Tökéletes számok

Készítette: Takács Bendegúz

Számelmélet algoritmikus problémái - Prímteszt

- **Prímteszt**en a matematikában vagy informatikában olyan (determinisztikus) algoritmust vagy indeterminisztikus (például valószínűség-elméleti) módszereket is megengedő eljárást értünk,
- melynek ismeretében bármely adott egész számról, vagy csak bizonyos típusú számokról (véges sok lépésben) el tudjuk dönteni, hogy prímszám-e, vagy pedig összetett.
- A Prímtesztelés eddig ismert és használt algoritmusai:
  - Wilson-prímteszt
  - Fermat-prímteszt
  - A Solovay–Strassen-teszt
  - **AKS-algoritmus (2001) – legelső polinomiális. gyors algoritmus!!!!**
  - BPSW-teszt
  - …

Számelmélet algoritmikus problémái - Prímfelbontás

- **Prímfelbontás** az a folyamat, amikor egy összetett számot prím osztóira törzstényezőire bontjuk.
- A törzstényezők szorzata az eredeti egész számmal egyenlő. Az eljárás eredménye prímhatványok szorzata. Ezt a formulát az eredeti szám kanonikus alakjának nevezzük.
- A számelmélet alaptétele szerint minden 1-nél nagyobb pozitív egész szám egyértelműen, azaz egy és csak egyféleképpen bontható fel prímszámok szorzatára.
- Nagy számok esetében nem ismerünk minden esetben hatékony algoritmust a prímtényezőkre bontásra:
  - nemrégiben egy az RSA-eljárás által kiírt pályázaton mintegy másfél évet, és kb. fél évszázadnyi gépidőt vett igénybe egy 200 jegyű szám felbontása.

Számelmélet egyéb híres problémái

- Ikerprímek
  - két olyan prímszám együttesét nevezzük, amelyek 2-vel térnek el egymástól
- Goldbach sejtés
  - Minden 5-nél nagyobb páratlan szám előáll három prímszám összegeként.
- Nagy Fermat Sejtés/Tétel
  - Az $a^n + b^n = c^n$ diofantoszi egyenletnek nincs megoldása 2-nél nagyobb egész n esetén a nemnulla egész számok körében.
- Mersenne prímek
  - a kettő-hatványnál eggyel kisebb, azaz a $2^n - 1$ alakban felírható prímszámokat, ahol *n* szintén prímszám.
- …

https://en.wikipedia.org/wiki/List_of_unsolved_problems_in_mathematics#Number_theory

Mi ezekben a közös?

- könnyű megérteni a problémát
- megoldani szinte lehetetlen, több ezer év alatt sem sikerült
- egyelőre csak játék, de később vagy napjainkban létfontosságú lesz megfejtésük (titkosírások, kódolások, tömörítések…)



Mik a tökéletes számok?

- A számelméletben **tökéletes számnak** nevezzük azokat a természetes számokat, amelyek megegyeznek az önmaguknál kisebb osztóik összegével.
- Tökéletes szám minden olyan n egész, amelyre az
  - Osztóösszeg-függvény $\sigma(n) = 2n$
  - Valódi osztók összege $s(n) = \sigma(n) - n = 2n - n = n$
- A társas számok speciális esetei.
  - olyan pozitív egész számok, melyek osztóösszeg-sorozatában osztóösszeg-kör található; tehát az elejétől kezdve állandóan egy periódus ismétlődik. A tökéletes számok esetében a periódus 1.
  - Pl.: 6=1+2+3=6

Egy kis történelem

- A definíció az ókorból származik, már **Eukleidész: Elemek** c. művében is megjelenik (VII.22).
- Eukleidész meghatározott egy képzési szabályt:
  - Ha $2^p - 1$ prím, akkor $2^{p-1}(2^p - 1)$ tökéletes szám.
- **Nicomachus (60 – 120)** görög matematikus az alábbi pontokat sejtette:
  - Az *n*-edik tökéletes szám n hosszú szám.
  - Minden tökéletes szám páros.
  - Minden tökéletes szám 6-al, illetve 8-al végződik felváltva.
  - Az Euklideszi képzési szabály által kapott számok között az összes tökéletes szám megtalálható.
  - Végtelen sok tökéletes szám van.
- Az első négy tökéletes számot már a görögök is tudták.
- (1=6 , 2=28 , 3=496 , 4=8128)

Egy kis történelem

- Egy egyiptomi matematikus, **Ismail ibn Fallūs (1194–1252)**, feljegyezte a következő 3 tökéletes számot
  - 33,550,336
  - 8,589,869,056
  - 137,438,691,328
- Az első Európai említések az ötödik számról egy 1456 és 1461 közötti feljegyzésben lelhetők meg egy ismeretlen matematikustól.

Egy kis történelem

- 1588-ban, az olasz matematikus, **Pietro Cataldi(1548-1626)**, feljegyezte a hatodik (8,589,869,056), illetve hetedik (137,438,691,328) tökéletes számot, és bebizonyította, hogy az Euklideszi képzési szabály által kiszámolt tökéletes számok 6-al és 8-al végződnek.
- Jóval később **Euler (1707-1783)** igazolta, hogy az összes páros tökéletes szám ebben az alakban ($2^{p-1}(2^p-1)$) írható fel.
- Ez az **Eukleidész–Euler-tétel**.

Euklidész IX/36. tételének bizonytása

Legyen tehát k olyan pozitív egész szám, amelyre a k darab tagból áll

$$1 + 2 + 2^2 + \ldots + 2^{k-1} = 2^k - 1 = p$$

Összeg értéke prímszám. Az

$$n = p \cdot 2^{k-1}$$

számról kell megmutatni, hogy tökéletes.
A fenti n szám n-nél kisebb pozitív osztói:

$$1, 2, 2^2, \ldots, 2^{k-2}, 2^{k-1},$$

Továbbá

$$p, 2p, 2^2p, \ldots, 2^{k-2}p,$$

ezek összegének egyik része

$$1 + 2 + 2^2 + \ldots + 2^{k-1} = 2^k - 1 = p$$

másik része pedig

$$1 \cdot p + 2 \cdot p + 2^2 \cdot p + \ldots + 2^{k-2} \cdot p = (2^{k-1} - 1) \cdot p$$

Így az osztók összege mindösszesen

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

azaz n tényleg tökéletes.

(Forrás:Freud Róbert : Ősi problémák - új eredmények (Számelmélet, prímszámok) Ismeretterjesztő előadás a Fazekas M. Gimnáziumban, 2005. november 22.)

Páros prím számok, Mersenne-prímek

- Az ókori görög matematikus, Eukleidész felfedezte, hogy az első négy tökéletes szám felírható $2^{n-1}(2^n - 1)$ alakban:
- n = 2-re: $2^1(2^2 - 1) = 6$
- n = 3-ra: $2^2(2^3 - 1) = 28$
- n = 5-re: $2^4(2^5 - 1) = 496$
- n = 7-re: $2^6(2^7 - 1) = 8128$
- Észrevéve, hogy a fent említett n-ekre $2^n - 1$ minden esetben prímszám, Eukleidész bebizonyította, hogy minden olyan esetben, amikor $2^n - 1$ prím, $2^{n-1}(2^n - 1)$ tökéletes szám.
- Az is megmutatható, hogy **ha $2^n - 1$ prím, akkor n is az**, de fordítva nem feltétlenül igaz. Azokat a prímeket, amelyek felírhatók $2^n - 1$ alakban, Mersenne-prímeknek nevezzük a 17. században élt francia szerzetes, **Marin Mersenne (1588-1648)** után.

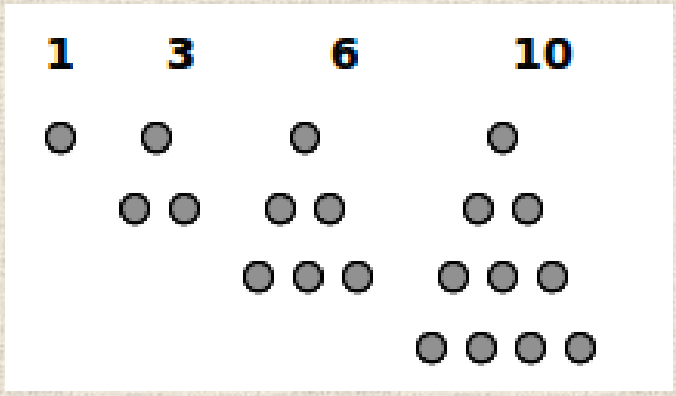
https://hu.wikipedia.org/wiki/T%C3%B6k%C3%A9letes_sz%C3%A1mok

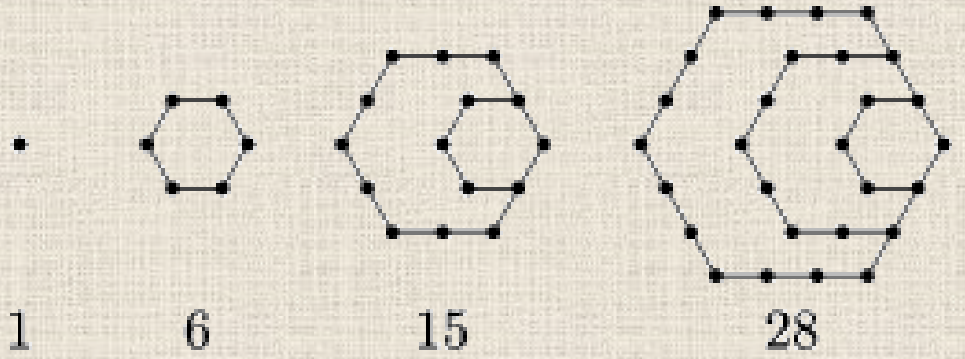
További érdekességek, kisebb eredmények

- A tökéletes számok osztóinak (az 1-et és saját magukat is beleszámítva) reciprok értékeit összeadva mindig 2 lesz az eredmény. Pl. 28 esetében:
- $\frac{1}{28}+\frac{1}{14}+\frac{1}{7}+\frac{1}{4}+\frac{1}{2}+\frac{1}{1}=2$
- Az ismert többjegyű tökéletes számok tizes számrendszerbeli számjegyeit egymással összeadva, majd az eredmény számjegyeit újra összeadva, mindaddig amíg egy számjegyet kapunk, mindig 1 lesz a végeredmény.
  - Vagyis a 6-ot leszámítva mindegyik kilences maradéka 1_{10}. Pl. a 496_{10} esetében: 4+9+6=19, 1+9=10, 1+0=1
- A tökéletes számok (a 6-ot kivéve) a hatos számrendszerben két 4-esre végződnek.
  - Pl.: $28_{10}=44_6$

További érdekességek

- A $2^{p-1}(2^p - 1)$ alak mellett minden tökéletes szám egyben a $(2^p - 1)$-edik háromszögszám
  - Olyan szám, amely megegyezik 2^p -1-ig vet természetes számok összegével
  - Ábrázolási szempontból felfogható olyan számként amely darab kőből kirakható egy egyenlő szárú háromszög
- 2^{p-1}-edik hatszögszám.
  - Az *n*-edik hatszögszám h_n a közös csúcsból rajzolt, legfeljebb *n* pont oldalhosszúságú szabályos hatszögek körvonalai egymástól *különböző* pontjainak száma.





További érdekességek

- Továbbá, minden páros tökéletes szám a hat kivételével a $((2^p + 1)/3)$-adik középpontos kilencszögszám
  - Az *n*-edik kilencszögszám, K_n a közös csúcsból rajzolt, legfeljebb *n* pont oldalhosszúságú szabályos kilencszögek körvonalai egymástól *különböző* pontjainak száma.
- és megegyezik az első $2^{(p-1)/2}$ páratlan köbszám összegével
  - A köbszámok, az $n^3 = n \cdot n \cdot n$ alakban írható számok, ahol *n* egész.
- A $2^{p-1}(2^p - 1)$ alakból következően minden páros tökéletes szám bináris alakban úgy néz ki, hogy p 1-est $p - 1$ nulla követ:
- $6_{10} = 110_2$, $28_{10} = 11100_2$, $496_{10} = 111110000_2$

További érdekességek

- Ezért minden tökéletes szám Hamming-súlya prímszám.
  - a sorozat azon karaktereinek száma, amelyek különböznek a zérószimbólumtól.
- Minden tökéletes szám egyben praktikus szám.
  - Olyan szám, amelynél az egymástól különböző osztóinak összegével az összes nála kisebb pozitív egész szám kifejezhető.
- Valamennyi tökéletes szám osztóharmonikus szám
  - tehát olyan pozitív egész szám, melynek osztóiból harmonikus közepet képezve egész számot kapunk.

Páratlan tökéletes számok

- Nyitott kérdés, hogy léteznek-e páratlan tökéletes számok.
- Számos eredmény született ebben a témában, de egyik sem mutatott rá egy páratlan tökéletes számra vagy cáfolta ezek létezését.
- Többen vélik úgy heurisztikus érvek alapján, hogy páratlan tökéletes számok nem léteznek.
- Minden tökéletes szám Ore-szám (osztóharmonikus) is, és egy sejtés szerint páratlan Ore-számok szintén nem léteznek.
  - Ore-szám:olyan pozitív egész szám, melynek osztóiból harmonikus közepet képezve egész számot kapunk.

Páratlan tökéletes számok

- Bármely páratlan N tökéletes számnak a következő feltételeknek kell eleget tennie:
- $N > 10^{1500}$.
- N nem osztható 105-tel.
- $N \equiv 1 \pmod{12}$ vagy $N \equiv 117 \pmod{468}$ vagy $N \equiv 81 \pmod{324}$.
- N felírható a következő alakban: $N = q^{\alpha} {p_1}^{2e_1} \ldots {p_k}^{2e_k}$
- ahol:
  - q, p1, ..., pk különböző prímszámok (Euler).
  - $q \equiv \alpha \equiv 1 \pmod{4}$ (Euler).
  - N legkisebb prímtényezője kisebb mint (2k + 8) / 3.
  - Vagy $q^{\alpha} > 10^{62}$, vagy $p\, j^{2ej} > 10^{62}$ néhány j-re.
  - $N < 2^{4^{k+1}}$.

Páratlan tökéletes számok

- N legnagyobb prímtényezője nagyobb mint 108.
- A második legnagyobb prímtényező nagyobb mint 104, a harmadik legnagyobb pedig nagyobb mint 100.
- N-nek legalább 101 prímtényezője van, ezek közül legalább 10 különböző.
- Ha a 3 nincs N prímtényezői között, akkor N-nek legalább 12 különböző prímtényezője kell legyen.

Források

- School of Mathematics and Statistics University of St Andrews, Scotland Perfect Numbers:
  - http://mathshistory.st-andrews.ac.uk/HistTopics/Perfect_numbers.html?fbclid=IwAR2DtL6j4ZZqk0v8y7MTmIrojEiwbu8Fx7ibpT_aV_ZLxrPHG5YXrW8ExFY#s14
- Wikipedia: Perfect Numbers
  - https://en.wikipedia.org/wiki/Perfect_number
- Wikipedia: AKS primality test
  - https://en.wikipedia.org/wiki/AKS_primality_test
- Wikipedia: Tökéletes számok
  - https://hu.wikipedia.org/wiki/T%C3%B6k%C3%A9letes_sz%C3%A1mok
- Wikipedia: Hamming weight (Hamming súly)
  - https://en.wikipedia.org/wiki/Hamming_weight
- Wikipedia: Sociable Number (Páros számok)
  - https://en.wikipedia.org/wiki/Sociable_number
- Wikipedia: List of unsolved problems in Number Theory (Számelmélet megoldatlan problémái)
  - https://en.wikipedia.org/wiki/List_of_unsolved_problems_in_mathematics#Number_theory
- Freud Róbert : Számelmélet (2014)
  - https://regi.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_519_Szamelmelet/index.html
- Freud Róbert : Ősi problémák - új eredmények (Számelmélet, prímszámok) Ismeretterjesztő előadás a Fazekas M. Gimnáziumban, 2005. november 22.
  - Az előadás alapján a cikket írták:
  - Balogh Máté, Nagy Dániel és Hraskó András

Köszönöm a figyelmet!