Eötvös Loránd Tudományegyetem
Természettudományi Kar

A tökéletes számok és társaik

BSc szakdolgozat

Írta: **Orthmayr Flóra**
Matematika BSc, matematikai elemző szakirány

Témavezető: **Dr. Freud Róbert**, egyetemi docens
Algebra és Számelmélet Tanszék

Budapest, 2012

Tartalomjegyzék

1. Bevezetés

Szakdolgozatom témája a tökéletes, barátságos és egyéb, osztóösszegükkel kapcsolatos tulajdonságaik miatt különleges számok jellegzetességei, és megismerésük több mint kétezer éves története – mellőzve a misztikus kitérőket a barátságos számok talizmánként való hasznosításáról, vagy a tökéletesség olyan alátámasztásait, mint hogy Isten hat nap alatt teremtette a világot, és a Hold huszonnyolc nap alatt kerüli meg a Földet. Bár többen is kijelentették, hogy a tökéletes számok „kevés elméleti jelentőséggel bírnak"[1], és „csupán érdekesek anélkül, hogy hasznosak volnának"[2], mégis számos nagy matematikus vizsgálta őket az ókortól napjainkig, és dolgozott ki új módszereket, máshol is hasznos tételeket munkája során.

A dolgozatban párhuzamosan fejtettem ki a témakör matematikai és történeti részét, ott tárgyalva az egyes tulajdonságokat, ahol a felismerésük sorra került a történetben, amelyet különböző magyar és angol nyelvű források alapján állítottam össze. Először a tökéletes, majd a barátságos számok megismerésének történetét követtem, aztán sorra vettem néhány „társukat", a többszörösen tökéletes, szupertökéletes és kvázitökéletes számokat, valamint az osztóösszeg-sorozatokat, az érinthetetlen és a szociális számokat. Az állítások bizonyítását önállóan (vagy némi útmutatás alapján) készítettem el, egyetlen nehezebb tétel kivételével, amelyhez a tankönyvben szereplő bizonyítást dolgoztam fel. Az osztóösszeg-sorozatok viselkedésének szemléltetésére készítettem egy számítógépes programot is, amely a dolgozat mellékletét képezi.

2. Az osztóösszeg-függvény

Azok a számok, amelyekről a továbbiakban szó lesz, mind abból a szempontból különlegesek, hogy osztóik összege adott viszonyban áll magával a számmal vagy más számokkal, tehát definiálásukhoz és alapvető tulajdonságaik megismeréséhez is ismernünk kell az osztók összegzését megkönnyítő szabályokat és az osztóösszeg-függvény néhány alapvető tulajdonságát.

2.1. Definíció. $\sigma(n)$ jelöli az n pozitív osztóinak összegét.

Egyes definícióknál azonban érdemes inkább a valódi osztók összegét használni:

2.2. Definíció. $s(n)$ jelöli az n pozitív osztóinak összegét az n kivételével (a továbbiakban ezeket valódi osztóknak nevezzük): $s(n) = \sigma(n) - n$.

Alapvetően a $\sigma(n)$-t nevezzük „osztóösszeg-függvénynek", de az $s(n)$ külön megnevezése híján az „osztóösszeg" kifejezés szerepelhet a valódi osztók összegével kapcsolatban is (például az *aliquot parts problems, aliquot sequences, aliquot cycles* kifejezések mint osztóösszeg-problémák, osztóösszeg-sorozatok, osztóösszeg-körök fordításában).

2.3. Definíció. Az f számelméleti függvény (pozitív egészeken értelmezett komplex értékű függvény) multiplikatív, ha bármely $(a, b) = 1$ esetén $f(ab) = f(a)f(b)$ teljesül. Az f teljesen multiplikatív, ha $f(ab) = f(a)f(b)$ teljesül minden a, b esetén.

2.4. Tétel. *A $\sigma(n)$ osztóösszeg-függvény multiplikatív, vagyis bármely $(a, b) = 1$ esetén $\sigma(ab) = \sigma(a)\sigma(b)$ teljesül.*

Bizonyítás. Ha a összes osztója: $1 = a_0, a_1, \ldots, a_n$ és b összes osztója: $1 = b_0, b_1, \ldots, b_m$, akkor ab összes osztóját úgy kapjuk meg, hogy a minden osztóját megszorozzuk b minden osztójával: $a_0b_0 = 1, a_0b_1, \ldots, a_nb_{m-1}, a_nb_m$. Így megkaptuk az összes osztót, de vannak-e a listán ismétlések? Azt szeretnénk belátni, hogy ha $(a, b) = 1$, akkor a listán ab minden osztója csak egyszer

szerepel. Legyen $a_i = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ az a szám egyik osztója és $b_j = q_1^{\beta_1} \cdots q_s^{\beta_s}$ a b szám egyik osztója, ahol a p_k és q_k számok különböző prímek. Tegyük fel, hogy $a_i b_j = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s} = a_h b_l$, ahol a_h az a egy osztója és b_l a b egy osztója. A p_k számok egyike sem lehet osztója b_l-nek, hiszen akkor b-nek lenne egynél nagyobb közös osztója a_i-vel. Ugyanígy a q_k számok egyike sem lehet osztója a_h-nak, tehát $b_l = b_j$ és $a_i = a_h$, vagyis az $a_i b_j$ szorzatok mind különbözőek, tehát összegük (amelyet az a_i számok összegének és a b_i számok összegének szorzataként kapunk) az ab összes osztójának összegével egyenlő. □

2.5. Tétel. *Ha az n kanonikus alakja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, akkor*

$$\sigma(n) = \prod_{i=1}^{r} (1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Bizonyítás. A $\sigma(ab) = \sigma(a)\sigma(b)$ állítás nyilvánvalóan több tagú szorzat esetén is ugyanígy igaz ($\sigma(abc) = \sigma(a)\sigma(bc) = \sigma(a)(\sigma(b)\sigma(c))$ stb.), ha a tényezők páronként relatív prímek, tehát különböző prímek hatványainak szorzatára mindenképp. Így $\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i})$. A $p_i^{\alpha_i}$ prímhatvány összes osztója $1, p_i, \ldots, p_i^{\alpha_i}$, vagyis az 1 kezdőtagú, p_i hányadosú mértani sorozat első $\alpha_i + 1$ tagja, amelyeket a mértani sorozatokra vonatkozó képlettel összegezve $\frac{p_i^{\alpha_i+1}-1}{p_i-1}$-et kapjuk. □

A továbbiakban néhány, a $\sigma(n)$ lehetséges értékeire vonatkozó állítás következik, amelyek hasznosak lehetnek a későbbi bizonyítások során.

2.6. Állítás. *$\sigma(n)$ akkor és csak akkor páratlan, ha $n = 2t^2$ vagy $n = t^2$.*

Bizonyítás. Legyen n kanonikus alakja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

$\sigma(n) = \prod_{i=1}^{r} (1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i})$ akkor és csak akkor lesz páratlan, ha a szorzat minden tényezője páratlan. $1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i}$ páratlan lesz $p_i = 2$ esetén bármilyen α_i kitevőre. Ha $p_i \neq 2$, akkor az összeg minden tagja páratlan, tehát páratlan sok tag esetén lesz az összeg is páratlan, így α_i páros kell, hogy legyen n minden $p_i \neq 2$ prímtényezőjére. Egy szám négyzetszám,

ha minden prímtényezője páros kitevőn szerepel. Tehát $\sigma(n)$ akkor és csak akkor lesz páratlan, ha $n = 2t^2$ vagy $n = t^2$. $\square$

2.7. Állítás. *$\sigma(n)$ akkor és csak akkor kettőhatvány, ha n egy Mersenne-prím (vagyis $2^k - 1$ alakú prímszám) vagy különböző Mersenne-prímek szorzata.*

Bizonyítás. Nyilvánvaló, hogy $\sigma(n)$ kettőhatvány, ha n Mersenne-prím vagy különböző Mersenne-prímek szorzata, hiszen ekkor $\sigma(n)$ képletében minden tényező $(1 + (2^k - 1))$ alakú. Lássuk be, hogy egyébként nem az!

Tegyük fel, hogy $\sigma(n)$ kettőhatvány és $(1+p+p^2+\ldots+p^\alpha)$ az egyik tényező a képletében, vagyis a p prím α kitevővel szerepel n kanonikus alakjában. Ekkor $(1 + p + p^2 + \ldots + p^\alpha)$ is kettőhatvány, tehát biztosan páros, így $p \neq 2$ és α páratlan. Ekkor $2^k = (1+p+p^2+\ldots+p^\alpha) = (1+p)(1+p^2+p^4+\ldots+p^{\alpha-1})$. Mivel a bal oldal kettőhatvány, ezért a jobb oldalon is mindkét tényezőnek kettőhatványnak kell lennie, tehát p Mersenne-prím.

Tegyük fel, hogy az $1 + p^2 + p^4 + \ldots + p^{\alpha-1}$ kettőhatvány páros sok szám összege, ekkor a fentihez hasonlóan felbontható:

$$(1 + p^2 + p^4 + \ldots + p^{\alpha-1}) = (1 + p^2)(1 + p^4 + p^8 + \ldots + p^{\alpha-3}).$$

Mivel a bal oldal kettőhatvány, ezért a jobb oldalon is mindkét tényezőnek kettőhatványnak kell lennie, tehát $2^l = 1 + p^2 \Rightarrow 2^l - 1 = p^2$. Mivel négyzetszám nem lehet $4k - 1$ alakú, ez csak akkor teljesülhetne, ha $l = 1 \Rightarrow p = 1$, tehát p prímszámra ellentmondást kaptunk. Ebből következik, hogy az $1+p^2+p^4+\ldots+p^{\alpha-1}$ kettőhatvány páratlan sok szám összege, és mivel páratlan sok páratlan szám összegeként mindenképp páratlan, csak 1 lehet, vagyis $\alpha = 1$. Ezzel beláttuk, hogy n csak különböző Mersenne-prímek szorzata lehet. $\square$

2.8. Állítás. *A $\sigma(n)$ függvény értékkészletéből végtelen sok természetes szám kimarad.*

Bizonyítás. Lássuk be, hogy a $\sigma(n)$ értékkészletéből végtelen sok páratlan szám kimarad! Tetszőleges N számnál kisebb páratlan $\sigma(n)$ esetén teljesülnie kell a következő feltételeknek: $n < N$ és $n = s^2$ vagy $n = 2t^2$, ahol t és s pozitív egész szám.

$2t^2 < N \Leftrightarrow t^2 < \frac{N}{2} \Leftrightarrow t < \sqrt{\frac{N}{2}} \Rightarrow t$ lehetséges értékeinek száma kevesebb mint $\sqrt{\frac{N}{2}}$.

$s^2 < N \Leftrightarrow s < \sqrt{N} \Rightarrow s$ lehetséges értékeinek száma kevesebb mint $\sqrt{N}$.

A fenti kettő összege felső korlátot ad az n lehetséges értékeinek számára, és ezáltal a $\sigma(n)$ N-nél kisebb páratlan értékeinek számára is. Ezt az összeget az N-nél kisebb páratlan számok mennyiségéből kivonva a $\sigma(n)$ függvény értékkészletéből kimaradó páratlan számok mennyiségére alsó korlátot kapunk: $\lfloor \frac{N}{2} \rfloor - (\sqrt{N} + \sqrt{\frac{N}{2}})$, ez pedig tart a végtelenhez, ha N tart a végtelenhez, mivel a gyökös kifejezések elhanyagolhatóan kisebbek. $\square$

3. A tökéletesség keresése

3.1. Az ókori görögök

A tökéletes számok definíciója és a páros tökéletes számok előállítására vonatkozó tétel először Euklidésznél szerepel. Az *Elemek*en belül önálló egységet alkot a három számelméleti témájú könyv (a hetedik, a nyolcadik és a kilencedik), amelyek nem építenek a korábbi könyvek eredményeire, és nem szükségesek a következőkhöz. Ennek az egységnek a koronája – a definíciók és a tételek között is az utolsó – a tökéletes számok elmélete.

Az *Elemek* definíciója szerint (VII. 23.): „Egy szám tökéletes, ha egyenlő az osztói összegével."[3] Az osztó itt (a VII. 3. definíció alapján) a számnál kisebb (pozitív) osztókat, vagyis a valódi osztókat jelenti, tehát:

3.1. Definíció. Az n pozitív egész tökéletes szám, ha $\sigma(n) = 2n$. (Tökéletes szám az az n, amelyre $s(n) = n$.)

A három számelméleti könyvön belül is külön egység a IX. könyv 21-34. tétele, az elemi állításokból felépülő „páros és páratlan elmélete", mely a tökéletes számokra vonatkozó 36. tétellel együtt önálló rendszert alkot – bár a 36. tételnek az *Elemek*ben szereplő bizonyítása épít a másik két számelméleti könyv tételeire is, O. Becker megmutatta, hogy a bizonyításhoz elég csupán a 21-34. tételek használata is.[4] A tökéletes számok gondolatát egyébként is szokás a pithagoreusoknak tulajdonítani, és egyes feltételezések szerint az elsősorban már ismert eredményeket rendszerező és pontosító *Elemek* ezen részét Euklidész különösebb változtatás nélkül emelte át egy korai pithagoreus tankönyvből.

A páros tökéletes számok konstruálásáról szóló tétel Euklidész megfogalmazásában (IX. 36.): „Ha az egységtől kezdve kétszeres arányban képzünk egy mértani sorozatot, amíg a sorösszeg prím nem lesz, és az összeggel megszorozzuk az utolsó tagot, akkor a szorzat tökéletes szám lesz."[3] Modern változatban:

3.2. Tétel. *Egy n páros szám tökéletes, ha $n = 2^{p-1}(2^p - 1)$ alakú, ahol $2^p - 1$ prím.*

Bizonyítás. Ha $2^p - 1$ prím, akkor $n = 2^{p-1}(2^p - 1)$ osztóinak összege:

$$\sigma(n) = \sigma(2^{p-1}) \cdot (1 + 2^p - 1) = (1 + 2 + \ldots + 2^{p-1}) \cdot 2^p =$$
$$= (2^p - 1) \cdot 2^p = 2^{2p} - 2^p = 2 \cdot 2^{p-1}(2^p - 1) = 2n,$$

tehát n tökéletes szám. □

Nikomakhosz (i. sz. 100 körül) három csoportra osztotta a páros számokat: hiányos, tökéletes és bővelkedő számokra. Hiányos egy szám, ha nagyobb, mint a nála kisebb pozitív osztóinak összege és bővelkedő, ha kisebb.

3.3. Definíció. Az n pozitív egész hiányos szám, ha $\sigma(n) < 2n$, és bővelkedő, ha $\sigma(n) > 2n$.

Nikomakhosz példákat is említett mindhárom csoportra, ő írta le az ókori görögök által is ismert első négy tökéletes számot: 6, 28, 496, 8128. Ezek alapján megfogalmazta azt a (téves, de hosszú évszázadokon keresztül számos nagy matematikus által megismételt) állítást is, hogy a tökéletes számok felváltva végződnek 6-ra és 8-ra. Iamblikhosztól (i. sz. 300 körül) származik az akkor ismert négy tökéletes szám egy másik, Nikomakhosz által is megállapított tulajdonságának szintén téves, de hosszan igaznak vélt általánosítása, miszerint a tíz minden egymást követő két hatványa közé pontosan egy tökéletes szám esik.

3.4. Állítás. *Minden prímhatvány hiányos szám.*

Bizonyítás. Lássuk be, hogy $\sigma(n) < 2n$ minden $n = p^\alpha$ esetén, ahol p tetszőleges prímszám, α tetszőleges pozitív egész. Az alábbiak ekvivalensek:

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1} < 2p^\alpha \Leftrightarrow p^{\alpha+1} - 1 < 2p^{\alpha+1} - 2p^\alpha \Leftrightarrow -1 < p^{\alpha+1} - 2p^\alpha.$$

$p^{\alpha+1} - 2p^\alpha = (p-2)p^\alpha$ biztosan nagyobb egy negatív számnál, mivel $0 \leq (p-2)$ és $0 < p^\alpha$, tehát az utolsó egyenlőtlenség igaz, így a vele ekvivalens első egyenlőtlenség is igaz, ezzel az állítást beláttuk. □

3.5. Állítás. *Ha egy n páratlan számnak csak két különböző prímosztója van, akkor n hiányos szám.*

Bizonyítás. Legyenek p, q páratlan prímek, $n = p^\alpha q^\beta$. Azt szeretnénk belátni, hogy

$$\frac{p^{\alpha+1}-1}{p-1} \cdot \frac{q^{\beta+1}-1}{q-1} < 2p^\alpha q^\beta, \text{ vagyis } \frac{p-\frac{1}{p^\alpha}}{p-1} \cdot \frac{q-\frac{1}{q^\beta}}{q-1} < 2.$$

Mivel $\frac{p-\frac{1}{p^\alpha}}{p-1} < \frac{p}{p-1}$, tehát a fentiek helyett igazolhatjuk az erősebb $\frac{p}{p-1} \cdot \frac{q}{q-1} < 2$ állítást. p növelésével $\frac{p}{p-1}$ szigorúan csökkenő sorozatot alkot. Mivel p és q különböző páratlan prímek, a legkisebb lehetséges értékeik 3 és 5, tehát $\frac{p}{p-1} \cdot \frac{q}{q-1} \leq \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < 2$, ezzel az állítást beláttuk. □

3.6. Állítás. *Egy bővelkedő szám minden többszöröse is bővelkedő.*

Bizonyítás. Lássuk be, hogy ha $\sigma(a) > 2a$, akkor $\sigma(ka) > 2ka$ is teljesül minden k pozitív egész számra.

Ha a minden osztóját megszorozzuk k-val, akkor a kapott számok mind osztói ka-nak és mind különbözőek, viszont (a triviális $k = 1$ eset kivételével) biztosan hiányzik közülük az 1, tehát: $\sigma(ka) > k\sigma(a) > 2ka$, ezzel az állítást beláttuk. □

Ezen állítások alapján látható az is, hogy végtelen sok hiányos és végtelen sok bővelkedő szám létezik, de ennél több is igaz:

3.7. Állítás. *Minden $k \geq 3$ egész számra végtelen sok olyan páratlan bővelkedő szám és végtelen sok olyan páratlan hiányos szám létezik, amelynek pontosan k különböző prímosztója van.*

Bizonyítás. 1. Mivel egy bővelkedő szám minden többszöröse bővelkedő, az állítás első feléhez elég találnunk egyetlen olyan bővelkedő számot, amelynek három különböző prímosztója van: $3^3 \cdot 5 \cdot 7 = 945$ ilyen, mert $\sigma(945) = 1920$. Ezt a számot (vagy bármely más olyan bővelkedő számot, amelynek három különböző prímosztója van) olyan prímek hatványaival szorozva, amelyek

már szerepelnek a felbontásában, végtelen sok bővelkedő számot kapunk $k = 3$-ra, tetszőleges c darab ezektől és egymástól különböző prímmel (illetve hatványaikkal) szorozva pedig végtelen sok bővelkedő számot kapunk $k = 3 + c$-re.

2. Egy minden prímtényezőjét csak egyszeresen tartalmazó hiányos számra

$$2p_1p_2 \dots p_k > (p_1 + 1)(p_2 + 1) \dots (p_k + 1).$$

Ennek elégséges feltétele, ha a szám minden p_i prímosztójára teljesül, hogy:

$$\sqrt[k]{2}p_i > p_i + 1 \Leftrightarrow p_i(\sqrt[k]{2} - 1) > 1 \Leftrightarrow p_i > \frac{1}{\sqrt[k]{2} - 1}.$$

Ez egy alsó korlátot ad a prímtényezőkre, tehát mindig lesz végtelen sok prím, amely megfelel ennek a feltételnek, és k darab különböző ilyen prím szorzata mindig hiányos szám lesz. □

3.2. Mersenne és levelezőtársai

Az 1630-as évektől kezdve élénkült fel a számok osztóival kapcsolatos problémák vizsgálata, a tökéletes, barátságos és többszörösen tökéletes számok keresése Fermat, Mersenne, Frénicle és Descartes levelezésében. Marin Mersenne francia minorita szerzetes a korabeli tudományos élet koordinátora és információs központja volt: csaknem az összes jelentős nyugat-európai tudóssal aktívan levelezett, értesítette őket egymás eredményeiről, kérdéseivel ígéretes problémák vizsgálatára biztatta őket.

Mersenne először 1636-ban írt Fermat-nak, aki már korábban is foglalkozott az osztókkal kapcsolatos számelméleti problémákkal, és nagyon nehéznek nyilvánította őket, ugyanakkor kijelentette, hogy van általános módszere a megoldásukra. Erre válaszul hívta ki Frénicle 1640-ben (Mersenne-en keresztül) egy 20 vagy 21 jegyű tökéletes szám megtalálására. Fermat a tökéletes számok keresésének módszereként három tételt közölt Mersenne-nel 1640 júniusában írt levelében:

„I. Ha n nem prím, akkor $2^n - 1$ nem prím.

II. Ha n prím, akkor $2^n - 2$ többszöröse $2n$-nek.

III. Ha n prím, és p prímosztója $2^n - 1$-nek, akkor $p - 1$ többszöröse n-nek"[1],

majd Frénicle-nek írta meg októberben ezek általánosítását mint „az osztóösszeg-problémák alaptételét" (*la proposition fondamentale des parties aliquotes*): „Bármely p prímre és bármely $1, a, a^2$ stb. mértani sorozatra p kell, hogy osszon valamely $a^n - 1$-et, amelyre n osztja $p-1$-et; ekkor ha N bármely többszöröse a legkisebb ilyen n-nek, akkor p osztja $a^N - 1$-et is."[1]

Vizsgáljuk meg Fermat ezen állításait!

I. triviális: ha $n = km$ összetett szám, akkor $2^{km} - 1$-ből $(2^k - 1) \geq 3$ kiemelhető.

II. a „kis Fermat-tétel" $a = 2$-re (kiegészítve azzal, hogy páratlan n prímekre $2^n - 2$ az n prímen kívül még kettővel is osztható):

3.8. Tétel. (A "kis" Fermat-tétel) *Ha p prím, akkor bármely a egész számra $a^p \equiv a \pmod{p}$.*

Bizonyítás. Bizonyítás a szerinti teljes indukcióval: $1^p = 1 \equiv 1 \pmod{p}$ igaz bármilyen p prímre. Tegyük fel, hogy $n^p \equiv n \pmod{p}$ is teljesül. Mivel $\binom{p}{k}$ osztható p-vel minden $0 < k < p$ esetén, ezért a binomiális tétel és az indukciós feltevés alapján

$$(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \ldots + \binom{p}{n-1} n + 1 \equiv n^p + 1 \equiv n + 1 \pmod{p},$$

tehát ha az állítás igaz n-re, akkor $(n+1)$-re is. □

III. és általánosítása az „alaptételben" a kis Fermat-tétel másik alakját írja le, kiegészülve „a legkisebb ilyen n-re" vonatkozó állítással, ami a rend fogalmának és egyik tulajdonságának felel meg. Modern megfogalmazásban:

3.9. Definíció. Az n pozitív egészt az a rendjének nevezzük modulo p (prím), ha $a^n \equiv 1 \pmod{p}$, de bármely $k < n$ pozitív egészre $a^k \not\equiv 1 \pmod{p}$. Az a rendjét $o_p(a)$-val jelöljük.

3.10. Állítás. $a^N \equiv 1 \pmod{p} \Leftrightarrow o_p(a) | N$.

Frénicle kihívásában a valódi feladat annak eldöntése volt, hogy $2^{37}-1$ prímszám, vagy sem: nem az, ahogy Fermat helyesen megállapította, mikor azt válaszolta, hogy nincs 20 vagy 21 jegyű tökéletes szám. Ugyanis III. szerint ha p prímosztója $2^{37}-1$-nek, akkor $37|p-1$, tehát $2^{37}-1$ prímosztóit $37k+1$ alakban kell keresni, ahol k páros. A második ilyen, prímszámot adó k-ra megkapjuk a szám felbontását: $2^{37}-1 = 223 \cdot 616318177$.

Descartes 1638-ban azt írta Mersenne-nek, bizonyítani tudja, hogy minden páros tökéletes szám euklideszi típusú, de a bizonyítást nem közölte. (A tökéletes számokra vonatkozó tétel megfordításának első ismert bizonyítása Eulertől származik.)

3.11. Tétel. *Ha egy n páros szám tökéletes, akkor $n = 2^{p-1}(2^p-1)$ alakú, ahol 2^p-1 prím.*

Bizonyítás. n páros szám, tehát $n = 2^k \cdot t$ alakban írható, ahol t páratlan szám és $k \geq 1$. Ekkor 2^k és t relatív prímek, tehát

$$\sigma(n) = \sigma(2^k) \cdot \sigma(t) = (2^{k+1}-1) \cdot \sigma(t).$$

Ugyanakkor $\sigma(n) = 2n$, mivel n tökéletes szám, tehát $2^{k+1} \cdot t = (2^{k+1}-1) \cdot \sigma(t)$. Vonjunk ki t-t az egyenlet mindkét oldalán!

$$(2^{k+1}-1)t = (2^{k+1}-1) \cdot \sigma(t) - t \Leftrightarrow t = (2^{k+1}-1)(\sigma(t)-t).$$

Mivel $(2^{k+1}-1) \geq 3$, ezek szerint $(\sigma(t)-t) \neq t$ valódi osztója t-nek. Ekkor rajta kívül az egyetlen másik osztó csak maga a t lehet (hiszen $(\sigma(t)-t)+t = \sigma(t)$). Tehát t-nek összesen két osztója van, vagyis t prím és $\sigma(t)-t = 1$, az egynél nagyobb osztó pedig $2^{k+1}-1 = t$. Így $n = 2^k(2^{k+1}-1)$, ahol $(2^{k+1}-1)$ prím. $\square$

Descartes ugyanebben a levelében azt is kijelentette, hogy ha létezik páratlan tökéletes szám (úgy vélte, létezik), az ps^2 formájú kell, hogy legyen, ahol p prím. Frénicle 1657-ben ugyanezt a megállapítást azzal a kiegészítéssel közölte, hogy a p prím $4k+1$ alakú kell, hogy legyen.

3.12. Állítás. *Ha létezik egy páratlan n tökéletes szám, akkor szükségképpen $n = s^2p$, ahol p egy $4k+1$ alakú prím, és $n \equiv 1 \pmod{12}$ vagy $n \equiv 9 \pmod{36}$.*

Bizonyítás. Ha n páratlan tökéletes szám, akkor minden osztója páratlan, $\sigma(n)$ pedig mint a páratlan n kétszerese kettővel osztható, de néggyel már nem, vagyis a képletében pontosan egy páros tényező szerepel, tehát $n = s^2p$.

Tegyük fel, hogy $p = 4k-1$. Ekkor a páros számú tagból álló $(1+p+p^2+\ldots+p^\alpha)$ összeg tagjai felváltva $4k+1$ és $4k-1$ alakúak, tehát az összegük néggyel osztható. Mivel feltétel, hogy $\sigma(n)$ képletében egyetlen tényező se legyen néggyel osztható, p nem lehet $4k-1$ alakú, tehát p szükségképpen $4k+1$ alakú prímszám.

Tehát ha létezik páratlan tökéletes szám, az mindenképpen $n = s^2p$, ahol $p = 4k+1$ prím. Mivel páratlan négyzetszám, $s^2 \equiv 1 \pmod{4}$, tehát $n \equiv 1 \pmod{4}$. Vizsgáljuk meg n-t a hárommal oszthatóság szempontjából!

$p \neq 3$ prím, tehát ha $3 \mid n$, akkor $3 \mid s^2 \Rightarrow 3 \mid s \Rightarrow 9 \mid s^2 \Rightarrow 9 \mid n$. Tehát ha n osztható hárommal, akkor osztható kilenccel is, tehát ebben az esetben $n \equiv 9 \pmod{36}$.

Ha $3 \nmid n \Rightarrow 3 \nmid s$, akkor $s^2 \equiv 1 \pmod{3}$, mivel négyzetszám. Tegyük fel, hogy $p \equiv -1 \pmod{3}$. Ekkor a páros számú tagból álló $(1+p+p^2+\ldots+p^\alpha)$ összeg tagjai felváltva $3k+1$ és $3k-1$ alakúak, tehát az összegük hárommal osztható. Ez ellentmond annak, hogy $3 \nmid n$, tehát p szükségképpen $3k+1$ alakú, így $n \equiv 1 \pmod{3}$, tehát ebben az esetben $n \equiv 1 \pmod{12}$. □

A páratlan tökéletes számok létezésének kérdése egyébként máig megválaszolatlan: nem ismerünk egyet sem, de azt sem sikerült bizonyítani, hogy ne léteznének, csupán egyre szigorúbb feltételeket, amelyeknek meg kell felelniük, ha mégis léteznek. Egy páratlan tökéletes szám biztosan nagyobb, mint 10^{300}, legalább 75 prím szorzata, amelyek közül legalább 9 különböző; a legnagyobb prímosztója 10^8 fölötti és még a harmadik legnagyobb is nagyobb 100-nál.[5]

Mersenne 1644-ben megjelent *Cogitata Physico-Mathematica* című köny-

vének előszavában bizonyítás nélkül kijelentette, hogy $2^p - 1$ prím, ha $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$; más 257-nél kisebb p értékekre viszont összetett. A tökéletes számok keresésének történetében már korábban is sokan közöltek megalapozatlan vagy hibásan alátámasztott listákat arról, hogy mely p értékekre lesz a $2^p - 1$ szám prím: Mersenne Peter Bungus bő fél évszázaddal korábbi munkájára hivatkozik, mikor megállapítja, hogy a Bungus által felsorolt 28 (valójában csak 24) „tökéletes számból" csak 8 tökéletes ($p = 2, 3, 5, 7, 13, 17, 19, 31$), és ezeken kívül csak 3 további tökéletes szám ($p = 67, 127, 257$) ismert.

Peter Bungus táblázata, amely (nem elsőként és nem is utolsóként) azt a hibás feltételezést követte, hogy $2^{n-1}(2^n - 1)$ tökéletes szám lesz minden páratlan n esetén, az első huszonnégy ilyen számot tartalmazta. Ennél megalapozottabb listák is születtek már Mersenne előtt: Cataldi még a tizenhetedik század elején kijelentette, hogy $2^n - 1$ prím $n = 2, 3, 5, 7, 13, 17, 19, 23, 29, 31, 37$ esetén, és az összes lehetséges prímosztó végigpróbálásával állítását bizonyította is az $n \leq 19$ számokra, és ugyanígy (nem elsőként) azt is, hogy $2^{11} - 1$ összetett szám; azonban négy bizonyítás nélküli feltételezéséből három tévedés. Cataldi megállapította, hogy az ötödik és a hatodik tökéletes szám is hatra végződik, és bebizonyította, hogy ha nem is felváltva, de minden euklideszi tökéletes szám hatra vagy nyolcra végződik.

3.13. Állítás. *Minden páros tökéletes szám utolsó számjegye 6 vagy 8 (a tízes számrendszerben).*

Bizonyítás. A páros tökéletes számok $n = 2^{p-1}(2^p - 1)$ alakúak, ahol $(2^p - 1)$ prím. Az utolsó számjegyekkel mint tízes maradékokkal számolhatunk. Az első tényező kettőhatvány, tehát nemnulla páros számra végződik, a második tényező pedig eggyel kevesebb az első kétszeresénél, tehát a lehetséges végződések a következőképpen alakulnak:

$$2 \cdot (2 \cdot 2 - 1) \equiv 2 \cdot 3 \equiv 6 \pmod{10}$$

$$4 \cdot (4 \cdot 2 - 1) \equiv 4 \cdot 7 \equiv 8 \pmod{10}$$

$$6 \cdot (6 \cdot 2 - 1) \equiv 6 \cdot 1 \equiv 6 \pmod{10}$$

$(8 \cdot 2 - 1) \equiv 5 \pmod{10}$, de prímszám nem végződhet ötre, ahogy kettőhatvány nem végződhet nullára, tehát a fenti három az összes lehetséges variáció páros tökéletes számok utolsó számjegyére. □

Bár Mersenne csak négy elemmel bővítette az akkori hiteles listát (a négyből kettő valóban prímet ad, a másik kettő azonban nem), de ezek közül három 15 számjegynél nagyobb, ráadásul ugyanilyen nagyságrendű számok sokaságáról állította határozottan (és az esetek többségében helyesen), hogy mind összetett – pedig ő maga jelentette ki néhány mondattal később, hogy egy 15 vagy 20 jegyű szám prím voltának megállapítására a világ minden ideje sem volna elég!

3.3. A Mersenne-lista későbbi vizsgálata

Ebben a részben két bizonyításhoz is szükségünk lesz a Legendre-szimbólum definíciójára és néhány tulajdonságára.

3.14. Definíció. Legyen $p > 2$ prím és $(a, p) = 1$. Az a számot aszerint nevezzük kvadratikus maradéknak vagy kvadratikus nemmaradéknak modulo p, hogy az $x^2 \equiv a \pmod{p}$ kongruencia megoldható-e, vagy sem.

3.15. Definíció. Az $(\frac{a}{p})$ Legendre-szimbólumot a következőképpen értelmezzük:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{, ha } a \text{ kvadratikus maradék modulo } p, \\ -1 & \text{, ha } a \text{ kvadratikus nemmaradék modulo } p. \end{cases}$$

3.16. Tétel. *Legyen $p > 2$ prím és $(a, p) = 1$. Bármely ilyen a esetén $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod{p}$.*

3.17. Tétel. (Kvadratikus reciprocitási tétel) *Legyen $p > 2$ és $q > 2$ két különböző prím. Ekkor*

$$\left(\frac{q}{p}\right) = \begin{cases} -(\frac{p}{q}) & \text{, ha } p \equiv q \equiv -1 \pmod{4}; \\ (\frac{p}{q}) & \text{egyébként.} \end{cases}$$

3.18. Tétel. *Legyen $p > 2$ prím.*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , \text{ ha } p \equiv \pm 1 \pmod 8; \\ -1 & , \text{ ha } p \equiv \pm 3 \pmod 8. \end{cases}$$

Több mint száz évig senkinek sem sikerült bizonyítania vagy cáfolnia a Mersenne-féle lista bármely új állítását: $2^{31} - 1$ prím voltát Euler igazolta 1772-ben, miután végigpróbálta az összes lehetséges ($8 \cdot 31 \cdot n + 1$ vagy $8 \cdot 31 \cdot n + 63$ alakú) prímosztót 46339-ig (a legnagyobb páratlan számig, amely még kisebb, mint a vizsgált szám gyöke).

3.19. Állítás. *Legyenek p és q páratlan prímek. Ha $q | M_p$, akkor $q \equiv 1 \pmod p$ és $q \equiv \pm 1 \pmod 8$.*

Bizonyítás. A feltétel szerint $q | 2^p - 1$, vagyis $2^p \equiv 1 \pmod q$, tehát $o_q(2) | p$. Mivel p prímszám, ez csak úgy teljesülhet, ha $o_q(2) = p$. Mivel q prím, $2^{q-1} \equiv 1 \pmod q$, szóval $o_q(2) = p$ osztója $q - 1$-nek:

$$ap = q - 1 \Rightarrow ap + 1 = q \Rightarrow q \equiv 1 \pmod p.$$

A fentiekben láttuk, hogy $p | q - 1$. Mivel $(p, 2) = 1$, ez azt is jelenti, hogy $p | \frac{q-1}{2}$. A 3.16 tétel szerint $2^{\frac{q-1}{2}} \equiv (\frac{2}{q}) \pmod q$. A 3.18 tétel szerint pedig $1 = (\frac{2}{q})$ éppen akkor, ha $q \equiv \pm 1 \pmod 8$. $\square$

Újabb évszázadnak kellett eltelnie a következő bizonyítás és az első hiba felfedezéséig: 1876-ban É. Lucas a részben az ő nevét viselő teszt korai változatát használva igazolta, hogy $2^{127} - 1$ prím (mégpedig máig a legnagyobb, amit számológépek használata nélkül találtak meg), de $2^{67} - 1$ összetett. Később Mersenne további négy tévedésére derült fény: I. M. Pervusin 1883-ban kiderítette, hogy $2^{61} - 1$ viszont prím, majd R. E. Powers fedezett fel még két hiányosságot a listán: $2^{89} - 1$ és $2^{107} - 1$ szintén prímek. Végül 1922-ben M. Kraitchik találta meg az utolsó hibát, mikor igazolta, hogy $2^{257} - 1$ összetett szám, de csak 1947-re (összesen háromszáz év elteltével) igazolódott teljesen, hogy ez az öt volt az összes hiba Mersenne listáján.

Lucas módszerét D. H. Lehmer 1930 körül egyszerűsítette a ma ismert teszt formájára:

3.20. Tétel. (Lucas—Lehmer-teszt) *Legyen $p > 2$ prím, továbbá $a_1 = 4$ és $a_{i+1} = a_i^2 - 2$, ha $i \geq 1$. Ekkor M_p pontosan akkor prím, ha $M_p | a_{p-1}$.*

Bizonyítás. A bizonyításban felhasználjuk, hogy az $a + \sqrt{3}b$ számok (ahol a és b egészek) a szokásos műveletekre gyűrűt alkotnak (ezt nevezzük H-nak), amelyben a H-beli oszthatóság, rendfogalom és kongruencia szabályai ugyanúgy érvényesülnek, mint az egész számoknál.

A bizonyításhoz szükségünk lesz a következő lemmára:

Tetszőleges $q > 3$ prím esetén $(a + \sqrt{3}b)^q \equiv a + (\frac{3}{q})\sqrt{3}b \pmod{q}$.

Ezt a következőképpen igazolhatjuk: a binomiális tétel alapján

$$(a + \sqrt{3}b)^q = a^q + \binom{q}{1} a^{q-1}\sqrt{3}b + \ldots + \binom{q}{q-1} a \cdot 3^{\frac{q-1}{2}} b^{q-1} + 3^{\frac{q-1}{2}}\sqrt{3}b^q,$$

ahol a $\binom{q}{k}$ számok mind oszthatók q-val, a kis Fermat-tétel (3.8) szerint $a^q \equiv a \pmod{q}$ és $b^q \equiv b \pmod{q}$, végül a 3.16 tétel szerint $3^{\frac{q-1}{2}} \equiv (\frac{3}{q}) \pmod{q}$, és ezeket beírva a fenti alakba valóban a lemma állítását kapjuk vissza.

1. A feltétel átalakítása

$a_k = (2 + \sqrt{3})^{2^{k-1}} + (2 - \sqrt{3})^{2^{k-1}}$ (Ez teljes indukcióval könnyen igazolható: $k = 1$-re $a_1 = (2 + \sqrt{3})^1 + (2 - \sqrt{3})^1 = 4$ igaz. Tegyük fel, hogy $k = n$-re $a_n = (2 + \sqrt{3})^{2^{n-1}} + (2 - \sqrt{3})^{2^{n-1}}$ teljesül. Ennek felhasználásával $k = n + 1$-re $a_{n+1} = a_n^2 - 2 = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n} + 2(4 - 3)^{2^{n-1}} - 2 = = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$ is igaznak bizonyul.) Eszerint

$$a_{p-1} = (2 + \sqrt{3})^{2^{p-2}} + (2 - \sqrt{3})^{2^{p-2}} = (2 - \sqrt{3})^{2^{p-2}}((2 + \sqrt{3})^{2 \cdot 2^{p-2}} + 1).$$

Mivel $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ miatt a $2 \pm \sqrt{3}$ számok minden egész kitevős hatványa, így $(2 - \sqrt{3})^{2^{p-2}}$ is egység H-ban, az alábbiak ekvivalensek:

$$M_p | (2 - \sqrt{3})^{2^{p-2}}((2 + \sqrt{3})^{2 \cdot 2^{p-2}} + 1) \Leftrightarrow M_p | (2 + \sqrt{3})^{2^{p-1}} + 1,$$

vagyis a tételben szereplő feltétel: $M_p | a_{p-1} \Leftrightarrow (2 + \sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p}$.

2. $(2 + \sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p} \Rightarrow M_p$ prím igazolása

Legyen $q > 3$ az M_p egy prímosztója. Ekkor a fenti kongruencia modulo q is teljesül, és ezt négyzetre emelve azt kapjuk, hogy $(2+\sqrt{3})^{2^p} \equiv 1 \pmod{q}$. Eszerint tehát $o_q(2+\sqrt{3})|2^p$, viszont a négyzetre emelés előtti állapot alapján $o_q(2+\sqrt{3})$ nem osztja a 2^p egyetlen másik osztóját sem, tehát $o_q(2+\sqrt{3}) = 2^p$.

Tegyük fel, hogy $(\frac{3}{q}) = 1$. Ekkor

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

Ebből $q - 1 \geq 2^p$ következik, ami viszont ellentmond a kiindulási feltételnek, miszerint $q \leq M_p = 2^p - 1$.

Tehát $(\frac{3}{q}) = -1$. Ekkor

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

Ebből $q + 1 \geq 2^p$ következik, amit $q \leq M_p$-vel összevetve azt kapjuk, hogy $2^p - 1 \leq q \leq 2^p - 1$, vagyis $q = M_p$, tehát M_p prím.

3. M_p prím $\Rightarrow (2+\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p}$ igazolása

Ehhez a részhez szükségünk lesz a következő két állításra:

$M_p = 2^p - 1$, tehát $p > 2$ esetén $M_p \equiv -1 \pmod 8$, ebből pedig a 3.18 tétel alapján következik, hogy $(\frac{2}{M_p}) = 1$.

$M_p \equiv 1 \pmod 3$ és $M_p \equiv -1 \pmod 4$ miatt a 3.17 tétel szerint $(\frac{3}{M_p}) = -(\frac{M_p}{3}) = -(\frac{1}{3}) = -1$.

Tekintsük most az $(1+\sqrt{3})^2 = 2(2+\sqrt{3})$ egyenlőséget, és emeljük mindkét oldalát a (2^{p-1})-edik hatványra: $(1+\sqrt{3})^{2^p} = 2^{2^{p-1}}(2+\sqrt{3})^{2^{p-1}}$.

A bal oldalon $(1+\sqrt{3})^{2^p} = (1+\sqrt{3})(1+\sqrt{3})^{2^p-1}$ lett. A feltétel szerint $M_p = 2^p - 1$ prím, tehát

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

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

A jobb oldal első tényezője

$$2^{2^{p-1}} = 2 \cdot 2^{2^{p-1}-1} = 2 \cdot 2^{\frac{2^p-2}{2}} \equiv 2 \cdot \left(\frac{2}{M_p}\right) = 2 \pmod{M_p}.$$

A fentiek alapján az eredeti egyenletből $-2 \equiv 2(2+\sqrt{3})^{2^{p-1}} \pmod{M_p}$ adódik, és ezt a kongruenciát 2^{p-1}-nel szorozva és $2^p \equiv 1 \pmod{M_p}$ felhasználásával éppen azt kapjuk, hogy $(2+\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p}$. $\square$

3.4. A számítógépek kora

Az óriásprímek (és elsősorban a tökéletes számokat is meghatározó Mersenne-prímek, amelyek 1952 óta csak egyszer engedték át a „legnagyobb" címet más alakú prímeknek) keresése és találása új lendületet vett a számítógépes korszak kezdetével: 1952-ben Raphael Robinson egy éven belül öt új „legnagyobb ismert" Mersenne-prímet fedezett fel a SWAC (Standards Western Automatic Computer) számítógépre írt programjával, és azóta minden évtizedben legalább négy újat találtak: 1996 óta mindegyiket a GIMPS projekt résztvevői.

A GIMPS, vagyis a *Nagy internetes Mersenne-prím keresés* (Great Internet Mersenne Prime Search) elindítója George Woltman programozó, aki 1995 végén nekilátott a keresés akkori állapotát rögzítő különböző adatbázisok egyesítésének, majd létrehozta a GIMPS weboldalát, ahol közzétette az így elkészült adatbázist és ingyenesen letölthető számítógépes programját, amelynek használatával bárki csatlakozhat a közös kereséshez. A projekt elve a „sok kicsi sokra megy": a különböző, akár átlagos vagy gyenge személyi számítógépek együttese gyorsabb munkára képes a szuperszámítógépeknél. A kezdeti időkben Woltman személyesen regisztrálta az e-mailben beküldött eredményeket, amelyek 1996 novemberében már több mint 700 tesztelőtől érkeztek. Ez a korszak 1997 végén a PrimeNet szerver létrehozásával zárult le, Scott Kurowskinak köszönhetően. A résztvevő számítógépeken a tesztelést végző *prime95* program az 1998-tól elérhető 15-ös verziójától kezdve emberi beavatkozás nélkül kommunikál a PrimeNet központi adatbázisával, továbbítja az elért eredményeket és kapja meg a következő feladatokat. Ezeket a szerver az adott számítógép teljesítményének megfelelően osztja ki: a leggyorsabbak tesztelhetik a korábban még nem vizsgált Mersenne-számokat, a

gyengébbek az első teszt alapján összetettnek nyilvánítottakat ellenőrzik újra, a leglassabb gépek pedig előkészítő munkával, próbafaktorizációkkal foglalkoznak. A GIMPS programja ugyanis számos ismert feltételt és algoritmust használ fel a feladat (a Mersenne-számok prím vagy összetett voltának megállapítása) minél hatékonyabb elvégzésére:

I. Először elkészíti a lehetséges p prímek listáját, amelyekre $M_p = 2^p - 1$ prím volta vizsgálandó.

II. A lehetséges q prímosztók körét szűkíti a 3.19 állítás szerint, és eliminálja a kis (< 40000) prímekkel osztható számokat az eratoszthenészi szita (a feltételek alapján módosított) módszerével.

III. A megmaradt q osztók közül a kisebbekre (a vizsgált számtól függő korlátig) a következő algoritmus segítségével vizsgálja meg, hogy q osztója-e $2^p - 1$-nek: alakítsuk át p-t bináris alakra, a kezdőértéke legyen 1, majd ismételjük a következő lépéseket:

1. $a := a^2$;
2. vegyük el p bináris alakjának (balról) első számjegyét, és amennyiben ez 1, akkor $a := 2a$;
3. a új értéke legyen az a-nak q-val való osztási maradéka;

ismételjük 1-2-3-at, amíg p-nek még maradt elvehető számjegye. A végén $a \equiv 2^p \pmod{q}$, tehát ha $a = 1$, akkor $2^p - 1 \equiv 0 \pmod{q}$, vagyis M_p nem prím.

IV. Prímosztókat keres a John Pollard-féle $(p-1)$-módszer segítségével. A kis Fermat-tételen (3.8) alapuló módszer akkor tudja megtalálni egy N szám q prímosztóját, ha $q-1$-nek csak kis prímosztói vannak (konkrétan mindegyik kisebb egy adott $B1$ korlátnál). Mivel a Mersenne-számokhoz $q = 2kp + 1$ alakú prímosztókat keresünk, a módszer kicsit módosítható: q megtalálásához k prímosztóinak kell $B1$ alatt lenniük. Tegyük fel, hogy ez a feltétel teljesül, és legyen $E = 2^{e_2} \cdot 3^{e_3} \cdots b$, ahol $b \leq B1$ a legnagyobb ilyen prím, és a szorzatban minden $B1$-nél kisebb r prím olyan e_r kitevőn szerepel, hogy r^{e_r} a

legközelebb legyen $B1$-hez. Ez az E szám (nagyon nagy valószínűséggel: ha k felbontásában nem szerepel $\sqrt[c]{B1}$-nél nagyobb prím c vagy nagyobb kitevővel) többszöröse k-nak, mivel minden prímhatvány osztójának többszöröse, tehát $2kp|2Ep$. A kis Fermat-tétel miatt $3^{2Ep} \equiv 1 \pmod{q}$, tehát $3^{2Ep}-1$ többszöröse q-nak, de M_p-nek általában nem, és ekkor a $(3^{2Ep}-1, M_p)$ legnagyobb közös osztó M_p egy valódi osztóját fogja adni.

A módszer második lépcsője akkor találja meg a q prímosztót, ha k-nak ez az egy prímosztója van $B1$ és $B2$ korlátok között, az összes többi $B1$ alatt. Az első lépcső eredménye legyen $F = 3^{2Ep}$. Vegyünk minden olyan $B1 \leq z \leq B2$ számot, amely 1-gyel vagy 5-tel kongruens modulo 6 (hiszen a többi nyilván nem lehet prímosztó). Ezen z kitevőkkel olyan (F^z-1) számokat kapunk, amelyek egyike az első lépcsőben használt elv alapján (valószínűleg) többszöröse lesz q-nak. Ezeket modulo M_p összeszorozzuk, és a kapott szám és M_p legnagyobb közös osztója M_p valódi osztója lesz.

V. Ha a fenti módszerek egyikével sem talált osztót M_p-hez, akkor elvégzi a Lucas-Lehmer tesztet (3.20). Ebben a nagyon nagy számok hatékony négyzetre emeléséhez a program gyors Fourier-transzformációt alkalmazó algoritmust használ, az ehhez szükséges komplex számsorozatok bináris ábrázolása azonban nem lesz teljesen pontos, így kerekítési hibák kerülhetnek a számításokba. Ezek többségét az algoritmus még a folyamat során kiszűri, de nem mindet, ezért szükséges az első teszt igazolására a már említett ellenőrző tesztelés (az összetettnek nyilvánított Mersenne-számok esetén) nagyjából két évvel az első után, az elsődleges tesztelést végzőknél lassabb gépeken.[6]

4. És társaik?

4.1. Barátságos számok

Iamblikhosz személyesen Pithagorasznak tulajdonítja a barátságos számpárok „felfedezését”, aki a történet szerint a „Mi egy barát?” kérdésre azt válaszolta: „Másik én.”

4.1. Definíció. Az $a \neq b$ pozitív egészek barátságos számpárt alkotnak, ha $\sigma(a) = \sigma(b) = a + b$ (vagyis $s(a) = b$ és $s(b) = a$).

4.2. Állítás. *Egy barátságos számpár egyik tagja bővelkedő, a másik pedig hiányos szám.*

Bizonyítás. Legyen a és b barátságos számpár: $\sigma(a) = \sigma(b) = a + b$.

Ekkor a következők ekvivalensek:

$$\sigma(a) > 2a \Leftrightarrow a + b > 2a \Leftrightarrow b > a \Leftrightarrow 2b > a + b \Leftrightarrow 2b > \sigma(b),$$

tehát ha az egyik bővelkedő, akkor a másik hiányos, és viszont, hiszen a és b szerepe itt felcserélhető. Ha egyik sem hiányos vagy bővelkedő, akkor mindkettő tökéletes, de ekkor $\sigma(a) = \sigma(b) = 2a = 2b$, vagyis $a = b$, hiszen a tökéletes számok „önmagukkal barátságosak”, tehát ez már nem egy barátságos számpár. □

4.3. Állítás. *Barátságos számpár egyik tagja sem lehet kettőhatvány.*

Bizonyítás. Legyen a és b egy barátságos számpár. Ha $a = 2^k$ (ahol $k > 1$ egész), akkor $\sigma(a) = 2^{k+1} - 1$, és $a + b = \sigma(a) = \sigma(b)$ alapján

$$b = 2^{k+1} - 1 - 2^k = 2^k - 1.$$

Mivel b és $\sigma(b)$ is páratlan szám, ezért a 2.6 állítás szerint $b = t^2$ alakú, ahol t páratlan szám. $b = 2^k - 1 \equiv -1 \pmod 4$, míg egy páratlan szám négyzetére $t^2 \equiv 1 \pmod 4$ teljesül, tehát a kettő nem lehet egyenlő, így ellentmondásra jutottunk. □

Az ókori görögöktől nem maradt ránk a barátságos számokkal kapcsolatos tétel, az általuk ismert egyetlen barátságos számpár a 220 és a 284 volt. Szábit ibn Kurra kilencedik századi arab tudós volt az első, aki a barátságos számok (egy nem túl gyakori típusának) megtalálására vonatkozó szabályt közölt:

4.4. Tétel. *Legyen $n > 1$-re $p_n = 3 \cdot 2^n - 1$, $q_n = 9 \cdot 2^{2n-1} - 1$. Ekkor ha p_{n-1}, p_n és q_n prímszámok, akkor $a = 2^n \cdot p_{n-1} \cdot p_n$ és $b = 2^n \cdot q_n$ barátságos számpárt alkotnak.*

Bizonyítás. Mivel p_n és p_{n-1} páratlan prímek, $\sigma(a) = \sigma(2^n)\sigma(p_{n-1})\sigma(p_n) = = (2^{n+1}-1)(9 \cdot 2^{2n-1})$, és hasonlóan $\sigma(b) = \sigma(2^n)\sigma(q_n) = (2^{n+1}-1)(9 \cdot 2^{2n-1})$. Másfelől

$$\begin{aligned} a + b &= 2^n(3 \cdot 2^n - 1)(3 \cdot 2^{n-1} - 1) + 2^n(9 \cdot 2^{2n-1} - 1) = \\ &= 9 \cdot 2^{3n-1} - 3 \cdot 2^{2n} - 3 \cdot 2^{2n-1} + 2^n + 9 \cdot 2^{3n-1} - 2^n = \\ &= 2(9 \cdot 2^{3n-1}) - 3(2^{2n} + 2^{2n-1}) = 9 \cdot 2^{3n} - 3 \cdot 2^{2n-1}(2+1) = \\ &= 9 \cdot 2^{3n} - 9(2^{2n-1}) = (2^{n+1} - 1)(9 \cdot 2^{2n-1}), \end{aligned}$$

tehát $\sigma(a) = \sigma(b) = a + b$, vagyis a és b barátságos számpárt alkotnak. □

Fermat és Descartes egymástól függetlenül újra felfedezték ugyanezt a szabályt, és ennek segítségével találta meg 1636-ban Fermat a 17296 és 18416, illetve 1638-ban Descartes a 9363584 és 9437056 párt. Bár a barátságos számok története kapcsán néhány könyv csak nem említi és van, amelyik konkrétan tagadja[2], hogy az arabok ismertek volna egynél több barátságos számpárt, más források szerint viszont a Fermat-féle párt Ibn al-Banna és Kamál al-Dín al-Fáriszi is megtalálta már a tizennegyedik században, a Descartes-féle párt pedig Muhammad Baqir Yazdi fedezte fel először a tizenhatodik században.[7]

Euler később általánosította a fenti tételt, és több módszert is kidolgozott barátságos számpárok keresésére abból a tényből kiindulva, hogy az ismert párok egy közös osztó és további, hozzá relatív prím különböző prímek szorzataként álltak elő, megkülönböztetve az eseteket aszerint, hogy a közös osztón túl kettő-egy, kettő-kettő, kettő-több vagy több-több prím szerepelt-e a szorzatban. 1747-ben egy 30 párból álló listát tett közzé, amelyet később

64 eleműre bővített (ebből kettő hibás volt, egyet pedig félrenyomtattak). A módszeresen dolgozó matematikusok által mindaddig meg nem talált második legkisebb barátságos számpárt (1184 és 1210) a 16 éves Niccolò Paganini fedezte fel 1866-ban.

L. E. Dickson barátságos számhármasoknak nevezte az olyan számokat, amelyek közül bármely kettő valódi osztóinak az összege egyenlő a harmadik számmal, és megadott két különböző számokból álló ilyen számhármast, valamint nyolc olyat, amelyben a három számból kettő azonos.

4.2. Többszörösen tökéletes számok

4.5. Definíció. Azokat az n számokat, amelyekre $\sigma(n) = kn$, többszörösen (k-szorosan) tökéletes számoknak nevezzük.

A k-szorosan tökéletes számokat szokás P_k-val jelölni, P_2 tehát a tökéletes számokat jelenti. Az akkor egyedüliként ismert $P_3^{(1)} = 120$-on túl további többszörösen tökéletes számok és rájuk vonatkozó szabályok megtalálását mint kihívást először Marin Mersenne említette 1631-ben Descartes-nak írt levelében, de hét éven át nem kapott rá választ. Eközben Fermat megtalálta a másodikat ($P_3^{(2)} = 672$), André Jumeau a harmadikat ($P_3^{(4)} = 523776$), az ő kihívására válaszul pedig Descartes a negyediket ($P_3^{(4)} = 1476304896$). Nem sokkal később Descartes közzétett hat P_4-et és egy P_5-öt is, majd 1638. november 15-én megírta Mersenne-nek az általa megállapított szabályokat, amelyek a többszörösen tökéletes számok megtalálását segíthetik – közülük a második és a harmadik alkalmazásával talált rá az említett hat P_4-re az akkor már ismert négy P_3 alapján:

4.6. Állítás. *P_k k-szorosan tökéletes számokra teljesülnek a következők:*

I. Ha n egy P_3, amely nem osztható 3-mal, akkor $3n$ egy P_4.

II. Ha n egy P_3, amely osztható 3-mal, de nem osztható 5-tel és 9-cel, akkor $45n$ egy P_4.

III. Ha n egy P_3, amely osztható 3-mal, de nem osztható 7-tel, 9-cel és 13-mal, akkor $3 \cdot 7 \cdot 13n$ egy P_4.

IV. Ha n osztható 2^9-nel, de nem osztható a $2^{10}, 31, 43, 127$ számok egyikével sem, akkor $31n$ és $16 \cdot 43 \cdot 127n$ aránya megegyezik az osztóik összegének arányával.

V. Ha n nem osztható 3-mal és $3n$ egy P_{4k}, akkor n egy P_{3k}.

Bizonyítás. A fenti szabályok mind nagyon egyszerűen beláthatók:

I. Mivel $(3, n) = 1$, ezért $\sigma(3n) = 4 \cdot 3n$, tehát $3n$ valóban P_4.

II. Mivel n osztható hárommal, de nem osztható kilenccel, ezért $\sigma(n)$ szorzatként való felírásában szerepel az $(1 + 3) = 4$ tényező, ezzel elosztva $\sigma(n) = 3n$-t megkapjuk $\sigma(\frac{n}{3})$-t, amely már relatív prím a kilenchez, így $\sigma(45n) = \sigma(\frac{n}{3})\sigma(3 \cdot 45) = \frac{3n}{4} \cdot 40 \cdot 6 = 180n = 4 \cdot 45n$, tehát $45n$ valóban P_4.

III. Ugyanígy $\sigma(3 \cdot 7 \cdot 13n) = \frac{3n}{4} \cdot 13 \cdot 8 \cdot 14 = 1092n = 4 \cdot (3 \cdot 7 \cdot 13n)$, tehát ez a szám is egy P_4.

IV. Ugyanígy

$$\begin{aligned}\sigma(16 \cdot 43 \cdot 127n) &= \frac{\sigma(n)}{(2^{10} - 1)} \cdot (2^{14} - 1) \cdot 44 \cdot 128 = \\ &= \frac{\sigma(n)}{3 \cdot 11 \cdot 31} \cdot (3 \cdot 43 \cdot 127) \cdot (2^2 \cdot 11) \cdot 2^7 = \\ &= \frac{\sigma(n)}{31} \cdot 43 \cdot 127 \cdot 2^9 = \frac{1}{31} \cdot 43 \cdot 127 \cdot 16 \cdot 32 \cdot \sigma(n),\end{aligned}$$

tehát $\frac{\sigma(31n)}{\sigma(16 \cdot 43 \cdot 127n)} = \frac{32 \cdot \sigma(n)}{\frac{1}{31} \cdot 43 \cdot 127 \cdot 16 \cdot 32 \cdot \sigma(n)} = \frac{31}{16 \cdot 43 \cdot 127}$.

V. Eszerint $\sigma(3n) = \sigma(3)\sigma(n) = 4 \cdot 3kn \Rightarrow \sigma(n) = 3kn$, vagyis n egy P_{3k}. □

Mersenne a megtaláló neve nélkül közölte $P_3^{(5)}$-öt, majd Fermat 1643-ban az általa megtalált négyszeresen, ötszörösen és hatszorosan tökéletes számok mellett közölte $P_3^{(6)}$-ot is, ezzel megtalálta az utolsó háromszorosan tökéletes számot. Jelenleg összesen 5303 többszörösen tökéletes számot ismerünk (az eggyel mint egyedüli P_1-gyel és a 47 tökéletes számmal együtt) $k = 11$-ig, és valószínűleg $2 \neq k < 7$-re már minden P_k-t megtaláltak. Az 1 kivételével nem ismerünk páratlan többszörösen tökéletes számot.[8]

4.3. Szupertökéletes és kvázitökéletes számok

4.7. Definíció. Az n pozitív egészt szupertökéletesnek nevezzük, ha $\sigma(\sigma(n)) = 2n$.

4.8. Állítás. *Egy n páros szám akkor és csak akkor szupertökéletes, ha $n = 2^{p-1}$ alakú, ahol $2^p - 1$ prím. (Tehát a páros szupertökéletes számok is ugyanannyian vannak, mint a Mersenne-prímek.)*

Bizonyítás. 1. Egyértelműen látszik, hogy minden ilyen n szupertökéletes: $n = 2^{p-1} \Rightarrow \sigma(n) = 2^p - 1$, ami a feltétel szerint prím, tehát $\sigma(2^p - 1) = 2^p = 2 \cdot 2^{p-1} \Rightarrow \sigma(\sigma(2^{p-1})) = 2 \cdot 2^{p-1}$.

2. Legyen $n = 2^k t$ szupertökéletes szám, ahol t páratlan szám és k pozitív egész. Ekkor $\sigma(n) = (2^{k+1} - 1)\sigma(t)$, és mivel n szupertökéletes, $\sigma(\sigma(n)) = \sigma((2^{k+1} - 1)\sigma(t)) = 2^{k+1}t$. Összegezzük $\sigma(n)$ ismert osztóit! $(2^{k+1} - 1) \neq \sigma(t)$, mivel ellenkező esetben a szorzatuk egy páratlan szám négyzete, ennek osztóösszege pedig szintén páratlan szám lenne. Tegyük fel, hogy $\sigma(t) > 1$. Ekkor

$$\begin{aligned}\sigma(\sigma(n)) &\geq 1 + (2^{k+1} - 1) + \sigma(t) + (2^{k+1} - 1)\sigma(t) \geq \\ &\geq 2^{k+1} + (t + 1) + (2^{k+1}t + 2^{k+1} - t - 1) = 2^{k+1}t + 2^{k+2} > 2^{k+1}t,\end{aligned}$$

vagyis ellentmondásra jutottunk. Ebből következik, hogy $\sigma(t) = 1 \Rightarrow t = 1$ teljesül, tehát $n = 2^k$. Ekkor $\sigma(2^{k+1} - 1) = 2^{k+1}$, vagyis $2^{k+1} - 1$ prímszám. □

4.9. Állítás. *Egy páratlan szupertökéletes szám szükségképpen négyzetszám.*

Bizonyítás. A 2.6 állítás szerint egy páratlan n akkor és csak akkor négyzetszám, ha $\sigma(n)$ páratlan. Az állítás igazolásához tehát elég belátnunk, hogy páratlan n-re $\sigma(\sigma(n)) = 2n$ csak akkor teljesül, ha $\sigma(n)$ páratlan. Most tegyük fel, hogy nem az, vagyis $\sigma(n) = 2^k t$, ahol k pozitív egész. Mivel n szupertökéletes, ezért $\sigma(\sigma(n)) = \sigma(2^k t) = (2^{k+1} - 1)\sigma(t) = 2n$. Az utolsó egyenlőség mindkét oldalát elosztjuk kettővel, felhasználva, hogy mivel $2^{k+1} - 1$

páratlan, a jobb oldal viszont páros, ezért $\sigma(t) = 2z$ (ahol z pozitív egész). Így azt kapjuk, hogy $(2^{k+1} - 1)z = n$. Mivel feltettük, hogy $k > 0$, ezért $2^{k+1} - 1 \geq 3$, így $(2^{k+1} - 1)$ és z egyaránt valódi osztója n-nek, tehát $(2^{k+1} - 1)z + z = 2^{k+1}z = 2^k\sigma(t) \leq \sigma(n) = 2^k t$, ez pedig ellentmondás, hiszen $2^k\sigma(t) > 2^k t$ minden $t > 1$-re, tehát a $k > 0$ kiinduló feltevés hamis, ezzel az állítást beláttuk. □

Nem tudjuk, létezik-e egyáltalán páratlan szupertökéletes szám.

4.10. Definíció. Az n pozitív egészt kvázitökéletesnek nevezzük, ha egyenlő a nem triviális osztóinak összegével, vagyis $\sigma(n) = 2n + 1$.

Nem tudjuk, hogy létezik-e ilyen tulajdonságú n szám, de ha igen, akkor legalább hét különböző prímosztója van, és $n > 10^{35}$.

4.11. Állítás. *Ha létezik kvázitökéletes szám, az szükségképpen egy páratlan szám négyzete.*

Bizonyítás. A 2.6 állítás szerint $\sigma(n)$ csak $n = 2^\alpha t^2$ esetén lehet páratlan, tehát azt kell belátnunk, hogy ha $\sigma(n) = 2n+1$, akkor $\alpha = 0$. A kvázitökéletesség alapján $\sigma(2^\alpha t^2) = \sigma(t^2)(2^{\alpha+1}-1) = 2^{\alpha+1}t^2+1 = 2^{\alpha+1}t^2-t^2+(t^2+1)$, ez pedig átrendezés után ekvivalens azzal, hogy $(\sigma(t^2)-t^2)(2^{\alpha+1}-1) = t^2+1$. Ha $\alpha = 0$, akkor $2^{\alpha+1}-1 = 1$, egyébként $2^{\alpha+1}-1 \equiv -1 \pmod 4$. Tegyük fel, hogy $p = 4k - 1$ prímosztója $t^2 + 1$-nek, vagyis $t^2 \equiv -1 \pmod p$. A kis Fermat-tétel (3.8) miatt $t^{p-1} \equiv 1 \pmod p$, ugyanakkor $t^{p-1} = (t^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Mivel $p = 4k-1$, ezért $\frac{p-1}{2} = 2k-1$ páratlan szám, tehát az előzőekből $1 \equiv -1 \pmod p$ következne, ami nem teljesülhet semmilyen $p = 4k-1$ számra. Emiatt $t^2 + 1$-nek egyáltalán nem lehet $4k - 1$ alakú osztója, vagyis $\alpha \neq 0$ esetben ellentmondásra jutottunk. Ezért $\alpha = 0$ kell legyen, tehát a kvázitökéletes szám csak $n = t^2$ alakú lehet, ahol t páratlan szám. □

A fenti definícióhoz hasonlóan kvázibarátságos (vagy eljegyzett) számpárnak nevezik a $\sigma(m) = \sigma(n) = m + n + 1$ tulajdonságú $m \neq n$ számpárokat, mint például a 48 és a 75. Minden ismert kvázibarátságos számpár tagjai ellenkező paritásúak.

4.4. Érinthetetlen számok

4.12. Definíció. Azokat az n számokat, amelyekre az $s(x) = n$ függvénynek nincs megoldása, érinthetetlennek (*untouchable*) nevezzük.

Erdős Pál bebizonyította, hogy végtelen sok érinthetetlen szám van, vagyis a $\sigma(x)$-hez hasonlóan (ld. 2.8 állítás) az $s(x)$ értékkészletéből is végtelen sok szám kimarad.

Az első tíz érinthetetlen szám: $2, 5, 52, 88, 96, 120, 124, 146, 162, 178$. Az 5 az egyetlen olyan érinthetetlennek ismert szám, amely páratlan. Hogy az 5 érinthetetlen szám, könnyen látható, hiszen nem bontható 1 és különböző prímek és szorzataik összegére: $4 = 1 + 3 = 2 + 2$ (ha 4 osztója lenne, akkor 2 is, ugyanaz az osztó kétszer viszont nem szerepelhet).

Az a sejtés, hogy egyáltalán nem is létezik másik páratlan érinthetetlen szám. Ez az állítás (hétnél nagyobb számokra) következne abból, ha feltesszük, hogy minden hatnál nagyobb páros szám előáll két különböző prímszám összegeként (ez a páros Goldbach-sejtésnek, miszerint minden páros szám előáll két prímszám összegeként, egy erősebb változata). Ekkor ugyanis bármely $2k + 1 > 7$ páratlan számra van olyan p, q prím, hogy $p + q = 2k$ és $s(pq) = 1 + p + q = 2k + 1$, vagyis pq megoldása lesz az $s(x) = 2k + 1$ függvénynek.

Ezzel kizártuk a hétnél nagyobb páratlan számokat, a többit pedig egyszerűen ellenőrizhetjük: $7 = 1+2+4 = s(8)$; 5-ről láttuk, hogy értinthetetlen; $3 = 1 + 2 = s(4)$.

$n = 1$ esetben nemcsak hogy létezik megoldása az $s(x) = n$ függvénynek, de könnyen beláthatjuk, hogy csak $n = 1$ esetén létezik végtelen sok megoldása: egyértelmű, hogy $s(p) = 1$ minden p prímszámra, tehát $n = 1$-re végtelen sok megoldás létezik; bármely $n > 1$ szám esetén viszont $(n - 1)$ csak véges sok módon bontható a megoldást egyértelműen meghatározó nem triviális osztók összegére.

Természetesen nemcsak $n = 1$-re létezik több megoldás, $n = 8$-ra például a $7 = 0+7 = 1+6 = 2+5 = 3+4$ felbontási lehetőségek közül pontosan kettő ad prímeket (és egy sem különböző prímek vagy prímhatványok összegét): a

7 és a $2 + 5$, így az $s(x) = 8$ két megoldása 49 és 10. Ez a tény teszi lehetővé a következő pontban tárgyalt osztóösszeg-sorozatok közt a különbözően kezdődő, de azonos elemet tartalmazó (és így onnantól ugyanúgy folytatódó) sorozatok, így többek közt a nem tisztán periodikus osztóösszeg-sorozatok létezését.

4.5. Osztóösszeg-sorozatok

4.13. Definíció. Az $a_0 = n$, $a_k = s(a_{k-1})$ $(k = 1, 2, ...)$ sorozatot az n osztóösszeg-sorozatának (*aliquot sequence*) nevezzük.

Ez a sorozat háromféleképp viselkedhet:

1) A sorozat véget ér, ha valamely a_k-ra $a_{k+1} = s(a_k)$ prímszám, ekkor $a_{k+2} = 1$, $a_{k+3} = 0$-ra pedig az osztóösszeg-függvény már nem értelmezhető.

2) A sorozat t szerint periodikus, ha van olyan k_0, hogy $\forall k \geq k_0$: $a_{k+t} = a_k$. A sorozat *tisztán periodikus*, ha $k_0 = 0$. Ekkor $t = 1$ esetén n tökéletes szám, $t = 2$ esetén n és $s(n)$ barátságos számpárt alkotnak. $t > 2$ esetén a tisztán periodikus osztóösszeg-sorozatot t-edrendű osztóösszeg-körnek (*aliquot cycle*), tagjait szociális számoknak (*sociable numbers*) nevezzük. Az első két ilyen $t > 2$ osztóösszeg-kört P. Poulet tette közzé 1918-ban ($t = 5$ és $t = 28$), majd ötven évvel később H. Cohen bővítette a listát kilenc negyedrendű körrel. Ugyanekkor közölte a sejtést, hogy a negyedrendű osztóösszeg-körök száma végtelen. A jelenleg ismert 217 kör közül 206 negyedrendű (a továbbiak: $t = 5 : 1$; $t = 6 : 5$; $t = 8 : 3$; $t = 9 : 1$; $t = 28 : 1$).[9]

3) A sorozat nem korlátos. Megoldatlan probléma, hogy létezik-e nem korlátos osztóösszeg-sorozat: Catalan és Dickson sejtése szerint nincs, későbbi megállapítások arra utalnak, hogy valószínűbb, hogy van. A legkisebb n, amelyhez még nem találták meg a sorozat végét (tehát akár végtelen is lehet), a 276 – osztóösszeg-sorozatának már több mint 1700 eleme ismert, közülük az utolsók 180 számjegyűek.[10]

Az osztóösszeg-sorozatok viselkedésének szemléltetésére készítettem egy egyszerű C++ programot, amelynek programkódja a dolgozat mellékletét képezi. A program a felhasználó által megadott n számot egyszerű osztással bontja prímtényezőkre ([11] Prímfelbontás c. fejezetében leírt „A algoritmus" alapján), majd ennek alapján kiszámítja a $\sigma(n)$ osztóösszeget, azonosítja a többszörösen tökéletes számokat, megadja az osztóösszeg-sorozat első néhány elemét, és amennyiben ennyi elem alapján lehetséges, beazonosítja a sorozat viselkedését is. Itt a következő variációk lehetségesek:

0) Az osztóösszeg-sorozatot nem sikerül a fenti kategóriák valamelyikébe besorolni, ha a számítás valamilyen korlát miatt leáll, mielőtt a sorozatban ismétlődő elem vagy prímszám következne. (A program által adott válasz ekkor „*This aliquot sequence does not terminate under <b>.*", illetve „*We cannot determine the behaviour of this aliquot sequence from the first <k> elements.*") Az elemszámra vonatkozó k korlátot a felhasználó határozhatja meg a program futtatásának kezdetén. A vizsgálható számok nagyságára vonatkozó b korlát elsősorban a forrásfájlból beolvasott prímlistától függ.

1) A program 1-ig folytatja a prímszámot tartalmazó osztóösszeg-sorozatok kiírását. („*This aliquot sequence terminates in 1 after <k> elements.*")

2) Periodikus sorozatok elemeit az első periódus végéig adja meg, megkülönböztetve tökéletes („*<n> is a perfect number.*"), barátságos („*<n> and <m> are members of an amicable pair.*") és szociális számokat („*<n> is a member of an aliquot cycle of <k> elements.*"), valamint a nem tisztán periodikus sorozatokat. („*This aliquot sequence is periodic of period <t>, but not purely periodic.*")

3) A nem korlátos osztóösszeg-sorozatok, amennyiben léteznek, természetesen a 0. választ váltják ki.

Irodalomjegyzék

Hivatkozások

[1] WEIL, André: *Number Theory. An approach through history from Hammurapi to Legendre.* Boston–Basel–Stuttgart: Birkhäuser, 1984.

[2] ORE, Oystein: *Number Theory and its History.* New York–Toronto–London: McGraw-Hill Book Comp., 1948.

[3] EUKLIDÉSZ: *Elemek.* Budapest: Gondolat, 1983.

[4] WAERDEN, B. L. van der: *Science Awakening.* Groningen: P. Noordhoff, 1954.

[5] *Odd Perfect Number Search.* A hozzáférés módja: http://oddperfect.org/against.html (A letöltés ideje: 2012. november 30.)

[6] *Mathematics and Research Strategy – GIMPS.* A hozzáférés módja: http://www.mersenne.org/various/math.php (A letöltés ideje: 2012. november 20.)

[7] COSTELLO, Patrick J.: New Amicable Pairs of Type (2,2) and Type (3,2). *Mathematics of Computation*, vol. 72 (2003), no. 241, pp. 489–497.

[8] *The Multiply Perfect Numbers Page.* A hozzáférés módja: http://wwwhomes.uni-bielefeld.de/achim/mpn.html (A letöltés ideje: 2012. november 12.)

[9] *A List of Aliquot Cycles of Length Greater Than 2 (by David Moews).* A hozzáférés módja: http://djm.cc/sociable.txt (A letöltés ideje: 2012. november 7.)

[10] *Factordb adatbázis.* A hozzáférés módja: http://factordb.com (A használat ideje: 2012. november 7.)

[11] KNUTH, Donald E.: *A számítógép-programozás művészete. 2. köt.: Szeminumerikus algoritmusok.* Budapest: Műszaki Könyvkiadó, 1994.

Felhasznált irodalom – nyomtatott források

[12] BEILER, Albert H.: *Recreations in the Theory of Numbers. The Queen of Mathematics Entertains.* New York: Dover Pub., 1966.

[13] COHEN, Henri: On Amicable and Sociable Numbers. *Mathematics of Computation*, vol. 24 (1970), no. 110, pp. 423–429.

[14] DICKSON, L. E.: *History of the Theory of Numbers. Vol. 1: Divisibility and Primality.* New York: Chelsea Pub. Comp., 1952.

[15] EVES, Howard W.: *An Introduction to the History of Mathematics.* Philadelphia: Saunders College Pub., 1990.

[16] FREUD Róbert, GYARMATI Edit: *Számelmélet.* Budapest: Nemzeti Tankönyvkiadó, 2006.

[17] GUY, Richard K.: *Unsolved Problems in Intuitive Mathematics. Vol. 1: Unsolved Problems in Number Theory.* New York–Berlin–Paris: Springer Verlag, 1994.

[18] HEALTH, Thomas, Sir: *A History of Greek Mathematics. Vol. 1: From Thales to Euclid.* New York: Dover Pub., 1981.

[19] KATZ, Victor J.: *A History of Mathematics. An introduction.* Reading: Addison-Wesley, 1998.

[20] SHANKS, Daniel: *Solved and Unsolved Problems in Number Theory.* New York: Chelsea Pub. Comp., 1978.

[21] SIERPIŃSKI, Wacław: *Elementary Theory of Numbers.* Warszawa: Państwowe Wydawnictwo Naukowe, 1964.

[22] SIMMONS, George F.: *Calculus Gems. Brief Lives and Memorable Mathematics.* New York–Toronto–London: McGraw-Hill Book Comp., 1992.

Felhasznált irodalom – internetes források

[23] *Chapter XIX of the Preface of Cogitata Physico-Mathematica by Marin Mersenne.* A hozzáférés módja: http://primes.utm.edu/mersenne/LukeMirror/lit/lit_069s.htm (A letöltés ideje: 2012. október 23.)

[24] *How GIMPS Works – GIMPS.* A hozzáférés módja: http://www.mersenne.org/various/works.php (A letöltés ideje: 2012. november 27.)

[25] *Mersenne Primes: History, Theorems and Lists.* A hozzáférés módja: http://primes.utm.edu/mersenne/index.html (A letöltés ideje: 2012. október 23.)

[26] *P-1 Factorization Method – Mersennewiki.* A hozzáférés módja: http://mersennewiki.org/index.php/P-1 (A letöltés ideje: 2012. november 20.)

[27] *Perfect, Amicable and Sociable Numbers (by David Moews).* A hozzáférés módja: http://djm.cc/amicable.html (A letöltés ideje: 2012. november 7.)

[28] *The Mersenne Newsletter, issue #13 (February 2, 1998)* A hozzáférés módja: http://www.mersenne.org/newsletters/news13.txt (A letöltés ideje: 2012. október 23.)