BEVEZETÉS A SZÁMELMÉLETBE

vázlat az előadáshoz[†]

(2013 őszi félév)

Waldhauser Tamás

1. Oszthatóság, legnagyobb közös osztó, prímfaktorizáció az egész számok körében

Az oszthatósági reláció alapvető tulajdonságai

1.1. Definíció. Azt mondjuk, hogy az a egész szám ***osztója*** a b egész számnak (b ***többszöröse*** a-nak), ha létezik olyan c egész szám, amelyre $b = ac$.

Jelölés. Az oszthatósági relációt $\mid$ jelöli: $a \mid b \iff \exists c \in \mathbb{Z} : b = ac$.

1.2. Tétel. *Tetszőleges a, b, c egész számokra érvényesek az alábbiak:*

(1) $a \mid a$;
(2) $(a \mid b \text{ és } b \mid c) \implies a \mid c$;
(3) $(a \mid b \text{ és } b \mid a) \iff b = \pm a$;
(4) $1 \mid a$;
(5) $a \mid 0$;
(6) $a \mid 1 \iff a = \pm 1$;
(7) $0 \mid a \iff a = 0$;
(8) $(a \mid b \text{ és } a \mid c) \implies a \mid b \pm c$;
(9) $a \mid b \implies a \mid bc$;
(10) $a \mid b \iff ac \mid bc$, *ha* $c \neq 0$;
(11) $a \mid b \implies |a| \leq |b|$, *ha* $b \neq 0$.

Részbenrendezések

1.3. Definíció. Adott A halmazon értelmezett ***reláció***n 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 $a \rho b$.

1.4. Definíció. ***Részbenrendezési reláció***nak 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 rendezés***nek (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 $a < b$.

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

1.6. 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 reláció***nak hívjuk.

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

1.8. Definíció. Egy véges $(A; \leq)$ részbenrendezett halmaz ***Hasse-diagram***ján egy ábrát értünk, amelynél A elemeit (síkbeli) pontokkal ábrázoljuk oly módon, hogy $a < b$ esetén a b-nek megfelelő pont „följebb” van, mint az a-nak megfelelő pont, és e két pontot akkor és csak akkor kötjük össze, ha b fedi a-t.

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

1.9. Definíció. Legyen $(A;\leq)$ egy részbenrendezett halmaz. Az $a \in A$ elemet ***minimális elem***nek nevezzük, ha nincs nála kisebb elem, és ***legkisebb elem***nek 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 $\iff \forall b \in A$: $a \geq b$.

1.10. Megjegyzés. Az 1.2. Tételbeli (1)-(5) tulajdonságok szerint $(\mathbb{N}_0;|)$ részbenrendezett halmaz, amelynek a legkisebb eleme 1, a legnagyobb eleme pedig 0 (!).

1.11. 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.*

Legnagyobb közös osztó

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

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

A t egész szám ***legkisebb közös többszörös***e a-nak és b-nek, ha kielégíti a következő két feltételt:

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

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.

1.13. Megjegyzés. A legnagyobb közös osztó nem egyértelmű: az 1.2. Tétel (3) állítása szerint 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.

1.14. Megjegyzés. Jelölje D_a az a természetes szám pozitív osztóinak halmazát: $D_a = \{c \in \mathbb{N} : c \mid a\}$. Az 1.12. Definíció szerint $\operatorname{lnko}(a,b)$ nem más, mint a $(D_a \cap D_b;|)$ részbenrendezett halmaz legnagyobb eleme. Az oszthatósági reláció nem dichotóm, így nem világos, hogy létezik-e egyáltalán legnagyobb eleme ennek a részbenrendezett halmaznak. Természetesebbnek tűnhetne a legnagyobb közös osztót a $(D_a \cap D_b;\leq)$ részbenrendezett halmaz legnagyobb elemeként definiálni (erről legalább világos, hogy létezik).

Tegyük fel, hogy $d = \operatorname{lnko}(a,b)$ az 1.12. Definíció értelmében. Ha $k \in D_a \cap D_b$, akkor $k \mid d$ és így az 1.2. Tétel utolsó állítása szerint $k \leq d$. Tehát d legnagyobb eleme a $(D_a \cap D_b;\leq)$ részbenrendezett halmaznak is. Látjuk tehát, hogy a legnagyobb közös osztó kétféle lehetséges definíciója egybeesik, amennyiben létezik bármely két számnak legnagyobb közös osztója az 1.12. Definíció szerint. Az euklideszi algoritmus segítségével be fogjuk bizonyítani, hogy a legnagyobb közös osztó valóban mindig létezik.

Maradékos osztás, euklideszi algoritmus, lineáris diofantoszi egyenletek

1.15. Tétel (a maradékos osztás tétele). *Ha $a, b \in \mathbb{Z}$, és $b \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és r egész számok, amelyekre $a = bq + r$ és $0 \leq r < |b|$.*

1.16. Definíció. Adott a és b egész számok esetén az előző tételbeli q és r kiszámítását ***maradékos osztás***nak nevezzük. Az a szám az ***osztandó***, b az ***osztó***, q a ***hányados***, és r a ***maradék***.

1.17. Lemma. *Tetszőleges $a, b, k \in \mathbb{Z}$ esetén a és b közös osztói ugyanazok, mint $a - kb$ és b közös osztói.*

1.18. 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* $ax + by = \operatorname{lnko}(a,b)$.

1.19. Definíció. Azt mondjuk, hogy az a, b egész számok ***relatív prím***ek, ha $\operatorname{lnko}(a,b) = 1$.

1.20. Tétel. *Tetszőleges a, b nemnulla egész számok esetén* $\frac{a}{\operatorname{lnko}(a,b)}$ *és* $\frac{b}{\operatorname{lnko}(a,b)}$ *relatív prím.*

1.21. Tétel. *Tetszőleges $a, b, c \in \mathbb{Z}$ esetén ha a és b relatív prím, akkor* $a \mid bc \iff a \mid c$.

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

1.23. 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, y) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t szám alkalmas megválasztásával:*

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

Prímszám, felbonthatatlan szám, a számelmélet alaptétele

1.24. Definíció. A $p \geq 2$ természetes számot ***felbonthatatlan szám***nak nevezzük, ha csak úgy bontható két természetes szám szorzatára, hogy az egyik tényező maga p. (Ekkor a másik tényező szükségképpen 1; ilyenkor ***triviális faktorizáció***ról beszélünk.) Formálisan:

$$\forall a, b \in \mathbb{N} : p = ab \implies (p = a \text{ vagy } p = b).$$

1.25. Definíció. A $p \geq 2$ természetes számot ***prímszám***nak nevezzük, ha valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall a, b \in \mathbb{N} : p \mid ab \implies (p \mid a \text{ vagy } p \mid b).$$

1.26. Tétel. *A prímszámok és a felbonthatatlan számok ugyanazok.*

1.27. Lemma. *Legyen p prímszám, $n \in \mathbb{N}$ és $a_1, \ldots, a_n \in \mathbb{N}$. Ha $p \mid a_1 \cdot \ldots \cdot a_n$, akkor $p \mid a_i$ valamely $i \in \{1, \ldots, n\}$-re.*

1.28. Tétel (a számelmélet alaptétele). *Bármely természetes szám felbontható prímszámok szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.*

1.29. Következmény. *Legyen az a és b természetes számok prímfelbontása $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ és $b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$ (azokat a prímeket, amelyek csak az egyik számban fordulnak elő, a másikban nulla kitevővel tüntetjük fel). Ekkor teljesülnek az alábbiak:*

(1) $a \mid b \iff \alpha_i \leq \beta_i \ \ (i = 1, \ldots, n)$;
(2) $\operatorname{lnko}(a,b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$;
(3) $\operatorname{lkkt}(a,b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

1.30. Következmény. *Bármely két a, b természetes számnak létezik legkisebb közös többszöröse, és*

$$\operatorname{lnko}(a,b) \cdot \operatorname{lkkt}(a,b) = ab.$$

2. Számelméleti kongruenciák

Kongruenciareláció, maradékosztályok

2.1. 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 ***modulus***ának nevezzük.

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

2.2. 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.*

2.3. 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) $a \equiv a \pmod{m}$;
(2) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$;
(3) $(a \equiv b \pmod{m}$ *és* $b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$;
(4) $\left.\begin{matrix} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{matrix}\right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$, $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$;
(5) *ha* $c \neq 0$, *akkor* $ca \equiv cb \pmod{m} \iff a \equiv b \left(\mathrm{mod}\ \frac{m}{\mathrm{lnko}(m,c)}\right)$;
(6) *ha* $\mathrm{lnko}(m,c) = 1$, *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* $\mathrm{lnko}(a,m) = \mathrm{lnko}(b,m)$.

2.4. Definíció. Egy a egész szám modulo m ***maradékosztály***án 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

$$\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}.$$

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

2.6. Tétel. *A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (különbsége, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik számot választjuk reprezentánsnak.*

2.7. Megjegyzés. A 2.3. Tételbeli utolsó állítás szerint van értelme egy $\mathrm{mod}\, m$ 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.

2.8. Definíció. Az $\overline{a} \in \mathbb{Z}_m$ maradékosztályt ***redukált maradékosztály***nak hívjuk, ha $\mathrm{lnko}(a,m) = 1$.

Jelölés. A $\mathrm{mod}\, m$ redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli. Tehát

$$\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m : \mathrm{lnko}(a,m) = 1\}.$$

Ekvivalenciák és osztályozások

2.9. Definíció. ***Ekvivalenciareláció***nak 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) $\forall a, b, c \in A : (a \rho b$ és $b \rho c) \implies a \rho c$ (tranzitivitás).

Példa. Tetszőleges $f \colon A \to B$ leképezés esetén a $\ker f := \{(a_1, a_2) : f(a_1) = f(a_2)\} \subseteq A \times A$ reláció ekvivalenciareláció az A halmazon, amelynek neve az f leképezés ***mag***ja.

2.10. Definíció. Legyen $\rho \subseteq A \times A$ egy ekvivalenciareláció és a tetszőleges eleme A-nak. Ekkor a $\{b \in A : a \rho b\}$ halmazt az a elem ρ szerinti ***(ekvivalencia)osztály***ának (vagy blokkjának), az ekvivalenciaosztályok halmazát pedig az A halmaz ρ szerinti ***faktorhalmaz***ának 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 $A/\rho = \{\overline{a} : a \in A\}$.

2.11. Definíció. Egy nemüres halmaz ***osztályozás***án olyan páronként diszjunkt nemüres részhalmazainak halmazát értjük, amelyek együtt lefedik az alaphalmazt. Formálisan: $\mathcal{C} \subseteq P(A)$ 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) $\bigcup_{B \in \mathcal{C}} B = A$.

2.12. Tétel. *Legyen A egy nemüres halmaz. Ha $\rho \subseteq A \times A$ ekvivalenciareláció, akkor A/ρ osztályozás az A halmazon. Ha pedig $\mathcal{C} \subseteq P(A)$ 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.*

Lineáris kongruenciák és kongruenciarendszerek

2.13. Definíció. ***Lineáris kongruenciá***nak 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.

2.14. 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, modulo m pedig $\operatorname{lnko}(a,m)$ a megoldások száma. Ha x_0 egy megoldás, akkor az összes megoldás:*

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

2.15. Definíció. Azt mondjuk, hogy az a, b egész számok egymás ***multiplikatív inverz***ei 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.

2.16. Tétel. *Az a egész számnak akkor és csak akkor van multiplikatív inverze modulo m, ha $\operatorname{lnko}(a,m) = 1$. 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.*

2.17. 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 $(\overline{a})^{-k} = \left(\overline{a}^k\right)^{-1}$.

2.18. Megjegyzés. Meg lehet mutatni, hogy a hatványozás szokásos azonosságai érvényben maradnak az egész kitevős $\bmod m$ hatványok fenti értelmezése mellett.

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

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{n_k} \end{aligned}\right\}$$

2.20. Megjegyzés. A 2.14. Tétel segítségével a kongruenciarendszerbeli kongruenciákat külön-külön megoldhatjuk (ha van megoldásuk), és így a kongruenciarendszert a következő alakra hozhatjuk:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}\right\} \qquad (*)$$

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

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

2.23. Tétel*. *A $(*)$ lineáris kongruenciarendszer akkor és csak akkor oldható meg, ha bármely két kongruenciából álló részrendszere megoldható. Speciálisan, páronként relatív prím modulusok esetén mindig van megoldás.*

2.24. 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 $(i = 1, 2, \ldots, k)$. Ekkor a $(*)$ lineáris kongruenciarendszer megoldása:*

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

Maradékrendszerek, az Euler-féle φ függvény, nevezetes kongruenciatételek

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

2.26. Definíció. Modulo m ***teljes maradékrendszer***nek nevezzük egész számok egy olyan rendszerét, amely minden mod m maradékosztályból pontosan egy elemet tartalmaz.

2.27. Tétel. *Ha az $a_1, a_2, \ldots, a_m$ egész számok teljes maradékrendszert alkotnak modulo m, és $b, c \in \mathbb{Z}, \operatorname{lnko}(c, m) = 1$, akkor $ca_1 + b, ca_2 + b, \ldots, ca_m + b$ is teljes maradékrendszer modulo m.*

2.28. Definíció. Modulo m ***redukált maradékrendszer***nek nevezzük egész számok egy olyan rendszerét, amely minden mod m redukált maradékosztályból pontosan egy elemet tartalmaz.

2.29. Tétel. *Ha az $a_1, a_2, \ldots, a_k$ egész számok redukált maradékrendszert alkotnak modulo m, és $c \in \mathbb{Z}, \operatorname{lnko}(c, m) = 1$, akkor $ca_1, ca_2, \ldots, ca_k$ is redukált maradékrendszer modulo m.*

2.30. Definíció. Jelöljük $\varphi(m)$-mel az m-nél nem nagyobb természetes számok közül azoknak a számát, amelyek m-hez relatív prímek: $\varphi(m) = |\{a : 1 \le a \le m \text{ és } \operatorname{lnko}(a, m) = 1\}|$. Az így kapott függvényt ***Euler-féle φ függvény***nek nevezzük. Tömörebben:

$$\varphi \colon \mathbb{N} \to \mathbb{N},\ m \mapsto |\mathbb{Z}_m^*|\,.$$

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

2.32. Következmény (kis Fermat-tétel). *Ha p prímszám, akkor minden a egész számra $a^p \equiv a \pmod{p}$.*

2.33. Következmény. *Ha $a \in \mathbb{Z}$ relatív prím az m modulushoz, és $k_1 \equiv k_2 \pmod{\varphi(m)}$, akkor $a^{k_1} \equiv a^{k_2} \pmod{m}$.*

3. Számelméleti függvények

Nevezetes számelméleti függvények, tökéletes számok

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

3.2. Definíció. Definiálunk néhány számelméleti függvényt (az egyik már ismert):

- $\tau(n) = \sum_{d \mid n} 1$ — n pozitív osztóinak száma;
- $\sigma(n) = \sum_{d \mid n} d$ — n pozitív osztóinak összege;
- $\varphi(n) = |\mathbb{Z}_n^*|$ — az első n természetes szám közül az n-hez relatív prímek száma;
- $\mathrm{id}(n) = n$;
- $\mathbf{1}(n) = 1$;
- $\delta(n) = \begin{cases} 1, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1. \end{cases}$

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

$$\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1)\,;$$

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

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

3.4. Definíció. Azt mondjuk, hogy az f számelméleti függvény ***gyengén multiplikatív***, ha $f(1) = 1$ és bármely egymáshoz relatív prím a, b természetes számok esetén $f(ab) = f(a) \cdot f(b)$.

3.5. Tétel. *Egy f számelméleti függvény akkor és csak akkor gyengén multiplikatív, ha $f(1) = 1$ és tetszőleges $p_1, \ldots, p_n$ prímszámok és $\alpha_1, \ldots, \alpha_n$ pozitív kitevők esetén*

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

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

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

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

3.9. Definíció. Az előző tételben szereplő $2^p - 1$ alakú prímszámokat ***Mersenne-prím***eknek nevezzük.

3.10. Megjegyzés. Nem nehéz belátni, hogy ahhoz, hogy az $M_n = 2^n - 1$ Mersenne-féle szám prímszám legyen, szükséges, hogy n maga is prím legyen. De ez a feltétel nem elegendő, például M_{11} nem prím. 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* ismert legnagyobb prímszám is Mersenne-prím: $M_{57\,885\,161}$, ami tízes számrendszerben 17 425 170 számjegyből áll.

Konvolúció, összegzési és megfordítási függvény, Möbius-féle inverziós formula

3.11. Definíció. Az f és g számelméleti függvények ***konvolúció***ján az alábbi képlettel definiált $f * g$ számelméleti függvényt értjük:

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

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

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

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

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

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

3.16. Tétel. *A tanult nevezetes számelméleti függvények között fennállnak az alábbi összefüggések:*

$$\delta \to \mathbf{1} \to \tau, \quad \varphi \to \mathrm{id} \to \sigma.$$

3.17. Definíció. Az n természetes számot ***négyzetmentes***nek nevezzük, ha nem osztható egyetlen 1-nél nagyobb négyzetszámmal sem.

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

3.19. Definíció. ***Möbius-függvény***nek nevezzük az alábbi képlettel definiált μ számelméleti függvényt:

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

3.20. Tétel. *A Möbius-függvény összegzési függvénye a δ függvény, azaz $\mu \to \delta$.*

3.21. 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*

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

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

*2013.08.20. Forrás: `www.mersenne.org`.

4. Hatványozás modulo m

Rend, primitív gyök, index

4.1. Definíció. Azt mondjuk, hogy k ***jó kitevő*** az a egész számhoz az m modulusra nézve, ha $a^k \equiv 1 \pmod{m}$.

4.2. Definíció. A legkisebb pozitív jó kitevőt, ami az a egész számhoz tartozik az m modulusra nézve, az a szám modulo m ***rend***jének nevezzük (amennyiben létezik egyáltalán pozitív jó kitevő).

Jelölés. Az a egész szám $\bmod m$ rendjét $o_m(a)$ jelöli. Tehát $o_m(a) = \min\left\{k > 0 : a^k \equiv 1 \pmod{m}\right\}$.

4.3. Megjegyzés. Világos, hogy $\operatorname{lnko}(a, m) > 1$ esetén nincs jó kitevő, tehát ilyenkor $o_m(a)$ nem értelmezett. Ha viszont a és m relatív prímek, akkor az Euler–Fermat-tétel szerint $\varphi(m)$ jó kitevő, tehát ekkor $o_m(a) \leq \varphi(m)$.

4.4. Tétel. *A jó kitevők éppen a rend többszörösei. Precízebben: ha a és m relatív prímek, k pedig tetszőleges egész szám, akkor*

$$a^k \equiv 1 \pmod{m} \iff o_m(a) \mid k.$$

Következésképp $o_m(a) \mid \varphi(m)$.

4.5. Következmény. *A kitevők modulo $o_m(a)$ számítanak. Precízebben: ha a és m relatív prímek, k_1, k_2 pedig tetszőleges egész számok, akkor*

$$a^{k_1} \equiv a^{k_2} \pmod{m} \iff k_1 \equiv k_2 \pmod{o_m(a)}.$$

4.6. Következmény. *Ha a és m relatív prímek, akkor a hatványai $o_m(a)$-féle különböző maradékot adnak modulo m, és ezeket mind megkapjuk, ha a kitevőt egy $\bmod o_m(a)$ teljes maradékrendszeren futtatjuk végig (például 1-től $o_m(a)$-ig). Formálisan:*

$$\left|\left\{\overline{a^k} : k \in \mathbb{Z}\right\}\right| = o_m(a) \quad \text{és} \quad \left\{\overline{a^k} : k \in \mathbb{Z}\right\} = \left\{\overline{a}, \overline{a^2}, \ldots, \overline{a^{o_m(a)}}\right\} \subseteq \mathbb{Z}_m.$$

4.7. Definíció. Azt mondjuk, hogy a g egész szám ***primitív gyök*** modulo m, ha rendje éppen $\varphi(m)$.

4.8. Tétel. *A g egész szám akkor és csak akkor primitív gyök modulo m, ha az összes $\bmod m$ redukált maradékosztály megkapható $\overline{g}$ hatványaként.*

4.9. Lemma*. *Ha p prímszám, akkor az $x^d \equiv 1 \pmod{p}$ kongruenciának legfőljebb d megoldása lehet modulo p.*

4.10. Megjegyzés. Meglepő lehet, hogy az állítás nem igaz, ha a modulus nem prím (keressünk ellenpéldát!).

4.11. Tétel. *Ha p prímszám és $d \mid p-1$, akkor a d-edrendű egészek száma modulo p éppen $\varphi(d)$. Speciálisan $\varphi(p-1)$ modulo p inkongruens primitív gyök van.*

4.12. Tétel*. *A következő modulusokhoz létezik primitív gyök (és csak ezekhez): $2, 4$, páratlan prímhatványok, páratlan prímhatványok kétszeresei. Ezekben az esetekben $a \bmod m$ primitív gyökök száma $\varphi(\varphi(m))$.*

4.13. Definíció. Tegyük fel, hogy g primitív gyök az m modulushoz. Az a egész szám ***index***én (az m modulusra és a g primitív gyökre nézve) olyan i kitevőt értünk, amelyre $g^i \equiv a \pmod{m}$.

Jelölés. A modulust az egyszerűség kedvéért nem írjuk ki (ez többnyire amúgy is világos a szövegkörnyezetből), tehát a indexét röviden $\operatorname{ind}_g a$ jelöli.

4.14. Megjegyzés. Világos, hogy ha a és m nem relatív prím, akkor $\operatorname{ind}_g a$ nem értelmezett (ugyanis g^i mindig relatív prím m-hez). Ha viszont a és m relatív prím, akkor a 4.8. Tétel szerint a előáll g hatványaként modulo m, tehát ekkor $\operatorname{ind}_g a$ értelmezett.

4.15. Megjegyzés. Figyeljük meg, hogy az index nem más, mint a logaritmus $\bmod m$ analógja. Nem meglepő tehát, hogy hasonló tulajdonságokkal rendelkezik, amint ezt a következő tételben látjuk. A 4.5. Következmény szerint az index (ha létezik) csak modulo $\varphi(m)$ van meghatározva, ezért az indexre vonatkozó alábbi azonosságokban nem egyenlőségeket, hanem $\bmod \varphi(m)$ kongruenciákat írunk.

4.16. Tétel. *Legyen g primitív gyök modulo m, legyen k tetszőleges egész szám, a és b pedig relatív prímek m-hez. Ekkor érvényesek az alábbi azonosságok:*

(1) $\operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$;
(2) $\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$;
(3) $\operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;
(4) $\operatorname{ind}_g \left(ab^{-1}\right) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

4.17. Definíció. Azt mondjuk, hogy az a egész szám ***n-edik hatványmaradék*** modulo m, ha az $x^n \equiv a \pmod{m}$ kongruenciának van megoldása.

4.18. Tétel. *Legyen g primitív gyök modulo m, és legyen a relatív prím m-hez. Ekkor a pontosan akkor n-edik hatványmaradék modulo m, ha $(n, \varphi(m)) \mid \operatorname{ind}_g a$.*

Négyzetes maradékok, Legendre-szimbólum

4.19. Definíció. Az a egész számot ***négyzetes maradék***nak nevezzük modulo m, ha az $x^2 \equiv a \pmod{m}$ kongruenciának van megoldása. Ellenkező esetben azt mondjuk, hogy a ***négyzetes nemmaradék*** modulo m. (Nem elírás, valóban úgy mondjuk, hogy a négyzetes nemmaradék, nem pedig úgy, hogy a nem négyzetes maradék.)

4.20. Tétel. *Legyen p páratlan prímszám, g primitív gyök modulo p. Ekkor $a \in \mathbb{Z}$ pontosan akkor négyzetes maradék modulo p, ha $p \mid a$ vagy $\operatorname{ind}_g a$ páros.*

4.21. Definíció. Tetszőleges p páratlan prímszám és p-vel nem osztható a egész szám esetén értelmezzük az $\left(\frac{a}{p}\right)$ ***Legendre-szimbólum***ot a következőképpen:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék } \bmod p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék } \bmod p. \end{cases}$$

4.22. Tétel (Euler-kritérium). *Ha p páratlan prímszám és $p \nmid a$, akkor*

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

4.23. Tétel. *Tetszőleges p páratlan prímszám és p-vel nem osztható a, b egész számok esetén teljesülnek az alábbiak:*

(1) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
(3) $\left(\frac{a^2}{p}\right) = 1$.

4.24. Tétel. *Tetszőleges p páratlan prímszám esetén*

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

4.25. Tétel (Gauss-lemma). *Legyen p páratlan prímszám, a pedig p-vel nem osztható szám. Jelölje n az $a, 2a, \ldots, \frac{p-1}{2}a$ számok közül azoknak a számát, amelyek p-vel adott osztási maradéka nagyobb, mint $\frac{p}{2}$. Ekkor az $\left(\frac{a}{p}\right)$ Legendre-szimbólum értéke $(-1)^n$.*

4.26. Tétel. *Az előző tétel jelöléseit használva páratlan a esetén*

$$n \equiv \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ai}{p}\right] \pmod{2}.$$

4.27. Tétel (négyzetes reciprocitási tétel). *Tetszőleges p, q különböző páratlan prímszámok esetén*

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

4.28. Tétel. *Tetszőleges p páratlan prímszámra*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{ha } p \equiv 1, 7 \pmod{8}; \\ -1, & \text{ha } p \equiv 3, 5 \pmod{8}. \end{cases}$$

5. Számok felbontása hatványok összegére

Pitagoraszi számhármasok, a nagy Fermat-tétel

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

5.2. 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).

5.3. Lemma. *Primitív pitagoraszi számhármasban a tagok páronként is relatív prímek. Fordítva, ha egy pitagoraszi számhármasban valamelyik két tag relatív prím, akkor a számhármas primitív.*

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

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

$$u>v,\ u\not\equiv v\pmod 2,\ \operatorname{lnko}(u,v)=1,\ \text{és } x=2uv,\ y=u^2-v^2,\ z=u^2+v^2. \tag{$\triangle$}$$

Fordítva, a $(\triangle)$ formulákkal definiált (x,y,z) számhármas mindig primitív pitagoraszi számhármas.

5.6. Tétel. *Az $x^4+y^4=z^2$ egyenletnek nincs pozitív egészekből álló megoldása.*

5.7. Következmény. *Az $x^4+y^4=z^4$ egyenletnek nincs pozitív egészekből álló megoldása.*

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

Négyzetszámok összegei

5.9. Lemma. *Ha a és b előáll két négyzetszám összegeként, akkor ab is előáll.*

5.10. Lemma. *A $4k+1$ alakú prímszámok előállnak két négyzetszám összegeként.*

5.11. Lemma. *Tegyük fel, hogy n előáll két relatív prím négyzetszám összegeként. Ekkor n egyetlen prímosztója sem lehet $4k+3$ alakú.*

5.12. 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.*

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

5.14. 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-ra, bár ezt már Waring is sejtette. Hilbert igazolta Waring sejtését, és van egy feltételezett képlet is a $g(k)$ számokra:

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

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.

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

6. A prímszámok eloszlása

Elemi állítások a prímszámok eloszlásáról

6.1. Tétel. *Végtelen sok prímszám van.*

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

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

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

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

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

6.7. Definíció. ***Ikerprím***nek nevezünk két prímszámot, ha különbségük 2.

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

Analitikus eredmények a prímszámok eloszlásáról, a prímszámtétel

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

6.10. Lemma*. *Minden nemnegatív valós x-re teljesül a $\log(1+x) \leq x$ egyenlőtenség.*

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

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

6.12. Megjegyzés. Ez a tétel durván fogalmazva azt állítja, hogy „sok" prímszám van (négyzetszámból viszont a 6.9. 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).

6.13. Megjegyzés. A harmonikus sor lassan divergál, a prímszámok reciprokaiból alkotott sor még lassabban. Például $\sum_{p<10^{18}} \frac{1}{p} < 4$ (ez kb. a sor első ötvenmillió tagja).

6.14. 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:

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

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

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

6.16. Következmény*. *Az n-edik prímszám aszimptotikusan $n \log n$, azaz $\lim_{n \to \infty} \frac{p_n}{n \log n} = 1$ (p_n az n-edik prímszámot jelöli).*