Matematikatanítási és Módszertani Központ

Egyetemi matematika az iskolában

Hegyvári Norbert

2013

Tartalomjegyzék

Előszó

A matematikával való foglalkozás eddig jobbára egyirányú volt; Az általános iskolai ismeretekre épült a középiskolai, a középiskolaira az egyetemi.

A fenti cím alatt meghirdetett előadás valamiképpen ezen út megfordítását is ígéri; célként tűzi ki, hogy megmutassa, az egyetemi oktatás hogyan jelenik meg az általános iskolában és a középiskolában. Szeretnénk megmutatni, hogy bizonyos az iskolai matematikaoktatásban szereplő témáknak mi a háttere, hogyan ágyazódik be a matematika nagy hálójába.

Az előadás formájából adódóan természetesen ez nem lehet teljes. Noha témakörökre és fejezetekre osztott a tematika, ezek azonban korántsem lezártak. Az előadás sikeres teljesítéséhez (és így a sikeres vizsgához is) az anyaghoz tematikájában, de inkább szellemében kapcsolódó ú.n. *portfólió* beadása szükséges. Néhány előadás és néhány oldal elolvasása után remélhetőleg világos lesz, mi is ez.

Ez az ellentétes irányú vizsgálat, amit az előadás célként tűzött ki, talán választ ad arra a néha-néha (főleg sikertelen vizsga utáni) felcsattanó hallgatói kifogásra "Minek ez nekem! Úgy se fogom ezt tanítani!".

Egy rövid anekdotát hadd illesszek végül ide:

Székely Mihályt, a kiváló magyar operaénekest egyszer megállította az egyik barátja az operaház előtt. "Mihály! Tegnap csodálatos voltál a Don Carlosban! Azok a mély regiszterek, amit kiénekeltél!" Székely így felelt: "Köszönöm! De tudod miért volt ilyen tiszta a mély regiszterem? Nos, mert tudok még két hanggal lejjebb is..."

A pargrafusokvégén található **MM** a "Módszertani Megjegyzések"-re utalnak. A tárgy fonos része, hogy a hallgatók átgondolják ezeket; n.b. kiegészítsék, megjegyzéseket fűzzenek hozzá. E megjegyzéseket köszönettel veszem és várom a hegyvari@vipmail.hu címre.

Göd, 2012. január hava

1. A tárgy célja

A fenti címmel meghirdetett tárgy célja hármas:

1. Adott (közép)iskolai feladat egyetemi szemszögből, egyetemen tanult módszerekkel történő megoldása.

Ez sok esetben egy általánosabb struktúrára mutat rá, tágabb összefüggésbe helyezi az adott feladatot ill. ezen keresztül összekapcsol egyetemen tanult témaköröket.

2. Adott (közép)iskolai feladat általánosítása egyetemi szintű állítássá , tétellé (pl. Fermat-tétel $\rightarrow$ Euler-tétel $\rightarrow$ véges (ciklikus) csoportok elemeinek rendjéről)

2. Olyan (közép)iskolai feladatok precíz átgondolása, ahol elfogadjuk indoklásként a szemléletből fakadó tényeket, igazolni azonban itt, az egyetemen tettük meg.

Az alább következő gyűjteményben ezekre példa néhány függvény tulajdonsága (konvexitás, monotonitás stb.)

További szempontok is elképzelhetőek és bátorítjuk az olvasót ilyen szempontok figyelembevételére.

2. Irracionális számok; $\sqrt{2}$

A köznapi ember, ha megkérnénk, hogy mondjon egy irracionális számot, nagy többségében feltehetőleg a π-t mondaná, annak ellenére, hogy középiskolában a közelébe se jut, hogy ezt bizonyítsa. A $\sqrt{2}$ ókori görögöktől származó bizonyítása kerül terítékre a középiskolákban, ami így szól:

TÉTEL:
A $\sqrt{2}$ irracionális.

BIZONYÍTÁS:
Ez jól ismert, csak a teljesség kedvéért:
Indirekt tegyük fel, hogy létezik $a, b \in \mathbb{Z}$, $b > 0$ és $(a, b) = 1$ úgy, hogy

$$\sqrt{2} = \frac{a}{b}.$$

Négyzetre emeléssel

$$2b^2 = a^2$$

így tehát a^2 és ezért $a = 2a'$ $(a' \in \mathbb{Z})$ páros szám. Helyettesítéssel

$$b^2 = 2a'^2$$

azaz b is páros, ami ellentmond az $(a, b) = 1$ feltételnek. $\square$

MM

Ebben a fejezetben két dolgot szeretnénk megmutatni. Az egyik, hogy a fenti állításnak több olyan bizonyítása is van, ami ú.n. "egyetemi matematikát" igényel (érzékeltetve azt, hogy a matematika egy háló is, ahol sok minden szorosan összefügg egymással).

A másik dolog talán még fontosabb: Középiskolában elvétve találkozunk irracionális számokkal (talán a $\sqrt{2}, \sqrt{3}$, stb. kivételével mással nem is(?)) és

csak az egyetemen szembesülhetünk, (ha előtte nem olvastunk halmazelméleti könyveket) hogy valójában az irracionális számok vannak "többségben". (népszerűen fogalmazva a valós számok zsákjából egy számot véletlenszerűen kivéve az 1 valószínűséggel lesz irracionális – sőt transzcendens – szám). Ezért adunk egy csokor irracionális számot, talán szokatlanokat is, amit viszont középiskolában is elmondhatunk.

Akkor tehát a többi bizonyítás:

2. Bizonyítás: Indirekt tegyük fel, hogy létezik $a, b \in \mathbb{Z}$, $b > 0, (a, b) = 1$ ahol b minimális. Úgy, hogy

$$\sqrt{2} = \frac{a}{b}.$$

Nyilván

$$a > b,\ \frac{a}{b} < 2 \Leftrightarrow b > a - b.$$

$$\frac{2b - a}{a - b} = \frac{2 - a/b}{a/b - 1} = \frac{2 - \sqrt{2}}{\sqrt{2} - 1} = (2 - \sqrt{2})(\sqrt{2} + 1) = \sqrt{2},$$

ellentmondásban azzal, hogy b a legkisebb nevezőjű előállítás ($a - b < b$). □

3. Bizonyítás:

Bizonyítjuk a következő tételt:

Tétel:
Ha $\alpha \in \mathbb{R}^+$ *és* $\exists p_1, p_2, \ldots, q_1, q_2, \cdots \in \mathbb{N}$, *úgy. hogy bármely* n *esetén*

$$|\alpha p_n - q_n| \neq 0,$$

és $p_n, q_n \to \infty$ *esetén*

$$|\alpha p_n - q_n| \to 0,$$

akkor α *irracionális.*

Bizonyítás:
Indirekt, ha $\alpha = \frac{a}{b}$, $b > 0, (a, b) = 1$, akkor mivel $|\alpha p_n - q_n| \to 0$, van olyan n, hogy

$$|\alpha p_n - q_n| = |\frac{a}{b} p_n - q_n| < \frac{1}{b},$$

és így

$$0 < |ap_n - bq_n| < 1,$$

ami nem lehet, mivel $ap_n - bq_n$ egész szám. □

Ebből következik $\sqrt{2}$ irracionalitása; legyen $p_1 = q_1 = 1$, továbbá $q_{n+1} = q_n^2 + 2p_n^2$ és $p_{n+1} = 2p_n q_n$. Ekkor indukcióval könnyen ellenőrizhető, hogy

$$0 < |\sqrt{2}p_n - q_n| < \frac{1}{2^{2^{n-1}}}.$$

4. Bizonyítás:

Legyen

$$A = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}.$$

Elsőként számítsuk ki A sajátértékeit:

$$det(A - \lambda I) = det \begin{pmatrix} -1-\lambda & 2 \\ 1 & -1-\lambda \end{pmatrix} = 0,$$

amiből

$\lambda_1 = \sqrt{2} - 1 \quad \lambda_2 = -\sqrt{2} - 1.$

A $\lambda_1 = \sqrt{2} - 1$-hez tartozó sajátaltér

$$W = \left\{ \begin{pmatrix} \sqrt{2}x \\ x \end{pmatrix} : \quad x \in \mathbb{R}. \right\}$$

A sajátaltér egy egyenes, melynek meredeksége $\sqrt{2}/2$.

Az A leképezés *kontrakció* (összehúzó), ami azt jelenti, hogy ha $\underline{v} \in W$, akkor

$$|A\underline{v}| = |(\sqrt{2} - 1)\underline{v}| < |\underline{v}|,$$

ezért

$$|A^k\underline{v}| = |(\sqrt{2} - 1)^k\underline{v}| \to 0,$$

mivel $(\sqrt{2} - 1)^k \to 0$.

Végül vegyük észre, hogy A egy $\neq (0,0)$ rácspontot $\neq (0,0)$ rácspontba visz át, mert

$$A \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -a + 2b \\ a - b \end{pmatrix}, \quad a, b \in \mathbb{Z}.$$

Így azonban a sajátaltéren (az origót kivéve) nincs rácspont, mert egyrészt rácspontot rácspontba visz át A^k, másrészt kontrakció a sajátaltéren. □

3. További irracionális számok

TÉTEL: *A következő valós számok irracionálisak:*

$$\cos\frac{\pi}{2^n};\ n>1 \quad \log_3(1+\sqrt{2}); \quad \log_2 3+\log_4 5.$$

Ezek bizonyítása középiskolai feladat.

Útmutatás: Valamely $0<\alpha<\pi/2$ értékre $\cos(\alpha/2)=\sqrt{\frac{\cos\alpha+1}{2}}$. Így ha $x_n:=\cos\frac{\pi}{2^n}$; akkor $n>1$ esetén $x_{n+1}=\sqrt{\frac{x_n+1}{2}}$.

FELADATOK:

1. Ha $r, r', \ldots$ racionális számokat, $i, i', \ldots$ irracionális számokat jelölnek, milyen számok lesznek:

$$r+r';\ r+i;\ i+i';\ rr';\ ri;\ ii';r^{r'};\ r^i;\ i^r;\ i^{i'}\ ?$$

(feltéve, hogy léteznek)

Irracionális-e

2. $\log_2 3$?
3. $\log_3(1+\sqrt{2})$?
4. $\sqrt{2}+\sqrt{3}$?
5. $\log_2 3+\log_4 5$?

4. Végtelen tizedestörtek

Ismeretes, hogy egy végtelen tizedestört akkor és csak akkor racionális, ha felírásában a jegyei valahonnan kezdve periodikusak.

Így tizedestört alakban is könnyű irracionális számokat gyártani.

A következő tételben egy kevéssé nyilvánvaló tizedestörtről igazoljuk, hogy irracionális:

TÉTEL: *Legyenek* $(2), (3), (p_3), (p_4), (11), (p_6) \dots$ *a prímszámok sorozata a tízes számrendszerben felírva. Ekkor az*

$$\alpha := 0, \overline{23p_3p_411p_6 \dots}$$

végtelen tizedestört irracionális szám.

Erre a tételre két bizonyítást adunk.

I. BIZONYÍTÁS:

Az első bizonyítás a következő (nem túl könnyen bizonyítható) Dirichlettől származó állításon alapszik:

Ha $a, b \in \mathbb{N}$; *és* $(a, b) = 1$ *akkor az* $x_n = a + b \cdot n; \quad n = 1, 2, \dots$ *sorozatban végtelen sok prímszám található.*

Tegyük akkor most fel, hogy α racionális, tehát van egy $q_1 \dots, q_k$ peródusa ($q_i \in \{0, 1, \dots, 9\}; i = 1, 2, \dots, k.$). Mivel végtelen sok prímszám van (lásd a következő fejezetet) a periódus nem minden eleme 0. Dirichlet tétel miatt a $10^{2k} \cdot n + 1$ sorozatban végtelen sok prím van. Ezek olyan számok, amik a tízes számrendszerben felírva jobbról az első jegy 1, utána $2k - 1$ 0 jegy következik, ami ellentmond annak, hogy a periódus nem a konstans 0 sorozat.

II. BIZONYÍTÁS:

Az előző bizonyításban nem tudtunk utánajárni a Dirichlet tétel bizonyításának. A most következő bizonyításban minden részletet igazolunk. Sőt, egy kicsit többet bizonyítunk:

TÉTEL: *Tegyük fel, hogy* $\{b_i\}_{i=1}^{\infty} \subseteq \mathbb{N}$ *és*

$$\sum_{i=1}^{\infty} \frac{1}{b_i} = \infty.$$

Ekkor a $\beta = 0, \overline{b_1 b_2 \dots b_k \dots}$ *végtelen tizedestört irracionális szám, ahol a* b_i *elemeket a tízes számrendszerben írtuk fel.*

A következő fejezetben igazolni fogjuk, hogy a prímszámok reciprok összege divergens. Ezzel teljessé fogjuk tenni a bizonyítást.

Legyen $(u_1)(u_2) \dots (u_s)$ egy tetszőleges, rögzített mintázat a tízes számrendszerben és legyen X azon pozitív egészek halmaza, amelyek a tízes számrendszerben ezt a mintázatot nem tartalmazzák. Tehát például ha 2012 ez a mintázat, akkor $2.1\mathbf{20}.\mathbf{12}4 \notin X$, de $421.012 \in X$.

Az általánosabb tétel igazolásához a következő állításra van szükségünk.

TÉTEL: *Legyen X a fent definiált halmaz. Ekkor*

$$\sum_{z\in X}\frac{1}{z}<\infty,$$

azaz e pozitív tagú végtelen sor konvergens.

E tétel pl. abban a formában talán ismert feladat, hogy *"Bizonyítsuk be, hogy a 7 számjegyet nem tartalmazó természetes számok reciprok összege konvergens!"*

BIZONYÍTÁS:

A bizonyítást arra az esetre végezzük el, amikor a mintázat mondjuk a 17. Az általános eset e bizonyítás másolata. Nyilván 100-ig 99 olyan szám van ami nem tartalmazza mintázatként a 17-t. Jelölje S_n az n-edik részletösszeget és H_n a harmonikus sor n-edik részletösszegét, továbbá $\lfloor x\rfloor$ az x szám egészrészét, tehát pl. $\lfloor 1,01\rfloor=1$. Ekkor

$$S_n=\left(H_{100}-\frac{1}{17}\right)+\frac{1}{101}+\cdots+\frac{1}{116}+\frac{1}{118}+\ldots\frac{1}{x_n}$$

(x_n az X n-edik tagja.)

$$S_n=\left(H_{100}-\frac{1}{17}\right)+\frac{1}{100}\left(\frac{1}{1,01}+\cdots+\frac{1}{1,16}+\frac{1}{1,18}+\ldots\frac{1}{x_n/100}\right)<$$

$$<\left(H_{100}-\frac{1}{17}\right)+\frac{1}{100}\left(\frac{1}{\lfloor 1,01\rfloor}+\cdots+\frac{1}{\lfloor 1,16\rfloor}+\frac{1}{\lfloor 1,18\rfloor}+\ldots\frac{1}{\lfloor x_n/100\rfloor}\right).$$

Vegük észre, hogy egy $\lfloor x_n/100\rfloor$ szám 99-szer fordul elő és hogy az $\{\lfloor x_n/100\rfloor\}$ sorozat is olyan, amelyik nem tartalmazza a 17 mintázatot. Így

$$S_n<H_{100}-\frac{1}{17}+\frac{99}{100}S_n,$$

így

$$S_n<100\left(H_{100}-\frac{1}{17}\right),$$

azaz az S_n sorozat korlátos, nyilván monoton növő, így konvergens.

Most már könnyen igazolhatjuk a $\beta=0,\overline{b_1b_2\ldots b_k\ldots}$ szám irracionalitását: tegyük fel indirekt, hogy β racionális. Akkor tehát van egy $(p_1)(p_2)\ldots(p_t)$

periódus a tízes számrendszerbeli felírásában. Legyen $s > 2t$ és az $(u_1)(u_2)\dots(u_s)$ 2 és 3 számokból álló olyan mintázat, amelyikben nem fordul elő a $(p_1)(p_2)\dots(p_t)$ mintázat. Ilyen nyilván van. Mivel az $(u_1)(u_2)\dots(u_s)$ mintázatot nem tartalmazó egészek reciprok összege konvergens, ám $\sum_{i=1}^{\infty}\frac{1}{b_i}=\infty$ divergens, ebből következőleg a $\{b_i\}$ sorozatnak végtelen sok olyan tagja van, amelyik az $(u_1)(u_2)\dots(u_s)$ mintázatot tartalmazza. Azaz β-ban végtelen sokszor előfordul egy olyan mintázat, amelyik a $(p_1)(p_2)\dots(p_t)$ periódust nem tartalmazza ellentmondásként. □□□

Kulcsszavak:

5. Végtelen sok prímszám van

A címben szereplő kijelentés egyike azoknak, amelyek jól ismertek. Eukleidésztől származó gyönyörű bizonyítás sokaknak az első lépés a matematikában.

TÉTEL: *Végtelen sok prímszám van.*

Ebben a fejezetben erre az állításra öt bizonyítást adunk, a matematika különböző területeire "evezve". Emiatt sok közülük többetmondó lesz, pusztán az adott kijelentésnél.

I. BIZONYÍTÁS:
Ez a jól ismert Eukleidésztől származó bizonyítás: ha $p_1, p_2, \dots, p_k$ az első k prímszám, akkor az

$$N := p_1 \cdot p_2 \cdots p_k + 1$$

szám prímtényezői között nem szerepelhet $p_1, p_2, \dots, p_k$ közül egyik se. □□□

Megjegyzés: Ez a közel 2300 éves bizonyítás azonfelül, hogy gyönyörű (Erdős Pál említette, hogy gyerekkorában e bizonyítás fordította figyelmét a számelmélet felé) egy igen modern bizonyítási formának is az előfutára; az ú.n. *nem konstruktív bizonyítási módszernek* (amit Erdős munkássága

alapján lett gyakran használt módszer); Eukleidész *nem mutat* egy új prímszámot, hanem annak létezésére következtet. Ugyanez történik egyébként a következő bizonyításban is. Megjegyeznénk egy kimagaslóan forradalmian új bizonyítást a naív halmazelméletből; Cantor bizonyítása a transzcendens számok létezéséről.

II. Bizonyítás:

A bizonyítás Pólya Györgytől származik és így hangzik:

Tekintsük az $\{F_k = 2^{2^k} + 1;\ k = 0, 1, 2, \dots\}$ ú.n. Fermat-számok sorozatát.

(Megjegyeznénk, hogy megoldatlan probléma, hogy ezek között van-e végtelen sok prímszám. Az első öt ilyen szám az; azonban $F_5 = 2^{2^5} + 1 = 641 \cdot 6700417$.)

Igazolni fogjuk, hogy $k \neq n$ esetén $(F_k, F_n) = 1$. (Ebből következik, hogy végtelen sok prím van, hiszen végtelen sok Fermat-számunk van és mindegyik prímtényezős felbontásában az előzőek felbontásában szereplő prímektől különböző prím(ek) szerepel(nek)).

Ehhez azt fogjuk igazolni, hogy ha $k < n$, akkor

$$F_k | F_n - 2.$$

Valóban ebből következik: ha $d|F_k$, akkor $d|F_n - 2$ és ha $d|F_n$, akkor $d|F_n - (F_n - 2) = 2$. Tehát a legnagyobb közös osztó $d|2$; a Fermat számok páratlanok, azaz $d = 1$.

Az $F_k|F_n - 2$ bizonyításához mindössze azt kell észrevennünk, hogy

$$F_k(F_k - 2) = (2^{2^k} + 1)(2^{2^k} - 1) = (2^{2^k})^2 - 1 = 2^{2^{k+1}} - 1 = F_{k+1} - 2.$$

Ezért

$$F_{k+1}F_k(F_k - 2) = F_{k+1}(F_{k+1} - 2) = F_{k+2} - 2,$$

innen teljes indukcióval

$$F_{k+s} \cdots F_{k+1}F_k(F_k - 2) = F_{k+s+1} - 2,$$

azaz minden $s > 1$ esetén $F_k|F_{k+s+1} - 2$, ami $s := n - k - 1$ választással az állítás. □□□

III. Bizonyítás:

Ez a bizonyítás Erdőstől származik. Másfelől ez teszi teljessé az előző fejezetben igazolt $\alpha := \overline{23p_3p_4 11 p_6 \dots}$ valós szám irracionalitását.

TÉTEL: *Legyen $p_1 = 2, p_2 = 3, \dots,$ a prímszámok sorozata. Ekkor*

$$\sum_i \frac{1}{p_i} = \infty.$$

Nyilván ebből következik, hogy végtelen sok prímszám van; véges sok prímszám, véges összeget adna.

BIZONYÍTÁS:

Tegyük fel indirekt, hogy

$$\sum_i \frac{1}{p_i} < \infty$$

azaz, hogy a sor konvergens. Ekkor létezik egy olyan küszöbindex, n_0, hogy

$$\sum_{i=n_0+1} \frac{1}{p_i} < \frac{1}{2}.$$

Legyen $N = 4^{n_0+1} + 1$.

N-ig a számokat két osztályba fogjuk sorolni: Az A osztályba azokat, amiknek csak $p_1 < p_2 < \dots < p_{n_0}$ a prímosztójuk, a B halmazba a többi elemet, tehát azokat, amelyeknek van olyan prímosztójuk, p_k, amelyikre $k > n_0$.

Egy $n \in A$ elemet felírunk egy négyzetszám és egy négyzetmentes szám szorzataként. (Például a $600 = 10^2 \cdot 2 \cdot 3$.) Tehát

$$n = k^2 \cdot p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \dots \cdot p_{n_0}^{\varepsilon_{n_0}},$$

ahol $\varepsilon_i = 0$ vagy 1. Mivel

$$k^2 \le n \le N,$$

ezért $k \le \sqrt{N}$. Azaz az első tényező legfeljebb $\sqrt{N}$ különböző szám lehet. A

$$p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \dots \cdot p_{n_0}^{\varepsilon_{n_0}}$$

tényezőben $\varepsilon_i = 0$ vagy 1, ezért ez legfeljebb 2^{n_0} különböző érték lehet.

Így A halmazban legfeljebb

$$\sqrt{N} 2^{n_0}$$

szám lehet.

Vegyük most a B halmazt; ezekben tehát olyan számok vannak, amelyeknek **nem minden** prímosztója az első n_0 közül kerül ki, tehát **van** n_0 sorszámúnál nagyobb sorszámú osztója. Azaz lehet p_{n_0+1}-gyel osztható, p_{n_0+2}-vel osztható, stb. Így B-ben legfeljebb

$$\left\lfloor \frac{N}{p_{n_0+1}} \right\rfloor + \left\lfloor \frac{N}{p_{n_0+2}} \right\rfloor + \cdots \leq$$

$$N \cdot \left(\frac{1}{p_{n_0+1}} + \frac{1}{p_{n_0+2}} + \dots \right) < \frac{N}{2}$$

elem lehet (felhasználva, hogy $\sum_{i=n_0+1} \frac{1}{p_i} < \frac{1}{2}$). Ebből következik, hogy az A halmazban legalább $N/2$ elem van. Azt kapjuk tehát, hogy

$$\frac{N}{2} \leq |A| \leq \sqrt{N} 2^{n_0}.$$

Átrendezéssel

$$4^{n_0+1} + 1 = N \leq 4^{n_0+1}$$

ami ellentmondás. □□□

IV. Bizonyítás:

Euler bizonyítása. Ez volt a csírája annak a bizonyításnak, ami a prímszámok számára aszimptotikus becslést ad. A bizonyításban végtelen sorok szerepelnek, amelyek abszolút konvergensek tehát a véges összegeknél megszokott műveletet (pl. disztributivitást) szabadon használhatjuk.

Indirekt, ha véges sok prímszám lenne $p_1, p_2, \dots, p_k$, készítsük el a k számú végtelen mértani sort:

$$1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \frac{1}{p_i^3} + \cdots + \frac{1}{p_i^{t_i}} + \cdots = \frac{1}{1 - \frac{1}{p_i}},$$

$i = 1, 2, \dots k$. Szorozzuk össze őket, azaz vegyük a

$$\prod_{i=1}^{k} \left(\sum_{t_i=0}^{\infty} \frac{1}{p_i^{t_i}} \right) = \prod_{i=1}^{k} \frac{1}{1 - \frac{1}{p_i}}.$$

A jobb oldalon egy véges szám áll. A már említett szabály szerint a bal oldali zárójeleket felbonthatjuk. Vegyük észre, hogy a felbontás után bármely $n \in \mathbb{N}$ számra $\frac{1}{n}$ pontosan egyszer szerepel. Valóban, ha

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdot p_k^{\alpha_k},$$

ahol $\alpha_i \geq 0$ egész, $(i = 1, 2, \ldots k,)$ akkor $\frac{1}{n}$ úgy szerepel, ha az $i-$edik mértani sorból az

$$\frac{1}{p_i^{\alpha_i}}$$

tagot választjuk és ezeket a prímhatványokat összeszorozzuk. Tehát

$$\prod_{i=1}^{k} \left(\sum_{t_i=0}^{\infty} \frac{1}{p_i^{t_i}} \right) = \sum_{n=1}^{\infty} \frac{1}{n}.$$

A $\sum_{n=1}^{\infty} \frac{1}{n}$ sor divergens, a baloldal egy véges szám ellentmondásként.

V. Bizonyítás:

Ez Gelfand-tól származó bizonyítás.

1. Legyen

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

egész együtthatós nem azonosan 0 polinom, amelyikre az $x \in [0, 1]$ intervallum elemeire $p(x) \geq 0$. Mivel $p(x)$ folytonos és nem azonosan 0, azt kapjuk, hogy

$$0 < \int_0^1 p(x)dx = \left[a_n \frac{x^{n+1}}{n+1} + \cdots + a_1 \frac{x^2}{2} + a_0 x \right]_0^1 = \frac{A}{[1, 2, \ldots, n+1]},$$

ahol A pozitív egész, és $[1, 2, \ldots, n+1]$ az első $n+1$ egész szám legkisebb közös többszöröse. Tehát $A \geq 1$ és így

$$\int_0^1 p(x)dx \geq \frac{1}{[1, 2, \ldots, n+1]}.$$

2. Mi is $[1, 2, \ldots, N]$ prímtényezős felbontása?

Pl. $[1, 2, \ldots, 10]$: ebben a $2, 3, 5, 7$ prímek szerepelnek. 2 harmadik hatványon, 3 második, 5 és 7 első hatványon. Azaz $[1, 2, \ldots, 10] = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

Általában tehát $[1, 2, \ldots, N]$ prímtényezős felbontásában a $p_1, p_2, \ldots, p_k$ prímszámok szerepelnek, ahol

$$k = \pi(N),$$

az N-ig szereplő prímek száma és p_i az α_i hatványon, ahol

$$p_i^{\alpha_i} \leq N < p_i^{\alpha_i+1}.$$

Így

$$[1, 2, \ldots, N] = \prod_{i=1}^{k} p_i^{\alpha_i} \leq N^k = N^{\pi(N)}.$$

Tehát az 1. pontban elmondottakkal együtt:

$$\int_0^1 p(x)dx \geq \frac{1}{[1, 2, \ldots, n+1]} \geq \frac{1}{(n+1)^{\pi(n+1)}}.$$

3. Végül legyen $p(x) := (x(1-x))^k$. Ez nyilván egész együtthatós, a $[0, 1]$ intervallumban az $x(1-x)$ egy "lefelé nyíló" parabola, melynek a 0 és 1 a gyökei tehát $(0, 1)$-en pozitív értékű is, ezért $(x(1-x))^k$ is az. Itt $x(1-x) \leq 1/4$, így

$$p(x) := (x(1-x))^k \leq \frac{1}{4^k} \quad x \in [0, 1].$$

Ezért

$$\int_0^1 p(x)dx := \int_0^1 (x(1-x))^k dx \leq \int_0^1 \frac{1}{4^k} dx = \frac{1}{4^k}.$$

A $p(x)$ foka $n = 2k$. Tehát az 1. és 2. pontok miatt

$$\frac{1}{(n+1)^{\pi(n+1)}} = \frac{1}{(2k+1)^{\pi(2k+1)}} \leq \int_0^1 p(x)dx \leq \frac{1}{4^k}.$$

Átrendezve

$$4^k \leq (2k+1)^{\pi(2k+1)}$$

és mindkét oldal logaritmusát véve

$$2k \ln 2 \leq \pi(2k+1) \ln(2k+1)$$

azaz

$$\ln 2 \frac{2k}{\ln(2k+1)} \leq \pi(2k+1).$$

Egy kis analízissel kapjuk:

TÉTEL:
Bármely $\varepsilon > 0$ számhoz létezik k_0, hogy $N > N_0$ esetén

$$(\ln 2 - \varepsilon)\frac{N}{\ln(N)} \leq \pi(N).$$

Ha $\varepsilon < \ln 2$ és mivel

$$\lim_{N\to\infty} \frac{N}{\ln(N)} = \infty,$$

ezért

$$\lim_{N\to\infty} \pi(N) = \infty,$$

azaz végtelen sok prímszám van. □□□

VI. BIZONYÍTÁS:

Az alábbi egysoros bizonyítás S. Northshield-től származik. Minden magyarázat nélkül közöljük:

$$0 < \prod_{p\in\mathcal{P}} \sin\left(\frac{\pi}{p}\right) = \prod_{p\in\mathcal{P}} \sin\left(\pi \frac{1 + 2\prod_{p'\in\mathcal{P}} p'}{p}\right) = 0.$$

VII. BIZONYÍTÁS:

Ez a bizonyítás I. D. Mercer-től származik. A bizonyítás ötlete H. Fürstenberg topológiára alapozó bizonyítását követi, azonban nem szükséges a topológia alapfogalmainak az ismerete sem, mindössze az az elemi halmazelméleti gondolat, miszerint véges sok halmaz úniójának a véges sok metszete is véges sok halmaz metszetének az úniója.

Jelölje $NS(n)$ az $n-$nel nem osztható egész számok halmazát. Ezek szerint $NS(n)$ $n-1$ mindkét irányban végtelen számtani sorozat úniója.

Tegyük fel, hogy véges sok prímszám van: $p_1 = 2 < p_2 = 3 < \cdots < p_k$. A számelmélet alaptétele szerint így

$$X := NS(p_1) \cap NS(p_2) \cap \cdots \cap NS(p_k) = \{-1, 1\}.$$

Az X halmaz véges sok mindkét irányban végtelen számtani sorozat unió-jának a véges metszete; így véges sok mindkét irányban végtelen számtani sorozat metszetének az uniója.

Végül gondoljuk meg: két mindkét irányban végtelen számtani sorozat metszete vagy üres halmaz, vagy egy mindkét irányban végtelen számtani sorozat. Ez ellentmond annak, hogy $X = \{-1, 1\}$.

Kulcsszavak: A számelmélet alaptétele; egyszerű algabrai azonosságok alkalmazása, kombinatorika, végtelen sorok, integrálszámítás, Leibniz-Newton szabály, a topológia elemei.

6. Struktúrák I.

Talán magyarázni sem kell, hogy az egyetemi tanulmányok itt, a struktúrák vizsgálatában szélesítették ki az általános iskolában és a középiskolában tanultakat jelentős mértékben. Nem csak a zártság, asszociativitás, kommutativitás stb. fogalmát árnyalta, hanem beágyazott olyan tételeket is mint például a Euler-Fermat tétel egy általánosabb struktúra tulajdonságba. Ezekről a későbbiekben részletesen lesz szó.

Néhány feladat megoldásán keresztül szeretnénk néhány olyan bizonyítást mutatni, ami túlnő a középiskolai anyagon, ám arra visszavetülve más, szélesebb megvilágításban láttatja azt.

Kezdjük!

A következő feladatok bizonyítása során többször fogjuk használni a lineáris algebrában használt tételt:

Tétel:
Legyen A és B két négyzetes mátrix ($A, B \in \mathbb{R}^{n\times n}$). Ekkor

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

A feladatok:

FELADAT: *Legyen* $A := \{n : n = a^2 + b^2; a, b \in \mathbb{N}\}$. *Bizonyítsuk be, hogy a szorzásra nézve zárt!*

Ez középiskolában feladható feladat. Akik járatosak a kéttagú kifejezések négyzetének számolásában, könnyebben-nehezebben megoldják a feladatot.

Nézzünk két másik megoldást:

1. Megoldás: Ha $n = a^2 + b^2$, akkor könnyű látni, hogy $n = \det A = \det \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ és hasonlóan, ha $m = x^2+y^2$, akkor $m = \det B = \det \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$. Az AB mátrix szorzat

$$A \cdot B = \begin{pmatrix} ax - by & ay + bx \\ -bx - ay & ax - by \end{pmatrix}.$$

Használva az említett tételt, kapjuk, hogy

$$(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (ay + bx)^2.$$

2. Megoldás: Legyen $z_1 = a + bi$ komplex szám, $z_2 = x + yi$ a másik komplex szám. Használjuk fel, hogy

$$(a^2 + b^2) \cdot (x^2 + y^2) = |z_1|^2 \cdot |z_2|^2 = |z_1 \cdot z_2|^2 = (ax - by)^2 + (ay + bx)^2.$$

Egy hasonló

FELADAT: *Egy szám* $x = a^2 + 2b^2$ *(*$a, b \in \mathbb{N}$*) akkor a háromszorosa is ilyen:* $3x = A^2 + 2B^2$ *(*$A, B \in \mathbb{N}$*)*

Megoldhatjuk így is:

$$x = \det \begin{pmatrix} a & \sqrt{2}b \\ -\sqrt{2}b & a \end{pmatrix} \quad \Rightarrow$$

$$\Rightarrow x \cdot 3 = \det \begin{pmatrix} a & \sqrt{2}b \\ -\sqrt{2}b & a \end{pmatrix} \cdot \begin{pmatrix} 1 & -\sqrt{2} \\ \sqrt{2} & 1 \end{pmatrix} = (a + 2b)^2 + 2(a - b)^2.$$

Egy pillanatig sem szeretnénk azt a látszatott kelteni, hogy ez a megoldás *egyszerűbb*, mint rájönni, hogy mi is a háromszoros előállítása. Arra akartuk

csak felhívni a figyelmet, hogy ez egy *módszer*, ami alkalmas ilyen jellegű feladatok megoldására.

A következő feladatnál azonban némileg tanácstalanul állnánk, ha "elemi" megoldást keresnénk:

FELADAT: *Bizonyítsuk be, hogy az*

$$S = \{x : \exists a, b, c \in \mathbb{N}; x = a^3 + b^3 + c^3 - 3abc\}$$

halmaz zárt a szorzásra nézve.

MEGOLDÁS:

Legyen $x = a^3 + b^3 + c^3 - 3abc$ és $y = A^3 + B^3 + C^3 - 3ABC$. Ekkor találhatunk két 3×3-as mátrixot, melyeknek a determinánsai éppen x és y :

$$x = \det \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \quad y = \det \begin{pmatrix} A & B & C \\ C & A & B \\ B & C & A \end{pmatrix}.$$

Ekkor

$$x \cdot y = \det \left(\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \cdot \begin{pmatrix} A & B & C \\ C & A & B \\ B & C & A \end{pmatrix} \right) =$$

$$= \det \begin{pmatrix} aA + bC + cB & aB + bA + cC & aC + bB + cA \\ aC + bB + cA & aA + bC + cB & aB + bA + cC \\ aB + bA + cC & aC + bB + cA & aA + bC + cB \end{pmatrix}.$$

Ebből már leolvasható, hogy a szorzat is S-ben van;

$$x \cdot y = U^3 + V^3 + W^3 - 3UVW,$$

ahol $U = aA + bC + cB;\ V = aB + bA + cC;\ W = aC + bB + cA.$

Néhány nevezetes sorozatra vonatkozó ismert azonosságokat is levezethetünk az idézett tétel segítségével.

Legyen

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

és tekintsük az $\{F_k\}_{k=1}^{\infty} = \{1, 1, 2, 3, 5, 8, \dots\}$ Fibonacci sorozatot. Egyszerűen ellenőrizhető a következő tétel:

TÉTEL: *Ha* $k \in \mathbb{N}$, *akkor*

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}.$$

A bizonyítás teljes indukcióval egyszerű.

A tételnek számos, a középiskolából is ismerhető következménye van:

KÖVETKEZMÉNYEK:

1. Bármely $k \in \mathbb{N}$ *esetén*

$$F_{k+1}F_{k-1} - F_k^2 = (-1)^k.$$

Ez az előbbi tételből és abból következik, hogy

$$\det\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k\right) = \left(\det\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right)^k = (-1)^k.$$

2. Bármely $k, s \in \mathbb{N}$ *esetén*

$$F_{k+1}F_s + F_kF_{s-1} = F_{s+1}F_k + F_sF_{k-1} = F_{k+s}.$$

Ennek bizonyítása a mátrixok szorzásán alapszik:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^s = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} \cdot \begin{pmatrix} F_{s+1} & F_s \\ F_s & F_{s-1} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{k+s} = \begin{pmatrix} F_{k+1}F_{s+1} + F_kF_s & F_{k+1}F_s + F_kF_{s-1} \\ F_{s+1}F_k + F_sF_{k-1} & F_kF_s + F_{k-1}F_{s-1} \end{pmatrix} =$$

$$= \begin{pmatrix} F_{k+s+1} & F_{k+s} \\ F_{k+s} & F_{k+s-1} \end{pmatrix}.$$

A következő tétel a Fibonacci számok explicit előállítására vonatkozik.

TÉTEL:
Bármely $k \in \mathbb{N}$

$$F_k = \frac{1}{\sqrt{5}} \left(\left(\frac{\sqrt{5}+1}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right)$$

BIZONYÍTÁS:

1. Használni fogjuk, hogy ha A egy lineáris leképezés és $\underline{v}$ egy sajátvektora, λ sajátértékkel, azaz

$$A\underline{v} = \lambda \underline{v},$$

akkor bármely $k \in \mathbb{N}$, esetén

$$A^k \underline{v} = \lambda^k \underline{v}.$$

(Bizonyítása egyszerű teljes indukció segítségével.)

Legyen

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Számítsuk ki a sajátértékeit; azaz

$$\det \begin{pmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - \lambda - 1 = 0$$

egyenlet gyökeit kell meghatározni. Ezek

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \qquad \lambda_2 = \frac{1-\sqrt{5}}{2}.$$

Ha $\underline{v}_1 = \begin{pmatrix} a \\ b \end{pmatrix}$ sajátvektor, akkor

$$A\underline{v}_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a+b \\ a \end{pmatrix} = \lambda_1 \begin{pmatrix} a \\ b \end{pmatrix}.$$

Amiből például

$$\underline{v}_1 = \begin{pmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{pmatrix}.$$

Az előzőekben megkaptuk, hogy $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}$ és $\lambda_1^k = \left(\frac{1+\sqrt{5}}{2}\right)^k$. Így az $A^k \underline{v}_1 = \lambda_1^k \underline{v}_1$ vektor első koordinátáit összehasonlítva azt kapjuk, hogy

$$\frac{\sqrt{5}+1}{2} F_{k+1} + F_k = \left(\frac{\sqrt{5}+1}{2}\right)^{k+1}. \quad (*)$$

Hasonló számolással kapjuk, hogy ha a sajátérték $\lambda_2 = \frac{1-\sqrt{5}}{2}$ sajátvektora $\underline{v}_2 = \begin{pmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{pmatrix}$ és megint az $A^k \underline{v}_2 = \lambda_2^k \underline{v}_2$ vektor, akkor első koordinátáit összehasonlítva azt kapjuk, hogy

$$\frac{\sqrt{5}-1}{2} F_{k+1} - F_k = -\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}. \quad (**)$$

$(*)$-ot és $(**)$-ot összeadva és $\sqrt{5}$-tel osztva a tételbeli formulát kapjuk F_{k+1}-re.

7. Mennyi az F_N?

Valójában a Fibonacci sorozat elemeinek a kiszámítására a következő lehetőségeink vannak:

1. *A rekurzív képlet alapján.*
2. *Az előző "misztikus" képlet alapján.*
3. *...*

Az 1. nyilván nehézkes, lassú. A 2. elég reménytelen; $\sqrt{5}$ hatványaival számolni nehéz.

A 3. lehetőséget nyitva hagytuk.

Erre az $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}$ képlet lesz segítségünkre; ha a szorzást és az összeadást egy-egy lépésnek tekintjük, akkor két 2×2 (szimmetrikus) mátrix összeszorzása 9 lépés. Mivel F_N-et az $A^N = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^N$-ből ki tudjuk olvasni így járhatunk el:

Legyen N 2-es számrendszerbeli felírása

$$N = \sum_{i=0}^{k} \varepsilon_i 2^i,$$

ahol ε_i vagy 0 vagy 1. Mivel $2^k \leq N < 2^{k+1}$, ezért $k \leq \log_2 N$. Számítsuk ki az A^{2^i} $i = 1, 2, \ldots k$ mátrixokat, $9k$ lépésben, majd ahol $\varepsilon_i = 1$ azokat a hatványokat szorozzuk össze, ez megint legfeljebb $9k$ lépés. Így megkaptuk az

$$A^{\sum_{i=0}^{k} \varepsilon_i 2^i} = A^N$$

mátrixot.

Kaptuk tehát a következő tételt:

TÉTEL:
F_N értéke legfeljebb $18 \log_2 N$ lépésben meghatározható.

Ez nagy N értékekre jóval gyorsabb, mint rekurzív módon kiszámítani F_N értékét N lépésben.

8. Apropó, hogyan szorzunk össze két egész számot?

A válasz: nyilván ahogy az iskolában tanultuk.

Tehát ha két számunk x és y, n jegyű számok, akkor minden jegyet minden jeggyel összeszorzunk, ez $n \times n$ szorzás, majd összeadjuk; ez kb $2n$ lépés. Az összeadást a továbbiakban ne számoljuk, a lépésszám jóval kevesebb, mint a szorzásnál. A válasz így

Két n jegyű számot n^2 lépésben lehet összeszorozni.

Ez a múlt század elejéig nem is volt lényeges kérdés; nem volt mód nagy számokat gyorsan összeszorozni.

A következő tétel mondható egyetemi matematikának, amelyik az iskolában jelenik meg, de csak abban az értelemben, ahogy a *kérdést felveti.* A segédeszközök teljes mértékben rendelkezésre állnak középiskolában is.

TÉTEL:
Két n jegyű számot lehet $\leq 2n^{\log_2 3} \sim 2n^{1.585..}$ lépésben is összeszorozni.

Ezt a meglepő eredményt egyetemi hallgató korában Karacuba vette észre (Kolmogorov egy kérdésére válaszolva).

BIZONYÍTÁS:
Jelölje $L(n)$ a két n jegyű szám összeszorzásához szükséges lépések számát (itt tehát a számjegyekkel való szorzást számoljuk, a részösszeadásokat nem, mivel ezek nagyságrendben kisebbek).

Írjuk fel

$$2^{k-1} < n \leq 2^k.$$

Nyilván $L(n) \leq L(2^k)$. Tehát a két szám számjegyeinek a száma páros (sőt 2-hatvány). Tehát legyen adva x és y, mindkettő $2N := 2^k$ jegyű (ha nem, pótoljuk ki az elején nullákkal). Ha minden számjegyet minden számjeggyel összeszorzunk, akkor $4L(N)$ lépést tettünk. Ügyesebben a következőképpen járhatunk el: Írjuk fel x-et, y-t így

$$x = 10^N A + D \qquad y = 10^N B + C,$$

(tehát A, B, C, D N jegyű számok). Ekkor

$$x \cdot y = 10^{2N} AB + 10^N (AC + BD) + CD.$$

Szükségünk van tehát AB, CD és $AC + BD$-re (ha mind a négyre különkülön, akkor maradna a $4L(N)$ lépés). Ám megúszhatjuk mindössze háromval is: vegyük az

$$AB, \quad CD, \quad (A + D)(B + C) - AB - CD = AC + BD$$

szorzatokat. Evvel 3 N jegyű számot szoroztunk össze (megspóroltuk az AC és BD külön-külön kiszámítását). Így a rekurzióval

$$L(2^k) = L(2N) \leq 3L(N) = 3L(2^{k-1}).$$

Ezt az eljárást iterálva kapjuk, hogy

$$L(2^k) \leq 3^2 L(2^{k-2}),$$

és így tovább, azaz

$$L(n) \leq L(2^k) \leq 3^k L(1) = 2^{\log_2 3k} \leq 2n^{\log_2 3k}.$$

□□□

Kulcsszavak:

9. Struktúrák II.

Ebben a fejezetben olyan feladatokat gyűjtöttünk egybe, amelyek a megszokott műveleti tulajdonságokkal *nem* rendelkeznek ill. bizonyos műveleti tulajdonságokból kell következtetni másokra. A használt műveletek jól ismertek, a segítségükkel definiáltak műveletekről igazoljuk, a "szokatlant".

A feladatok egy része nemzetközi versenyfeladat, jelezni is fogjuk, hogy honnan származnak.

Többször fog szerepelni az ú.n. csoport fogalma.

Egy $G, \circ$ csoport, ha teljesül rá, hogy

1. zárt ($\forall a, b \in G,\ a \circ b \in G$)
2. asszociatív,
3. létezik egységelem ($\exists e \in G$, hogy $\forall a \in G, e \circ a = a \circ e = a$) valamint
4. létezik az inverz ($\forall a \in G,\ \exists a^{-1}$, hogy $a \circ a^{-1} = a^{-1} \circ a = e$.)

Tehát nem tettük fel a *kommutativitást.*

Az első feladat egy 1971-es Putnam (amerika) matematikai versenyfeladat:

FELADAT: *Egy* $(S, \circ)$ *struktúráról a következőket tudjuk:*
(1) $\forall x \in S, \quad x \circ x = x.$
(2) $\forall x, y, z \in S, \quad (x \circ y) \circ z = (y \circ z) \circ x.$
Bizonyítsuk be, hogy a $\circ$ *művelet kommutatív.*

MEGOLDÁS:
Legyen x, z két tetszőleges elem $S-$ben. Megmutatjuk, hogy $x \circ z = z \circ x$.
A (2)-ben legyen $x = y$. Ekkor

$$(x \circ x) \circ z = (x \circ z) \circ x,$$

mivel $x \circ x = x$ ezért

$$x \circ z = (x \circ z) \circ x.$$

"Szorozzuk" meg jobbról z-vel

$$(x \circ z) \circ z = ((x \circ z) \circ x) \circ z$$

és használjuk megint (2)-t

$$(z \circ z) \circ x = (x \circ z)(x \circ z).$$

(1)-et használva mindkét oldalra

$$z \circ x = x \circ z. \qquad \square\square\square$$

Egy hasonló feladat:

FELADAT: *Egy* $(T, \circ)$ *struktúráról a következőket tudjuk:*
$\forall x, y \in T,$
(1) $x \circ (x \circ y) = y,$
(2) $(y \circ x) \circ x = y.$
Bizonyítsuk be, hogy a $\circ$ *művelet kommutatív.*

MEGOLDÁS:

Megmutatjuk, hogy bármely $a, b \in T$ teljesül, hogy $a \circ b = b \circ a$.
(1)-ben legyen $x = b \circ a$, és $y = a$, ahol $a, b \in T$. Ekkor

$$(b \circ a) \circ ((b \circ a) \circ a) = a,$$

(2) miatt a második zárójelben levő kifejezés b, így

$$(b \circ a) \circ b = a.$$

"Szorozzuk" meg jobbról b-vel

$$((b \circ a) \circ b) \circ b = a \circ b.$$

Megint (2) miatt a bal oldal $b \circ a$, így

$$b \circ a = a \circ b. \qquad \square\square\square$$

Az előzőekben tárgyaltak mintapéldái lehetnek annak, ahogy bizonyos szabályokból következtetünk (az általános- és középiskolában kétkedés nélkül elfogadott) tulajdonságra; a kommutativitásra.
Ebben a tekintetben rokon azokhoz az algebrai feladatokhoz, amelyekbe algebrai azonosságokat kell igazolni.

Az előző két példával rokon, ám egy kicsit nehezebb, ugyancsak kommutativitásra vonatkozó feladatot mutatunk be:

FELADAT: *Legyen $(G, \cdot)$ egy csoport, melyen definiálunk egy leképezést: $\varphi : G \mapsto G$ $\varphi(x) = x^3$. Tegyük fel φ-ről, hogy* **homomorfizmus** *és hogy* **injektív**. *Igazoljuk, hogy ekkor a csoport kommutatív.*

Mielőtt a megoldáshoz fognánk, idézzük fel, mit is jelent a két feltétel:

1. φ **homomorfizmus**, ami azt jelenti, hogy $\forall a, b \in G$ teljesül, hogy $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
2. φ **injektív**, azaz, ha $a \neq b$ akkor $\varphi(a) \neq \varphi(b)$.

MEGOLDÁS:
Mivel φ homomorfizmus, így

$$(xy)^3 = x^3 y^3$$

teljesül minden $x, y \in G$ elemre. Balról x-szel, jobbról y-nal egyszerűsítve

$$y(xy)x = x^2y^2.$$

Az asszociativitást használva

$$y(xy)x = (yx)(yx) = (yx)^2,$$

így

$$(yx)^2 = x^2y^2.$$

Balról yx-szel beszorozva

$$(yx)^3 = yx^3y^2,$$

és mivel $(yx)^3 = y^3x^3$, egy y-nal balról leosztva

$$y^2x^3 = x^3y^2$$

teljesül. (Tehát az x^3 y^2 elemek már kommutálnak).

Most már be tudjuk bizonyítani, hogy $\forall a, b \in G$ $ab = ba$. Legyen $y = a^3$; $x = b^2$ és helyettesítsük ezeket be:

$$(a^3)^2(b^2)^3 = (b^2)^3(a^3)^2,$$

$$(a^2)^3(b^2)^3 = (b^2)^3(a^2)^3.$$

Mivel a köbre emelés homomorfizmus

$$(a^2b^2)^3 = (b^2a^2)^3$$

és mivel injektív

$$a^2b^2 = b^2a^2.$$

Balról a-val, jobbról b-vel szorozva

$$a^3b^3 = ab^2a^2b$$

vagy másként

$$(ab)^3 = a^3b^3 = ab^2a^2b,$$

$$(ab)(ab)(ab) = (ab)ba(ab).$$

Jobbról, balról (ab)-vel egyszerűsítve

$$ab = ba. \qquad \square\square\square$$

Az általános iskolában, a gimnáziumokban meggyökeresedhetett az az elképzelés, hogy az

$$a^{k_1}b^{s_1}\cdot a^{k_2}b^{s_2}\cdots a^{k_u}a^{s_v}=a^{m_1}b^{t_1}\cdot a^{m_2}b^{t_2}\cdots a^{m_w}a^{t_z},$$

egyenlőség eldöntéséhez csak át kell rendeznünk a bal, ill. jobb oldalt és a kitevőket össze kell hasonlítani:

$$k_1+k_2+\ldots k_u=m_1+m_2+\ldots m_w;$$

és

$$s_1+s_2+\ldots s_v=t_1+t_2+\ldots t_z$$

a szükséges és elégséges feltétele ennek. Az elképzelés a valós számok testében (és sok más középiskolában szokásosan használt struktúrákban) igaz.

A következő, nagyon szellemes megjegyzés példa arra, hogy nem kommutatív struktúrában ez nem igaz:

TÉTEL: *Legyen* $F=\begin{pmatrix}1&1\\1&0\end{pmatrix}$ *és* $G=\begin{pmatrix}0&1\\1&1\end{pmatrix}$.

Ekkor

$$F^{k_1}G^{s_1}\cdot F^{k_2}G^{s_2}\cdots F^{k_u}G^{s_v}$$

csak egyféleképpen lehet felírni, a szorzat egyértelmű.

BIZONYÍTÁS:

Azt mondjuk, hogy egy

$$\underline{v}=\begin{pmatrix}x\\y\end{pmatrix}$$

vektor pozitív, ha $x,y>0$. Mivel

$$F\underline{v}=\begin{pmatrix}x+y\\x\end{pmatrix};\quad G\underline{v}=\begin{pmatrix}y\\x+y\end{pmatrix},$$

ezért mind F, mind G pozitív vektort pozitív vektorba visz át.

A $\underline{v}$-ról azt mondjuk, hogy felső típusú, ha $x>y$ és azt, hogy alsó típusú, ha $x<y$ (tehát az (x,x) típusú vektorokról nem mondunk semmit). Jegyezzük meg, hogy ha $\underline{v}$ pozitív vektor, akkor $F\underline{v}$ képe felső típusú és $G\underline{v}$ képe alsó típusú. Tegyük most fel, hogy az F-ek hatványaiból és a G-k hatványaiból készítünk két különböző szorzatot, U-t és V-t, és tegyük fel, hogy ezek egyenlők $U=V$ és az összes ilyen példa közül ezek a legrövidebbek.

Az U és V nem kezdődhet ugyanúgy; mivel mind F, mind G invertálhatók, azért ha ugyanúgy kezdődnének, le lehetne velük egyszerűsíteni és lenne rövidebb példa. Tehát tegyük fel, hogy

$$U = F \cdot U'; \qquad V = G \cdot V'.$$

Legyen most $\underline{w}$ egy pozitív vektor. Ekkor, mint láttuk F és G és így minden hatványa pozitív vektorba viszi át a pozitív vektort. Ezért

$$U'\underline{w}; \qquad V'\underline{w}$$

vektorok pozitívak. Ám

$$U\underline{w} = F \cdot U'\underline{w}$$

felső típusú és

$$V\underline{w} = G \cdot V'\underline{w}$$

alsó típusú ellentmondásként. □□□

E paragrafusban utolsóként egy 2009-es Nemzetközi Matematikai Diákolimpiai feladatot tekintünk, amiben, ugyancsak felcserélhetőségről van szó:

FELADAT: *Ha A, B, C mátrixok, akkor*

$$(A - B)C = BA^{-1} \quad \Leftrightarrow \quad C(A - B) = A^{-1}B,$$

feltéve, hogy az A^{-1} és C^{-1} inverzek léteznek.

MEGOLDÁS:

1. Először megmutajuk, hogy $C = I$ esetén miért igaz az állítás, majd ebből levezetjük az általános esetet. Mindössze azt használjuk fel, hogy a multiplikatív inverzek felcserélhetőek; $X \cdot X^{-1} = 1 \Leftrightarrow X^{-1} \cdot X = 1$. Belátjuk, hogy

$$A - B = BA^{-1} \quad \Leftrightarrow \quad A - B = A^{-1}B.$$

Ha $A - B = BA^{-1}$, akkor $A - B - BA^{-1} + I = I$ teljesül. Ám

$$A - B - BA^{-1} + I = (A - B)(A^{-1} + I) = I,$$

azaz $(A - B)$ és $(A^{-1} + I)$ egymás multiplikatív inverzei. Ezért igaz, hogy

$$(A^{-1} + I)(A - B) = I,$$

felbontva a zárójeleket

$$I - A^{-1}B + A - B = I \quad \Leftrightarrow \quad A - B = A^{-1}B.$$

2. Az általános eset: felbontva a zárójelet

$$(A - B)C = BA^{-1};$$

$$AC - BC = BA^{-1} = (BC)(AC)^{-1}.$$

1.-ben A helyett AC-vel, B helyett BC-vel felírva

$$AC-BC = BA^{-1} = (BC)(AC)^{-1} \quad \Leftrightarrow \quad AC-BC = (AC)^{-1}(BC) = C^{-1}A^{-1}BC,$$

C^{-1}-zel jobbról C-vel balról beszorozva

$$C(A - B) = A^{-1}B. \qquad \square\square\square$$

Megjegyzés:

1. Az előző feladatban nem használtuk, hogy mátrixokról volt szó; valójában tetszőleges gyűrűben is elmondható lett volna a feladat.

2. Ezek a feladatok arra szerettek volna rávilágítani, hogy középiskolai versenyszintű feladatokban is fellelhető alapvető, a struktúrákkal kapcsolatos állítások. A következő paragrafusban még közvetlenebb kapcsolatra szeretnénk rámutatni.

Kulcsszavak:

10. Strukturák III.

Ezt a rövid fejezetet kezdjük egy feladatsorral:

Feladat:

Legyen $\mathbb{F}$ egy tetszőleges test és legyen $0_F = 0$ a nulla eleme. Bizonyítsuk be, hogy

$\forall a, b \in \mathbb{F},\ a, b \neq 0$ teljesül, hogy

1. $-(a \cdot b^{-1}) = (-a) \cdot b^{-1} = a \cdot (-b^{-1})$.
2. $(-a)^{-1} = -(a^{-1})$.
3. $a \cdot b^{-1} = (-a) \cdot (-b^{-1})$.

Milyen "szabályok" következnek ezekből az állításokból?

A következőkben hivatkozunk néhány jól ismert tételre a csoportelméletből:

Tétel: *1. Legyen G egy véges csoport. Ekkor bármely $H < G$ részcsoportjára igaz, hogy $|H|$ elemszáma osztója $|G|$ elemszámának.*

2. $\forall g \in G;\quad g^{|G|} = 1$, ahol 1 a csoport egységeleme.

Tétel:

Egy prímrendű csoport ciklikus.

Most kulcsszavak keresése helyett feladatokban tűzzük ki az iskolai kapcsolatot.

A középiskolákban is előkerül (néha csak speciális formában) az Euler-Fermat-tétel.

FELADAT

Az előző tételek közül melyik tétel és hogyan kapcsolódik az Euler-Fermat-tételhez?

Ugyancsak előkerül (megint néha csak speciális formában) a mod p *primitív gyök* fogalma.

FELADAT

Az előző tételek közül melyik tétel és hogyan kapcsolódik a primitív gyök fogalmához?

11. Szitaformula

Általános- és középiskolából jól ismert feladat a következő:

FELADAT: *Egy* 32 *fős osztályban a gyerekek négy nyelvet tanulnak:* 15*-en angolul,* 10*-en németül,* 9*-en franciául. Angolul és németül* 6*-an, angolul és franciául* 4*-en, németül és franciául* 4*-en tanulnak. A három nyelvet* 3*-an választották. Az osztály többi tanulója csak az oroszt tanulja. Hányan vannak ők?*

Ezt a feladatot általában ú.n. Venn-diagrammal szokás megoldani.

Van azonban másik megoldás is, a logikai szita segítségével: a 32-ből kiszitáljuk a 15 angolt, 10 németet, a 9 franciát, azonban kétszer vontuk le az angol-németet s.í.t. Tehát akik csak oroszul tanulnak:

$$32 - 15 - 10 - 9 + 6 + 4 + 4 - 3 = 9.$$

Ebben a pontban ennek a módszernek egy nagyon hasznos alkalmazását mutatjuk be, amit középiskolában is elmondhatunk, és amelynek egyetemi anyag a háttere. Ezeket a kulcsszavakat kellene összegyűjteni a paragrafus végén.

Ezen alkalmazás előtt két jól ismert feladatot (tétel formájában) említünk bizonyítás nélkül:

TÉTEL: *1. Egy hat pontú teljes gráf éleit két színnel színezve, mindig található a gráfban egyszínű háromszög. Sőt, legalább két egyszínű is van, és ennél több nem állítható.*

2. Egy 17 *pontú teljes gráf éleit három színnel színezzük. Ekkor mindig található a gráfban egyszínű háromszög.*

TÉTEL: *Ha egy n pontú gráf éleinek a száma $> \frac{n^2}{4}$, akkor a gráfban van háromszög.*

Az első tétel ú.n. Ramsey-típusú tétel, a második a Turán tételének speciális esete. E két tételt, mint következményt vezethetjük le a következő állításból, ahol a logikai szitát (és még más eszközt is) használunk:

TÉTEL: *Egy n pontú G gráfban az egyszínű háromszögek száma legalább*

$$\frac{n(n-1)(n-5)}{24}.$$

BIZONYÍTÁS:

Használjuk a szitaformulát: az összes háromszögek számából szitálunk: Először azokat hagyjuk el, amelyeknek van a komplementer gráfban élük; egy ilyen élhez $n-2$ pont csatlakozik egy háromszöget alkotva. Tehát

$$\Delta(G) = \binom{n}{3} - \overline{e}(n-2)\dots.$$

Most azokat a háromszögeket kell "visszaadnunk", amelyeknek két komplementer gráfbeli élük is van. Ezt most a csúcsoknál számoljuk le: az i-edik pontból $\overline{\varphi}_i$ komplementer él fut ki. Ebből kell két élt kiválasztani, ezek ugyanis akkor olyan háromszöget határoznak meg, amelyeknek van két komplementer éle. Végül le kell vonni azokat a háromszögeket, amelyeknek mindhárom oldala komplementer él. Ezek száma definíció szerint $\Delta(\overline{G})$. Így

$$\Delta(G) = \binom{n}{3} - \overline{e}(n-2) + \sum_{i=1}^{n} \binom{\overline{\varphi}_i}{2} - \Delta(\overline{G}).$$

A további becslésekhez az alábbi állításra van szükségünk:

ÁLLÍTÁS: Az $f(x) := \frac{x^2-x}{2}$ függvény konvex, tehát igaz rá, hogy bármely $x_1 < x_2 < \cdots < x_n$ esetén

$$f\left(\frac{\sum_{i=1}^n x_i}{n}\right) \leq \frac{\sum_{i=1}^n f(x_i)}{n}.$$

Mivel az $\binom{n}{2}$ binomiális együtthatót is az $\frac{n^2-n}{2}$ képlettel számoljuk ki, bevezethetjük f-re az $f(x) := \binom{x}{2}$ jelölést. Ekkor a fenti állítás így írható le:

$$\binom{\frac{\sum_{i=1}^n x_i}{n}}{2} \leq \frac{\sum_{i=1}^n \binom{x_i}{2}}{n}$$

Tehát a szita képletben a $\sum_{i=1}^n \binom{\overline{\varphi}_i}{2}$ tagot így becsülhetjük

$$\sum_{i=1}^n \binom{\overline{\varphi}_i}{2} \geq n \cdot \binom{\frac{\sum_{i=1}^n \overline{\varphi}_i}{n}}{2}.$$

A $\sum_{i=1}^n \overline{\varphi}_i$ éppen a komplementer élek kétszerese, tehát

$$\sum_{i=1}^n \binom{\overline{\varphi}_i}{2} \geq n \cdot \binom{\frac{\sum_{i=1}^n \overline{\varphi}_i}{n}}{2} = n \cdot \binom{\frac{2\overline{e}_i}{n}}{2} = \frac{2\overline{e}^2}{n} - \overline{e}.$$

Így a szitaképletben az egyszínű háromszögek számára (ha úgy gondolunk a gráfra és a komplementerére, mint a teljes gráf éleinek két-színezésére) azt kapjuk, hogy

$$\Delta(G) + \Delta(\overline{G}) \geq \binom{n}{3} - \overline{e}(n-2) + \frac{2\overline{e}^2}{n} - \overline{e}.$$

Ez $\overline{e}$-nak másodfokú függvénye, amelynek minimuma az $\overline{e} = \frac{n(n-1)}{4}$-ben van. Ezt behelyettesítve kapjuk, hogy

$$\Delta(G) + \Delta(\overline{G}) \geq \binom{n}{3} - \overline{e}(n-2) + \frac{2\overline{e}^2}{n} - \overline{e} \geq \frac{n(n-1)(n-5)}{24}.$$

□□□

Ha $n = 6$, akkor a jobb oldal nagyobb, mint 1, azaz egy 6 pontú gráf éleit két színnel színezve, van legalább két egyszínű háromszög található a gráfban.

Ha valaki mondjuk, azt szeretné bizonyítani, hogy egy $n = 8$ pontú gráfban van 7 egyszínű háromszög, akkor ez nem lenne olyan egyszerű feladat (azonban a fenti leszámlálásból rögtön következik).

TÉTEL: *Egy n pontú e élű gráfban a háromszögek száma legalább*

$$\frac{e(4e-n^2)}{3n}.$$

BIZONYÍTÁS:

A bizonyításhoz két dolgot kell észrevennünk:

1. A $\sum_{i=1}^{n}\binom{\overline{\varphi}_i}{2}$ összegben a $\Delta(\overline{G})$-t háromszor számoltuk, tehát

$$\sum_{i=1}^{n}\binom{\overline{\varphi}_i}{2} \geq 3\Delta(\overline{G}),$$

így a szita képletben

$$\Delta(G) \geq \binom{n}{3} - \overline{e}(n-2) + \frac{2}{3}\sum_{i=1}^{n}\binom{\overline{\varphi}_i}{2} \geq \binom{n}{3} - \overline{e}(n-2) + \frac{2}{3}\left(\frac{2\overline{e}^2}{n} - \overline{e}\right).$$

Másfelöl

2. Nyilván

$$\overline{e} = \binom{n}{2} - e.$$

Ezt a fenti becslésbe beírva, kis számolással adódik, hogy

$$\Delta(G) \geq \frac{e(4e-n^2)}{3n}. \qquad \square\square\square$$

Ebből pedig a másodikként említett tételt kapjuk; ha $e > \frac{n^2}{4}$, akkor $\frac{e(4e-n^2)}{3n} > 0$, azaz van háromszög a gráfban. Valójában sokkal többet olvashatunk le. Ha az él szám nagyobb az említettnél, *hirtelen* nagyon "sok" háromszög lesz G-ben.

Kulcsszavak:

12. Végtelen leszállás-Teljes indukció

Teljes indukcióval megoldható feladatokban bővelkednek mind a középiskolai, mind az egyetemi feladatsorok, tételek. Az ú.n. végtelen leszállás (infinite descent) módszerrel operáló bizonyítást viszont jóval kevesebbet találunk. Jól ismert Fermat tétele (ő írta le, és nevezte így el ezt a bizonyítási eljárást).

Mindenesetre szeretnénk rámutatni, hogy számos bizonyítás elmondtható a végtelen leszállás módszerével. Például a $\sqrt{2}$ irracionalitásának bizonyításakor elhagyható a $\sqrt{2} = \frac{a}{b};\ b > 0;\ (a, b) = 1$ feltételei közül az $(a, b) = 1$. Ekkor a bizonyítás úgy módosul, hogy az $a = 2a_1$ és $b = 2b_1$ feltételekből az egyszerűsítés után a $2b_1^2 = a_1^2$ marad, ahol ez előző gondolatmenetet követve az $2b_i^2 = a_i^2;\ i = 1, 2, \ldots$ végtelen sok azonosságot kapjuk, az $a_1 > a_2 > \cdots > 0$ végtelen sorozat mellett, ami nem lehetséges.

Vegyük észre, hogy a $\sqrt{2}$ irracionalitásának második bizonyítása is interpretálható így; ha $\sqrt{2} = \frac{a}{b};\ b > 0;\ (a, b) = 1$ feltétel teljeülne, akkor a $\sqrt{2} = \frac{2b-a}{a-b}$ is teljesülne a $b > a - b > 0$ mellett. Ezt ismételve a pozitív nevezők egy végtelen szigorúan csökkenő sorozatát kapnánk ellentmondásként.

Gondoljunk bele a $\sqrt{2}$ irracionalitásának geomteriai bizonyítása is elmondható a végtelen leszállás módszerével. Ennek belátását az olvasóra bizzuk.

Középiskolában ezek az egyszerű példák is alkalmasak arra, hogy bemutassuk ezt a ritkán alkamlmazott módszert.

Most tovább két állítást bizonyítunk ezzel a módszerrel. Ebben a paragrafusban is a kulcsszavak keresése helyett végtelen leszállás módszerével megoldható feladatok keresését ajánljuk.

TÉTEL: *Az*

$$a^2 + b^2 = 3(c^2 + d^2)$$

egyenletnek a pozitív egészek körében nincs megoldása.

BIZONYÍTÁS:

Mivel $3|a^2 + b^2$ és mivel $x^2 \equiv 0,\ 1(\mod 3)$ ezért $3|a$ és $3|b$. Így $a = 3a_1$; $b = 3b_1$ és így

$$3(a_1^2 + b_1^2) = c^2 + d^2.$$

Ezt az eljárást folytatva pozitív egész számok csökkenő és végtelen sorozatát kapjuk ellentmondásként.

A következő feladat, amiben ugyancsak a végtelen leszállás módszerét (és a teljes indukciót) használjuk, Terence Taotól származik.

TÉTEL: *Tegyük fel, hogy egy G véges csoport négy elemére, $a, b, c, d \in G$*

$$ab = ba^2 \quad bc = cb^2 \quad cd = dc^2 \quad da = ad^2.$$

Ekkor ez csak úgy teljesülhet, ha $a = b = c = d = 1$.

BIZONYÍTÁS:

1. A $ab = ba^2$ feltételt úgy is írhatjuk, hogy $a^2 = b^{-1}ab$. Innen teljes indukcióval igazolható, hogy

$$a^{2^n} = b^{-n}ab^n. \quad (*)$$

2. Jelölje egy x elem rendjét $o(x) = s$, azaz $x^s = 1$.

Igazolni fogjuk, hogy ha p egy prímszám és $p|o(a)$, akkor $o(b)|p-1$. Legyen $o(b) = n$. Akkor $(*)$ és $b^{-n} = b^n = 1$ miatt $a^{2^n} = a$, azaz

$$a^{2^n-1} = 1.$$

De így

$$p|o(a)|2^n - 1,$$

ezért a kis Fermat-tétel miatt $n = o(b)|p - 1$.

3. Ezért az 1. ill. 2. pontokban elmondottak alapján:

$$p_1|o(a) \Rightarrow o(b)|p_1 - 1$$

ezért, ha

$$p_2|o(b) \Rightarrow p_2 < p_1.$$
$$p_2|o(b) \Rightarrow o(c)|p_2 - 1$$

ezért, ha

$$p_3|o(c) \Rightarrow p_3 < p_2.$$
$$p_3|o(c) \Rightarrow o(d)|p_3 - 1$$
$$p_4|o(d) \Rightarrow p_3 < p_4.$$

Végül

$$o(a)|p_4 - 1; p_5|o(a) \Rightarrow p_5 < p_4.$$

Így prímek egy végtelen csökkenő sorozatát kaptuk.

Ellentmondást akkor nem kapunk, ha ezek a prímek nem léteznek, azaz mindegyik elem rendje 1, azaz maguk is az egységek, vagy akkor sincs ellentmondás, ha feltesszük, hogy a csoport végtelen számosságú.

13. Függvények, Egyenletek, Polinomok

Ebben a paragrafusban olyan egyenleteket tekintünk, amelyek megoldása nem a szokásos utat követi, és amik mögött lépten-nyomon fellelhetőek az egyetemen tanultak.

Feladatok:

1. Bizonyítsuk be, hogy ha $a < b < c$, akkor az

$$(x-a)(x-b) + (x-a)(x-c) + (x-c)(x-b) = 0$$

egyenletnek léteznek valós gyökei x_1, x_2, amelyekre $a < x_1 < b < x_2 < c$.

I. Megoldás:

Ha felbontjuk a zárójeleket és összegyűjtjük a közös tagokat, akkor egy másodfokú egyenletet kapunk:

$$3x^2 - 2(a+b+c) + (ab+ac+bc) = 0.$$

Két különböző valós gyökünk van, ha

$$D = 4(a+b+c)^2 - 12(ab+ac+bc) > 0.$$

Ám

$$D = 4(a^2+b^2+c^2-ab-ac-bc) = 2((a-b)^2+(a-c)^2+(c-b)^2),$$

ami nyilván pozitív. A $a < x_1 < b < x_2 < c$ feltétel bizonyítását most nem végezzük el.

II. Megoldás:

Legyen $p(x) = (x-a)(x-b)+(x-a)(x-c)+(x-c)(x-b)$. Az $a < b < c$ feltétel miatt

$$p(a) = (a-c)(a-b) > 0; \quad p(b) = (b-a)(b-c) < 0; \quad p(c) = (c-a)(c-b) > 0,$$

amiből következik az állítás. Részletes indoklást elhagytuk; a Kulcsszavaknák kell kiegészíteni, mit is használtunk pontosan itt.

III. Megoldás:

Legyen $f(x) = (x-a)(x-b)(x-x)$. Ekkor

$$f'(x) = (x-a)(x-b) + (x-a)(x-c) + (x-c)(x-b),$$

léteznek tehát x_1, x_2, amelyekre $a < x_1 < b < x_2 < c$ és $f'(x_1) = f'(x_2) = 0$.

Kulcsszavak:

2. Legyen

$$p(x) = x^4 + 3x^3 - 7x^2 + x + 2.$$

Írjuk fel $p(x)$-et, mint $(x-1)$ polinomját!

I. Megoldás (vázlat):

Tehát meg kell határozni az A, B, C, D és E értékét úgy, hogy

$$x^4 + 3x^3 - 7x^2 + x + 2 = A(x-1)^4 + B(x-1)^3 + C(x-1)^2 + D(x-1) + E$$

legyen.

Felbontva a zárójeleket, az öt ismeretlenre egy lineáris egyenletrendszert kapunk. Ezt a jól ismert Gauss-Jordan eliminációs módszerrel a középiskolában (is) megoldhatjuk.

II. Megoldás

Az E nyilván $p(1)$. $p'(1) = D$; $p"(1) = 2C$; $p'''(1) = 6B$; A nyilván 1.
Így

$$x^4 + 3x^3 - 7x^2 + x + 2 = (x-1)^4 + 14(x-1)^3 + 8(x-1)^2.$$

Kulcsszó: (Ezt a bizonyítási ötletet milyen általános tétel bizonyításánál használják?)

III. Megoldás:

Használjuk az $f(x)$ polinomra a maradékos osztást, azaz osszuk el $f(x)-$et $(x-1)$-gyel. A maradék nyilván E lesz, A hányadost megint osszuk el $(x-1)$-gyel, a maradék D lesz. Folytatva az eljárást megkapjuk az összes együtthatót.

3. Oldjuk meg a következő egyenletet!

$$8^x(3x+1) = 4$$

Megoldás

Gyorsan látható, hogy az $x = 1/3$ megoldás. (Talán ezt sugallja az is, hogy 8 – egy köbszám – az alapja az exponenciális tényezőnek).

Világos, hogy meg kell néznünk, van-e más megoldás: mivel mind 8^x, mind $(3x+1)$ szigorúan növekedő függvények, az egyenletnek legfeljebb egy megoldása lehet.

Kulcsszó: (A monotonitáson kívül miket is használtunk fel?)

4. Oldjuk meg!

$$4^x = 2x + 1$$

Megoldás

Az $x = 0$ és az $x = 1/2$ a megoldások.

Kulcsszó: (Milyen alaki tulajdonságait használtuk fel a 4^x és az $1 + 2x$ függvényeknek?)

5. Oldjuk meg!

$$2^x + 3^x = 5^x$$

Megoldás

Ekvivalens átalakítás után:

$$\left(\frac{2}{5}\right)^x + \left(\frac{3}{5}\right)^x = 1.$$

Ennek az $x = 1$ és csak ez a megoldása.

Kulcsszó: Mit használtunk fel?

6. Oldjuk meg!

$$4^x + 9^x + 25^x = 6^x + 10^x + 15^x$$

Megoldás

Legyen $a = 2^x;\ b = 3^x;\ c = 5^x$. Ekkor az egyenlet

$$a^2 + b^2 + c^2 = ab + ac + bc$$

alakba írható át. Ez ekvivalens az

$$(a-b)^2 + (a-c)^2 + (b-c)^2 = 0$$

egyenlettel.

A megoldás $x = 0$.

Kulcsszó:

A középiskolában előkerül a függvények **periódusának**, a periodikus függvényeknek a fogalma.

Például a trigonometrikus függvények és egyenletek megoldásánál fontos, hogy hangsúlyozott legyen a periodikus megoldások jelzése (és $+k2\pi :\ k \in \mathbb{Z}$ vagy $+k\pi :\ k \in \mathbb{Z}$ stb.) Általában is fontos, hogy tudjuk, milyen a *szerkezete* a periódusok halmazának. Erre a következő egyszerű állítás ad választ:

TÉTEL: *Legyen P_f a minden valós számon értelmezett függvény periódusainak a halmaza, azaz legyen*

$$P_f := \{p \in \mathbb{R} : \forall x \in \mathbb{R}\ f(x+p) = f(x)\}.$$

(értsük ebbe a halmazba a $p = 0$ értéket is).

Ekkor a $(P_f, +)$ egy additív csoport.

BIZONYÍTÁS:

Mivel $P_f \subseteq \mathbb{R}$, továbbá 0 az egységelem ezért csak a zártságot és inverz létezését kell igazolni.

1. Zárt

Ha $p_1, p_2 \in P_f$, akkor $\forall x \in \mathbb{R}$

$$f(x + (p_1 + p_2)) = f((x + p_1) + p_2) = f(x + p_1) = f(x).$$

Az első egyenlőségnél azt használtuk, hogy p_2, a másodiknál azt, hogy p_1 periódus.

2. Inverz
Ha $p \in P_f$, akkor

$$f(x) = f(x+p-p) = f((x-p)+p) = f(x-p) = f(x+(-p)),$$

azaz $-p \in P_f$.

A kérdést meg is fordíthatjuk; ha adott a $(P,+)$ additív csoport van-e olyan f, hogy $P_f = P$? A válasz igenlő:

TÉTEL: *Legyen $(P,+)$ egy additív csoport, $P \subseteq \mathbb{R}$. Ekkor létezik olyan mindenhol értelmezett f függvény, hogy*

$$P_f = P.$$

Az utóbbi tételt feladatként – speciális esetben – fel is adhatjuk szakkörön (természetesen nem szükséges megemlíteni, hogy a P csoport)

BIZONYÍTÁS:
Legyen

$$f(x) = \begin{cases} 1 & x \in P \\ 0 & x \notin P \end{cases}$$

Bebizonyítjuk, hogy $P_f = P$.
Legyen $p \in P$. Ekkor ha $x \in P$, akkor $f(x) = 1$ és $p+x \in P$, mivel P zárt az összeadásra, de így $f(x+p) = 1$. Ha $x \notin P$, akkor $x+p \notin P$, (ellenkező esetben, azaz ha $x+p = p'$, akkor $x = p'-p \in P$ ellentmondásként) így $f(x) = 0$ és $f(x+p) = 0$. Azt kaptuk, hogy mindkét esetben, azaz $\forall x \in \mathbb{R}$,

$$f(x+p) = f(x).$$

Végül azt kell igazolnunk, ha $q \notin P$, akkor q nem periódus. $0 \in P$, így $f(0) = 1$, de $f(0+q) = f(q) = 0$, azaz q nem periódus.
□□□

MEGJEGYZÉS:
1. A bizonyításban szereplő $f(x)$ függvény emlékeztet bennünket az analízisben megismert Dirichlet függvényhez. Ez persze nem véletlen.

FELADAT:

Határozzuk meg a Dirichlet függvény P_D periódushalmazát!

2. Ez is egy jó alkalom, hogy – mondjuk szakkörön – struktúrák-függvények ismereteket bővítsük. Például legyen $P = \{p = a+b\sqrt{2} : a, b \in \mathbb{Z}\}$ halmazzal definiáljuk a fenti megadásos függvényt. A bizonyítás során - mármint, hogy P halmaz (és csak ezek) elemei a periódusok, valójában végigmegy a csoport axiómákon.

Periodikus függvényekkel kapcsolatosan további sok szép feladatot lehet készíteni az előbb elmondottak alapján.

Ismert feladat a következő:

FELADAT:

Tegyük fel, hogy $f(x)$ és $g(x)$ mindenhol értelmezett függvények p ill. q szerint periodikusak és hogy p/q racionális szám.

Igazoljuk, hogy $f(x) + g(x)$ is periodikus függvény!

MEGOLDÁS:

A feltétel szerint $p/q = a/b;\ a, b \in \mathbb{Z}; b > 0$. Ekkor

$$p \cdot b = q \cdot a$$

és mivel ha egy szám periódus, annak egész számú többszöröse is az, ezért

$$f(x + p \cdot b) + g(x + q \cdot a) = f(x) + g(x)$$

azaz $f(x) + g(x)$, $P = p \cdot b = q \cdot a$ szerint periodikus függvény.

(Ebben a megoldásban is előjött a periódushalmaz csoport tulajdonsága).

14. Logika

Újsághír:

"Ha István napján szép az idő

A népi jóslat szerint, ha karácsony második napján szép, napos idő van, akkor száraz nyár és jó bor várható. A mai borús, esős nap tehát nem sok jót ígér a borászoknak."

NOL, 2012.12.25.

Talán ez az egyik legfontosabb fejezete e jegyzetnek. A köznapi beszédben is igencsak sokszor előfordul logikailag hibás indoklás, kijelentés, (mindjárt meg is vizsgáljuk a fenti idézett újsághírt).

A matematika órákon viszont kiemelt szerepe van annak, hogy a szabatos gondolkodást tanítsuk; ennek komoly része az, hogy minden nehézség, "gondolkodás nélkül" használjuk az alapvető logikai szabályokat, és (ha kell) észrevegyük a hamis következtetéseket.

Vizsgáljuk meg, mi a gond az idézett újsághírrel. Két állítás és a közöttük levő következtetés a megfigyelésen alapuló néphit: A állítás: A =karácsony második napján szép, napos idő van. B =száraz nyár és jó bor várható. A népi megfigyelés:

$$A \Rightarrow B.$$

Miért kesereg az újságíró? "A mai borús, esős nap tehát nem sok jót ígér a borászoknak." Azaz implicit azt mondja: $\neg A$ =*A mai borús, esős nap*; $\neg B$ =*nem sok jót ígér a borászoknak (= nem várható jó bor)* és a kijelentés:

$$\neg A \Rightarrow \neg B.$$

Azonban $A \Rightarrow B$ kijelentés nem azonos $\neg A \Rightarrow \neg B$ állítással. Az újságíró hamis következtetést tett.

Helyesen $\neg B \Rightarrow \neg A$, azaz a következő lenne a helyes (reméljük nem így lesz); "A 2013. év nyara borongós volt, rossz szőlő termést szüreteltek; persze, az elmúlt karácsony másnapja nem is volt szép, napos".

Érdemes tisztázni, és számos példán megerősíteni a szükséges, az elégséges és a szükséges és elégséges feltételeket. Számos ekvivalencia bizonyításakor, (ami nem is olyan ritka a középiskolában) azt mondjuk: Az

$$A \Leftrightarrow B$$

állítást bizonyítjuk; első lépésben a "szükséges"

$$A \Rightarrow B$$

feltételt bizonyítjuk, második lépésben a

$$B \Rightarrow A$$

"elégséges" feltételt igazoljuk.

NEM HAGYHATJUK KÉTSÉGEK KÖZÖTT A TANULÓKAT, HOGY PONTOSAN MIT ÉRTÜNK EZ ALATT,

azaz mi minek a szükséges illetve elégséges feltétele.

A "szükséges" és "elégséges" szavak az állítások egymáshoz viszonyított szerepében kapnak értelmet. Érdemes elmondani a klasszikus:

"Ha esik az eső, akkor vizesek az utcák"

kijelentést.

A "vizesek az utcák" az "esik az eső" szükséges feltétele (valóban ha esik az eső, szükségképpen vizesek az utcák); A=esik az eső; B=vizesek az utcák, az előbbi kijelentés $A \Rightarrow B$ formában írható le, míg az esik az eső mondat a vizes a járda mondat elégséges feltétele: (valóban a vizes járdához pl. elég, ha esik az eső). Természetesen hangsúlyozni kell, hogy nem azt állítottuk, hogy itt a feltételek szükséges **és** elégséges feltételek. Ezen a példán is szépen lehet illusztrálni, hogy ez se azonos $\neg A \Rightarrow \neg B$ állítással.

Talán érdemes megjegyezni, hogy a szükséges feltétel a sokszor használt latin "sine qua non" kifejezés.

Kijelentéslogika

Az egyetemi logika előadásain ismertetett kijelentéslogika elemei lehetőséget adnak arra, hogy számos, néha igencsak nehezen követhető, játékos matematikai – logikai feladat megoldását könnyebben átláthassuk.

Emlékeztetnénk, hogy egy

$$X_1, X_2, \ldots, X_n \models K$$

következetetés helyes, ha mindannyiszor, amikor a premisszák $(X_1, X_2, \ldots, X_n)$ helyesek, a konklúzió (K) helyes.

Lássunk néhány példát és annak didaktikai vonatkozását:

1. "– *A Van Gogh tényleg hiányzik a falról – szólt Watson, és odasétált a kandallóhoz – de vajon tényleg elllopták-e? – Nos, – nézett Watsonra Holmes, és kivette a pipát a szájából, – ha a Van Gogh-ot tényleg ellopták, és nem White a tolvaj, akkor csak nappal történhetett az eset. Holmes leült a bőrfotelbe és folytatta. – Ha a Van Gogh-ot tényleg ellopták, – ismételte meg - és éjszaka volt... nos, akkor világos: White a tolvaj.*"

Döntsük el, hogy Sherlock Holmes helyesen következtetett-e!

Felírjuk a következtetési sémáját Holmes kijelentéseinek. Legyen
A=Van Gogh-ot tényleg ellopták
B=nem White a tolvaj
C=nappal történt az eset.
Ekkor a kijelentés

$$A \wedge B \to C,\ A \wedge \neg C \ \models \neg B.$$

A következetetés helyes: ha a premisszák helyesek, akkor a konklúzió is helyes. Az állítás igazságtartalmát $|\cdot|-$vel jelöljük.

Mivel $|A \wedge \neg C| = i$, ezért $|A| = |\neg C| = i$ és így $|A| = i$, $|C| = h$. $|A \wedge B \to C| = i$ és $|C| = h$, ezért $|A \wedge B| = h$ (hamisból következhet hamis), így $|B| = h$, tehát $\neg B$, a konklúzió igaz. Mint sokszor, most is Holmes-nak volt igaza.

Az ilyen feladatok megoldásánál több probléma is felmerülhet:

1. A szövegértés. Ezeknél a feladatoknál sokszor kissé mesterkélt a szöveg (a feladat szerzője, jelen esetben e sorok írója a következtetési sémát írta fel, és kreált hozzá többé-kevésbé épkézláb történetet).

2. A mondatrészek értelmezése. Meggyőződésem, hogy ilyen feladatot csak bizonyos érettségi fok mellett lehet feladni (akkor is, mondjuk szakkörön), továbbá, talán meglepő módon a formalizmus segíti a megoldást. Tehát érdemes kijelentések értékéről beszélni, továbbá tisztázni a műveletek értékeit. (Az előbbi feladatban is fontos, a matematikában is hasznos műveletek, diszjunkció, konjunkció, implikáció, negáció szerepeltek.)

Tapasztalatom szerint az alábbi alapkövetkeztetések igazságának bizonyításai népszerűek a hallgatóság körében:

Modus ponens:

$$A, A \to B \models B$$

Indirket bizonyítás:

$$\neg A \to \neg B, B \models A$$

Kontrapozíció:

$$A \to B \models \neg B \to \neg A$$

Hipotetikus szillogizmuss:

$$A \to B, B \to C \models A \to C$$

Reductio ad absurdum:

$$\neg A \to B, \neg A \to \neg B \models A$$

1.Feladat: Készítsünk szöveget az alábbi következtetési formulához, és döntsük el igazságtartalmát.

$$\neg A \to (B \vee C), \neg B \to (\neg A \wedge D), D \to (B \vee C) \models B$$

2.Feladat: *"Amikor ... miskolci önkormányzati képviselő közleményben tudatta, hogy a támadások miatt felesége és anyósa lemond a trafikpályázaton elnyert négy-négy koncesszióról, egy kommentelő azt találta írni, hogy ez a képviselő legalább nyugodtan alszik majd ezután.*

Amiben ugyebár az is benne van, hogy akik viszont benne maradtak a trafikmutyiban, azoknak szörnyű éjszakáik vannak, egy percet se tudnak aludni"

Megyesi Gusztáv: Nyugodtan alszanak NOL (2013. 06.15.)

Milyen logikai hiba van a fenti mondatokban?

3.Feladat: *Az alábbi blogban olvasható:*

"A Kossuth téren látható ez a tömören megfogalmazott táblafelirat: 'Tourist stop!'

Aki nem turista, az ezek szerint ide bemehet, ugye?"

(http://leiterjakab.blog.hu/2013/05/11/turistamegallo)

Hát ebben hol a hiba?

MEGJEGYZÉS: Ez a feladat az egyetemi hallgatóság egy részében vitát váltot ki. Egy hangsúlyos érv (tehát az ellen, hogy ez hibás) az volt, hogy a *köznapi* értelemben vett következtetés nem szabad, hogy azonos legyen a matematikai logika szabatos következtetésével. A demokratikus társadalmakban amit nem tiltanak, azt szabad. Halkan megjegyezném, hogy már ez a *vita* is társadalom formáló volt (ha nem is jelentős mértékben); beszéltünk erről a dologról. Az 5. feladat még inkább egy szép példa erre.

4.FELADAT: *Már gyerekkorban rosszul kondícionáljuk a gyerekeket. Sokszor lehet ezt hallani: Apa: "Ha nem eszed meg a spenótot, nem kapsz csokit!" Valószínű, hogy a gyerek logikai készségét elég erősen javítaná, ha amint megettea spenótot, mégsem kapna csokit.*

De, hogy e jó példát is említsünk egy hír:

5.FELADAT:

Fordulópontot hozhat a kisebbségi nyelvhasználatban a kolozsvári törvényszék döntése, amely kötelezi a város polgármesterét a magyar nyelvű helységnévtáblák kifüggesztésére. ...Az ítélet kimondja, hogy a húsz százalék alatti kisebbségek is élhetnek a helyi közigazgatási törvényben meghatározott nyelvi jogokkal.

Ismeretes, hogy a törvény az írja elő, hogy húsz százalék felett a kisebbségek élhetnek e jogukkal. Ami viszont nem azonos azzal, hogy e százalék alatt nem élhetnek ezzel. A magyar nyelvű helységnévtáblákat saját pénzből ki lehet tenni.

Megjegyzés: Talán egy érdekes feladat lehetne hamis következtetések után vadászni a médiában. (Valószínú, hogy a fenti néhány példa nem az összes)