Freud Róbert
Ősi problémák - új eredmények
(Számelmélet, prímszámok)

című 2005. november 22-i előadása alapján írta
Balogh Máté, Nagy Dániel és Hraskó András

1. Tökéletes számok és Mersenne-prímek

A prímszámokkal kapcsolatban rengeteg megoldatlan probléma van ősidők óta. Kezdjük az egyik legrégebbivel! Ezzel már Euklidész is foglalkozott, tehát kb. az i. e. III. századból való. Euklidészt általában geométerként tartják számon, de ez nem fedi teljesen a valóságot: 13 könyvet írt és ebből 4 könyv – a VII-től a X-ig – a számelmélettel foglalkozott. Néha persze a számelméleti problémákat is geometriai köntösbe öltöztette. Tőle származik pl. annak bizonyítása – vagy legalábbis ő is leírta -, hogy végtelen sok prímszám van.

1. Tétel (Euklidész IX/36. tétele) *Ha az egységtől kezdve kétszeres arányban képzünk mértani sorozatot, amíg a sorösszeg prím nem lesz, és az összeggel megszorozzuk az utolsó tagot, tökéletes számot kapunk.*

Tökéletes szám *nak nevezzük az olyan számokat, amelyek önmagukon kívüli pozitív osztóinak összege egyenlő magával a számmal.*

Lássunk erre két példát:

1+2=3 prím, így 3·2=6 tökéletes szám. Valóban, 6 nála kisebb pozitív osztói: 1, 2 és 3, ezek összege 1+2+3=6.

1+2+4=7 prím, így 7·4=28 tökéletes szám. Valóban, 28 nála kisebb pozitív osztói: 1, 2, 4, 7 és 14, ezek összege 1+2+4+7+14=28.

Euklidész IX/36. tételének bizonyítása

Legyen tehát k olyan pozitív egész szám, amelyre a k darab tagból álló

$$(*)1 + 2 + 2^2 + ... + 2^{k-1} = 2^k - 1 = p$$

összeg értéke prímszám. Az $n = p \cdot 2^{k-1}$ számról kell megmutatni, hogy tökéletes. A fenti n szám n-nél kisebb pozitív osztói:

$$1, 2, 2^2, \ldots, 2^{k-2}, 2^{k-1},$$

továbbá

$$p, 2p, 2^2p, \ldots, 2^{k-2}p,$$

ezek összegének egyik része

$$1 + 2 + 2^2 + \ldots + 2^{k-1} = 2^k - 1 = p$$

másik része pedig

$$1 \cdot p + 2 \cdot p + 2^2 \cdot p + \ldots + 2^{k-2} \quad \cdot p = (2^{k-1} - 1) \cdot p$$

így az osztók összege mindösszesen

$$p + (2^{k-1} - 1) \cdot p = 2^{k-1} \quad \cdot p = n,$$

azaz n tényleg tökéletes.

Mikor lehet prím a (*) sorösszeg? Ezzel kapcsolatban először egy negatív eredményt fogalmazunk meg.

1. Észrevétel *Ha a k pozitív egész szám nem prím, akkor az 1 + 2 + ... + 2^{k-1} = 2^k -1 összeg értéke sem prím.*

Az 1. Észrevétel bizonyítása

Ha $k = u \cdot \quad v$, akkor az első u kettőhatvány összegét – azaz $(1 + 2 + ... + 2^{u-1})$-t – kiemelhetjük.

Ha például $k = 15$, akkor $k = 3 \cdot 5$, így az

$$(**)1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + \ldots + 2^{14}$$

összegből kiemelhető $1 + 2 + 2^2$. Valóban:

$$1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + \ldots + 2^{12} + 2^{13} + 2^{14} =$$
$$= (1 + 2 + 2^2) + 2^3(1 + 2 + 2^2) + \ldots + 2^{12}(1 + 2 + 2^2) =$$
$$= (1 + 2^3 + 2^6 + 2^9 + 2^{12}) \cdot (1 + 2 + 2^2).$$

Természetesen hasonló módon igazolható, hogy a (**) összegből $(1+2+2^2+2^3+2^4)$ is kiemelhető, de erre már nincs feltétlenül szükség, a korábbi szorzatalakkal beláttuk, hogy (**) nem prím.

Azt gondolhatnánk, hogy ha k prím, akkor a (*) sorösszeg értéke is prím. Sajnos ez nincs így.

2. Észrevétel *A (*) sorösszeg értéke k=11 esetén nem prím: 1 + 2 + ... + 2^{10} = 2^{11} -1= 2047 = 23·89.*

Máig megoldatlan, hogy mely k prímszámok esetén lesz $2^k - 1$ értéke is prím. A probléma egyik első kutatója a francia matematikus, tudományszervező Mersenne volt, Fermat és Descartes kortársa, ezért viseli az ő nevét az alábbi fogalom.

A 2^k-1 alakú prímeket – ahol tehát k is prímszám – Mersenne-prímeknek nevezzük. Jelben: M_k = 2^k-1.

A jegyzet készítésének idején (azaz 2006 januárjában) 43 Mersenne-prímet ismerünk[1].

1644-ben Mersenne két lényeges és egymással meglehetősen ellentmondó megállapítást jegyzett fel.

Mersenne 1. megállapítása *Ahhoz, hogy egy 15 vagy 20 jegyű számról eldöntsük, prím-e vagy sem, egy élet sem elég, bárhogy is használjuk minden tudásunkat.*

Mersenne 1. megállapításának „korabeli" indoklása

[1] Lásd pl. http://primes.utm.edu/mersenne/

Ahhoz, hogy eldöntsük egy számról, hogy prím-e, el kell osztanunk a számot minden egyes pozitív egésszel, egészen a gyökéig. Ha pl. egy 17 jegyű, azaz 10^{16}-nál nagyobb számról van szó, akkor ez a gyök legalább 10^8. Ha a 2-n kívül kihagyjuk a páros számokkal való osztást, akkor csak $5{\cdot}10^7$, ha a 3-n kívül a hárommal osztható számokkal sem osztunk többet, akkor csak kb. $3{,}33{\cdot}10^7$ osztás marad. Kerekítsünk 10^7 osztásra! Ha egy osztás pl. 6 percig tart, akkor egy óra alatt 10-et végezhetünk el, egy munkanap alatt kb 100-at, egy év alatt kb. 400-at. Így 25 000 évre is szüksége lehet egy embernek a számolás elvégzéséhez.

Ennek ellenére sikerült készítenie egy elég pontos listát a legkisebb ilyen alakú prímekről.

Mersenne 2. megállapítása *2^k – 1 prím, ha k = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 vagy 257 és minden további k <257-re összetett.*

Mersenne listájához kb. 250 éven keresztül senki sem tudott hozzászólni. 1876-ban kiderült, hogy a lista nem tökéletes, bebizonyították, hogy k=67 esetén a kapott szám összetett. A listáról ráadásul hiányzik k= 61, 89 és 107. 1922-ben pedig k=257-ről is kiderült, hogy nem prím. A számolási nehézséget figyelembe véve ez nem túl sok hiba.

De hogyan lehet rájönni arra, hogy 2^{67}-1 nem prím? Ehhez az alábbi teszt segít.

2. Tétel (Lucas tétele, 1876) *Egy $k>2$ prím esetén$M_k = 2^k - 1$ akkor és csak akkor prím, ha*

$$M_k | a_{k-1},$$

ahol $a_1 = 4$ és $a_{i+1} = a_i^2 - 2$.

Vizsgáljuk meg pl. a teszt működését $k = 5$ esetén, tehát ,,teszteljük le", hogy $M_5 = 2^5 - 1 = 31$ prím! Ehhez a_{5-1}, azaz a_4 kiszámítására van szükség.

$$a_1 = 4, \quad a_2 = 4^2 - 2 = 14, \quad a_3 = 14^2 - 2 = 194$$

és

$$a_4 = 194^2 - 2 = (6 \cdot 31 + 8^2 - 2 = s \cdot 31 + 8^2 - 2 = s \cdot 31 + 62,$$

ahol s egész szám, tehát $M_5 \,|a_4$, így $M_5 = 31$ prím.

Látható, hogy a fenti eljárás segítségével nagyobb k, pl. k=67 esetén is emberi időn belül eldönthető, hogy M_k prím-e. Gyorsít az is, hogy nem kell a_1, a_2, ..., a_{k-1} pontos értéke, elég tudni az M_k-s maradékaikat.

Ajánló

Az eljárás helyességének – tehát Lucas tételének – igazolása részben megtalálható Freud Róbert Kömalban megjelent cikkében (Kömal, 2004/2, Százezer dolláros prímek).

Ez a cikk az interneten is elérhető: http://www.komal.hu/cikkek/2004-02/freud.h.shtml.

Lásd még http://primes.utm.edu/notes/proofs/LucasLehmer.html,

http://www.jt-actuary.com/lucas-le.htm, http://www.mathpages.com/home/kmath473.htm.

A Lucas-teszt nem konstruktív, tehát nem állítja elő a 2^k – 1 alakú szám felbontását, ha az nem prím. 1903-ban egy matematikai kongresszuson F. N. Cole amerikai matematikus[2] előadást

[2]lásd http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Cole.html

hirdetett meg ,,Nagy számok felbontása" címmel. Az előadás első felében a táblán akkurátusan kiszámolta $2^{67} - 1$ pontos értékét és kétszer aláhúzta a végeredményt:

$$\underline{\underline{147573952589676412927}}.$$

Az előadás második felében egy másik táblán a $193707721 \cdot 761838257287$ szorzat értékét határozta meg a szokásos akkurátussággal, az eredmény itt (is)

$$\underline{\underline{147573952589676412927}}.$$

Cole előadása ezzel be is fejeződött, pont akkor, amikor a hallgatóság rájött, hogy miről szól. A felbontás megtalálása mindazonáltal még most is nagyon nehéz probléma.

Jelenleg (2005. decemberében) a legnagyobb ismert Mersenne-prím a maga 9 152 052 jegyével a

$$2^{30402457} - 1.$$

Az interneten Gimps néven (http://www.mersenne.org/prime.htm, Great Internet Mersenne Prime Search) kb. 200 000 fős ,,csapat" keres minél nagyobb Mersenne-prímet. A fő inspirációt az Electronic Frontier Foundation (EFF) százezer dolláros felajánlása adja, amit annak fizetnek ki, aki először állít elő legalább tízmillió jegyű prímszámot. A kereső csapatba bárki jelentkezhet, gépén a project programja a komputer ,,szabadidejében" fut.

2. A ,,prímség" eldöntése

Gauss (1777-1855), a matematikusok fejedelme így fogalmazott: ,,a tudomány méltósága megkövetelni látszik, hogy egy olyan alapvető kérdést miszerint egy számról eldöntsük, hogy prím-e, és ha nem, akkor megtaláljuk prímtényezőit, megfelelően kezelni tudjunk".

Az előző fejezetben láttuk, hogy a speciális alakú M_k számokról hogyan dönthető el hatékonyan, hogy prím-e. Miképp lehet általában eldönteni gyorsan egy számról, hogy prím-e? Erre ma már tudunk hatékony algoritmust, tudunk tesztelni egy adott számot, hogy prím-e, azaz Gauss alapvető problémája felerészt megoldottnak tekinthető. A probléma másik felére, a prímtényezők gyors előállítására máig nincs kielégítő módszer.

Ez a kontraszt azért is érdekes, mert a teszt segítségével könnyen találhatunk prímszámokat, két nagy prímszámot gyorsan össze tudunk szorozni, de kellően nagy prímeknél a szorzatot még senki sem képest felbontani tényezőire, annak ellenére, hogy képes felismerni azt, hogy a szám összetett. Azon kívül, hogy ez egy jó játék, ezen alapulnak a nyilvános kulcsú titkosírások közül a leghatékonyabbak. Ezek úgy működnek, hogy nyilvánosságra hozhatjuk, milyen eljárással kódolunk, mégsem fogja senki sem tudni dekódolni a nekünk szánt üzeneteket, mert a dekódoló pontosan olyan problémába ütközik, hogy két nagy prím szorzatát kellene prímtényezőire bontania. Így működnek az elektronikus aláírások, a bankkártya-biztonsági eljárások, diplomáciai és katonai titkosító rendszerek is.

Ajánló

A titkosírásról bővebben lásd

Csirmaz László: Kriptográfia a középiskolában, http://www.math-inst.hu/~csirmaz/kript/mattan.html

Catherine A. Gorini: Üzenetek titkosítása az óra-aritmetika alkalmazásával, http://matek.fazekas.hu/portal/kutatomunkak/codes/codesm.html

Simon Singh: Kódkönyv (A rejtjelezés és rejtjelfejtés története), Park Könyvkiadó http://www.parkkiado.hu/konyv.php?id=42&katid=K&alkatid=8

Persze nem állíthatjuk teljes biztonsággal, hogy senki sem tud nagy számokat prímtényezőire bontani. Lehet, hogy valaki képes erre, és, mondjuk, minden bankszámláról levesz 1-1 centet, és így többszörös milliárdos lesz, de ez meglehetősen valószínűtlennek tűnik.

Kicsit kitérünk a ,,Millenniumi problémák"-ra. 2000-ben hét darab egyenként 1 millió dolláros problémát nyitottak, úgyhogy bármelyik megoldásért jár az 1 millió dollár, megfelelő feltételek mellett. Ennek az az előzménye, hogy száz évvel korábban, 1900-ban Hilbert a II. Nemzetközi Matematikai Kongresszuson 23 matematikai problémacsokrot vázolt fel és ezzel nagyjából kijelölte a XX század matematikájának legfontosabb irányait. A Millenniumi problémák között kettő olyan van, amely kapcsolódik az eddig elmondottakhoz. Az egyik a Riemann sejtés, amelynek már megértése is komoly előismereteket követel, megoldása pedig jelentősen bővítené a prímszámokra vonatkozó ismereteinket is. A másik az algoritmusok bonyolultságával kapcsolatos ,,P=NP?" probléma. Lényege: igaz-e, hogy ha valamit gyorsan le tudunk ellenőrizni, hogy úgy van, akkor gyorsan ki is tudjuk találni. Pl. ha adott két szám, akkor gyorsan le lehet ellenőrizni, hogy prímek-e, össze is lehet őket szorozni, tehát ha kiderülne, hogy P=NP, akkor adódna, hogy van gyors algoritmus a szorzat tényezőkre bontására.

Ajánló

A Clay Intézet oldalai (Millenniumi problémák): http://www.claymath.org/millennium/

Katona Gyula: Egyszerű és bonyolult, Magyar Tudomány, 2003/3, http://www.matud.iif.hu/03mar/katona.html

Wikipédia a Riemann sejtésről:
http://hu.wikipedia.org/wiki/Riemann-sejt%C3%A9s

Térjünk most rá a gyors prímtesztekre! Kb. 30 éve vannak jó prímtesztek és három éve pedig csináltak egy bombabiztos prímtesztet is. Az eddigiekben ugyanis mindig volt egy kis bizonytalanság. A ,,bizonytalan" prímtesztek és ez a biztos is részben az alábbi tételen alapul.

3. Tétel (kis Fermat-tétel) *Ha p prím és c tetszőleges egész szám, akkor $p|c^p - c$.*

Bizonyítás (Teljes indukció c-re) $c = 1$-re az állítás nyilvánvalóan igaz: $1^p = 1$, így $1^p - 1 = 0$ és $p|0$.

Tegyük most fel, hogy az állítás igaz $c = k$-ra és igazoljuk $c=(k+1)$-re. Használjuk fel a binomiális tételt!

$$(*) \quad (k+1)^p = k^p + pk^{p-1} + \frac{p(p-1)}{2}k^{p-2} + ... + \binom{p}{l}k^{p-l} + ... + pk + 1,$$

ahol

$$(**) \quad \binom{p}{l} = \frac{p \cdot (p-1) \cdot ... (p-l+1)}{l \cdot (l-1) \cdot ... \cdot 1}.$$

Vegyük észre, hogy (*) jobb oldalán majdnem minden tag osztható p-vel! Valóban pk^{p-1} nyilván osztható p-vel; $p(p-1)/2$ is osztható p-vel, hiszen ez a tag csak $p > 2$ esetén szerepel, ilyenkor pedig a p prímtényező páratlan, a $(p-1)$ tényezőt leoszthatjuk 2-vel és így megmarad a p. Vegyünk még egy konkrét példát: ha $p=11$ és a binomiális együttható, mondjuk $\binom{11}{3} = \frac{11 \cdot 10 \cdot 9}{3 \cdot 2 \cdot 1}$,akkor sem esik ki a 11-es prímtényező a tört egyszerűsítésekor. Általában: $p \left| \binom{p}{l} \right.$, ha $0 < l < p$, hiszen (**)-ban a számlálóban szerepel a p prím, a nevezőben pedig csupa p-nél kisebb tényező van, így az nem egyszerűsödik ki.

Ennek alapján (*) így is írható:

$$(k+1)^p = k^p + ps + 1,$$

ahol s is egész szám. Az alábbi kifejezésről kellene igazolnunk, hogy p-vel osztható:

$$(k+1)^p - (k+1) = (k^p - k) + ps.$$

Itt a jobb oldalon látható összeg második tagja nyilván osztható p-vel, az első tag pedig az indukciós feltevés miatt osztható vele. Ezzel az indukciós gondolatmenetet be is fejeztük. Ha minden egész c-re akarjuk igazolni az állítást, akkor egy lefelé menő indukciót is alkalmaznunk kell, az hasonlóan megy.

Ajánló

A kis Fermat-tétel két másik bizonyítása elérhető az alábbi oldalon:
http://matek.fazekas.hu/eloadas/2005/kisfermat.html.

Most rátérünk az első, ,,bizonytalan"-nak mondott prímtesztre. Tekintsünk egy nagy n számot, erről szeretnénk eldönteni, hogy prím-e. Ha n páros, akkor könnyű dolgunk van: $n=2$ esetén

prímszámról van szó, egyébként nem. Ha $n \neq 2$, akkor megnézzük, hogy n vajon osztója-e 2^n-2-nek. Kétféle választ kaphatunk.

Ha nem teljesül az oszthatóság, akkor n biztosan nem prím, ez következik a kis Fermat-tételből. Valóban, ha n prím, akkor a tétel c=2-re épp azt mondja ki, hogy $n|2^n$-2. Ebben az esetben tehát rájöttünk, hogy hogy n összetett, de vegyük észre, hogy $n$prímtényezőire vonatkozóan nem adott felvilágosítást az eljárás.

Ha teljesül az oszthatóság, akkor nincs kizáró ok arra, hogy n prím legyen. Mi következik ebből? Több mint 1000 évvel ezelőtt a kínaiak azt gondolták, hogy ilyenkor n biztosan prím. Ez sajnos nem igaz, de annyit mondhatunk: „n valószínűleg prím".

A legkisebb ellenpélda a $341 = 11 \cdot 31$ összetett szám, amelyre tehát $341|2^{341}$-2 (ezt úgy könnyű ellenőrizni, hogy megmutatjuk, hogy 2^{341}-2 osztható 11-gyel és 31-gyel is). A 341 tehát álprím, pontosabban *2-es alapú álprím*[3], mert a 2-es kis Fermat teszten úgy viselkedik, mintha prím lenne. Hogyan lehet vajon lebuktatni a 341-et? Hogyan lehet rájönni, hogy nem összetett? Van-e vajon tanú, olyan c szám, amelyre már $c^{341} - c$ nem osztható 341-gyel? A 2 nem volt hajlandó tanúskodni, kipróbálhatjuk a 3-at. A 3 tényleg leleplezi a 341-et: 3^{341}- 3 nem osztható 341-gyel. Sajnos azonban vannak olyan összetett számok – ezeket *univerzális álprím*eknek vagy Carmichael számoknak nevezik –, amelyeket nem lehet így leleplezni, minden c-re tudják a kis Fermat-tételt. Ilyen szám pl. az 1729, amelyre tehát $1729|c^{1729} - c$ minden c egész szám esetén teljesül.

Milyen alapon mondhatjuk mégis azt, hogy ha valamely n-re $n|2^n$-2, akkor n valószínűleg prím? Hiszen itt van a 341, itt van az 1729 és még más 2-es alapú vagy univerzális álprímek? Ezt úgy kell érteni, hogy viszonylag kevés ilyen szám van, amely összetett és mégis imitálja a prímséget, azzal, hogy teljesíti a kis Fermat-tételt. A kevés nem azt jelenti, hogy véges sok. Tíz éve bizonyították be, hogy az univerzális álprímekből is végtelen sok van. A kevés azt jelenti, hogy ezek nagyon ritkán fordulnak elő a prímekhez képest: ha elmegyünk egy nagy határig, akkor addig sokkal kisebb a 2-es alapú álprímek száma, pláne az univerzális álprímek száma, mint a prímeké. Íme egy statisztika (a 3., 4. és 5. oszlop adatait a

http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi?Anum=A055550,

http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi?Anum=A114246

http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi?Anum=A055553

oldalakról vettük):

[3] A 2-es alapú álprímeket Poulet vagy Sarrus számoknak is nevezik.

	prímek száma	2-es alapú álprímek száma	2-re és 3-ra is álprím számok száma	univ. álprímek (Carmichael számok) száma
10-ig	4	0	0	0
100-ig	25	0	0	0
1000-ig	168	3	0	1
10 000-ig	1 229	22	7	7
100 000-ig	9 592	78	23	16
1 000 000-ig	78 498	245	66	43
10^7-ig	664 579	750	187	105
10^8-ig	5 761 455	2 057	485	255
10^9-ig	50 847 534	5 597	?	646
10^{10}-ig	455 052 511	14 884	?	1547
10^{11}-ig	4 118 054 813	38 975	?	3605
10^{12}-ig	37 607 912 018	101 629	?	8241
10^{13}-ig	346 065 536 839	264 239	?	19279

Ellentmondásnak tűnik, hogy létezik háromjegyű univerzális álprím, de 2-es és egyben 3-as alapú álprím nincs. Ennek az az oka, hogy az 561, az egyetlen háromjegyű univ. álprím, osztható 3-mal.

Ha például egy százmilliónál (10^8) kisebb pozitív egész szám prímségét teszteljük és a 2-es alapú kis Fermat teszt prímnek mutatja, akkor csak $\frac{2057}{5761455+2057} \approx 0,000357$ a valószínűsége, hogy nem prím, ha még a 3-as teszten is megfelel, akkor már csak $\frac{485}{5761455+485} \approx 0,000084$ az esélye, hogy összetett szám, tehát 99,9916 % az esélye, hogy prím.

Ha véletlen módszerrel választunk egy legfeljebb 13 jegyű pozitív egészt, akkor 3,46 % az esélye, hogy prím lesz – ez egyáltalán nem elhanyagolható –, és ha megfelel a 2-es alapú teszten, akkor

$$\frac{346\ 065\ 536\ 839}{346\ 065\ 536\ 839 + 264\ 239} \approx 0,999999236,$$

azaz kb. 99,9999236% a valószínűsége, hogy tényleg prím. Ez azt mutatja, hogy a véletlen segítségével gyorsan találhatunk olyan nagy számot, ami igen nagy valószínűséggel prím. Később látni fogjuk, hogy a módszer még erősíthető is, a biztonság tetszőlegesen növelhető.

Ajánló

Univerzális álprímek (Carmichael számok) a Számsorozatok Sloane-féle Enciklopédiájában:

http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi?Anum=A002997

A 2-es alapú álprímek ugyanott:

http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi?Anum=A001567

Nagy László Tibor és Stan Johann Bolyai Jánosról készített weboldalain az álprímek is előkerülnek:
http://bolyai.port5.com/kisfermat.htm

Mathworld az álprímekről: http://mathworld.wolfram.com/FermatPseudoprime.html

Térjünk vissza az 1729-re, hogy megmutassuk, ez a szám valóban univerzális álprím! Tényleg összetett számról van szó, nevezetesen 1729=7·13·19. Azt akarjuk igazolni, hogy $1729|c^{1729} - c$ bármely c egész szám esetén. Ehhez elég külön-külön bizonyítani, hogy $7|c^{1729} - c$, $13|c^{1729} - c$ és $19|c^{1729} - c$, hiszen ha egy szám osztható 7-tel, 13-mal és 19-cel, akkor a szorzatukkal is osztható. Alább csak a 13-mal való oszthatóságot igazoljuk, a többi ugyanúgy megy.

Vegyük észre, hogy $c^{1729} - c = c \cdot (c^{1728} - 1)$, így ha c osztható 13-mal, akkor készen is vagyunk, ha pedig c nem osztható 13-mal, akkor azt kell megmutatnunk, hogy $13|(c^{1728} - 1)$. A 13 prímszám, így teljesül rá a kis Fermat-tétel, azaz bármely k egész számra $13|c^{13} - c = c \cdot (c^{12}\text{- } 1)$, és ha c nem osztható 13-mal, akkor az előbbi oszthatóság csak úgy teljesülhet, ha $13|(c^{12}\text{- } 1)$. Most már csak a 12-es kitevőt kellene 1728-re változtatni. Az a ,,szerencsénk", hogy 1728 osztható 12-vel: $(c^{12})^{144} = c^{1728}$. Nevezetes, hogy $(a^k\text{-}1)$ bármely a egész szám és pozitív egész k kitevő esetén osztható $(a\text{-}1)$-gyel, ehhez ugyanis az algebra segít: $a^k\text{-}1 = (a\text{-}1)\cdot(a^{k-1} + a^{k-2}+...+1)$.

Ha ezt $a = c^{12}$-re alkalmazzuk, akkor láthatjuk, hogy $(c^{12}\text{- } 1)|\ (c^{1728}\text{- } 1)$, tehát $13|(c^{12}\text{- } 1)$ miatt kész a bizonyítás.

A lényeg: az 1729 prímtényezőinél eggyel kisebb számok mind osztják az 1729-nél eggyel kisebb számot: 6|1728, 12|1728, 18|1728. A fenti gondolatmenet szerint az 1729 ezért univerzális álprím.

Nevezetes az a történet, amely szerint a XIX század végén született indiai matematikus zseni, Ramanujan 1729 egy másik érdekes tulajdonságára hívta fel a figyelmet. Ez a furcsa természetű, szótlan ember még a középiskoláit sem tudta elvégezni, matematikából is megbukott. 14 éves korában kezébe került egy képletgyűjtemény, amely annyira megragadta, hogy szinte a formulák szerelmese lett, s maga is százasával kezdte gyártani a különleges képleteket. Barátai rávették, hogy mutassa meg egy matematikusnak az eredményeit, így végül 1912-ben elküldte azokat a világ akkori vezető ,,számelmélészének", Hardynak, pár soros levél kíséretében, amelyben azt kérte, hogy ha Hardy talál benne érdekeset, akkor jelezze. Hardy megnézte, először azt gondolta, hogy megint egy félbolonddal van dolga, úgyhogy előbb elment a teniszpartijára. Azután jobban megnézte a képleteket, néhány nagyon újszerűnek tűnt, megpróbálta őket bebizonyítani, nem sikerült. Levelezés kezdődött köztük és Hardy Angliába hívta Ramanujant. Itt történt az az eset, hogy együtt utaztak taxival és Hardy az autóban felejtette az esernyőjét. Bosszankodott, hogy ezt már biztos nem fogják megtalálni, amikor Ramanujan közölte vele a taxi rendszámát: 1729. ,,Hogyan lehet egy ilyen közönséges számot megjegyezni" csodálkozott Hardy. Mire Ramanujan felháborodott: ,,Dehogy közönséges! Ez a legkisebb olyan egész, amely kétféleképpen is előáll, mint két pozitív köbszám összege." Az egyik előállítással fent már találkoztunk: $1729=1+12\cdot144$, azaz $1729=12^3+1^3$. A másik előállítás megkeresését az Olvasóra bízzuk. Ebből a kis történetből is látszik, hogy Ramanujan fejében másként éltek a számok, mint a kiművelt főkben. Sajnos azonban ő nem igazán tudott beszámolni gondolatmeneteiről, amelyekben rengeteg ugrás volt, heurisztikusan látta, hogy miről van szó. Rövid élete során Hardyval együttműködve sok maradandót alkotott, és tételei, képletei közül sokat máig sem tudtak igazolni.

Térjünk vissza az 1729-re, mint álprímre! Hogyan lehet mégis lebuktatni, a prímtényezők előállítása nélkül? Bontsuk tovább a $c^{1729} - c = c \cdot (c^{1728}\text{- } 1)$ szorzatot az $a^2 - b^2 = (a - b) \cdot (a + b)$ azonosság alkalmazásával!

$c^{1729} - c = c \cdot (c^{1728}\text{- } 1) = c \cdot (c^{864}\text{- } 1)\cdot(c^{864}\text{+ } 1)$. Ha 1729 prím lenne, akkor abból, hogy osztja a szorzatot, következne, hogy legalább az egyik tényezőt is osztja: vagy a c-t, vagy a $(c^{864}\text{- } 1)$-t, vagy a $(c^{864}\text{+ } 1)$-t. Nem prímnél ez nincs így. Lássuk illusztrációképp a $15|4^2\text{-}1$ nyilvánvaló összefüggést! Ha most alkalmazzuk a szorzattá alakítást, látjuk, hogy $15|(4\text{-}1)\cdot(4+1)$, de a $15|(4\text{-}1)$ és $15|(4+1)$ relációk egyike sem teljesül. A 15 helyett prímszámmal ez nem volna lehetséges. Tovább erősíthetjük az eljárást, ha a szorzattá bontásban is tovább megyünk!

$c^{1729} - c = c \cdot (c^{864}\text{- } 1)(c^{864}\text{+ } 1)=c \cdot (c^{432}\text{- } 1)\ (c^{432}\text{+ } 1)\ (c^{864}\text{+ } 1)=c \cdot (c^{216}\text{- } 1)\ (c^{216}\text{+ } 1)\ (c^{432}\text{+ } 1)\ (c^{864}\text{+ } 1) = ...$

$= c \cdot (c^{27}\text{- } 1)\ (c^{27}\text{+ } 1)\ (c^{54}\text{+ } 1)\ (c^{108}\text{+ } 1)\ (c^{216}\text{+ } 1)\ (c^{432}\text{+ } 1)\ (c^{864}\text{+ } 1)$.

Ha 1729 prím lenne, akkor bármely c szám esetén az utolsó nyolctényezős szorzatnak legalább az egyik tényezője osztható lenne 1729-cel. Hasonló módon 1729 helyett bármely más páratlan szám esetén is erősíthetjük a módszert, $c^n - c$ helyett tekinthetjük a

$$c \cdot \left(c^{\frac{n-1}{2}} - 1\right) \cdot \left(c^{\frac{n-1}{2}} + 1\right)$$

szorzat vagy annak egy tovább-bontásának tényezőit. A kutatási eredményekből az derült ki, hogy bármely álprím ezen az erősebb teszten a c-k legalább felénél elbukik, így egymás után több véletlenszerűen választott c kipróbálásával a teszt hatékonysága tetszőleges mértékben erősíthető. Ha például egymás után száz véletlenszerűen választott c-vel is kipróbáljuk a tesztet, és mindig prímnek adódik a szám, akkor legfeljebb $(1/2)^{100}$ az esélye, hogy nem prím. Ezzel a módszerrel tehát elvi tévedés lehetősége ugyan van, gyakorlatié azonban nincs.

A matematikusokat persze az elvi dolgok is izgatják. 2002-ben végre Agrawal, Kayak és Saxena találtak egy százszázalékos prímtesztet (AKS teszt). A teszt maga nem sokkal nehezebb, a bizonyítás bonyolultabb, de egy másod-, vagy harmadéves egyetemista számára már érthető, és nem is hosszú. A három szerző egyike maga is még doktorandusz hallgató volt cikkük írásakor.

Ebben a tesztben is egy olyan összefüggést vizsgáltak, amely prímszámra biztos teljesül és amit sikerült megfordítaniuk, megmutatni, hogy nem prímszámra már csak jól kontrollálható esetekben nem teljesül. A teszt alapötlete az, hogy számok helyett polinomokkal dolgozunk. Ha az $n$számról szeretnénk tudni, hogy prím-e, akkor vizsgáljuk az $f = x^n - a$, $g = (x-a)^n$ polinomokat! Ha n (páratlan) prím, akkor a binomiális tétel és a binomiális együtthatókra vonatkozó korábbi megállapításunk szerint (lásd a kis Fermat-tétel bizonyítását) a $g$polinom $(x^n - a^n)$-tól csak n-nel osztható tagokban tér el.

Konkrét x, a értékekre kiszámolni a polinomok értékét, majd összehasonlítani n-es maradékaikat továbbra sem lenne biztos módszer. Biztonságos, de nagyon időigényes eljárás lenne kiszámolni a polinomokat és együtthatónként (mod n) összevetni egyenlőségüket. Köztes, gyors és ugyanakkor biztonságos módszer a két polinomnak bizonyos polinomokkal vett maradékait összehasonlítani. Ha ugyanis egyenlők a polinomok, akkor bármilyen polinommal vett osztási maradékaik is egyenlők. Alkalmas (x^r-1) alakú polinomot választani, mert ezzel nagyon könnyű osztani: ilyenkor úgy kell számolni, mintha (x^r-1) nulla lenne, azaz x^r helyébe mindenhol 1-et kell helyettesíteni. Kiderült, hogy megfelelő olyan $r$prímet venni, amelynek értéke nagyságrendileg $(\log n)^6$, és amelyre r-1-nek van egy alkalmas tulajdonságú nagy prímosztója. Ilyen esetben az a szerencse, hogy összetett n szám esetén a kapott maradék-polinomok rendkívül kevés a-ra lesznek egyenlők: ha 10^{100} körül van az n, akkor csak néhány száz kivétel lehet. Elég a maradékban a helyébe behelyettesíteni az első néhány száz értéket, és ellenőrizni az f-ből ill. g-ből származó értékek n-es maradékai megegyeznek. Ha mindegyik próbában egyezés van, akkor kizárt, hogy n összetett, ha egyszer is nincs egyezés, akkor n biztosan összetett.

Ajánló

AKS teszt a Mathworldön: http://mathworld.wolfram.com/AKSPrimalityTest.html

AKS teszt a Wikipédán: http://www.answers.com/topic/aks-primality-test

Andrew Granville: It is easy to determine whether a given integer is prime, Bull. Amer. Math. Soc. **42** (2005), 3-38. http://www.ams.org/bull/2005-42-01/S0273-0979-04-01037-7/home.html

Végül emlékeztetünk rá, hogy nagy összetett szám prímtényezőinek megtalálására nem ismerünk hatékony algoritmust. Ugyanakkor arra sincs bizonyíték, hogy ilyen algoritmus nem létezik.

3. Szabályosságok a prímszámok sorozatában

A prímszámok sorozata meglehetősen szabálytalan. Ebben a fejezetben azt fogjuk vizsgálni, hogy lehet-e ebben a sorozatban valamiféle szabályosság. Konkrétabban arra térünk ki, hogy lehetnek-e számtani sorozatok, ill., milyen számtani sorozatok lehetnek a prímszámok halmazában. Ezzel kapcsolatban 2004-ben született komoly új eredmény. Kezdjük egy korábbi problémával!

1. kérdés: Mely számtani sorozatokban van végtelen sok különböző prímszám?

Tekintsük pl. az alábbi számtani sorozatot!

$$28,\ 28 + 35,\ 28 + 2{\cdot}35,\ 28 + 3{\cdot}35,\ \ldots$$

Ebben nyilvánvalóan nincs végtelen sok prímszám, sőt egy sincs: mindegyik elem osztható 7-tel (és nagyobb 7-nél). Ehhez hasonlóan intézhetők el az olyan számtani sorozatok, amelyek első elemének – a_0 – és differenciájának – d – legnagyobb közös osztója – $D = (a_0, d)$ – nagyobb, mint 1. Az ilyen sorozat minden eleme osztható D-vel így legfeljebb egy (két) prímszám lehet benne: D (és -D, ha negatív prímeket is megengedünk).

A D=1 eset meglehetősen nehéz, de viszonylag régen megoldott. Erre vonatkozik az alábbi tétel.

4. Tétel (Dirichlet tétele, 1837) *Bármely olyan számtani sorozat, amelynek elemei egész számok és első eleme relatív prím a differenciához, végtelen sok prímszámot tartalmaz.*

A tétel állítása szerint pl. a

$$27,\ 27 + 35,\ 27 + 2{\cdot}35,\ 27 + 3{\cdot}35,\ \ldots$$

sorozatban is végtelen sok prímszám van, hiszen 27-nek és 35-nek a ± 1-en kívül nincs közös osztója.

Ajánló

Dirichlet tételének bizonyítása elolvasható a speciális matematika tagozatos számelmélet könyvben:

Szalay Mihály: Számelmélet, Typotex Kiadó, http://www.typotex.hu/book/m_0092.htm

Dirichlet tételével számos feladat is megoldható. Lássunk egy példát!

1. feladat Hány olyan prímszám van, amelynek utolsó kilenc jegye kilences?

A feladat így is fogalmazható: „hány prímszám van a 999 999 999 + $k{\cdot}10^9$ számtani sorozatban:”. Itt a kezdő elem 999 999 999, a differencia pedig 1 000 000 000, ezek relatív prímek, így végtelen sok prímszám van a sorozatban, végtelen sok olyan prím van, amelynek utolsó kilenc jegye kilences.

2. feladat (Házi feladat) Hány olyan prímszám van, amelyben legalább 2005 darab 0 szerepel?

Térjünk vissza az eredetileg ígért problémára!

2. kérdés Milyen hosszú olyan számtani sorozat van, amelynek minden tagja prímszám?

Vajon lehet-e végtelen hosszú? Erre tagadó a válasz és középiskolás szinten is végiggondolható.

5. Tétel *Nincs olyan (nem konstans) végtelen számtani sorozat, amelynek minden tagja prímszám.*

Az 5. Tétel bizonyítása Az a_0, $a_0 + d$, $a_0 + 2d$, ... sorozatban előfordulnak az $a_0 + a_0d$, $a_0 + (2a_0)d$,... – illetve, ha a_0 negatív, akkor az $a_0 - a_0d$, $a_0 - (2a_0)d$,... – tagok, ezek mind oszthatók a_0-lal. Ha itt $a_0 \neq \pm 1$, akkor máris találtunk sok elemet, amely biztosan nem prím. Ha $a_0 = \pm 1$, akkor ugyanez a gondolatmenet működik a_0 helyett a sorozat bármely másik – ± 1-től különböző – tagjából kiindulva.

Van-e felső korlát, tehát igaz-e, hogy egy adott számnál hosszabb számtani sorozatot már nem lehet készíteni prímekből, vagy nincs ilyen felső korlát, tehát akármilyen hosszú sorozat készíthető?

Öt elemből álló számtani sorozat még fejben is készíthető: pl. 5, 11, 17, 23, 29. A differencia itt elég szabályos, 6, ami 2·3. Azt állítjuk, hogy, ha hattagút akarunk, akkor ez a differencia már nem fog működni.

3. feladat Mutassuk meg, hogy ha egy pozitív számokból álló számtani sorozatnak több mint öt különböző eleme van, akkor a sorozat differenciája osztható 5-tel!

A 3. feladat megoldása Fel fogjuk használni, hogy ilyen esetben a differencia biztosan osztható 2-vel és 3-mal. Ez az alábbiakhoz hasonlóan igazolható. Valójában csak az kell, hogy a differencia legalább 6.

Tekintsük először csak négy elemet: a, $a + b$, $a+2b$, $a+3b$, $a+4b$, ahol a és b tetszőleges pozitív egészek. Ha b nem osztható öttel, akkor ezek a számok csupa különböző maradékot adnak öttel osztva. Valóban, ha volna köztük két azonos maradékú, akkor azok különbsége osztható lenne öttel, de ez a különbség a b, $2b$, $3b$, $4b$ számok egyike, így nem osztható öttel, ha b sem.

Az öt felsorolt szám ötös maradékai – nem feltétlenül ebben a sorrendben – tehát 0, 1, 2, 3 és 4. Vagyis a számok között van 5-tel osztható, és az csak úgy lehet prím, ha személyesen az 5. Tehát ez azt jelenti, hogy a sorozat elemei között szerepel az 5. Mivel a differencia legalább 6, így ez csak az első elem lehet, azaz a. Ilyenkor azonban a hatodik tag, a korábban nem említett $a+5b$ is osztható öttel, így nem lehet prím. Tehát öttel nem osztható differenciával nem készíthető hat pozitív prím elemből álló számtani sorozat.

4. (Házi) feladat Mutassuk meg, hogy ha egy pozitív számokból álló számtani sorozatnak több mint n különböző eleme van, akkor a sorozat differenciája osztható az összes n-nél nem nagyobb prímmel!

A 3-4. feladatok állítása szerint hattagú sorozathoz olyan differenciát kell választanunk, ami 2-vel, 3-mal és 5-tel is osztható, vagyis hattagú sorozat differenciájának osztója a 30. Ilyen van, például a 7, 37, 67, 97, 127, 157. Tovább is mehetünk: ha nyolctagú sorozatot akarunk gyártani, akkor a 7-tel való oszthatóság is bejön, minél hosszabb számtani sorozatot akarunk, annál több mindennel kell oszthatónak lennie a differenciának. Tehát mondjuk a 15 tagú, csak prímekből álló számtani sorozat differenciájának oszthatónak kell lennie 2·3·5·7·11·13-mal. Ez már egy elég nagy szám!

Vajon milyen hosszú ilyen számtani sorozatot ismerünk? Azt gondolhatnánk, hogy számítógépeink jelenlegi fejlettsége mellett már 30 000 vagy talán már 500 000 prímszámból álló számtani sorozatot is találtak. Ehhez képest a válasz meglepően kicsi. A pillanatnyilag – azaz 2005. november 22-én – ismert leghosszabb sorozat csak 22, azaz huszonkét tagú! Ilyen hosszúból viszont hármat is tudunk, íme ($k \in \{0, 1, 2, ..., 21\}$):

$28\,383\,220\,937\,263 + 1\,861\,263\,814\,410\,k$, ahol $1\,861\,263\,814\,410 = 2{\cdot}3^5{\cdot}5{\cdot}7{\cdot}11{\cdot}13{\cdot}17{\cdot}19{\cdot}23{\cdot}103$;

$11\,410\,337\,850\,553 + 4\,609\,098\,694\,200\,k$, ahol $4\,609\,098\,694\,200 = 2^3{\cdot}3{\cdot}5^2{\cdot}7{\cdot}11{\cdot}13{\cdot}17{\cdot}19{\cdot}23{\cdot}1033$;

$376\,859\,931\,192\,959 + 18\,549\,279\,769\,020\,k$, ahol $18\,549\,279\,769\,020 = 2^2{\cdot}3{\cdot}5{\cdot}7^2{\cdot}11{\cdot}13{\cdot}17{\cdot}19{\cdot}23{\cdot}5939$.

A differenciák meglehetősen gazdaságosak: felbontásukban szerepel az összes 22-nél kisebb prím – láttuk, ez feltétlenül szükséges – , illetve a 23 – amit igazán érdemes belevenni –, és ezeken kívül csak nagyon kevés tényező.

Tehát ott tartunk, hogy 22, de hol vagyunk az akármilyen hosszútól? Másfél évvel ezelőtt jött a megdöbbentő hír, hogy bebizonyították:

6. Tétel (Ben Green, Terence Tao, 2004) *Tetszőleges véges hosszúságú, csak prímekből álló számtani sorozat létezik.*

Nem tudjuk, hogy miképp lehet egy 23 vagy 100000 tagú ilyen sorozatot találni, de azt már tudjuk, hogy ilyenek léteznek.

Ajánló

Korábbi eredmények a témában: http://mathworld.wolfram.com/PrimeArithmeticProgression.html

Ben Green és Terence Tao cikke: http://arxiv.org/PS_cache/math/pdf/0404/0404188.pdf vagy http://front.math.ucdavis.edu/m

Érdekességként megjegyezzük, hogy az egyik szerző, Ben Green, Budapesten dolgozott fél évig a Rényi Matematikai Kutatóintézetben.

4. Ikerprímek

Csak két olyan szomszédos szám van, amelyek közül mindkettő prím: a 2 és a 3, hiszen szomszédos számok egyike páros és a 2 az egyetlen páros prím. Ősidők óta foglalkoztatja a gondolkodókat, hogy hányszor fordul elő, hogy két prím különbsége 2.

Ikerprím *nek nevezünk két prímet, ha különbségük kettő.*

Ikerprímek pl. a 3 és az 5, az 5 és a 7, a 11 és 13, a 17 és 19, a 29 és 31, stb. Máig megoldatlan, hogy hány ikerprím számpár van.

Ikerprím-sejtés *végtelen sok ikerprím van.*

Tavaly megjelent a hír az interneten, hogy ,,majdnem" megoldották a sejtést. A bizonyítás hibásnak bizonyult, de a szerzők, kiegészülve a magyar Pintz Jánossal és egy Y. Motohashi nevű japán úrral, 2005-ben tényleg előreléptek a kérdésben, de szó sincs róla, hogy igazolták volna a sejtést. Az alábbiakban megpróbálom érzékeltetni ezt az előrelépést. Előzetesen lássunk néhány kapcsolódó eredményt!

Az eddigi legnagyobb ikerprímeket Járai Antal és munkatársai találták meg 2005 szeptember 9-én. Ezek a prímek 51779 jegyből állnak. Konkrét alakjuk:

$$16\ 869\ 987\ 339\ 975 \cdot 2^{171960} \quad \pm 1.$$

5. (házi) feladat (hármasikrek) Hányszor fordul elő, hogy p, p+2 és p+4 is prím?

A számelmélet sajátossága, hogy nagyon egyszerűen megfogalmazhatók olyan kérdések, amelyek az Ókortól máig megoldatlanok, ugyanakkor számos ezektől alig különböző kérdést már a középiskolások is meg tudnak válaszolni.

7. Tétel *Az ikerprímek sokkal ,,kevesebben" (azaz jóval ritkábban) vannak, mint a prímek.*

A pontos állítást nem mondjuk ki, csak rávilágítunk, hogy miről van szó. Meglehetősen jól le tudjuk írni, hogy valamely adott számig hány prím van és ehhez képest egy sokkal kisebb, elenyésző függvénnyel tudjuk felülről becsülni az ikerprímek számát. Ez az eredmény kb. 80 éve ismert.

Most engedjük meg, hogy a két számnak, melyek különbsége 2, csak az egyike legyen prím, a másik csak ,,majdnem-prím" legyen! ,,Majdnem-prímen" mondjuk értsük azt, hogy legfeljebb 100 000 prímosztója lehet. Ilyen eredmény van: végtelen sok (prím, majdnem-prím) pár van kettes különbséggel. Mit gondolnak, mennyit lehet engedni a 100 000-ből, hogy igaz maradjon az állítás? Az eredmény megdöbbentő:

8. Tétel a majdnem ikerprímekről *Végtelen sokféleképpen választható ki két szám úgy, hogy különbségük kettő és egyikük prím, másikuk pedig legfeljebb két prím szorzata.*

Ez az eredmény kb. negyven éves. A hasonlóság ellenére az Ikerprím-sejtés megoldása nem tűnik reményteljesnek.

Nézzük meg mi történ az idei évben, azaz 2005-ben! A következőt vizsgáljuk: ,,milyen közel lehet egymáshoz két szomszédos prím?".

Jelölje P_n az n-edik prímszámot (tehát P_1=2, P_2=3, P_3=5, stb.)!

3. kérdés Vajon milyen kicsi lehet $P_{n+1} - P_n$ végtelen sokszor?

Ez a különbség persze időnként nagy, sőt akármilyen nagy is lehet, de ez nem baj. Az Ikerprímsejtés szerint végtelen sokszor lehet 2. Azt gondolhatnánk, hogy talán már ismert: az említett különbség végtelen sokszor legfeljebb 4. Erről szó sincs. Még azt sem tudjuk bebizonyítani, hogy végtelen sokszor lehet egy adott konstansnál kisebb, pl. nem tudjuk bizonyítani, hogy végtelen sokszor lehet $10^{10^{10}}$-nél kisebb, pedig ez egy hihetetlenül nagy szám. Akkor mégis, mi lehet az eredmény?

Ehhez meg kell először értenünk egy klasszikus eredményt.

9. Prímszámtétel (Hadamard, de la Vallée Poussin, 1896) $P_n \approx n \cdot \ln n$.

A tétel tehát azt mondja ki, hogy az n-edik prímszám kb $(n\cdot \ln n)$, ahol ln az $e \approx 2{,}71$ alapú logaritmust jelöli. A ,,kb" pontos jelentése itt ,,aszimptotikus egyenlőség", azaz

$$\lim_{n\to\infty} \frac{P_n}{n \cdot \ln n} = 1.$$

Megjegyezzük, hogy a fenti tétel azt is igazolja, hogy a számelmélettel az egészségünk érdekében is ajánlott foglalkozni, hiszen de la Vallée Poussin 96 éves korában, Hadamard pedig 98 évesen halt meg.

Később látni fogjuk, hogy a Prímszámtételből következik az alábbi tétel:

10. Tétel *Létezik olyan c konstans, amelyre $P_{n+1}-P_n < c \ln n$ végtelen sok n-re teljesül.*

Sokáig foglalkoztak azzal, hogy ezt a c konstanst a lehető legkisebbre csökkentsék. 2005-ig sikerült $c \approx 0.4$-ig eljutni. Ekkor, tehát 2005-ben, jött ebben a megközelítésben az emlegetett jelentős áttörés:

11. Tétel (Goldston, Motohashi, Pintz és Yildirim) *Tetszőleges pozitív c konstanshoz végtelen sok olyan különböző n pozitív egész található, amelyre $P_{n+1} - P_n < c \ln n$ teljesül.*

Itt tartunk ma.

Megjegyezzük, hogy $\log_{10} \quad n$ (ami ln n-től csak egy konstans szorzóban különbözik) lényegében azt mondja meg, hogy az n szám hány jegyből áll. Tehát a 11. Tétel jelentése az, hogy két szomszédos prím távolsága végtelen sokszor kisebb lesz, mint a prímek jegyeinek szám, sőt a jegyek számának tizedénél, századánál, ezredénél, stb is végtelen sokszor kisebb lesz a különbség. Ez még mindig nagyon messze van attól, hogy 2-nél is végtelen sokszor kisebb a különbség.

Felelevenítjük a ,,Beharangozóban" írt hasonlatot: azt ,,sejtjük", hogy egy gyufaszál mérete 2 cm. Eddig azt tudtuk belátni, hogy egy gyufaszál rövidebb, mint az Egyenlítő és a Margit-híd távolsága, most pedig már azt is tudjuk, hogy az Egyenlítő és a Lánchíd távolságánál is rövidebb. Másrészt a 11. Tétel bíztató, mert minőségileg más a korábbi eredményeknél és új módszereket is hozott.

Végül térjünk vissza a 10. Tételre, hogy vázoljuk miként adódik a Prímszámtételből.

A 10. Tétel bizonyítása Becsüljük meg a $\sqrt{N}$-edik és az N-edik prím közti intervallum hosszát!

$P_N \approx N \cdot \ln N$, míg $P_{\sqrt{N}} \approx \sqrt{N} \cdot \ln \sqrt{N} = 0,5\sqrt{N} \cdot \ln N$, így a vizsgált intervallum hossza: $\left(N - 0,5\sqrt{N}\right) \cdot \ln N$. Ebben az intervallumban $\left(N - \sqrt{N}\right)$ db prím van, melyek között az átlagos

távolság:

$$\frac{\left(N-0,5\sqrt{N}\right)\ln N}{N-\sqrt{N}} = \ln N \cdot \left(1+\frac{0,5\sqrt{N}}{N-\sqrt{N}}\right) = \ln N \cdot \left(1+\frac{0,5}{\sqrt{N}-1}\right).$$

Látható, hogy a jobb oldali képletben $\ln N$ szorzója N növekedtével 1-hez tart. Tehát elég nagy N-re a $\sqrt{N}$ -edik és az N-edik prím közti egymás utáni prímek átlagos távolsága kisebb pl. $(1,0001 \cdot \ln N)$-nél, így van köztük két olyan – P_n és P_{n+1} –, melyek távolsága kisebb (1,0001·ln N)-nél. Mivel $\sqrt{N} \leq n$,így $\ln\, N \leq (2 \cdot \ln n)$, amiből

$$P_{n+1} - P_n \quad < 1,0001 \cdot \ln N \quad \leq 2,0002 \ln n.$$

Elég nagy N-hez tehát mindig található a fenti egyenlőtlenségnek megfelelő n szám és könnyű meggondolni, hogy az N-ek egy megfelelő növekvő sorozatához (pl. N, N^2, N^4, N^8 ...) tartozó n-sorozat tagjai különbözőek. Ez igazolja a 10. Tételt a c = 2,0002 konstanssal.

Ajánló

A Prímszámtétel a Mathworld Enciklopédiában:
http://mathworld.wolfram.com/PrimeNumberTheorem.html
Ugyanott az ikerprímekről: http://mathworld.wolfram.com/TwinPrimes.html
A 11. Tétel első publikációja: http://front.math.ucdavis.edu/math.NT/0505300