

Fermat kongruencia-tétele, pseudoprím számok

Dr. TÓTH LÁSZLÓ
Pécsi Tudományegyetem

2005. december 15.
Bolyai János születésének napja

1. Fermat kongruencia-tétele

A kínai matematikusok már K. e. 500 körül használták, hogy ha p prímszám, akkor p osztója $(2^p - 2)$ -nek. PIERRE FERMAT (1601-1665) francia matematikus és fizikus egy 1640. október 18-án FRENICLE DE BESSY-nek írt levelében közölte bizonyítás nélkül, hogy ha p prímszám és a egész szám, akkor p osztója $(a^p - a)$ -nak. Ezt a tulajdonságot nevezzük Fermat kongruencia-tételének, a továbbiakban röviden Fermat-tételnek, vagy „kis Fermat-tételnek” - megkülönböztetésül a „nagy Fermat-tételtől” (amely szerint az $x^n + y^n = z^n$ egyenletnek nincs $x, y, z \in \mathbb{Z} \setminus \{0\}$ megoldása, ha $n \in \mathbb{N}, n \geq 3$). Pontosabban,

1.1. FERMAT-tétel.

- i) Ha p prímszám és $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod{p}$, (1)
ii) Ha p prímszám, $a \in \mathbb{Z}$ és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$. (2)

Bizonyítás. Elég csak i)-et vagy ii)-t igazolni, mert ezek egymásból azonnal következnek. Ha pl. ii) igaz, akkor $p \nmid a$ esetén a (2) kongruenciát a -val szorozva éppen (1) adódik, ha pedig $p \mid a$, akkor $p \mid a^p$, így $p \mid (a^p - a)$, tehát az (1) kongruencia ekkor is igaz. Lássuk be, hogy fordítva, i)-ből is azonnali a ii).

A ii) állítást LEONHARD EULER (1707-1783, svájci) 1736-ban publikált kongruencia-tételéből szokás levezetni, amely szerint ha $(a, m) = 1$, akkor $a^{\phi(m)} \equiv 1 \pmod{m}$, ahol ϕ az Euler-függvény. Ha $m = p$ prím, akkor $\phi(p) = p - 1$ és ii)-t kapjuk.

Az i) állítás egy közvetlen igazolása: elegendő $a \geq 0$ -ra bizonyítani, Ha $a = 0$, akkor (1) igaz. Az a szerinti indukcióval tegyük fel, hogy (1) igaz a -ra, akkor

$$(a + 1)^p = \sum_{k=0}^p \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 \pmod{p},$$

használva, hogy p osztója $\binom{p}{k}$ -nak, ahol $1 \leq k \leq p - 1$ (ez igaz, mert $k! \binom{p}{k} = p(p-1) \cdots (p-k+1)$ és ennek p osztója, de p nem osztója $k!$ -nak). \square

Megjegyzés. Az első ismert bizonyítás WILHELM GOTTFRIED LEIBNIZ (1646-1716, német) egy publikálatlan, 1683 előtti kéziratában található, és a polinomiális-tételt használja:

$$(x_1 + \cdots + x_a)^p = \sum_{k_1 + \cdots + k_a = p} \frac{p!}{k_1! \cdots k_a!} x_1^{k_1} \cdots x_a^{k_a},$$

ahol az összegzés mindazon $k_1, \dots, k_a \geq 0$ egészek szerint történik, amelyek összege p . Ha most $x_1 = \dots = x_a = 1$, akkor a jobb oldalon p osztója minden tagnak, kivéve azt az a számú tagot, amelyekben k_1, \dots, k_a egyike p és a többi 0 (Forrás: [B96], 97. old). \square

1.2. Állítás. Ha az $m \geq 2$ egész számhoz létezik olyan a egész szám, hogy $a^m \not\equiv a \pmod{m}$, akkor m összetett szám.

Bizonyítás. Azonnali a Fermat-tétel alapján. \square



PIERRE FERMAT

Ez alkalmas annak igazolására, hogy egy konkrét (nagy) szám összetett. Például ezt használva mutatta meg G.A. PAXSON 1961-ben, hogy az $F_{13} = 2^{2^{13}} + 1$ Fermat-szám összetett, igazolva, hogy $3^{F_{13}} \not\equiv 3 \pmod{F_{13}}$ (Math. Comp. **15** (1961), 420, forrás: [B96], 100. old).

A Fermat-tétel fordítottja nem igaz. Pontosabban,

1.3. Állítás. a) Léteznek olyan $m \geq 2$ összetett számok, amelyekre $a^m \equiv a \pmod{m}$ valamely a egész számra.

b) Léteznek olyan $m \geq 2$ összetett számok, amelyekre $a^m \equiv a \pmod{m}$ minden a egész számra.

Bizonyítás. a) Ha például $a = 2$ és $n = 341 = 11 \cdot 31$, akkor $2^{341} \equiv 2 \pmod{341}$. Valóban, $2^{10} = 1024 \equiv 1 \pmod{11}$, közvetlen számítással vagy a Fermat-tétel alapján, ahonnan $2^{340} \equiv 1 \pmod{11}$. Továbbá, $2^{10} = 1024 \equiv 1 \pmod{31}$, $2^{340} \equiv 1 \pmod{31}$ és kapjuk, hogy $2^{340} \equiv 1 \pmod{11 \cdot 31}$, tehát $2^{341} \equiv 2 \pmod{341}$.

b) A legkisebb m szám, amelyre ez igaz az $561 = 3 \cdot 11 \cdot 17$. Igazoljuk, hogy $a^{561} \equiv a \pmod{561}$ minden a egész számra! \square

A Fermat-tétel egy lehetséges megfordítása a következő, amelyet E. LUCAS igazolt 1878-ban (Amer. J. Math. **1** (1878), 302, forrás: [HW85], 81. old).

1.4. LUCAS-tétel. Legyen $m \geq 2$ egy egész szám. Ha létezik olyan a egész szám, amelyre $a^{m-1} \equiv 1 \pmod{m}$ és $a^x \not\equiv 1 \pmod{m}$ az $m-1$ minden $x < m-1$ osztójára, akkor m prímszám.

Bizonyítás. Az elem rendje fogalmának és tulajdonságainak használatával: Legyen d az a elem rendje \pmod{m} . Akkor $a^d \equiv 1 \pmod{m}$, $d \mid (m-1)$ és $d \mid \phi(m)$. A feltétel szerint következik, hogy $d = m-1$. Így $m-1 = d \leq \phi(m) \leq m-1$, innen $\phi(m) = m-1$ és következik, hogy m prím. Megjegyezzük, hogy itt a primitív gyök \pmod{m} .

Az elem rendje fogalmát nem használva: Legyen E azoknak az $e \geq 1$ kitevőknek a halmaza, amelyekre $a^e \equiv 1 \pmod{m}$. Akkor $m-1 \in E$ és $x \notin E$ az $m-1$ minden $x < m-1$ osztójára. Legyen e_0 az E legkisebb pozitív eleme, akkor $m-1 = e_0q + r$, ahol $0 \leq r < e_0$. Továbbá $r = m-1 - e_0q \in E$, mert $a^r = a^{m-1} \cdot a^{-e_0q} \equiv 1 \pmod{m}$. Nem lehet $r > 0$, mert ez ellentmondana az e_0 minimalitásának, ezért $r = 0$ és így $e_0 \mid m-1$. De a feltétel szerint innen $e_0 = m-1$, azaz $E = \{m-1\}$. Az $a^{m-1} \equiv 1 \pmod{m}$ feltétel miatt $(a, m) = 1$ teljesül és az Euler-tételt használva $a^{\phi(m)} \equiv 1 \pmod{m}$, azaz $\phi(m) \in E$, tehát $\phi(m) = m-1$ és következik, hogy m prím. \square



D. H. LEHMER

Az 1.4. Tétel feltétei módosíthatók. Igazoljuk a következő, DERRICK HENRY LEHMERTŐL (1905-1991, amerikai) származó állítást (lásd [M97], 170. old.) !

1.5. LEHMER-tétel. Legyen $m \geq 3$ egy egész szám, $m-1 = \prod_{j=1}^r q_j^{a_j}$, ahol $a_j \geq 1$ és a q_j -k különböző prímszámok, $1 \leq j \leq r$. Ha létezik olyan a egész szám, amelyre $a^{(m-1)/q_j} \not\equiv 1 \pmod{m}$, ahol $1 \leq j \leq r$ és $a^{m-1} \equiv 1 \pmod{m}$, akkor m prímszám. \square

2. Pszeudoprímszámok

Ha $n \geq 1$ összetett szám és $2^n \equiv 2 \pmod{n}$, akkor n számot **2-alapú Fermat-pszeudoprímnek**, röviden **pszeudoprímnek** (vagy **álprímnek**) nevezzük. A legkisebb ilyen pszeudoprímszám az 1.3. Állítás kapcsán vizsgált $341 = 11 \cdot 31$, további pszeudoprímek:

$561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$, $1105 = 5 \cdot 13 \cdot 17$, $1387 = 19 \cdot 73$, $1729 = 7 \cdot 13 \cdot 19$, valamint 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 10585, 11305, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 16705, 18705, 18721, 19951, 23001, 23377, 25761, 29341,...

D.H. LEHMER [Le36] 1936-ban és P. POULET [Po38] 1938-ban meghatározták az összes $n \leq 10^8$ pszeudoprímet.

2.1. Állítás. Végtelen sok pszeudoprímszám létezik.

Bizonyítás. Igazoljuk, hogy ha n pszeudoprím, akkor $2^n - 1$ is pszeudoprím. Valóban, ha n összetett, akkor $2^n - 1$ is összetett (ez ismert elemi tulajdonság) és $2^n \equiv 2 \pmod{n}$ alapján

$2^n - 2 = nq$, ahonnan $2^{2^n-1} - 2 = 2(2^{2^n-2} - 1) = 2(2^{nq} - 1) = 2((2^n)^q - 1)$ osztható $(2^n - 1)$ -gyel.

Tekintsük az $(a_n)_{n \geq 1}$, $a_1 = 341$, $a_{n+1} = 2^{a_n} - 1$, $n \geq 1$ szigorúan növekvő számsorozatot, ennek minden tagja pszeudoprím szám a fentiek szerint. \square

2.2. Állítás. (ERDŐS PÁL) Ha $p > 3$ prím, akkor $E_p = \frac{1}{3}(2^{2p} - 1)$ pszeudoprím.

Bizonyítás. $E_p = \frac{1}{3}(2^p + 1)(2^p - 1)$ összetett, ahol $3 \mid 2^p + 1$, mert p páratlan. A Fermat-tétel szerint $p \mid (4^p - 4)$, ugyanakkor $2 \mid (4^p - 4)$, innen $2p \mid \frac{1}{3}(4^p - 4)$, mert $p > 3$. Kapjuk, hogy $\frac{1}{3}(4^p - 4) = 2pk$ és így

$$2^{E_p} - 2 = 2(2^{E_p-1} - 1) = 2(2^{(4^p-4)/3} - 1) = 2(2^{2pk} - 1) = 2(4^{pk} - 1),$$

ami osztható $(4^p - 1)$ -gyel és így $\frac{1}{3}(4^p - 1) = E_p$ -vel is. \square

Ha pl. $p = 5$, akkor $E_5 = 341$, ha $p = 7$, akkor $E_7 = 5461 = 43 \cdot 127$, stb.

Mivel végtelen sok prím van, a 2.2. Állítás újabb bizonyítása annak, hogy végtelen sok pszeudoprím szám létezik.

2.3. Állítás. Minden $F_n = 2^{2^n} + 1$, $n \geq 0$, Fermat-szám prím vagy pszeudoprím.

Bizonyítás. $2^{2^n} \equiv -1 \pmod{F_n}$, amit 2^{2^n-n} -hatványra emelve: $2^{2^n} \equiv 1 \pmod{F_n}$, azaz $2^{F_n} \equiv 2 \pmod{F_n}$. \square

Az első páros pszeudoprímet D. H. LEHMER találta meg 1950-ben, ez a szám a $161\,038 = 2 \cdot 73 \cdot 1103$ (forrás: [S64], 215. old). N. G. W. H. BEEGER (1951) igazolta, hogy végtelen sok páros pszeudoprím van.

10^{11} -ig 38 975 páratlan pszeudoprím van, 10^{12} -ig 101 629, 10^{13} -ig 264 239 páratlan pszeudoprím.

Pl. a 10^{12} alatti páratlan pszeudoprímek listáját lásd itt:

<http://www.chalcedon.demon.co.uk/rgep/psp-12.gz>

Az $n \geq 1$ számot **a -alapú Fermat-pszeudoprímnek**, röviden **a -alapú pszeudoprímnek** nevezzük, ha n összetett és $a^n \equiv a \pmod{n}$.

A 2-alapú pszeudoprímek tehát a pszeudoprímek, 3-alapú pszeudoprímek pl. a következők: 91, 121, 286, 561, 671, 703, Valóban, pl. $3^{91} \equiv 3 \pmod{91}$, mert $91 = 7 \cdot 13$, $3^6 \equiv 1 \pmod{7}$ a Fermat-tétel szerint, innen $3^{6 \cdot 15} = 3^{90} \equiv 1 \pmod{7}$, $3^{91} \equiv 3 \pmod{7}$, továbbá hasonlóan $3^{12} \equiv 1 \pmod{13}$, $3^{84} \equiv 1 \pmod{13}$, innen $3^{91} = 3^{84} \cdot (3^3)^2 \cdot 3 \equiv 3 \pmod{13}$.

Megjegyzés. Szokásos a következő definíció is: az $n \geq 1$ számot a -alapú pszeudoprímnek (vagy a -alapú álprímnek) nevezzük, ha n összetett és $a^{n-1} \equiv 1 \pmod{n}$. Ekkor szükségképpen $(a, n) = 1$. Ezen definíció szerint tehát a (2-alapú) pszeudoprímek páratlanok, a 3-alapú pszeudoprímeknek 3 nem osztója, így pl. 561 nem ilyen, stb.

A következő tétel M. CIPOLLA eredménye (Annali Mat. Pura Appl. (3) **9** (1903), 139-160), lásd [HW85], Th. 89.

2.4. Tétel. (M. CIPOLLA) Minden $a > 1$ esetén létezik végtelen sok a -alapú pszeudoprím.

Bizonyítás. Legyen $p > 2$ prím, $p \nmid a(a^2 - 1)$ és $m = \frac{a^{2p}-1}{a^2-1}$. Igazoljuk, hogy m a -alapú pszeudoprím. Itt

$$m = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1},$$

amely összetett szám. Továbbá,

$$(*) \quad (a^2 - 1)(m - 1) = a^{2p} - 1 - (a^2 - 1) = a^{2p} - a^2 = a(a^{p-1} - 1)(a^p + a)$$

Itt $2 \mid (a^p + a)$, mert a és a^p egyszerre páros vagy páratlan, $p \mid (a^{p-1} - 1)$ (Fermat-tétel) és $(a^2 - 1) \mid (a^{p-1} - 1)$ mert $p - 1$ páros. Ezért $p \nmid (a^2 - 1)$ miatt (*) alapján $2p(a^2 - 1) \mid (a^2 - 1)(m - 1)$, innen $2p \mid (m - 1)$, tehát $m = 1 + 2pu$ alakú, ahol u egész. Használva újra (*)-ot:

$$a^{2p} = (a^2 - 1)(m - 1) + a^2 \equiv -a^2 + 1 + a^2 \equiv 1 \pmod{m},$$

$a^{m-1} = a^{2pu} \equiv 1 \pmod{m}$. Különböző p prímeke különböző m -eket kapunk, ezért végtelen sok ilyen m van. \square

Az $n \geq 1$ számot **abszolút pszeudoprímnek** nevezzük, ha n összetett és ha az $a^n \equiv a \pmod{n}$ kongruencia igaz minden $a \in \mathbb{Z}$ számra. A 341 nem abszolút pszeudoprím, hiszen $11^{341} \not\equiv 11 \pmod{341}$. Valóban, a Fermat tétel szerint $11^{30} \equiv 1 \pmod{31}$, s innen $11^{330} \equiv 1 \pmod{31}$. Ugyanakkor, $11^2 \equiv -3 \pmod{31}$, $11^{10} \equiv (-3)^5 \equiv -243 \equiv 5 \pmod{31}$. Így $11^{11} \equiv 55 \equiv -7 \pmod{31}$. Kapjuk, hogy $11^{341} = 11^{330} \cdot 11^{11} \equiv -7 \pmod{31}$, $11^{341} - 11 \equiv -18 \pmod{31}$. 31 tehát nem osztója a $11^{341} - 11$ számnak, s így 341 sem osztója annak.

A legkisebb abszolút pszeudoprímszám az $561 = 3 \cdot 11 \cdot 17$. Hogy valóban az, következik az alábbi egyszerű tulajdonságból:

2.5. Állítás. Az n szám akkor és csak akkor abszolút pszeudoprím, ha

- 1) $n = q_1 q_2 \cdots q_k$, ahol $k \geq 3$, q_i különböző prímszámok, és
- 2) $(q_i - 1) \mid (n - 1)$, $1 \leq i \leq k$.

Bizonyítás. Tegyük fel, hogy n -re teljesül az 1) és 2) tulajdonság. A Fermat-tétel szerint, ha $q_i \nmid a$, akkor $a^{q_i-1} \equiv 1 \pmod{q_i}$, ahonnan $a^{n-1} = a^{k_i(q_i-1)} \equiv 1 \pmod{q_i}$ és innen $a^n \equiv a \pmod{q_i}$, amely kongruencia igaz akkor is, ha $q_i \mid a$, $1 \leq i \leq k$. Innen $a^n \equiv a \pmod{n}$ minden a számra.

Fordítva, tegyük fel, hogy n abszolút pszeudoprím és $q \mid n$, ahol q prím. Ha $q^2 \mid n$, akkor használva, hogy $n \mid (q^n - q)$ kapjuk, hogy $q^2 \mid (q^n - q)$, ahonnan $q^2 \mid q$, ami lehetetlen. Tehát n négyzetmentes kell legyen. Továbbá, legyen $q \mid n$, q prím és a egy primitív gyök \pmod{q} , ahol $(a, q) = 1$. Akkor a rendje $q - 1$, ugyanakkor $a^{n-1} \equiv 1 \pmod{q}$ és kapjuk, hogy $(q - 1) \mid (n - 1)$. Itt n összetett, ezért $k \geq 2$. Ha $k = 2$, akkor $n = q_1 q_2$ és következik, hogy $q_1 - 1 \mid q_1 q_2 - 1 = q_1(q_2 - 1) + (q_1 - 1)$, innen $q_1 - 1 \mid q_2 - 1$, ugyanakkor $q_2 - 1 \mid q_1 q_2 - 1 = q_2(q_1 - 1) + (q_2 - 1)$, ahonnan $q_2 - 1 \mid q_1 - 1$ és így $q_1 - 1 = q_2 - 1$, $q_1 = q_2$, ellentmondás. Ezért $k \geq 3$. \square

További abszolút pszeudoprímszámok:

$$1105 = 5 \cdot 13 \cdot 17, \quad 1729 = 7 \cdot 13 \cdot 19, \quad 2465 = 5 \cdot 17 \cdot 29, \quad 2821 = 7 \cdot 13 \cdot 31,$$

$$15\,841 = 7 \cdot 31 \cdot 73, \quad 16\,046\,641 = 13 \cdot 37 \cdot 73 \cdot 457,$$

könnyen ellenőrizhető, hogy teljesülnek a 2.5. Állítás tulajdonságai.

Léteznek olyan képletek, amelyek ilyen számokat szolgáltatnak. Ezek közül a legegyszerűbb:

2.6. Állítás. (J. CHERNICK [Ch39], 1939) Ha $p = 6m + 1$, $q = 12m + 1$ és $r = 18m + 1$ egyidőben prímekek, akkor $n = pqr$ abszolút pszeudoprímszám.

Bizonyítás. Valóban az $n = pqr$ számra teljesülnek a 2.5. Állítás feltételei. \square

Ha pl. $m = 1, 6, 35$, akkor az $n = 7 \cdot 13 \cdot 19$, $37 \cdot 73 \cdot 109$, $211 \cdot 421 \cdot 621$ abszolút pszeudoprímeket kapjuk. Nem tudjuk, hogy létezik-e végtelen sok olyan m , amelyre $p = 6m + 1$, $q = 12m + 1$ és $r = 18m + 1$ egyidőben prímekek, ezért ilyen úton nem igazolható, hogy végtelen sok abszolút pszeudoprím van.

Az n számot **Carmichael-számnak** nevezzük, ha n összetett és ha $a^{n-1} \equiv 1 \pmod{n}$ minden $a \in \mathbb{Z}$, $(a, n) = 1$ számra. Azonnali, hogy minden abszolút pszeudoprímszám Carmichael-szám. Valóban, ha $a^n \equiv a \pmod{n}$ és ha $(a, n) = 1$, akkor következik, hogy $a^{n-1} \equiv 1 \pmod{n}$. Igaz fordítva is, ha n Carmichael-szám, akkor n abszolút pszeudoprím, lásd a 2.8. Állítást.

ROBERT DANIEL CARMICHAEL (1879-1967) amerikai matematikus volt, aki a [Ca10] és [Ca12] dolgozataiban megadott 16 ilyen számot, köztük a felsoroltakat. További nagy számú abszolút pszeudoprímet határozott meg POULET 1938-ban ([Po38]).

A Carmichael-szám elnevezést BEEGER [Be50] használta először 1950-ben. A legkisebb 20 prímtevezős Carmichael-szám:

$$n = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot 73 \cdot 97 \cdot 101 \cdot 109 \cdot 113 \cdot 151 \cdot 181 \cdot 193 \cdot 641,$$

amelyet R. G. E. PINCH [Pi93] adott meg 1993-ban.

10¹⁶-ig 246 683 számú Carmichael-szám van, ezek listáját lásd itt:

<http://www.chalcedon.demon.co.uk/rgep/carmichael-16.gz>

Azt, hogy végtelen sok Carmichael-szám (abszolút pszeudoprím szám) létezik 1992-ben sikerült igazolni, a dolgozat 1994-ben jelent meg.

2.7. Tétel. (R. ALFORD, A. GRANVILLE, C. POMERANCE [AGP94]) A Carmichael-számok száma x -ig több mint $x^{2/7}$, ha x elég nagy, tehát végtelen sok Carmichael-szám létezik.

Egy, a Carmichael-számok meghatározására szolgáló új algoritmus leírás szerepel az [LN96] cikkben, amellyel a szerzők 1 101 518 számú prímfaktort tartalmazó Carmichael-számokat is meghatároznak.

2.8. Állítás. Ha n összetett szám, akkor egyenértékűek a következő feltételek:

- 1) n Carmichael-szám, azaz $a^{n-1} \equiv 1 \pmod{n}$ minden $a \in \mathbb{Z}$, $(a, n) = 1$ számra,
- 2) n négyzetmentes és n minden p prímosztójára $p - 1 \mid n - 1$,
- 3) n abszolút pszeudoprím, azaz $a^n \equiv a \pmod{n}$ minden $a \in \mathbb{Z}$ számra.

Bizonyítás. 1) \Rightarrow 2) (Lásd [FGy2000], 5.7.7 feladat megoldása, 549. old.) Tegyük fel, hogy n Carmichael-szám. Ha n nem négyzetmentes, akkor létezik olyan q prím, amelyre $q^2 \mid n$. Legyenek n különböző prímosztói $q = q_1, q_2, \dots, q_k$ és legyen g egy primitív gyök $(\text{mod } q^2)$. Tekintsük a következő kongruenciarendszert: $x \equiv g \pmod{q^2}$, $x \equiv 1 \pmod{q_i}$, $2 \leq i \leq k$, amelynek a kínai maradéktétel szerint van $x = x_0$ megoldása (ha $k = 1$, legyen $x_0 = g$). Akkor $(x_0, q_i) = 1$ minden $1 \leq i \leq k$ esetén (ha $q_1 = q \mid x_0$, akkor $q \mid g$, ellentmondás), ezért $(x_0, n) = 1$. A feltétel alapján így $x_0^{n-1} \equiv 1 \pmod{n}$, innen $q^2 \mid n$ miatt $x_0^{n-1} \equiv 1 \pmod{q^2}$ és $g^{n-1} \equiv 1 \pmod{q^2}$. Következik, hogy g rendje $(\text{mod } q^2)$ osztója $(n-1)$ -nek, azaz $\phi(q^2) = q(q-1) \mid n-1$. De $q^2 \mid n$, innen $q \mid (n, n-1) = 1$, ellentmondás. Ezzel beláttuk, hogy n négyzetmentes.

Ha most q prím, $q \mid n$, akkor legyen h olyan primitív gyök $(\text{mod } q)$, amelyre $(h, n) = 1$. Ilyen h létezik. Valóban, legyen j egy tetszőleges primitív gyök $(\text{mod } q)$ és az $n = qq_2 \cdots q_k$ jelöléssel tekintsük a fentihez hasonló $x \equiv j \pmod{q}$, $x \equiv 1 \pmod{q_i}$, $2 \leq i \leq k$ rendszert, amelynek a kínai maradéktétel szerint van $x = h$ megoldása. Akkor $h \equiv j \pmod{q}$ szerint h primitív gyök $(\text{mod } q)$ és $(h, q_i) = 1$ minden $1 \leq i \leq k$ esetén, azaz $(h, n) = 1$. A feltétel (n Carmichael-szám) alapján $h^{n-1} \equiv 1 \pmod{n}$, innen $h^{n-1} \equiv 1 \pmod{q}$ és így h rendje $(\text{mod } q)$ osztója $(n-1)$ -nek, azaz $q-1 \mid n-1$.

2) \Rightarrow 3) Ezt már láttuk a 2.5. Állításban.

3) \Rightarrow 1) Azonnali, ezt is láttuk. \square

A Carmichael-számoknak a 2) feltétellel való jellemzése A. KORSELT-től származik 1899-ből ([Ko99]), aki nem adott meg egy ilyen számot sem.

D. H. LEHMER egyik problémája (Lehmer's totient problem) arra vonatkozik, hogy létezik-e olyan n összetett szám, amelyre $\phi(n) \mid (n-1)$, ahol ϕ az Euler-függvény. Nem ismert ilyen szám. De egy ilyen n szükségképpen Carmichael-szám, mert minden a egészre a rendje $(\text{mod } n)$ osztója $\phi(n)$ -nek és innen $a^{n-1} \equiv 1 \pmod{n}$.



BOLYAI JÁNOS

Nemrég derült ki KISS ELEMÉR kutatásai nyomán, hogy BOLYAI JÁNOS (1802-1860), akinek eddig csak geometriai munkássága volt közismert, számelmélettel is foglalkozott, vizsgálta pl. a Fermat-tétel fordított állítását, a Fermat-számokat, ismerte a pszeudoprím (álprím) fogalmát és néhány tulajdonságát, több olyan eredménye is van, amit nem publikált és amit később mások újra felfedeztek, lásd pl. KISS ELEMÉR, "Bolyai János kéziratának rejtett matematikai kincsei" című dolgozatát: <http://www.kfki.hu/chemonet/TermVil/kulonsz/k983/kiss.html> és a [K95] cikket.

3. A Carmichael-függvény

Ha n rögzített, jelölje $\lambda(n)$ a legkisebb olyan k pozitív egész számot, amelyre $a^k \equiv 1 \pmod{n}$ minden $(a, n) = 1$ esetén. A $\lambda(n)$ függvényt **Carmichael-függvénynek** nevezzük, ezt R.

D. CARMICHAEL vezette be és vizsgálta a róla elnevezett számokkal kapcsolatban. Használatos a **legkisebb univerzális exponens (kitevő)** elnevezés is. A $\lambda(n)$ érték nem más, mint a redukált maradékosztályok $R_n = U(\mathbb{Z}_n)$ multiplikatív csoportjának az exponense. Általánosan egy (G, \cdot) véges csoport exponense a legkisebb olyan k pozitív egész szám, amelyre $x^k = 1$ minden $x \in G$ -re.

Megjegyezzük, hogy ezt a függvényt korábban már KARL FRIEDRICH GAUSS (1777-1855, német) is vizsgálta az 1801-ben megjelent "Disquisitiones arithmeticae" (Aritmetikai vizsgálatok) című művében (Article 92).

Azonnali, hogy $\lambda(n) \leq \phi(n)$, pontosabban $\lambda(n) \mid \phi(n)$ minden n -re, ahol $\phi(n)$ az Euler-függvény.

3.1. Állítás.

$$\lambda(n) = \begin{cases} \phi(n), & \text{ha } n = p^a, \text{ ahol } p = 2 \text{ és } a \leq 2, \text{ vagy } p \geq 3 \text{ és } a \geq 1, \\ \frac{1}{2}\phi(n), & \text{ha } n = 2^a, \text{ ahol } a \geq 3, \\ [\lambda(p_1^{a_1}), \dots, \lambda(p_r^{a_r})], & \text{ha } n = p_1^{a_1} \cdots p_r^{a_r}, \end{cases}$$

ahol $[x_1, \dots, x_r]$ az x_1, \dots, x_r legkisebb közös többszöröse.

Bizonyítás. Ha $n = 2$, $n = 4$, vagy $n = p^a$, ahol $a \geq 1$, akkor létezik primitív gyök (mod n), amelynek rendje $\phi(n)$ és azonnali, hogy ekkor $\lambda(n) = \phi(n)$.

Ha $n = 2^a$, ahol $a \geq 3$, akkor nem létezik primitív gyök (mod n), ezért $\lambda(2^a) \neq \phi(2^a) = 2^{a-1}$ és $\lambda(2^a) \mid \phi(2^a) = 2^{a-1}$, tehát $\lambda(2^a) = 2^j$, ahol $j \leq a - 2$. Megmutatjuk, hogy $j = a - 2$.

Ehhez elég igazolni, hogy az 5 rendje (mod 2^a) éppen 2^{a-2} : $o_{2^a}(5) = 2^{a-2}$, ahol $a \geq 3$.

Határozzuk meg 2 kitevőjét $5^{2^k} - 1$ kanonikus alakjában. Ha $k = 0$: $5^{2^0} - 1 = 4 = 2^2$; ha $k = 1$: $5^{2^1} - 1 = 24 = 2^3 \cdot 3$; ha $k = 2$: $5^{2^2} - 1 = 624 = 2^4 \cdot 39$. Így a sejtés az, hogy a kitevő $k + 2$. Ez bizonyítható indukcióval, vagy a következőképpen: ha $k \geq 1$, akkor

$$\prod_{j=0}^{k-1} (5^{2^j} + 1) = \prod_{j=0}^{k-1} \frac{5^{2^{j+1}} - 1}{5^{2^j} - 1} = \frac{5^{2^k} - 1}{5^{2^0} - 1},$$

ahonnan

$$5^{2^k} - 1 = 2^2 \prod_{j=0}^{k-1} (5^{2^j} + 1),$$

ahol $5^{2^j} + 1 \equiv 2 \pmod{4}$, így $2^{k+2} \mid 5^{2^k} - 1$ és $2^{k+3} \nmid 5^{2^k} - 1$. A kitevő tehát valóban $k + 2$ és így $5^{2^{k-2}} \equiv 1 \pmod{2^k}$, $5^{2^{k-3}} \not\equiv 1 \pmod{2^k}$. Kapjuk, hogy $j = a - 2$ és $o_{2^a}(5) = 2^{a-2}$.

Ha n -nek több prímosztója van, akkor a képlet a definícióból adódik. \square

Következik, hogy $\lambda(n)$ nem multiplikatív függvény.

3.2. Állítás. (CARMICHAEL) Az n szám akkor és csak akkor Carmichael-szám (abszolút pseuodoprím), ha $\lambda(n) \mid n - 1$.

Bizonyítás. Ha $\lambda(n) \mid n - 1$, akkor $a^{n-1} \equiv a^{\lambda(n)k} \equiv 1 \pmod{n}$ minden $a \in \mathbb{Z}$, $(a, n) = 1$ számra, ezért n Carmichael-szám.

Fordítva, ha n Carmichael-szám, akkor tudjuk, hogy $n = q_1 \cdots q_k$ alakú, ahol $q_i - 1 \mid n - 1$ minden i -re. Ekkor $\lambda(n) = [\lambda(q_1), \dots, \lambda(q_k)] = [q_1 - 1, \dots, q_k - 1] \mid n - 1$. \square

Irodalom

Könyvek:

[B96] P. BUNDSCHUH, Einführung in die Zahlentheorie, Springer Verlag, Berlin Heidelberg New York, 1996.

[FGy2000] FREUD R., GYARMATI E., Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2000.

[HW85] G. H. HARDY, E. M. WRIGHT, An Introduction to the Theory of Numbers, Clarendon Press, Oxford, Fifth edition, 1985.

[M97] MEGYESI L., Bevezetés a számelméletbe, Polygon, Szeged, 1997.

[S64] W. SIERPINSKI, Elementary Theory of Numbers, Warszawa, 1964.

Folyóiratcikkek:

[AGP94] W. R. ALFORD, A. GRANVILLE, C. POMERANCE, There are infinitely many Carmichael numbers, *Ann. of Math. (2)* **139** (1994), 703-722.

[Be50] N. G. W. H. BEEGER, On composite numbers n for which $a^{n-1} \equiv 1 \pmod{n}$ for every a prime to n , *Scripta Math.* **16** (1950), 133-135.

[Ca10] R. D. CARMICHAEL, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1910), 232-238.

[Ca12] R. D. CARMICHAEL, On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, *Amer. Math. Monthly* **19** (1912), 22-27.

[Ch39] J. CHERNICK, On Fermat's simple theorem, *Bull. Amer. Math. Soc.* **45** (1939), 269-274.

[Ko99] A. KORSELT, Problème chinois, *L'intermédiaire mathématiciens* **6** (1899), 142-143.

[Le36] D.H. LEHMER, On the converse of Fermat's theorem, *Amer. Math. Monthly* **43** (1936), 347-354.

[Pi93] R. G. E. PINCH, The Carmichael numbers up to 10^{15} , *Math. Comp.* **61** (1993), 381-391.

[Po38] P. POULET, Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à 100.000.000, *Sphinx* **8** (1938), 42-52; Corrections: MTE 485, *Math. Comp.* **25** (1971), 944-945; MTE 497, *Math. Comp.* **26** (1972), 814.

[LN96] G. LÖH, W. NIEBUHR, A new algorithm for constructing large Carmichael numbers, *Math Comp.* **65** (1996), 823-836.

Ismertető cikkek:

[G92] A. GRANVILLE, Primality testing and Carmichael numbers, *Notices Amer. Math. Soc.*, **39** (1992), 696-700.

[K95] KISS E., Álprímek Bolyai János kézirati hagyatékában, *Mat. Lapok (Kolozsvár)*, 1995, 9. szám, 321-324.

[T86] TÓTH L., Pseudoprím számok, *Mat. Lapok (Kolozsvár)*, 1986, 10. szám, 386-388.