NAGY ÁTTÖRÉSEK A SZÁMELMÉLETBEN
ERDŐS PÁL (1913–1996) EMLÉKÉRE

Komjáth Péter

az MTA levelező tagja, egyetemi tanár,
Eötvös Loránd Tudományegyetem Természettudományi Kar Számítógéptudományi Tanszék
kope@cs.elte.hu

A modern matematika minden ágának sok megoldatlan problémája van, ám a számelmélet bővelkedik egyszerűen megfogalmazható, híres sejtésekben, amelyek évtizedekig vagy akár századokig rendületlenül ellenálltak minden megoldási, megközelítési kísérletnek. Az utóbbi időben azonban, meglepő módon, ezek közül jónéhányat megoldottak, vagy legalábbis döntő áttörést értek el a megoldás felé.

Speciális alakú prímek

Leonhard Euler 1749-ben igazolta *Pierre de Fermat* sejtését: minden $4k+1$ alakú prím előáll x^2+y^2 alakban. Később meghatározta az x^2+2y^2 és az x^2+3y^2 alakú prímeket is. Az algebrai számelmélet klasszikus elmélete lehetővé teszi, bár nem könnyen, hogy meghatározzuk, adott n-re mely prímek írhatók fel x^2+ny^2 alakban. Ezek a módszerek speciálisak az ilyen típusú polinomokra, és a legutóbbi időkig reménytelennek tűnt a magasabb fokú polinomok esete, noha kézenfekvő a sejtés, hogy minden egész együtthatós polinom végtelen sokszor felvesz prímszám értéket, kivéve, ha valami nagyon egyszerű oszthatósági ok ezt megakadályozza. Itt hatalmas áttörés következett be: 1997-ben *Henryk Iwaniec* és *John Friedlander* bebizonyították, hogy végtelen sok x^2+y^4 alakú prím van, majd módszerüket finomítva 2001-ben *Roger Heath-Brown* igazolta végtelen sok x^3+2y^3 alakú prím létezését. (Mivel $x^3+y^3=(x+y)(x^2-xy+y^2)$, nem érdemes x^3+y^3 alakú prímeket keresni.)Ma is reménytelen annak a sejtésnek a bizonyítása, amely szerint végtelen sok x^2+1 alakú prímszám van.

Lefedő kongruenciarendszerek

Erdős Pál egyik észrevétele volt az 1950-es években, hogy a természetes számokat le lehet fedni véges sok különböző differenciájú számtani sorozattal: egy példa erre a rendre a $2x$, $3x+1$, $4x+1$, $6x+3$, $12x+11$ alakú számokat tartalmazó öt számtani sorozat. E lefedések vizsgálatához meglepő alkalmazásaik lehetősége vezette. Erdős, szokásához híven, ötletes és szép kérdéseket vetett fel az ilyen rendszerekkel kapcsolatban. Megkérdezte például, hogy lehet-e ilyen tulajdonságú lefedő rendszer közös elem nélküli számtani sorozatokkal (példánkban rögtön az első és a második számtani sorozatnak van közös eleme). Erre egyszerűen igazolható a „nem” válasz, a bizonyítás azonban a komplex számok tulajdonságait használja.

Egy másik, igen nehéznek bizonyuló kérdés az volt, van-e hasonló példa úgy is, hogy a szereplő differenciák közül a legkisebb (ami fenti példánkban 2) akármilyen nagy. Már

olyan példát sem könnyű megadni, ahol a legkisebb differencia 3. Az idők folyamán sikerült a legkisebb differenciát 40-ig feltornászni. Sok cikk foglalkozott ezzel a problémával, de Erdős állítása hatvan évig megtámadhatatlannak bizonyult. Végül 2013-ban éppen az Erdős 100. születésnapja tiszteletére rendezett konferencián jelentette be *Bob Hough*, hogy a válasz „nem". E váratlan tétel bizonyítása igen bonyolult, kétszer is használja *Lovász László* ún. lokális lemmáját. (Ebbe és a többi témakörbe is jó bevezetést ad Erdős Pál és *Surányi János* könyve [1996].)

A Prímek P-ben van!

Ezzel a blikkfangos címmel hirdették világszerte egy komplexitáselméleti alapprobléma megoldását. A számítógép-tudomány egyik nagy fejezete azt vizsgálja, hogy különböző problémák megoldása milyen gyors algoritmussal (tehát tulajdonképpen programmal) adható meg. Itt egy probléma bármi lehet, ami minden megadott *inputhoz* egy *igen* vagy *nem* választ rendel. Például az input lehet két természetes szám, és azt kérdezzük, relatív prímek-e. Egy másik problémánál az input egy természetes szám, és a megoldandó feladat annak eldöntése, hogy az prímszám-e. Nagyon fontos egyéb problémák az inputként megadott gráfok alaptulajdonságait vizsgálják. Megoldásnak bármilyen konkrét algoritmust elfogadunk, és itt, elméleti tudomány lévén, eltekintünk a valódi számítógépek korlátaitól. A számítások hosszúsága alapján a problémákat osztályokba soroljuk. Így pl. a P osztály azon problémákat tartalmazza, amelyekre az igen/nem válasz mindig megadható úgy, hogy a lépések száma az input hosszának legfeljebb egy polinomja, mondjuk minden n hosszú inputra legfeljebb $100n^2$. A fenti problémák közül a relatív prímségre *Eukleidész* adott egy ilyen gyors algoritmust. A „Prímek" problémára ilyen gyors algoritmus megadása a 2000-es évekig váratott magára, bár a korábbi eredmények alapján igen valószínűnek tűnt, hogy van ilyen algoritmus. Ilyen eredmény pl., hogy mind az *igen,* mind a *nem* válasz megindokolható egy polinom hosszúságú számítással. Valóban, könnyű gyors számítással tanúsítani, hogy egy szám összetett: elég megadni egy valódi osztóját, az osztás már gyorsan elvégezhető. 1975-ben *Vaughan Pratt* adott meg egy ehhez hasonló megindoklási algoritmust a prímszámok esetére, ez sokkal agyafúrtabb.

Végül 2002-ben *Manindra Agrawal, Neeraj Kayal* és *Nitin Saxena*, a Kanpuri Indiai Műszaki Egyetem számítógép-tudománnyal foglalkozó kutatói adtak meg egy polinom hosszúságú algoritmust, amely eldönti egy adott számról, hogy prím-e. Módszerük váratlan ötlete, hogy polinomokat használnak.

Szemerédi tétele

Erdős Pál és *Turán Pál* 1936-ban a következő sejtést fogalmazták meg. Ha $k \geq 3$ természetes szám, akkor minden n természetes számra jelölje $r_k(n)$ az 1 és n közötti természetes számokból álló legnagyobb olyan halmaz elemszámát, amely nem tartalmaz k tagú számtani sorozatot. A sejtés szerint $r_k(n)/n \to 0$, ha n tart végtelenhez, tehát rögzített k esetén minél nagyobb n-re vesszük az első n természetes számot, annál kisebb részét tudjuk kiválasztani úgy, hogy ne keletkezzen k tagú számtani sorozat. Ez minden k-ra ad egy állítást, nagyobb k-ra nehezebbet. Erdősék elsősorban az (itt nem tárgyalandó) van der Waerden-tételhez reméltek használható becslést nyerni a bizonyításból, de minden valószínűség szerint arra az igen régi és sokáig reménytelen sejtésre is gondoltak, amely szerint van akármilyen hosszú, prímszámokból álló

számtani sorozat. Ez azonnal következne, ha sikerülne belátni a $r_k(n)/\pi(n) \to 0$ relációt, ahol $\pi(n)$ jelöli az n-nél kisebb prímek számát.

Először *Klaus F. Roth* igazolta, az analitikus számelmélet módszereivel, a sejtést a (legegyszerűbb) k=3 esetre, 1952-ben. A következő lépés 1969-ben történt, amikor *Szemerédi Endre* (aki függetlenül felfedezte az állítást) igazolta a jóval nehezebb k=4 esetet. Módszere igen finom, de elemi kombinatorikus okoskodás volt. Ezt a módszert számos új ötlettel és mély gondolattal továbbfejlesztve 1973-ban végül eljutott a teljes sejtés bizonyításához, ami ma a Szemerédi-tétel nevet viseli. Még a hetvenes években *Hillél Fürstenberg* átfogalmazta Szemerédi tételét egy tisztán ergodelméleti (tehát analízisbeli) állítássá, amit be is bizonyított. Az az érdekes helyzet állt tehát elő, hogy két különböző bizonyítás is volt az Erdős–Turán-sejtésre, de egyik sem volt alkalmas arra, hogy használható becslést kapjunk $r_k(n)$-re: az egyik csak használhatatlanul gyenge becslést ad, a másik elvileg sem adhat semmilyent.

Szemerédi bizonyításának fontos eleme az úgynevezett *regularitási lemma* volt, ami nagyjából azt fogalmazza meg, hogy a legnagyobb gráfok is előállíthatók néhány konkrét $G_1,\ldots,G_n$ gráfból véletlen gráfok, majd egy bizonyos „zaj" hozzáadásával. A zajt a G_i gráfok számának és méretének növelése árán tetszőlegesen kicsire lehet csökkenteni. Ez a nagy jelentőségű lemma kulcsfontosságúvá vált az igen nagy gráfok, hálózatok tanulmányozásánál. Szemerédi munkatársaival számos, a korábbi módszerekkel nem elérhető tételt igazolt segítségével.

A kilencvenes évek második fele óta élénk kutatások indultak el a Szemerédi-tétellel kapcsolatban, *Tim Gowers* az analitikus számelméleti módszereket átfogalmazta Fourier-analízisbeliekké, majd átdolgozta, kibővítette azokat. Újabb bizonyítások, általánosítások és alkalmazások születtek *Jean Bourgain*, *Ben Green*, *Terence Tao*, *Vojtech Rödl*, *Solymosi József* és *Tamar Ziegler* nyomán. Ma már tíznél több különböző bizonyítás van, és ezek között van olyan is, amelyik úgy fogalmazható, hogy a tételben szereplő halmazt szétvágja egy „szabályos" és egy „véletlen" részre, majd külön-külön igazolja a tételt.

A legváratlanabb eredményt Ben Green és Terry Tao 2004-ben igazolta: van tetszőleges hosszú számtani sorozat prímszámokból. Ez igen régi sejtés volt (lásd a fentebb írottakat Erdős és Turán motivációjáról), de korábban csak három tagú számtani sorozatokra igazolták, és nehézsége alapján nem volt várható, hogy a közeljövőben általánosan is igazolják. A bizonyítás számos, külön-külön is nehéz módszert kombinál. Az olvasó meggondolhatja, hogy a Green–Tao-tételből adódik tetszőleges $k \geq 3$-ra $k \times k$-as, különböző prímekből álló bűvös négyzet létezése.

Ikerprímek

Mivel két egymás utáni természetes szám közül az egyik mindenképpen páros, nem lehet mindkettő prím, leszámítva a (2,3) párt. Ez az okoskodás nem zárja ki, hogy egymás utáni páratlan számok prímek legyenek, és éppen ez az ikerprím-sejtés: van végtelen sok egymás utáni páratlan számokból álló prímszámpár: (3,5),…, (17,19),… Először *Alphonse de Polignac* publikálta 1849-ben ezt a sejtést abban az általánosított formában, hogy minden k-ra van végtelen sok egymás utáni prímből álló $2k$ különbségű számpár.

A prímszámok száma n-ig aszimptotikusan $n/\log n$ (ez a híres prímszámtétel, itt és később log a természetes logaritmust jelenti), így a szomszédosak különbsége átlagosan log

n. Mivel a prímek sorozata nem egyenletes, várható, hogy sokszor lényegesen log *n* alá megy egy *n* nagyságú prím távolsága a rákövetkezőtől. Először Erdős igazolta 1940-ben, hogy létezik olyan $c<1$ szám, amelyre a fenti távolság végtelen sokszor kisebb $c\log n$-nél. Erdős bizonyítása nem adott konkrét értéket c-re. Később *Enrico Bombieri* és *Harold Davenport* a $c=0{,}467$ értéket nyerte, amit lassan szorítottak le, *Helmut Maier* 1985-ös $c=0{,}248$ értékét sokáig nem javították meg. Csak 2005-ben történt további előrehaladás, de az szenzációs volt: *Daniel Goldston*, *Pintz János* és *Cem Yıldırım* igazolták, hogy bármilyen pozitív *c* érték megfelelő. Később igazolták, hogy a különbség végtelen sokszor lecsökken kb. $\sqrt{\log n}$-re. Már ez is váratlan és hatalmas előrelépés volt, de 2013-ban jött a még nagyobb szenzáció: a korábbi eredményeket további ötletekkel kiegészítve az amerikai *Yitang Zhang* igazolta, hogy van olyan *K* szám, amely végtelen sokszor fordul elő szomszédos prímek különbségeként. Ő a $K\leq 70\,000\,000$ becslést kapta, később ezt sikerült 4680-ra leszorítani. A bizonyítás érdekessége, hogy noha tudjuk, hogy van ilyen fenti tulajdonságú *K* szám, semmilyen konkrét számra nem tudjuk megmutatni ezt a tulajdonságot.

Polymath

Az utóbbi években a matematikusok együttműködésének új formái kezdenek kialakulni.

Sokan, főleg a fiatalabbak, felrakják cikkeiket honlapjaikra. Ez a törekvés a másik végen is érzékelhető, egyre több folyóirat teszi mindenki számára hozzáférhetővé korábbi tartalmait, többnyire egy néhány éves „mozgó fal" közbeiktatásával. Szaporodnak a nyíltan hozzáférhető elektronikus folyóiratok. Sok kutató valamennyi cikkét elhelyezi az *arXiv* internetes cikkgyűjteményben.

A számos matematikai blog közül csak Timothy Gowersét és Terence Taóét emelem ki. Gowers blogja szorosan vett matematikai tárgyú közlemények mellett érdekes esszéket is közöl például a blogger vitájáról az Elsevier tudományos könyvkiadóval. Tao pedig elképesztő terjedelemben vázolja a legkülönbözőbb (általa vagy mások által kitalált) bizonyításokat, ezeket időről időre kötetben adja közre, eddig 6 ilyen kötet jelent meg. Gowers javaslatára jött létre a *Polymath* kezdeményezés, ami az intenzív internetes együttműködés egy formája. Polymath projekt jöhet létre egy konkrét feladat megoldására. A tagok ahelyett, hogy egy teremben a tábla előtt beszélnének, a számítógépükön keresztül kommunikálnak. Az internet különböző helyein levő releváns információkat a résztvevők által szerkesztett honlap fogja össze. Végül a cikk megírása is közösen történik. Ha a cikk megjelenik, szerzőjeként *Polymath*-ot adják meg (a valódi szerzőket és grantjaik adatait feltüntetve). Egy ilyen Polymath projekt adta az eddigi legegyszerűbb bizonyítást Szemerédi Endre tételére (ez a Szemerédi tiszteletére rendezett konferencia kötetében jelent meg), egy másik projekt pedig Zhang tételére a fent említett $K\leq 4680$ becslést számolta ki. Ez utóbbi projekt mintegy tizenöt résztvevője között van a magyar *Harcos Gergely* és Pintz János is.

Támogatás: OTKA K 81121

Kulcsszavak: *matematika, számelmélet, prímszámok, híres problémák*

IRODALOM

Erdős Pál – Surányi János (1996): *Válogatott fejezetek a számelméletből.* Második, bővített kiadás. Polygon, Szeged • ArXiv: http://arxiv.org/ • Gowers weblogja: http://gowers.wordpress.com/ • Tao blogja: http://terrytao.wordpress.com/