Mersenne- és Fermat-prímek

Definíció.

Az $M_n = 2^n - 1$ alakú számokat **Mersenne-számoknak**, az ilyen alakú prímeket **Mersenne-prímeknek** nevezzük.

Lemma.

Ha M_n prímszám, akkor n is prímszám.

- 1536 Regius: $2^{11} - 1$ osztható 23-mal.
- 1644 Mersenne: $p \leq 257$ esetén $2^p - 1$ akkor és csak akkor prím, ha $p \in \{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$.
- 1876 Lucas: $2^{67} - 1$ mégsem prím (faktorizálás nélkül!)
- 1876 Lucas: $2^{127} - 1$ valóban prím
- 1883 Pervusin: $2^{61} - 1$ mégis prím
- 1903 Cole: $2^{67} - 1 = 193\,707\,721 \cdot 761\,838\,257\,287$
- 1911 Powers: $2^{89} - 1$ mégis prím
- 1914 Powers: $2^{107} - 1$ mégis prím
- 1932 Lehmer: $2^{257} - 1$ mégsem prím
- 1952 Robinson: teljes ellenőrzés $p \leq 257$-re

Mersenne-prímek

p	$M_p = 2^p - 1$	$2^{p-1}\left(2^p - 1\right)$	
2	3	6	ókori görögök
3	7	28	ókori görögök
5	31	496	ókori görögök
7	127	8128	ókori görögök
13	8 191	3 3550 336	1456?, 1461?
17	131 071	8 589 869 056	1588 Cataldi
19	524 287	137 438 691 328	1588 Cataldi
31	2 147 483 647	2 305 843 008 139 952 128	1772? Euler
61	$\sim$ 2 trillió	$\sim$ 2 szextillió	1883 Pervusin
89	27-jegyű szám	54-jegyű szám	1911 Powers
107	33-jegyű szám	65-jegyű szám	1914 Powers
127	39-jegyű szám	77-jegyű szám	1876 Lucas
$\vdots$	$\vdots$	$\vdots$	$\vdots$
82 589 933	24 862 048-jegyű szám	49 724 095-jegyű szám	2018 GIMPS

Fermat-prímek

Állítás.

Ha $2^n + 1$ prímszám, akkor n kettőhatvány. (HF)

n	$F_n = 2^{2^n} + 1$	státusz	
0	3	prím	
1	5	prím	
2	17	prím	
3	257	prím	
4	65 537	prím	
5	4 294 967 297	$641 \cdot 6\,700\,417$	1732 Euler
⋮	⋮	⋮	⋮
18 233 954	igen nagy szám	összetett	2020 Propper et al.

Összesen 310 Fermat-számról `tudjuk`, hogy összetett.

A legkisebb, amire nyitott a kérdés: $F_{33} = 2^{2^{33}} + 1$.

Szabályos sokszögek szerkeszthetősége

Tétel (Gauss 1801, Wantzel 1837).

A szabályos n-szög akkor és csak akkor szerkeszthető, ha az n prímfelbontásában fellépő páratlan prímek mind Fermat-prímek, és mindegyik első hatványon lép fel.

Szerkesztési eljárások:

- $F_0 = 2^1 + 1 = 3$: ókori görögök
- $F_1 = 2^2 + 1 = 5$: ókori görögök
- $F_2 = 2^4 + 1 = 17$: Gauss 1796, Erchinger $\sim$1800
  $\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\right)$
- $F_3 = 2^8 + 1 = 257$: Richelot 1832
- $F_4 = 2^{16} + 1 = 65537$: Hermes 1894 (10 év, 200 oldal!)