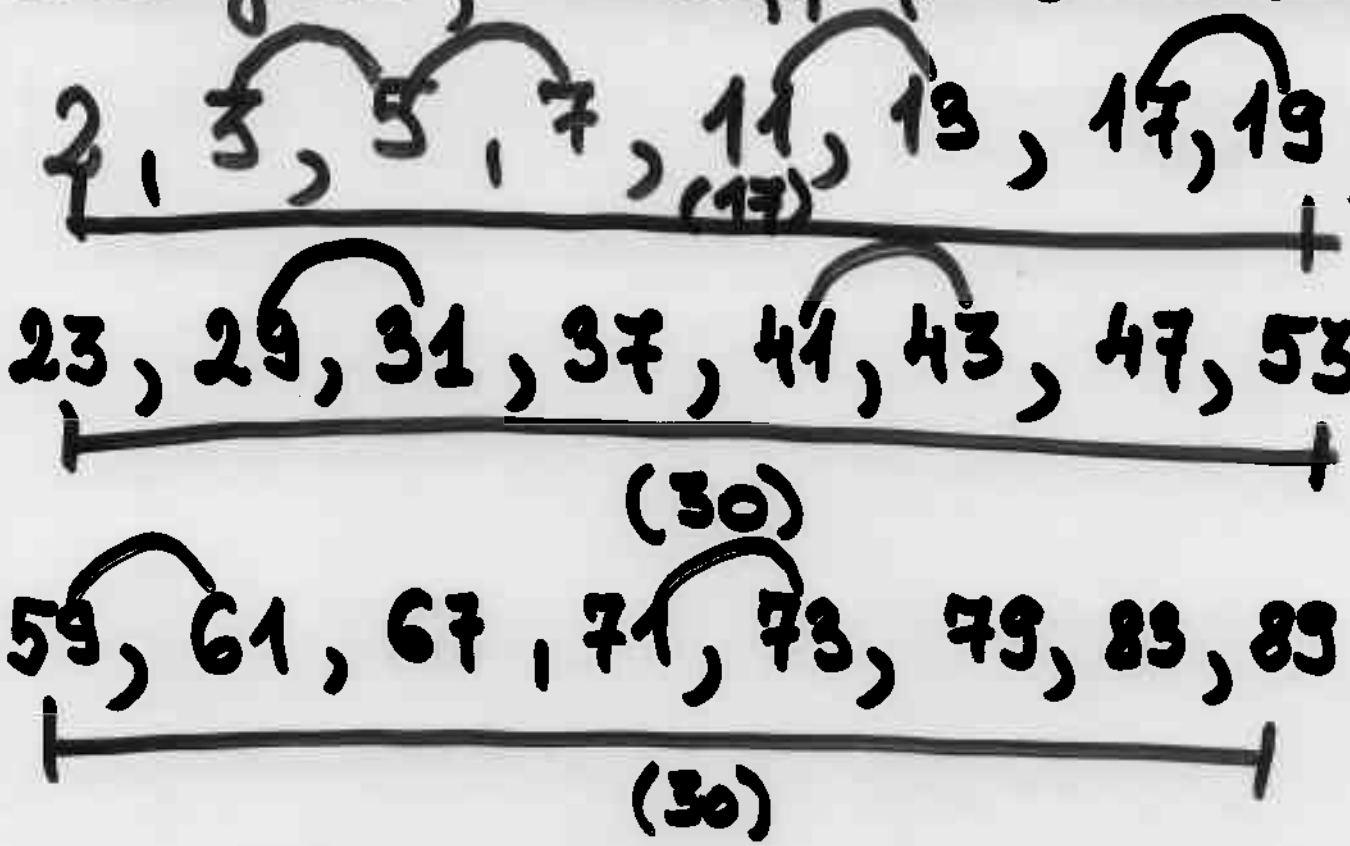
Néhány híres probléma prímszámokra

(Pintz János)

2013.04.03.

Prímszámok: nincs valódi osztójuk; mdosabb felbonthatatlanok



Ikerprímek (iker prímpárok)

Két szomszédos páratlan szám, amelyik mindkettő prím.

Ha a prímek sorozata

$p_1, p_2, p_3, \ldots$ akkor

$$p_{n+1} - p_n = 2$$

Melyik a matematika legrégibb (máig is megoldatlan) problémája? Lehetséges, hogy az

IKERPRIMSEJTTÉS:

Bármilyen nagy szám felett is találunk újabb ikerprímpárokat, azaz az ikerprímek száma

VÉGTELEN

Euklidesz (Eratoszthenesz?) 2300 éve igazolta, hogy a PRÍMEK SZÁMA VÉGTELEN

Biz. Ha csak véges sok

prímszám lenne, szorozzuk ezeket mind össze és adjunk hozzá 1-et:

$$N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$$

↓

ez a feltételezett legnagyobb (utolsó) prím

N nem osztható semmilyen prímmel, hiszen elosztva bármelyikkel 1 maradékot kapunk

Így N maga is prím, azaz mégse $p_1, p_2, p_3, \ldots p_n$ az összes prím. ELLENTMONDÁS

Mire jó a matematika?

Mire jók a prímszámok?

(i) Mire jók a prímszámok a matematikán belül

SZÁMELMÉLET ALAPTÉTELE
(Euklidesz, GAUSS 1801)

Bármely pozitív egész szám egyértelműen írható fel

prímek szorzataként (eltekintve a sorrendtől)

PRÍMSZÁMOK = ATOMOK
(felbonthatatlanok) a szorzásra nézve

Prímszám-e az 1? (NEM)

(ii) Mire jók a prímszámok a valós életben?

Hardy (50-es években): szerinte SEMMIRE és ez szerinte mindörökre így is marad

RIVEST, SHAMIR, ADLEMAN (1978): TITKOS KÓDOK KÉSZÍTÉSÉRE (RSA) [MIT]

(Cocks, u.ez 1973-ban)

Két nagy prím kell hozzá (50 - 100 - 200 jegyű)

SOK EGYÉB KÓDELMÉLETI ALKALMAZÁSUK IS VAN

Mire jók az ikerprímek?

~ ~ ~

Mire nem jók az ikerprímek?

RSA titkos kódokban történő alkalmazásra

Mekkora a legnagyobb ismert prím?

$$2^{43.112.609} - 1 = 2^P - 1$$

Mersenne prím: kb. 13 millió jegyű

(1588-1648) francia szerzetes

(Mersenne prímeket "gyorsan" lehet tesztelni - 100,000 USD)

2008.08.23.

Mekkorák a legnagyobb ismert ikerprímek?

$655\,164\,68.355 \cdot 2^{333\,333} \pm 1$

(100 355 jegyű)

Hány prímszám van egy nagy X határig? (Pa prímek halmaz)

PRÍMSZÁMTÉTEL (1896 Hadamard, ill. || de la Vallée Poussin)

$$\#\{p \le x,\ p \text{ prím}\} \sim \frac{x}{\log x} \sim \int_2^x \frac{1}{\log t}\,dt$$

Köv. $\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty$ (DIVERGENS)

1920 BRUN $\sum_{p,\,p+2 \in \mathbb{P}} \frac{1}{p} + \frac{1}{p+2} = B_2 = 1.90$

Milyen matematikai problémák megoldásával lehet a legtöbb pénzt keresni?

Wolfskehl díj (1905-1906)

100 ezer német (birodalmi) márka

≈ 1 Millió mai angol font £

[~300 Millió Ft]

Fermat sejtés $X^n + Y^n = Z^n$ $(n>2)$

esetén nincs pozitív egész

megoldás. A. Wiles 1994-1995

1997 Wolfskehl díj 30.000 £

(~ 9-10 Millió Ft)

[Richard Taylor]

Faber and Faber Könyvkiadó

2000.03.20 ⇒ 2002.03.20.

1 Millió $ (≈200 Millió Ft)

GOLDBACH SEJTÉS:

(1742.06.07.)

Tetszőleges 2-nél nagyobb

páros szám felírható

KÉT PRÍM ÖSSZEGEKÉNT.

2000.05.24. Clay Intézet

7 Milleneumi problémára à

1 Millió $ - RIEMANN SEJTÉS

Megoldva Poincaré sejtés (1904)

Megoldó: G. Perelman (2002-2003)

Clay-díj 2010.06.08

Melyik matematikai probl. ma megoldása került eddig a legtöbb pénzbe?

Említettük, hogy az ikerprím probléma egy ellenkező irányú megközelítése

$$\sum_{p,\,p+2\in\mathbb{P}}\left(\frac{1}{p}+\frac{1}{p+2}\right)=B_2=1.902160\ldots$$

kilenc tizedes pont.

Thomas Nicely (1996)

Költség 475 Mó $ ≈ 100 Milliárd Ft

Miért?

Pentium bug Intel Pentium P5

Melyik az a matematikai feladat, amit egy átl. iskolás (fejben ill. papíron) kb. tud számolni, az Intel Pentium P5 processzor (1994) nem?

$$\frac{3.145.727 \cdot 4.195.835}{3.145.727} = 4.195.835$$

(átl. iskolás)

$$\frac{3.145.727 \cdot 4.195.835}{3.145.727} = 4.195.579$$

(Pentium P5)

Relatív hiba $\frac{256}{4.195.579} > 6 \cdot 10^{-5}$

majdnem egy tízezred

Milyen közel kerülhetnek a szomszédos prímek, p_n és p_{n+1} egymáshoz?

Prímszámtétel: $\#\{p \le x\} \sim \frac{x}{\log x}$

Következmény: p_{n+1} és p_n távolsága átlagosan $\log p_n$

Pl. 1000 jegyű prímek átlagos távolsága kb. 2300 (2302,58.)

Van-e olyan $c < 1$, hogy

$p_{n+1} - p_n < c \log p_n$ a sokszor?

Igaz-e bármely $0 < c < 1$-re ez?

$$\Delta_1 = \liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} \overset{?}{=} 0$$

1940 (Erdős Pál):

Létezik egy $c < 1$, hogy

$p_{n+1} - p_n < c \log p_n$ végtelen sokszor

1966 (Bombieri-Davenport)

$p_{n+1} - p_n < \frac{1}{2} \log p_n$ végtelen sokszor

1988 (H. Maier)

$p_{n+1} - p_n < \frac{1}{4} \log p_n$ végtelen sokszor

2005/2009 (Goldston-Pintz-Yıldırım)

Tetszőlegesen kicsi $c > 0$-ra

$p_{n+1} - p_n < c \log p_n$ végtelen sokszor

2006/2010 (Goldston - Yildirim - Pintz)

$p_{n+1} - p_n < \sqrt{\log p_n}$ végtelen sokszor

Goldbach sejtés megközelítései:

(1937-38 Estermann, Van der Corput

Čudakov): Majdnem minden

páros szám előáll 2 prím összegeként

Vinogradov (1937): Minden

elég nagy páratlan szám előáll

3 prímszám összegeként.

Tétel (Pintz J., 2003/?)

Elegendően nagy X-re a páros számok közül X-ig legfeljebb

$$X^{2/3} = \left(\sqrt[3]{X}\right)^2$$

nem írható fel két prímszám összegeként.

Definíció: Egy pozitív egészekből álló A sorozat pozitív sűrűségű, ha létezik valamilyen fix $c>0$ szám, hogy A-nak elegendően nagy X-ig legalább cX eleme van

Erdős–Turán sejtés (1936):

Egy pozitív sűrűségű sorozat bár-
mely k-ra tartalmaz k hosszú
számtani sorozatot

k elem

Tétel (K.F. Roth 1953) Ez igaz k=3-ra

Tétel (Szemerédi Endre 1968) Igaz k=4

Tétel (Szemerédi) (1974). Ez
igaz bármilyen nagy (fix) k-ra.

2012 Abel díj: Szemerédi Endre

A prímek 0 sűrűségű sorozatot alkotnak: x-ig $\sim \frac{x}{\log x}$ prím van

Erdős-Turán (1936), XVIII. szd.

Waring, Legendre: milyen hosszúságú számtani sorozatok vannak a prímek közt?

Tétel (Van der Corput 1939) A prímek közt végtelen sok 3-tagú számtani sorozat van

Tétel (B. Green - T. Tao, 2004/2008) Legyen k bármilyen nagy szám. A prímek közt végtelen sok k-tagú számtani sorozat van.