1. Oszthatóság

Szorzatra bontás

Oldjuk meg az $x^3 - 19x + 30 = 0$ egyenletet.

$x^3 - 19x + 30 = (x-2)(x-3)(x+5)$, így a megoldások 2, 3, -5. Ha már tudunk egy megoldást, a gyöktényező kiemelhető (Horner). De hogyan lehet megtippelni egy gyököt?

Ha d gyök, akkor $d(d^2 - 19) = d^3 - 19d = -30$. Így ha d egész szám, akkor osztója a 30-nak. Vagyis a 30 osztóit érdemes kipróbálni.

Középiskola: $30 = 2 \cdot 3 \cdot 5$ a prímszámokra való felbontás. Ezért a lehetséges osztók: 1, 2, 3, 5, $2 \cdot 3$, $2 \cdot 5$, $3 \cdot 5$, $2 \cdot 3 \cdot 5$, valamint ezek ellentettjei. Honnan tudjuk, hogy nincs más osztó?
Mik $x^3 - 19x + 30$ osztói $\mathbb{R}[x]$-ben? Hány normált osztója van?
Válasz: *a számelmélet alaptétele* (egész számokra és polinomokra).

Oszthatóság számokra és polinomokra

Definíció (FGy1.1.1)
Azt mondjuk, hogy a b egész szám *osztója* az a egész számnak, ha van olyan q egész szám, hogy $a = bq$. Jele: $b \mid a$. Ilyenkor a *többszöröse* b-nek. Ha b nem osztója a-nak, annak jele $b \nmid a$.

A nullának minden szám osztója. A nulla csak önmagának osztója.

Definíció (K3.1.3)
Azt mondjuk, hogy $g \in \mathbb{R}[x]$ *osztója* az $f \in \mathbb{R}[x]$ polinomnak, ha van olyan $q \in \mathbb{R}[x]$, hogy $f = gq$. Jele: $g \mid f$. Ha g nem osztója f-nek, annak jele $g \nmid f$.

Példa: $x + 1 \mid x^2 - 1$, hiszen $x^2 - 1 = (x+1)(x-1)$.
$2x \mid 3x^2$, hiszen $3x^2 = 2x\big((3/2)x\big)$ és $(3/2)x \in \mathbb{R}[x]$.
$x \nmid x + 1$, mert ha volna olyan $q \in \mathbb{R}[x]$, hogy $x + 1 = xq(x)$, akkor $x = 0$-t helyettesítve $1 = 0$ adódna.

Prímekre bontás pozitív egészekre

Középiskolában így tanultuk
Egy $p > 1$ egész szám prímszám, ha csak 2 pozitív osztója van: 1 és önmaga. Minden 1-nél nagyobb egész szám *sorrendtől eltekintve egyértelműen* felírható prímszámok szorzataként.

Az egyértelműség azon múlik, hogy ha p prímszám, és $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$. Ez a *prímtulajdonság*. A következő dián igazoljuk ezt a tulajdonságot az alsó tagozaton tanult *maradékos osztás* segítségével.

A polinomok egész gyökeinek meghatározásához a *negatív osztókat* is figyelembe kell venni, például $x^3 - 19x + 30$-nak különben kifelejtenénk a -5 gyökét.

Ezért a későbbi diákon módosítjuk a fenti fogalmakat úgy, hogy negatív egészekre is és polinomokra is jól működjenek.

A prímtulajdonság bizonyítása

Tétel (FGy1.4.3)
Ha $p > 1$-nek csak 2 osztója van: 1 és önmaga, akkor *prímtulajdonságú*: $p \mid ab$ esetén $p \mid a$ vagy $p \mid b$.

Tegyük fel, hogy p nem osztója sem a-nak, sem b-nek, és erre azt a példát választottuk, ahol ab a lehető legkisebb. Tehát van egy $a \times b$ oldalú téglalap egy kockás papíron, amelynek a területe osztható p-vel.
Ha $a > p$ lenne, akkor egy $p \times b$-s csíkot levágva kisebb ellenpéldát kapnánk. Ezért $a < p$, és hasonlóan $b < p$.

Vegyünk egy $p \times b$-s téglalapot, és vagdossunk le $a \times b$-s csíkokat, ameddig lehet. Egy $r \times b$-s téglalap marad, ahol $r < a$, ennek a területe is osztható p-vel. Ha $r = 0$ lenne, akkor $a \mid p$, de p felbonthatatlan és $a < p$, tehát $a = 1$, azaz $p \mid ab = b$. Ha $r \neq 0$, akkor $rb < ab$ ellentmond ab minimalitásának. □
Kulcs: a $(p : a)$ *maradékos osztás* (ahol r a maradék).

Az oszthatóság tulajdonságai

Állítás (FGy1.1.5)
Legyenek a, b, c tetszőleges egész számok (negatívak is lehetnek).

(1) Minden a-ra $a \mid a$ (*reflexivitás*).

(2) Ha $a \mid b$ és $b \mid c$, akkor $a \mid c$ (*tranzitivitás*).

(3) Ha $a \mid b$ és $a \mid c$, akkor $a \mid b + c$.

(4) Ha $a \mid b$, akkor $a \mid kb$, sőt $ka \mid kb$ minden k egészre. Megfordítva, ha $k \neq 0$, akkor $ka \mid kb$-ből $a \mid b$ következik.

HF, K3.1.4: Igazoljuk a fentieket számok helyett polinomokra is.

Az oszthatóság *nem szimmetrikus*: $a \mid b$-ből nem következik $b \mid a$. Például $2 \mid 4$, de $4 \nmid 2$.
HF: Ha $a \mid b$ és $b \mid a$, akkor a és b oszthatóság szempontjából egyformán viselkednek: ugyanazok az osztóik is, a többszöröseik is.

2. Egységek és felbonthatatlanok

Asszociáltak és egységek

Definíció (vö. K3.1.7)
Az a és b egész számok *asszociáltak*, ha egymás osztói, jele $a \sim b$.

Definíció (FGy1.1.2)
Az e egész szám *egység*, ha minden egész számnak osztója.
HF: Ehhez elegendő feltenni, hogy $e \mid 1$.

Tétel (FGy1.1.3), HF
Az egész számok között az egységek az 1 és a -1.

Tétel (FGy1.1.5/(iii), K3.1.10), HF
Két egész szám akkor és csak akkor asszociált, ha egymás egységszeresei, vagyis ha egyenlők vagy ellentettek.

Egységek a polinomok között

Definíció (K3.1.9)
Azt mondjuk, hogy a $g \in \mathbb{R}[x]$ polinom *egység*, ha minden $\mathbb{R}[x]$-beli polinomnak osztója.

Állítás (K3.1.11)
$\mathbb{R}[x]$ egységei a nem nulla konstans polinomok.

Bizonyítás
Egy $g(x) \in \mathbb{R}[x]$ polinom pontosan akkor egység, ha osztója a konstans 1 polinomnak, azaz ha van reciproka $\mathbb{R}[x]$-ben. Korábban beláttuk, hogy ezek pontosan a nem nulla konstans polinomok. □

HF: $\mathbb{C}[x]$ és $\mathbb{Q}[x]$ egységei is a nem nulla konstans polinomok, míg $\mathbb{Z}[x]$ egységei csak a ± 1 konstansok.

3. Felbonthatatlanok és prímek

Egyértelmű felbontás és egységek

A 6 szám „egyetlen” szorzatra bontása $6 = 2 \cdot 3$. De valójában
$6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$. Sőt még
$6 = 1 \cdot 6 = 6 \cdot 1 = (-1) \cdot (-6) = (-6) \cdot (-1)$.
Tehát az „egyetlen” felbontás valójában nyolcféle. Az első négy felbontás csak a tényezők *sorrendjében*, illetve *egységszeresben* különbözik. A második négy pedig „nem érdekes”, *triviális*, mert egységet emeltünk ki.

Definíció (K3.1.12)
Az $a = bc$ felbontás *triviális*, ha a és b valamelyike egység.

Az $a \in \mathbb{Z}$ triviális felbontásai $a = 1 \cdot a = a \cdot 1 = (-1) \cdot (-a) = a \cdot (-1)$. Ha e egység, akkor van olyan f, hogy $ef = 1$. Ekkor az a egy triviális felbontása: $a = (af)e$.
Példa: $x^2 + 1 = (3/2)\big((2/3)x^2 + (2/3)\big)$ egy triviális felbontás.

Felbonthatatlan számok

Definíció (FGy1.4.1)
A p egész szám *felbonthatatlan*, ha nem nulla, nem egység, és nincs nemtriviális felbontása. Másképp: p-nek pontosan négy osztója van az egészek között: 1, -1, p és $-p$.

$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \ldots$. Ezeket (pontosabban közülük a pozitívakat) középiskolában prímszámnak hívtuk, mert láttuk, hogy *prímtulajdonságúak*.

Tétel (FGy1.4.3, beláttuk)
Ha $p \in \mathbb{Z}$ felbonthatatlan, és $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$.

Adunk egy (első olvasásra kihagyható, nehezebb) példát, ami mutatja, hogy ez a tétel miért nem nyilvánvaló. A tételt később levezetjük a legnagyobb közös osztó tulajdonságaiból is.

Példa nem prím felbonthatatlanra*
Adott n egészre keressük az $x^2 + 5y^2 = n$ egész x, y megoldásait. Ehhez az $a + bi\sqrt{5}$ alakú számok R halmazát érdemes vizsgálni, ahol $a, b \in \mathbb{Z}$. Ezek körében ugyanúgy definálható az oszthatóság, mint egészekre és polinomokra, és a tulajdonságai is hasonlóak. Nyilván $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.

Állítás (F10.3.5, K3.1.34)
R-ben az egységek csak a ± 1. A 2, 3 és $1 \pm i\sqrt{5}$ is felbonthatatlan, és páronként nem asszociáltak. A 3 nem prímtulajdonságú, mert osztója $(1 + i\sqrt{5})(1 - i\sqrt{5})$-nek, de nem osztója egyik tényezőnek sem.

A bizonyítás ötlete: Legyen $N(a + bi\sqrt{5}) = a^2 + 5b^2$. Ekkor $\alpha, \beta \in R$ esetén $N(\alpha\beta) = N(\alpha)N(\beta)$. Ezért ha $\alpha = a + bi\sqrt{5}$ egység, akkor $a^2 + 5b^2 = 1$, így $\alpha = \pm 1$. Ha $3 = \alpha\beta$, akkor $9 = N(3) = N(\alpha)N(\beta)$. De $a^2 + 5b^2 \neq 3$.

4. A maradékos osztás

A maradékos osztás tétele egész számokra

Tétel (FGy1.2.1)
Ha a, b egész számok, és $b \neq 0$, akkor van olyan q és r egész, hogy $a = bq + r$ és $0 \leq r < |b|$. Ez a q és r egyértelmű.

Itt a az *osztandó*, b az *osztó*, q a *hányados*, r a *maradék*. Alsó tagozaton tanultuk, hogy az osztás tényleg elvégezhető.

Bizonyítás (létezés)
Tekintsük az $\ldots, a - 2b, a - b, a, a + b, a + 2b, \ldots$ sorozatot. Analízisből tudjuk, hogy ez nem korlátos sem alulról, sem fölülről, ezért van két olyan szomszédos tagja, ami közrefogja a nullát. Ha $b > 0$, $a - b(q - 1) < 0$, de $a - bq \geq 0$, akkor ez a q és $r = a - bq$ megfelelő, hiszen $a - b(q - 1) = r - b < 0$. Ha $b < 0$, $a - b(q + 1) < 0$, de $a - bq \geq 0$, akkor ez a q és $r = a - bq$ megfelelő, mert $a - b(q + 1) = r + b = r - |b| < 0$.

A maradékos osztás egyértelműsége

Tétel (FGy1.2.1)
Ha a, b egész számok, és $b \neq 0$, akkor van olyan q és r egész, hogy $a = bq + r$ és $0 \leq r < |b|$. Ez a q és r egyértelmű.

Bizonyítás (egyértelműség)
Ha $a = bq_1 + r_1$ és $a = bq_2 + r_2$, ahol $0 \leq r_1, r_2 < |b|$, akkor $b(q_1 - q_2) = r_2 - r_1$.
De $|r_2 - r_1| < |b|$ és $|b(q_1 - q_2)| \geq |b|$, kivéve ha $q_1 - q_2 = 0$.
Ekkor $r_1 = a - q_1 b = a - q_2 b = r_2$. □

Néha hasznos úgy osztani, hogy a maradék lehessen negatív is, és az abszolút értéke legyen a lehető legkisebb. Elérhető, hogy $|r| \leq |b|/2$ teljesüljön (FGy1.2.1A, HF.)

A valós együtthatós polinomok körében is elvégezhető a maradékos osztás. Ezzel a témával később foglalkozunk (K3.2.1).

5. Összefoglaló

A 8. előadáshoz tartozó vizsgaanyag

Fogalmak
Oszthatóság számokra és polinomokra (FGy1.1.1, K3.1.3). Asszociált, egység (FGy1.1.2, K3.1.7, K3.1.9). Triviális felbontás (K3.1.12). Felbonthatatlan szám, prímtulajdonság (FGy1.4.1, 1.4.2).

Tételek
Oszthatóság (FGy1.1.5, K3.1.4). Asszociáltak és egységek (FGy1.1.3, 1.1.5/(iii), K3.1.10, 3.1.11). Felbonthatatlan egész prím (FGy1.4.3). Maradékos osztás (FGy1.2.1).