MTN113E: Számelmélet
(előadásvázlat)

Kátai-Urbán Kamilla

1. Oszthatóság, maradékos osztás

1. Definíció. Azt mondjuk, hogy az a egész szám osztója a b egész számnak (b többszöröse a-nak), ha létezik olyan k egész szám, amelyre $ak = b$. Ha a osztója b-nek, akkor ezt úgy jelöljük, hogy $a \mid b$.

2. Definíció. Egy egész számot egységnek nevezünk, ha minden egész számnak osztója.

3. Tétel. Az egész számok körében két egység van, az 1 és a -1.

4. Tétel (oszthatóság tulajdonságai). Tetszőleges a, b, c egész számokra érvényesek az alábbiak:

(1) $a \mid a$;
(2) ha $a \mid b$ és $b \mid c$, akkor $a \mid c$;
(3) $a \mid b$ és $b \mid a$ akkor és csak akkor, ha $a = \pm b$;
(4) $a \mid 0$;
(5) $a \mid 1$ akkor és csak akkor, ha $a = \pm 1$;
(6) $0 \mid a$ akkor és csak akkor, ha $a = 0$;
(7) ha $a \mid b$ és $a \mid c$, akkor $a \mid b \pm c$;
(8) ha $a \mid b$, akkor $a \mid bc$;
(9) ha $c \neq 0$, akkor $a \mid b$ akkor és csak akkor, ha $ac \mid bc$;
(10) ha $a \mid b$ és $b \neq 0$, akkor $|a| \leq |b|$.

5. Tétel (maradékos osztás). Ha a és b egész számok és $b \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és r egész számok, amelyekre $a = bq + r$ és $0 \leq r < |b|$.

6. Definíció. Az előző tételben szereplő a számot osztandónak, b-t osztónak, q-t hányadosnak és r-et maradéknak nevezzük.

2. Legnagyobb közös osztó

7. Definíció. A d egész számot az a és b egész számok legnagyobb közös osztójának nevezzük, ha teljesülnek a következők:

(lnko1) $d \mid a$ és $d \mid b$;
(lnko2) bármely k egész számra, ha $k \mid a$ és $k \mid b$, akkor $k \mid d$.

Az a és b számok legnagyobb közös osztóját $\text{lnko}(a, b)$-vel jelöljük.

8. Megjegyzés. A legnagyobb közös osztó az egész számok körében nem egyértelmű, ha d legnagyobb közös osztó, akkor $-d$ is. Ha $a, b \in \mathbb{N}$, akkor a legnagyobb közös osztót is az $\mathbb{N}$ halmazból választjuk, így egyértelműen meghatározott.
Az előző definícióhoz hasonlóan megadható a és b legkisebb többszöröse is, jele $\text{lkkt}(a, b)$.

9. Definíció. Azt mondjuk, hogy az a és b egész számok asszociáltak, ha $a \mid b$ és $b \mid a$ teljesül (azaz $a = \pm b$), és az $a \sim b$ jelölést használjuk.

10. Definíció. Az a és b egész számok relatív prímek, ha $\text{lnko}(a, b) \sim 1$.

11. Tétel (euklideszi algoritmus). Bármely két a és b természetes számnak van legnagyobb közös osztója, amely az alábbi euklideszi algoritmussal megkapható. Az $r_0 = a$ és $r_1 = b$ természetes

számokon végrehajtott euklideszi algoritmus maradékos osztások ismételt elvégzését jelenti:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 && (0 < r_2 < r_1);\\ r_1 &= q_2 r_2 + r_3 && (0 < r_3 < r_2);\\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n && (0 < r_n < r_{n-1});\\ r_{n-1} &= q_n r_n + r_{n+1} && (r_{n+1} = 0). \end{aligned}$$

Az eljárás véges számú lépés után véget ér, azaz létezik olyan n természetes szám, hogy $r_{n+1} = 0$. Ekkor a legnagyobb közös osztó az utolsó nemnulla maradék, azaz $\operatorname{lnko}(a, b) = r_n$.

12. Tétel (lnko tulajdonságai). Tetszőleges a, b, c egész számokra érvényesek az alábbiak:

(1) $\operatorname{lnko}(a, 0) \sim a$;
(2) $\operatorname{lnko}(a, b) \sim a$ akkor és csak akkor, ha $a \mid b$;
(3) $\operatorname{lnko}(a + bc, b) \sim \operatorname{lnko}(a, b)$;
(4) ha $\operatorname{lnko}(a, b) \neq 0$, akkor $\frac{a}{\operatorname{lnko}(a,b)}$ és $\frac{b}{\operatorname{lnko}(a,b)}$ relatív prímek;
(5) ha $\operatorname{lnko}(a, b) \neq 0$, akkor $\operatorname{lkkt}(a, b) \sim \frac{ab}{\operatorname{lnko}(a,b)}$;
(6) ha $\operatorname{lnko}(a, c) \sim 1$ és $c \mid ab$, akkor $c \mid b$.

3. Prímszám, számelmélet alaptétele

13. Definíció. Egy egész szám triviális osztóinak az egységeket és saját maga egységszereseit nevezzük.

14. Definíció. Egy egész szám összetett szám, ha triviálistól különböző osztója is van.

15. Definíció. A p egységektől és nullától különböző egész számot felbonthatatlannak nevezzük, ha csak úgy bontható fel két egész szám szorzatára, hogy valamelyik egység, azaz ha $p = ab$, akkor a vagy b egység. (Ha a egység, akkor $p \sim b$.)

16. Megjegyzés. A felbonthatatlan számoknak csak triviális osztói vannak, azaz csak triviálisan lehet szorzattá alakítani.

17. Definíció. A p egységektől és nullától különböző egész számot prímelemnek nevezzük, ha valahányszor osztója egy szorzatnak, mindannyiszor osztója valamelyik tényezőnek, azaz ha $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$.

18. Tétel. A p egész szám pontosan akkor prímelem, ha felbonthatatlan.

19. Definíció. Egy $p \geq 2$ természetes számot prímszámnak nevezünk, ha valahányszor osztója egy szorzatnak, mindannyiszor osztója valamelyik tényezőnek, azaz ha $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$.

20. Megjegyzés. A prímszámok tehát a prímelemek közül a pozitív egész számok.

21. Tétel. Végtelen sok prímszám létezik.

22. Tétel (számelmélet alaptétele (prímelemekkel)). Bármely 0-tól és egységektől különböző egész szám felbontható prímelemek szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű.

23. Tétel (számelmélet alaptétele (prímszámokkal)). Bármely 0-tól különböző egész szám felbontható prímszámok szorzatára (negatív szám esetén -1-gyel szorozva), és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

24. Megjegyzés. Az 1 prímtényezős felbontása az üres szorzat.

25. Következmény (prímhatványtényezős alak). Bármely 0-tól különböző egész szám előáll páronként különböző prímszámok hatványainak szorzataként (negatív szám esetén -1-gyel szorozva), és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

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

(1) $a \mid b$ akkor és csak akkor, ha $\alpha_i \leq \beta_i$ minden i-re;
(2) $\text{lnko}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$;
(3) $\text{lkkt}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

4. Racionális számok tizedestört alakja

27. Tétel. Bármely racionális szám tizedestört alakja véges vagy végtelen szakaszos.

28. Tétel. Egy $q = \frac{a}{b} \in \mathbb{Q}$ ($a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\text{lnko}(a, b) \sim 1$) racionális szám tizedestört alakja pontosan akkor véges, ha b prímtényezős felbontásában legfeljebb a 2 vagy az 5 szerepel.

29. Megjegyzés. A racionális számok tizedestört alakja nem egyértelmű, például a $\frac{3}{4}$ megadható $0,75$ és $0,749\dot{9}$ alakban is, ez úgy kerülhető el, ha a végtelen sok kilencest nem engedjük meg.