SZÁMELMÉLET ELŐADÁS
Összefoglaló

2024. Február 20.

1. Legnagyobb közös osztó, kitüntetett közös osztó

1.1. Definíció (FGY. 1.3.1). *Az a és b egész számok legnagyobb közös osztója d, ha*

(i) $d \mid a,\ d \mid b$ *és*

(ii) ha egy c-re $c \mid a,\ c \mid b$ *teljesül, akkor* $|c| \leq |d|$

Jelölés: $d = (a, b)$ vagy $d = \text{lnko}(a, b)$. Ha $a = b = 0$, akkor nem létezik legnagyobb közös osztójuk, hiszen minden egész szám közös osztó, és ezek között nincs legnagyobb abszolút értékű.

Minden más esetben viszont a fenti definíciót pontosan két d szám elégíti ki, amelyek egymás ellentetjei. Mivel egy szám és a negatívja oszthatósági szempontból teljesen egyenértékű, ezért a és b összes közös osztóját úgy kapjuk meg, hogy a pozitív közös osztók mellé vesszük azok negatívjait. A pozitív közös osztók P halmaza nem az üres halmaz, hiszen az 1 biztosan osztó, továbbá P-nek csak véges sok eleme lehet, mert egy nemnulla számnak csak véges sok osztója van. Ennélfogva P elemei között létezik egy legnagyobb, jelöljük h-val. Ekkor nyilván $d = h$ és $d = -h$ kielégítik a definíciót, más szám viszont nem.

1.2. Definíció (FGY. 1.3.2). *Az a és b számok kitüntetett közös osztója δ, ha*

(i) $\delta \mid a,\ \delta \mid b$ *és*

(ii') *ha egy c-re $c \mid a,\ c \mid b$ teljesül, akkor $c \mid \delta$*

A kitüntetett közös osztó tehát olyan közös osztó, amely minden közös osztónak többszöröse.

A definícióból következik, hogy ha két számnak létezik kitüntetett közös osztója, akkor az egységszerestől eltekintvbe egyértelmű.

Ha $a = b = 0$, akkor a kitüntetett közös osztójuk a definíció szerint 0.

Megmutatjuk, hogy ha egyáltalán létezik a δ kitüntetett közös osztó, akkor δ csak a legnagyobb közös osztó (valamelyik értéke) lehet. Jelöljük d-vel a δ-val azonos előjelű legnagyobb közös osztót. Ekkor egyrészt (ii) miatt

$$|\delta| \leq |d|$$

másrészt (ii') alapján $d \mid \delta$ amiből

$$|d| \leq |\delta|$$

következik. A két egyenlőségből kapjuk, hogy $|d| = |\delta|$ és így az azonos előjel miatt $\delta = d$.

Egyáltalán nem magától értetődő azonban, hogy a legnagyobb közös osztó valóban rendelkezik a (ii') kitüntetett tulajdonsággal is, vagyis hogy bármely két egész számnak létezik kitüntetett közös osztója.

1.1. Tétel (FGY: 1.3.3). *Bármely két egész számnak létezik kitüntetett közös osztója.*

1.1. Bizonyítás. *A kitüntetett közös osztó létezését a matematika egyik legősibb eljárásával, az euklideszi algoritmussal igazoljuk. Az egyik számot maradékosan elosztjuk a másikkal, majd a másik számot a maradékkal stb., mindig az osztót a maradékkal, amíg 0 maradékhoz nem jutunk. Megmutatjuk, hogy az eljárás véges, és az utolsó nemnulla maradék lesz a két szám (egyik) kitüntetett közös osztója.*

Nézzük mindezt részletesen. Tegyük fel, hogy (pl.) $b \neq 0$. Ha $b \mid a$, akkor $\delta = b$ megfelel.

Ha $b \nmid a$, akkor alkalmas q_i, r_i egészekkel

$$\begin{aligned}
a &= bq_1 + r_1, && ahol && 0 < r_1 < |b| \\
b &= r_1q_2 + r_2, && ahol && 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, && ahol && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, && ahol && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} && && (r_{n+1} = 0)
\end{aligned}$$

Az eljárás biztosan befejeződik véges sok lépésben, ugyanis a maradékok nemnegatív egészekből álló szigorúan csökkenő sorozatot alkotnak:

$$|b| > r_1 > r_2 > \dots$$

Most belátjuk, hogy r_n valóban az a és b számok (egyik) kitüntetett közös osztója.

Az algoritmus egyenlőségein alulról felfelé haladva először azt igazoljuk, hogy r_n közös osztója a-nak és b-nek. Az utolsó egyenlőségből $r_n \mid r_{n-1}$. Az utolsó előtti egyenlőségre rátérve

$$r_n \mid r_{n-1},\ r_n \mid r_n \implies r_n \mid r_{n-1}q_n + r_n = r_{n-2}$$

Ugyanígy folytatva végül $r_n \mid b$, majd (az első egyenlőségből) $r_n \mid a$ adódik.

A kitüntetett tulajdonság igazolásához felülről lefelé haladunk. Legyen $c \mid a,\ c \mid b$, ekkor az első egyenlőségből $c \mid a - bq = r_1$. A második egyenlőségre rátérve

$$c \mid b,\ c \mid r_1 \implies c \mid b - r_1q_2 = r_2.$$

Ugyanígy folytatva végül az utolsó előtti egyenlőségből kapjuk, hogy $c \mid r_n$. ■

1.1. Megjegyzés. *1. Az euklideszi algoritmust a legkisebb nemnegatív maradékok helyett a legkisebb abszolút értékű maradékokkal is végezhetjük; ebben az esetben a maradékok abszolút értékei alkotnak nemnegatív egészekből álló szigorúan csökkenő sorozatot, és így az eljárás ekkor is véges sok lépésben biztosan befejeződik.*

2. Szokás a legnagyobb közös osztót eleve pozitívnak definiálni. Mivel azonban egy szám és a negatívja egymás egységszeresei, azaz bármely oszthatósági kérdésnél teljesen azonosan viselkednek, ezért semmi ok sincs arra, hogy a legnagyobb közös osztó fogalmából a negatív számokat eleve kirekesszük. Ezért adtuk meg a legnagyobb közös osztó definícióját úgy, hogy abba a két legnagyobb abszolút értékű közös osztó egyenrangúan beleférjen.

3. Az előrebocsátott megjegyzések alapján nem jelent megszorítást, ha a továbbiakban kényelmi okokból a legnagyobb közös osztó, illetve a (vele már bizonyítottan megegyező) kitüntetett közös osztó két értéke közül mindig a pozitívat fogjuk tekinteni. Ezentúl az $(a; b)$, illetve $lnko(a; b)$ jelölés is ezt a(z egyértelműen meghatározott) pozitív számot fogja jelenteni, és (általában) a kitüntetett közös osztóra is a legnagyobb közös osztó elnevezést fogjuk használni.

4. A legnagyobb közös osztó gyakorlati kiszámításánál az egyszerűen adódó $(a, b) = (b, a - kb)$ összefüggés alapján gyakran kényelmesebb az euklideszi

algoritmusnak az

$$(a,b) = (b,r_1) = (r_1,r_2) = \cdots = (r_{n-1},r_n) = (r_n,0) = r_n$$

alakját használni.

5. Az 1.3.2 Definíciót, az ottani (ii′) kitüntetett tulajdonság bevezetését az indokolja, hogy csak oszthatósági relációt használ fel, szemben az 1.3.1 Definícióval, amelyben rendezési reláció (nagyobb–kisebb) is szerepel. Ennélfogva nem meglepő, hogy az egész számok számelméleti vizsgálatainál - amint hamarosan látni fogjuk - mind elméleti, mind pedig gyakorlati szempontból elsősorban a (ii') kitüntetett tulajdonságra tudunk majd támaszkodni.

A csak az oszthatóságra épülő fogalomalkotás további előnye, hogy bizonyos számkörökben (illetve általánosabban integritási tartományokban) az 1.3.1 Definíció nem is értelmes. Ennek egyik nyilvánvaló oka az, ha nem definiálható a számkörben (a szokásos „jó" tulajdonságokkal bíró) rendezés, ilyenek pl. a komplex számok bizonyos részhalmazai.

Az 1.3.1 Definícióval azonban olyan számkörökben is adódhat probléma, amelyekben van rendezés, például a $c+d\sqrt{2}$ (c,d egészek) számkörben is ez a helyzet. Itt ugyanis a végtelen sok egység miatt bármely két elemnek végtelen sok közös osztója van, és ezek között nincs legnagyobb abszolút értékű. (Ha csak páronként nem egységszeres közös osztókat tekintünk, akkor sincs értelme az 1.3.1 Definíciónak, mert bármely két közös osztó esetén létezik az elsőnek olyan egységszerese, amely nagyobb a második osztónál.) Ezért a számelmélet további fejezeteiben egyenesen az 1.3.2 Definíció szerint értelmezzük majd a legnagyobb közös osztót.

1.1. Példa. *Számítsuk ki* $(753,420)$ *legnagyobb közös osztóját:*

$$\begin{aligned}
753 &= 1\cdot 420 + 333\\
420 &= 1\cdot 333 + 87\\
333 &= 3\cdot 87 + 72\\
87 &= 1\cdot 72 + 15\\
72 &= 4\cdot 15 + 12\\
15 &= 1\cdot 12 + 3\\
12 &= 4\cdot 3 + 0
\end{aligned}$$

Tekintsük (az egész számok körében) a legnagyobb közös osztó néhány fontos tulajdonságát:

1.2. Tétel (FGY: 1.3.4). *Ha* $c>0$, *akkor* $(ca,cb) = c(a,b)$

1.2. Bizonyítás. *Tekintsük az (a, b) előállítására szolgáló euklideszi algoritmust, legyen az utolsó nemnulla maradék $r_n = (a, b)$. Szorozzunk meg minden egyenlőséget c-vel, ekkor éppen a (ca, cb)-t előállító euklideszi algoritmushoz jutunk. Ebben az utolsó nemnulla maradék $(ca, cb) = cr_n = c(a, b)$.* ■

1.3. Tétel (FGY: 1.3.5). *Az a és b számok legnagyobb közös osztója alkalmas u és v egészekkel kifejezhető $(a, b) = au + bv$ alakban.*

1.3. Bizonyítás. *Az euklideszi algoritmus első egyenlőségéből r_1-et kifejezve*

$$r_1 = a - bq_1$$

adódik. Ennek felhasználásával a második egyenlőségből az

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = a(-q_2) + b(1 + q_1q_2)$$

előállításhoz jutunk, azaz r_2 felírható $aU + bV$ alakban. Hasonlóan továbbhaladva az utolsó előtti egyenlőségből azt kapjuk, hogy $(a, b) = r_n$ is kifejezhető $au + bv$ alakban. ■

FGY: Freud-Gyarmati: Számelmélet. Nemzeti Tankönyvkiadó Rt., Budapest, 2000.

Müllner Károly
Email: mullni@hotmail.com
https://mullni.elte.hu