SZÁMELMÉLET ELŐADÁS
Összefoglaló

2024. Február 27.

1. Diofantikus egyenlet

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

1.1. 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. ■

Az 1.3.5 Tétel fontos következménye az $ax+by = c$ kétismeretlenes lineáris diofantikus egyenlet megoldhatóságára vonatkozó alábbi tétel. Diofantikus egyenletnek általában olyan egész együtthatós algebrai egyenletet nevezünk, melynek a megoldásait is az egész számok körében keressük. A fenti $ax+by = c$ egyenletben tehát a, b, c rögzített egész számok, és megoldáson egy x, y egész számpárt értünk.

1.2. Tétel (FGY: 1.3.6). *Legyenek a, b, c rögzített egész számok. Az $ax + by = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha $(a, b) \mid c$.*

Az 1.3.6 Tételt kiegészíthetjük azzal, hogy megoldhatóság esetén az euklideszi algoritmus egyúttal eljárást is szolgáltat a lineáris diofantikus egyenlet (egyik) megoldásának a megkereséséhez.

1.1. Definíció. *Az $a_1, a_2, \ldots, a_k$ számok relatív prímek, ha nincs egységtől különböző közös osztójuk, azaz $(a_1, a_2, \ldots, a_k) = 1$.*

1.2. Definíció. *Az $a_1, a_2, \ldots, a_k$ számok páronként relatív prímek, ha közülük semelyik kettőnek sincs egységtől különböző közös osztója, azaz minden $1 \leq i \neq j \leq k$ esetén $(a_i, a_j) = 1$.*

Nyilvánvaló, hogy a páronként relatív prím számok egyúttal relatív prímek is, de ez ($k > 2$ esetén) megfordítva nem igaz.

1.3. Tétel. *Ha $c \mid ab$ és $(a, c) = 1$, akkor $c \mid b$.*

1.2. Bizonyítás. *Nyilván elég arra az esetre szorítkoznunk, ha a, b és c pozitív. Ekkor a $c \mid ab$ és $c \mid cb$ oszthatóságokból a legnagyobb közös osztó kitüntetett tulajdonsága, valamint az 1.3.4 Tétel alapján következik, hogy*

$$c \mid (ab, cb) = (a, c)b = b. \quad \blacksquare$$

2. Felbonthatatlan szám és prímszám

2.1. Definíció (Felbonthatatlan szám, FGY 1.4.1). *A p egységtől (és nullától) különböző számot felbonthatatlan számnak nevezzük, ha csak úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység. Azaz*

$$p = ab \implies a \text{ vagy } b \text{ egység.}$$

2.2. Definíció (prímszám, FGY 1.4.2). *A p egységtől (és nullától) különböző számot prímszámnak (röviden prímnek) nevezzük, ha csak úgy lehet osztója két egész szám szorzatának, ha legalább az egyik tényezőnek osztója. Azaz*

$$p \mid ab \implies p \mid a \text{ vagy } p \mid b.$$

2.1. Tétel (1.4.3). *Az egész számok körében p akkor és csak akkor prím, ha felbonthatatlan.*

2.1. Bizonyítás. *Nyilván feltehető, hogy p nem nulla és nem egység.*

I. Először tegyük fel, hogy p prím, és lássuk be, hogy felbonthatatlan is. Induljunk ki egy $p = ab$ szorzat-előállításból; azt kell igazolnunk, hogy a és b valamelyike egység.
Mivel $p = ab$, így $p \mid ab$ is igaz. Mivel p prím, ezért ebből $p \mid a$ vagy $p \mid b$ következik. Az első esetben $ab \mid a$, tehát ($a \neq 0$ miatt) $b \mid 1$, vagyis b egység, a második esetben pedig ugyanígy kapjuk, hogy a egység.

II. Most tegyük fel, hogy p felbonthatatlan, és lássuk be, hogy prím is. Induljunk ki egy $p \mid ab$ oszthatóságból; azt kell igazolnunk, hogy $p \mid a$ és $p \mid b$ közül legalább az egyik teljesül.

Ha $p \mid a$, akkor készen vagyunk. Hap $\nmid a$, akkor p felbonthatatlansága és $(p, a) \mid p$ miatt $(p, a) = 1$. A $p \mid ab$ és$(p, a) = 1$ feltételekből az 1.3.9 Tétel alapján $p \mid b$ következik. ■

Ezzel megmutattuk, hogy az egészek körében a felbonthatatlan számok és a prímszámok egybeesnek. A két fogalom azonban sok más számkörben nem ekvivalens. Például a páros számok körében a 6 felbonthatatlan, hiszen egyáltalán nem bontható két páros szám szorzatára, azonban nem prím, mert osztója a $18 \cdot 2$ szorzatnak, de nem osztja egyik tényezőt sem.

Az egészek körében a prímszámok vizsgálata a számelmélet egyik legfontosabb területe. Már Euklidész bebizonyította, hogy végtelen sok prímszám létezik, ugyanakkor a prímszámokkal kapcsolatban rengeteg az olyan egyszerűen megfogalmazható probléma, amely még ma is megoldatlan.

2.2. Tétel (A számelmélet alaptétele, 1.5.1). *Minden, a 0-tól és egységektől különböző egész szám felbontható véges sok felbonthatatlan szám szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű. (Az egyértelműség azt jelenti, hogy ha*

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

ahol a p_i és q_j számok valamennyien felbonthatatlanok, akkor $r = s$, és a p_i és q_j számok párba állíthatók úgy, hogy mindegyik p_i a hozzá tartozó q_j-nek egységszerese.) ■

2.1. Megjegyzés. *1. A 0-t és az egységeket azért kellett kizárni, mert azok egyáltalán nem bonthatók fel felbonthatatlan számok szorzatára: az egységek csak úgy írhatók fel szorzatként, hogy minden tényező egység, a 0 pedig csak úgy, hogy legalább az egyik tényező 0 (és akkor ez a tényező nem felbonthatatlan).*

2. Magukra a felbonthatatlan számokra a tétel olyan formában érvényes, hogy ezeket egytényezős szorzatoknak tekintjük.
3. A tétel kimondásánál mindenképpen a felbonthatatlan szám fogalmát érdemes használni, hiszen a tétel éppen azt fejezi ki, hogy ilyen „építőkövekből" lényegében minden szám lényegében egyértelműen „összerakható". A bizonyítás során is meg fogjuk különböztetni a felbonthatatlan és a prím fogalmát. Ezek ekvivalenciája - amint látni fogjuk - szoros összefüggésben áll a számelmélet alaptételének az érvényességével.
4. Sok számkörben (illetve integritási tartományban) nem érvényes a számelmélet alaptétele. Például a páros számok körében a 100*-nak két lényegesen különböző felbontása létezik felbonthatatlanok szorzatára:* $100 = 2 \cdot 50 = 10 \cdot 10$.

FGY: Freud-Gyarmati: Számelmélet. Nemzeti Tankönyvkiadó Rt., Budapest, 2000.
FL: Fuchs László: Bevezetés az algebrába és a számelméletbe I. Tankönyvkiadó, Budapest, 1964.

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