ALGEBRA ÉS SZÁMELMÉLET 3

vázlat az előadáshoz[†]

2017 őszi félév, OT

Waldhauser Tamás

1. Relációk

Ekvivalenciák és osztályozások

1.1. Definíció. Adott A halmazon értelmezett ***reláción*** A-beli elemekből alkotott elempárok halmazát értjük, azaz egy tetszőleges $\rho \subseteq A \times A$ halmazt.

Jelölés. Az egyszerűség kedvéért $(a,b) \in \rho$ helyett gyakran azt írjuk, hogy $a\rho b$.

1.2. Definíció. ***Ekvivalenciarelációnak*** nevezzük a $\rho \subseteq A \times A$ relációt, ha rendelkezik az alábbi három tulajdonsággal:

(1) $\forall a \in A : a\rho a$ (reflexivitás);

(2) $\forall a,b \in A : a\rho b \implies b\rho a$ (szimmetria);

(3) $\forall a,b,c \in A : (a\rho b \text{ és } b\rho c) \implies a\rho c$ (tranzitivitás).

1.3. Definíció. Az A halmazon értelmezett legszűkebb ekvivalenciareláció az $\omega_A := \{(a,a) : a \in A\}$ ***egyenlőség reláció***, a legbővebb ekvivalenciareláció pedig az $A \times A$ ***teljes reláció***.

1.4. Állítás. *Tetszőleges $f\colon A \to B$ leképezés esetén a*

$$\ker f := \{(a_1,a_2) : a_1 f = a_2 f\} \subseteq A \times A$$

reláció ekvivalenciareláció az A halmazon, amelynek neve az f leképezés **magja**.

1.5. Definíció. Legyen $\rho \subseteq A \times A$ egy ekvivalenciareláció és a tetszőleges eleme A-nak. Ekkor az

$$\overline{a} := \{b \in A : a\rho b\}$$

halmazt az a elem ρ szerinti ***(ekvivalencia)osztályának***, az ekvivalenciaosztályok halmazát pedig az A halmaz ρ szerinti ***faktorhalmazának*** nevezzük.

Jelölés. Az a elem ρ szerinti osztályát szokás a/ρ-val, $\overline{a}^{\rho}$-val vagy $[a]_{\rho}$-val jelölni, de mi inkább az egyszerűbb $\overline{a}$ jelölést használjuk. Ez ugyan nem utal ρ-ra, de általában kiderül a szövegkörnyezetből, hogy mi a szóban forgó ekvivalenciareláció. A faktorhalmazt A/ρ jelöli, tehát

$$A/\rho = \{\overline{a} : a \in A\}.$$

1.6. Definíció. Egy nemüres halmaz ***osztályozásán*** olyan páronként diszjunkt nemüres részhalmazainak halmazát értjük, amelyek együtt lefedik az alaphalmazt. Formálisan: $\mathcal{C} \subseteq \mathcal{P}(A)$ osztályozás a nemüres A halmazon, ha

(1) $\forall B \in \mathcal{C} : B \neq \emptyset$;

(2) $\forall B_1 \neq B_2 \in \mathcal{C} : B_1 \cap B_2 = \emptyset$;

(3) $\bigcup_{B \in \mathcal{C}} B = A$.

1.7. Tétel. *Legyen A egy nemüres halmaz.*

- *Ha $\rho \subseteq A \times A$ ekvivalenciareláció, akkor A/ρ osztályozás az A halmazon.*
- *Ha pedig $\mathcal{C} \subseteq \mathcal{P}(A)$ osztályozás, akkor az*

$$a\rho b \iff \exists B \in \mathcal{C} : a,b \in B$$

formulával definiált ρ reláció ekvivalenciareláció az A halmazon.

*A most megadott „*ekvivalenciareláció $\mapsto$ osztályozás*” és „*osztályozás $\mapsto$ ekvivalenciareláció*” megfeleltetések egymás inverzei.*

[†]A természetes számok halmazát $\mathbb{N}$, a nemnegatív egész számok halmazát $\mathbb{N}_0$ jelöli, azaz $\mathbb{N} = \{1,2,3,\ldots\}$ és $\mathbb{N}_0 = \{0,1,2,\ldots\}$.

Részbenrendezések

1.8. Definíció. ***Részbenrendezési relációnak*** nevezzük a $\rho \subseteq A \times A$ relációt, ha rendelkezik az alábbi három tulajdonsággal:

(1) $\forall a \in A : a \rho a$ (reflexivitás);

(2) $\forall a, b \in A : (a \rho b \text{ és } b \rho a) \implies a = b$ (antiszimmetria);

(3) $\forall a, b, c \in A : (a \rho b \text{ és } b \rho c) \implies a \rho c$ (tranzitivitás).

Ha még a következő tulajdonság is teljesül, akkor ρ-t ***teljes rendezésnek*** (vagy lineáris rendezésnek) nevezzük:

(4) $\forall a, b \in A : a \rho b$ vagy $b \rho a$ (dichotómia).

Jelölés. A részbenrendezéseket szokás a $\leq$ szimbólummal jelölni, még akkor is, ha az alaphalmaz elemei esetleg nem is számok. Ha $a \leq b$ de $a \neq b$, akkor azt írjuk, hogy $a < b$.

1.9. Definíció. ***Részbenrendezett halmazon*** egy $(A; \leq)$ párt értünk, ahol A egy nemüres halmaz, és $\leq$ részbenrendezés A-n.

1.10. Definíció. Legyen $(A; \leq)$ egy részbenrendezett halmaz, és legyen $a, b \in A$. Azt mondjuk, hogy b ***fedi*** a-t, ha $a < b$, de nem létezik olyan $c \in A$, amelyre $a < c < b$. Ezt a tényt $a \prec b$ jelöli, és a $\prec$ relációt az adott részbenrendezéshez tartozó ***fedési relációnak*** hívjuk.

1.11. Tétel. *Véges részbenrendezett halmazt egyértelműen meghatározza a fedési relációja.*

1.12. Definíció. Legyen $(A; \leq)$ egy részbenrendezett halmaz. Az $a \in A$ elemet ***minimális elemnek*** nevezzük, ha nincs nála kisebb elem, és ***legkisebb elemnek*** nevezzük, ha ő mindenki másnál kisebb. Hasonlóan $a \in A$ ***maximális***, ha nincs nála nagyobb elem, és $a \in A$ ***legnagyobb***, ha ő mindenki másnál nagyobb. Formálisan:

- a minimális $\iff \nexists b \in A : b < a$;
- a legkisebb $\iff \forall b \in A : a \leq b$;
- a maximális $\iff \nexists b \in A : b > a$;
- a legnagyobb $\iff \forall b \in A : a \geq b$.

1.13. Tétel. *Részbenrendezett halmazban legföljebb egy legkisebb elem létezhet. Ha van legkisebb elem, akkor az minimális elem is, sőt ő az egyetlen minimális elem. Hasonló érvényes a legnagyobb elemre is.*

2. Számelméleti kongruenciák

Diofantoszi egyenletek

2.1. Definíció. A d egész számot az a és b egész számok ***legnagyobb közös osztójának*** nevezzük, ha kielégíti a következő két feltételt:

(1) $d \mid a$ és $d \mid b$;

(2) $\forall k \in \mathbb{Z} : (k \mid a \text{ és } k \mid b) \implies k \mid d$.

Hasonlóan definiálható egész számok ***legkisebb közös többszöröse*** is.

Jelölés. Az a és b számok legnagyobb közös osztóját $\operatorname{lnko}(a, b)$ vagy (a, b), legkisebb közös többszörösüket pedig $\operatorname{lkkt}(a, b)$ vagy $[a, b]$ jelöli.

2.2. Megjegyzés. A legnagyobb közös osztó nem egyértelmű: ha d legnagyobb közös osztója a-nak és b-nek, akkor $-d$ is az (de e két számon kívül nincs más legnagyobb közös osztó). Általában a két érték közül a nemnegatívat szoktuk tekinteni.

2.3. Tétel (euklideszi algoritmus). *Bármely két természetes számnak van legnagyobb közös osztója, és az az euklideszi algoritmussal megkapható. Az $a = r_0, b = r_1$ természetes számokon végrehajtott* **euklideszi algoritmus** *maradékos osztások ismételt elvégzését jelenti:*

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 \quad && (0 \leq r_2 < r_1)\,; \\
r_1 &= q_2 r_2 + r_3 \quad && (0 \leq r_3 < r_2)\,; \\
r_2 &= q_3 r_3 + r_4 \quad && (0 \leq r_4 < r_3)\,; \\
&\vdots \\
r_{i-1} &= q_i r_i + r_{i+1} \quad && (0 \leq r_{i+1} < r_i)\,; \\
&\vdots
\end{aligned}$$

Az eljárás véges számú lépés után véget ér: létezik olyan $n \in \mathbb{N}$, hogy $r_{n+1} = 0$. A legnagyobb közös osztó az utolsó nemnulla maradék, azaz $\operatorname{lnko}(a,b) = r_n$. *A legnagyobb közös osztó kifejezhető a két szám „lineáris kombinációjaként": léteznek olyan x, y egész számok, melyekre* $ax + by = \operatorname{lnko}(a,b)$.

2.4. Definíció. Azt mondjuk, hogy az a, b egész számok ***relatív prímek***, ha $\operatorname{lnko}(a,b) = 1$. Jelölés: $a \perp b$.

2.5. Tétel. *Tetszőleges $a, b, c \in \mathbb{Z}$ esetén ha $a \perp b$, akkor $a \mid bc \iff a \mid c$.*

2.6. Tétel (Euklidesz lemmája). *Tetszőleges a, b, c egész számok esetén ha $\operatorname{lnko}(a,b) \neq 0$, akkor*

$$a \mid bc \iff \frac{a}{\operatorname{lnko}(a,b)} \mid c.$$

2.7. Tétel. *Tetszőleges adott a, b, c (nemnulla) egész számok esetén az $ax + by = c$* **kétismeretlenes lineáris diofantoszi egyenlet** *akkor és csak akkor oldható meg, ha $\operatorname{lnko}(a,b) \mid c$. Ha (x_0, y_0) egy megoldás, akkor bármely $t \in \mathbb{Z}$ esetén az alábbi (x_t, y_t) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t szám alkalmas megválasztásával:*

$$x_t = x_0 + \frac{b}{\operatorname{lnko}(a,b)} \cdot t; \qquad y_t = y_0 - \frac{a}{\operatorname{lnko}(a,b)} \cdot t.$$

Kongruenciareláció, maradékosztályok

2.8. Definíció. Legyen $m \geq 2, a, b \in \mathbb{Z}$. Ha $a - b$ osztható m-mel, akkor azt mondjuk, hogy a ***kongruens*** b***-vel modulo*** m. Az m számot a kongruencia ***modulusának*** nevezzük.

Jelölés. A kongruenciát $\equiv$ jelöli, a modulust utána zárójelben tüntetjük fel a mod rövidítést használva (de ezt időnként elhagyjuk). Tehát $a \equiv b \pmod m \iff m \mid a - b$.

2.9. Tétel. *Tetszőleges $m \geq 2, a, b \in \mathbb{Z}$ esetén $a \equiv b \pmod m$ akkor és csak akkor teljesül, ha a és b ugyanazt a maradékot adja m-mel osztva.*

2.10. Tétel. *Tetszőleges $m, m_1, m_2 \geq 2, a, b, c, a_1, b_1, a_2, b_2 \in \mathbb{Z}$ esetén érvényesek az alábbiak:*

(1) $a \equiv a \pmod m$ *(reflexivitás);*

(2) $a \equiv b \pmod m \implies b \equiv a \pmod m$ *(szimmetria);*

(3) $(a \equiv b \pmod m$ *és* $b \equiv c \pmod m) \implies a \equiv c \pmod m$ *(tranzitivitás);*

(4) $\left.\begin{matrix} a_1 \equiv b_1 \pmod m \\ a_2 \equiv b_2 \pmod m \end{matrix}\right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2,\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m$;

(5) *ha* $c \neq 0$, *akkor* $ca \equiv cb \pmod m \iff a \equiv b \left(\mod \frac{m}{\operatorname{lnko}(m,c)}\right)$;

(6) *ha* $m \perp c$, *akkor* $ca \equiv cb \pmod m \iff a \equiv b \pmod m$;

(7) $\left.\begin{matrix} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{matrix}\right\} \iff a \equiv b \pmod{[m_1, m_2]}$;

(8) *ha* $a \equiv b \pmod m$, *akkor* $\operatorname{lnko}(a,m) = \operatorname{lnko}(b,m)$.

2.11. Definíció. Egy a egész szám modulo m ***maradékosztályán*** az $\overline{a} = \{b \in \mathbb{Z} \colon a \equiv b \pmod m\}$ halmazt értjük.

Jelölés. A modulo m maradékosztályok halmazát $\mathbb{Z}_m$ jelöli. Tehát $\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}$.

2.12. Definíció. A modulo m maradékosztályok halmazán értelmezzük az első három alapműveletet a következőképpen: tetszőleges $a, b \in \mathbb{Z}$ esetén legyen $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a} - \overline{b} = \overline{a-b}$, $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

2.13. Tétel. *A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (különbsége, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik számot választjuk reprezentánsnak. Ezekkel a műveletekkel $\mathbb{Z}_m$ kommutatív egységelemes gyűrűt alkot (modulo m* **maradékosztály-gyűrű**).

2.14. Megjegyzés. A 2.10. Tételbeli utolsó állítás szerint van értelme egy $\bmod m$ maradékosztály és az m modulus legnagyobb közös osztójáról beszélni (hiszen nem függ a reprezentáns választásától). Később fontos szerepet játszanak majd azok a maradékosztályok, amelyek relatív prímek a modulushoz, ezért erre külön elnevezést és jelölést vezetünk be.

2.15. Definíció. Az $\overline{a} \in \mathbb{Z}_m$ maradékosztályt ***redukált maradékosztálynak*** hívjuk, ha $\operatorname{lnko}(a,m) = 1$.

Jelölés. A $\bmod m$ redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli. Tehát $\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m : a \perp m\}$.

Lineáris kongruenciák és multiplikatív inverzek

2.16. Definíció. ***Lineáris kongruenciának*** nevezzük az $ax \equiv b \pmod{m}$ alakú „egyenletet”, ahol a, b, m adott egész számok, és az x ismeretlent is az egész számok körében keressük.

2.17. Tétel. *Az $ax \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg, ha $\operatorname{lnko}(a,m) \mid b$. Ha ez teljesül, akkor a megoldások egyetlen modulo $\frac{m}{\operatorname{lnko}(a,m)}$ maradékosztályt alkotnak. Az eredeti m modulusra vonatkozóan pedig $\operatorname{lnko}(a,m)$ különböző megoldás van. Ha x_0 egy megoldás, akkor az általános megoldás:*

$$x \equiv x_0 + t \cdot \frac{m}{\operatorname{lnko}(a,m)} \pmod{m} \quad (t = 0, 1, \ldots, \operatorname{lnko}(a,m) - 1).$$

2.18. Definíció. Azt mondjuk, hogy az a, b egész számok egymás ***multiplikatív inverzei modulo*** m, ha $ab \equiv 1 \pmod{m}$. Hasonlóan $\overline{a}, \overline{b} \in \mathbb{Z}_m$ egymás multiplikatív inverzei, ha $\overline{a} \cdot \overline{b} = \overline{1}$.

Jelölés. Ha nem fenyeget a félreértés veszélye, akkor az a egész szám $\bmod m$ multiplikatív inverzét a^{-1}-gyel jelöljük. Hasonlóan $\overline{a} \in \mathbb{Z}_m$ multiplikatív inverzét $\overline{a}^{-1}$ jelöli.

2.19. Tétel. *Az a egész számnak akkor és csak akkor van multiplikatív inverze modulo m, ha $a \perp m$. Ilyenkor a multiplikatív inverz $\bmod m$ egyértelműen meghatározott. Hasonlóan, $\overline{a} \in \mathbb{Z}_m$ akkor és csak akkor rendelkezik multiplikatív inverzzel, ha $\overline{a} \in \mathbb{Z}_m^*$. Ilyenkor a multiplikatív inverz egyértelműen meghatározott.*

2.20. Tétel (Wilson tétele). *Ha p prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.*

2.21. Következmény. *A $\mathbb{Z}_m$ maradékosztály-gyűrű akkor és csak akkor test, ha m prímszám.*

2.22. Definíció. Ha a és m relatív prímek, akkor tetszőleges $k \in \mathbb{N}$ esetén értelmezzük az a^{-k} negatív kitevőjű hatványt modulo m: legyen $a^{-k} \equiv \left(a^k\right)^{-1} \pmod{m}$. Hasonlóképpen $\overline{a} \in \mathbb{Z}_m^*$ esetén legyen $(\overline{a})^{-k} = \left(\overline{a}^k\right)^{-1}$.

2.23. Megjegyzés. Meg lehet mutatni, hogy a hatványozás szokásos azonosságai érvényben maradnak az egész kitevős modulo m hatványozás fenti értelmezése mellett.

Kongruenciarendszerek

2.24. Definíció. Adott a_i, b_i, n_i $(i = 1, 2, \ldots, k)$ egész számok esetén az alábbi „egyenletrendszert” ***lineáris kongruenciarendszernek*** nevezzük (az x ismeretlent is természetesen az egész számok körében keressük):

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ &\vdots \\ a_k x &\equiv b_k \pmod{n_k} \end{aligned}\right\}$$

2.25. Megjegyzés. A 2.17. Tétel segítségével a kongruenciarendszerbeli kongruenciákat külön-külön megoldhatjuk (ha van megoldásuk), és így a kongruenciarendszert a következő alakra hozhatjuk:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}\right\} \qquad (*)$$

2.26. Tétel. *A $(*)$ lineáris kongruenciarendszer $k = 2$ esetén pontosan akkor oldható meg, ha $\operatorname{lnko}(m_1, m_2) \mid c_1 - c_2$.*

2.27. Tétel. *A $(*)$ lineáris kongruenciarendszer akkor és csak akkor oldható meg, ha bármely két kongruenciából álló részrendszere megoldható, azaz $\forall i, j:\ \operatorname{lnko}(m_i, m_j) \mid c_i - c_j$. Speciálisan, páronként relatív prím modulusok esetén mindig van megoldás.*

2.28. Tétel. *Ha a $(*)$ lineáris kongruenciarendszernek van megoldása, akkor megoldásai egyetlen $\bmod [m_1, m_2, \ldots, m_k]$ maradékosztályt alkotnak.*

2.29. Tétel (kínai maradéktétel). *Tegyük fel, hogy az $m_1, m_2, \ldots, m_k$ modulusok páronként relatív prímek, jelölje a szorzatukat M, továbbá legyen $M_i = \frac{M}{m_i}$ $(i = 1, 2, \ldots, k)$. Jelölje y_i az $M_i y_i \equiv 1 \pmod{m_i}$ segédkongruencia egy megoldását $(i = 1, \ldots, k)$, és legyen $x_i = M_i y_i$. Ekkor a $(*)$ lineáris kongruenciarendszer megoldása:*

$$x \equiv \sum_{i=1}^{k} c_i x_i \pmod{M}.$$

2.30. Következmény. *Ha $m \perp n$, akkor az alábbi β leképezés bijektív:*

$$\beta \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ \overline{x} \mapsto (x \bmod m,\ x \bmod n).$$

3. Polinomok

Diofantoszi egyenletek

Test fölötti polinomokra éppúgy elvégezhető a maradékos osztás és az arra épülő euklideszi algoritmus, mint egész számokra. Ennek segítségével lehet például „diofantoszi" egyenletet is megoldani $T[x]$-ben. A következő tétel a 2.7. Tétel polinomos megfelelője; bizonyítása szinte szó szerint ugyanaz (HF végiggondolni!).

3.1. Tétel. *Legyen T egy test és $f, g, h \in T[x]$ (nemnulla) polinomok. Ekkor az $fu + gv = h$ kétismeretlenes lineáris „diofantoszi" egyenlet akkor és csak akkor oldható meg az ismeretlen $u, v \in T[x]$ polinomokra nézve, ha $\operatorname{lnko}(f,g) \mid h$. Ha (u_0, v_0) egy megoldás, akkor bármely $t \in T[x]$ esetén az alábbi (u_t, v_t) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a $t \in T[x]$ polinom alkalmas megválasztásával:*

$$u_t = u_0 + \frac{g}{\operatorname{lnko}(f,g)} \cdot t; \qquad v_t = v_0 - \frac{f}{\operatorname{lnko}(f,g)} \cdot t.$$

A modulo m kongruencia és a modulo m maradékosztályok szintén ugyanúgy definiálhatóak polinomokra, mint az egész számok körében, és hasonló tulajdonságokkal rendelkeznek (HF végiggondolni!). A modulo m maradékosztály-gyűrűt itt $\mathbb{Z}_m$ helyett $T[x]/(m)$ jelöli ($m \in T[x]$).

3.2. Tétel. *Ha m egy n-edfokú polinom a T test felett, akkor a $T[x]/(m)$ maradék- osztály-gyűrű kommutatív egységelemes gyűrű, melyenek elemei egyértelműen felírhatók az alábbi alakban:*

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \qquad (a_{n-1}, \ldots, a_1, a_0 \in T).$$

3.3. Tétel. *Az $\overline{f} \in T[x]/(m)$ maradékosztálynak akkor és csak akkor van multiplikatív inverze, ha f és m relatív prímek.*

3.4. Következmény. *A $T[x]/(m)$ maradékosztály-gyűrű akkor és csak akkor test, ha m irreducibilis T felett.*

Irreducibilis polinomok a racionális számtest felett

3.5. Tétel (Rolle(?) tétele). *Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és $p \perp q$), akkor*

$$f\left(\tfrac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

3.6. Állítás. *Legyen T egy test és $p \in T[x]$. A p polinom akkor és csak akkor irreducibilis T felett, ha legalább elsőfokú, és nem bontható $\deg p$-nél kisebb fokszámú polinomok szorzatára:*

$$\nexists f, g \in T[x] : \; p = f \cdot g \quad \text{és} \quad 1 \leq \deg f, \deg g < \deg p.$$

3.7. Megjegyzés. Gyűrűk felett ez általában nem igaz! Például a $p = 2x \in \mathbb{Z}[x]$ polinom nem irreducibilis $\mathbb{Z}$ felett, mert a $p = 2 \cdot x$ felbontás itt nem triviális (miért?).

3.8. Állítás. *Tetszőleges T test esetén...*

- *ha $f \in T[x]$ elsőfokú polinom, akkor f irreducibilis T felett;*
- *ha $f \in T[x]$ irreducibilis és $\deg f \geq 2$, akkor f-nek nincs gyöke T-ben;*
- *ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke T-ben.*

3.9. Tétel. *Test feletti polinomgyűrűben minden legalább elsőfokú polinom felbomlik irreducibilis polinomok szorzatára, és ez a felbontás lényegében (azaz a tényezők sorrendjétől és asszociáltságtól eltekintve) egyértelmű.*

3.10. Tétel. *Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:*

(1) $\exists g, h \in \mathbb{Z}[x] : f = gh$ *és* $0 < \deg g, \deg h < n$;
(2) $\exists g, h \in \mathbb{Q}[x] : f = gh$ *és* $0 < \deg g, \deg h < n$.

3.11. Megjegyzés. A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett. Az első viszont *nem* ekvivalens azzal, hogy f reducibilis $\mathbb{Z}$ felett (miért?). Tehát a fenti tételt *nem* fogalmazhatjuk meg egyszerűen úgy, hogy egy egész együtthatós polinom akkor és csak akkor (ir)reducibilis $\mathbb{Z}$ felett, ha (ir)reducibilis $\mathbb{Q}$ felett.

3.12. Definíció. Azt mondjuk, hogy a p prímszám ***pontos osztója*** az a egész számnak, ha a osztható p-vel, de p^2-tel már nem.

Jelölés. A pontos oszthatóságot $\parallel$ jelöli: $p \parallel a \iff p \mid a$ és $p^2 \nmid a$.

3.13. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). *Legyen* $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Ha létezik olyan* p *prímszám amelyre*

$$p \nmid a_n,\ p \mid a_{n-1}, \ldots,\ p \mid a_1,\ p \parallel a_0,$$

akkor f *irreducibilis a racionális számok teste felett.*

3.14. Következmény. *Minden* $n \geq 1$ *egész számra létezik* $\mathbb{Q}$ *felett irreducibilis* n*-edfokú polinom.*

3.15. Megjegyzés. A Schönemann–Eisenstein-tétel megfordítása nem igaz. Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, *nem következik*, hogy a polinom nem irreducibilis (keressünk ellenpéldát!). A megfordítás helyett következzék inkább a tétel „tükörképe".

3.16. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). *Legyen* $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Ha létezik olyan* p *prímszám amelyre* $p \parallel a_n, p \mid a_{n-1}, \ldots, p \mid a_1, p \nmid a_0$, *akkor* f *irreducibilis a racionális számok teste felett.*

Elemi törtekre bontás

3.17. Definíció. A T test feletti ***racionális törtön*** $\dfrac{f}{g}$ alakú formális kifejezést értünk, ahol $f, g \in T[x]$ és $g \neq 0$. Minden racionális törthöz tartozik egy ***racionális törtfüggvény*** (a két fogalom nem összekeverendő!). A T feletti racionális törtek halmazát $T(x)$ jelöli.

3.18. Definíció. A T test felett ***elemi törtnek*** (vagy parciális törtnek) olyan racionális törtet nevezünk, amelyben a nevező T felett irreducibilis (fő)polinom hatványa, és a számláló foka kisebb ezen irreducibilis polinom fokánál:

$$\frac{f}{p^k} \in T(x), \quad \text{ahol } f, p \in T[x],\ k \in \mathbb{N},\ p \text{ irreducibilis } T \text{ felett},\ \deg f < \deg p.$$

3.19. Tétel. *Tetszőleges* T *test felett minden racionális tört felírható egy polinom és elemi törtek összegeként.*

3.20. Következmény. *A komplex számok teste felett minden racionális tört felírható egy polinom és véges sok*

$$\frac{A}{(x+a)^k} \quad (A, a \in \mathbb{C},\ k \in \mathbb{N})$$

alakú racionális tört összegeként.

3.21. Következmény. *A valós számok teste felett minden racionális tört felírható egy polinom és véges sok*

$$\frac{A}{(x+a)^k} \quad (A, a \in \mathbb{R},\ k \in \mathbb{N}), \qquad \text{és} \qquad \frac{Bx+C}{(x^2+bx+c)^k} \quad (B, C, b, c \in \mathbb{R},\ b^2 - 4c < 0,\ k \in \mathbb{N})$$

alakú racionális tört összegeként.

Szimmetrikus polinomok

3.22. Tétel. *Legyenek az* n*-edfokú* $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ *főpolinom komplex gyökei* $\alpha_1, \ldots, \alpha_n$ *(mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:*

$$\begin{aligned}
-a_{n-1} &= \alpha_1 + \alpha_2 + \cdots + \alpha_n;\\
a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n;\\
-a_{n-3} &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n;\\
&\vdots\\
(-1)^{n-1} a_1 &= \alpha_1\alpha_2\cdots\alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2\cdots\alpha_{n-2}\alpha_n + \cdots + \alpha_2\alpha_3\cdots\alpha_{n-1}\alpha_n;\\
(-1)^n a_0 &= \alpha_1\alpha_2\alpha_3\cdots\alpha_{n-1}\alpha_n.
\end{aligned}$$

3.23. Megjegyzés. A fenti képleteket ***Viète-formuláknak*** hívjuk. A k-adik sor bal oldalán $(-1)^k a_{n-k}$ áll, a jobb oldalon pedig az $\alpha_1, \ldots, \alpha_n$ betűkből képezett összes k-tényezős szorzat összege, tehát egy $\binom{n}{k}$-tagú összeg. Formálisan:

$$(-1)^k a_{n-k} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \alpha_{i_1} \cdot \alpha_{i_2} \cdot \ldots \cdot \alpha_{i_k}.$$

3.24. Definíció. Az $f \in \mathbb{C}[x]$ főpolinom ***diszkriminánsa***:

$$\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2,$$

3.25. Definíció. Adott T test feletti ***n-határozatlanú monomnak*** nevezzük az $ax_1^{k_1}\cdot\ldots\cdot x_n^{k_n}$ alakú formális kifejezéseket, ahol $0\neq a\in T$ és $k_1,\ldots,k_n\in\mathbb{N}_0$. Az ilyen monomok véges összegeit pedig T feletti ***n-határozatlanú polinomoknak*** oknak nevezzük.

Jelölés. A T feletti n-határozatlanú polinomok halmazát $T[x_1,\ldots,x_n]$ jelöli.

3.26. Tétel. *A természetes módon definiált szorzással és összeadással $T[x_1,\ldots,x_n]$ integritástartomány.*

3.27. Megjegyzés. Az n-határozatlanú polinomok gyűrűjét lehetne rekurzívan is definiálni: legyen

$$T[x_1,\ldots,x_n]=(T[x_1,\ldots,x_{n-1}])[x_n],$$

azaz a $T[x_1,\ldots,x_{n-1}]$ integritástartomány feletti (egyhatározatlanú) polinomgyűrű.

3.28. Definíció. Az $f\in T[x_1,\ldots,x_n]$ polinomot ***szimmetrikus polinomnak*** nevezzük, ha invariáns a határozatlanok minden permutációjára, azaz

$$\forall\pi\in S_n: f(x_{1\pi},\ldots,x_{n\pi})=f(x_1,\ldots,x_n).$$

3.29. Definíció. A k-adik n-határozatlanú ***elemi szimmetrikus polinom*** az $x_1,\ldots,x_n$ határozatlanokból képezett összes k-tényezős szorzatok összege ($k=1,\ldots,n$).

Jelölés. A k-adik n-határozatlanú elemi szimmetrikus polinomot σ_k jelöli (az alaptest és n értéke általában világos a szövegkörnyezetből), tehát

$$\sigma_k=\sum_{1\leq i_1<i_2<\cdots<i_k\leq n}x_{i_1}\cdot x_{i_2}\cdot\ldots\cdot x_{i_k}\in T[x_1,\ldots,x_n].$$

3.30. Megjegyzés. Az elemi szimmetrikus polinomokkal már találkoztunk: segítségükkel fejezhetők ki egy komplex együtthatós főpolinom együtthatói a polinom gyökeiből. Tehát a Viète-formulák $\sigma_k(\alpha_1,\ldots,\alpha_n)=(-1)^k a_{n-k}$ alakban is felírhatók.

3.31. Tétel. *A szimmetrikus polinomok részgyűrűt alkotnak a $T[x_1,\ldots,x_n]$ polinomgyűrűben.*

3.32. Tétel (a szimmetrikus polinomok alaptétele). *Bármely szimmetrikus polinom felírható, mégpedig egyetlen módon, az elemi szimmetrikus polinomok polinomjaként. Formálisan:*

$$\forall f\in T[x_1,\ldots,x_n]: f\ \textit{szimmetrikus}\implies\exists!h\in T[x_1,\ldots,x_n]: f=h(\sigma_1,\ldots,\sigma_n).$$

4. Számelméleti függvények

Osztók száma, osztók összege

4.1. Definíció. ***Számelméleti függvényen*** olyan leképezést értünk, amely a természetes számok halmazán van értelmezve, értékei pedig valós (vagy komplex) számok.

4.2. Definíció. Néhány nevezetes számelméleti függvény:

- $\tau(n)=\sum_{d\mid n}1$ (n pozitív osztóinak száma);
- $\sigma(n)=\sum_{d\mid n}d$ (n pozitív osztóinak összege);
- $\mathrm{id}(n)=n$;
- $\mathbf{1}(n)=1$;
- $\delta(n)=\begin{cases}1, & \text{ha } n=1;\\ 0, & \text{ha } n>1.\end{cases}$

4.3. Definíció. Azt mondjuk, hogy az f számelméleti függvény ***gyengén multiplikatív***, ha $f(1)=1$ és minden $a,b\in\mathbb{N}$ esetén $a\perp b\implies f(ab)=f(a)\cdot f(b)$.

4.4. Tétel. *Egy f számelméleti függvény akkor és csak akkor gyengén multiplikatív, ha $f(1)=1$ és tetszőleges páronként különböző $p_1,\ldots,p_k$ prímszámok és tetszőleges $\alpha_1,\ldots,\alpha_k$ pozitív kitevők esetén*

$$f(p_1^{\alpha_1}\cdot\ldots\cdot p_n^{\alpha_n})=f(p_1^{\alpha_1})\cdot\ldots\cdot f(p_n^{\alpha_n}).$$

4.5. Tétel. *A $\tau,\sigma,\mathrm{id},\mathbf{1},\delta$ számelméleti függvények gyengén multiplikatívak.*

4.6. Tétel. *Legyen az n természetes szám prímtényezős felbontása $n=\prod_{i=1}^{k} p_i^{\alpha_i}$. Ekkor*

$$\tau(n)=\prod_{i=1}^{k}(\alpha_i+1); \qquad \sigma(n)=\prod_{i=1}^{k}\left(1+p_i+p_i^2+\cdots+p_i^{\alpha_i}\right)=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}.$$

4.7. Definíció. Az n természetes számot ***tökéletes számnak*** nevezzük, ha megegyezik pozitív valódi osztóinak összegével, azaz $\sigma(n)=2n$.

4.8. Tétel (Euler tétele). *Az n páros szám akkor és csak akkor tökéletes, ha előáll $n=2^{p-1}(2^p-1)$ alakban, ahol 2^p-1 prímszám (ekkor p is szükségképpen prím).*

4.9. Definíció. Az $M_n=2^n-1$ alakú számokat ***Mersenne-számoknak***, az ilyen alakú prímeket ***Mersenne-prímeknek*** nevezzük.

4.10. Megjegyzés. Abból, hogy n prím, még nem következik, hogy M_n is az, például M_{11} összetett szám. Nem ismert, hogy létezik-e végtelen sok Mersenne-prím, tehát azt sem tudjuk, hogy létezik-e végtelen sok páros tökéletes szám. Páratlan tökéletes számot egyet sem ismerünk, de nincs bizonyítva az sem, hogy ilyen nem létezik. A jelenleg (2017. szeptember 7.) ismert legnagyobb prímszám is Mersenne-prím: $M_{74\,207\,281}$, ami tízes számrendszerben 22 338 618 számjegyből áll.

4.11. Definíció. Az $F_n=2^{2^n}+1$ alakú számokat ***Fermat-számoknak***, az ilyen alakú prímeket ***Fermat-prímeknek*** nevezzük.

4.12. Megjegyzés. Fermat azt sejtette, hogy F_n mindig prím. Az első öt Fermat-szám valóban prím:

$$F_0=3,\ F_1=5,\ F_2=17,\ F_3=257,\ F_4=65537,$$

de Euler észrevette, hogy $F_5=641\cdot 6\,700\,417$. Minden további Fermat-szám, amit sikerült megvizsgálni (részben számítógéppel), összetettnek bizonyult. Az általánosan elfogadott sejtés az, hogy csak véges sok Fermat-prím van (valószínűleg csak a fenti öt).

Az Euler-féle φ-függvény

4.13. Definíció. Jelöljük $\varphi(m)$-mel az m-nél nem nagyobb természetes számok közül azoknak a számát, amelyek m-hez relatív prímek:

$$\varphi(m)=|\{a: 1\le a\le m \text{ és } a\perp m\}|.$$

Az így kapott függvényt ***Euler-féle φ függvénynek*** nevezzük. Tömörebben: $\varphi\colon \mathbb{N}\to\mathbb{N}$, $m\mapsto|\mathbb{Z}_m^*|$.

4.14. Állítás. *Minden n természetes szám esetén, a primitív n-edik egységgyökök száma $\varphi(n)$.*

4.15. Definíció. Modulo m ***teljes maradékrendszernek*** nevezzük egész számok egy olyan rendszerét, amely minden $\bmod m$ maradékosztályból pontosan egy elemet tartalmaz.

4.16. Állítás. *Ha a $c_1,c_2,\ldots,c_m$ egész számok teljes maradékrendszert alkotnak modulo m, és $a,b\in\mathbb{Z}, a\perp m$, akkor $ac_1+b, ac_2+b,\ldots,ac_m+b$ is teljes maradékrendszer modulo m.*

4.17. Definíció. Modulo m ***redukált maradékrendszernek*** nevezzük egész számok egy olyan rendszerét, amely minden $\bmod m$ redukált maradékosztályból pontosan egy elemet tartalmaz.

4.18. Állítás. *Ha a $c_1,c_2,\ldots,c_{\varphi(m)}$ egész számok redukált maradékrendszert alkotnak modulo m, és $a\in\mathbb{Z}, a\perp m$, akkor $ac_1,ac_2,\ldots,ac_{\varphi(m)}$ is redukált maradékrendszer modulo m.*

4.19. Tétel. *Az Euler-féle φ függvény gyengén multiplikatív.*

4.20. Tétel. *Legyen az n természetes szám prímtényezős felbontása $n=\prod_{i=1}^{k} p_i^{\alpha_i}$. Ekkor*

$$\varphi(n)=n\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=\prod_{i=1}^{k}\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)=\prod_{i=1}^{k}p_i^{\alpha_i-1}(p_i-1).$$

4.21. Tétel (Euler–Fermat-tétel). *Ha az a egész szám relatív prím az m modulushoz, akkor $a^{\varphi(m)}\equiv 1 \pmod m$.*

4.22. Következmény (kis Fermat-tétel). *Ha p prímszám és a nem osztható p-vel, akkor $a^{p-1}\equiv 1 \pmod p$. Más (ekvivalens) megfogalmazásban: Ha p prímszám, akkor minden a egész számra $a^p\equiv a \pmod p$.*

4.23. Következmény. *Ha $a\in\mathbb{Z}$ relatív prím az m modulushoz, akkor*

$$k_1\equiv k_2 \pmod{\varphi(m)} \implies a^{k_1}\equiv a^{k_2} \pmod m.$$

Összegzési és megfordítási függvény

4.24. Definíció. Az f és g számelméleti függvények ***konvolúcióján*** az alábbi képlettel definiált $f*g$ számelméleti függvényt értjük:

$$(f*g)(n)=\sum_{d|n} f(d)\cdot g\left(\frac{n}{d}\right)=\sum_{ab=n} f(a)\,g(b).$$

4.25. Tétel. *A konvolúció művelete kommutatív és asszociatív, továbbá minden f számelméleti függvényre $f*\delta=\delta*f=f$.*

4.26. Tétel. *Gyengén multiplikatív számelméleti függvények konvolúciója is gyengén multiplikatív.*

4.27. Definíció. Az f számelméleti függvény ***összegzési függvényén*** az $F(n)=\sum_{d|n} f(d)$ számelméleti függvényt értjük. Az f függvényt az F függvény ***megfordítási függvényének*** nevezzük.

Jelölés. Azt a tényt, hogy F az f összegzési függvénye gyakran egyszerűen csak $f\to F$ jelöli.

4.28. Tétel. *Gyengén multiplikatív számelméleti függvény összegzési függvénye is gyengén multiplikatív.*

4.29. Tétel. *A tanult nevezetes számelméleti függvények között fennállnak a következő összefüggések: $\delta\to\mathbf{1}\to\tau$ és $\varphi\to\mathrm{id}\to\sigma$.*

4.30. Definíció. Az n természetes számot ***négyzetmentesnek*** nevezzük, ha nem osztható egyetlen 1-nél nagyobb négyzetszámmal sem.

4.31. Megjegyzés. Könnyű meggondolni, hogy egy szám akkor és csak akkor négyzetmentes, ha prímfelbontásában minden prím csak egyszer (azaz első hatványon) fordul elő.

4.32. Definíció. ***Möbius-függvénynek*** nevezzük az alábbi képlettel definiált μ számelméleti függvényt:

$$\mu(n)=\begin{cases}0, & \text{ha } n \text{ nem négyzetmentes;}\\ (-1)^k, & \text{ha } n \text{ előáll } k \text{ különböző prím szorzataként.}\end{cases}$$

4.33. Tétel. *A Möbius-függvény összegzési függvénye a δ függvény, azaz $\mu*\mathbf{1}=\delta$.*

4.34. Tétel (Möbius-féle megfordítási képlet). *Tetszőleges F számelméleti függvény esetén F-nek egyetlen megfordítási függvénye van, mégpedig $F*\mu$. Másképpen fogalmazva $f\to F$ akkor és csak akkor áll fenn, ha $f=F*\mu$. Részletesebben: tetszőleges f,F számelméleti függvények esetén*

$$\forall n\in\mathbb{N}: F(n)=\sum_{d|n} f(d) \quad\Longleftrightarrow\quad \forall n\in\mathbb{N}: f(n)=\sum_{d|n} F(d)\cdot\mu\left(\frac{n}{d}\right).$$

4.35. Következmény. *Gyengén multiplikatív számelméleti függvény megfordítási függvénye is gyengén multiplikatív.*

5. Permutációk

Permutációk szorzása, ciklusfelbontás

5.1. Definíció. ***Permutációnak*** nevezzük egy nemüres (véges) halmaz önmagára való bijektív leképezését.

5.2. Definíció. Az $\{1,2,\dots,n\}$ halmaz összes permutációi csoportot alkotnak a leképezésszorzás műveletével. Ezt a csoportot ***n-edfokú szimmetrikus csoportnak*** nevezzük, és S_n-nel jelöljük.

5.3. Állítás. *Tetszőleges $\pi,\rho\in S_n$ permutációk esetén $(\pi\rho)^{-1}=\rho^{-1}\pi^{-1}$.*

5.4. Definíció. Legyen $\pi\in S_n$ és $a\in\{1,2,\dots,n\}$. Ha $a\pi=a$, akkor azt mondjuk, hogy a ***fixpontja*** π-nek. Ha $a\pi\neq a$, akkor azt mondjuk, hogy a ***mozgatott eleme*** π-nek.

5.5. Definíció. Két permutáció ***idegen***, ha mozgatott elemeik halmaza diszjunkt.

5.6. Tétel. *Ha $\pi,\rho\in S_n$ idegen permutációk, akkor fölcserélhetőek, azaz $\pi\rho=\rho\pi$.*

5.7. Definíció. Legyenek $a_1,\dots,a_k\in\{1,2,\dots,n\}$ különböző elemek, és legyen $\pi\in S_n$ az alábbi permutáció:

$$a_1\pi=a_2,\ a_2\pi=a_3,\dots,\ a_{k-1}\pi=a_k,\ a_k\pi=a_1 \qquad\text{és}\qquad b\pi=b \text{ ha } b\notin\{a_1,\dots,a_k\}.$$

Ezt a π permutációt így jelöljük: $\pi=(a_1\,a_2\,\cdots\,a_{k-1}\,a_k)$ és ***ciklikus permutációnak*** vagy röviden ***ciklusnak*** nevezzük.

5.8. Tétel. *Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelmű.*

Páros és páratlan permutációk

5.9. Definíció. A 2 hosszúságú ciklusokat, vagyis az $(i\,j)$ alakú permutációkat ***transzpozícióknak*** nevezzük.

5.10. Tétel. *Az S_n csoportot* generálják *a transzpozíciók, azaz minden S_n-beli permutáció előáll transzpozíciók szorzataként.*

5.11. Tétel. *Egy S_n-beli permutáció transzpozíciók szorzataként való felírásában a tényezők számának paritása egyértelműen meghatározott. Eszerint beszélhetünk* **páros permutációkról** *és* **páratlan permutációkról**.

5.12. Állítás. *A páros hosszúságú ciklusok páratlan permutációk, míg a páratlan hosszúságú ciklusok páros permutációk.*

5.13. Definíció. Az S_n-beli páros permutációk csoportot alkotnak (miért?). Ezt a csoportot ***n-edfokú alternáló csoportnak*** nevezzük, és A_n-nel jelöljük.

5.14. Tétel. *Az S_n-beli permutációk fele páros és fele páratlan.*

5.15. Következmény. $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$

6. Nevezetes számelméleti problémák

Számok felbontása hatványok összegére

6.1. Definíció. Az $(x, y, z) \in \mathbb{N}^3$ számhármast ***pitagoraszi számhármasnak*** nevezzük, ha $x^2 + y^2 = z^2$. Az (x, y, z) pitagoraszi számhármas ***primitív***, ha $\operatorname{lnko}(x, y, z) = 1$.

6.2. Megjegyzés. Tetszőleges (x, y, z) pitagoraszi számhármas esetén $(x/d, y/d, z/d)$ primitív pitagoraszi számhármas, ahol $d = \operatorname{lnko}(x, y, z)$. Tehát elegendő a primitív pitagoraszi számhármasokat meghatározni, mert ezekből minden pitagoraszi számhármas megkapható (egy konstanssal való szorzással).

6.3. Lemma. *Primitív pitagoraszi számhármasban a tagok páronként is relatív prímek.*

6.4. Lemma. *Ha (x, y, z) primitív pitagoraszi számhármas, akkor x és y paritása különböző, z pedig páratlan.*

6.5. Tétel. *Legyen (x, y, z) primitív pitagoraszi számhármas, és tegyük fel, hogy x páros. Ekkor léteznek olyan u, v természetes számok, melyekre*

$$u > v,\ u \not\equiv v \pmod 2,\ u \perp v, \text{ és } x = 2uv,\ y = u^2 - v^2,\ z = u^2 + v^2.$$

Fordítva, a fenti formulákkal definiált (x, y, z) számhármas mindig primitív pitagoraszi számhármas.

6.6. Tétel (Fermat). *Az $x^4 + y^4 = z^4$ egyenletnek nincs pozitív egészekből álló megoldása.*

6.7. Tétel (nagy Fermat-tétel, Wiles és Taylor). *Ha $n \geq 3$, akkor az $x^n + y^n = z^n$ egyenletnek nincs pozitív egészekből álló megoldása.*

6.8. Lemma. *Ha m és n előáll két négyzetszám összegeként, akkor mn is előáll.*

6.9. Lemma. *A $4k + 1$ alakú prímszámok előállnak két négyzetszám összegeként, a $4k + 3$ alakú prímek viszont nem.*

6.10. Tétel (Fermat-féle két négyzetszám tétel). *Pontosan azok a számok állnak elő két négyzetszám összegeként, amelyek prímfelbontásában a $4k + 3$ alakú prímek páros kitevővel szerepelnek.*

6.11. Tétel (Lagrange-féle négy négyzetszám tétel). *Minden természetes szám előáll négy négyzetszám összegeként.*

6.12. Megjegyzés. Lagrange tétele éles abban az értelemben, hogy három négyzetszám összegeként nem lehet minden természetes számot előállítani (keressünk ellenpéldát!). A természetes számok hatványösszegekként való előállításaival kapcsolatos problémákat összefoglaló néven Waring-problémakörnek szokás nevezni. Edward Waring XVIII. századi angol matematikus Meditationes Algebraicae című művében azt állította (bizonyítás nélkül), hogy minden szám előállítható kilenc köbszám összegeként, illetve tizenkilenc negyedik hatvány összegeként. Ezek az állítások helyesnek bizonyultak, de csak a huszadik században találtak rájuk bizonyítást.

Általában $g(k)$ jelöli azt a legkisebb számot, amelyre igaz az, hogy minden természetes szám előállítható $g(k)$ darab k-adik hatvány összegeként. Az előzőek alapján tehát $g(2) = 4, g(3) \leq 9, g(4) \leq 19$, és példák mutatják, hogy 8 köb, illetve 18 negyedik hatvány nem mindig elég, tehát $g(3) = 9$ és $g(4) = 19$. A $g(k)$ számok meghatározása igen nehéz probléma, még az sem világos, hogy egyáltalán léteznek minden k esetén;[§] ezt Hilbert igazolta 1909-ben. Van egy feltételezett képlet is a $g(k)$ számokra; bizonyított tény, hogy ez a képlet legfeljebb véges sok k-ra nem helyes, és általánosan elfogadott az a sejtés, hogy valójában minden k-ra érvényes:

$$g(k) = 2^k + \left[\frac{3^k}{2^k}\right] - 2.$$

[§]Mit jelentene az, hogy $g(k)$ nem létezik?

Prímszámok

6.13. Tétel. *Végtelen sok prímszám van.*

6.14. Tétel. *Végtelen sok $4k-1$ alakú prímszám van.*

6.15. Tétel. *Végtelen sok $4k+1$ alakú prímszám van.*

6.16. Tétel (Dirichlet tétele). *Ha egy nemkonstans számtani sorozat kezdőtagja és differenciája egymáshoz relatív prím, akkor a számtani sorozatban végtelen sok prímszám található.*

6.17. Tétel (Csebisev tétele). *Bármely szám és a kétszerese között van prímszám. Pontosabban: minden n természetes számhoz létezik olyan p prímszám, amelyre $n < p \leq 2n$.*

6.18. Tétel. *A szomszédos prímek között tetszőlegesen nagy hézagok találhatók. (Azaz minden $N \in \mathbb{N}$ esetén lehet találni N egymást követő összetett számot.)*

6.19. Definíció. ***Ikerprímnek*** nevezünk két prímszámot, ha különbségük 2.

6.20. Megjegyzés. Azt sejtik, hogy végtelen sok ikerprím van. Yitang Zhang 2013 áprilisában bebizonyította, hogy létezik olyan K korlát, amelyre végtelen sok olyan prímpár létezik, ahol a két tag különbsége legfeljebb K ($K = 70\,000\,000$ értékre, de ezt később levitték $K = 246$-ra).

6.21. Lemma. *A $\sum_{n=1}^{\infty} \frac{1}{n}$ harmonikus sor divergens, míg a $\sum_{n=1}^{\infty} \frac{1}{n^2}$ sor konvergens.*

6.22. Tétel. *A prímszámok reciprokaiból alkotott sor divergens, azaz*

$$\sum_{p} \frac{1}{p} = \infty.$$

6.23. Megjegyzés. Ez a tétel durván fogalmazva azt állítja, hogy „sok” prímszám van (négyzetszámból viszont a 6.21. Lemma szerint „kevés” van). Ismert tény, hogy „kevés” páratlan tökéletes szám, illetve „kevés” ikerprím van (ebből persze még nem derül ki, hogy végtelen sok van-e belőlük).

6.24. Megjegyzés. A harmonikus sor lassan divergál, a prímharmonikus sor még lassabban. Például $\sum_{p<10^{18}} \frac{1}{p} < 4$ (ez kb. a sor első huszonnégybilliárd tagja).

6.25. Tétel. *Az n-edik prímszám nem nagyobb, mint $2^{2^{n-1}}$.*

6.26. Definíció. A prímszámok eloszlásának pontosabb vizsgálatánál hasznos a $\pi(x)$ függvény, az úgynevezett ***prímszámláló függvény***, amely megadja az x pozitív valós számnál nem nagyobb prímek számát:

$$\pi(x) = \sum_{p \leq x} 1.$$

6.27. Tétel (prímszámtétel). *A $\pi(x)$ prímszámláló függvény aszimptotikusan ekvivalens az $\frac{x}{\log x}$ függvénnyel, azaz*

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

6.28. Következmény. *Az n-edik prímszám aszimptotikusan $n \log n$, azaz $\lim_{n\to\infty} \frac{p_n}{n \log n} = 1$.*

Algebrai és transzcendens számok

6.29. Definíció. Az α komplex számot ***algebrai számnak*** nevezzük, ha gyöke valamely nemzéró racionális együtthatós polinomnak. A nem algebrai számokat ***transzcendens számoknak*** nevezzük.

6.30. Definíció. Ha $f \in \mathbb{Q}[x]$ minimális fokszámú mindazon nemzéró racionális együtthatós főpolinomok között, melyeknek α gyöke, akkor f-et az α algebrai szám ***minimálpolinomjának*** nevezzük.

6.31. Tétel. *Algebrai szám minimálpolinomja mindig egyértelműen meghatározott, és irreducibilis a racionális számtest felett. Továbbá, ha $f \in \mathbb{Q}[x]$ olyan irreducibilis főpolinom melynek az α algebrai szám gyöke, akkor f megegyezik α minimálpolinomjával.*

6.32. Tétel. *Létezik transzcendens szám.*

6.33. Megjegyzés. A fenti tétel (egyik) bizonyítása azon múlik, hogy algebrai számokat nem lehet nagyon jól közelíteni racionális számokkal (lásd a 6.38. Tételt). Ez a *diofantoszi approximáció* témaköre: adott α valós számhoz szeretnénk olyan $\frac{p}{q}$ közelítő törtet találni ($p, q \in \mathbb{Z}, q > 0, p \perp q$), amelyre $\left|\alpha - \frac{p}{q}\right|$ kicsi, és q nem túl nagy.

6.34. Tétel (Dirichlet approximációs tétele). *Minden α valós szám és minden N természetes szám esetén van α-nak olyan $\frac{p}{q}$ közelítése, amelyre*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq} \quad \text{és} \quad q \leq N.$$

6.35. Következmény. *Ha α irracionális szám, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.*

6.36. Állítás. *Ha α racionális szám, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.*

6.37. Tétel (Hurwitz). *Ha α irracionális szám, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Ha $\alpha = \frac{1+\sqrt{5}}{2}$, akkor az állítás nem javítható: nem írhatunk a nevezőbe semmilyen $\sqrt{5}$-nél nagyobb számot.

6.38. Tétel (Liouville, Thue, Siegel, Roth). *Ha α irracionális algebrai szám és $\varepsilon > 0$, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}.$$

6.39. Tétel. *Az algebrai számok résztestet alkotnak a komplex számok testében.*

6.40. Tétel. *Ha α algebrai szám és $n \geq 2$, akkor $\sqrt[n]{\alpha}$ is algebrai szám (a gyöknek mind az n értékére).*

6.41. Definíció. Az α komplex számot ***gyökmennyiségnek*** nevezzük, ha megkapható racionális számokból kiindulva a négy alapművelet (összeadás, kivonás, szorzás, osztás) és egész kitevős gyökvonás véges számú alkalmazásával.

6.42. Következmény. *A gyökmennyiségek algebrai számok.*

6.43. Tétel. *Van olyan algebrai szám, ami nem gyökmennyiség.*

A fenti ártatlannak látszó tételből következik, hogy nem minden egyenlet oldható meg gyökjelek segítségével. Az ötödfokú egyenletnek már nincs általános megoldóképlete, sőt, például az $x^5 - 4x + 2 = 0$ egyenletnek még „ad hoc” megoldóképlete sincs, mert gyökei nem gyökmennyiségek.

6.44. Tétel. *Az algebrai számok teste algebrailag zárt, azaz ha $\alpha \in \mathbb{C}$ gyöke a legalább elsőfokú $f = a_n x^n + \cdots + a_1 x + a_0$ polinomnak, ahol $a_0, \ldots, a_n$ algebrai számok, akkor α maga is algebrai szám.*