Számelmélet, kémia, Boole-algebrák

Haladvány Kiadvány 131107.pdf

Szalkai István
Pannon Egyetem, Matematika Tanszék, Veszprém
szalkai@almos.uni-pannon.hu

0. Bevezetés

Egyszerűsége ellenére az elemi számelmélet sok diáknak okoz nehézséget, tanításukhoz próbálunk segítséget nyújtani. Nem a számelmélet alapjait írjuk le (azt ismertnek tételezzük fel), hanem csak az új szemléletmódunkat, ami nem csak a szokatlan $\mathfrak{p}(n)$ és Δ és ∇ jelölésekből[1)] áll, és néhány részlet fontosságát emeljük ki. (A témát részletesebben mutatja be [2011].)

Például legtöbb diáknak (és felnőttnek) a prímszámokról csak annyi jut eszébe, hogy "*csak* 1 *-gyel és önmagával osztható*". Ez ugyan igaz, hasonlóan a kémiai atomokhoz, de nem ez a prímszámok lényege, hanem a Számelmélet Alaptétele, a prímfelbontás és a maradékok, ami szintén szemléltethető a kémiai molekulák atomokból történő felépítéséhez. A Boole algebrák, polinomok és a $\mathbb{Z}[\alpha]$ halmazok is segíthetik a szemléltetést (4. és 5. fejezetek).

Sajnos a prímfelbontás már 5-6 jegyű számokkal sem egyszerű számológéppel, nagyobb számokkal pedig a számítógépek is évmilliókig (!) számolnának.

A cikk nagy része általános és középiskolás diákoknak is elmondható. Sajnos találkoztam olyan diákokkal is, akik nem szerették a kémiát, ezirányú gondolataimat nem is hallgatták tovább.

A cikkben említett gondolatok nem újak, csak még kevesen ismerik őket!

Egész számok oszthatóságánál az előjel nyilván nem lényeges, ezért elegendő csak a nemnegatív (azaz természetes) számokkal foglalkoznunk. Tehát "szám" alatt ezután *természetes számot* értünk.

[1)] ld. 7. és 15. Definíciók

1. lnko(lkkt(a,b),lkkt(b,c),lkkt(c,a)) = = lkkt(lnko(a,b),lnko(b,c),lnko(c,a))

Kezdjük a KöMaL **B. 4493.** feladatával:

Jelölje az n és k pozitív egészek *legnagyobb közös osztóját* (n,k), *legkisebb közös többszörösét* pedig $[n,k]$. Mutassuk meg, hogy tetszőleges a, b, c pozitív egészek esetén az $[a,b]$, $[b,c]$, $[c,a]$ számok legnagyobb közös osztója megegyezik az (a,b), (b,c), (c,a) számok legkisebb közös többszörösével.

A szokásos megoldást [2013K]-ban megtaláljuk. Az *lnko* és *lkkt* szokásos (iskolai) számolása a prímosztók kitevőinek, vagyis a prímtényezők *darabszám* szerinti (multiplicitással) "leltározása" alapján történik, ami alapján kézenfekvő a halmazműveletekkel való kapcsolat részletesebb megvizsgálása: *lnko* $= \cap$ és *lkkt* $= \cup$.

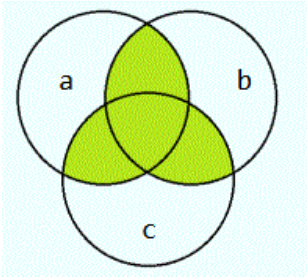
A feladat állítása:

$$([a,b],[b,c],[c,a]) = [(a,b),(b,c),(c,a)] \ ,$$

ami halmazműveletekkel:

$$(a \cup b) \cap (b \cup c) \cap (c \cup a) = (a \cap b) \cup (b \cap c) \cup (c \cap a) \ .$$

Ez utóbbit könnyen igazolhatjuk akár Venn diagrammal:



vagy használhatjuk pl. [2012] számoló-rajzoló programját, vagy szokásos levezetéssel:

$(a \cup b) \cap (b \cup c) \cap (c \cup a) = (b \cup (a \cap c)) \cap (a \cup c) = (b \cap (a \cup c)) \cup (a \cap c \cap (a \cup c))$
$= (b \cap (a \cup c)) \cup (a \cap c) = (b \cap a) \cup (b \cap c) \cup (a \cap c)$. $\square$

Vegyük észre, hogy itt csak az $\cup$ és $\cap$ szokásos tulajdonságait használtuk fel: **kommutatív, asszociatív, disztributív, elnyelési tulajdonságok, idempotencia** (pl. [2001] és [2013w]). Ezek azonban egyszerű és

fontos tételek a számelméletben, bizonyítás után bármikor automatikusan alkalmazhatjuk őket, mint a fenti levezetésben. Például az (egyik) disztributivitási szabálynak

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c) \tag{1}$$

megfelel

$$lkkt\,(a\ ,\ lnko\,(b,c)) = lnko\,(lkkt\,(a,b)\ \ ,\ lkkt\,(a,c))\ \ , \tag{2}$$

az (egyik) elnyelési szabályból

$$a \cap (a \cup b) = a \tag{3}$$

pedig

$$lnko\,(a\ ,\ lkkt\,(a,b)) = a \tag{4}$$

lesz. Az (2), (4) egyenlőségeket akár írhatnánk

$$a\nabla\,(b\Delta c) = (a\nabla b)\,\Delta\,(a\nabla c) \tag{5}$$

ill.

$$a\Delta\,(a\nabla b) = a$$

alakban is: Δ és ∇ jelöli *lnko* -t illetve *lkkt* -t. (Javasoljuk Olvasónak, hogy a Boole algebrák többi axiómáját is írja fel *lnko* és *lkkt* segítségével, akár a szokásos, akár az Δ , ∇ jelekkel, sőt állítjuk, be is tudja bizonyítani ezeket az "új" összefüggéseket.) További részleteket találhatunk [**?**] és [2011] -ben.

A *komplementer* művelet sajnos már nem ilyen egyszerű: rögzítenünk kell egy tetszőleges *négyzetmentes* N számot (N -nek nincs négyzet-osztója), és csak N osztóinak D_N halmazára szorítkozhatunk. *lnko* és *lkkt* a szokásos, továbbá egy $x \in D_N$ (vagyis $x \mid N$) szám **komplementere** az $\frac{N}{x} \in D_N$ szám. A D_N halmazban ekkor a Boole-algebrák (halmazműveletek) *összes* axiómája teljesül (pl. [2001] vagy [2013w]), például az (egyik) De Morgan azonosság:

$$\overline{a\nabla b} = \overline{a}\ \Delta\ \overline{b} \tag{6}$$

vagyis

$$\frac{N}{lkkt\,(a,b)} = lnko\left(\frac{N}{a}, \frac{N}{b}\right)\ . \tag{7}$$

Érdemes lenne megismerkednünk még a *Dualitás* és *Teljesség* elveivel, további Boole-algebrákkal (pl.[2001], [2013w]) és kémiai (!) alapokkal.

2. Számok és molekulák

Csak a teljesség igénye miatt írjuk le a jólismert meghatározást:

1. Definíció. *A $p \in \mathbb{N}$ egész számot ($p \neq 1,\ 0$) **prímszám**nak (=primitív szám) röviden **prím**nek, vagy törzsszámnak nevezünk, ha **irreducibilis** (**felbonthatatlan**), azaz nem írható fel két nála kisebb szám szorzataként.* □

ami nem tévesztendő össze a *prímtulajdonsággal*:

2. Definíció. *Egy $x \in \mathbb{N}$ egész számot ($x \neq 1,\ 0$) **prímtulajdonságú**nak nevezünk, ha tetszőleges $u, v \in \mathbb{N}$ számok esetén $x \mid uv$ -ből $x \mid u$ vagy $x \mid v$ következik.* □

$\mathbb{N}$ -ben[2] ugyan ez a két fogalom egybeesik, a 10. Állítás alapján könnyen belátható, de az 5. fejezetben látunk olyan struktúrákat is, ahol különbözőek.

3. Megjegyzés. *Az 1. és 2. Definíciókból ki kellett zárnunk az* 1*-et és a* 0*-át, mert egészen más tulajdonságokkal rendelkeznek mint a prímszámok.*

Azonban a prímszámok legfontosabb tulajdonsága *nem* felbonthatatlanságuk, hanem az, hogy minden egész szám *lényegében egyértelmű módon* (sorrendtől eltekintve) előállítható belőlük (ld. 5. Tétel), HASONLÓAN ahogyan a molekulák (kémiai) atomokból épülnek fel az öszegképletben. Ezt a szemléletet szeretnénk erősíteni a diákokban a kémai hasonlattal.

4. Megjegyzés. *Mivel a prímszámok tovább már nem osztható számok, ezért **atom**oknak is nevezhetnénk őket, hiszen görögül éppen "*oszthatatlant*" jelent az* atomosz *szó! A molekulákat atomok építik fel - a természetes számokat prímszámok. A molekulák összegképlete megegyezik az (8) képlettel, ezért az (8) képletet hívhatnánk az $n \in \mathbb{N}$ szám* összegképletének *is* [3].

5. Tétel. ***Számelmélet Alaptétele:*** *Minden $n \in \mathbb{N}$, $n \neq 0$ egész szám felbontható ("**faktorizálható**") prímszámok szorzatára, lényegében egyértelműen (azaz csak a tényezők sorrendjében és előjelekben lehet eltérés).* □

[2] és minden Euklideszi gyűrűben (39. Definíció)

[3] "Sajnos" a prímszámok száma végtelen (Euklidesz), tehát nem csak a periodikus rendszerben található pár tucat atomunk van. Szerencsére azonban *szerkezeti képlet* a matematikában nincs.

Az előbbi tétel szerint tehát minden $n \in \mathbb{Z}$, $|n| > 1$ egész szám felírható

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \tag{8}$$

alakban, ahol a $p_i \in \mathbb{P}$ számok páronként különböző prímszámok, és $\alpha_i \geq 1$, ez az előállítás lényegében egyértelmű. Ezt alkalmazzuk a legtöbb számelméleti feladat megoldásakor.

Gyermekeimet már általános iskolában is arra neveltem, ha természetes szám és oszthatóság szerepel a feladatban, akkor kezdjék a prímfelbontással.

6. Megjegyzés. *Igen ám, de még zsebszámológéppel is legfeljebb 3-4 jegyű számokat tudunk felbontani! A 3. fejezetben részletesebben elemezzük, hogy már* 30 *jegyű számokat* $5\,GHz$ *-es számítógépek is csak évmilliók alatt képesek felbontani! (A [2011] könyv egésze is ezzel a kérdéssel foglalkozik.)*

Pedagógiailag sokszor segített a következő jelölés is:

7. Definíció. *Tetszőleges* $n \in \mathbb{N}$, $n \geq 1$ *egész számra* $\mathfrak{p}(\mathbf{n})$ *jelölje az (8) egyenlőségben szereplő prímszámok "**multihalmazát**" multiplicitással, vagyis*

$$\mathfrak{p}(n) := \{p_1, ..., p_1, p_2, ..., p_2, \quad ... \quad , p_r, ..., p_r\} \ , \tag{9}$$

$\mathfrak{p}(n)$*-ben a* p_i *prímszám pontosan* α_i*-szer szerepel az (8) egyenlőség esetén.*□

Például $\mathfrak{p}(12) = \{2, 2, 3\}$ és $\mathfrak{p}(1) = \varnothing$, mint ahogyan $\mathfrak{p}(víz) = \{H, H, O\}$ és $\mathfrak{p}(semmi) = \varnothing$.

8. Megjegyzés. *Negatív* $n \in \mathbb{Z}$ *számokra is ki lehetne terjeszteni a* $\mathfrak{p}(n)$ *jelölést, de sok probléma merülne fel, feleslegesen ezzel nem foglalkozunk.*

A $\mathfrak{p}(0)$ *(multi)halmazt ugyancsak nem definiáljuk, hiszen az* $n = 0$ *számnak nincs törzstényezős felbontása, de szerencsére szükségünk sem lesz rá.*

Persze $\mathfrak{p}(n)$ legtöbbször nem halmaz, mert elemei többször is szerepelhetnek benne, a "multihalmaz" precíz általános definíciójától most eltekintünk. Szükségünk lesz azonban multihalmazok "*szokásos-*" és "*multi-*" műveleteire:

9. Definíció. *Tetszőleges* $\mathfrak{a} = \{p_1..., p_2..., \ , ..., p_r\}$ *és* $\mathfrak{b} = \{p_1..., p_2..., \ , ..., p_r\}$ *multihalmazokra, ha* $p_i \quad \mathfrak{a}$ *-ban pontosan* α_i *-szer szerepel és* $\mathfrak{b}$ *-ben pontosan* β_j *-szer szerepel (*$0 \leq \alpha_i, \beta_i$*), akkor legyen*
$\mathfrak{a} \cup \mathfrak{b} :=$ *a **halmazelméleti únió**:*

$a\ p_i$ *elem pontosan* $\max\{\alpha_i, \beta_i\}$ *-szer szerepel,*

$\mathfrak{a} \Cup \mathfrak{b} :=$ *a* ***multihalmazelméleti únió****:*

$a\ p_i$ *elem pontosan* $\alpha_i + \beta_i$ *-szer szerepel,*

$\mathfrak{a} \cap \mathfrak{b} :=$ *a* ***halmazelméleti metszet****:*

$a\ p_i$ *elem pontosan* $\min\{\alpha_i, \beta_i\}$ *-szer szerepel.* $\square$

A *multihalmazok* között nincs komplementer, mert minden $\mathfrak{a}$ multihalmazra $\mathbb{P}\backslash\mathfrak{a}$ nem véges halmaz, a *multimetszet*nek sincs értelme.

Könnyen láthatóak az alábbi hasznos tulajdonságok:

10. Állítás. Tetszőleges $n, m \in \mathbb{N}$, $n, m \geq 1$ *természetes számokra*

$$n \in \mathbb{P} \iff \mathfrak{p}(n) = \{n\} \tag{10}$$

$$\mathfrak{p}(n \cdot m) = \mathfrak{p}(n) \Cup \mathfrak{p}(m) \ , \tag{11}$$

$$n \mid m \quad \iff \quad \mathfrak{p}(n) \subseteq \mathfrak{p}(n) \ , \tag{12}$$

és $n \mid m$ *esetén*

$$\mathfrak{p}\left(\frac{m}{n}\right) = \mathfrak{p}(m) \ \setminus \ \mathfrak{p}(n) \ . \quad \square \tag{13}$$

Továbbá

11. Tétel. *Tetszőleges* $n, m \in \mathbb{N}$ *számokra*

$$lnko(n, m) = \mathfrak{p}(n) \cap \mathfrak{p}(m) \ ,$$
$$lkkt(n, m) = \mathfrak{p}(n) \cup \mathfrak{p}(m) \ ,$$

sőt tetszőleges $a_1, \ldots, a_t \in \mathbb{N}$ *számokra*

$$lnko(a_1, \ldots, a_t) = \mathfrak{p}(a_1) \cap \ldots \cap \ \mathfrak{p}(a_t) \ ,$$
$$lkkt(a_1, \ldots, a_t) = \mathfrak{p}(a_1) \cup \ldots \cup \ \mathfrak{p}(a_t) \ . \qquad \square$$

hiszen

12. Tétel. *Legyen* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *és* $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ *ahol* $0 \leq \alpha_i$, β_i . *Ekkor*

$$lnko(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_r^{\min(\alpha_r, \beta_r)} \ , \tag{14}$$
$$lkkt(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \ldots \cdot p_r^{\max(\alpha_r, \beta_r)} \ .$$

Hasonlóan több számra:

$$lnko(a,b,\ldots,z) = p_1^{\min(\alpha_1,\ldots,\omega_1)} \cdot p_2^{\min(\alpha_2,\ldots,\omega_2)} \cdot \ldots \cdot p_r^{\min(\alpha_r,\ldots,\omega_r)}$$
$$lkkt\,(a,b,\ldots,z) = p_1^{\max(\alpha_1,\ldots,\omega_1)} \cdot p_2^{\max(\alpha_2,\ldots,\omega_2)} \cdot \ldots \cdot p_r^{\max(\alpha_r,\ldots,\omega_r)}$$

ahol $\quad z = p_1^{\omega_1} p_2^{\omega_2} \cdots p_r^{\omega_r} \quad$ *és* $\quad 0 \leq \omega_i$. $\quad \square$

13. Megjegyzés. ***(i)*** *A 3. "Prímfelbontás a gyakorlatban" fejezetben említett algoritmikus problémák miatt a fenti képletek* csak elméleti jelentőségűek. *Felhívjuk a figyemet, hogy lnko és lkkt értékét a gyakorlatban mégis gyorsan ki lehet számítani egy másik módszerrel: Euklidesz algoritmusával, amit (további alkalmazásaival) [2011] 4.2. "Euklidesz algoritmusa" fejezetében ismertetünk.*
(ii) *A* ***legnagyobb közös osztó****t és* ***legkisebb közös többszörös****t nem kell definiálnunk. Bár széles körben elterjedtek az* (a,b) *és* $[a,b]$ *jelölések, mi* kizárólag *csak az* $lnko(a,b)$ *,* $lkkt(a,b)$ *jelöléseket használjuk az esetleges félreértések elkerülése végett.*

További, ismert és kevésbé ismert összefüggéseket új szemléletmódban találunk a következő fejezetben.

14. Megjegyzés. *Hangsúlyozzuk ismét, hogy a fenti felbontás alapján a legtöbb számelméleti kérdés és vizsgálat egyszerűnek tűnik, de maga a felbontás megkeresése közepesen nagy (egy-kétszáz -jegyű) számok esetén* évbilliókig *is eltarthat - még a "modern" több teraHz-es többmagos párhuzamos processzszorokkal működő szuperszámítógépekkel is! Ezeket a kérdéseket a 3. fejezetben (és [2011]-ben) vizsgáljuk.*

3. Boole algebrák

A 10. és 11. eredményekben már láttuk, hogy a számelméleti műveletek szoros kapcsolatban vannak a halmazműveletekkel: mindkettő *Boole-algebrát* alkot (19. Tétel). A "Boole algebra" szakkifejezést említenünk sem kell a gyerekeknek, de mi is könnyebben megjegyezzük a tételeket így. (A Boole algebrák definícióját és alapvető tulajdonságait megtaláljuk például a jelen cikk vagy [2011] Függelékében, [2001]-ben, vagy az interneten [2013w]-ben.)

A $\mathfrak{p}\,(a)$ és az alábbi Δ , ∇ jelölésekkel sok hasznos összefüggést sokkal könnyebben megérthetünk illetve megjegyezhetünk:

15. Definíció. *Tetszőleges $a, b \in \mathbb{Z}$ számok esetén legyen*

$$\mathbf{a\Delta b} := lnko(a,b) \ ,$$
$$\mathbf{a\nabla b} := lkkt(a,b) \ . \quad \square$$

Ugyanis: Δ és ∇ nemcsak kommutatív, hanem asszociatív és disztributív műveletek is:

16. Tétel. *Tetszőleges $a, b, c \in \mathbb{Z}$ számokra:*
kommutativitás:

$$a\Delta b = b\Delta a \quad azaz \quad lnko(a,b) = lnko(b,a) \ ,$$
$$a\nabla b = b\nabla a \quad azaz \quad lkkt(a,b) = lkkt(b,a) \ ,$$

asszociativitás:

$$(a\Delta b)\,\Delta c = a\Delta\,(b\Delta c) \ ,$$
$$[a\nabla b]\,\nabla c = a\nabla\,[b\nabla c] \ ,$$

hiszen

$$lnko\,(lnko(a,b)\ ,\ c) = lnko\,(a\ ,\ lnko(b,c)) \ ,$$
$$lkkt\,(lkkt\,(a,b)\ ,\ c) = lkkt\,(a\ ,\ lkkt\,(b,c)) \ ,$$

disztributivitás:

$$(a\Delta b)\,\nabla c = [a\nabla c]\,\Delta\,[b\nabla c] \ , \tag{15}$$
$$[a\nabla b]\,\Delta c = (a\Delta c)\,\nabla\,(b\Delta c) \ ,$$

azaz

$$lkkt\,(lnko\,(a,b)\,,c) = lnko\,(lkkt\,(a,c)\,,lkkt\,(b,c)) \ , \tag{16}$$
$$lnko\,(lkkt\,(a,b)\,,c) = lkkt\,(lnko\,(a,c)\,,lnko\,(b,c)) \ . \quad \square$$

Közeledünk a Boole-algebrához! A fenti összefüggések nem meglepőek: a 12. Tétel (14) klasszikus összefüggései. Az asszociativitás alapján tudjuk:

17. Tétel. ***(több szám)*** *Tetszőleges $a, b, c \in \mathbb{Z}$ számokra*

$$lnko(a,b,c) = lnko\,(lnko(a,b),c) = lnko\,(a,lnko(b,c)) \ ,$$
$$lkkt(a,b,c) = lkkt\,(lkkt(a,b),c) = lkkt\,(a,lkkt(b,c)) \ . \quad \square$$

A 19. Tételhez szükségünk van egy fogalomra:

18. Definíció. *Az $n \in \mathbb{Z}$ számot **négyzetmentes**nek nevezzük, ha prímfelbontásában minden prímosztója csak egyszer szerepel ($p_i^2 \nmid n$), azaz (8) -ben mindegyik $\alpha_i = 1$.* $\square$

$n \in \mathbb{N}$ nyilván pontosan akkor négyzetmentes, ha $\mathfrak{p}(n)$ "hagyományos" halmaz.

A $\mathfrak{p}(a)$ jelölés segítségével érthetjük meg *lnko* és *lkkt* (Δ és ∇) többi tulajdonságait is, amit legrövidebben az alábbi Tételben foglalhatunk össze:

19. Tétel. *Legyen $n \in \mathbb{N}$ egy tetszőleges négyzetmentes szám. Ekkor a*

$$\mathcal{D}_n := \left(\ D_n \ , \ lnko \ , \ lkkt \ , \ \frac{n}{x} \ , \ n \ , \ 1 \ \right)$$

*struktúra **Boole algebra**[4], ahol*

$$D_n := \{ \ n \text{ osztóinak halmaza } \} \ . \qquad \square$$

20. Példa. *Például a jól ismert $\overline{A \cup B} = \overline{A} \cap \overline{B}$ és $\overline{A \cap B} = \overline{A} \cup \overline{B}$ De Morgan azonosságok a számelmélet nyelvén:*

$$\frac{n}{lkkt\,(x,y)} = lnko\left(\frac{n}{x} \ , \ \frac{n}{y}\right) \quad \text{és} \quad \frac{n}{lnko\,(x,y)} = lkkt\left(\frac{n}{x} \ , \ \frac{n}{y}\right) \ . \quad \square$$

Érdemes a Boole algebrák többi axiómáit, valamint a **Dualitás Elvét** ([2001]) is felírni a számelmélet nyelvén. Még egy hasznos összefüggés:

21. Tétel. *Tetszőleges $a, b \in \mathbb{Z}$ esetén*

$$lkkt(a,b) = \frac{a \cdot b}{lnko(a,b)} \ . \qquad \square$$

[4] ld. Függelék

4. Prímfelbontás a gyakorlatban

Bár Eratoszthenesz "ikszelős" algoritmusa kicsit gyorsabbnak tűnik az "elosztom 2,3,5,7,... -tel" módszernél, sok különbség nincs közöttük.

22. Gyakorlat. ***(a)*** *Mennyi ideig fut az Eratoszthenészi szita-algoritmus egy k* ***-jegyű*** *input esetén, a $k = 20$, $k = 30$, $k = 40$ és $k = 50$, $k = 100$, ... esetekben egy* 5GHz *-es gépen futtatva (ha csak az osztásokat számítjuk egy-egy lépésnek, azaz feltételezzük, hogy a gép minden órajel alatt elvégez egy k -jegyű osztást (!) és ellenőrzést, vagyis másodpercenként $5 \cdot 10^9$ osztást) ?*
(b) *Mennyire csökkenne a futásidő, ha a $\sqrt{n}$ alatti prímszámokat egy tömbben (táblázatban) tárolnánk, és csak e prímszámokat próbálnánk ki ?*
(c) *Mi változna, ha mondjuk* 1000 *-szer gyorsabb gépünk lenne?*

Megoldás: ***(a)*** *Az osztások száma* $\frac{\sqrt{n}}{2} \approx 10^{k/2}$ *, ez*
k=20 esetén $5 \cdot 10^9$ *lépés = 1 mp ,*
k=30 esetén $5 \cdot 10^{14}$ *lépés =* 10^5 *mp* $\approx$ *27 óra 46 perc,*
k=40 esetén $5 \cdot 10^{19}$ *lépés =* 10^{10} *mp* $\approx$ *317 év 35 nap 18 óra,*
k=50 esetén $5 \cdot 10^{24}$ *lépés =* 10^{15} *mp* $\approx$ *31,7 millió év ,*
k=100 esetén $5 \cdot 10^{49}$ *lépés =* 10^{40} *mp* $\approx 3,17 \times 10^{23}$ milliárd év ... .
(c) *Semmi.* □

A [2011] könyvhöz mellékelt PRIM1D.EXE program éppen az Eratoszthenészi szitamódszer *lassúságát* szemlélteti: hűségesen végigpróbálgatja az összes, $\sqrt{n}$ -nél kisebb páratlan számot. Vigyázat: 10 jegyű számoknál már napokig fut a program! A [2011] könyv egyik célja éppen a lehetséges gyorsítások bemutatása.

Ha csak a prímszmokkal osztogatjuk az n számot, akkor sok esetben a prímek beolvasása fájlból még lassíthatja is a program futását összességében, hiszen pl. az egymilliomodik prímszám $p_{1000000} = 15\ 485\ 863$ még csak 8-jegyű ! (és ráadásul 1 -el kezdődik).

23. Megjegyzés. *A* ***Prímfelbontás problémára*** *(azaz tetszőleges $n \in \mathbb{N}$ számot bontsunk fel törzstényezőkre)* nem ismert *gyors (megvárható!) algoritmus.* □

Tehát óvatosan fogadjunk minden olyan tételt és képletet, amely használja a prímfelbontás (8) képletet! Megjegyezzük: éppen ez a jó, mert ellenkező esetben a ma használatos titkosírások könnyen feltörhetőek lennének ([2011])!

Egészen friss azonban a következő, nagyon nehéz eredmény:

24. Tétel. *(Agrawal-Kayal-Saxena, 2001): A* ***Prímtesztelés problémára*** *(tetszőleges $n \in \mathbb{N}$ számról döntsük el, hogy prím-e)* ***van*** *gyors algoritmus. Az algoritmus hivatalos rövidítése:* ***AKS*** *- algoritmus.* □

5. Maradékok

Az osztási maradékok vizsgálatánál hasznos az alábbi tömör jelölés:

25. Definíció. *Tetszőleges $a, b, m \in \mathbb{Z}$, $m \neq 0$ egész számokra jelölje*

$$a \equiv_m b \quad \textit{vagy} \quad a \equiv b \pmod{m} \tag{17}$$

az

$$\textit{"}a \textit{ és } b \textbf{ ugyanazt a maradékot adják } m\textit{-el osztva"} \tag{18}$$

relációt (összefüggést). A (17) relációt "a ***kongruens*** *b-****vel modulo***[5)] *m" -nek olvassuk, m a kongruencia* ***modulusa.*** □

A "kongruencia" szó helyett elég csak annyit mondanunk a diákoknak: a hosszú (18) mondat rövidítése (17). A maradékokat nyilván kukoricaszemekkel szemléltetjük az asztalon: egy-egy dobozba m fér, mennyi marad a végé?. Általában a maradék 0 és $m-1$ között van, de **negatív maradékok** is vannak: még ennyi kellene a dobozba. Sajnos a zsebszámológépen nincs **mod** gomb, érdemes a diákokkal ennek pótlását is megbeszélni.

(17) helyett a szakkönyvek a rövidebb $m \mid a-b$ képletet írják, de szerintem a (17) mondat érthetőbb.

A maradékok (kukoricaszemek) legfontosabb tulajdonsága, hogy az alapműveletekkel összhangban vannak[6)]:

26. Tétel. *Tetszőleges (*rögzített*) $m \in \mathbb{Z}$, $m \neq 0$ számra, valamint bármely $a, b, c, d \in \mathbb{Z}$ számokra* ***ha*** *$a \equiv_m b$ és $c \equiv_m d$,* ***akkor*** *$a \pm c \equiv_m b \pm d$ és $a \cdot c \equiv_m b \cdot d$.* □

A 26.Tétel hasznát a következőképpen foglalhatjuk össze:

[5)] *kongruencia*=megegyezés,megfelelés,egybevágóság, *modulus*=viszonyítási alap (lat.)

[6)] A Tétel összefüggései miatt hívjuk $\equiv_m$ -t **kongruenciának**, vagyis művelettartó ekvivalencia relációnak.

27. Megjegyzés. *Ha egy nagyméretű kifejezés kiértékelésénél (nagy számolásnál) csak a végeredmény* (mod m) *maradéka érdekel minket,* rögzített m *modulus esetén, akkor* minden lépésben *vehetjük/vegyük a részeredmény maradékát és csak a (kisméretű) maradékokkal kell tovább számolnunk. Vagyis egyetlen lépésben sem kell nagyméretű számokkal bajlódnunk. (Ezt hívják* ***moduláris aritmetiká****nak.)*

28. Példa. *Mennyi maradékot ad a* $132465+46587\cdot 83152\cdot 731052-208645^5$ *kifejezés* 753 *-mal osztva?*
Megoldás: *mindegyik tényezőnek külön-külön vesszük a* 753 *-mal való osztási maradékát, és a számolás minden lépésében is a részeredmények helyett* 73 *-mal való osztási maradékukat tekintjük:*

$$\begin{aligned}
&132465 + 46587 \cdot 83152 \cdot 731052 - 208645^5 \equiv \\
&\quad \equiv 690 + 654 \cdot 322 \cdot 642 - 64^5 \equiv \\
&\quad \equiv 690 + 654 \cdot 206724 - 64^2 \cdot 64^3 \equiv \\
&\quad \equiv 690 + 654 \cdot 402 - 331 \cdot 100 = \\
&\quad \equiv 230498 \equiv 80 \pmod{753}\ . \qquad \square
\end{aligned}$$

Hasonló kérdéssel már találkozunk az iskolában: "milyen számjegyekre végződik a megadott HATALMAS kifejezés?" : ha $n \in \mathbb{N}$ legutolsó ℓ számjegyét kérdezzük, akkor valójában a $\pmod{10^\ell}$ maradékra vagyunk kíváncsiak. A fenti 26. Tétel alapján megint egy jólismert *szabályt* kapunk:

"A végeredmény utolsó ℓ jegyének meghatározásához mindössze csak a tagok/tényezők utolsó ℓ jegyeit kell figyelembe vennünk."
De miért csak modulo 10^ℓ tanítjuk ezt az összefüggést, ha *tetszőleges* m modulusra is ugyanígy érvényes? Ezt nem csak általános- és középiskolai feladatoknál, hanem a jelen és a későbbi fejezetekben is használhatjuk, ennek látványos alkalmazása például [2011] 5.6. "Nagy kitevőjű hatványozás" alfejezete is.

Az iskolában tanult "*oszthatósági*" szabályok is a fenti 26. Tétel következményei.

29. Példa. *A* 11 *-gyel oszthatóság szabálya azon alapszik, hogy*

$$10^j \equiv (-1)^j \pmod{11}$$

tehát egy $a_k a_{k-1} \ldots a_1 a_0$ számjegyekkel, tízes számrendszerben leírt n szám

$$n = \overline{a_k a_{k-1} \ldots a_1 a_0}^{\,(10)} := \sum_{j=0}^{k} 10^j \cdot a_j$$

11 *-gyel való osztási maradéka* $n \equiv \sum_{j=0}^{k} (-1)^j \cdot a_j \pmod{11}$, *vagyis kapjuk a jólismert* szabályt:
"Egy tízes számrendszerben felírt szám pontosan akkor osztható 11 ***-gyel, ha a számjegyeit váltakozó előjellel összeadva a kapott összeg osztható*** 11 ***-gyel."*** *(A váltakozó előjelek a* 0 *számjegyekre is vonatkoznak, például* $n = 1032002$ *maradéka* $\equiv 1-0+3-2+0-0+2 \equiv 4 \pmod{11}$ *.)*

Sok gyakorló feladatot részletes megoldásokkal találhatunk [2005] 39-45. ill. 97-109. oldalain a fenti *szabályok* gyakorlására és alkalmazására.

30. Megjegyzés. ***VIGYÁZAT:*** páratlan *modulus esetén általában már* ***nem igazak*** *az alábbi, jól megszokott állítások:*

"páros±páros=páros" , *"páratlan±páratlan=páros"* , **...** , $\pmod{m}$
"páros·páros=páros" , *"páratlan·páratlan=páratlan"* $\pmod{m}$,

például $6 + 4 \equiv 1$, $6 \cdot 2 \equiv 3$ *de* $6 \cdot 4 \equiv 6 \pmod{9}$, *stb.*

Különböző modulusok között is vannak összefüggések, amikkel vigyázzunk:

31. Tétel. ***(i)*** Tetszőleges $m_1, m_2 \in \mathbb{Z}$ $(m_1 m_2 \neq 0)$ *modulusokra:*
ha $x \equiv y \pmod{m_1}$ *és* $x \equiv y \pmod{m_2}$ *akkor* $x \equiv y \pmod{lkkt(m_1, m_2)}$,
(ii) *ha* $ac \equiv bc \pmod{m}$ *és* $d = lnko(c, m)$, *akkor* $a \equiv b \pmod{\frac{m}{d}}$. □

6. Polinomok és $\mathbb{Z}[\alpha]$

Az oszthatóság (és a [2011] könyvben tárgyalt összes fogalom és algoritmus, mint pl. *lnko*, *lkkt*, *Euklideszi algoritmus, lineáris Diophantoszi egyenletek, Kínai maradéktétel, stb.*) nem csak az egész számok $\mathbb{Z}$ halmazán, hanem sok más gyűrűben (összeadás és szorzás műveletével ellátott halmazon) is léteznek, mint például a polinomoknál, a komplex számok bizonyos részhalmazain. Ezen vizsgálatok nagy része nem csak elméleti, hanem gyakorlati problémák megoldásához is segítséget nyújt a felsőfokú matematikában.

Most csak a legalapvetőbb definíciókat és tételeket említjük meg. Az érdeklődők bővebb elméletet [2011]-ben, részletesen kidolgozott feladatokat [2005]-ben találhatnak.

32. Definíció. ***(i)*** $\mathbb{Z}[x]$, $\mathbb{R}[x]$ *ill.* $\mathbb{C}[x]$ *jelöli rendre az egész-, valós- ill. komplex együtthatójú (egyismeretlenes) polinomok halmazát.*
(ii) *Az azonosan c értéket felvevő* 0 *fokú* ***konstans*** *polinomot* $\underset{\sim}{c}$ *-al jelöljük. Minden* $\underset{\sim}{c}$ *konstans polinom fokszáma* 0 , *de a* $\underset{\sim}{0}$ *polinom fokszáma* $-\infty$. □

33. Definíció. ***(i)*** *Egy $\alpha \in \mathbb{C}$ szám k* ***-adfokú*** *($k \in \mathbb{N}$)* ***algebrai*** *szám, ha α gyöke egy k -adfokú* valós *együtthatós (azaz $\mathbb{R}[x]$ -beli) polinomnak,*
(ii) *$\alpha \in \mathbb{C}$* ***algebrai egész,*** *ha α gyöke egy* egész *együtthatós (azaz $\mathbb{Z}[x]$ -beli) polinomnak.*
(iii) *Legyen $\alpha \in \mathbb{C}$ egy tetszőleges* másodfokú *algebrai egész szám, gyöke az*

$$\alpha^2 + p\alpha + q = 0 \tag{19}$$

egész együtthatós polinomnak. Ekkor legyen

$$\mathbb{Z}[\alpha] := \{a + b \cdot \alpha \mid a, b \in \mathbb{Z}\} \ . \quad \square$$

Természetesen $\mathbb{Z}[\alpha] \subset \mathbb{C}$.

34. Példa. *$\mathbb{Z}[i]$ elemeit* ***Gauss-egészek****nek, $\mathbb{Z}[\rho]$ elemeit* ***Euler-egészek****nek ($\rho = \cos(30^o) + i \sin(30^o)$), $\mathbb{Z}[\sqrt{2}]$ elemeit* ***H-egészek****nek, $\mathbb{Z}[i\sqrt{5}]$ elemeit* ***L-egészek****nek hívjuk.* $\square$

35. Állítás. *$\mathbb{Z}[\alpha]$ zárt az alapműveletekre (összeadás és szorzás) ha α* másodfokú *algebrai egész szám.*
Bizonyítás: $(a + b\alpha) \cdot (c + d\alpha) = (ac - bdq) + (ad + bc - bdp)\,\alpha$
a (19) egyenlet alapján. $\square$

Több számelméleti kérdésre is a $\mathbb{Z}[\alpha]$ halmazok segítségével kaptunk választ, mint például a *Nagy Fermat Tétel* $n = 3$ és $n = 4$ eseteire (Euler és Fermat), valamint Fermat "*Karácsonyi*" Tételére (Bolyai János), ld. pl. [2011]-ben.

36. Definíció. *Jelölje $2\mathbb{Z}$ a* ***páros számok*** *halmazát.* $\square$

Az alábbiakban az $\mathcal{R}$ gyűrű helyére nyugodtan gondolhatjuk a $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}[\alpha]$ és $2\mathbb{Z}$ halmazok bármelyikét.

Bármely $\mathcal{R}$ gyűrűben[7)] értelmezhetjük a *oszthatóság/többszörös*, *felbonthatatlan* (=*irreducibilis*) és *prímtulajdonságú* elemeket. és az *egyértelmű felbontás* tulajdonságát.

37. Definíció. *Az $\mathcal{R}$* gyűrűben teljesül *az* ***egyértelmű prímfelbontás,*** *röviden* ***EPF*** tulajdonsága, *ha bármely $a \in \mathcal{R}$ felbontható irreducibilis elemek szorzatára* lényegében egyértelmű módon *(sorrendtől és asszociáltaktól*[8)] *eltekintve).* $\square$

[7)] $\mathcal{R}$ -ről még fel kell tennünk, hogy **integritási tartomány** (39. Definíció)
[8)] ld. pl. [2011]-ben

A fenti elnevezés nagyon hasznos tulajdonságot takar: ha minden elemet **atomok**ra (="*tovább már nem bontható*" elemek, gör.) tudunk bontani, *és* egyértelmű módon, akkor így könnyebben tudjuk az elemek tulajdonságait, a műveleteket vizsgálni.

38. Megjegyzés. *A páros számoknál* nem *egyértelmű a prímfelbontás, pl.* $60 = 2 \cdot 30 = 10 \cdot 6$ *két különböző felbontás irreducibilis elemekre.*

$\mathbb{Z}[\sqrt{10}]$ *-ben* sem *teljesül az EPF.*

39. Definíció. *(i) A kommutatív, egységelemes és nullosztómentes gyűrűket* ***integritási tartományoknak*** *nevezzük,*
(ii) az $\mathcal{R}$ *gyűrűben elvégezhető a* ***maradékos osztás****, ha van egy* $\varphi : \mathcal{R} \to \mathbb{N}$ *függvény (****norma****,* ***abszolút érték****) a következő tulajdonsággal: bármely* $a, b \in \mathcal{R}$ *,* $\varphi(b) \neq 0$ *elemekhez találhatók* $c, d \in \mathcal{R}$ *elemek , amelyekre* $a = bc + d$ *és* $\varphi(d) < \varphi(b)$ *, vagyis a-t eloszthatjuk b-vel, a maradék d ,*
(iii) $\mathcal{R}$ ***Euklideszi gyűrű****, ha benne elvégezhető a maradékos osztás.* □

40. Tétel. *Euklideszi gyűrűkben teljesül az egyértelmű prímfelbontás.* □

41. Következmény. *A fenti Tételből (pontosabban a maradékos osztás létéből) következik a* 5. Számelmélet Alaptétele*, valamint az* Algebra Alaptételének fele*: "Minden egész/valós/komplex együtthatós polinom (vagyis* $\mathbb{Q}[x]$ *és* $\mathbb{R}[x]$ *elemei) lényegében egyértelműen (sorrendtől és konstans szorzóktól eltekintve) bonthatók fel irreducibilis polinomok".* □

42. Megjegyzés. ***(i)*** *Például a* $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$,$\mathbb{Z}[\rho]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{6}]$, $\mathbb{Z}[\sqrt{7}]$, $\mathbb{Z}[\sqrt{11}]$, $\mathbb{Z}[\sqrt{19}]$ *struktúrák Euklideszi gyűrűk, tehát bennük érvényes az EPF.*
(ii) *A 40. Tétel következtetése azonban nem fordítható meg: vannak olyan gyűrűk, amelyek ugyan* nem Euklidesziek*, de bennük mégis érvényes az EPF. Ilyenek például a* $\mathbb{Z}[x]$, $\mathbb{Z}[\sqrt{23}]$, $\mathbb{Z}[i\sqrt{3}]$, $\mathbb{Z}[i\sqrt{19}]$, $\mathbb{Z}[i\sqrt{43}]$, $\mathbb{Z}[i\sqrt{67}]$, $\mathbb{Z}[i\sqrt{163}]$ *struktúrák.*

Máig **megoldatlan** többek között a következő probléma:

43. Probléma. ***(o)*** *Mely* $m \in \mathbb{Z}$ *(nem négyzetszám) egész számokra teljesül* $\mathbb{Z}[\sqrt{m}]$ *-ben az egyértelmű prímfelbontás?*

Az alábbi eredmények ismertek:
(i) Negatív *m esetén ismert az összes megfelelő m szám:* $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$,

$\mathbb{Z}[i\sqrt{3}]$, $\mathbb{Z}[i\sqrt{7}]$, $\mathbb{Z}[i\sqrt{11}]$, $\mathbb{Z}[i\sqrt{19}]$, $\mathbb{Z}[i\sqrt{43}]$, $\mathbb{Z}[i\sqrt{67}]$, $\mathbb{Z}[i\sqrt{163}]$ *-ben* igaz *az EPF (kb. 1970 óta tudjuk biztosan, hogy nincs több megfelelő negatív* m*).*
(ii) Nem *érvényes az EPF* $\mathbb{Z}[\sqrt{m}]$ *-ben minden olyan* pozitív $m \in \mathbb{N}$ *(nem négyzet-) számra, amelyre* $4 \mid m-1$.
(iii) *Ismertek még:* $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{6}]$, $\mathbb{Z}[\sqrt{7}]$, $\mathbb{Z}[\sqrt{11}]$, $\mathbb{Z}[\sqrt{19}]$ *és* $\mathbb{Z}[\sqrt{23}]$ *-ben érvényes az EPF, míg* $\mathbb{Z}[\sqrt{10}]$ *-ben nem.* □

A [2011] könyvhöz mellékelt POLIOSZ5.COM program segítségével gyakorolhatjuk a polinomok maradékos osztását, Euklideszi algoritmust, *lnko* keresését ... a $\mathbb{Z}[x]$ gyűrűben.

A jelen fejezetben leírtak nem csak elméletileg, hanem gyakorlati problémáknál is fontosak és hasznosak. A [2005] Feladatgyűteményben sok részletesen kidolgozott feladatot találunk polinomokról és a $\mathbb{Z}[\alpha]$ struktúrákról.

Érdekesek és hasznosak még a **primitív gyökök** és a **számelméleti logaritmus**, ezekről [2011] 6.7. fejezetében olvashatunk.

Függelék

44. Definíció. *A* $\mathcal{B} = (P, \cup\cap, \emptyset, I)$ *struktúrát* ***Boole algebrá****nak nevezzük, ha tetszőleges* $A, B, C \in P$ *elemekre teljesülnek az alábbi azonosságok:*

kommutativitás	$A \cup B = B \cup A$	*(BA1)*
	$A \cap B = B \cap A$	*(BA2)*
asszociativitás	$A \cup (B \cup C) = (A \cup B) \cup C$	*(BA3)*
	$A \cap (B \cap C) = (A \cap B) \cap C$	*(BA4)*
disztributivitás	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	*(BA5)*
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	*(BA6)*
elnyelési tulajdonságok	$A \cup (A \cap B) = A$	*(BA7)*
	$A \cap (A \cup B) = A$	*(BA8)*
$\emptyset$ *és* I *tulajdonságai*	$A \cup \overline{A} = I$	*(BA9)*
	$A \cap \overline{A} = \emptyset$	*(BA10)*
	$A \cup \emptyset = A$	*(BA11)*
	$A \cap \emptyset = \emptyset$	*(BA12)*
	$A \cup I = I$	*(BA13)*
	$A \cap I = A$	*(BA14)*

□

Hivatkozások

[1997] **Szalkai István:** *Lineáris algebra, sztöchiometria és kombinatorika*, Polygon VII. (1997), 35–51.
http://math.uni-pannon.hu/~szalkai/SzI-Polygon1997-jav.pdf

[2001] **Szalkai István:** *Diszkrét matematika és algoritmuselmélet alapjai*, Pannon Egyetem Kiadó Veszprém, 2001, javított kiadás: 2006.

[2005] **Szalkai István:** *Algebra és számelmélet feladatgyűjtemény*, Pannon Egyetem Kiadó, Veszprém, 2005.

[2011] **Szalkai István, Dósa György**: *Algoritmikus számelmélet*, Egyetemi jegyzet digitális mellékletekkel:
http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/adatok.html ,
http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/Szalkai_Dosa_Alg_szamelm_1_1.html .

[2012] **Bálint Attila:** *A logika tanításának számítógépes támogatása*, Szakdolgozat (digitális melléklettel), Pannon Egyetem, Veszprém, 2012,
http://math.uni-pannon.hu/~szalkai/BalintA-xdsi73.docx ,
http://math.uni-pannon.hu/~szalkai/Logika.exe

[2013K] Középiskolai Matematikai Lapok, B.4493.feladat, 2012/10 és 2013/8, 478-479.,
http://www.komal.hu/verseny/feladat.cgi?a=feladat&f=B4493&l=hu

[2013w] **Wikipédia:** *Boole-algebra*, [Részletes definíció],
http://hu.wikipedia.org/wiki/Boole-algebra