

Páros tökéletes számok oszthatósági tulajdonságai

SÁNDOR JÓZSEF

Bevezetés. Jelölje $\sigma(n)$ az n természetes szám osztóinak az összegét. Az n számot tökéletesnek nevezzük, ha

$$(1) \quad \sigma(n) = 2n.$$

Euklidesznek tulajdonítjuk azt az észrevételt, hogy ha $n = 2^{k-1}(2^k - 1)$ alakú szám, ahol $2^k - 1$ prímszám, akkor n kielégíti (1)-et, vagyis n páros tökéletes szám. 2000 évvel később, Euler volt az, aki először kimutatta, hogy minden páros tökéletes szám ilyen alakú, tehát, ha n páros megoldása (1)-nek, akkor

$$(2) \quad n = 2^{k-1}(2^k - 1),$$

ahol $2^k - 1 = q$ prímszám. Ennek, a szerző által adott új bizonyításai megtalálhatók például az [1], [2] dolgozatokban.

Megjegyezzük, hogy a mai napig nem ismert az, hogy vannak-e páratlan tökéletes számok, tehát csupán a (2) alakú páros megoldások az ismert tökéletes számok. A páros tökéletes számoknak nagy története van, és az első négy ilyen szám – azaz 6, 28, 496, 8128 – után minden rákövetkezőnek külön felfedezője van. Ennek ellenére, és a modern számítógépek nagy kapacitása dacára, csupán 47 darab ilyen számot ismerünk manapság. Ennek egyik oka az $M_k = 2^k - 1$ alakú „Mersenne számok” prím-voltának nehéz eldönthetősége ([3]).

A tökéletes számok iránti érdeklődés Euklidesz után lényegében i.sz. 100 körül lángolt fel újra, amikor is Gerasai Nicomachus a híres „Introductio Arithmetica” című könyvében a számokat három csoportra osztotta: tökéletesek ($\sigma(n) = 2n$), hiányosak ($\sigma(n) < 2n$) és bővelkedők ($\sigma(n) > 2n$). Nicomachus könyvében öt kijelentés található (bizonyítás nélkül): a) Az n -edik tökéletes számnak n számjegye van; b) A tökéletes számok mind párosak; c) Minden tökéletes szám 6-ban vagy 8-ban végződik (váltakozva); d) Végtelen sok tökéletes szám van; e) A tökéletes számok $2^{k-1}(2^k - 1)$ alakúak.

Az újabb tökléletes számok felfedezése azonnal cáfolta az a) állítást és c) azon részét, hogy váltakozva 6 és 8-ban végződnek. (Az, hogy 6 és 8-ban végződnek, helyes észrevétel volt.) Másfelől a b), d), e) állítások gyakorlatilag a mai napig nyitottak.

A páros n tökléletes számok azon tulajdonsága, hogy mind 6-ban vagy 8-ban végződnek, még

$$(3) \quad n \equiv 6 \pmod{10} \quad \text{vagy} \quad n \equiv 8 \pmod{10}$$

alakban is írható. A továbbiakban (3) alakú oszthatósági tulajdonságokkal foglalkozunk. Ezek közül a tulajdonságok közül számos jólismert (bennük vannak a „matematikai folklór”-ban), mások talán nem annyira ismeretesek (néhány észrevétel talán új lesz).

Oszthatósági tulajdonságok

1. Lemma. 1) Minden páratlan p prímszám $4m + 1$ vagy $4m + 3$ alakú (m természetes szám).

2) Minden $p \geq 5$ prímszám $6k + 1$ vagy $6k + 5$ alakú (k természetes szám).

Bizonyítás. 1) Egy páratlan szám 4-gyel osztva csak 1 és 3 maradékokat adhatja (ha a maradék 0 vagy 2, akkor páros szám).

2) Osszuk el maradékosan $p \geq 5$ számot 6-tal! Ekkor $p = 6k + r$ alakú, ahol $r \in \{0, 1, 2, 3, 4, 5\}$. Mivel $r = 0, 2, 3, 4$ esetben p osztható 6-tal, 2-vel, 3-mal, illetve 2-vel; csupán $r = 1$ és $r = 5$ esetek maradhatnak.

2. Lemma. Ha $2^k - 1$ prímszám, akkor k is prímszám.

Bizonyítás. Legyen k összetett szám, vagyis $k = ab$, hol $a > 1$, $b > 1$. Ekkor $2^k - 1 = 2^{ab} - 1 = (2^a)^b - 1 = x^b - 1$, ahol $x = 2^a$. Az ismert

$$x^b - 1 = (x - 1)(x^{b-1} + \dots + x + 1)$$

képlet alapján $x^b - 1$ osztható $x - 1$ -gyel, vagyis $2^a - 1 \geq 2^2 - 1 = 3$ -mal. Ezért $2^k - 1$ osztható $2^a - 1 \geq 3$ -mal, ahol $2^k - 1 > 2^a - 1$. Így $2^k - 1$ nem lehet prímszám, ami ellentmondás.

3. Megjegyzés A 2. Lemma alapján a páros tökéletes számok (2) alakja

$$(4) \quad n = 2^{p-1}(2^p - 1)$$

lesz, ahol p egy prímszám és $2^p - 1 = q$ is prímszám. Megjegyezzük, hogy a 2. Lemma fordítottja nem igaz. Például $k = 11$ prímszám, de $2^{11} - 1 = 2047 = 23 \cdot 89$ nem az.

4. Tétel. A (3) alatti oszthatóságok igazak; azaz minden páros tökéletes szám 6-ban vagy 8-ban végződik.

Bizonyítás. Az 1. Lemma 1) állítása szerint két eset lehetséges p -re az n szám (4)-beli alakjában.

1) Ha $p = 4m + 1$, akkor

$$n = 2^{4m}(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m.$$

Mivel $6 \cdot 6 = 36$, 6-ban végződik, úgy 16 hatványai is mind 6-ban végződnek, más szavakkal $16^t \equiv 6 \pmod{10}$. Tehát $n \equiv 2 \cdot 6 - 6 \pmod{10} \equiv 6 \pmod{10}$.

2) Ha $p = 4m + 3$, akkor

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) = 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m \equiv \\ &\equiv 2 \cdot 6 - 4 \cdot 6 \pmod{10} \equiv -12 \pmod{10} \equiv 8 \pmod{10}. \end{aligned}$$

5. Megjegyzés. 1) Mivel $6 \equiv 1 \pmod{5}$ és $8 \equiv 3 \pmod{5}$, innen következik az is, hogy egy páros n tökéletes számra $n \equiv 1 \pmod{5}$ vagy $n \equiv 3 \pmod{5}$.

2) A második esetben, vagyis ha $p = 4m + 3$, észrevehető egy élesebb tulajdonság. Ugyanis,

$$2^{p-1} = 2^{4m+2} \equiv 4, 24, 44, 64, 84 \pmod{100}.$$

Így

$$2^p - 1 = 2 \cdot 2^{p-1} - 1 \equiv 7, 47, 87, 27, 67 \pmod{100};$$

ahonnan

$$n = 2^{p-1} \cdot (2^p - 1) \equiv 4 \cdot 7, 24 \cdot 47, 64 \cdot 7, 84 \cdot 67 \pmod{100}.$$

Kis számítással látható, hogy ez utóbbi szorzatok mind $\equiv 28 \pmod{100}$. Így a 4. Tétel alábbi élesítését nyertük:

6. Tétel. Minden páros tökéletes szám 6-ban vagy 28-ban végződik.

Hasonló okoskodással (amelyet az Olvasóra bízunk), megmutatható az alábbi:

6'. Tétel. Ha $n \neq 6$ és $n \neq 496$ páros tökéletes szám, akkor n utolsó két számjegye az alábbiak közt kell legyen: 16, 28, 36, 56, 76.

Most igazoljuk az alábbi kongruenciát:

7. Tétel. *Ha $n \neq 6$ páros tökéletes szám, akkor*

$$n \equiv 4 \pmod{6}.$$

Bizonyítás. Mivel (4)-ben $p \geq 3$, úgy p páratlan, tehát $p - 1 = 2s$ páros. De ekkor

$$2^{p-1} = 2^{2s} = 4^s = (3 + 1)^s \equiv 1 \pmod{3}.$$

Tehát $2^{p-1} = 3a + 1$ alakú. Itt a nem lehet páros, tehát $a = 2b + 1$, amikor is $3a + 1 = 3(2b + 1) + 1 = 6b + 4$. Mivel $2^{p-1} = 6b + 4$, úgy $2^p = 12b + 8$; ahonnan $2^p - 1 = 12b + 7 = 6c + 1$. Végül is, $n = 2^{p-1}(2^p - 1) = (6b + 4)(6c + 1) = 6d + 4$, vagyis $n \equiv 4 \pmod{6}$.

Alkalmazás. *Az (5, 7) az egyetlen ikerprím-páros, melyeknek számtani közepe tökéletes szám.*

Valóban, ha $(r, r + 2)$ egy ikerprím-páros (azaz r és $r + 2$ mindketten prímszámok), akkor $\frac{r+r+2}{2} = r + 1$ számtani közepük páros szám, és $r + 1 = n$ = tökéletes szám lenne, akkor $r = n - 1$ prímszám lenne. Ez igaz, ha $n = 6$. De ha $n \neq 6$, akkor 7. Tétel alapján $n - 1 \equiv 3 \pmod{6}$, tehát $n - 1$ osztható 3-mal, ami ellentmondás.

8. Tétel. *Ha $n \neq 28$ páros tökéletes szám, akkor $n \equiv 1 \pmod{7}$, vagy $n \equiv 6 \pmod{7}$.*

Bizonyítás. Ha $p \geq 5$, $p = 6k + 1$ alakú; akkor

$$2^{p-1} = 2^{6k} = (2^3)^{2k} = (7 + 1)^{2k} \equiv 1 \pmod{7}$$

és innen $2^p - 1 \equiv 1 \pmod{7}$, tehát $n = 2^{p-1}(2^p - 1) \equiv 1 \pmod{7}$. Ha $p = 6k + 5$ alakú, akkor

$$2^{p-1} = 4^{3k+2} = 4^2(4^3)^k = (14 + 2)(63 + 1)^k \equiv 2 \pmod{7},$$

hiszen 14 és 63 oszthatók 7-tel. Innen $2^p \equiv 4 \pmod{7}$, azaz

$$2^{p-1}(2^p - 1) \equiv 2 \cdot 3 \pmod{7} \equiv 6 \pmod{7},$$

és ezzel az 8. Tétel bizonyítva van.

9. Tétel. *Ha $n \neq 6$ páros tökéletes szám, akkor $n \equiv 1 \pmod{13}$, vagy $n \equiv 2 \pmod{13}$, vagy $n \equiv 3 \pmod{13}$, vagy $n \equiv 8 \pmod{13}$.*

Bizonyítás. Mivel $28 \equiv 2 \pmod{13}$, tegyük fel, hogy (4)-ben $p \geq 5$. Ha $p = 6k + 1$, akkor

$$2^{p-1} = 2^{6k} = 64^k = (65 - 1)^k \equiv (-1)^k \pmod{13},$$

hiszen $5 \cdot 13 = 65$. Véve külön a k páros és k páratlan eseteket, a 8. Tétel bizonyításához hasonlóan kapjuk, hogy ebben az esetben $n \equiv 1$ vagy $3 \pmod{13}$.

Ha $p = 6k + 5$, akkor

$$2^{p-1} = 4^{3k+2} = 16 \cdot (65 - 1)^k = (13 + 3)(65 - 1)^k \equiv 3(-1)^k \pmod{13}.$$

Így $2^p - 1 \equiv 6(-1)^k - 1 \pmod{13}$ és innen $n \equiv 2$ vagy $8 \pmod{13}$, ha k páros vagy páratlan eseteket tekintjük.

Az alábbi tétel bizonyítása hasonlóan történik:

10. Tétel. *Ha $n \neq 6$ páros tökéletes szám, akkor $n \equiv 1 \pmod{9}$.*

Következmény. *Egy $n \neq 6$ páros tökéletes szám számjegyeit összeadva, a kapott szám legyen n_1 . Az n_1 számjegyeit összeadva kapjuk n_2 -t. Az eljárást addig folytatjuk, míg egy egyjegyű számot kapunk. Ekkor ez az egyjegyű szám 1.*

Valóban, legyen $s(n)$ az n számjegyeinek összege. Jólismert, hogy $n - s(n) \equiv 0 \pmod{9}$. Innen, a 10. Tétel alapján

$$s(n) \equiv 1 \pmod{9},$$

ahonnan

$$s(s(n)) \equiv s(n) \pmod{9} \equiv 1 \pmod{9},$$

stb. és végül

$$s(s \dots (s(n)) \dots) = 1,$$

ha már egyjegyű számot kapunk.

Irodalom

- [1] Sándor József, Despre numerele pare perfecte și superperfecte, Lucrările Seminarului de Didactica Matematicii, **8**(1992), 167–168.
- [2] Sándor József, On even perfect and superperfect numbers, Notes Number Theory Discrete Math., **7**(2001), no.1, 4–5.
- [3] Mersenne prime, <http://mathworld.wolfram.com/MersennePrime.html>

