

Bízhatunk-e a matematikában ?

Szalkai István

Pannon Egyetem, Veszprém

szalkai@almos.uni-pannon.hu

Micsoda? - kaphatja fel fejét az Olvasó. "Hát korunk változásai már a matematika alapjait is megrengették?" Hiszen tudjuk, hogy a többi alap- és mérnöki tudomány is erre épül, sőt! Az iskolában megtanultuk, hogy a matematika (szinte) mindenre ad receptet: terület és térfogatképletek, rejtélyes szövegű feladatok megoldási módszerei, másodfokú egyenletek megoldóképlete, geometriai szerkesztési fogások, stb. Az egyetemeken a differenciál- és integrálszámítás segítségével bonyolult mechanikai feladatokat oldhatunk meg "könnyedén" (görbületi sugár, tehetetlenségi nyomaték, differenciálegyenletek megoldása, stb.). A modern optimumszámítási eredmények és numerikus módszerek arra is kielégítő választ adnak, hogy terjedelmes képletek és eljárási utasítások helyett hogyan kaphatunk algoritmusok (számítógépek) segítségével áttekinthető végeredményeket. Repülőgépek, űrhajók, GPS -ez mind matematika! Sőt, szinte már helyettünk is gondolkodnak ezek az okos masinák!

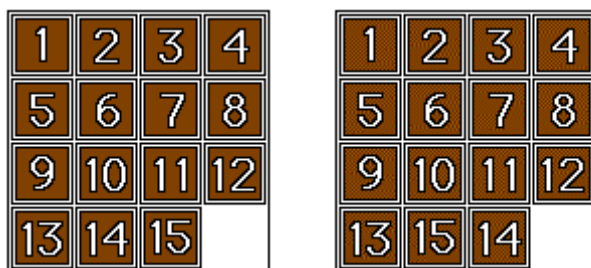
De sajnos a tanult módszereknek korlátai vannak, mint ezt nem csak a bennfentesek tudják.

Jelen összeállításunk elsősorban laikus Olvasókhöz szól: a MATEMATIKA néhány ismert és kevésbé ismert, meglepő eredményét, problémáját mutatjuk be. Ha egyik-másik fejezet nem nyeri meg tetszését, kérjük ne adja fel - lapozzon tovább, hátha a következő érdekesebb lesz.

I.

Kombinett

Mielőtt azonban fejest ugornánk a komoly matematikai eredmények tárgyalásába, bemelegítésként nézzük meg közelebbről az ún. *kombinett* vagy más néven a *15-ös* játékot. 15 kis négyzet alakú kő van egy 4x4 -es nagyobb négyzet alakú tartóban, 1-től 15-ig megszámozva. Így egy üres hely marad, mint az 1.a) ábrán látható. A köveket kiborítjuk, majd össze-vissza berakjuk őket a tartóba, például mint az 1.b) ábrán látható. A cél az, hogy az üres hely kihasználásával a köveket jobbra-balra és fel-le tologatva visszaállítsuk eredeti sorrendjükbe. Azonban az 1.b) ábra szerinti elrendezésből kiindulva sohasem jutunk vissza az eredeti állapotba.



A kombinett játék eredeti és egy összekevert állása

1. ábra

A játék felfedezését Sam Loyd (1841-1911) múlt században élt amerikai "mindenestudó"-nak tulajdonítják. (Loyd úr fenti feladványa sajnos sok ember életét követelte, ld. pl. [WWW].)

Matematikai eszközökkel hogyan lehet valamilyen feladatról bebizonyítani, hogy lehetetlen annak megoldása? Egyszerűen!

Minden lépésünkben a kövek sorrendjét változtatjuk. Célunk az olyan "kellemetlen" helyzetek megszüntetése, amelyekben valamelyik nagyobb szám a sorban (a táblázatot jobbról balra és felülről lefelé olvasva) megelőz egy kisebb számot. Nevezzünk minden ilyen helyzetet (azaz min-

den ilyen helyzetű nagyobb-kisebb számpárt) *inverzió*nak. (Az 1.b. ábrán pontosan 1 inverzió található: 15-14.) A lépések szerkezetét elemezve beláthatjuk, hogy ha vízszintesen toljuk valamelyik követ, akkor az inverziók száma nem változik, míg minden függőleges elmozdítás esetén számuk pontosan 3 -mal változik. Tehát az inverziók számát a függőleges mozgások változtatják. Minden függőleges lépésnél a "lyuk" is egy-egy szinttel feljebb vagy lejjebb kerül. De a játék befejezésekor visszakerül eredeti szintjére, vagyis összesen páros sok függőleges lépésünk volt. De ez azt jelenti, hogy az inverziók száma páros*3 azaz páros számmal változott meg. Mivel az 1.b) ábrán páratlan, míg az 1.a) ábrán 0 azaz páros számú inverziót találunk, így valóban soha nem juthatunk megengedett lépések sorozatával az 1.b. ábra szerinti elrendezésből az eredeti sorrendhez. (A fenti okoskodást részletesebben megtaláljuk az Élet és Tudomány folyóirat 1963/39., 40. és 42. számaiban.)

Rubik kocka

Hasonló ötlettel mutathatjuk meg például azt is, hogy a Rubik Ernő féle bűvös kockát alaphelyzetéből kiindulva nem tudjuk úgy tekergetni, hogy a tekergetés után minden kockája alaphelyzetébe kerüljön vissza, kivéve egyetlen sarokkockát, amely eredeti állapotához képest valamire elfordult. A részletesebb elemzést például Csákány Béla [CsB] könyvében találhatjuk.

Most néhány komolyabb eredményt ismertetünk, amelyek bizonyítása azonban hasonló ötleteken alapszik.

Algebrai egyenletek

A harmad- és negyedfokú algebrai egyenletek (vagyis az $ax^3+bx^2+cx+d=0$ illetve az $ax^4+bx^3+cx^2+dx+e=0$ alakú egyenletek, ahol a,b,c,d,e tetszőleges adott valós számok, $a \neq 0$) gyökeit *Girolamo Cardano* (1501-1576), *Nicolo Fontana Tartaglia* (1500-1557) és *Ludovico Ferrari* (1522-1565) olasz matematikusok jóvoltából pontosan meg tudjuk határozni az alpműveletek és gyökvonások segítségével. A másodfokú egyenletek megoldóképletét már ie. 250-ben leírta *Diophantos* görög matematikus. Csak többszáz éves próbálkozás után sikerült *Paolo Ruffini* (1765-1822) olasz matematikusoknak megmutatnia, hogy nem létezik olyan, csak alpműveleteket és gyökvonásokat használó általános eljárás, amely tetszőleges ötöd- vagy magasabbfokú egyenletek gyökeit megadná! Ruffini eredeti bizonyítása hiányos volt, a hiányt *Niels Henrik Abel* (1802-1829) norvég és *Bolyai János* (1802-1860) magyar matematikusok pótolták, ez a híres **Abel-Ruffini-Bolyai Tétel**. (Speciális egyenletek persze egyedi módszerekkel megoldhatóak, mint pl. $x^5-1=0$ vagy $x^5-x^4+x^3-x^2+x-1=0$.) Sőt, *Évariste Galois* (1811-1832) francia matematikus halála előtti éjszakán (!) megírt munkájában általánosan leírta azon magasabbfokú egyenletek típusait, amelyek a megengedett műveletekkel megoldhatóak.

Geometriai szerkesztések

A középiskolai feladatgyűjtemények bővelkednek különböző szerkesztési feladatokban, és e feladatokat oldogatva talán eszünkbe sem jut, hogy vannak körzővel és vonalzóval nem megszerkeszthető feladatok. Ráadásul nem csak a nevezetes problémák (a kör négyeszetesítése, szög harmadolása, kocka kettőzése) ilyenek, hanem például háromszöget sem tudunk szerkeszteni (csak körző és mm-beosztás nélküli egyenes vonalzó segítségével), ha mondjuk csak a három szögfelezője adott. Hogy miért? Belátható ugyanis, hogy munkánk során csak olyan szakaszokat tudunk megszerkeszteni, melyek hossza kifejezhető a négy alpművelet és a négyzetgyökvonás segítségével, az adott szakaszok és az egységszakasz hosszának felhasználásával. Az algebra eszközeivel *Carl Friedrich Gauss* (1777-1855) német matematikus igazolta, hogy nem szerkeszthető meg olyan szakasz, amelynek hossza nem gyöke egyetlen racionális együtthatójú egyenletnek sem. Márpedig a kockakettőzés $\sqrt[3]{2}$, a szögharmadolás a tetszőleges b valós számra a $4x^3-3x-b=0$ egyenletek gyökeinek, és végül a kör négyeszetesítése π megszerkesztését kívánna meg. Ez utóbbiról *Ferdinand Lindemann* (1852-1929) német matematikus 1882-ben mutatta meg, hogy transzcendens, azaz nem gyöke egyetlen racionális együtthatójú egyenletnek sem.

Átdarabolások

A Természet Világa 1991 februári számában egy olvasmányos cikkben *Pálfy Péter Pál* arról értesít bennünket, hogy *Lackovich Miklós*, az ELTE TTK Analízis Tanszékének docense 1990-ben mégis négyzögesítette a kört. Persze most nem a szokásos körzós-vonalzós szerkesztésről van szó! Lackovich megközelítési módja *Bolyai Farkas* (Bolyai János apja, 1775-1856) következő eredményéhez kapcsolódik (a részleteket Pálfy Péter cikkében vagy Weszely Tibor [WT] könyvének 81-84 oldalain megtalálhatjuk). Bolyai Farkas 1832-ben kiadott [BF] "Tentamen" c. könyvében igazolta azt a tételt, hogy bármely két egyenlő területű sokszög felbontható véges sok kisebb sokszögre úgy, hogy a két (nagy) sokszöget alkotó kisebb sokszögek egymással párosával egybevágóak legyenek. Vagyis, ha az egyik sokszöget papírból kivágjuk, akkor ollóval apróbb sokszögekre vágjuk úgy, hogy e kis darabokból éppen a másik nagy sokszöget tudjuk kirakni, tehát az egyik sokszöget átdaraboltuk a másik sokszöggé. Be kell vallanunk azért, hogy Lackovich Miklós nem közönséges ollóval darabol, hanem (matematikai) részhalmozokra bontotta a kört és a négyzetet.

Térben azonban bonyolultabb a helyzet: *Max Dehn* német matematikus 1902-ben igazolta, hogy pl. két, egyenlő alapterületű és egyenlő magasságú gúla sem darabolható át mindig egymásba!

Dehn bizonyítása nehéz, azonban a következő rejtélyt az Olvasó maga is megoldhatja, kis fejtörés után. Egy nagy kockát ügyesen vagdosva elérhetjük, hogy minden lépésünkben a már megkapott részekből annyit vágjunk ketté, amennyit akarunk, még hozzá egyetlen nyisszantással. Vagyis 5 vágás után akár $2^5=32$ részünk is lehetne. Mégis, egy $3 \times 3 \times 3$ -as méretű nagy kockát 5 vágással nem tudjuk a 27 kis kockára felvágni! Miért?

Integrálhatóság

A differenciál- és integrálszámításba kicsit is belekóstolt Olvasó bizonyára találkozott már a következő problémával: vannak olyan függvények, melyek primitív függvénye, mint pl.

$$\int e^{x^2} dx, \quad \int \frac{e^x}{x} dx, \quad \Phi(x) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt, \quad Li(x) := \int \frac{1}{\ln(x)} dx,$$
$$\int \sin(x^2) dx, \quad \int \cos(x^2) dx, \quad Ci(x) := \int \frac{\cos(x)}{x} dx, \quad Si(x) := \int \frac{\sin(x)}{x} dx,$$
$$\int \sqrt{1 - k \cdot \sin^2(x)} dx \quad (k \neq 1)$$

nem adható meg *képlettel*. Nem tanultuk rosszul! *Isaac Newton* (1643-1727) egyik tételéből ugyan következik, hogy *tetszőleges* folytonos f függvény esetén $\int f(t) dt$ létezik, azonban *Joseph Liouville* (1809-1882) francia matematikus tétele szerint ezen primitív függvényekre képlet nincs: nem írható fel az elemi függvények: x^n , $\sqrt[n]{x}$, a^x , $\log_a(x)$, $\sin(x)$, $\cos(x)$, ..., valamint a négy alapművelet, a kompozíció (összetett függvény képzése) és az inverz-függvény képzése "operációk" segítségével. Erről bővebben [KI] -ben vagy [Szi4] -ben olvashatunk.

Pihenésképpen hallgassuk meg *Zerkovitz Béla* (1881-1948) magyar zeneszerző, még építész-mérnök hallgató korában írt *Integrál Böske* kuplóját: "Az életem a matematikáé', az analízist szörnyen szeretem, rajongok, ah, a geometriáé', Integrál Böske a nevem"

II.

Vannak azonban még súlyosabb problémák is.

Már *Gottfried Wilhelm Leibniz* (1646-1716) német matematikus és filozófus is foglalkozott a matematikai *állítások helyessége eldöntésének* és a *bizonyítások "gépesítésének"* gondolatával. Néhány évszázad múlva azonban világossá vált, hogy a számítógépek sem mindentudóak.

Megállási probléma

Például nézzük meg, hogy miért *nem készíthető* olyan univerzális számítógép (-program), amely tetszőleges programról és tetszőleges bemeneti adatról legalább annyit eldönt, hogy az adott programot a kérdéses adattal elindítva, a program futása megáll -e valamikor, véges idő után (bár ez elvben akár pl. 10^{6000} év is lehet), avagy végtelen sokáig számol, sohasem áll meg. Ezt a problémát hívják *megállási problémának*.

Nézzük, miért nem lehet ilyen programot készíteni. Ennek nem technikai akadályok vagy ügyetlen programozók az okai! Foglalkozzunk most csak olyan programokkal, melyek bemenete egyetlen természetes szám. Mint tudjuk, minden programot egy rögzített jelkészlettel írunk le (mint pl. a számítógép billentyűin látható jelek). E programok végül is véges hosszúak, így tekinthetjük őket e jelkészletből felépített "szavaknak". E szavakat abc- sorrendbe rakva kapjuk a $P_1, P_2, P_3 \dots P_i \dots$ listát, az összes lehetséges program listáját. Ugyanígy felsorolhatjuk az összes lehetséges input listáját: $I_1, I_2, I_3 \dots I_j \dots$. Tegyük fel most, hogy mégis van egy fenti tulajdonságú univerzális programunk: H . Például H inputként két természetes számot vár: tetszőleges i és j számra 1 -et ad ki, ha a P_i programot I_j -vel, mint inputtal elindítva a P_i program akármennyi, de véges idő múlva megáll, és mondjuk a H program 0 végeredményt ad, ha P_i sohasem áll meg j "hatására".

Most H felhasználásával írjuk meg a következő, mondjuk G -nek nevezett programot: *tetszőleges* x természetes számra, $H(x,x)=1$ esetén G fusson egy végtelen ciklusba, és $H(x,x)=0$ esetén állítsuk le G -t. G egy közönséges program, tehát szerepel a $P_1, P_2, P_3 \dots$ listán. Legyen mondjuk G éppen a P_K program.

Most nézzük meg, mit csinálna P_K , ha éppen a K adattal intítanánk. Ha P_K megállna valamikor, akkor $H(K,K)=1$ lenne, de ekkor, P_K a fentiek szerint végtelen ciklusba futna, ellentmondás. Ha pedig P_K nem állna meg a K adattal elindítva, akkor persze $H(K,K)=0$, vagyis P_K definíciója miatt P_K azonnal megáll, újabb ellentmondás.

Tehát a H univerzális gép *nem létezhet*, befejeztük a bizonyítást. \square

A P_K definíciójában alkalmazott csavaros ötletet szokás Cantor -féle átlós eljárásnak nevezni, *Georg Ferdinand Cantor* (1845-1918) német matematikus, a halmazelmélet atyja tiszteletére.

Diophantoszi egyenletek

Sajnos, a számítógépek még "hétköznapi" problémák megoldásához is alkalmatlanok. *Diophantos* (kb.200-kb.284) görög matematikus tiszteletére *diofantikus egyenleteknek* nevezzük az olyan egész együtthatós algebrai egyenleteket, melyeknek csak egész (pozitív és negatív) gyökeire vagyunk kíváncsiak. Például egy tetszőleges egyváltozós

$$\sum_{0 \leq i \leq n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 = 0 \quad (a_i \in \mathbb{Z})$$

algebrai egyenlet egész gyökei csak az a_0 (konstans) tag osztói lehetnek, ezeket számítógéppel meg lehet találni és ki lehet próbálni. *David Hilbert* (1862-1942) német matematikus 1900-ban, a párizsi Nemzetközi Matematikai Kongresszuson a XX. század kutatási irányát meghatározó előadásában többek között a következő problémát is megfogalmazta (melyet Hilbert 10. problémájaként is emlegetnek): Adjunk algoritmikus eljárást tetszőleges kétváltozós $\sum_{0 \leq i \leq n} \sum_{0 \leq j \leq m} a_{i,j} x^i y^j = 0 \quad (a_{i,j} \in \mathbb{Z})$ algebrai egyenlet egész gyökeinek megkeresésére. Csak 1969-ben sikerült *Juri Matijaszevics* fiatal orosz matematikusnak megmutatnia, hogy többváltozós, magasabbfokú diofantikus egyenletekre ilyen általános algoritmus nem létezik (akármilyen teljesítményű gépek és akármilyen ügyes programozók is lesznek a távoli jövőben) !

További megoldhatatlan problémák

Sajnos nagyon sok fontos probléma sem oldható meg számítógéppel, például a *génprobléma* sem: Adott kezdeti génállomány és mutációk adott halmaza esetén döntsük el, hogy egy adott betegség létrejöhet-e? A számítógépek működésének "furcsaságairól", korlátairól például az [AHU], [GJ],[GL],[GT], [LL], [NFR],[SzI2],[SzI3], [TV] vagy [TB] művekben olvashatunk részletesebben.

NP - teljes problémák

A számítógéppel megoldhatatlan problémák ellentétei az "univerzális" problémák. Leegyszerűsítve: Egy problémát NP-teljesnek (Nondeterministic Polynomial Complete) nevezünk, ha az alábbi kijelentés igaz rá: "Ha erre a problémára lenne gyors algoritmus, akkor a világ összes problémájára is lenne (azonnal!) gyors algoritmus". Példákat, precíz megfogalmazást és bizonyítást [SzI3] és [LL] -ben találhatunk.

"Mi ebben a meglepő?" -kérdézheti az Olvasó, aki eddig figyelmesen követte gondolatmenetünket. "A matematika egzakt tudomány, így minden módszerről pontosan megmondja, mik a korlátai. Legfeljebb újabb módszerek után kell néznünk." Sajnos ez távolról sem ilyen egyszerű. Ennek megértéséhez érdemes egy kicsit részletesebben megismerkednünk a matematika felépítésével, a matematikai bizonyítások mibenlétével. (Többek között így Leibniz problémájára is választ kapunk.) Az alábbiak megértése még több figyelmet kíván az Olvasótól, vegyünk tehát mély lélegzetet!

III.

A párhuzamossági axióma

A geometriában megtanultuk Euklidész *axiómáit*, melyeket ie. 300 körül vetett papírra. Az axiómák olyan "alapállítások", amelyekből kiindulva csupán logikus gondolkodás segítségével bebizonyíthatjuk a geometria összes tételét. (Euklidész az axiómákat "Elemek" c. művében foglalta össze, aminek magyar fordítása 1983-ban jelent meg a Gondolat kiadónál, interneten is megtalálható a MEK honlapján, ld. [EE].) Köztudott, hogy *Bolyai János* (1802-1860) 1831-ben, és *Nyikolaj Lobacsevszkij* (1792-1856) 1830-ban megjelent dolgozataiban megmutatták, hogy Euklidész ún. "párhuzamossági" axiómája (amely szerint egy adott ponton keresztül pontosan egy olyan egyenes húzható, amely egy másik, adott egyenessel párhuzamos) nem feltétlenül kell, hogy igaz legyen. Ha ugyanis ennek az axiómának a tagadását csatoljuk a többi megmaradt axiómához, akkor szintén egy értelmes, ellentmondást szintén nem tartalmazó axiómarendszert kapunk, ráadásul ennek alapján egy újabb, ún. "nem-euklideszi" geometriát is.

A geometriához hasonlóan a matematika többi ága is axiomatizálható. Pl. a számelmélet axiómái *Giuseppe Peano* (1858-1932) olasz matematikus nevéhez fűződnek, a halmazelméletben pedig *Ernst Zermelo* (1871-1953) német és *Adolf Fraenkel* (1891-1965) német-izraeli matematikusok axiómáit használjuk. Sőt, mint Hilbert, *Paul Bernays* és *Gerhard Gentzen* (1909-1945) kutatásai kimutatták, egyedül a halmazelmélet segítségével nemcsak a geometria és a számelmélet, hanem a matematika összes többi ága felépíthető (azaz fogalmai definiálhatók és tételei bebizonyíthatók). Így tehát elegendő a halmazelmélet "ingotag" épületét bemutatnunk. (A halmazelmélet modern leírását megtaláljuk például Halmos Pál [HP] valamint Hajnal András és Hamburger Péter [HH] könyveiben.)

A kontinuum-hipotézis

A halmazelmélet és a matematikai logika fejlődésére nagy hatást gyakorolt az ún. "kontinuum-hipotézis" (=folytonossági feltevés). Georg Cantor a XIX. század végén megmutatta (a róla elnevezett "átlós eljárással"), hogy a valós számok halmaza *nagyobb* számosságú, mint a természetes számok halmaza. (Két végtelen halmazt akkor nevezünk egyenlő számosságúnak, ha létezik közöttük egy kölcsönösen egyértelmű függvény azaz bijekció.) Már ő is felvetette azt a kérdést, vajon van -e a valós számok halmazának olyan részhalmeze, amely ugyan kisebb számosságú a valós számok halmazánál, de ugyanakkor nagyobb számosságú a természetes számok halmazánál. Ilyen halmaz létezését tagadja a *kontinuumhipotézis*, röviden KH kijelentés. A kontinuum hipotézist cáfoló halmazok keresése közben alakult ki a matematika egyik új ága, a leíró halmazelmélet. Később, az 1930-as években Gödel vizsgálta az ún. "konstruálható" (azaz definiálható) halmazok osztályát. Kimutatta: ha a "*minden halmaz konstruálható*" axióma (röviden $V=L$) igaz, akkor KH

is igaz, vagyis " $V=L \Rightarrow KH$ ". Gödel még azt is kimutatta, hogy a $V=L$ állítás a halmazelmélet axiómáiból nem cáfolható, és így KH sem.

Az 1960-as évek elején *Paul J. Cohen* amerikai matematikusnak véletlenül(!) sikerült megmutatnia, hogy a KH , sőt a $V=L$ állítás sem igazolható a halmazelmélet axiómáiból. Olyan modelleket (halmazokat) "kényszerített ki" (szakkifejezéssel "forszolt ki"), melyek teljesítik a halmazelmélet összes axiómáját, de bennük KH illetve $V=L$ hamis. (KH történetéről részletesebben olvashatunk Urbán János [UJ3] cikkében.) Cohen felfedezéséért Fields medált kapott, amely kitüntetés helyettesíti a matematikai Nobel díjat (ami tudvalevőleg nem létezik), és nem véletlenül. Olyan általános *módszert* fedezett fel, a "forszólást", amellyel szinte bármely állításról majdhogynem gépiesen (!) el lehet dönteni, hogy konzisztens-e, azaz nem vezet-e ellentmondásra a halmazelmélet axiómáival. Pontosabban, Cohen módszerével olyan modelleket (halmazokat) tudunk konstruálni, melyekben a halmazelmélet axiómái és a kérdéses állítás is teljesül. Ha pedig olyan másikat is sikerül "kiforszolni", amelyben a kérdéses állítás tagadása teljesül, akkor e két modell birtokában már biztosan mondhatjuk, hogy az állítás független az axiómáktól. Másként fogalmazva: nem bizonyítható, és nem is cáfolható az axiómákból.

További eldönthetetlen állítások

Századunkban, a matematikai logika precíz megalapozása következtében még meglepőbb tételeket ismerhettünk meg: *Alonzo Church* (1903-1995) 1936-ban igazolta a következő állítást: Minden "elégé bő" Γ axiómarendszer esetén, ha Γ nem vezet ellentmondásra, akkor nincs olyan *algorithmus*, amely tetszőleges állításról eldöntené, hogy az állítás Γ -ból bizonyítható-e. (A bizonyítás ötlete hasonlít az univerzális gépünk lehetetlenségére feljebb adott bizonyításunkhoz.)

Továbbmenve, *Kurt Gödel* (1906-1978) német származású matematikus 1931-ből származó ún. első "nemteljességi tétele" szerint ha Γ tetszőleges, szintén elégé bő és ellentmondást nem tartalmazó axiómarendszer, akkor létezik olyan φ állítás, mely nem bizonyítható és nem is cáfolható (csak Γ felhasználásával). Ekkor röviden azt mondjuk, hogy a φ állítás *független* a Γ axiómarendszerrel. A tétel szerint persze ha a kérdéses φ állítást (vagy éppenséggel annak tagadását) hozzávesszük a Γ axiómarendszerhez, akkor még mindig lesz olyan ψ állítás, mely független a kibővített axiómarendszerrel, s.i.t. Gödel bizonyítása csupán az ilyen φ állítás létezését mutatta meg. A rövid bizonyítás például [SzI1]-ben megtalálható.

Hamarosan azonban a matematika többi ágában is egymás után merültek fel olyan kérdések, melyek a használatos axiómarendszerektől *függetlenek*, azaz a használatos axiómarendszerekben sem bizonyítani sem cáfolni nem lehet őket. Először Gödel "második nemteljességi tételét" kell megemlítenünk, amely szerint: amennyiben Γ ellentmondástalan, akkor Γ *ellentmondástalansága* (szakkifejezéssel Γ **konzisztenciája**) csak Γ felhasználásával nem bizonyítható, és "természetesen" nem is cáfolható.

Következő példánk *Jeff Paris* eredménye, amelyre *Csirmaz László* adott meglepően szép bizonyítást néhány éve: A következő állítás nem bizonyítható és nem is cáfolható a számelmélet Peano-féle axiómarendszerében. "Legyenek k és n tetszőleges természetes számok, és színezzé az F függvényt a természetes számok k -elemű részhalmazait ki n színnel. Ekkor van a természetes számoknak olyan H részhalmaza, amelyre $F(A)=i$ valamely rögzített $i \leq n$ színre de H minden k -elemű A részhalmazára, és ha H legkisebb eleme h , akkor H legalább $h+1$ -elemű, és természetesen H legalább k -elemű."

Csirmaz ötletesen megmutatja, hogy egyrészt a fenti állítás a természetes számok standard, az iskolában megismert halmazában (ún. modelljében) igaz. Másrészt egy másik, ún. nem standard modellel is megismertet bennünket, amelyben a fenti állítás hamis: "Fűjjük fel" a pozitív racionális számokat oly módon, hogy mindegyik racionális szám helyett az egész (pozitív és negatív) számok halmazának egy miniatűr képmása álljon mégpedig úgy, hogy e kis halmazok "ne lógjanak egymásba". A 0 helyére pedig hasonló módon a természetes számok standard halmazának egy (kicsinyített) példányát illesszük. Az így kapott halmaz - hisszük vagy sem - teljesíti a számelmélet Peano-féle axiómarendszerét, sőt mi több, a Paris féle állítás itt hamis. Mivel pedig egyik modellben a Paris-

féle állítás igaz, míg egy másikban hamis, így (Gödel egy régebbi tétele szerint) független a Peano-axiómarendszerétől.

Mint említettük, a Cohen által feltalált forszolás módszere segítségével a matematika számos ágában sok felmerülő problémáról derült ki, hogy az axiómáktól függetlenek. Végezetül felsorolunk néhány ilyen állítást, azonban az Olvasó elnézését kérjük, ha ezek némelyike nehezen érthető:

- (a) Ha két Banach teret és a közöttük ható lineáris operátort formulákkal definiálhatunk, akkor az operátor folytonos (ld. [HJSz]).
- (b) \mathbf{R} -ben "alef-1" sok nullmértékű halmaz úniója is nullmértékű.
- (c) Ha R egy teljes, sűrű, végpont nélküli rendezett halmaz, melynek van megszámlálható sűrű részhalmaza, akkor R izomorf \mathbf{R} -el, a valós számok rendezett halmazával.
- (d) Ha κ olyan számosság, mely \mathbf{R} számosságánál kisebb de \mathbf{N} számosságánál nagyobb, és A_1, A_2, \dots, κ -nak tetszőleges részhalmazai, akkor van olyan A_{i1}, A_{i2}, \dots részsorozat, melynek van limesze, azaz $\bigcap_{k \in \mathbf{N}} \bigcup_{j > k} A_{ij} = \bigcup_{k \in \mathbf{N}} \bigcap_{j > k} A_{ij}$.

A matematikai logika precíz felépítése, és Cohen módszerének vázlatos leírása megtalálható Horváth Miklós, Joó István(†) és Szalkai István [HJSz] cikkében, mely tudomásunk szerint [UL] mellett az egyetlen magyar nyelvű modern bevezetés.

A címben feltett kérdésre pedig tömören így felelhetnénk: Igen, bízhatunk a matematikában, mert a tőle megszokott alapossággal nem csak a módszerek, hanem axiómarendszerünk és bizonyításaink lehetséges határait is megmutatja.

Végül álljon itt még néhány további javasolt olvasnivaló az Érdeklődő Olvasók számára.

Halmazelmélet, matematikai logika

- [HB] Barwise, J.(ed.): *Handbook of Mathematical Logics*, 3. rész, North-Holland, 1977.
- [HH] Hajnal András-Hamburger Péter: *Halmazelmélet*, Tankönyvkiadó, 1983.
- [HJSz] Horváth Miklós, Joó István, Szalkai István: A "Banach-elv" -ről, Matematikai Lapok, 34 (1991), 253-300., <http://math.uni-pannon.hu/~szalkai/BanachMatL.pdf>
- [HP] Halmos Pál: *Elemi halmazelmélet*, Műszaki Kiadó, 1981.
- [PR] Péter Rózsa: *Játék a végtelennel*, többszöri kiadás, utolsó fejezet
- [SzI1] Szalkai István: *Gödel's 1'st Incompleteness Theorem*, oktatási segédlet, 2006, <http://math.uni-pannon.hu/~szalkai/Godel-sk.pdf>
- [UL] Úry László: *Ellentmondásos-e a matematika?*, Középiskolai Matematikai Lapok, 1976/5, 194-205., [http://math.uni-pannon.hu/~szalkai/UryL-cikke\(bmp\).zip](http://math.uni-pannon.hu/~szalkai/UryL-cikke(bmp).zip)
- [UJ1] Urbán János: *Matematikai logika*, Gimnáziumi tankönyv, Tankönyvkiadó, 1987.
- [UJ2] ----- : *Matematikai logika*, Műszaki Kiadó, 1987. ("Bolyai könyvek" sorozat)
- [UJ3] ----- : *A kontinuum-sejtés*, Középiskolai Matematikai Lapok 1991 január, 1-7. oldalak

Számítógépekről

- [AHU] Aho, A.V., Hopcroft, J.E., Ullman, J.D.: *Számítógép algoritmusok tervezése és analízise*, 1., 10., 11. fejezetek, Műszaki Kiadó, 1982.
- [CLR] Cormen, T.H., Leiserson, C.E., Rivest, R.L.: *Algoritmusok*, 36. fejezet, Műszaki Kiadó, 1997.
- [CsB] Csákány Béla: *Diszkrét matematikai játékok*, Polygon könyvtár, Szeged, 1998.
- [GT] Gaizer Tamás: *Mindenható számítógép?*, Polygon VI.(1996), 23-31.
- [GJ] Garey, Johnson: *The Guide of NP-complete Problems*, 1970.
- [GL] Gács Péter, Lovász László: *Algoritmusok*, 4. fejezet, Tankönyvkiadó, 1987.
- [KG] Kós Géza: *Ismét egy egyszerű sejtautomatáról, avagy kutyák a Marsról*, KöMaL 46 (1996)
- [KD] Knuth, D.: *A számítógép-programozás művészete*, Műszaki Kiadó, 1988

- [LL] **Lovász László:** *Algoritmusok bonyolultsága*, ELTE egyetemi jegyzet, 1994,
<http://www.cs.elte.hu/~kiralay/alg.pdf>
- [LP] **Lewis,R.,Papadimitriou,H.:** *Elements of the Theory of Computation*, Prentice Hall, 1981.
- [NFR] **Nievergelt,J.,Farrar,J.C.,Reingold,E.M.:** *Matematikai problémák megoldásainak számítógépes módszerei*, 6.fejezet, Műszaki Kiadó, 1977.
- [SzI2] **Szalkai István:** *On the Algebraic Structure of Primitive Recursive Functions*, Zeitschrift für Math. Logik und Grundl. der Math. 31 (1985), 551-556,
<http://math.uni-pannon.hu/~szalkai/ZMLG-sk.pdf>
- [SzI3]-----: *Diszkrét matematika és algoritmuselmélet alapjai*, Veszprémi Egyetemi Kiadó, 2001
- [TV] **Totik Vilmos:** *Az élet játék(a)*, Polygon, VI.(1996), 9-21 (lemez melléklettel)
- [TB] **Trahtenbrot,B.A.:** *Algoritmusok és absztrakt automaták*, Műszaki Kiadó, 1978.

Egyéb

- [BF] **Bolyai Farkas:** *Tentamen*, <http://mek.oszk.hu/06500/06507/>
- [EE] **Euklidesz:** *Elemek*, <http://mek.oszk.hu/06200/06232/index.phtml>
- [KE] **Kiss Elemér:** *Kétszáz éve született Bolyai János*, KöMaL 2002.november, 457 - 466.old.,
<http://www.komal.hu/cikkek/bolyai200/bolyai200.h.shtml>
- [KI] **Kovács István:** *Bizonyos függvények határozatlan integráljának kiszámíthatatlanságáról*, Polygon folyóirat II (1992), 51-60.
- [SzI4] Szemléletes analízis - Explanatory Analysis, <http://www.tankonyvtar.hu>,
<http://math.uni-pannon.hu/~szalkai/Anal-Tk1B-c.pdf>
<http://tananyagfejlesztés.mik.uni-pannon.hu/index.php/elkeszult-tananyagok-digitalis-mellekletekkel>
- [WT] **Wesely Tibor:** *Bolyai Farkas*, Tudományos Könyvkiadó, Bukarest, 1974.
- [WWW] <http://www-history.mcs.st-and.ac.uk/BiogIndex.html>
 (Weblap életrajzokkal)