az eredményről eldöntjük, hogy Gauss-egész lesz-e: próbáljuk először elosztani $1 + i$ -vel³:

$$\frac{1 + 9i}{1 + i} = \frac{1 + 9i}{1 + i} \cdot \frac{1 - i}{1 - i} = \frac{(1 + 9i) \cdot (1 - i)}{(1 + i) \cdot (1 - i)} = \frac{10 + 8i}{2} = 5 + 4i$$

tehát

$$1 + 9i = (1 + i) \cdot (5 + 4i)$$

A keresett szám prímfelbontása:

$$78 + 702i = (-i) \cdot 3 \cdot (1 + i)^3 \cdot (3 + 2i)^1 \cdot (3 - 2i)^1 \cdot (5 + 4i)^1$$

9.3. Alkalmazások

Ebben a fejezetben két „rég” tételt fogunk Gauss-egészekkel újra bebizonyítani, első a két-négyzetszám tétel egyik fele lesz, másik a Pitagorasz számhármak kinézete.

9.3.1. Tétel (Két-négyzetszám tétel). Legyen n egész kanonikus alakja

$$n = 2^\alpha \cdot \prod p_i^{\alpha_i} \cdot \prod q_i^{\beta_i}$$

ahol $\forall p_i = 4k + 1$ és $\forall q_j = 4k - 1$ alakú prím. Ha az n szám előáll két négyzetszám összegeként, akkor $\forall \beta_j$ páros. ♣

³osztásnál a szokásos módon konjugálttal célszerű bővíteni

Bizonyítás. Tegyük fel, hogy $n = x^2 + y^2 = (x + yi) \cdot (x - yi)$. Bontsuk fel az utóbbi szorzat mindkét tényezőjét Gauss-prímek szorzatára. Milyen Gauss-prímeket ismerünk? Van az $1 + i$, vannak a $q_i = 4k - 1 \in \mathbb{Z}$ egész prímek és az olyan π_i egyéb Gauss-prímek, melyek konjugáltja is prím és melyekre $\pi_i \cdot \overline{\pi_i} = N(\pi_i) = p_i = 4k + 1 \in \mathbb{Z}$ egész prím.

A Gauss-egész prímfelbontásában tegyünk különbséget köztük és az előbbi jelölésekkel akkor általánosságban az $x + yi$ Gauss-egész kanonikus alakja:

$$x + yi = (1 + i)^b \cdot \prod \pi_i^{c_i} \cdot \prod \overline{\pi_i}^{d_i} \cdot \prod q_i^{\gamma_i}$$

Tudjuk, hogy $x + yi$ konjugáltja: $\overline{x + yi} = x - yi$. Hogyan néz ki annak a kanonikus alakja? Fogjuk $x + yi$ kanonikus alakját és azt a szorzatot kell konjugálnunk. Ekkor használva hogy szorzat konjugáltja a konjugáltak szorzata, minden egyes tényezőt külön konjugálhatunk:

$$x - yi = \overline{(1 + i)^b \cdot \prod \pi_i^{c_i} \cdot \prod \overline{\pi_i}^{d_i} \cdot \prod q_i^{\gamma_i}} = (1 - i)^b \cdot \prod \overline{\pi_i}^{c_i} \cdot \prod \pi_i^{d_i} \cdot \prod q_i^{\gamma_i}$$

Hogyan néz ki akkor n ? Hát ezek szorzata:

$$n = (1 + i)^b \cdot \prod \pi_i^{c_i} \cdot \prod \overline{\pi_i}^{d_i} \cdot \prod q_i^{\gamma_i} \cdot (1 - i)^b \cdot \prod \overline{\pi_i}^{c_i} \cdot \prod \pi_i^{d_i} \cdot \prod q_i^{\gamma_i}$$

összevonva

$$= ((1 + i) \cdot (1 - i))^b \cdot \prod \pi_i^{c_i + d_i} \cdot \prod \overline{\pi_i}^{c_i + d_i} \cdot \prod q_i^{2 \cdot \gamma_i} = 2^b \cdot \prod p_i^{c_i + d_i} \cdot \prod q_i^{2 \cdot \gamma_i}$$

ahonnan látható, hogy n kanonikus alakjában a $4k - 1$ alakú q_i prímek kitevője páros. ■

9.3.2. Tétel. Ha n előáll két szám négyzetösszegeként és n kanonikus alakja

$$n = 2^b \cdot \prod p_i^{c_i} \cdot \prod q_i^{2 \cdot \gamma_i}$$

ahol minden $p_i = 4k + 1$ és $q_i = 4k - 1$ alakú prímszám, akkor $n = x^2 + y^2 = (x + yi) \cdot (x - yi)$ esetén $x + yi$ megválasztására $4 \cdot \prod (c_i + 1)$ lehetőségünk van. ♣

Bizonyítás. Az előző bizonyítás alapján $x + yi$ kanonikus alakjában $1 + i$ kitevője b kell legyen, a q_i -k kitevője γ_i , viszont a π_i -k esetében van választásunk, hogy hanyadik hatványon vesszük be őket $x + yi$ kanonikus alakjába és mennyi marad a $x - yi$ kanonikus alakjába. Tehát $x + yi$ prímtényezőss alakja

$$x + yi = \varepsilon \cdot (1 + i)^b \cdot \prod \pi_i^{e_i} \cdot \prod \pi_i^{c_i - e_i} \cdot \prod q_i^{\gamma_i}$$

ahol van lehetőségünk megválasztani ε egységet négyféleképpen, illetve e_i kitevőt 0-tól c_i -ig bárminek, tehát $c_i + 1$ féleképpen. Összességében tehát $4 \cdot \prod (c_i + 1)$ -féleképpen választhatjuk meg $x + yi$ -t. ■

9.3.1. Lemma. Legyenek $x, y \in \mathbb{Z}$ és $x + yi, x - yi \in \mathcal{G}$. Ha $(x, y) = 1$ és $N(x + yi)$ páratlan akkor $(x + yi, x - yi) = 1$. ♣

Bizonyítás. Legyen $d = (x + yi, x - yi)$. Ekkor

$$d \mid x + yi \quad \text{és} \quad d \mid x - yi$$

akkor az összegüket és a különbségüket is osztja

$$d \mid x + yi + x - yi = 2x \quad \text{és} \quad d \mid x + yi - x + yi = 2yi \quad \xRightarrow{i \text{ egység}} \quad d \mid 2y$$

A kitüntetett közös osztó definíciója szerint ekkor

$$d \mid (2x, 2y) = 2 \cdot (x, y) = 2 \cdot 1 = 2$$

Tehát $d = 2$ vagy $d = 1$.

A 9.1.1. lemma szerint $x + yi \mid N(x + yi)$, tehát $d \mid N(x + yi)$. Feltettük, hogy ez egy páratlan szám, tehát d sem lehet páros, így $d = 1$. ■

9.3.3. Tétel. Az $x^2 + y^2 = z^2$ egyenlet alapmegoldásai (melyekre $(x, y, z) = 1$):

$$x = r^2 - s^2 \quad \text{és} \quad y = 2 \cdot r \cdot s \quad \text{és} \quad z = r^2 + s^2$$

alakú. ♣

Bizonyítás. Ha $2 \mid z$ akkor $4 \mid z^2$, tehát modulo 4 tekintve $x^2 + y^2 = 0$ kellene teljesüljön, de mivel egy négyzetszám csak 0 vagy 1 maradékot adhat modulo 4, ezért ez csak $0 + 0 = 0$ esetben volna lehetséges, akkor azonban $4 \mid x$ és $4 \mid y$, de ez ellentmond annak, hogy $(x, y, z) = 1$. Tehát z páratlan.

Átírva az egyenletet

$$z^2 = x^2 + y^2 = (x + yi) \cdot (x - yi)$$

Mivel $(x, y) = 1$ és $N(x + yi) = x^2 + y^2 = z^2$ páratlan, így 9.3.1. lemma szerint $(x + yi, x - yi) = 1$. Ha viszont ők relatív prímek, és mivel \mathcal{G} alaptételes gyűrű, ezért alkalmazható a 8.1.1. szorzat-hatvány lemma, vagyis $\exists \alpha \in \mathcal{G}$, melyre $x + yi = \alpha^2$. Legyen $\alpha = r + si$ alakú, ekkor

$$x + yi = (r + si)^2 = r^2 - s^2 + 2rs \cdot i$$

ahonnan $x = r^2 - s^2$ és $y = 2rs$. ■

Megjegyzés. A szorzat-hatvány lemma alkalmazásakor csaltam némileg, lehagytam az egység-szerest, valójában

$$x + yi = \varepsilon \cdot (r + si)^2 = \varepsilon \cdot (r^2 - s^2 + 2rs \cdot i)$$

Belátható, hogy mindegy hogyan választjuk meg ε értékét x és y , illetve r és s szimmetriája miatt. Például $\varepsilon = -i$ esetén

$$x + yi = 2rs - (r^2 - s^2) \cdot i$$

azaz $x = 2rs$ és $y = s^2 - r^2$, ami „lényegében” az előzőleg megkapott érték, csak x és y itt fordított paritású, illetve r és s szerepe is felcserélődött.

10. előadás

Színes becslések

10.1. Körosztási polinomok

Emlék: Körosztási polinomok

Definíció szerint a n -edik körosztási polinom az a bizonyos 1 főegyütthatós polinom, melynek gyökei pontosan az n -edik primitív egységgyökök, vagyis olyan n -edik egységgyökök, melyek rendje n :

$$\Phi_n(x) = \prod_{o(\varepsilon)=n} (x - \varepsilon)$$

Mivel n -edik primitív egységgyökből $\varphi(n)$ darab van, így $\Phi_n(x)$ foka $\varphi(n)$. Tanultuk azt is (bizonyítás nélkül Algebra2-ből), hogy $\Phi_n(x)$ egész együtthatós, tehát \mathbb{Z} feletti polinom. Ez azért lesz lényeges nekünk, mert ha egy egész számot helyettesítünk egy egész együtthatós polinomba, akkor egész értéket kapunk.

Szintén Algebra2-ből tanultuk, hogy

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Most definiálni fogunk egy formális deriválást polinomokra. Fontos hangsúlyozni, hogy ez nem az analízisből megszokott deriválás, csupán formálisan hasonló, de azért is van lényegi különbség, mert ezt tetszőleges gyűrű fölött értelmezzük!

10.1.1. Definíció. Legyen R tetszőleges gyűrű és $f(x)$ az R gyűrű fölötti polinom. Ekkor

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$

polinom **formális deriváltja** alatt

$$f'(x) = n \cdot a_n x^{n-1} + \dots + a_1$$

polinomot értjük.



10.1.1. Állítás. Polinomok összegének, illetve szorzatának formális deriváltjára

$$(f(x) + g(x))' = f'(x) + g'(x) \quad \text{és} \quad (f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$$

szabályok érvényesek



Ezt most bizonyítás nélkül hagyjuk, helyette azt vizsgáljuk meg mi az összefüggés polinomok többszörös gyökei és formális deriváltjai között. Emlékezzünk vissza a fogalomra, mellyel Algebra2-ből már találkoztunk:

Az f polinomnak **többszörös** gyöke α , ha $\exists k > 1$, melyre $(x - \alpha)^k \mid f(x)$.

Az f polinomnak **k -szoros** gyöke α , ha $(x - \alpha)^k \mid f(x)$.

Az f polinomnak **pontosan k -szoros** gyöke α , ha $(x - \alpha)^k \mid f(x)$, de $(x - \alpha)^{k+1} \nmid f(x)$.

10.1.1. Tétel. Legyen $k \geq 1$ és f egy T test feletti polinom. Ekkor az f polinomnak pontosan k -szoros gyöke $\alpha \Leftrightarrow \alpha$ gyöke f -nek és α pontosan $k - 1$ -szeres gyöke f' -nak. ♣

Bizonyítás. Szokásosan külön látjuk be a 2 irányt.

\Rightarrow *irány:*

Amennyiben α pontosan k -szoros gyöke f -nek, akkor $(x - \alpha)^k \mid f(x)$ ami azt jelenti, hogy $\exists g(x)$, melyre

$$f(x) = (x - \alpha)^k \cdot g(x)$$

és g -nek nem gyöke α , hiszen különben $g(x) = (x - \alpha) \cdot h(x)$ lenne, vagyis

$$f(x) = (x - \alpha)^k \cdot (x - \alpha) \cdot h(x) = (x - \alpha)^{k+1} \cdot h(x)$$

miatt $(x - \alpha)^{k+1} \mid f(x)$ ami nem lehetséges, mert akkor nem pontosan k -szoros gyöke lenne. Tehát $g(\alpha) \neq 0$. Ekkor

$$f'(x) = (x - \alpha)^k \cdot g'(x) + k \cdot (x - \alpha)^{k-1} \cdot g(x) = (x - \alpha)^{k-1} \cdot \left((x - \alpha) \cdot g'(x) + k \cdot g(x) \right)$$

Ahonnán azt látjuk, hogy f' -nak $k - 1$ -szeres gyöke α , de azt is, hogy k -szoros már nem, hiszen a „megmaradó” $(x - \alpha) \cdot g'(x) + k \cdot g(x)$ -nek már nem gyöke α , mert helyettesítve nem 0-t kapunk, mivel:

$$(\alpha - \alpha) \cdot g'(\alpha) + k \cdot g(\alpha) = 0 + k \cdot g(\alpha) = k \cdot g(\alpha)$$

ami biztosan nem nulla, hiszen $k \neq 0$ és $g(\alpha) \neq 0$ és testben nem lehetnek nullosztók, így ebből következően szorzatuk sem lehet nulla.

Ha pedig f' -nak $k - 1$ -szeres gyöke α , de nem k -szoros, akkor pontosan $k - 1$ -szeres gyöke.

\Leftarrow *irány:*

Most tegyük fel, hogy f' -nak pontosan $k - 1$ -szeres gyöke α , és f -nek is gyöke, n jelölje, hogy pontosan hányiszoros. Azt kellene belátnunk, hogy $n = k$. Mivel f -nek pontosan n -szeres gyöke, az előző irány miatt f' -nak $n - 1$ -szeres. De hát azt mondtuk, hogy annak $k - 1$ -szeres, ekkor tehát $n - 1 = k - 1$, ahonnán $n = k$. ■

Emlékszünk még rá, hogy $\Phi_n(x)$ helyettesítési értéke egy $a \in \mathbb{Z}$ helyen egész szám. Beszélhetünk tehát neki a prímosztóiról, amik igencsak speciális alakúak, erről szól a következő tétel.

10.1.2. Tétel. Legyen $a \in \mathbb{Z}$. Ha p prímre $p \mid \Phi_n(a)$ akkor $p \mid n$ vagy $p = n \cdot k + 1$ alakú. ♣

Bizonyítás. Tegyük fel, hogy $p \mid \Phi_n(a)$ (vagyis $\Phi_n(x)$ -nek modulo p gyöke az a) és $p \nmid n$, azt fogjuk belátni, hogy ekkor $p = n \cdot k + 1$ alakú. Mivel

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

és $n \mid n$, ezért a jobboldali szorzatban szerepel $\Phi_n(x)$, azaz $\Phi_n(x) \mid x^n - 1$

$$p \mid \Phi_n(a) \text{ és } \Phi_n(a) \mid a^n - 1 \Rightarrow p \mid a^n - 1$$

másképp fogalmazva $a^n \equiv 1 \pmod{p}$. Van tehát olyan hatvány, melyre emelve a -t 1-et kapunk modulo p , vagyis van jó kitevő, akkor beszélhetünk a rendjéről is. Tudjuk, hogy a rend osztja a jó kitevőket, vagyis $o_p(a) \mid n$. Azt fogjuk belátni, hogy ekkor $o_p(a) = n$ kell legyen.

Indirekt tegyük fel, hogy $o_p(a) = d < n$ (de természetesen mivel a jó kitevőket osztja, így $d \mid n$ teljesül), ekkor $a^d \equiv 1 \pmod{p}$, azaz $p \mid a^d - 1$ azaz

$$p \mid a^d - 1 = \prod_{k \mid d} \Phi_k(a)$$

Használva p prímtulajdonságát, ha egy szorzatot oszt, akkor annak egyik tényezőjét is, tehát $\exists k \mid d$, melyre $p \mid \Phi_k(a)$, azaz $\Phi_k(x)$ -nek modulo p gyöke az a . Úgy indultunk, hogy $\Phi_n(x)$ -nek is gyöke az a , így mivel

$$x^n - 1 = \prod_{i \mid n} \Phi_i(x)$$

ezért a jobboldali szorzat tényezői között szerepel $\Phi_n(x)$ és $\Phi_k(x)$, melyekről tudjuk, hogy modulo p tekintve őket mindkettőnek gyöke az a . Ezek szerint a jobboldalon két tényezőből is kiemelhető $(x - a)$ -tényező, vagyis a jobboldali polinomnak 2-szeres gyöke az a . Ekkor persze a baloldali $f(x) = x^n - 1$ -nek is legalább 2-szeres, de a 10.1.1. tétel szerint ekkor $f'(x)$ -nek is (legalább 1-szeres) gyöke, viszont

$$f'(x) = (x^n - 1)' = n \cdot x^{n-1}$$

Mivel $p \nmid n$, így $(n, p) = 1$, vagyis a jobboldali polinom nem a 0 polinom (aminek minden gyöke). Ennek akkor viszont csak a 0 a gyöke, márpedig $a \neq 0$, különben n -edik hatványa se lehetne modulo p kongruens 1-gyel.

Ellentmondásra jutottunk abból az indirekt feltételből, hogy $o_p(a) < n$, így tehát $o_p(a) = n$, és mivel $\varphi(p) = p - 1$ a kis Fermat-tétel miatt jó kitevő, és a rend osztja a jó kitevőket, így $n \mid p - 1$, tehát $\exists k \in \mathbb{Z}$, melyre $p - 1 = n \cdot k$, ezzel beláttuk, hogy $p = n \cdot k + 1$ alakú. ■

10.2. Faktoriálisok számelmélete

Ebben a fejezetben fogjuk előkészíteni a Csebisev-tétel bizonyításához szükséges állításokat. Ezek többnyire az $n!$ vagy a binomiális együtthatók számelméletével lesznek kapcsolatosak, azokat próbálják becsülni, vagy prímtenyezős alakjukat leírni.

Emlék:

A **Pascal-háromszög** úgy készül, hogy a binomiális együtthatókat elhelyezzük háromszög formában a következő módon:

$$\begin{array}{ccccccc}
 & & & & \binom{0}{0} & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\
 \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
 \end{array}$$

kiírva a konkrét értékeket:

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & 1 & & 1 & \\
 & & 1 & & 2 & & 1 \\
 & 1 & & 3 & & 3 & & 1 \\
 1 & & 4 & & 6 & & 4 & & 1
 \end{array}$$

Miért hasznos nekünk ez a háromszög? Több okból is, például a binomiális tételben az együtthatók ennek egyes soraiból származnak. Például $(a+b)^3$ esetén az együtthatók a háromszög 3. sorából, ugyanis a sorokat 0-tól számozzuk azon okból, hogy $(a+b)^n$ esetén azt mondhassuk, hogy az együtthatók az n . sorból kerülnek ki.

Fontos, hogy a sorok elemeit is 0-tól sorszámozzuk, így azt mondhatjuk, hogy az n . sor k . eleme éppen $\binom{n}{k}$. Tanultuk véges matematikából, hogy az n . sorban lévő elemek összege 2^n , ismételten 0-tól kezdődően értve a sorok számozását.

10.2.1. Tétel. Becslés binomiális együtthatókra ($n \geq 1$): $\frac{4^n}{2n+1} < \binom{2n}{n} < 4^n$



Bizonyítás. Mit jelent az előbbiek alapján $\binom{2n}{n}$? A Pascal-háromszög $2n$ -edik sorának n -edik elemét. Mivel $2n$ páros, így ebben a sorban páratlan sok elem van, ezek közül az n -edik éppen a középső.

Nyilvánvalóan mivel nem a nulladik sorról van szó, így a középső elemen kívül vannak más elemek is, tehát a vizsgált elem kisebb, mint a teljes sor összege, ami $2^{2n} = (2^2)^n = 4^n$. Ezzel a bizonyítandó jobboldalát meg is kaptuk: $\binom{2n}{n} < 4^n$.

Hasonlóan meggondolható, hogy mivel a középső elem a legnagyobb, így az átlagnál biztosan nagyobb. Mennyi az átlag? Sorösszeg osztva a sorban lévő elemek számával. Mivel a $2n$ -edik sort vizsgáljuk, itt $2n+1$ elem van, vagyis az átlag

$$\frac{\text{sorösszeg}}{\text{elemszám}} = \frac{4^n}{2n+1} < \binom{2n}{n}$$

Ezzel a másik részét is beláttuk az egyenlőtlenségnek. ■

10.2.2. Tétel. Becslés binomiális együtthatókra ($n \geq 1$): $\frac{2^{2n+1}}{2n+2} < \binom{2n+1}{n} < 4^n$ ♣

Bizonyítás. Most a $2n+1$ -edik sor n -edik elemét vizsgáljuk. Páratlan sorszámot viselő sorban páros sok elem található, itt most $2n+2$, ezek közül a középső 2 egyforma, melyek egyike az n -edik. Tehát hasonlóan csinálhatjuk a becsléseket. Az átlagnál most is nagyobb ez az elem, viszont mivel van egy „párja” akivel megegyezik az értéke (ez $\binom{2n+1}{n+1}$ lesz), így a sorösszeg felénél is kisebb:

$$\frac{2^{2n+1}}{2n+2} = \text{átlag} < \binom{2n+1}{n} < \text{sorösszeg fele} = \frac{2^{2n+1}}{2} = 2^{2n} = 4^n$$

■

Klasszikus számelméleti kérdés, hogy $n!$ hány 0-ra végződik? Ehhez azt kell megvizsgálni, 10-nek maximum hanyadik hatványával osztható. Vagyis mi a maximális olyan kitevő, amelyen 2 és 5 is szerepel az $n!$ prímtényezőzős felbontásában? Most egy picit általánosabb dolgot vizsgálunk, hogyan néz ki $n!$ prímtényezőzős felbontása? Nézzünk először egy konkrét példát!

10.2.1. Példa. Határozzuk meg $15!$ prímtényezőzős felbontását!

Tudjuk jól, hogy $15! = 15 \cdot 14 \cdot \dots \cdot 2 \cdot 1$, így a kanonikus alak minden prímtényezője legfeljebb 15 lehet, így a szóba jöhető prímek: 2, 3, 5, 7, 11, 13. Mivel 13 csak a 13 és 11 csak a 11 miatt került bele a szorzatba, így ők csak első hatványon szerepelnek.

A 7 már a 7 és a 14 miatt is benne van. Általánosan annyi számban szerepel egy adott p prím, ahány szám osztható 15-ig p -vel, tehát $\left\lfloor \frac{15}{p} \right\rfloor = 2$.

Hasonló az 5 esete is: $\left\lfloor \frac{15}{5} \right\rfloor = 3$

A 3 esete viszont némileg más. Indulásnak itt is jó, hogy minden 3-mal osztható szám miatt belekerül 1-szer, tehát 5-ödik hatványon biztosan szerepel az 3. Viszont így a 9-es számot is úgy számoltuk, hogy csak 1-gyel növeli a 3 kitevőjét, holott az 3^2 -nel is osztható, tehát azt látjuk, hogy valójában a 3 kitevője:

$$\left\lfloor \frac{15}{3} \right\rfloor + \left\lfloor \frac{15}{3^2} \right\rfloor = 5 + 1 = 6$$

A 2 még érdekesebb, itt már a 8 is belép a képbe, a 16 még éppen nem:

$$\left\lfloor \frac{15}{2} \right\rfloor + \left\lfloor \frac{15}{2^2} \right\rfloor + \left\lfloor \frac{15}{2^3} \right\rfloor = 7 + 3 + 1 = 11$$

Így tehát felírva a prímtényezőzős alakot:

$$15! = 1307674368000 = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1$$

Mindez általánosan is megfogalmazható!

10.2.3. Tétel. Az $n!$ kanonikus alakja: $n! = \prod_{\substack{p \leq n \\ p \text{ prím}}} p^\alpha$ ahol $\alpha = \sum_{\substack{p^i \leq n \\ p^{i+1} > n}} \left\lfloor \frac{n}{p^i} \right\rfloor$ ♣

Bizonyítás. Az előző példa után nyilvánvaló ez a tétel. Legfeljebb n lehet minden p prímtényező értéke, továbbá először megnézzük hány olyan szám van, amik 1-gyel növelik a végső kitevőt, majd hány ami 2-vel (azaz még további 1-gyel), stb... Ezt addig csináljuk, amíg a nevezőben lévő prímtényező legfeljebb n , hiszen vele osztjuk el n -et és ha n -nél nagyobb számmal osztanánk, 1-nél kisebbet kapnánk, aminek egészrésze 0, tehát elegendő addig menni, amíg $p^i \leq n$, hiszen utána már csak 0-kat adogatnánk össze. ■

10.2.4. Tétel. Becslés a prímek szorzatára (p pozitív prímszám) $x \in \mathbb{Z}$ -ig: $\prod_{p \leq x} p < 4^x$ ♣

Bizonyítás. Valójában erősebb állítást fogunk belátni, azt hogy

$$\prod_{p \leq x} p < 4^{x-1}$$

csupán azért szerepel a tételben x kitevővel, mert későbbiekben nekünk azt elegendő lesz használnunk a Csebisev bizonyításához.

Az első hasznos észrevételünk, hogy elegendő $x \geq 2$ -vel foglalkoznunk, különben a baloldali szorzat 0 (hiszen 2 alatti pozitív prímszám nincs), a 4^x exponenciális függvényre pedig valóban alsó korlát a 0. Látható továbbá, hogy $x = 2$ és $x = 3$ esetén is igaz:

$$x = 2: \quad 2 < 4^1 \quad \text{és} \quad x = 3: \quad 2 \cdot 3 = 6 < 4^2$$

innenről tehát $x \geq 4$.

Látható az is, hogy elegendő az állítást $x = 2n + 1$ páratlan számokra belátni. Hiszen ha egy páratlan számra igaz, akkor az utána következő párosra is, hiszen ha egy számmal tovább megyünk, akkor a baloldal nem változik (nem találunk új prímet amit bevehetnénk a szorzatba, mert páros szám biztosan nem prím), a jobboldal pedig növekszik.

Teljes indukciót alkalmazunk, $n = 1$ esetén $x = 2 \cdot 1 + 1 = 3$ -ra már láttuk. Tegyük fel, hogy tetszőleges $x = 2n - 1$ -ig minden számra igaz (speciálisan $n + 1$ -re is), és be kellene látnunk, hogy a következő páratlan számra, $x = 2n + 1$ -re:

$$\prod_{p \leq 2n+1} p < 4^{2n} = 4^{x-1}$$

Ehhez a szorzatot 2 részre bontjuk, vesszük $n + 1$ -ig a prímek szorzatát, majd az $n + 1$ és $2n + 1$ közöttieket:

$$\prod_{p \leq 2n+1} p = \prod_{p \leq n+1} p \cdot \prod_{n+1 < p \leq 2n+1} p$$

Az első szorzótényező az indukciós feltétel szerint felülről becsülhető

$$< 4^n \cdot \prod_{n+1 < p \leq 2n+1} p$$

Mit kezdünk a másodikkal? Tekintsük a következő binomiális együtthatót:

$$\binom{2n+1}{n} = \frac{(2n+1)!}{n! \cdot (n+1)!} = \frac{(2n+1) \cdot \dots \cdot (n+2) \cdot (n+1) \cdot \dots \cdot 2 \cdot 1}{n! \cdot (n+1) \cdot \dots \cdot 2 \cdot 1} = \frac{(2n+1) \cdot \dots \cdot (n+2)}{n!}$$

Látható, hogy az összes olyan prím, melyek szorzatát vesszük, tehát $n+1 < p \leq 2n+1$ az megtalálható a kapott tört számlálójában, de a nevezőjében nem (hiszen ha $n+1$ -nél nagyobb p , akkor n -nél is), így nem „egyszerűsödik ki”, ami azt jelenti, hogy ezen prímelek szorzata felülről becsülhető $\binom{2n+1}{n}$ értékével. Most ott tartunk tehát a becslésekben, hogy

$$\prod_{p \leq 2n+1} p < 4^n \cdot \binom{2n+1}{n} \stackrel{10.2.2. \text{ tétel}}{<} 4^n \cdot 4^n = 4^{2n} = 4^{x-1}$$

Ezzel beláttuk a tételt. ■

A következő tétel lesz az utolsó amire szükségünk lesz, ez azt mondja, hogy $\binom{2n}{n}$ prímfelbontásában a prímtényezők „kicsik”, olyan értelemben, hogy legfeljebb $2n$ lehet bármelyik.

10.2.5. Tétel. Amennyiben $n \geq 1$ akkor $\binom{2n}{n} = \prod p^\alpha$ esetén $p^\alpha \leq 2n$. ♣

Bizonyítás. Írjuk fel definíció szerint a binomiális együtthatót:

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

Használjuk a 10.2.3. tételben megszerzett tudásunkat és írjuk fel a számláló és a nevező kanonikus alakját. Egy adott p prímszám esetén ha annak $(2n)!$ kanonikus alakjában a kitevője α , valamint $n!$ esetén β , akkor végül $\alpha - 2\beta$ lesz a kitevő a hatványozás szabályai szerint. Tehát p kitevője:

$$\alpha - 2\beta = \sum_{\substack{p^i \leq 2n \\ p^{i+1} > 2n}} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \cdot \sum_{\substack{p^i \leq 2n \\ p^{i+1} > 2n}} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Igaz, hogy a második szumma esetében elegendő lenne $p^i \leq n$ -ig menni, de korábban (az említett tétel bizonyításakor) megbeszéltük, hogy ha tovább is megyünk az sem gond, mert csak 0-kat adunk össze. Csupán azért választjuk most ezt a feltételt, mert így láthatóan összevonhatóak a szummák:

$$= \sum_{\substack{p^i \leq 2n \\ p^{i+1} > 2n}} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^i} \right\rfloor \right)$$

Az egészrész definíciója szerint $x - 1 < \lfloor x \rfloor \leq x$, így

$$\left\lfloor \frac{2n}{p^i} \right\rfloor \leq \frac{2n}{p^i} \quad \text{és} \quad \left\lfloor \frac{n}{p^i} \right\rfloor > \frac{n}{p^i} - 1$$

becslésekkel felülről becsülhetők az összeadandók:

$$\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^i} \right\rfloor < \frac{2n}{p^i} - 2 \cdot \left(\frac{n}{p^i} - 1 \right) = 2$$

De ha a szumma minden egyes tagja kisebb 2-nél, akkor csak 0-kat vagy 1-eseket, pontosabban mivel előbbi lényegtelen csak 1-eseket adunk össze amíg $p^i \leq 2n$.

Ha k a legnagyobb kitevő, amire még teljesül, hogy $p^k \leq 2n$, akkor legfeljebb k egyest adunk össze, tehát a kitevő $\alpha \leq k$. Az exponenciális függvény monotonitása miatt ekkor

$$p^\alpha \leq p^k \leq 2n$$

ahonnan $p^\alpha \leq 2n$ és ezt kellett belátnunk. ■

Érdekességek: Volt három érdekes formula, melyek előadáson előkerültek, de őket nem bizonyítottuk (ha valakit érdekel Freud: Számelmélet könyvében mindegyik megtalálható: 5.4.4. feladat b része, 5.4.1. Tétel és 5.4.2. Tétel). A három formula ($\pi(x)$ jelöli a prímek számát x -ig):

$$\prod_{p \leq x} p < e^x \quad \text{és} \quad p_n \sim n \cdot \log n \quad \text{és} \quad \pi(x) \sim \frac{n}{\log n}$$

10.3. Csebisev-tétel

10.3.1. Tétel. Ha $n \geq 1$ akkor $\exists p : n < p \leq 2n$ prím. (Szám és kétszerese között van prím.) ♣

Bizonyítás. Azt fogjuk belátni, hogy az $n < p \leq 2n$ prímek szorzata nagyobb mint 1, ekkor lennie kell ott ténylegesen prímszámnak, nem üres a szorzat. Ehhez vizsgáljuk szokásos kedvenc binomiális együtthatónkat és annak prímtényező felbontását. Most négy részre bontjuk a produktumot, attól függően, hogy mekkora prímek szorzatát vizsgáljuk:

$$\binom{2n}{n} = \prod p^\alpha = \prod_{p \leq \sqrt{2n}} p^\alpha \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^\alpha \cdot \prod_{\frac{2}{3}n < p \leq n} p^\alpha \cdot \prod_{n < p \leq 2n} p^\alpha$$

Ezen 4 tényező közül az utolsóról kellene belátnunk, hogy nagyobb 1-nél. Ehhez felülről fogjuk becsülni az első 3 tényezőt.

I. becslés:

A 10.2.5. tétel szerint minden $p^\alpha \leq 2n$, tehát az első szummának prímhatalványait becsülve:

$$\prod_{p \leq \sqrt{2n}} p^\alpha \leq \prod_{p \leq \sqrt{2n}} 2n$$

és mivel $p \leq \sqrt{2n}$, így ez egy legfeljebb $\sqrt{2n}$ tényező szorzat, még ha 1-től $\sqrt{2n}$ -ig az összes számot prímnek veszem akkor is, tehát tovább becsülve

$$\prod_{p \leq \sqrt{2n}} p^\alpha \leq \prod_{p \leq \sqrt{2n}} 2n \leq (2n)^{\sqrt{2n}} \leq (2n+1)^{\sqrt{2n}}$$

II. becslés:

Itt először vegyük észre, hogy innentől kezdve a kitevők igazából feleslegesek is, merthogy az összes prímtényező legfeljebb 1. hatványon lehet. Hiszen innentől kezdve olyan p prímekkel van dolgunk, melyekre $\sqrt{2n} < p$, azaz $2n < p^2$, tehát $p^2 \nmid 2n$ vagyis csak első hatványon szerepelhet legfeljebb:

$$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^\alpha = \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p$$

Ezt most felülről becsüljük úgy, hogy nem csak a $\sqrt{2n}$ és $\frac{2}{3}n$ közötti prímeket szorozzuk össze, hanem $\frac{2}{3}n$ -ig az összeset:

$$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq \prod_{p \leq \frac{2}{3}n} p$$

most használjuk a 10.2.4. tételt, így

$$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq \prod_{p \leq \frac{2}{3}n} p < 4^{\frac{2}{3}n}$$

becsléshez jutunk.

III. becslés:

Ez a legizgalmasabb mind közül, legalábbis Erdős Pál szerint. Ugyanis itt becsülni sem igazán fogunk, azt látjuk be, hogy a harmadik tényező egészen pontosan 1, ugyanis nincs prímosztója $\binom{2n}{n}$ binomiális együtthatónak $\frac{2}{3}n$ és n között. Megint csak a definíciót felírva:

$$\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!} = \frac{1 \cdot 2 \cdot \dots \cdot \frac{2}{3}n \cdot \dots \cdot p \cdot \dots \cdot n \cdot (n+1) \cdot \dots \cdot 2p \cdot \dots \cdot 2n}{(1 \cdot \dots \cdot p \cdot \dots \cdot n) \cdot (1 \cdot \dots \cdot p \cdot \dots \cdot n)}$$

Amennyiben $\frac{2}{3}n < p \leq n$ akkor $\frac{4}{3}n < 2p \leq 2n$ és $2n < 3p$, ami azt jelenti, hogy a számlálóban pontosan 2-szer szerepel p , ugyanakkor mivel $p \leq n$, így a nevezőben is szerepel 2-szer, vagyis egyszerűsíthetünk vele. Tehát ilyen p biztosan nem lehet végül osztója $\binom{2n}{n}$ -nek, a harmadik produktum értéke egészen pontosan 1.

Konklúzió:

Összességében tehát a következő becslést kaptuk:

$$\binom{2n}{n} \leq (2n+1)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \cdot 1 \cdot \prod_{n < p \leq 2n} p$$

becsüljük alulról is a binomiális együtthatót a 10.2.1. tétel szerint:

$$\frac{4^n}{2n+1} < \binom{2n}{n} \leq (2n+1)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \cdot 1 \cdot \prod_{n < p \leq 2n} p$$

Vagyis

$$\frac{4^{\frac{1}{3}n}}{(2n+1)^{\sqrt{2n+1}}} < \prod_{n < p \leq 2n} p$$

Itt elegendő volna azt belátnunk, hogy a baloldal legalább 1, azzal kész is volnánk. Nos ez sajnos nem mindig igaz, de belátható, hogy $n \geq 514$ esetén igen¹. Először ehhez be kell látni 514-re, majd pedig, hogy monoton növekszik a függvény. Ezt az utóbbit viszont nem is olyan egyszerű, nekem nem sikerült, és előadáson sem láttuk be, tehát feltételezem, hogy vizsgára sem követelmény.

Viszont be kell látni $n < 514$ -re is:

- $n = 1$ -re $1 < 2 \leq 2$
- $n = 2$ -re $2 < 3 \leq 4$
- $n = 3$ -ra $3 < 5 \leq 6$ (ez persze $n = 4$ -re is jó)

¹Innentől a bizonyítás kétfelé mehet tovább, az egyik irány amire előadáson Szabó Csaba tanár úr utalt, a másik megtalálható a mellékletek között, az a Bizonyítások a könyvből című könyvből származik.

- $n = 5$ -re $5 < 7 \leq 10$ (ez $n = 6$ -ra is jó)
- $n = 7$ -re $7 < 13 \leq 14$ (ez $n = 8, 9, 10, 11, 12$ -re is jó)
- $n = 13$ -ra $13 < 23 \leq 26$ (...)
- $n = 23$ -ra $23 < 43 \leq 46$ (...)
- $n = 43$ -ra $43 < 83 \leq 86$ (...)
- $n = 83$ -ra $83 < 163 \leq 166$ (...)
- $n = 163$ -ra $163 < 311 \leq 326$ (...)
- $n = 311$ -re $311 < 619 \leq 622$ (...)

Röviden: 2, 3, 5, 7, 13, 23, 43, 83, 163, 311, 619 megfelelő prímek, így $n < 514$ -re is igaz, ezzel beláttuk a tételt. ■

11. előadás

Számelméleti függvények

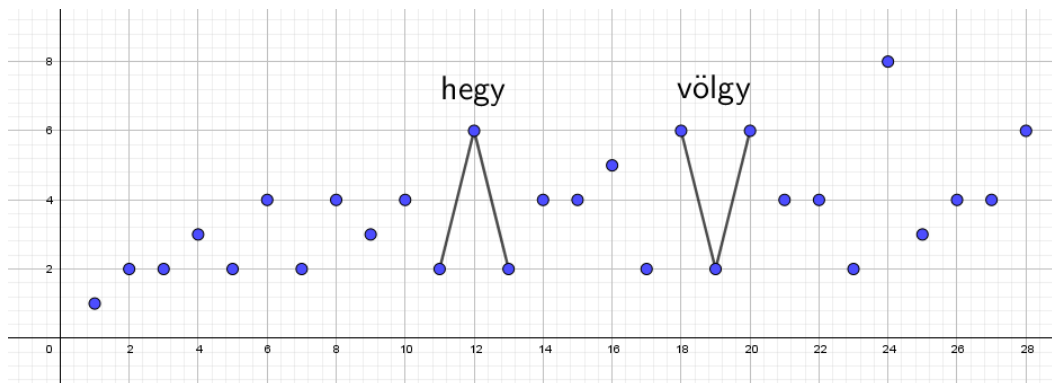
11.1. Hegy- és völgytétel

Emlék:

11.1.1. Tétel (Dirichlet-tétel). Ha $(a, d) = 1$ akkor végtelen sok $d \cdot k + a$ alakú prím van. ♣

Tanultunk Algebra1-ből a $d(n)$ számelméleti függvényről, ami az n szám osztóinak a számát adja eredményül. Vizsgáljuk meg ennek egy különleges tulajdonságát.

Bármely p prím esetén $d(p) = 2$, hiszen minden prímnek 2 osztója van. Ugyanakkor például $d(2^n) = n + 1$, tehát a függvény tetszőleges nagy értéket is felvehet. Hogyan néz ki nagyjából kezdetben a függvény?



11.1. ábra. A $d(n)$ függvény

Belátható, hogy bármilyen nagy völgy, illetve hegy található a grafikonon. Szemléletesen hegy alatt azt értjük, hogy egy kis érték után egy nagy, majd újra egy kicsi következik közvetlenül egymás után, völgy alatt pedig, hogy egy nagy érték után egy kicsi, majd újra nagy. Pontosabban, hogy ez mit is jelent, a következő tétel állításából érthető meg.

11.1.2. Tétel (Hegytétel). Adott $k > 0$ egész esetén $\exists n$ melyre $d(n) - d(n+1) > k$, valamint $d(n) - d(n-1) > k$ ♣

Ezt nem fogjuk belátni, de a párját, a völgytételt igen.

11.1.3. Tétel (Völgytétel). Adott $k > 0$ egész esetén $\exists n$ melyre $d(n-1) - d(n) > k$, valamint $d(n+1) - d(n) > k$. ♣

Bizonyítás. Erősebb lesz amit belátunk, azt fogjuk belátni, hogy létezik ilyen $n = p$ prímszám is, amire ez teljesül, sőt végtelen sok ilyen p létezik.

Tekintsük adott k esetén a $t \cdot 3^{k+2}$ és a $q \cdot 2^{k+2}$ számokat. Elegendő volna belátni, hogy létezik olyan p prím, melyre:

$$t \cdot 3^{k+2} + 1 = p = q \cdot 2^{k+2} - 1$$

vagyis amelyre a $t \cdot 3^{k+2}$, p és $q \cdot 2^{k+2}$ egymást követő számok, és ez egy megfelelő völgy, hiszen az osztóik száma

$$d(t \cdot 3^{k+2}) \geq k+3 \quad \text{és} \quad d(p) = 2 \quad \text{és} \quad d(q \cdot 2^{k+2}) \geq k+3$$

vagyis a különbség mindkét esetben $\geq k+3 - 2 = k+1 > k$.

Mért létezik ilyen p prímszám? Mit kellene neki teljesítenie? Például 3^{k+2} -vel osztva 1 maradékot ad, illetve 2^{k+2} -vel osztva -1 maradékot, tehát

$$p \equiv 1 \pmod{3^{k+2}} \quad \text{és} \quad p \equiv -1 \pmod{2^{k+2}}$$

Mivel $(3^{k+2}, 2^{k+2}) = 1$, így ennek a szimultán kongruenciarendszernek egyértelműen létezik egy $p \equiv A$ megoldása modulo $2^{k+2} \cdot 3^{k+2} = 6^{k+2}$. Ez a megoldás

$$p = s \cdot 6^{k+2} + A$$

alakú, ami azt jelenti, hogy olyan prímre volna szükségünk, ami $s \cdot 6^{k+2} + A$ alakú, és minden ilyen prím esetén található egy k -től függő völgy. Miért létezik ilyen alakú prím?

Vegyük észre, hogy mivel $p \equiv 1 \pmod{3^{k+2}}$, így $3^{k+2} \mid p-1$ azaz $3 \mid p-1$, azaz $3 \nmid p$. Hasonlóan látható, hogy $2 \nmid p$.

Ezek miatt $(A, 6^{k+2}) = 1$, hiszen közös osztóként 1-en kívül csak 2-vel vagy 3-mal osztható számok jöhetnének szóba, de az A egyikkel sem lehet osztható, hiszen különben $s \cdot 6^{k+2} + A = p$ is osztható lenne vele, de p -ről láttuk, hogy sem 2-vel, sem 3-mal nem lehet osztható.

A relatív prímesség miatt alkalmazhatjuk a Dirichlet-tételt, azaz létezik $p = 6^{k+2} \cdot s + A$ alakú prímszám, még hozzá végtelen sok is. Ezek mind megfelelőek számunkra. ■

11.2. Tökéletes

Emlék:

A $\sigma(n)$ függvény az n osztóinak a számát adja értékül, képlete (feltéve, hogy n kanonikus alakja szokásosan $p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$):

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

Speciálisan p prím esetén $\sigma(p) = \frac{p^2 - 1}{p - 1} = p + 1$, amin nem is lepődünk meg, hiszen p osztói pontosan az 1 és a p , és $\sigma(p)$ az osztók összege, vagyis $1 + p$.

Tanultuk azt is, hogy σ multiplikatív függvény, tehát $(a, b) = 1$ esetén $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.

11.2.1. Definíció. Az $n \in \mathbb{Z}^+$ számot **tökéletes számnak** nevezzük, amennyiben megegyezik valódi osztóinak összegével, azaz osztóinak kétszeresével: $\sigma(n) = 2n$ ♣

Tökéletes szám például a $6 = 1 + 2 + 3$ vagy a $28 = 1 + 2 + 4 + 7 + 14$. Nem tudjuk hány tökéletes szám létezik, mint ahogy azt sem, hogy van-e páratlan.

Emlék: Mersenne-prímeknek nevezzük a $2^p - 1$ alakú prímeket. Láttuk Algebra1-ből, hogy ha egy ilyen alakú szám prímszám, akkor p is szükségképpen prím. Most vizsgáljuk meg a Mersenne-prímek és a tökéletes számok kapcsolatát.

11.2.1. Tétel. Az n páros szám akkor és csak akkor tökéletes, ha $n = 2^p \cdot (2^{p+1} - 1)$ alakú, ahol $2^{p+1} - 1$ Mersenne-prím. ♣

Bizonyítás. Az első irány triviális, ha $n = 2^p \cdot (2^{p+1} - 1)$ alakú, akkor mivel $(2^p, 2^{p+1} - 1) = 1$ (előbbi csak 2-vel osztható, utóbbi azzal pont nem), így σ multiplikativitása miatt

$$\sigma(n) = \sigma\left(2^p \cdot (2^{p+1} - 1)\right) = \sigma(2^p) \cdot \sigma(2^{p+1} - 1)$$

majd használva σ képletét, és hogy $2^{p+1} - 1$ prím:

$$= \frac{2^{p+1} - 1}{2 - 1} \cdot (2^{p+1} - 1 + 1) = (2^{p+1} - 1) \cdot 2^{p+1} = 2 \cdot 2^p \cdot (2^{p+1} - 1) = 2n$$

Azaz $\sigma(n) = 2n$, így n tökéletes.

Nézzük a másik irányt és lássuk be, hogy minden páros tökéletes szám ilyen alakú. Legyen α a legnagyobb olyan pozitív egész, melyre $2^\alpha \mid n$. Ekkor

$$n = 2^\alpha \cdot m$$

ahol m páratlan. Mivel ez a két szám megegyezik, így σ értékük is (most használjuk, hogy n tökéletes):

$$2^{\alpha+1} \cdot m = 2n = \sigma(n) = \sigma(2^\alpha \cdot m)$$

mivel m páratlan, így $(2^\alpha, m) = 1$, vagyis σ multiplikativitása miatt

$$2^{\alpha+1} \cdot m = \sigma(2^\alpha) \cdot \sigma(m)$$

ami $\sigma(n)$ képlete miatt

$$2^{\alpha+1} \cdot m = \frac{2^{\alpha+1} - 1}{2 - 1} \cdot \sigma(m) = (2^{\alpha+1} - 1) \cdot \sigma(m) \quad (11.2.1)$$

Mivel $2^{\alpha+1} - 1$ osztja a jobboldalt, így a baloldalt is, de $(2^{\alpha+1}, 2^{\alpha+1} - 1) = 1$, így m -et osztja:

$$2^{\alpha+1} - 1 \mid m \quad \Leftrightarrow \quad \exists k: m = (2^{\alpha+1} - 1) \cdot k$$

a 11.2.1 egyenletbe $m = (2^{\alpha+1} - 1) \cdot k$ -t helyettesítve

$$2^{\alpha+1} \cdot (2^{\alpha+1} - 1) \cdot k = (2^{\alpha+1} - 1) \cdot \sigma\left((2^{\alpha+1} - 1) \cdot k\right)$$

egyszerűsítve $2^{\alpha+1} - 1$ -gyel¹

$$2^{\alpha+1} \cdot k = \sigma\left((2^{\alpha+1} - 1) \cdot k\right) \quad (11.2.2)$$

Azt fogjuk belátni, hogy $k = 1$. Indirekt tegyük fel, hogy $k \neq 1$. Ekkor a $(2^{\alpha+1} - 1) \cdot k$ számnak különböző² osztói az 1, a k , és a $k \cdot (2^{\alpha+1} - 1)$. Ezek szerint az osztóinak összege alulról becsülhető ezen három osztójának összegével:

$$2^{\alpha+1} \cdot k = \sigma\left((2^{\alpha+1} - 1) \cdot k\right) \geq 1 + k + k \cdot (2^{\alpha+1} - 1) = 1 + k \cdot 2^{\alpha+1}$$

azaz $0 \geq 1$, ami nyilvánvaló ellentmondás.

Így tehát $k = 1$, ami azt jelenti, hogy $m = 2^{\alpha+1} - 1$, ahonnan 11.2.2 miatt

$$2^{\alpha+1} = \sigma(2^{\alpha+1} - 1)$$

ami azt jelenti, hogy $2^{\alpha+1} - 1$ osztóinak összege csupán a két triviális osztójának (1-nek és önmagának) az összege. Ezek szerint nincs más osztója, vagyis ő egy prímszám.

Azt mondhatjuk tehát, hogy

$$n = 2^{\alpha} \cdot m = 2^{\alpha} \cdot (2^{\alpha+1} - 1)$$

ahol $2^{\alpha+1} - 1$ prímszám (és mivel ilyen alakú, így egyben Mersenne-prím is). ■

11.3. Melyik fákat látom?

Tegyük fel, hogy a koordináta-rendszer origójában állunk és minden rácspontban (vagyis egész koordinátájú pontban) van egy fa, kivéve ahol mi vagyunk. A kérdés: Hány százalékát látjuk a fáknak? Na persze itt jó matematikus lévén felteszünk néhány igen furcsa dolgot, például hogy egyszerre látunk az összes irányba, tehát valójában csak azokat a fákat nem látjuk, akit egy másik fa (akit látunk) takar.

Például látjuk a $(2; 1)$, illetve a $(3; 1)$ koordinátájú pontokban lévő fákat, de a $(4; 2)$ -ben lévő nem, mert a $(2; 1)$ takarja. Általános is könnyen látható, hogy pontosan azokat a fákat látjuk, melyek $(a; b)$ koordinátáira igaz, hogy $(a, b) = 1$, tehát a kérdés valójában: mi a valószínűsége annak, hogy két egész szám relatív prímek?

Az ehhez kapcsolódó tétel bizonyításához szükségünk lesz egy másik nevezetes tételre, amiben nem vagyok biztos, hogy korábban szerepelt (talán Egyváltozós analízis 2-ből említettük, de nem láttuk be), ezt először kimondom, de nem bizonyítom, előadáson is csak hivatkoztunk rá.

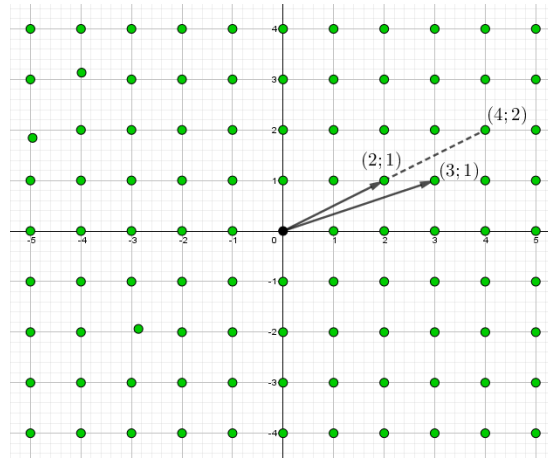
11.3.1. Tétel. A négyzetszámok reciprokösszege

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$



¹Az egyszerűsítés elvégezhető, hiszen ha $2^{\alpha+1} - 1 = 0$ volna, akkor $2^{\alpha+1} = 1$, azaz $\alpha + 1 = 0$, így $\alpha = -1$, ami lehetetlen, hiszen $\alpha > 0$, mert n -ről feltettük, hogy páros.

²Itt a harmadik azért nem lehet k , mivel akkor $2^{\alpha+1} - 1 = 1$ volna, azaz $2^{\alpha+1} = 2$ így $\alpha = 0$, de $\alpha > 0$, mert n páros.

11.2. ábra. A fák közepén állók, körbevesznek $(a; b)$ párok

És most jöjjön a fejezethez közvetlenül kapcsolódó tétel.

11.3.2. Tétel. Annak a valószínűsége, hogy a és b relatív prímek:

$$P((a, b) = 1) = \frac{6}{\pi^2}$$



Bizonyítás. Mit jelent az, hogy az a és b számok relatív prímek? Ez egy elég tág kérdés, mit jelent ez a 2 prímszámra nézve? Egy dolog biztos, nem oszthatja mindkét számot. Mi a valószínűsége annak, hogy a 2 nem osztja a vagy b számot. Tekintsük a komplementer eseményt, mi a valószínűsége, hogy a 2 osztja a -t és b -t is. Na ez már könnyű, függetlenek az események és a számok fele osztható 2-vel, így:

$$P(2 \nmid (a, b)) = 1 - P(a \text{ páros} \wedge b \text{ páros}) = 1 - P(a \text{ páros}) \cdot P(b \text{ páros}) = 1 - \frac{1}{2} \cdot \frac{1}{2}$$

Folytassuk a 3-mal, mivel az a következő prímszám. Hasonlóan gondolható végig, ismét komplementer eseménnyel a valószínűség:

$$P(3 \nmid (a, b)) = 1 - \frac{1}{3} \cdot \frac{1}{3}$$

Ezt végig kell nézni az összes többi prímre is:

$$x = P((a, b) = 1) = \prod_{p \text{ prím}} P(p \nmid (a, b)) = \prod_{p \text{ prím}} \left(1 - \frac{1}{p^2}\right) = \left(1 - \frac{1}{2^2}\right) \cdot \left(1 - \frac{1}{3^2}\right) \cdot \dots$$

Tekintsük az egészek a reciprokát:

$$\frac{1}{x} = \frac{1}{\left(1 - \frac{1}{2^2}\right) \cdot \left(1 - \frac{1}{3^2}\right) \cdot \dots} = \frac{1}{1 - \frac{1}{2^2}} \cdot \frac{1}{1 - \frac{1}{3^2}} \cdot \dots$$

Vegyük észre, hogy mivel a mértani sor összegképlete szerint

$$1 + q + q^2 + q^3 + \dots = \frac{1}{1 - q}$$

ezért jobboldalon valójában végtelen sok mértani sor összege van, azaz

$$\frac{1}{x} = \left(1 + \frac{1}{2^2} + \frac{1}{(2^2)^2} + \dots\right) \cdot \left(1 + \frac{1}{3^2} + \frac{1}{(3^2)^2} + \dots\right) \cdot \dots$$

vagyis elvégezve a beszorzásokat a lehetséges összes féle módon:

$$\frac{1}{x} = \sum \frac{1}{(2^2)^{\alpha_1} \cdot (3^2)^{\alpha_2} \cdot (5^2)^{\alpha_3} \dots} = \sum \frac{1}{(2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \dots)^2}$$

Vagyis jobboldalon a nevezőben ott áll az összes létező kanonikus alak négyzete (és még az 1 is). Márpedig mivel minden 1-nél nagyobb számnak egyértelműen létezik kanonikus alakja, így ami jobboldalon áll, az egészen pontosan a négyzetszámok reciprokösszege:

$$\frac{1}{x} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \quad \Leftrightarrow \quad x = \frac{6}{\pi^2}$$

Kész is vagyunk. ■

Végtelen sok prím

Ebbe a fejezetbe kerülnek a bizonyításai annak, hogy végtelen sok prím létezik.

12.1. $\sum_{n=1}^{\infty} \frac{1}{n}$ divergenssel

Ehhez a bizonyításhoz szükségünk van egy Egyváltozós analízis 2 tárgyból tanult tételre, ezt lemmaként kimondom és be is látom most.

12.1.1. Lemma. A $\sum_{n=1}^{\infty} \frac{1}{n}$ sor divergens.



Bizonyítás. Azt kellene belátnunk, hogy

$$S_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}$$

sorozat esetén $\lim_{n \rightarrow \infty} S_n = \infty$. Indirekt tegyük fel, hogy véges a határérték, konvergens a sorozat. Ekkor az S_n sorozat minden részsorozata is konvergens.

Tekintsük az S_{2^n} részsorozatát (csak a 2-hatvány indexek vannak a részsorozatban) és becsüljük alulról:

$$S_{2^n} = 1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\geq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\geq \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2}} + \dots + \frac{1}{2^{n-1}} + \underbrace{\frac{1}{2^{n-1}+1} + \dots + \frac{1}{2^n}}_{\geq \frac{1}{2^n} + \dots + \frac{1}{2^n} = 2^{n-1} \cdot \frac{1}{2^n} = \frac{1}{2}} \geq 1 + n \cdot \frac{1}{2}$$

Azt kaptuk tehát, hogy $S_{2^n} \geq 1 + \frac{n}{2}$, ekkor viszont $\lim_{n \rightarrow \infty} S_{2^n} \geq \lim_{n \rightarrow \infty} 1 + \frac{n}{2} = \infty$. Ezzel beláttuk, hogy S_{2^n} divergens, tehát S_n is. ■

Elevenítsük fel bizonyítás nélkül a mértani sor összegképletét is ($|q| < 1$): $\sum_{i=0}^{\infty} q^i = \frac{1}{1-q}$.

Most térjünk rá a tételünk bizonyítására: végtelen sok prím van. Indirekt tegyük fel szokásosan, hogy csak véges sok, legyenek ezek: p_1, p_2, \dots, p_u . Tekintsük a következő szorzatot:

$$P = \prod_{j=1}^u \left(\sum_{i=0}^{\infty} \frac{1}{p_j^i} \right) = \left(\sum_{i=0}^{\infty} \frac{1}{p_1^i} \right) \cdot \left(\sum_{i=0}^{\infty} \frac{1}{p_2^i} \right) \cdot \dots \cdot \left(\sum_{i=0}^{\infty} \frac{1}{p_u^i} \right) =$$

$$= \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \dots\right) \cdot \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \dots\right) \cdot \dots \cdot \left(1 + \frac{1}{p_u} + \frac{1}{p_u^2} + \dots\right)$$

Erre az összegre kétféleképpen is tekinthetünk, egyrészt ez véges sok mértani sor összegének szorzata, tehát véges:

$$P = \frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}} \cdot \dots \cdot \frac{1}{1 - \frac{1}{p_u}} \in \mathbb{R}$$

Másrészt elvégezve a beszorzásokat $\frac{1}{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_u^{\alpha_u}}$ alakú törtet adok össze az összes lehetséges α_i kitevőkkel. Vagyis előállítom az összes lehetséges prímtényező alakot és a kapott számok reciprokait adom össze. Vagyis a felírt szorzat valójában a számok reciprokösszege.

Tehát $P = \sum_{n=1}^{\infty} \frac{1}{n}$ végtelen sor, mely a 12.1.1. lemma szerint divergens. Ezzel meg is kaptuk várva várt ellentmondásunk, hiszen P nem lehet egyszerre véges és végtelen.

12.2. $\sum_{p \text{ PRÍM}} \frac{1}{p}$ divergenssel

Most azt fogjuk bebizonyítani, hogy a prímszámok reciprokösszege végtelen, ebből automatikusan következik az is, hogy végtelen sok prímszám van (hiszen ha csak véges sok volna, akkor azok reciprokösszege egy véges szám kellene legyen).

Indirekt tegyük fel, hogy $\sum_{\substack{i=1 \\ p_i \text{ PRÍM}}}^{\infty} \frac{1}{p_i}$ konvergens, legyen a sor összege A . Jelölje a részletösszeg sorozatot szokásosan S_n , illetve a továbbiakban p_i mindenhol az i -edik prímszámot jelenti. Sor összegének definíciója szerint ekkor

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \lim_{n \rightarrow \infty} \sum_{i=1}^n \frac{1}{p_i} = \lim_{n \rightarrow \infty} S_n = A$$

A határérték definíciója szerint $\forall \varepsilon > 0$ -ra (most speciálisan $\varepsilon = \frac{1}{2}$ -re) $\exists N$ küszöbindex, melyre ha $n > N$ akkor

$$|S_n - A| < \frac{1}{2} \Rightarrow -\frac{1}{2} < S_n - A \Rightarrow A - S_n < \frac{1}{2}$$

Legyen k egy olyan egész, mely már az előbb kapott küszöbindex fölött van: $k > N$. A legfeljebb k indexű prímekeket fogjuk kis prímeknek, a k -nál nagyobb indexű prímekeket pedig nagy prímeknek nevezni. Mivel $k > N$, így

$$A - S_k < \frac{1}{2}$$

most visszaírva, hogy A az S_n sorozat határértéke, S_k pedig egy szumma, mely nem függ n -től:

$$A - S_k = \lim_{n \rightarrow \infty} S_n - S_k = \sum_{i=1}^{\infty} \frac{1}{p_i} - \sum_{i=1}^k \frac{1}{p_i} = \sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$$

Ez a kis gondolkodás csak azért kellett, hogy analitikus szívem megnyugtassa, előadáson elintéztük annyival ami a lényege és amire végül is hajtottunk, hogy „nyilvánvalóan” $\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$

Azért valami haszna mégis csak volt ennek az oldalnyi analízisnek, bevezettük kis és nagy prímszámok fogalmát. Képzeljünk el egy rögzített n számot. 1-től n -ig vannak számok, egészen pontosan n darab. Kétféle szám van 1-től n -ig. Olyan, aminek van nagy prímosztója, és olyan aminek csak kicsik vannak. Hány van az egyes fajtákból?

Hány olyan $m \leq n$ szám létezik, melynek csak kicsi prímosztói vannak? Az ilyen szám prímosztói csakis a p_1, \dots, p_k prímek közül kerülhetnek ki, tehát m kanonikus alakja:

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

Emeljük ki a kanonikus alakból a legnagyobb négyzetszámot, amivel m osztható, legyen ez r^2 , ekkor az összes többi prím kitevője 0 vagy 1 kell legyen, hiszen ha p_i kitevője legalább 2 volna, akkor még p_i^2 is kiemelhető volna és r^2 nem lenne maximális:

$$m = r^2 \cdot p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \dots \cdot p_k^{\varepsilon_k}$$

ahol $\forall \varepsilon_i \in \{0; 1\}$. Mivel $r^2 \leq m \leq n$ ezért $r \leq \sqrt{n}$, tehát r legfeljebb \sqrt{n} féleképpen választható meg. Mivel minden ε_i kétféleképpen választható (0 vagy 1), így ilyen m számból legfeljebb $2^k \cdot \sqrt{n}$ darab van.

Hány olyan $M \leq n$ szám van, aminek van nagy prímosztója? A szóba jöhető nagy prímosztók: p_{k+1}, p_{k+2}, \dots . Hány olyan M van n -ig aminek osztója p_{k+1} ? Hát legfeljebb $\frac{n}{p_{k+1}}$. Hasonlóan p_{k+2} esetén legfeljebb $\frac{n}{p_{k+2}}$, stb... Összesen tehát hány olyan szám van, ami osztható nagy prímmel? Hát ha külön-külön már vannak felsőbecsléseink az egyes számosságokra, akkor adjuk össze ezeket, az aztán bőséges felső becslés lesz (hiszen lehet, hogy valami több nagy prímmel is osztható és akkor őt nagyon sokszor is megszámolhattuk), de most nekünk csak az számít, hogy a nagy prímszámmal osztható számokra felsőbecslés:

$$\frac{n}{p_{k+1}} + \frac{n}{p_{k+2}} + \dots = \sum_{i=k+1}^{\infty} \frac{n}{p_i} = n \cdot \sum_{i=k+1}^{\infty} \frac{1}{p_i} \stackrel{\text{„analízis”}}{<} n \cdot \frac{1}{2}$$

Már csak egy lépés van hátra. Ha megszámoljuk hány darab csupán kis prímosztókkal rendelkező szám van n -ig, illetve hány nagy prímosztókkal rendelkező, akkor n -et kell kapjunk, hiszen minden szám pontosan az egyik halmazba sorolható. Tehát az előbbi becslésekkel egyben n -re is kaptunk felső becslést:

$$n = \overbrace{|\{m \leq n \mid \nexists i > k: p_i \mid m\}|}^{\text{kis prímosztójú számok száma}} + \overbrace{|\{M \leq n \mid \exists i > k: p_i \mid M\}|}^{\text{nagy prímosztójú számok száma}} < 2^k \cdot \sqrt{n} + \frac{1}{2} \cdot n$$

Szóval azt kaptuk, hogy adott k esetén (amit analízissel kijelöltünk, ő határozta meg hogy mit nevezünk kis prímszámnak) ez az egyenlőtlenség minden n -re igaz. Akkor speciálisan $n = 2^{2k+2}$ -re is:

$$2^{2k+2} < 2^k \cdot 2^{k+1} + 2^{-1} \cdot 2^{2k+2} = 2^{2k+1} + 2^{2k+1} = 2 \cdot 2^{2k+1} = 2^{2k+2}$$

vagyis azt kaptuk, hogy a $2^{2k+2} < 2^{2k+2}$, ami nyilván ellentmondás, tehát beláttuk, hogy a $\sum \frac{1}{p}$ konvergens indirekt feltétel hamis, vagyis $\sum \frac{1}{p}$ divergens. Ezzel kész vagyunk.

12.3. $4k + 1$ alakúak

Tegyük fel, hogy csak véges sok $4k + 1$ alakú prím van, legyenek ezek p_1, p_2, \dots, p_k . Tekintsük a következő számot:

$$N = (2 \cdot p_1 \cdot \dots \cdot p_k)^2 + 1$$

Nilvánvaló, hogy $N \neq 0, 1, -1$, tehát létezik prímtényező felbontása, legyen ez

$$N = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

és rövidítés kedvéért jelöljük a $4k + 1$ alakú prímek szorzatának kétszeresét x -szel:

$$x = 2 \cdot p_1 \cdot \dots \cdot p_k$$

Ekkor persze $N = x^2 + 1$. Könnyen láthatjuk, hogy egyetlen q_i sem egyezhet meg egyetlen p_j -vel sem, hiszen különben

$$q_i \mid N \text{ és } q_i = p_j \mid x^2 \Rightarrow q_i \mid N - x^2 = 1$$

ami lehetetlen, mert 1-nek nincs prímosztója.

Az is világos, hogy $q_i > 2$, hiszen a $2 \nmid N$, mert $2 \mid x$, de $2 \nmid 1$.

Akkor azt látjuk, hogy $q_i > 2$ prím osztója egy $x^2 + 1$ alakú számnak. A 7.1.1. lemma alapján q_i egy $4k + 1$ alakú prím. Ez viszont ellentmondás, hiszen ekkor meg kellene egyeznie az „összes” $4k + 1$ alakú prím valamelyikével, de láttuk, hogy egyetlen p_j -vel sem azonos. Tehát végtelen sok $4k + 1$ alakú prím van.

12.4. $8k + 1$ alakúak

Ez szinte teljesen azonos lesz az előző bizonyításhoz, de szükségünk van hozzá egy lemmára, ami itt is a bizonyítás végén fog segíteni.

12.4.1. Lemma. Legyen $p > 2$ prím és $x \in \mathbb{Z}$. Ha $p \mid x^4 + 1$, akkor $p = 8k + 1$ alakú. ♣

Megjegyzés. Feltehető $(p, x) = 1$ is, de nincs rá szükség, mert ha $p \mid x$ eset volna, akkor $p \mid 1$ is igaz lenne, de az 1-nek nincs prímosztója. Ez a megjegyzés csak ahhoz kellett, hogy nyugodtan beszélhessünk x rendjéről modulo p .

Bizonyítás. Ha $p \mid x^4 + 1$, akkor annak többszörösét is:

$$p \mid (x^4 + 1) \cdot (x^4 - 1) = x^8 - 1$$

vagyis $x^8 \equiv 1 \pmod{p}$. Mivel a rend osztja a jó kitevőket, ezért $o_p(x) \mid 8$. Azt fogjuk belátni, hogy a rendje pontosan 8.

Ugyanis ha kevesebb lenne a rendje, akkor 8 osztói közül kerülhetne ki, de nem 8 lenne, azaz $o_p(x) \mid 4$, tehát a 4 a rend többszöröse, azaz jó kitevő: $x^4 \equiv 1 \pmod{p}$. Ekkor viszont

$$p \mid x^4 + 1 \text{ és } p \mid x^4 - 1$$

tehát a különbségüket, $x^4 + 1 - (x^4 - 1) = 2$ -t is osztja. A 2-nek azonban nincs 2-nél nagyobb p prímosztója, tehát ellentmondást kaptunk, azaz x -nek nem lehet 8-nál kevesebb a rendje.

Tudjuk azt is, hogy $\varphi(p)$ jó kitevő, tehát $8 = o_p(x) \mid \varphi(p) = p - 1$. Ez éppen azt jelenti, hogy $p = 8k + 1$ alakú. ■

Innentől a bizonyítást csak másolni kell az előző $4k + 1$ alakúról.

Tegyük fel, hogy csak véges sok $8k + 1$ alakú prím van, legyenek ezek p_1, p_2, \dots, p_k . Tekintsük a következő számot:

$$N = (2 \cdot p_1 \cdot \dots \cdot p_k)^4 + 1$$

Nyilvánvaló, hogy $N \neq 0, 1, -1$, tehát létezik prímtényező felbontása, legyen ez

$$N = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

és rövidítés kedvéért jelöljük a $8k + 1$ alakú prímelek szorzatának kétszeresét x -szel:

$$x = 2 \cdot p_1 \cdot \dots \cdot p_k$$

Ekkor persze $N = x^4 + 1$. Könnyen láthatjuk, hogy egyetlen q_i sem egyezhet meg egyetlen p_j -vel sem, hiszen különben

$$q_i \mid N \text{ és } q_i = p_j \mid x^4 \Rightarrow q_i \mid N - x^4 = 1$$

ami lehetetlen, mert 1-nek nincs prímosztója.

Az is világos, hogy $q_i > 2$, hiszen a $2 \nmid N$, mert $2 \mid x$, de $2 \nmid 1$.

Akkor azt látjuk, hogy $q_i > 2$ prím osztója egy $x^4 + 1$ alakú számnak. A 12.4.1. lemma alapján q_i egy $8k + 1$ alakú prím. Ez viszont ellentmondás, hiszen ekkor meg kellene egyeznie az „összes” $8k + 1$ alakú prím valamelyikével, de láttuk, hogy egyetlen p_j -vel sem azonos. Tehát végtelen sok $8k + 1$ alakú prím van.

12.5. $8k - 1$ alakúak

Indirekt fel, hogy csak véges sok $8k - 1$ alakú prím van, legyenek ezek p_1, p_2, \dots, p_k . Tekintsük a következő számot:

$$N = (p_1 \cdot \dots \cdot p_k)^2 - 2$$

Nyilvánvaló, hogy $N \neq 0, 1, -1$, tehát létezik prímtényező felbontása, legyen ez

$$N = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

és rövidítés kedvéért jelöljük a $8k - 1$ alakú prímelek szorzatát x -szel:

$$x = p_1 \cdot \dots \cdot p_k$$

Ekkor persze $N = x^2 - 2$. Könnyen láthatjuk, hogy egyetlen q_i sem egyezhet meg egyetlen p_j -vel sem, hiszen különben

$$q_i \mid N \text{ és } q_i = p_j \mid x^2 \Rightarrow q_i \mid x^2 - N = 2$$

ami lehetetlen, mert ekkor q_i csak a 2 lehetne, de N -nek nem osztója 2, hiszen

$$\forall p_j = 8k - 1 \equiv 1 \pmod{2} \Rightarrow N = (p_1 \cdot \dots \cdot p_k)^2 - 2 \equiv 1 \pmod{2}$$

Most jön a lényeg, belátjuk, hogy q_i -k között van $8k - 1$ alakú (eddig azt láttuk be szokásosan, hogy bármik is ezek a q_i -k, nincsenek a p_j -k között).

Ha tekintek egy tetszőleges q_i -t, akkor mivel $q_i \mid N = x^2 - 2$, így $x^2 \equiv 2 \pmod{q_i}$, ami azt jelenti, hogy a 2 kvadratikusan maradék modulo q_i , azaz

$$\left(\frac{2}{q_i}\right) = 1 \Leftrightarrow q_i = 8k \pm 1$$

Lehetséges-e, hogy az összes $q_i = 8k + 1$ alakú? Az a baj, hogy akkor szorzatuk, N is az volna, amiről viszont könnyen látható, hogy

$$N \equiv ((-1) \cdot \dots \cdot (-1))^2 - 2 \equiv -1 \pmod{8} \Rightarrow N = 8k - 1 \text{ alakú}$$

Tehát kell lennie q_i -k között $8k - 1$ alakúnak, amivel találtunk egy új $8k - 1$ alakú prímet, ezzel ellentmondáshoz jutottunk, vagyis végtelen sok $8k - 1$ alakú prím van.

12.6. $8k + 3$ alakúak

Indirekt fel, hogy csak véges sok $8k + 3$ alakú prím van, legyenek ezek p_1, p_2, \dots, p_k . Tekintsük a következő számot:

$$N = (p_1 \cdot \dots \cdot p_k)^2 + 2$$

Nyilvánvaló, hogy $N \neq 0, 1, -1$, tehát létezik prímtényezős felbontása, legyen ez

$$N = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

és rövidítés kedvéért jelöljük a $8k + 3$ alakú prímek szorzatát x -szel:

$$x = p_1 \cdot \dots \cdot p_k$$

Ekkor persze $N = x^2 + 2$. Könnyen láthatjuk, hogy egyetlen q_i sem egyezhet meg egyetlen p_j -vel sem, hiszen különben

$$q_i \mid N \text{ és } q_i = p_j \mid x^2 \Rightarrow q_i \mid N - x^2 = 2$$

ami lehetetlen, mert ekkor q_i csak a 2 lehetne, de N -nek nem osztója 2, hiszen

$$\forall p_j = 8k + 3 \equiv 1 \pmod{2} \Rightarrow N = (p_1 \cdot \dots \cdot p_k)^2 + 2 \equiv 1 \pmod{2}$$

Most jön a lényeg, belátjuk, hogy q_i -k között van $8k + 3$ alakú (eddig azt láttuk be szokásosan, hogy bármik is ezek a q_i -k, nincsenek a p_j -k között).

Ha tekintek egy tetszőleges q_i -t, akkor mivel $q_i \mid N = x^2 + 2$, így $x^2 \equiv -2 \pmod{q_i}$, ami azt jelenti, hogy a -2 kvadratikusan maradék modulo q_i , azaz

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

Milyen alakú lehet akkor q_i ? Csináljunk egy táblázatot aszerint, hogy q_i mennyi maradékot ad modulo 8 és gondoljuk meg, hogy a 4 esetből 2 kizárható³:

| q_i | $\left(\frac{-1}{q_i}\right)$ | $\left(\frac{2}{q_i}\right)$ | $\left(\frac{-2}{q_i}\right) = \left(\frac{-1}{q_i}\right) \cdot \left(\frac{2}{q_i}\right)$ |
|--------|-------------------------------|------------------------------|--|
| $8k+1$ | 1 | 1 | 1 |
| $8k-1$ | -1 | 1 | -1 |
| $8k+3$ | -1 | -1 | 1 |
| $8k-3$ | 1 | -1 | -1 |

A táblázat szerint minden $q_i = 8k+1$ vagy $8k+3$ alakú. Lehetséges-e, hogy az összes $q_i = 8k+1$ alakú? Az a baj, hogy akkor szorzatuk, N is az volna, amiről viszont könnyen látható, hogy modulo 8

$$N \equiv (3 \cdot \dots \cdot 3)^2 + 2 = 9 \cdot \dots \cdot 9 + 2 \equiv 1 \cdot \dots \cdot 1 + 2 = 3 \pmod{8}$$

Tehát kell lennie q_i -k között $8k+3$ alakúnak, amivel találtunk egy új $8k+3$ alakú prímet, ezzel ellentmondáshoz jutottunk, vagyis végtelen sok $8k+3$ alakú prím van.

12.7. Mersenne-számokkal: $q \mid 2^p - 1$

12.7.1. Tétel. Ha $p > 2$ prím és q prímre $q \mid M_p = 2^p - 1$, akkor $q = 2kp + 1$ alakú. ♣

Vegyük észre, hogy a tételt belátva, megint megkapjuk, hogy végtelen sok prím létezik. Hiszen ha csak véges sok, akkor van közöttük utolsó, legnagyobb. Legyen ez p_u . Ekkor azonban $2^{p_u} - 1$ nem egység, tehát van neki q prímosztója, melyről tudjuk, hogy $q = 2kp + 1$ alakú, tehát azt kaptuk, hogy $q > p_u$. Ez viszont ellentmondás, hiszen feltettük, hogy p_u a legnagyobb prím, de találtunk nála nagyobbat. Lássuk be most a tételt⁴.

Bizonyítás. Amennyiben $q \mid 2^p - 1$, akkor másképp írva $2^p \equiv 1 \pmod{q}$. Ekkor viszont a p egy jó kitevője a 2-nek, tehát $o_q(2) \mid p$. Mivel p felbonthatatlan, így $o_q(2) = 1$ vagy $o_q(2) = p$. Az első eset nem lehetséges, hiszen ha már $2^1 = 2 \equiv 1 \pmod{q}$ az azt jelentené, hogy $q \mid 2 - 1 = 1$, de az 1-nek nincs prímosztója.

Tehát csakis az lehetséges, hogy $o_q(2) = p$. Viszont $o_q(2) \mid \varphi(q) = q - 1$, tehát $p \mid q - 1$ azaz $\exists t \in \mathbb{Z}: q - 1 = t \cdot p$ ahonnan $q = tp + 1$.

Állapítsuk meg azt is, hogy $p > 2$ prím feltétel miatt p páratlan és $q \mid 2^p - 1$ miatt q is páratlan. Viszont ha t is páratlan lenne akkor $q = tp + 1$ miatt a páratlan baloldal lenne egyenlő a páros jobb oldallal, ami nyilván nem lehetséges, tehát t -nek párosnak kell lennie, vagyis $t = 2k$ alakú. Ezzel beláttuk, hogy $q = 2kp + 1$ alakú. ■

³2. oszlop kitöltéséhez az 5. szabályt, 3. oszlophoz a 7.2.2. tételt, 4. oszlophoz pedig a 2. szabályt használtam

⁴Freud: Számelmélet, 5.2.3 Tétel

12.8. Csebisev-tétellel

Ebben a fejezetben a feladat tulajdonképpen a Csebisev-tétel (és a hozzá kapcsolódó becsléses lemmák) bizonyítása, abból automatikusan következik, hogy végtelen sok prím van: Ha feltesszük, hogy véges sok prím van, akkor legyen p közülük a legnagyobb. A Csebisev tétel szerint mivel $p+1 > 1$, így van q prím $p+1 \leq q \leq 2p+2$, azaz $p < q$, ami lehetetlen, hiszen p volt a legnagyobb prím.

Még egyszer hangsúlyozom, ennél a fejezetnél a bizonyítás „lényegi” része a 10. előadás 2. és 3. fejezete.

12.9. Alsó becslés $\pi(n)$ -re

Ezen a bizonyításon egy picit változtattam az óraihoz képest, mert az egyik lépésben szerintem $\pi(n+1)$ tényezősszorzatot kapunk, melynek tagjai is $n+1$ -gyel becsülhetők felül (ugyanis gondolnunk kell arra az esetre, hogy $n+1$ is lehet prímszám). Éppen ezért picit máshogy mondom ki a fő állítást, az órai az volt, hogy $\pi(n) \geq \frac{n}{\log_2 n}$ feltéve, hogy $n > 2$ páros szám.

A továbbiakban $\pi(n)$ jelöli a prímszámok számát 2-től n -ig, azaz: $\pi(n) = |\{2 \leq p \leq n \text{ prím}\}|$

12.9.1. Tétel. Ha $n > 0$ páros egész, akkor $\pi(n+1) \geq \frac{n}{\log_2(n+1)}$ ♣

Megint csak vegyük észre, hogy a tételből következik, hogy végtelen sok prím van. Ha indirekt feltesszük, hogy csak véges sok prím van, akkor az $a_n = \pi(n)$ sorozat felülről korlátos. Mivel monoton (növekszik) és (felülről) korlátos, így konvergens is. Ekkor viszont bármely részsorozata is konvergens, tehát $b_n = a_{2n}$ is. Erről viszont azt tudjuk a tétel miatt, hogy ha $n > 1$ akkor

$$b_n = \pi(2n) = \pi(2 \cdot (n-1) + 2) \geq \pi(2 \cdot (n-1) + 1) \stackrel{\text{tétel}}{\geq} \frac{2n-2}{\log_2(2n-2+1)}$$

Nagyságrendek miatt

$$\lim_{n \rightarrow \infty} \frac{2n-2}{\log_2(2n-1)} = \infty$$

így határérték és rendezés kapcsolata miatt

$$\lim_{n \rightarrow \infty} b_n = \infty$$

Ekkor viszont b_n nem konvergens, hiszen határértéke végtelen: Ellentmondás, tehát végtelen sok prím van. Lássuk be a tételt.

Bizonyítás. Tekintsük az $f: [0; 1] \rightarrow \mathbb{R}$, $f(x) = x \cdot (1-x)$ függvényt. A számtani-mértani egyenlőtlenség miatt

$$G(x, 1-x) = \sqrt{x \cdot (1-x)} \leq \frac{x+1-x}{2} = \frac{1}{2}$$

vagyis f -nek felső korlátja

$$x \cdot (1-x) \leq \frac{1}{4}$$

mindkét oldalt $\frac{n}{2}$ -edik hatványra (ami egész, hiszen n páros) emelve:

$$(x - x^2)^{\frac{n}{2}} \leq \left(\frac{1}{4}\right)^{\frac{n}{2}} = \frac{1}{4^{\frac{n}{2}}} = \frac{1}{2^n}$$

A felső becslés nem függ x -től, az egy konstans függvény. Integráljuk az egyenlőtlenség mindkét oldalán lévő függvényt a $[0; 1]$ intervallumon, ekkor a Riemann-integrál és rendezés kapcsolata miatt:

$$\int_0^1 (x - x^2)^{\frac{n}{2}} dx \leq \int_0^1 \frac{1}{2^n} dx = \left[\frac{1}{2^n} \cdot x \right]_0^1 = \frac{1}{2^n}$$

Hogyan tudnánk kiszámolni, vagy legalábbis alulról tovább becsülni a baloldali integrál értékét? Mivel n páros, így a binomiális tétel miatt igazából csak egy polinomfüggvény az integrandus, tehát a feladat valójában:

$$\int_0^1 a_n x^n + \dots + a_1 x + a_0 dx = \left[\frac{a_n}{n+1} \cdot x^{n+1} + \dots + \frac{a_1}{2} \cdot x^2 + \frac{a_0}{1} \cdot x \right]_0^1 = \frac{a_n}{n+1} + \dots + \frac{a_1}{2} + \frac{a_0}{1}$$

Hogyan adjuk össze ezt a végén kapott csomó törtet? Közös nevező a nevezők legkisebb közös többszöröse lesz, az pedig hogy a számlálóban mit kapunk nem is igazán érdekes számunkra, nem 0 számot (a terület bármely rögzített n esetén nem 0) és ez már elegendő:

$$= \frac{\text{valami egész}}{[1, 2, \dots, n, n+1]} \geq \frac{1}{[1, 2, \dots, n, n+1]}$$

Mit tudunk az első $n+1$ szám legkisebb közös többszöröséről? Hogyan állítjuk elő? Felírjuk a számok prímtényezői felbontásait, aztán minden előforduló prímet a legmagasabb előforduló kitevőn kiválasztunk.

$$[1, 2, \dots, n, n+1] = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$$

Tehát minden p prímre, ami szerepel a legkisebb közös többszörösben igaz, hogy $p \leq n+1$, másrészt azért választottuk α kitevővel, mert valamelyik számot (1-től $n+1$ -ig) osztja p^α . De ha van olyan $k \leq n+1$, melyre $p^\alpha \mid k$, akkor oszthatóság definíciója szerint $\exists b$, melyre $p^\alpha \cdot b = k \leq n+1$, ami azt jelenti, hogy igazából $p^\alpha \leq n+1$ is igaz. Vagyis a legkisebb közös többszörös kanonikus alakjának minden prímhatalmánya felülről becsülhető $n+1$ -gyel.

És hány prím fordul elő a prímtényezői felbontásban? Ahány prím van $n+1$ -ig, erre még je-lölésünk is van: $\pi(n+1)$. Tehát a legkisebb közös többszörös egy $\pi(n+1)$ tényezői szorzat, melynek minden tényezője felülről becsülhető $n+1$ -gyel:

$$\frac{1}{2^n} \geq \int_0^1 (x \cdot (1-x))^{\frac{n}{2}} dx \geq \frac{1}{[1, 2, \dots, n, n+1]} \geq \frac{1}{(n+1) \cdot (n+1) \cdot \dots \cdot (n+1)} \geq \frac{1}{(n+1)^{\pi(n+1)}}$$

Az elejét és a végét összeolvasva, átrendezve:

$$(n+1)^{\pi(n)} \geq 2^n$$

átírva a logaritmus definíciója szerint

$$(n+1)^{\pi(n)} = 2^{\log_2(n+1)^{\pi(n)}} = 2^{\pi(n) \cdot \log_2(n+1)} \geq 2^n$$

és a 2^x exponenciális függvény (szigorú) monoton növekedése miatt

$$\pi(n+1) \cdot \log_2(n+1) \geq n$$

ahonnan $\log_2(n+1)$ -gyel osztva adódik a bizonyítandó állítás. ■

12.10. Körosztási polinomokkal: $nk + 1$ alakúak

Ebben a bizonyításban is el fogok picit térni az előadáson elhangzottaktól, alapvetően igyekszem azt követni, de számomra így érthetőbb volt az a bizonyos fontos lépés, hogy miért alkalmazható a SZAT. **Fontos!** Vizsgára készüléskor szerintem lényeges tudni a 10. előadás 1. fejezetében lévő tételek (de legalább a 10.1.2. tétel) bizonyítását.

Most azt fogjuk belátni, hogy adott $n \geq 1$ esetén végtelen sok $n \cdot k + 1$ alakú prím létezik. Ez az állítás $n = 1$ -re annyit mond, hogy végtelen sok $k + 1$ alakú prím (tehát végtelen sok prím), $n = 2$ esetén, hogy végtelen sok $2k + 1$ alakú prím (tehát végtelen sok páratlan prím) létezik. Ezek nyilván nem nagy információk, eddig is tudtuk, hogy végtelen sok páratlan prím van. Innentől kezdve tehát felteszem⁵, hogy $n > 2$.

Adott tehát $n > 2$ és indirekt tegyük fel szokásosan, hogy csak véges sok $nk + 1$ alakú prím van, legyenek ezek p_1, p_2, \dots, p_u .

Mivel $\Phi_n(x) \mid x^n - 1$, ezért helyettesítve $x = p_1 \cdot p_2 \cdot \dots \cdot p_u \cdot n$ -et:

$$\Phi_n(p_1 \cdot p_2 \cdot \dots \cdot p_u \cdot n) \mid (p_1 \cdot p_2 \cdot \dots \cdot p_u \cdot n)^n - 1$$

Feltettük, hogy $n > 2$, így a továbbiakban m -mel jelölt $m = p_1 \cdot p_2 \cdot \dots \cdot p_u \cdot n$ -re is teljesül, hogy $m > 2$. Definíció szerint

$$\Phi_n(m) = \prod_{o(\varepsilon)=n} (m - \varepsilon)$$

Azt fogjuk megmutatni, hogy ez nem lehet sem 0, sem 1, sem -1 , mert abszolútértéke nagyobb 1-nél⁶:

$$|\Phi_n(m)| = \left| \prod_{o(\varepsilon)=n} (m - \varepsilon) \right| = \prod_{o(\varepsilon)=n} |m - \varepsilon| > \prod_{o(\varepsilon)=n} 1 = 1$$

Elég volna tehát belátnunk, hogy $|m - \varepsilon|$ tetszőleges primitív n -edik egységgyök esetén nagyobb lesz 1-nél.

Itt most visszaléptünk picit a komplex számok világába. Az $m > 2$ egy egész szám, de mint komplex szám ő $m = m - 0i$ alakú, hasonlóan ε egy primitív n -edik egységgyök, így tehát $\varepsilon = a + bi$ komplex szám, melyre $1 = |\varepsilon| = \sqrt{a^2 + b^2}$, ahonnan $a^2 + b^2 = 1$, vagyis $a \leq 1$, hiszen ha $a > 1$ volna akkor $a^2 > 1$ miatt $a^2 + b^2 > 1$ lenne, ami nem igaz.

Hogyan néz ki akkor $|m - \varepsilon|$?

$$|m - \varepsilon| = |m - 0i - a - bi| = \sqrt{(m - a)^2 + b^2} = \sqrt{m^2 - 2ma + a^2 + b^2} = \sqrt{m^2 - 2ma + 1}$$

A gyökvonás monoton növekedése miatt ha alulról becsüljük az alatta lévő kifejezést, akkor a gyökjellel együtt is alulról becsültük az egészet, márpedig itt alsó becsléshez elegendő a -t felülről becselnünk, hiszen negatív előjellel szerepel, így az a -ra adott felsőbecsléssel a gyökös

⁵Ezt most tényleg én teszem fel, előadáson nem tettük, de hasonlóan elmondható a bizonyítás, ha azt mondom, hogy ismerünk páratlan prímet, például a 3 ilyen. Ez a feltétel itt csak azért kellett nekem, hogy egy szorzatról azt mondhasam, hogy legalább 2, és $n = 1$ vagy $n = 2$ esetén mivel a 3 a tényezők között van, akkor is teljesül, általánosan pedig $n > 2$ szorzótényező miatt fog teljesülni.

⁶Bár $\Phi_n(m)$ egész, itt most komplex számként értelmezzük az abszolútértéket és alkalmazzuk a szokásos "szorzat abszolútértéke az abszolútértékek szorzata" tulajdonságot.

kifejezésre alsó becslést kaphatunk. Használva tehát az $a \leq 1$ megállapítást:

$$|m - 0i - a + bi| = \sqrt{m^2 - 2ma + 1} \geq \sqrt{m^2 - 2m + 1} = \sqrt{(m - 1)^2} = |m - 1| > 1$$

hiszen $m > 2$. Ezzel tehát beláttuk, hogy minden $|m - \varepsilon| > 1$, tehát a szorzatuk is, kijelenthetjük végre, hogy $|\Phi_n(m)| > 1$.

Innentől ismerős lesz a sztori, immáron csaknem tizedjére: Mivel $|\Phi_n(m)| > 1$, így ő nem lehet 1, 0 és -1 sem, vagyis ő nem egység és nem nulla, tehát a számelmélet alaptétele szerint felírható prímek szorzataként:

$$\Phi_n(m) = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

ahol minden q_i különbözik az eddigi összes p_j -től, hiszen ha $q_i = p_j$ esete állna fenn, akkor $q_i \mid \Phi_n(m)$ és $\Phi_n(m) \mid m^n - 1$, így $q_i \mid m^n - 1$, vagyis

$$q_i \mid (p_1 \cdot \dots \cdot p_u \cdot n)^n - 1$$

ahonnan az $q_i = p_j$ miatt az első tagot osztja, tehát a másodikat is kellene, de $q_i \nmid 1$, mert az 1-nek nincs prímosztója.

Vagyis minden q_i olyan prím, mely eddig nem szerepelt a p -k között, már csak azt kellene látni, hogy $nk + 1$ alakú. Ezt a 10.1.2. tétel garantálja nekünk, hiszen $q_i \mid \Phi_n(m)$ és $q_i \nmid n$ (különben ha osztaná, akkor m -et is és megint az előző probléma állna fenn, meg kellene egyeznie az m szám egyik prímtényezőjével), így tehát $q_i = nk + 1$ alakú, ami az eddigi „összes” egyikével sem egyezik, ezáltal beláttuk, hogy végtelen sok $nk + 1$ alakú prím van.

Mi várható?

Valószínűleg ez a jegyzet végleges változata! A jelzett hibákat természetesen javítani fogom, de a **8. előadás** végül NEM került kidolgozásra és NEM IS FOG ebben a vizsgaidőszakban.

Akit érint, az ott található témaköröknek (Pitagoraszai számhármassok, Fermat-sejtés, RSA) érdemes utána olvasni Freud: Számelmélet könyvében, illetve meghallgatni az előadás hanganyagát.

Az utolsó előadáson vetített 3 diasorral kapcsolatban sem fog szerepelni semmi a jegyzetben, kivéve a 3 link:

1. Harcos Gergely: Prímek, Polignac, Polymath
2. Pintz János: Prímek közti különbségekről
3. Pethő Attila: Párhuzamosságok az ismert Mersenne prímszámok növekedése és az informatika fejlődése között

Sok sikert kívánok mindenkinek a vizsgákhoz! :)

Mellékletek

13.1. Miért a bővítése?

Ebben a fejezetben tisztázásra kerül egy gondolat, ami fölött átsiklottam egy egyébként sem triviális bizonyítás során. Az 5.2.2. lemma bizonyításának egy pontján használjuk a fokszámtételezt, ugyanakkor azt is meg kellene mutatnunk, hogy a testek amikre használjuk, azok valóban egymás bővítései, tehát kérdés, hogy miért igaz

$$\mathbb{Q} \leq \mathbb{Q}\left(\cos \frac{2\pi}{n}\right) \leq \mathbb{Q}(\varepsilon)$$

Az első bővítés nyilvánvaló, a második nem az. Miért van az, hogyha a racionális számainkhoz hozzávettük ε primitív egységgyököt, akkor már $\cos\left(\frac{2\pi}{n}\right)$ -et is?

Hát ekkor benne van a testünkben $\varepsilon = \cos\left(\frac{2\pi}{n}\right) + i \cdot \sin\left(\frac{2\pi}{n}\right)$, tehát ennek bármely hatványa, például az $n-1$ -edik is:

$$\varepsilon^{n-1} = \cos\left(\frac{2\pi \cdot (n-1)}{n}\right) + i \cdot \sin\left(\frac{2\pi \cdot (n-1)}{n}\right) = \cos\left(2\pi - \frac{2\pi}{n}\right) + i \cdot \sin\left(2\pi - \frac{2\pi}{n}\right)$$

használva, hogy a \sin és \cos függvények periodikusak 2π szerint

$$= \cos\left(-\frac{2\pi}{n}\right) + i \cdot \sin\left(-\frac{2\pi}{n}\right)$$

majd pedig, hogy a \sin páratlan, \cos pedig páros

$$= \cos\left(\frac{2\pi}{n}\right) - i \cdot \sin\left(\frac{2\pi}{n}\right)$$

Tehát ez is benne van a testünkben. De ha két szám benne van, akkor azok összege is:

$$\varepsilon + \varepsilon^{n-1} = \cos\left(\frac{2\pi}{n}\right) + i \cdot \sin\left(\frac{2\pi}{n}\right) + \cos\left(\frac{2\pi}{n}\right) - i \cdot \sin\left(\frac{2\pi}{n}\right) = 2 \cdot \cos\left(\frac{2\pi}{n}\right)$$

akkor viszont ennek fele is, azaz beláttuk, hogy valóban $\mathbb{Q}\left(\cos \frac{2\pi}{n}\right) \leq \mathbb{Q}(\varepsilon)$.

13.2. Klasszikus bizonyítás

A végtelen sok prímek bizonyítások közül a vizsga tematikában nem szerepel a klasszikus, középiskolában is elhangzó bizonyítás. Ugyanakkor mivel előadáson is elhangzott, és mégiscsak egy klasszikus bizonyításról van szó, helyet érdemel ez is a jegyzetben.

Indirekt tegyük fel, hogy véges sok prím van, legyenek ezek p_1, p_2, \dots, p_k . Tekintsük a következő számot

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$$

Első fontos észrevétel, hogy $N \geq 2$, mivel egy nemnulla számhoz adtunk hozzá 1-et. Ezek szerint $N \neq 0, 1, -1$. Márpedig ha N nem nulla és nem egység, akkor a számelmélet alaptétele szerint felírható prímek szorzataként, azaz $\exists q_1, q_2, \dots, q_t$ prímek, melyekre

$$q_1 \cdot q_2 \cdot \dots \cdot q_t = N = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$$

Tekintsük q_1 -et. Mivel ő egy prím, és a bizonyítás elején mi azt mondtuk, hogy az összes létező prím ott szerepel a felsorolásban, ezért $\exists i$, melyre $q_1 = p_i$. Ekkor azonban

$$q_1 \mid N \quad \text{és} \quad q_1 = p_i \mid p_1 \cdot \dots \cdot p_k = N - 1$$

De ha $q_1 \mid N$ és $q_1 \mid N - 1$, akkor a különbségüket is osztja, azaz $q_1 \mid 1$. Ellentmondás, hiszen q_1 prím, az 1-nek pedig nem létezik prímosztója.

13.3. Csebisev-tétel vége

Most a Csebisev-tétel bizonyításának a végére adok egy másik lehetséges indoklást, nekem így sikerült megértenem és szerintem egyszerűbb is, mint a deriválós.

Változtatunk egy korábbi tételen is, finomítunk rajta:

$$\binom{2n}{n} > \frac{4^n}{2n}$$

Mivel $\binom{2n}{n}$ a középső tag továbbra is a sorából, ezért az átlagnál nagyobb. De a korábbi, előadáson elhangzó bizonyításban erre úgy tekintettünk, hogy $2n + 1$ tag van a sorában. Valójában ebből a szélső kettő nagyon kicsi, csupán 1-ek mindig, vonjuk őket össze 1 taggá és a következő számokat átlagoljuk:

$$\binom{2n}{0} + \binom{2n}{2n}, \quad \binom{2n}{1}, \quad \binom{2n}{2}, \quad \dots \quad \binom{2n}{2n-1}$$

A sorösszeg ekkor továbbra is 4^n , viszont az átlagolandó elemek száma $2n$, így már ki is jött a finomabb állítás.

Ezzel az állítással nincs szükségünk a $(2n)^{\sqrt{2n+1}} \leq (2n+1)^{\sqrt{2n+1}}$ becslésre, így most a bizonyítandó egy picit változott:

$$\frac{4^{\frac{1}{3}n}}{(2n)^{\sqrt{2n+1}}} > 1$$

Először is indirekt tegyük fel, hogy

$$\frac{4^{\frac{1}{3}n}}{(2n)^{\sqrt{2n+1}}} \leq 1 \Leftrightarrow 4^{\frac{1}{3}n} \leq (2n)^{\sqrt{2n+1}} \Leftrightarrow 2^{2n} \leq (2n)^{3 \cdot (\sqrt{2n+1})} \quad (13.3.1)$$

Emlék:

Bernoulli-egyenlőtlenség: Amennyiben $n \in \mathbb{N}^+$ és $h \geq -1$ akkor $(1+h)^n \geq 1+nh$ és egyenlőség csak $n = 1$ vagy $h = 0$ esetén áll fenn.

Speciálisan

$$2^n = (1+1)^n > 1+n \quad (13.3.2)$$

Fontos visszaemlékeznünk arra is, hogy az egészrész definíciója szerint $x - 1 < \lfloor x \rfloor \leq x$ azaz $x < \lfloor x \rfloor + 1$.

Tekintsük a következő becslés sorozatot:

$$2n = (\sqrt[6]{2n})^6 < (\lfloor \sqrt[6]{2n} \rfloor + 1)^6 \stackrel{13.3.2}{<} \left(2^{\lfloor \sqrt[6]{2n} \rfloor}\right)^6 = 2^{6 \cdot \lfloor \sqrt[6]{2n} \rfloor} \leq 2^{6 \cdot \sqrt[6]{2n}} \quad (13.3.3)$$

Mivel $n < 50$ -re láttuk, hogy igaz a Csebisev-tétel eddig is, ezért feltehető, hogy $n \geq 50$, azaz

$$2n \geq 100 \Leftrightarrow \sqrt{2n} \geq 10 \Leftrightarrow 2 \cdot \sqrt{2n} \geq 20 > 18$$

Most pedig tekintsük a következő becslés sorozatot:

$$2^{2n} \stackrel{13.3.1}{\leq} (2n)^{3 \cdot (\sqrt{2n+1})} \stackrel{13.3.3}{<} \left(2^{6 \cdot \sqrt[6]{2n}}\right)^{3 \cdot (\sqrt{2n+1})} = 2^{18 \cdot (\sqrt{2n+1}) \cdot \sqrt[6]{2n}}$$

felülbecsülve az egyik 18-ast

$$= 2^{(18\sqrt{2n+18}) \cdot \sqrt[6]{2n}} < 2^{(18\sqrt{2n}+2 \cdot \sqrt{2n}) \cdot \sqrt[6]{2n}} = 2^{20\sqrt{2n} \cdot \sqrt[6]{2n}}$$

ahonnan a 2^x exponenciális függvény szigorú monoton növekedése miatt

$$2n < 20 \cdot \sqrt{2n} \cdot \sqrt[6]{2n} = 20 \cdot (2n)^{\frac{2}{3}}$$

osztva 2-vel és köbre emelve

$$n < 10 \cdot (2n)^{\frac{2}{3}} \Leftrightarrow n^3 < 1000 \cdot 4 \cdot n^2 \Leftrightarrow n < 4000$$

Vagyis azt kaptuk, hogy ha nem teljesül amit be akarunk látni, akkor $n < 4000$. Ez jó hír, mert ezek szerint $n \geq 4000$ -re beláttuk a Csebisev-tételt, az első 4000 szám ezután már semmiség, hasonlóan fejezzük be ahogy az előadáson elhangzott bizonyítást is, egy megfelelő prímsorozat (ahol minden prím kisebb az előtte levő kétszeresénél):

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$