# Számelmélet

(segédanyag)

Diszkrét modellek alkalmazásai

Gyakorlatvezető: Uray M. János

## 1 Definíciók

Oszthatóság: $a$ **osztható** $b$-vel (jele: $b \mid a$), ha van olyan $c$ egész szám, hogy $a = b \cdot c$.
Két szám, $a$ és $b$ **legnagyobb közös osztója** az a $c$ egész szám, melyre $c \mid a$ és $c \mid b$, de bármely $d$ egész számra ha $d \mid a$ és $d \mid b$, akkor $d \mid c$.
(Szavakkal: $d$ osztója $a$-nak és $b$-nek, azaz közös osztó, de bármely $d$ közös osztóra $c$ a ,,nagyobb", oszthatósági értelemben.)
Jele: $c = (a, b) = \text{lnko}(a, b) = \gcd(a, b)$. Példa: $\gcd(6, 8) = 2$.
Két szám, $a$ és $b$ **legkisebb közös többszöröse** az az $m$ egész szám, melyre $a \mid m$ és $b \mid m$, de bármely $n$ egész számra ha $a \mid n$ és $b \mid n$, akkor $m \mid n$.
(Szavakkal: $m$ többszöröse $a$-nak és $b$-nek, azaz közös többszörös, de bármely $n$ közös többszörösre $m$ a ,,kisebb", oszthatósági értelemben.)
Jele: $m = [a, b] = \text{lkkt}(a, b) = \text{lcm}(a, b)$. Példa: $\gcd(6, 8) = 24$.
Néhány tulajdonság:
- $\gcd(a, b) = \gcd(b, a)$,
- $\gcd(a, a) = a$,
- $\gcd(a, 1) = 1$,
- $\text{lcm}(a, b) = \text{lcm}(b, a)$,
- $\text{lcm}(a, a) = a$,
- $\text{lcm}(a, 1) = a$,
- $\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$.

Két szám, $a$ és $b$ **relatív prím**, ha $\gcd(a, b) = 1$. (Megjegyzés: ekkor $\text{lcm}(a, b) = a \cdot b$.)
Két szám, $a$ és $b$ **kongruens modulo** $m$ (jele: $a \equiv b \pmod{m}$), ha $m \mid a - b$, másképpen: $a$ és $b$ ugyanazt a maradékot adja $m$-mel osztva, harmadikféleképpen: van olyan $k$ egész, hogy $a = b + km$.

## 2 Euklideszi algoritmus

Két szám legnagyobb közös osztójának kiszámítása:
- írjuk egymás alá a két számot, csökkenő sorrendben;
- osszuk el egymással maradékosan, és írjuk a maradékot alájuk;
- vegyük az utolsó két számot, osszuk el egymással maradékosan, és írjuk a maradékot megint alájuk;
- ismételjük addig, amíg 0-t nem kapunk;
- a legnagyobb közös osztó a 0 előtti szám.

Példa $\gcd(30, 22)$-re:

$$\begin{aligned} &30 \\ &22 \\ &8 \quad (= 30 \bmod 22) \\ &6 \quad (= 22 \bmod 8) \\ &2 \quad (= 8 \bmod 6) \\ &0 \quad (= 6 \bmod 2), \end{aligned}$$

azaz $\gcd(30, 22) = 2$.

# 3 Bővített euklideszi algoritmus

Nemcsak a legnagyobb közös osztót számítjuk ki, hanem azt felírjuk a két szám *egész lineáris kombinációjaként*, azaz keresünk olyan $u$ és $v$ számokat, hogy:

$$\gcd(a, b) = au + bv.$$

Ehhez kibővítjük az euklideszi algoritmust úgy, hogy minden sorhoz hozzáírjuk az aktuális $u$-t és $v$-t:
• az első számhoz 1 és 0, mert $a = a \cdot 1 + b \cdot 0$;
• a második számhoz 0 és 1, mert $b = a \cdot 0 + b \cdot 1$;
• a harmadik számhoz, azaz $a \bmod b$-hez az előző két sorból számítjuk ki az együtthatókat: $a$-ból hányszorosát vontuk le $b$-nek, hogy $a \bmod b$-t kapjunk? a teljes első sorból ennyiszeresét vonjuk le a második sornak;
• ezt folytatjuk minden újabb sorban;
• a legnagyobb közös osztó mellett megkapjuk a keresett $u$-t és $v$-t.
Példa:

| | | | |
|---|---|---|---|
| 30 | 1 | 0 | |
| 22 | 0 | 1 | |
| 8 | 1 | −1 | (az első sorból kivontuk a második sort egyszer) |
| 6 | −2 | 3 | (a 22-es sorból kivontuk a 8-as sor kétszeresét) |
| 2 | 3 | −4 | (a 8-as sorból kivontuk a 6-os sort) |
| 0 | | | |

azaz $\gcd(30, 22) = 2 = 30 \cdot 3 + 22 \cdot (-4)$.

# 4 Lineáris diofantikus egyenletek

Keressük az

$$ax + by = c$$

egyenlet egész $x$ és $y$ megoldásait adott $a$-ra $b$-re és $c$-re. Például:

$$30x + 22y = 12.$$

Fontos hangsúlyozni, hogy *egész* megoldásokat keresünk, így az iskolai egyenletmegoldó módszerek nem működnek.
Ha a diofantikus egyenlet jobb oldalán a legnagyobb közös osztó van, azaz $c = \gcd(a, b)$, akkor a bővített euklideszi algoritmus közvetlenül ad egy megoldást. Ha $c \neq \gcd(a, b)$, de $\gcd(a, b) \mid c$, akkor végrehajtjuk a bővített euklideszi algoritmust, előállítjuk $\gcd(a, b)$-t lineáris kombinációként ($au + bv = \gcd(a, b)$), és megszorozzuk az egyenletet annyival, hogy a jobb oldalon $c$ legyen (azaz $c/\gcd(a, b)$-vel), így kapunk egy megoldást, azaz:

$$x_0 = u \cdot \frac{c}{\gcd(a, b)},$$
$$y_0 = v \cdot \frac{c}{\gcd(a, b)}.$$

Tekintsük a fenti példaegyenletet. A bővített euklideszi megadja, hogy

$$30 \cdot 3 + 22 \cdot (-4) = 2$$

(lásd fent). Ezt megszorozva 6-tal megkapjuk, hogy

$$30 \cdot 18 + 22 \cdot (-24) = 12,$$

ami egy megoldása az egyenletnek: $x_0 = 18$ és $y_0 = -24$.
Az összes megoldást úgy kapjuk meg, hogy $x_0$-hoz hozzáadunk, $y_0$-ból pedig levonunk valamennyit úgy, hogy az egyenletben pont kiejtsék egymást. Konkrétan:

$$x = x_0 + \frac{b}{\gcd(a, b)}k,$$
$$y = y_0 - \frac{a}{\gcd(a, b)}k$$

(ahol $k$ tetszőleges egész szám). Miért? Számoljuk ki:

$$ax + by = a\left(x_0 + \frac{b}{\gcd(a, b)}k\right) + b\left(y_0 - \frac{a}{\gcd(a, b)}k\right) = ax_0 + by_0,$$

ami, mivel $x_0$ és $y_0$ megoldás, egyenlő $c$-vel, tehát a bal oldalon álló $x$ és $y$ is megoldás.
Folytatva a fenti példát:

$$x = 18 + \frac{22}{2}k = 18 + 11k,$$
$$y = -24 - \frac{30}{2}k = -24 - 15k,$$

azaz a kezdő $(18, -24)$ mellett például megoldás a $(29, -39)$ (ha $k = 1$), a $(40, -54)$ (ha $k = 2$), vagy a $(7, -9)$ (ha $k = -1$) is.
Mi a helyzet akkor, ha $\gcd(a, b) \nmid c$? Ekkor a lineáris diofantikus egyenletnek nincs megoldása. Miért? Mert az egyenlet bal oldalán $a$ is és $b$ is osztható $\gcd(a, b)$-vel (definíció szerint), tehát az egész bal oldal is osztható vele, de akkor a jobb oldalnak is oszthatónak kell lennie $\gcd(a, b)$-vel.

# 5 Lineáris kongruencia

Keressük az

$$ax \equiv b \pmod{m}$$

egyenlet megoldását $x$-re adott $a$ és $b$ esetén. Emlékezzünk a kongruencia definíciójára: ez azt jelenti, hogy keresünk egy olyan $x$ egész számot, amelyre $a \cdot x$ ugyanolyan maradékot ad $m$-mel osztva, mint $b$. Például:

$$7x \equiv 3 \pmod{10},$$

ami azt jelenti, hogy 7-nek mely többszörösei végződnek 3-ra tízes számrendszerben.
Vegyük észre, hogy a megoldás $m$-enként ismétlődik, hiszen a példában is ha 9 megoldás, akkor $19, 29, \ldots$ is megoldások, azaz elég 0-tól $m-1$-ig keresni (a példában 0-tól 9-ig).
A legegyszerűbb megoldás nyilván a kimerítő keresés (brute force): 0-tól $m-1$-ig minden $x$-re megvizsgáljuk, hogy igaz-e az egyenlet. Ez azonban nagy $m$-ekre kivitelezhetetlen. Ilyenkor visszavezetjük a megoldást lineáris diofantikus egyenletre. A kongruencia definíciója alapján átírva:

$$\begin{aligned} ax &\equiv b \pmod{m} \\ m &\mid b - ax \\ my &= b - ax \\ ax + my &= b, \end{aligned}$$

ami egy lineáris kongruencia, amit a fenti módon tudunk megoldani (és itt csak $x$ érdekel bennünket, így a bővített euklideszi algoritmusban is elég csak az $x$-es oszlopot számolni).
A példaegyenletünk ekvivalens a

$$7x + 10y = 3$$

lineáris diofantikus egyenlettel, amelynek a megoldása a fenti módszerrel (csak $x$-et nézve) valóban:

$$x = 9 + 10k.$$

# 6 Feladatok (papíron)

1. Számítsuk ki 25 és 32 legnagyobb közös osztóját, és írjuk fel a két szám lineáris kombinációjaként.
2. Oldjuk meg a $25x + 32y = 3$ egyenletet az egész számok körében. (Vagyis: írjuk fel az összes megoldást.)
3. Oldjuk meg a $25x \equiv 3 \pmod{32}$ kongruenciát.