

A Mersenne- és a Fermat-számok története

TÓTH LÁSZLÓ, PTE

2005. november

1. Mersenne-számok

Tekintsük a $2^n - 1$ számokat, ahol $n \geq 1$. Melyek ezek közül a prímek ?

Az $1 \leq n \leq 8$ számokra:

$n = 1$: $2^1 - 1 = 1$ nem prím,

$n = 2$: $2^2 - 1 = 3$ prím,

$n = 3$: $2^3 - 1 = 7$ prím,

$n = 4$: $2^4 - 1 = 15$ nem prím,

$n = 5$: $2^5 - 1 = 31$ prím,

$n = 6$: $2^6 - 1 = 63$ nem prím,

$n = 7$: $2^7 - 1 = 127$ prím,

$n = 8$: $2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$ nem prím.

Ha n összetett, akkor $2^n - 1$ is összetett, mert igaz a következő

1.1. Állítás. Ha $n \geq 1$ és $2^n - 1$ prímszám, akkor n prímszám.

Bizonyítás. Ha n nem prím, akkor n felírható $n = ab$ alakban, ahol $a, b > 1$. Így $2^n - 1 = (2^a)^b - 1$ osztható $(2^a - 1)$ -gyel, és $a, b \geq 1$ miatt $2^a - 1 \neq 1$, $\frac{2^n - 1}{2^a - 1} \neq 1$, ami ellentmondás. \square

Ugyanakkor

$n = 11$: $2^{11} - 1 = 2047 = 23 \cdot 89$ nem prím,

tehát a fenti állítás megfordítása nem igaz.

Mersenne-számoknak nevezzük az $M_p = 2^p - 1$ alakú számokat, ahol p prím, az ilyen alakú prímszámok pedig a Mersenne-prímek.

MARIN MERSENNE (1588-1648) francia matematikus, minorita szerzetes volt, aki 1644-ben megadta az M_p prímek listáját, ahol $p \leq 257$. Szerinte $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ esetén kapunk M_p prímeket. De ez $p = 67, 257$ esetén nem igaz (!). Másrészt kimaradtak a $p = 61, 89, 107$ prímek, amelyekre M_p prímszám.



MARIN MERSENNE

Az $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$ prímeket már az ókorban ismerték, az M_{13}, M_{17}, M_{19} prímeket pedig P. A. CATALDI fedezte fel 1588-ban. LEONHARD EULER (1707-1783) nevéhez fűződik a következő Mersenne-prím, az M_{31} felfedezése 1750-ben, ez volt több mint 100 éven át a legnagyobb ismert prímszám.

1876-ban E. LUCAS (1842-1891) francia matematikus megállapította, hogy

$$M_{127} = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$$

prímszám, ennek 39 számjegye van.

A további M_p prímek, $p < 3000$, felfedezői (az első zárójelben M_p számjegyeinek száma):

- $p = 61$, (19), PERVUSIN (1883),
- $p = 89$, (27), FAUQUEMBERGUE és POWERS (1911),
- $p = 107$, (33), FAUQUEMBERGUE és POWERS (1914),
- $p = 521$, (157), LEHMER és ROBINSON (1952),
- $p = 607$, (183), LEHMER és ROBINSON (1952),
- $p = 1279$, (386), LEHMER és ROBINSON (1952),
- $p = 2203$, (664), LEHMER és ROBINSON (1952),
- $p = 2281$, (687), LEHMER és ROBINSON (1952).

Kezdetben papírral és ceruzával végezték a számításokat, később mechanikus számológépekkel, majd elektromos számológépekkel. Az egyre modernebb és nagyobb kapacitású elektronikus számítógépek használata lehetővé tette a kutatási határ kitolását.

Jelenleg 42 Mersenne-prím ismert. A 40-edik ilyen prímet MICHAEL SHAFER fedezte fel 2003. november 17-én, ez a $2^{20\,996\,011} - 1$ szám, amelynek 6 320 430 számjegye van. A 41-edik Mersenne-prím felfedezését JOSH FINDLEY jelentette be 2004. május 15-én, ez a $2^{24\,036\,583} - 1$ szám, amelynek több mint 1 millióval több számjegye van mint a 40-edik Mersenne-prímnél.

A 42-edik, a jelenlegi legnagyobb Mersenne-prím a

$$2^{25\,964\,951} - 1,$$

a bejelentés dátuma 2005. február 18, a felfedező MARTIN NOWAK, Németország. Ennek 7 816 230 számjegye van ! Ez utóbbi egyben a ma ismert legnagyobb prímszám. Mindhárom felfedezés nemzetközi csapatmunka során született, az 1996-ban létrehozott GIMPS (Great Internet Mersenne Prime Search) nevű projekt segítségével. A 42-edik Mersenne-prímhez több mint 50 nap számítás volt szükséges Nowak 2.4 GHz Pentium 4 gépén. Az ellenőrzést 5 nap alatt végezte el Tony Reix (Grenoble, Franciaország) egy 16 Itanium CPU Bull NovaScale 5000 HPC gép segítségével. Egy újabb ellenőrzést végzett Jeff Gilchrist (Elytra Enterprises Inc., Ottawa, Kanada), 15 nap alatt egy Compaq Alpha GS160 1.2 GHz CPU gépén.

Egy további GIMPS eredmény: 2004. szeptember 13-án jelentette be DAVID SYMCOX, hogy M_{971} -nek megtalálta egy 53 jegyű osztóját, ez volt a legkisebb összetett Mersenne-szám, amelynek nem volt ismert egy faktora sem.

A legújabb eredményekre vonatkozó további információk olvashatók például a következő helyeken:

(1) FREUD R., Százezer dolláros prímelek, KöMaL, 2004/2. szám, 72-77, lásd

<http://www.komal.hu/cikkek/2004-02/freud.h.shtml>

(2) a GIMPS lapja: <http://www.mersenne.org>

(3) <http://primes.utm.edu/mersenne>

Mindmáig nem tudjuk, hogy általában mely M_p számok a prímelek és nem tudjuk, hogy van-e végtelen sok Mersenne-féle prímszám.

Heurisztikusan levezethető, hogy az $M_p \leq x$ prímszámok száma aszimptotikusan

$$\frac{1}{\log 2} e^C \log \log x,$$

ahol C az Euler-állandó, de erre nincs pontos matematikai bizonyítás.

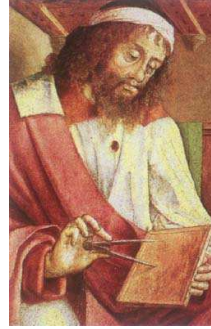
A Mersenne-prímelek kapcsolódnak a **tökéletes számok**hoz, maga Mersenne is a tökéletes számok kapcsán vizsgálta ezeket a prímeleket. Ez a fogalom PITHAGORÁSTól és tanítványaitól származik (K. e. 550 körül), akik tökéletesnek neveztek egy n számot, ha az "a részeiből előáll", tehát ha n egyenlő az önmagánál kisebb osztóinak összegével, azaz, ha $\sigma(n) = 2n$ a mai jelöléssel.

A legkisebb tökéletes számok az $n = 6, 28, 496, 8128$, ezeket már EUKLIDÉSZ (K. e. III. század) is ismerte, ő igazolta "Elemek" című, híres művében a következőt:

1.2. Állítás. Ha $2^k - 1$ prímszám, akkor $n = 2^{k-1}(2^k - 1)$ tökéletes szám.



PITHAGORÁSZ

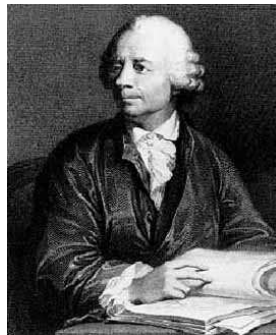


EUKLIDÉSZ

Eulertől származik a tétel megfordítása, aki mintegy 2000 évvel később igazolta:

1.3. Állítás. Ha n páros tökéletes szám, akkor $n = 2^{k-1}(2^k - 1)$ alakú, ahol $2^k - 1$ prímszám.

Bizonyítás. Legyen $n = 2^a m$, ahol $a \geq 1$ és m páratlan. Így $\sigma(n) = \sigma(2^a m) = \sigma(2^a)\sigma(m) = (2^{a+1} - 1)\sigma(m)$ és innen $\sigma(n) = 2n$ alapján $(2^{a+1} - 1)\sigma(m) = 2^{a+1}m$. Következik, hogy $2^{a+1} - 1 \mid 2^{a+1}m$, s mivel $(2^{a+1} - 1, 2^{a+1}) = 1$ kapjuk, hogy $2^{a+1} - 1 \mid m$, azaz $m = (2^{a+1} - 1)m_1$, amit visszahelyettesítve: $(2^{a+1} - 1)\sigma(m) = (2^{a+1} - 1)2^{a+1}m_1$, ahonnan $\sigma(m) = 2^{a+1}m_1$. Az m_1 és m osztói m -nek, $m_1 < m$ és $m_1 + m = m_1 + (2^{a+1} - 1)m_1 = 2^{a+1}m_1 = \sigma(m)$. Így m -nek m_1 -en és m -en kívül nincs más osztója, s kapjuk, hogy $m_1 = 1$ és $m = 2^{a+1} - 1$ prímszám. Tehát az $a = k - 1$ jelöléssel $n = 2^{k-1}(2^k - 1)$, ahol $2^k - 1$ prímszám. \square



LEONHARD EULER

Így n akkor és csak akkor páros tökéletes szám, ha $n = 2^{p-1}M_p$ alakú, ahol M_p Mersenne-prím. Nem tudjuk, hogy létezik-e végtelen sok Mersenne-féle prímszám, így azt sem tudjuk, hogy van-e végtelen sok tökéletes szám. Arra a kérdésre sem ismerjük a választ, hogy létezik-e páratlan tökéletes szám.

Milyen tulajdonságok alapján kereshetők meg az M_p számok prímtenyezői és dönthető el, hogy M_p prím vagy sem? A Mersenne-számok lehetséges prímfaktoraira vonatkoznak az alábbi eredmények. Az első tulajdonság azt mutatja, hogy M_p minden prímosztója $2kp + 1$ alakú és ugyanakkor $8m \pm 1$ alakú.

1.4. Állítás. Ha $p > 2$ prím és a q prímszám osztója az $M_p = 2^p - 1$ Mersenne-számnak, akkor $q \equiv 1 \pmod{2p}$ és $q \equiv \pm 1 \pmod{8}$.

Bizonyítás. Ha $q \mid M_p$, akkor $2^p \equiv 1 \pmod{q}$, ahonnan $o_q(2) \mid p$ (itt $o_q(2)$ a 2 rendje q -ra nézve), s mivel $o_q(2) \neq 1$, következik, hogy $o_q(2) = p \mid (q - 1)$ (a Fermat-tétel szerint). Ugyanakkor, $2 \mid (q - 1)$, tehát $2p \mid (q - 1)$.

Az $x = 2^{(p+1)/2}$ jelöléssel $x^2 - 2 = 2^{p+1} - 2 = 2M_p \equiv 0 \pmod{q}$, azaz $\left(\frac{2}{q}\right) = 1$, ahonnan $q \equiv \pm 1 \pmod{8}$. \square

Az $M_{11} = 2047$ szám esetén $q \equiv 1 \pmod{22}$ és $q \equiv \pm 1 \pmod{8}$, a legkisebb ilyen szám a 23 és $23|M_{11} = 23 \cdot 89$. Persze 89-re is teljesülnek a fenti kongruenciák.

1.5. Állítás. Legyen $p > 2$ olyan prím, melyre $q = 2p + 1$ is prím.

i) $q|M_p$ akkor és csak akkor, ha $q \equiv \pm 1 \pmod{8}$,

ii) $q|M_p + 2$ akkor és csak akkor, ha $q \equiv \pm 3 \pmod{8}$.

Bizonyítás. i) $q|M_p \Leftrightarrow M_p = 2^p - 1 = 2^{(q-1)/2} - 1 \equiv 0 \pmod{q} \Leftrightarrow 2^{(q-1)/2} \equiv 1 \pmod{q} \Leftrightarrow \left(\frac{2}{q}\right) \equiv 1 \pmod{q} \Leftrightarrow q \equiv \pm 1 \pmod{8}$. ii) $q|M_p + 2 \Leftrightarrow 2^{(q-1)/2} \equiv -1 \pmod{q} \Leftrightarrow \left(\frac{2}{q}\right) \equiv -1 \pmod{q} \Leftrightarrow q \equiv \pm 3 \pmod{8}$. \square

1.6. Állítás. Legyen $p \equiv 3 \pmod{4}$ olyan prím, amelyre $q = 2p + 1$ is prím. Akkor $q|M_p$ és $p > 3$ esetén M_p összetett.

Bizonyítás. Következik az előző Állításból: $p \equiv 3 \pmod{4}$ esetén $q \equiv -1 \pmod{8}$, ahonnan $q|M_p$. Ha $p > 3$, akkor $2p + 1 < 2^p - 1 = M_p$.

Innen azonnal adódik, hogy $p = 11, 23, 83, 131, 179, 191$ -re M_p összetett. Ha például $p = 19$, akkor $2p + 1 = 39$ nem prím, így nem teljesülnek az előbbi Állítás feltételei. Itt M_{19} osztói 191, 457, 647 lehetnek ($\sqrt{M_{19}} < 725$), s számolással ellenőrizhető, hogy egyik sem osztó, tehát $M_{19} = 524287$ prím.

Egy másik szükséges és elégséges feltétele annak, hogy M_p prím legyen, a következő. Lucas ezzel igazolta 1876-ban, hogy M_{127} prím és M_{67} összetett, anélkül, hogy ez utóbbinak valamely osztóját ismerte volna.

1.7. Állítás. (Lucas-Lehmer teszt) Legyen p prímszám és $(a_n)_{n \geq 1}$ a következő sorozat: $a_1 = 4, a_{n+1} = a_n^2 - 2, n \geq 1$. Az $M_p = 2^p - 1$ szám akkor és csak akkor prím, ha $M_p | a_{p-1}$.

Bizonyítás. A feltétel elégségességét igazoljuk a következő ötlettel (J. W. BRUCE, A really trivial proof of the Lucas-Lehmer test, Amer. Math. Monthly **100** (1993), no. 4, 370-371). Szükségünk van a következő elemi csoportelméleti tulajdonságra: Minden véges csoportban egy elem rendje kisebb vagy egyenlő mint a csoport rendje.

Legyen $\omega = 2 + \sqrt{3}, \bar{\omega} = 2 - \sqrt{3}$, ahol $\omega\bar{\omega} = 1$. Teljes indukcióval igazolható, hogy

$$a_n = \omega^{2^{n-1}} + \bar{\omega}^{2^{n-1}}$$

minden $n \geq 1$ -re. Ha $M_p | a_{p-1}$, akkor így $a_{p-1} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = kM_p, k \geq 1$, ahonnan $\omega^{2^{p-2}}$ -nel szorozva az

$$(1) \quad \omega^{2^{p-1}} = kM_p \omega^{2^{p-2}} - 1$$

egyenlőség következik. Négyzetreemelve:

$$(2) \quad \omega^{2^p} = \left(kM_p \omega^{2^{p-2}} - 1\right)^2.$$

Tegyük fel, hogy M_p összetett. Akkor M_p -nek létezik olyan q prímosztója, amelyre $q^2 \leq M_p$.

Tekintsük most az $A = \{a + b\sqrt{3} : a, b \in \mathbb{Z}_q\}$ halmazt, ahol \mathbb{Z}_q a maradékosztályok halmaza \pmod{q} . Ellenőrizhető, hogy $A \setminus \{0\}$ egy $(q^2 - 1)$ -edrendű kommutatív csoport a szorzásra nézve. Továbbá $\omega \in A \setminus \{0\}$ és (1) alapján $\omega^{2^{p-1}} = -1$, (2) szerint pedig $\omega^{2^p} = 1$, tehát ω rendje 2^p , s így $2^p \leq q^2 - 1$. Másrészt $q^2 - 1 \leq M_p - 1 < 2^p$, ami ellentmondás, tehát M_p prímszám. \square



E. LUCAS

2. Fermat-számok

Tekintsük a $2^k + 1$ számokat, ahol $k \geq 1$. Melyek ezek közül a prímek? Ha $1 \leq k \leq 8$, akkor:

- $k = 1$: $2^1 + 1 = 3$ **prím**,
- $k = 2$: $2^2 + 1 = 5$ **prím**,
- $k = 3$: $2^3 + 1 = 9$ nem prím,
- $k = 4$: $2^4 + 1 = 17$ **prím**,
- $k = 5$: $2^5 + 1 = 33$ nem prím,
- $k = 6$: $2^6 + 1 = 65$ nem prím,
- $k = 7$: $2^7 + 1 = 129$ nem prím,
- $k = 8$: $2^8 + 1 = 257$ **prím**.

Az $F_n = 2^{2^n} + 1$, $n \geq 0$ számokat **Fermat-számoknak**, az ilyen alakú prímeket pedig **Fermat-prímeknek** nevezzük. Igaz a következő

2.1. Állítás. Ha $k \geq 0$ és $2^k + 1$ prímszám, akkor létezik $n \geq 0$ úgy, hogy $k = 2^n$.

Bizonyítás. Ha $k = 2^n m$, ahol m páratlan, akkor $2^k + 1 = (2^{2^n})^m + 1$ osztható $2^{2^n} + 1$ -gyel, s így következik, hogy $2^{2^n} + 1 = 2^k + 1$, ahonnan $m = 1$. \square



PIERRE FERMAT

PIERRE FERMAT (1601-1665) francia matematikus és fizikus egy 1640-ben írott levelében azt sejtette, hogy az F_n számok mind prímek. Nos, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$ **prímek**, F_5 viszont nem prím, osztható 641-gyel:

$$F_5 = 641 \cdot 6\,700\,417,$$

ezt először Euler igazolta 1732-ben. Következik innen, hogy a fenti állítás fordítottja nem igaz.

A kongruenciatalajdonságok használatával igazoljuk mi is, hogy $641 | F_5 = 2^{2^5} + 1$. Valóban, $641 = 640 + 1 = 5 \cdot 2^7 + 1$, így $5 \cdot 2^7 \equiv -1 \pmod{641}$, s ezt negyedik hatványra emelve: $5^4 \cdot 2^{28} \equiv 1 \pmod{641}$. Másrészt, $641 = 625 + 16 = 5^4 + 2^4$, ahonnan $2^4 \equiv -5^4 \pmod{641}$. Összeszorozva ez utóbbi két kongruenciát $5^4 \cdot 2^{32} \equiv -5^4 \pmod{641}$, s osztva 5^4 -nel, ahol $(5^4, 641) = 1$, kapjuk, hogy $2^{32} + 1 = 2^{2^5} + 1 \equiv 0 \pmod{641}$.

1880-ban LANDRY megmutatta, hogy

$$F_6 = 274\,177 \cdot 67\,280\,421\,310\,721$$

összetett.

Mindmáig nem találtak további Fermat-prímet, az az újabb sejtés, hogy nem is létezik ilyen. Jelenleg 225 Fermat-számról tudjuk, hogy összetett.

Tudjuk, hogy F_n összetett és ismert F_n prímtényező felbontása $n = 5, 6, 7, 8$ -ra (2–2 prímtényező), $n = 9$ -re (3 prímtényező), $n = 10$ -re (4 prímtényező), $n = 11$ -re (5 prímtényező).

Tudjuk, hogy F_n összetett és ismert F_n legalább 1 prímfaktora, de nem ismert a teljes felbontása, ha $n = 12, 13, 15, 16, 17, 18, 19, 21, 23, 25, 26, 27, 28, 29, 30, 31, 32, 36, 37, 38, 39, 42, 43, \dots$. Tudjuk, hogy F_n összetett, de nem ismert F_n egyetlen prímfaktora sem, ha $n = 14, 20, 22, 24$. Nem tudjuk, hogy F_n összetett-e vagy sem $n = 33, 34, 35, 40, 41, 44, 45, 46, 47, 49, 50, \dots$ esetén.

További információk, eredmények olvashatók a Fermat-számokkal kapcsolatban itt:

(1) <http://www.fermatsearch.org>

(2) <http://www.prothsearch.net/fermat.html>

Három újabb eredmény:

JOHN COSGRAVE, 2003. október 10.: $3 \cdot 2^{2^{478} 785} + 1$ osztója $F_{2^{478} 782}$ -nek, ez a legnagyobb ismert összetett Fermat-szám,

M. PARCHER, 2005. május 15.: $2018719057 \cdot 2^{1162} + 1$ osztója F_{1160} -nak,

ASKO VUORI, 2005. szeptember 29.: $6213186413 \cdot 2^{605} + 1$ osztója F_{600} -nak.

A Fermat-prímek azért is érdekesek, mert CARL FRIEDRICH GAUSS (1777-1855) egy nevezetes eredménye szerint pontosan azok a szabályos n -szögek szerkeszthetők meg körzővel és vonalzóval, amelyekre n egyenlő 2 valamely hatványának és különböző Fermat-prímeknek a szorzatával.



CARL FRIEDRICH GAUSS

A Fermat-számok lehetséges prímfaktoraira vonatkozik az alábbi eredmény.

2.2. Állítás. (E. Lucas, 1877) Ha $n \geq 2$ és a p prímszám osztója az $F_n = 2^{2^n} + 1$ Fermat-számnak, akkor $p = 2^{n+2}k + 1$ alakú, ahol $k \geq 1$.

Bizonyítás. Ha $p|F_n$, akkor $2^{2^n} \equiv -1 \pmod{p}$, ahonnan négyzetreemeléssel $2^{2^{n+1}} \equiv 1 \pmod{p}$. Következik, hogy $o_p(2) = 2^{n+1}$ és $2^{n+1} | (p-1)$. Innen már megvan, hogy $p = 2^{n+1}q + 1$ alakú, de ennél többre van szükségünk.

Az $n \geq 2$ feltétel miatt $p \equiv 1 \pmod{8}$ és így ismert tétel alapján $\left(\frac{2}{p}\right) = 1$, tehát az $x^2 \equiv 2 \pmod{p}$ kongruenciának van egy $x = x_0$ megoldása és kapjuk, hogy $x_0^{2^{n+2}} \equiv 2^{2^{n+1}} \equiv 1 \pmod{p}$. Így $o_p(x_0) = 2^j$, ahol $j \leq n+2$. Megmutatjuk, hogy $j = n+2$. Valóban, $x_0^2 \equiv 2 \pmod{p}$ -t a 2^{j-1} -edik hatványra emelve: $1 \equiv 2^{2^{j-1}} \pmod{p}$, s mivel $o_p(2) = 2^{n+1}$, következik, hogy $j-1 \geq n+1$, $j \geq n+2$.

Azt nyertük, hogy $o_p(x_0) = 2^{n+2}$, innen $2^{n+2} | p-1$ és $p = 2^{n+2}k + 1$. \square

Ha $n = 5$, akkor kapjuk, hogy F_5 -nek a p prímosztói a $2^7k+1 = 128k+1 = 129, 257, 385, 513, 641, \dots$ számtani sorozatban keresendők. A felsorolt számok közül csak a $257 = F_3$ és a 641 prímek, s mivel $(F_3, F_5) = 1$, F_5 legkisebb lehetséges prímosztója a 641 , s számolással ellenőrizhető, hogy 641 valóban osztó: $F_5 = 641 \cdot 6700417$, lásd fennebb. Itt a hányados maga is prím és az előbbi állításnak megfelelően $2^7 \cdot 3 \cdot 17449 + 1$ alakú.

E. Lucas és I. Pervusin találták meg F_{12} -nek a $7 \cdot 2^{14} + 1$ prímosztóját, igazolva ezzel, hogy F_{12} összetett szám. Most a $d_k = 2^{14}k + 1$ sorozatot kell vizsgálni és $k = 7$ a legkisebb lehetséges érték, melyre d_k prím, hiszen $5|d_1, 3|d_2, 13|d_3, d_4 = F_4, 3|d_5, 5|d_6$.

Könnyen igazolható az az érdekes tulajdonság, amely szerint minden F_n , $n \geq 0$, Fermat-szám prím vagy pszeudoprím, azaz $2^{F_n} \equiv 2 \pmod{F_n}$ igaz minden n -re.

További irodalom

P. BUNDSCHUH, Einführung in die Zahlentheorie, Springer Verlag, Berlin Heidelberg New York, 1996.

ERDŐS P., SURÁNYI J., Válogatott fejezetek a számelméletből, Polygon, Szeged, 1996.

FREUD R., GYARMATI E., Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2000.