Prímszámok. Fermat- és Mersenne-számok

Megyesi László

Bolyai Intézet

2005. november 19.

1 Bevezetés
2 Idézet
2 Bolyai
2 Prímszám
2 Prímszám
2 Prímszám
2 A számelmélet alaptétele
2 Végtelen sok prímszám létezik
2 Végtelen sok prímszám létezik
2 Fermat
2 Bizonyítás 1
2 Bizonyítás 2
2 Gauss
2 Gauss-tétele
2 ötszög
2 tizenhétszög
2 17-szög ábra szerkesztés
2 17-szög ábra
2 Síremlék
2 257-szög

Idézet

Az egész számtan, sőt az egész tan mezején – alig van szebb és érdekesebb –... s a legnagyobb nyitászok (matematikusok) figyelme és eleje óta elfoglalt tárgy mint a főszámok (prímszámok) oly mély homályban rejlő titka.
Bolyai János

Bolyai János 1802-1860

Definíció (prímszám)

Egy $n \geq 2$ természetes számot prímszámnak nevezünk, ha pontosan két osztója van: az 1-es és önmaga.

Definíció (prímszám)

Egy $n \geq 2$ természetes számot prímszámnak nevezünk, ha pontosan két osztója van: az 1-es és önmaga.

Ekvivalens definició: Egy természetes szám akkor és csakis akkor prímszám, ha valahányszor osztója egy szorzatnak, akkor valamelyik tényezőjének osztója.

Definíció (prímszám)

Egy $n \geq 2$ természetes számot prímszámnak nevezünk, ha pontosan két osztója van: az 1-es és önmaga.

Ekvivalens definició: Egy természetes szám akkor és csakis akkor prímszám, ha valahányszor osztója egy szorzatnak, akkor valamelyik tényezőjének osztója.

A jelen előadásban a definíciók, tételek természetes számokra vonatkoznak.

A számelmélet alaptétele

A prímszámok alapvető fontosságát mutatja a számelmélet alaptétele:

Tétel. *Bármely $n \geq 2$ természetes szám kifejezhető prímszámok szorzataként, mégpedig a prímszámok sorrendjétől eltekintve egyértelműen.*

Tétel. *Végtelen sok prímszám létezik.*

Tétel. *Végtelen sok prímszám létezik.*

Bizonyítás (Pólya György, 1887-1985)

Tekintsük a Fermat-számokat! Az n-edik Fermat-szám

$$F_n = 2^{2^n} + 1,$$

azaz $F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \quad \ldots$
Bizonyítjuk, hogy bármely két különböző Fermat-szám relatív prím.

Pierre de Fermat
(1601-1665)

Végtelen sok prímszám létezik. Bizonyítás

Abból, hogy bármely két Fermat-szám relatív prím – azaz nincs közös prímtényezőjük – következik a tétel. Valóban végtelen sok Fermat-szám van, (minden természetes számhoz tartozik egy) és mindegyiknek a többitől különböző prímtényezői vannak.

Tekintsük az $F_m = 2^{2^m} + 1$ és az $F_{m+k} = 2^{2^{m+k}} + 1$ $(k > 0)$ Fermat-számokat. Bevezetve az $a = 2^{2^m}$ jelölést, a következőt kapjuk:

$$\frac{F_{m+k} - 2}{F_m} = \frac{2^{2^{m+k}} - 1}{2^{2^m} + 1} = \frac{a^{2^k} - 1}{a + 1} = a^{2^k - 1} - a^{2^k - 2} + \cdots - 1,$$

Felhasználtuk a következő jól ismert azonosságot: $x = a^{2^k}$ helyettesítéssel:

$$x^{2n} - 1 = (x + 1)(x^{2n-1} - x^{2n-2} + \ldots - 1)$$

Az itteni gondolatmenet azt mutatja, hogy $F_m | F_{m+k} - 2$ bármely k pozitív egész számra. Ha p olyan prímszám, amely osztója F_m-nek és F_{m+k}-nek, akkor az előző oszthatóság miatt p osztója $F_{m+k} - 2$-nek, következésképpen az $F_{m+k} - 2$ és az F_{m+k} különbségének 2-nek is. Ez nem teljesülhet (minden Fermat-szám páratlan). Ez az ellentmondás bizonyítja azt, hogy bármely két különböző Fermat-szám relatív prím.

Gauss-tétele

Karl Friedrich Gauss.

1777-1855

Gauss-tétele

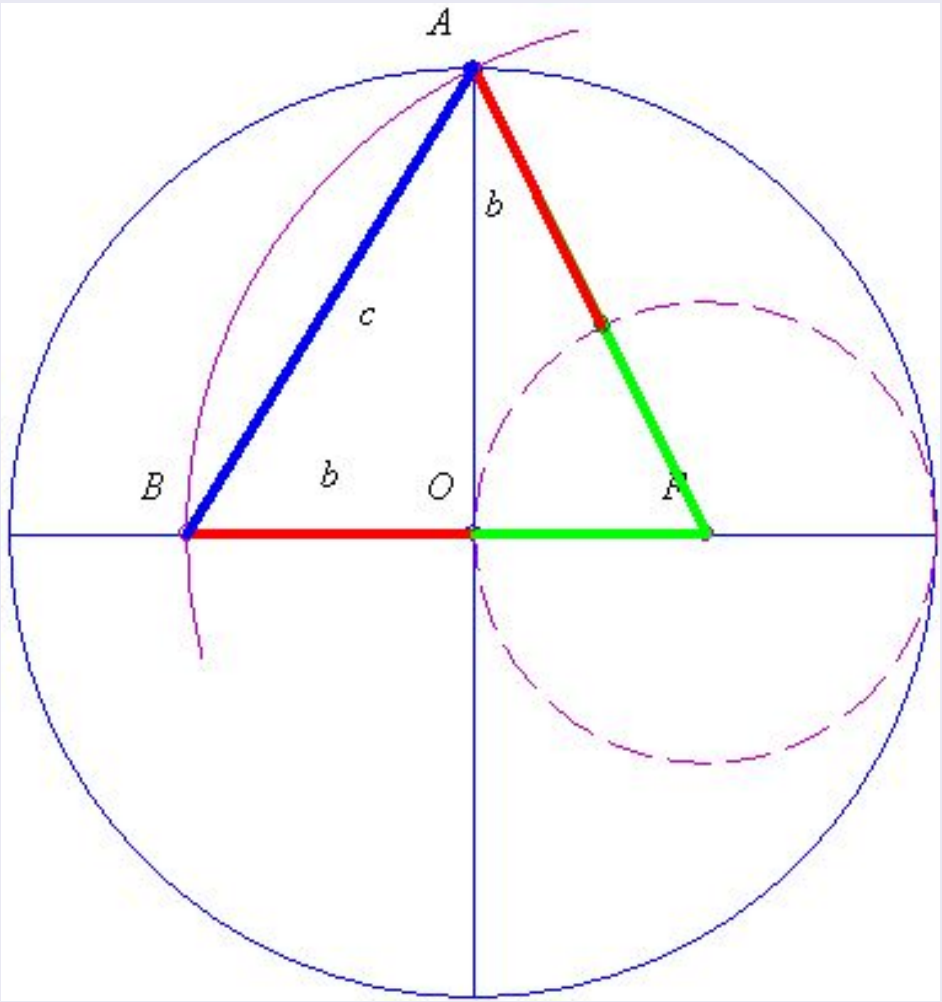
Tétel. *Egy szabályos n-szög akkor és csakis akkor szerkeszthető körzővel és egyélű vonalzóval, ha*

$$n = 2^k p_1 p_2 \dots p_r$$

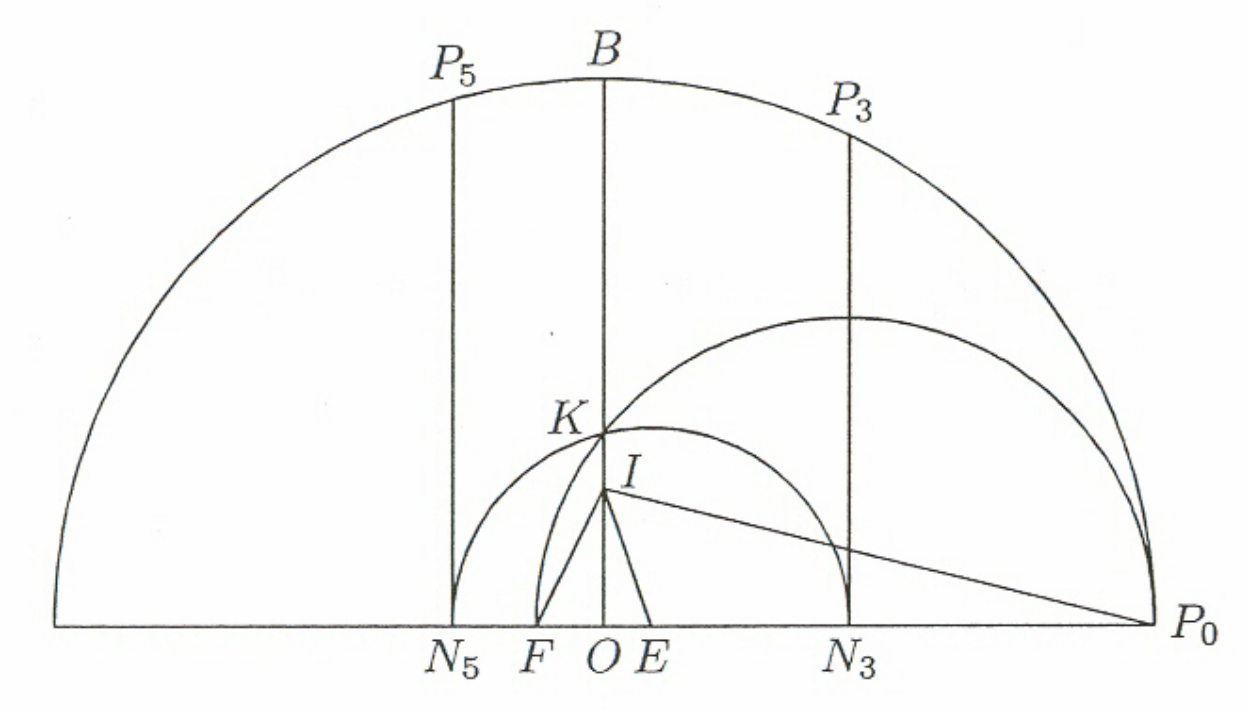
ahol $k = 0,\ 1,\ 2, \dots,\ p_1,\ p_2,\ \dots, p_r$ *különböző Fermat-prímszámok.*

Jelenleg csak öt Fermat-prímet ismerünk:
$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$ Gauss-tétele szerint szerkeszthető a szabályos háromszög, ötszög, tizenhétszög 257-szög, 65537-szög. És szerkeszthető a szabályos hatszög, tizenkétszög, tízszög, harmincnégyszög, tizenötszög, huszonegyszög, harmincötszög stb.

Szabályos ötszög szerkesztése



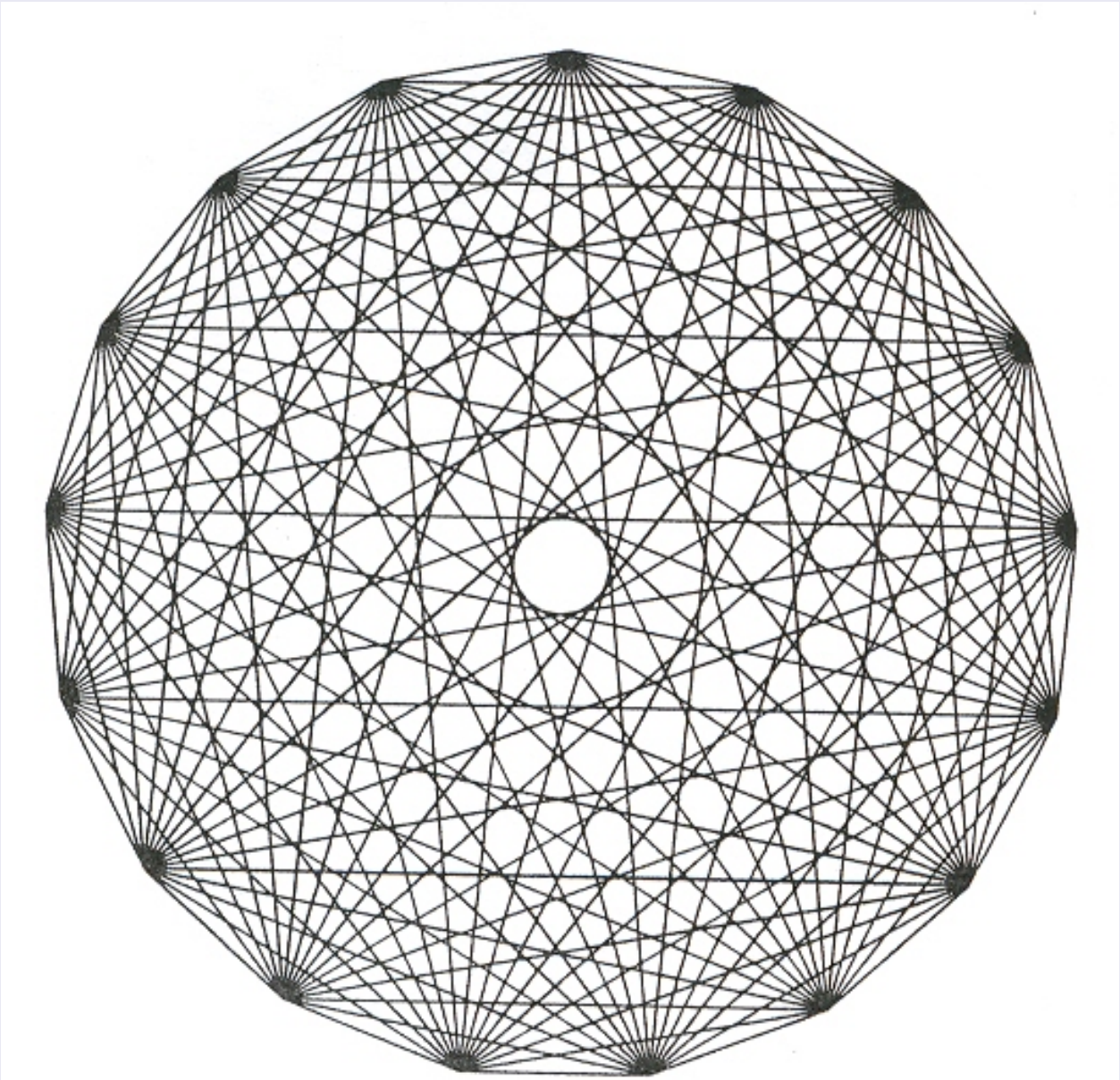
Szabályos tizenhétszög szerkesztése 1.



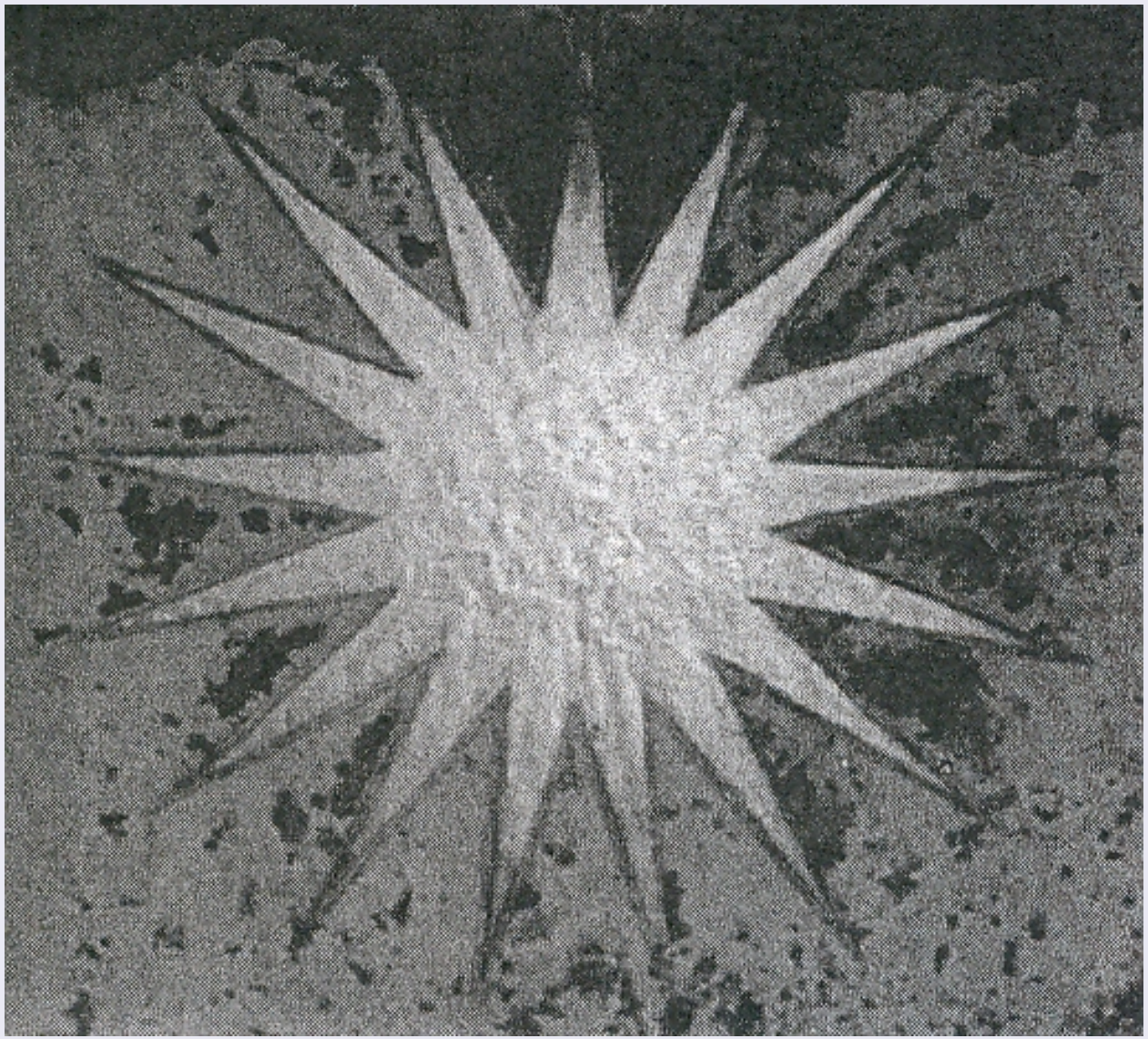
Szabályos tizenhétszög szerkesztés 2.

A kör középpontja O, OP_0 és OB egymásra merőleges sugarai a körnek. Az I pont az OB szakasz negyedelőpontja, azaz $|OI| = \frac{1}{4} \cdot |OB|$. Az E pontot szögnegyedeléssel kapjuk az OP szakaszon, úgy hogy $\angle|OIE| = \frac{1}{4} \cdot \angle|OIP_0|$. Az OP_0 folytatásában kijelöljük az F pontot, úgy hogy $\angle FIE = \frac{1}{4} \cdot \pi$. Jelölje K az FP_0 átmérőjű körnek a metszéspontját OB-val. Egy másik körnek, amelynek középpontja E és sugara az $|EK|$ szakasz az OP_0-val való metszéspontjait N_3-tel és N_5-tel jelöljük. Ebből a két pontból OB-val párhuzamosokat húzva megkapjuk P_3-at és P_5-öt azaz a tizenhétszög harmadik és ötödik csúcspontját. (P_0 a 0-adik csúcs).

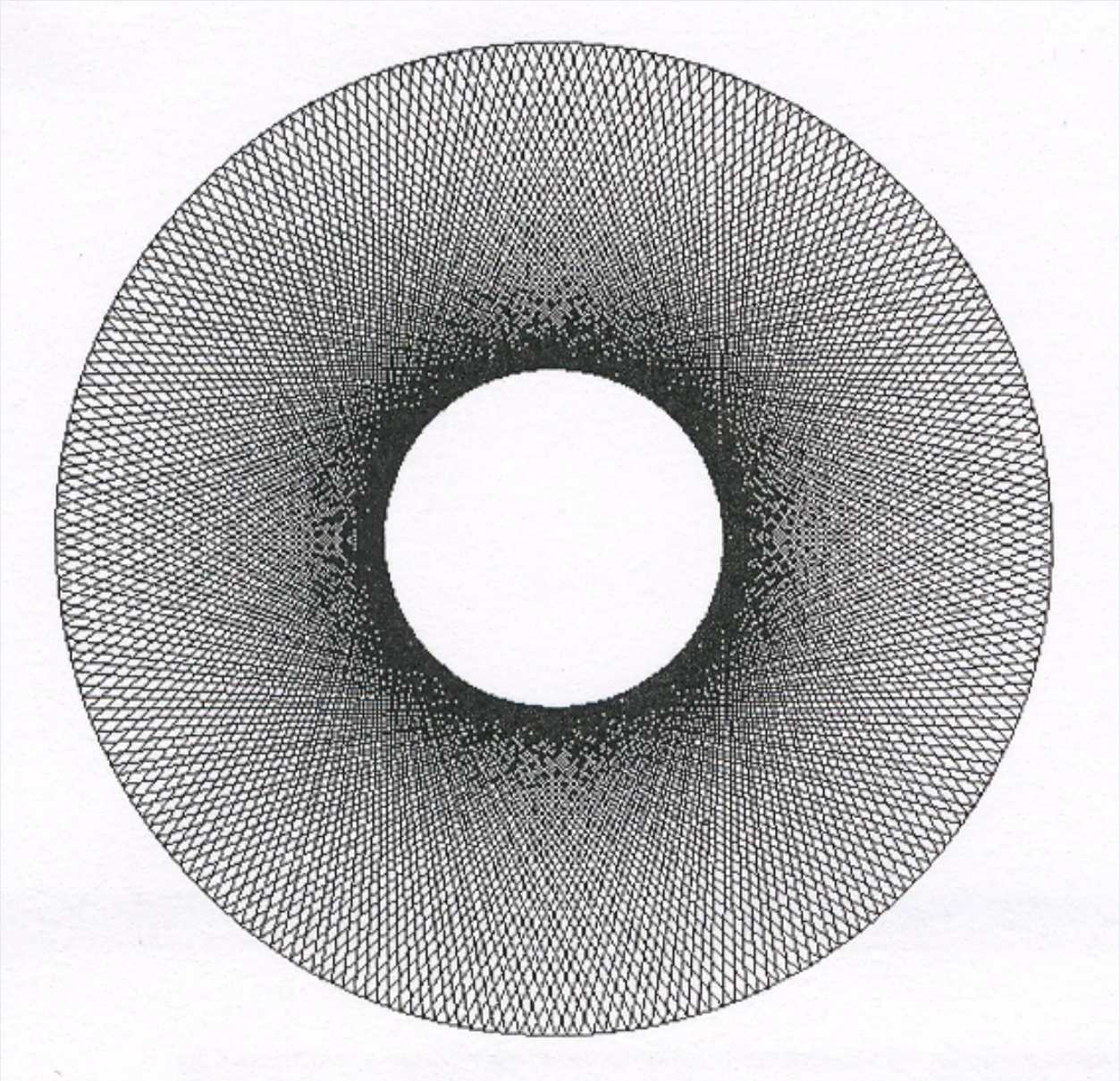
Szabályos tizenhétszög



Gauss síremlékének oldalán szabályos tizenhétcsillag van



Szabályos 257-szög

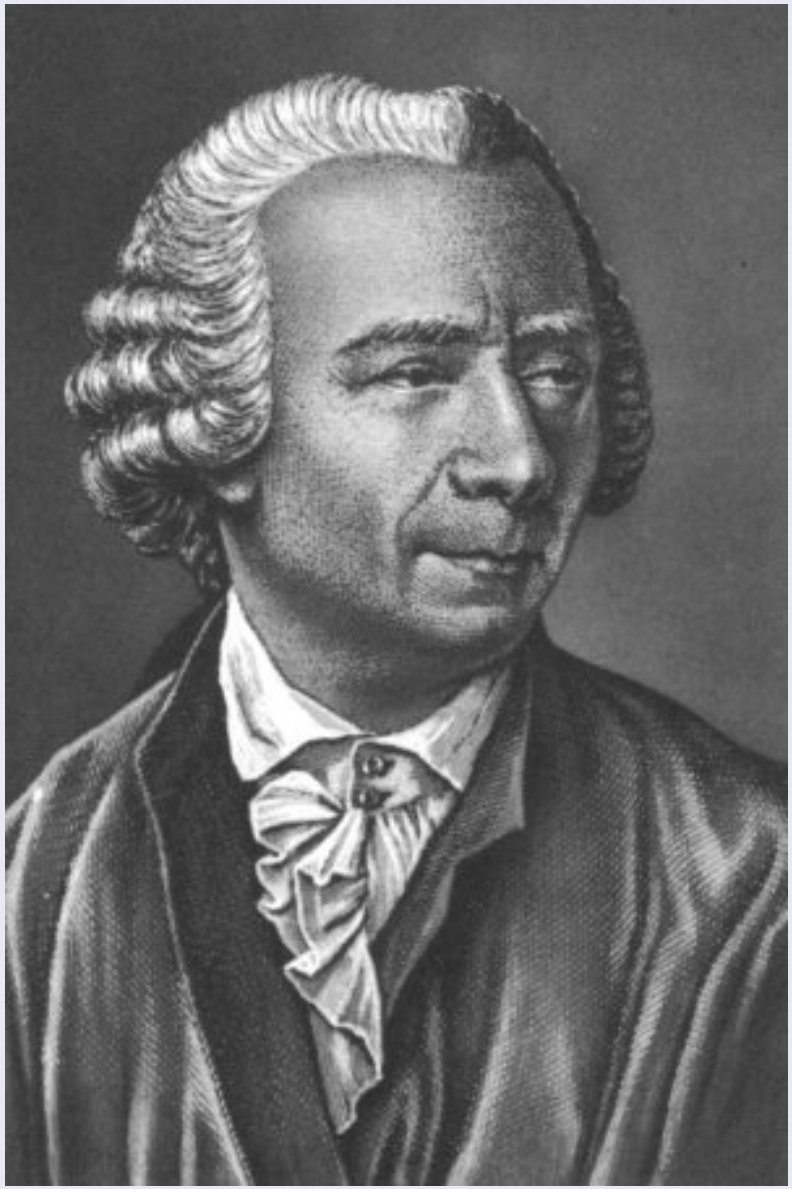


Hány Fermat-prímszám van?

Csak öt Fermat-prímet ismerünk. Ezek már szerepeltek az előadásban:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

Fermat azt gondolta, hogy minden Fermat-szám prímszám. Euler mutatta meg, hogy 641 osztója F_5-nek - ezzel megcáfolva Fermat-nak ezt a sejtését.



Leonhard Euler 1707-1783

Véges sok Fermat-prímszám van? Végtelen sok összetett Fermat-szám van?

Mind a két kérdés természetes. De egyikre sem tudjuk a választ. Számítógépekkel nagyon sok Fermat-számról kiderítették, hogy összetett, ujabb Fermat-prímet nem találtak. Elméleti úton elég könnyü megmutatni, hogy az $F_n = 2^{2^n} + 1$ Fermat-szám prímosztói csakis – $2^{n+1}k + 1$, ahol k pozitív egész – lehetnek. Ez sokat segít az osztók felkutatásában. Például: $F_{6537} = 2^{2^{6537}} + 1$ egy prímosztója $34 \times 2^{6538} + 1$. Egy nevezetes tétel: Pepin-tétele alapján pedig - meglehetősen sok számolással - eldönthető egy Fermat-számról, hogy prím-e vagy összetett szám.

Az internetről, W. Keller cikkéből

Mit tudunk most a Fermat-számokról azaz az F_m-ekről? 2005 október 5.-ei helyzetjelentés.
Pímszámok: m = 0, 1, 2, 3, 4
Teljes faktorizációját ismerjük a következő hét számnak: m = 5, 6, 7, 8 (kéttényezősök), 9 (3 tényezős), 10 (4 tényezős), 11 (5 tényezős)
A pímfelbontásából öt tényező ismert: m = 12* ,
négy tényező ismert: m = 13* ,
három tényező ismert: m = 15*, 25 ,
két tényező ismert: m = 16*, 18*, 19*, 27, 30, 36, 38, 52, 77, 147, 150, 284, 416 ,
csak egy tényező ismert: m = 17*, 21*, 23*, 26, 28, 29, 31, 32, 37, 39, 42, 43 és 185 szám, úgy hogy $43 < m < 2478782$
*tudjuk, hogy a társosztó összetett szám.

W. Keller cikkéből

Összetett szám, de a prímfelbontásáról semmit nem tudunk: $m = 14, 20, 22, 24$ (Itt használták Pepin tételét!)
Nem tudjuk,hogy összetett vagy prím: $m = 33, 34, 35, 40, 41, 44, 45, 46, 47, 49, 50, \ldots$
Összegzés:
258 pímtényezőt ismerünk a különböző Fermat-számokban, és
225 Fermat- számról tudjuk, hogy összetett szám.

A prímszámok eloszlásáról

Tétel. *A szomszédos prímszámok között akármilyen nagy hézagok előfordulnak.*

Bizonyítás. Tekintsük a következő számokat:

$$n! + 2,\ n! + 3,\ \ldots\ , n! + n$$

Ez $n - 1$ egymás után következő szám, amelyiknek egyike sem lehet prím, mert rendre oszthatók 2-vel, 3-mal, $\ldots$, n-nel. A nagy hézagok mellett az is nagyon érdekes kérdés, hogy a legkisebb hézagok milyen gyakran fordulnak elő. A 2-es és a 3-as közötti 1-es hézagon kívül a 2-es hézag az ami legkisebb lehet.

Definíció.

A p, p+2 prímszámpárt *ikerprímszámoknak* nevezzük. A legnevezetesebb kérdés, ami ikerprímekkel kapcsolatban felvethető az, hogy az ikerprímek sorozata végtelen-e. Sajnos erre a kérdésre nem sikerült választ adni.

A prímszámokkal kapcsolatban sokan törekedtek olyan képlet megadására, amely a prímszámokat megadná, avagy legalább sok prímszámot kapnánk egy formula révén. Nagyon érdekes, hogy már másodfokú polinomok között is van olyan, amelynek helyettesítési értékei valameddig prímszámot adnak. A legismertebb az Euler által felfedezett polinom az

$$x^2 + x + 41,$$

amelynek helyettesítési értékei $x = 0,\ 1,\ 2,\ \ldots, 39$ esetén rendre prímszámok.

Prímszámtétel

A prímszámok eloszlását illetően a legtöbbet a prímszámtétel mondja. Ebből egy adott pozitív számig a prímszámok száma –jó közelítéssel – megtudható. Szükségünk lesz a $\pi(x)$ függvényre.

Definíció. Legyen x pozitív valós szám. $\pi(x)$ jelöli az x-nél nem nagyobb prímszámok számát.

Prímszámtétel.

$$\pi(x) \sim \frac{x}{\ln x}$$

A prímszámtételt ketten egymástól függetlenül bizonyították be 1896-ban mély analízisbeli eszközöket használva, majd 1949-ben Erdős Pál és A. Selberg adott a tételre elemi de korántsem egyszerű bizonyítást.

További fontos tények a prímszámokról

Tétel. *A prímszámok reciprokaiból álló sor divergens.*
Csebisev-tétele. *Ha $n > 3$, akkor legalább egy prímszám van n és $2n - 2$ között.*
Sierpiński-tétele. *Ha $n > 5$, akkor legalább két prím van n és $2n$ között.*
Dirichlet-tétele. *Ha $a,\ b$ egymáshoz relatív prím számok, akkor az*

$$ax + b \quad (x = 1,\ 2,\ \ldots)$$

sorozatban végtelen sok prímszám van.

Marin Mersenne

Marin Mersenne 1588-1648

Mersenne-számok, Mersenne-prímek

Definíció. A *Mersenne-számok* az $M_p = 2^p - 1$ alakú számok (ahol p prímszám, közülük a prímek a *Mersenne-prímek.*

Mersenne fő érdeme hogy szoros kapcsolatban állt korának matematikusaival. A 257-es prímig kijelentette, hogy az egyes prímszámokra a $2^p - 1$ számok közül melyek a prímek és melyek nem.

Mersenne-számok, tökéletes számok

A Mersenne-számok, Mersenne-prímek jelentőségét a tökéletes számok adják meg.
A tökéletes számok problémáját a "régi görögök" vetették fel, az egész kérdéskör tőlük származik. A probléma érdekességét éppen az adja meg, hogy több mint 2000 éves és számos vonatkozásban ma is megoldatlan.
A pythagoraszi iskola képviselői mindent a számokból próbáltak megmagyarázni. Egy pozitív egész szám önmagánál kisebb osztóit a szám részeinek tekintették és különös jelentőséget tulajdonítottak azoknak a számoknak amelyek "részeikből visszanyerhetők" azaz "részeiknek összege" éppen az adott számmal egyenlő. Ezek a harmónia megtestesítői vagyis a "tökéletes számok". A legkisebb tökéletes szám a 6 hiszen 6=1+2+3. További három tökéletes számot is ismertek "régi görögök" a 28-at, a 496-ot, és a 8128-at.

Páros tökéletes számok

Definíció. Egy n természetes számot *tökéletes számnak* nevezünk, ha osztóinak összege egyenlő a szám kétszeresével.

A "régi görögök" tudását a tökéletes számokról Euklidesz foglalta össze az Elemek IX. könyvében (a könyv i. e. 300 körül íródott). A könyv 36. Tételét idézem (Mayer Gyula fordításában). Ha az egységtől kezdve kétszeres arányban képezünk egy mértani sorozatot, amíg a sorösszeg prím nem lesz, és az összeggel megszorozzuk, az utolsó tagot, akkor a szorzat tökéletes szám lesz. Ebben az áll, hogy ha $1 + 2 + 2^2 + \cdots + 2^n$ prímszám, akkor megszorozva 2^n-nel tökéletes számot kapunk. Euklidesz (egyébként teljes mértékben igaz) állításánál lényegesen többet bizonyított be 2000 évvel később Leonhard Euler.

Euler-tétele

Tétel. *Egy páros szám akkor és csakis akkor tökéletes szám, ha* $2^{p-1}(2^p - 1)$ *alakú, ahol* $2^p - 1$ *Mersenne-prím.*

Euler-tétele a páros tökéletes számok kérdését a Mersenne-prímek keresésére vezeti vissza. Könnyen kiszámolható, hogy $2^p - 1 \quad p = 2, 3, 5, 7$ esetén prímszám. A meglepetés akkor éri az embert, amikor észreveszi, hogy $2^{11} - 1 = 23 \cdot 89$, vagyis nem prím. Továbbhaladva, az állapítható meg, hogy rendkívüli módon "ritkulnak" a prímek a Mersenne-számok közt.

Euler nemcsak a fenti alapvető tételt találta, hanem az ő nevéhez fűződik a nyolcadik Mersenne-prím megtalálása is. (Előtte a középkorban három Mersenne-prímet találtak).
Euleren kívül a Mersenne-prímek, a tökéletes számok elméletében a legjelentősebbet Edouard Lucas 19. századi, majd D. H. Lehmer 20. századi matematikus alkotta. Bebizonyították ugyanis a következőt:

Tétel. *Tekintsük a következő sorozatot:* $r_1 = 4,\ r_{m+1} = r_m^2 - 2$. *Az* $M_p = 2^p - 1$ *Mersenne szám akkor és csakis akkor prím ha* M_p *osztója* r_{p-1}*-nek.*

Ma is ezt a tételt használják Mersenne-prímek keresésére. Az eljárást Lucas–Lehmer-tesztnek, vagy csak Lucas-tesztnek nevezik.

A legnagyobb ismert prímszámok

Jelenleg, 42 Mersenne-prímet ismerünk. 2005 februárjában jelentették be a 42-edik prím megtalálását. Ez a szám:

$$2^{25964951} - 1.$$

A számjegyeinek száma 7816230. A 41-edik és a 40-edik Mersenne-prím a következő:

$$2^{24036583} - 1, \qquad 2^{20996011} - 1.$$

Az elsőt 2004-ben, a másodikat 2003-ban találták.

GIMPS

1996-ban jött létre Amerikában a Great Internet Mersenne Prim Search. A GIMPS ingyenesen bocsát programot és megadja a vizsgálandó számot (számokat) azok rendelkezésére akik részt akarnak venni a Mersenne prímek keresésében. A részvételhez elegendő átlagos szinvonalú személyi számítógéppel rendelkezni. A világ legkülönbözőbb részein keresik a kijelölt Mersenne-számok esetleges osztóit. Ha a program lefut (egy Mersenne-szám esetében kb. 40-50 nap alatt) és azt jelzi, hogy van remény arra, hogy az adott szám prím legyen, akkor néhány szuperszámítógépen a Lucas-Lehmer-tesztet lefuttatják. Több gépen dolgoznak, hogy kellőképpen ellenőrízzék egymás munkáját is.

sorszám	p	M_p jegyei	évszám	a felfedező
5	13	4	1456	anonymous
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervushin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1279	386	1952	Robinson
16	2203	664	1952	Robinson
17	2281	687	1952	Robinson

sorszám	p	M_p jegyei	évszám	a felfedező
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tuckerman
25	21701	6533	1978	Noll, Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson, Slowinski
28	86243	25962	1982	Slowinski
29	110503	33265	1988	Colquitt, Welsh
30	132049	39751	1983	Slowinski

sorszám	p	M_p jegyei	évszám	a felfedező
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski, Gage
33	859433	258716	1994	Slowinski, Gage
34	1257787	378632	1996	Slowinski, Gage
35	1398269	420921	1996	Armengaud, Woltman
36	2976221	895932	1997	Spence, Woltman,
37	3021377	909526	1998	Clarkson**
38	6972593	2098960	1999	Hajratwala**
39	13466917	4053946	2001	Cameron **
40	20996011	6320430	2003	Shafer **
41	24036583	7235733	2004	Findley**
42	25964951	7816230	2005	Nowak**

**Woltman, Kurowski

Az öt legnagyobb ismert prímszám éppen az öt legnagyobb Mersenne-prímszám

Érdemes megvizsgálni, hogy egy-egy időszakban a legnagyobb ismert prím és a legnagyobb ismert Mersenne-prím milyen viszonyban áll egymással. 1876-tól kezdve egy rendkívül rövid (1951-52-ben egy kb. egy éves) időintervallumot leszámítva a kettő azonos volt. Ma a viszonylag nagy prímszámok a "titkosírás"-hoz, azaz a titkos üzenetküldéshez szükségesek. Számos módszert (tesztet) dolgoztak ki, amelynek célja viszonylag nagy prímszámok keresése, pontosabban egy pozitív egész számról eldönteni, hogy prím-e, vagy sem. Ezek a tesztek azonban nem vehetik fel a versenyt a Lucas-teszttel, hiszen az rendkívül egyszerű (amely természetesen csak a Mersenne-számokra használható), amelynél egyszerűbb, számítástechnikailag könnyebben kivitelezhető tesztet elképzelni sem nagyon lehet. A Lucas-teszt egyszerűsége hozza magával azt, hogy várhatóan a jövőben is a legnagyobb ismert prímek a Mersenne-prímek lesznek.

Páratlan tökéletes számok

A páratlan tökéletes számokkal kapcsolatban az a legfontosabb, hogy még egyetlen páratlan tökéletes számot sem találtak. Minden matematikus, aki valamennyire is foglalkozott a problémával, azt sejti, hogy nincs páratlan tökéletes szám. Eulert nemcsak a páros, hanem a páratlan tökéletes számok problémája is érdekelte. Ö bizonyította be a következőt:

Tétel. *Amennyiben létezik páratlan tökéletes szám, az*

$$n = p^{\alpha} m^2$$

alakú lehet csak. A p és az α olyan természetes számok, amelyek 4-gyel osztva 1 maradékot adnak; továbbá m egész szám