Amint a KöMaL 2004/1. száma is hírül adta, a fenti összeget az Electronic Frontier Foundation (EFF) annak fizeti ki, aki először állít elő legalább tízmillió jegyű prímszámot. A jelenlegi rekord a 6 320 430 jegyű $2^{20\,996\,011}-1$, amelyet a Great Internet Mersenne Prime Search (GIMPS) projekt keretében találtak 2003. november 17-én. Ebbe a programba bárki bekapcsolódhat, a részleteket lásd a `www.mersenne.org` honlapon.

Már Euklidész is tudta

Mersenne-prímeknek a 2^k-1 alakú prímeket nevezzük. A névadó *Marin Mersenne* a 17. század jelentős francia „tudományszervezője", Fermat, Descartes és más vezető tudósok intenzív levelezőpartnere volt. Ezek a prímek azonban már a régi görögöknél is felbukkannak, a tökéletes számok keresésénél. A tökéletes számok azok, amelyek „a részeikből összeállnak", azaz a valódi (= önmagukon kívüli) osztóik összege maga a szám. Ilyen a 6 vagy a 496. Euklidész *Elemek* c. könyvének IX.36 tétele így szól:

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.

Vagyis ha $1+2+2^2+\ldots+2^{k-1}=2^k-1$ prím, akkor $2^{k-1}(2^k-1)$ tökéletes szám. Pl. $k=2$-re a 6-ot, $k=5$-re a 496-ot kapjuk.

A bizonyításhoz (és ez volt lényegében Euklidész bizonyítása is) összegezni kell az $n=2^{k-1}(2^k-1)$ szám osztóit, ahol $q=2^k-1$ prímszám:

$$1+2+4+\ldots+2^{k-1}+q+2q+\ldots+2^{k-2}q=2^k-1+q(2^{k-1}-1)=q2^{k-1}=n.$$

Euklidész képlete csupa páros tökéletes számot ad. Ma is megoldatlan probléma, hogy létezik-e egyáltalán páratlan tökéletes szám (az valószínűsíthető, hogy nem). Viszont Euklidész algoritmusával az összes páros tökéletes számot megkapjuk, amint ezt mintegy 2000 évvel később Euler bebizonyította. Ez azt jelenti, hogy kölcsönösen egyértelmű megfeleltetés áll fenn a páros tökéletes számok és a 2^k-1 alakú prímek között. Sajnos ma sem tudjuk, hogy az ilyen prímek száma véges vagy végtelen (általában az utóbbira tippelnek). Erdős Pál megfogalmazásában „ez a kérdés talán a legnehezebb, ha nem is a legsürgősebb probléma, amivel az emberiség szemben áll."

A rejtélyes lista

Mersenne is a tökéletes számok kapcsán foglalkozott a fenti alakú prímekkel. 1644-ben előállt híressé vált listájával, miszerint 2^k-1 prím, ha $k=2,3,5,7,13,17,19,31,67,127$ és 257, de minden más 257-nél kisebb k esetén összetett.

A listát szemügyre véve azonnal feltűnik, hogy csak prím kitevők fordulnak elő. Ez nem véletlen, ugyanis ha k összetett, azaz $k=uv$, ahol $u,v>1$, akkor az $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\ldots+b^{n-1})$ azonosság alapján $2^k-1=(2^u)^v-1^v$ osztható 2^u-1-gyel, tehát 2^k-1 is összetett.

Az is világos, hogy kis k értékekre könnyen ellenőrizhető, hogy 2^k-1 prím vagy összetett, de akár már $2^{31}-1$ prím voltának igazolása is igen kemény számolást jelent, ha azt a „próbaosztásos" módszerrel végezzük, azaz végigszámoljuk, hogy nem osztható a négyzetgyökéig terjedő (1-nél nagyobb) egészek egyikével sem (illetve elég ezt csak a prímekre ellenőrizni, azonban ekkor az adott határig terjedő prímek ismeretére is szükség van). Maga Mersenne írja, hogy „ahhoz, hogy egy 15- vagy 20-jegyű számról megállapítsuk, prím-e vagy sem, egy egész élet ideje sem elég." Ezek után igazán meglepő, hogy (máig sem tisztázott meggondolások alapján) elő mert állni egy ilyen listával, és még meglepőbb, hogy amint közel 300(!) évvel később végleg tisztázódott, a lista mindössze öt hibát tartalmaz: $2^{67}-1$ és $2^{257}-1$ valójában összetett számok, ugyanakkor a hiányzó $2^{61}-1$, $2^{89}-1$ és $2^{107}-1$ prímek.

Rend a lelke mindennek

Természetesen Mersenne ismerhetett néhány olyan tételt, amelyek megkönnyítik egy $M_p=2^p-1$ alakú szám prímosztóinak a keresését, ahol p prím (az ilyen számokat nevezzük a továbbiakban Mersenne-számoknak). Az egyik ilyen tétel szerint ($p>2$-re) M_p minden prímosztója $2kp+1$, valamint egyben $8j\pm1$ alakú. Így például $M_{43}=2^{43}-1$ prímosztói egyszerre $86k+1$ és $8j\pm1$ alakúak, és a legkisebb ilyen prím, a 431 osztója is M_{43}-nak. Hasonlóan, M_{31} prím voltához elég csak azt ellenőrizni, hogy nem osztható a négyzetgyökénél kisebb $248t+1$ és $248t+63$ alakú prímek egyikével sem. Mindez esetleg magyarázatot adhat arra, hogy miért szerepel a listán a 31 kitevő, és miért nincs ott a 43 (de továbbra sem adhat támpontot a lista túlnyomó részének a megtippeléséhez).

Az alábbiakban bebizonyítjuk, hogy M_p minden prímosztója $2kp+1$ alakú. Ebben a *rend* fogalma lesz a segítségünkre.

Legyenek c és m relatív prímek, és vizsgáljuk meg, hogy a c hatványai, $1=c^0,c,c^2,c^3,\ldots,c^n,\ldots$ milyen maradékot adnak m-mel osztva. Mivel a maradékok száma véges, ezért lesz olyan $0\le i<j$, amelyre c^j és c^i azonos maradékot adnak, azaz $c^j-c^i=c^i(c^{j-i}-1)$ osztható m-mel. Ebből $(c;m)=1$ alapján következik, hogy $c^{j-i}-1$ is osztható m-mel,

azaz c^{j-i} maradéka 1. Legyen r a legkisebb pozitív egész, amelyre c^r maradéka 1. Ekkor $1 = c^0, c, c^2, c^3, \ldots, c^n, \ldots$ maradékai periodikus sorozatot alkotnak, amelyben a (legkisebb) periódus hossza éppen r. Ezt az r számot nevezzük a c szám rendjének modulo m, és $o_m(c)$-vel jelöljük és ordo m c-nek ejtjük.

Fel fogjuk még használni a kis Fermat-tételt, amely szerint a q prímmel osztva c^{q-1} maradéka 1, feltéve hogy c nem osztható q-val. Az előző bekezdés szerint így a c rendje osztója $(q-1)$-nek, azaz $o_q(c) \mid q-1$.

Legyen most q az $M_p = 2^p - 1$ Mersenne-szám egy prímosztója, ahol $p > 2$ prím. Ekkor 2^p maradéka q-val osztva 1. Ez azt jelenti, hogy $o_q(2) \mid p$. Mivel a p prím, és 2^1 maradéka nem 1, ezért $o_q(2)$ csak p lehet. Ebből az előző bekezdés alapján következik, hogy $p \mid q-1$, továbbá $q-1$ páros, ezért valóban $q = 2kp+1$ alakú.

A rend fogalmát és az iménti bizonyítást kényelmesebben megfogalmazhatjuk a kongruenciák segítségével. Itt $a \equiv b \pmod m$ azt jelenti, hogy a és b azonos maradékot adnak m-mel osztva, azaz $m \mid a-b$. A c rendje mod m a legkisebb olyan r pozitív egész, amelyre $c^r \equiv 1 \pmod m$. A kis Fermat-tétel szerint

$$c^{q-1} \equiv 1 \pmod q,$$

ha q prím és c nem osztható q-val, illetve $c^q \equiv c \pmod q$ bármely c esetén. A rendnek az említett periódushossz tulajdonsága azt fejezi ki, hogy

$$c^i \equiv c^j \pmod m \iff i \equiv j \pmod{o_m(c)}.$$

Azt, hogy M_p prímosztói egyben $8j \pm 1$ alakúak is, a másodfokú kongruenciák elméletével, az ún. Legendre-szimbólum segítségével lehet igazolni, lásd pl. a Freud–Gyarmati: Számelmélet c. egyetemi tankönyvben.

Az örökifjú teszt

Mersenne listájának helyességén az első rést 1876-ban ütötte *Edouard Lucas* egy egészen új eljárás segítségével, és lényegében ugyanezen az alapon keresi ma is a GIMPS több mint 200 000 számítógépből összekapcsolt hálózata az újabb és újabb Mersenne-prímeket. Ez a teszt az $a_1 = 4$, $a_{n+1} = a_n^2 - 2$ rekurzió alapján működik: Egy $p > 2$ prímet véve $M_p = 2^p - 1$ pontosan akkor prím, ha $M_p \mid a_{p-1}$.

Például $p = 7$-re $a_1 = 4$, $a_2 = 14$, $a_3 = 194 \equiv -60 \pmod{127}$, $a_4 \equiv 3598 \equiv 42 \pmod{127}$, $a_5 \equiv 1762 \equiv -16 \pmod{127}$, $a_6 \equiv 254 \equiv 0 \pmod{127}$, tehát $M_7 = 127$ prímszám.

A fenti példa természetesen csak illusztrációs jellegű, a módszer hatékonysága a nagyobb kitevők esetén érvényesül. Lucas ezzel bizonyította be 1876-ban, hogy M_{67} összetett, anélkül, hogy egy osztóját elő tudta volna állítani. M_{67}-et tényezőkre bontani csak jó negyedszázaddal később sikerült Cole-nak. Lucas azt is igazolta, hogy M_{127} valóban prím, és ez maradt a legnagyobb ismert prímszám a számítógépek megjelenéséig.

Amint az illusztrációs példából is kiderült, nem kell magukat az a_i számokat kiszámítani, elég mindig az M_p-vel való osztási maradékukat tekinteni. Az M_p-vel való maradékos osztás különösen egyszerűen hajtható végre a számítógépeken, ugyanis M_p kettes számrendszerbeli alakja csupa 1-esből áll. Így hasonló a helyzet ahhoz, mintha tízes számrendszerben mondjuk a 21 357 246 szám 999-cel való osztási maradékát keresnénk: mivel 10^3 és így 10^{3k} maradéka mindig 1, ezért $21\,357\,246 = 21 \cdot 10^6 + 357 \cdot 10^3 + 246 \equiv 21 + 357 + 246 \equiv 624 \pmod{999}$, azaz a maradékot számjegycsoportok egyszerű eltolásával kaphatjuk meg.

Kiruccanás más számkörbe

A teszt elégségességi részét igazoljuk az alábbiakban: *Ha*

$$M_p \mid a_{p-1}, \tag{1}$$

akkor M_p prím.

(A szükségesség igazolása hasonló eszközökkel történik, és alkalmazni kell a már említett Legendre-szimbólumot is.)

A bizonyításhoz az $a + b\sqrt{3}$ (a, b egész) alakú számok körében az egészek mintájára bevezetett oszthatóság, kongruencia és rendfogalom elemi tulajdonságait használjuk fel (ezek itt is ugyanúgy érvényesek, mint az egész számoknál).

Teljes indukcióval könnyen adódik, hogy $a_k = \left(2+\sqrt{3}\right)^{2^{k-1}} + \left(2-\sqrt{3}\right)^{2^{k-1}}$. Ennek alapján az (1) feltétel ekvivalens az

$$M_p \mid \left(2+\sqrt{3}\right)^{2^{p-2}} + \left(2-\sqrt{3}\right)^{2^{p-2}}$$

oszthatósággal. A jobb oldalt $\left(2+\sqrt{3}\right)^{2^{p-2}}$-vel szorozva $\left(2-\sqrt{3}\right)\left(2+\sqrt{3}\right) = 1$ miatt

$$M_p \mid \left(2+\sqrt{3}\right)^{2^{p-1}} + 1, \quad \text{azaz} \quad \left(2+\sqrt{3}\right)^{2^{p-1}} \equiv -1 \pmod{M_p} \tag{2}$$

adódik. M_p prím voltát (2)-ből fogjuk levezetni.

Szükségünk lesz a következő **lemmára:**

Ha $q > 3$ tetszőleges prímszám, akkor

$$\left(a + b\sqrt{3}\right)^q \equiv a + b\sqrt{3} \quad \text{vagy} \quad a - b\sqrt{3} \pmod{q}. \tag{3}$$

A lemma bizonyítása: A binomiális tétel alapján

$$\left(a + b\sqrt{3}\right)^q = a^q + \binom{q}{1} a^{q-1} b\sqrt{3} + \binom{q}{2} a^{q-2} 3b^2 + \ldots + b^q 3^{\frac{q-1}{2}}\sqrt{3}. \tag{4}$$

A kis Fermat-tétel szerint $a^q \equiv a \pmod{q}$ és $b^q \equiv b \pmod{q}$, továbbá q prím volta miatt $\binom{q}{1}, \binom{q}{2}, \ldots, \binom{q}{q-1}$ mindegyike osztható q-val. Végül ismét a kis Fermat-tétel alapján

$$q \,\Big|\, \left(3^{\frac{q-1}{2}}\right)^2 - 1 = \left(3^{\frac{q-1}{2}} - 1\right)\left(3^{\frac{q-1}{2}} + 1\right),$$

és mivel q prím, szükségképpen osztja az egyik tényezőt, azaz $3^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}$. Ezeket (4)-be beírva éppen (3), azaz a lemma állítása adódik.

Visszatérve a tételünk bizonyítására, tegyük fel, hogy (2) fennáll, és legyen q az M_p egy prímosztója (itt nyilván $q > 3$); azt kell igazolnunk, hogy $q = M_p$. Ekkor a (2)-beli kongruencia mod q is teljesül, azaz

$$\left(2 + \sqrt{3}\right)^{2^{p-1}} \equiv -1 \pmod{q}. \tag{5}$$

Ezt négyzetre emelve kapjuk, hogy

$$\left(2 + \sqrt{3}\right)^{2^p} \equiv 1 \pmod{q}. \tag{6}$$

(5)-ből és (6)-ból a rend tulajdonságai szerint következik, hogy $o_q\left(2+\sqrt{3}\right) \mid 2^p$, de $o_q\left(2+\sqrt{3}\right) \nmid 2^{p-1}$, azaz $o_q\left(2+\sqrt{3}\right) = 2^p$.

Másrészt (3) alapján $\left(2 + \sqrt{3}\right)^q \equiv 2 \pm \sqrt{3} \pmod{q}$. Ha itt a + előjel érvényes, akkor

$$\left(2 + \sqrt{3}\right)^{q-1} = \left(2 - \sqrt{3}\right)\left(2 + \sqrt{3}\right)^q \equiv \left(2 - \sqrt{3}\right)\left(2 + \sqrt{3}\right) = 1 \pmod{q},$$

és így $o_q\left(2 + \sqrt{3}\right) = 2^p \leq q - 1$, ami $q \leq M_p = 2^p - 1$ miatt lehetetlen.

Ha a − előjel érvényes, akkor hasonlóan adódik, hogy

$$\left(2 + \sqrt{3}\right)^{q+1} \equiv 1 \pmod{q},$$

tehát $o_q\left(2 + \sqrt{3}\right) = 2^p \leq q + 1$, ahonnan $q \leq M_p = 2^p - 1$ miatt kapjuk, hogy $q = M_p$, vagyis M_p prím.

Ki lesz a befutó?

Az EFF százezer dollárját jó eséllyel egy Mersenne-prímmel lehet majd megszerezni, bár egyre erősebb a konkurencia. A legnagyobb ismert prímek listáját 2004. január 17-én három Mersenne-prím vezeti, de a negyedik helyen a 2003. decemberében(!) talált $5359 \cdot 2^{5\,054\,502} + 1$ áll (a maga több mint másfél millió számjegyével). Az ilyen $r \cdot 2^k + 1$ alakú számok prím volta kis szerencsével szintén elég gyorsan kimutatható, ha r viszonylag kis páratlan szám. Emellett az ilyen típusú prímek valószínűleg sokkal sűrűbben fordulnak elő, mint a Mersenne-prímek, tehát nem kizárt, hogy előbb bukkannak ezek közül egy legalább tízmillió jegyűre, mint Mersenne-prímre. Ugyanakkor a Mersenne-prímek gyönyörűen kapcsolják össze több mint kétezer év matematikáját, elegendő munkát hagyva a következő kétezer évre is, és az igazi befutók talán azok lesznek, akik az eddigiekhez elméletileg is hozzá tudnak majd tenni egy keveset.