Barangolás a számolástechnika határvidékein

Pethő Attila

Debreceni Egyetem, Informatikai Kar

Debreceni Akadémiai Bizottság Közgyűlése

Debrecen, 2011. február 23.

A matematika természete

Azért van valami lebilincselő a kétségbevonhatatlan kijelentésben, hogy a világegyetem nem kizárólag egy entrópia-meddőhányó létrehozásával foglalkozik, hanem időnként és helyenként olyan lenyűgöző antientropikus képződményekben fejezi ki magát, mint amilyenek a *kettős pulzárok és a matematikusok*.

(Timothy Ferris)

A matematika antientropikus, de a matematikusok nem!

MOSESNEC NEGYEDIC KÖNYVE, KIT KÖZ NEWEL MAGYAROL, AZ IZRAELITAKNAC MEG SZAMLALASOKROL VALO KŐNYVNEC NEVEZNEC.

Meg iria Moſes ez kőnyvben, az ki iőueteltől fogua az máſodic eſtendőnec máſodic hólnapiától fogua, mind az negyuenedic eſtendőnec tizen egy edic hólnapiáig való lett dolgokat, és töruényeknec rendeléſét az Iſten néppe között. Az az, bé foglallya harmintz nyóltz eſtendónec és egy néhány hólnapnac hiſtoriáiát, Num: 1. Deutr: 1.

I. Réſz.

¶ Meg paranczollya Iſten az Moſesnec. Hogy minden nemzetſégből egy egy fő embert véuén melléie, meg ſámlállya az Aaron Pappal az Izraelnec egéſz nemzetſégét. Meg ſámlállya azért Moſes az Iſten paranczolattya ſerint az népet, az kic vóltac hús eſtendősőc és annál nagyobbac. De meg parantſollya az Iſten, hogy az Leui nemzetſégét ne ſámlallya az Izraelitác közzé, hanem azokra bizza az Iſten ſátorának és minden ahoz való ſerſámoknac gondgyat.

1. SZóllá pedig az WR Moſesnec, az Sinai puztaiában à gyülekőzetnec ſátorában, az máſodic eſtendőben Ægyptusból való ki iőuetel után, monduán.

2 Vegyétec ſámát az egéſz Izrael fiainac gyülekezetinec, az ő nemzetſégec ſierint, az Attyáknac házoc ſierint, az neueknec ſámoc ſierint, minden férfiat az ő feiec ſierint.

3 Húſz eztendős fiutól foguán és fellyeb, minden ki az hadba ki mehet az Izraelben: Meg ſámlállyátoc őket az ő ſeregőc ſierint, te és az Aaron.

4 Es légyen veletec egy egy férfiu minedenic nemzetſégből, mellyec közzül mindenic feie légyen az ő Attyoc házának.

5 Ezec pedig az férfiaknac neuec, az kic legyenec ti veletec: Ruben nemzetſégéből, Eliſur: Sedeurnac fia.

6 Simeonból, Selumiel: Suriſaddinac fia.

7 Iehudahbol, Nahſon: Aminadabnac fia.

8 Iſacharból, Nethanel: Suarnac fia.

9 Zebulunból, Eliab: Helonnac fia.

10 Ioſephnec fiai közzől: Az Ephraimból, Eliſamá: Ammihudnac fia. Manaſſehből, Gamliel: Pedahſurnac fia.

11 Beniaminból, Abidan: Gidioninac fia.

Bibliai népszámlálás

Vegyétek számba Izráel fiainak egész gyülekezetét, az ő nemzetségeik szerint, az ő atyáiknak háznépe szerint, a neveknek száma szerint, minden férfiút főről-főre.

Mózes IV. könyve I.1.

A népszámlálás a korabeli számolástudomány egyik csúcsteljesítménye.

Törzs neve	Törzs létszáma	Tábor létszáma
Rúben	46 500	
Simeon	59 300	151 450
Gád	45 650	
Júda	74 600	
Izsakhár	54 400	186 400
Zebulon	57 400	
Efraim	40 500	
Manasse	32 200	108 100
Benjámin	35 400	
Dán	62 700	
Áser	41 500	157 600
Nafthali	53 400	
Izráel fiai összesen		603 550

Nagy prímszámok

- Tökéletes szám: megegyezik osztóinak összegével. Pl.: $6 = 1 + 2 + 3$ és $28 = 1 + 2 + 4 + 7 + 14$.
- Eukleidész: egy páros szám akkor és csakis akkor tökéletes, ha $2^{p-1}(2^p - 1)$ alakú, ahol, p és $2^p - 1$ is prímszámok.
- Például a 2, a $3 = 2^2 - 1$ és a $7 = 2^3 - 1$ prímszámok, így $6 = 2 \cdot 3$ és $28 = 4 \cdot 7$ tökéletes számok.

Mersenne prímek

- A $2^p - 1$ alakú prímszámokat Mersenne prímeknek nevezzük.

- Kézi számolással ellenőrizhető, hogy $2^p - 1$ prímszám $p = 5, 7, 13, 17, 19$-re, de $2^{11} - 1 = 2047 = 23 \cdot 89$ nem.

L. Euler (1772)

$$2^{31} - 1 = 2\ 147\ 483\ 647$$

prímszám.

Peter Barlow (1811): " [it] is the greatest perfect number known at present, and probably the greatest that ever will be discovered; for, as they are merely curious without being useful, it is not likely that any person will attempt to find one beyond it."

Barlow nagyot tévedett, mert:

- Az embereket az is érdekli, ami nem hasznos!
- E. Lucas (1876) felfedezett egy nagyon hatékony módszert Mersenne számok prímtulajdonságának tesztelésére;
- a XX. sz. közepétől az elektronikus számítógépeken a Lucas-féle tesztet hatékonyan lehetett implementálni;
- A. Schönhage és V. Strassen (1971) a hagyományos szorzási algoritmusnál sokkal gyorsabb szorzási eljárást dolgoztak ki;
- a szuperkomputerek és a hálózatra kapcsolt számítógépek (cloud computing) igen nagy számítási erőt szolgáltatnak.

Ma már 47 Mersenne prímszámot ismerünk, a legnagyobb

$$2^{43\ 112\ 609} - 1.$$

Ez egy $12\ 978\ 189$ decimális jegyű, 3000 nyomtatott oldal(!) szám. A GIMPS (Great Internet Mersenne Prime Search) csoport találta 2008-ban.

Néhány hazai eredmény

- Gesztelyi Ernő és Jékel Pál (1976) tetszőleges nagyságú egész számokkal való számolásra dolgoztak ki algoritmust.
- Járai Antal 1994-től többször is vezette a legnagyobb ikerprímek listáját. A legnagyobb általuk talált párnak 51780 számjegye van (2007):

$$194772106074315 \cdot 2^{171960} \pm 1.$$

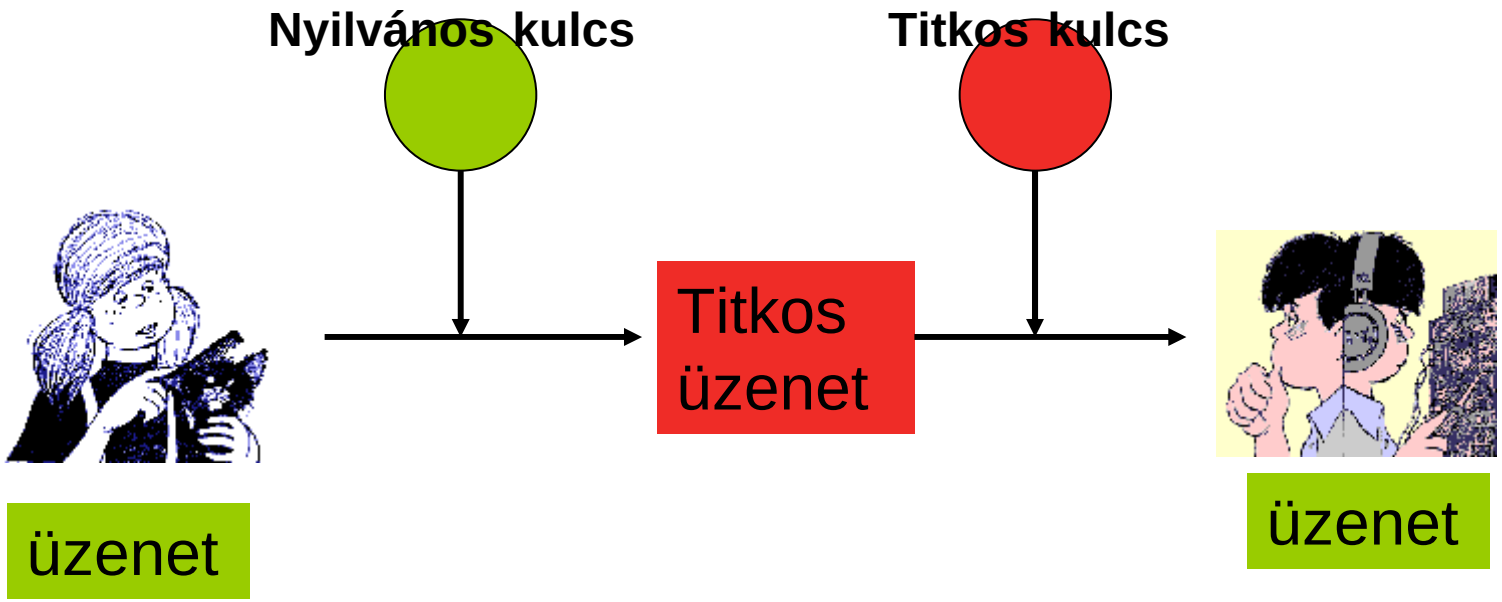
- PrimeGrid (2009) átvette a vezetést a 100355 decimális jegyű ikerprímmel:

$$65516468355 \cdot 2^{333333} \pm 1.$$

Kriptográfiai alkalmazások

- A számelmélet a tiszta (haszontalan) matematika mintapéldánya volt. Godfrey Hardy (1940): "I have never done anything useful. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world."
- Ő az egyik felfedezője a Hardy-Weinberg népességgenetikai szabálynak!
- 1976-ban drámai változás: Whitfield Diffie és Martin E. Hellman megfogalmazza a nyilvános kulcsú titkosítás elvét.

Nyilvános kulcsú vagy asszimmetrikus titkosítás



RSA

- Ronald Rivest, Adi Shamir és Leonard Adleman (1978)
- p, q nagy prímszámok, $n = pq$.
- $\varphi(n) = (p-1)(q-1)$. $1 < e < \varphi(n)$, amelynek $\varphi(n)$-nel nincs 1-től különböző közös osztója.
- $1 < d < \varphi(n)$, hogy ed-t a $\varphi(n)$-nel osztva 1 maradékot kapjon.
- Aladár nyilvános kulcsa az (e, n) pár, titkos kulcsa pedig a (d, n) pár.

Kriszta az M bizalmas üzenetet küldi Aladárnak.

$-$ Először M-et bináris számmá alakítja, majd kiszámítja M^e maradékát n-nel osztva, amit jelöljön T. Elküldi T-t Aladárnak.

$-$ Aladár kiszámolja T^d maradékát n-nel osztva és így visszanyeri M-et.

• A biztonságos RSA kulcs legalább 1024 bites, ami legalább 256 karaktert, azaz 3 gépelt sort jelent $\rightarrow$ a legtöbb ember képtelen memorizálni.

- A kriptográfia eredményei teszik lehetővé:

– csak mi férhessünk hozzá bárhonnan az otthoni számítógépünkön tárolt információkhoz;

– otthonról hajthassunk végre banki tranzakciókat;

– elektronikusan lehessen adóbevallást benyújtani és elektronikusan lehessen dokumentumokat közhiteles módon aláírni.

– szerencsejátékok: lottó, puttó, stb.

- Folláth János, Huszti Andrea és Pethő Attila, DESignin (2005): Az Informatikai Kar tanácsának tagjai RSA azonosító használatával érhetik el a bizalmas dokumentumokat.

Tizedes törtek

- Al-Kási Dzsamidsid Gijászaddin (1427) *Az aritmetika kulcsa*, $2\pi \approx 6,283\,185\,307\,179\,586\,5$.
- Simon Stevin (1585) *A tizedes egység*.
- John Napier (1550-1617): 0°-tól 90°-ig 1'-es ugrásokkal növekvő szögek szinuszai logaritmusa 8 tizedes jegy pontossággal. 20 évig dolgozott a táblázaton.
- Henry Briggs (1624) *Arithmetica logarithmica*: $1 - 20\,000$ és $90\,000 - 100\,000$ számolta ki az egész számok 10-es alapú logaritmusát 14 tizedes jegy pontossággal.

Néhány mai rekord és eredmény

- A.J. Yee és S. Kondo (2010): π kiszámítása $5 \cdot 10^{12}$ tizedes jegy pontossággal. A számítás és az ellenőrzés 90 napig tartott egy asztali számítógépen.
- S. Kondo (2010): e és $\sqrt{2}$ közelítése $5 \cdot 10^{12}$, illetve 10^{12} tizedes jegyig. 1 milliárd nyomtatott oldal!
- Kovács Gábor (2010) DE PTI BSc, grafikus kártyával néhány perc alatt kiszámolja e-t 1 millió jegy pontossággal.
- Normális számok: minden számjegy és számjegycsoport egyenletes eloszlású.

A Pentium FDIV hiba

- Thomas R. Nicely a prímszámok, ikerprímek, prímhármasok és -négyesek leszámlálásával, valamint ezen számok reciprokai összegének kiszámításával foglalkozott.
- 1994 júniusában egy Pentium processzoros gépet is beállított a munkába, de számítási hibákat tapasztalt.
- Egy ilyen hibás osztás:

$4195835.0/3145727.0 = 1.33382044913624100 25 \quad (helyes)$

$4195835.0/3145727.0 = 1.33373906890203758 94 \quad (Pentium)$.

- A processzorok kijavítása és cseréje 100 millió $-ba került.

Diofantikus egyenletek

Egy egyenletet diofantikusnak nevezünk, ha a megoldásait az egész számok körében keressük.
Hazánkban az elméletet Győry Kálmán honosította meg $\rightarrow$ debreceni számelméleti iskola.
Előfordulhat, hogy a diofantikus egyenletnek:

- egyáltalán nincs megoldása: $2x^2 + 3y^2 = 1$,
- véges sok megoldása van $x^2 + y^2 = 1$,
- végtelen sok megoldása van, $x^2 - 2y^2 = 1$.

Hilbert problémái a XX. századnak

- 2. Matematikus Kongresszus, 1900, Párizs.
- David Hilbert 10. problémája:

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

- Jurij Matiyasevich (1970): nincs ilyen eljárás.

Baker módszerrel megoldható egyenletek

- Thue egyenlet:

$$F(x,y) = x^n + a_{n-1}x^{n-1}y + \cdots + a_1xy^{n-1} + a_0y^n = m,$$

ahol $n \geq 3$.

- Elliptikus egyenletek:

$$y^2 = x^3 + ax + b.$$

- Hiperelliptikus egyenletek:

$$y^2 = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \; n > 3.$$

- Diszkrimináns- és indexforma egyenletek.

A Baker módszerrel bizonyítható korlátok igen nagyok.

A Thue egyenletre Y. Bugeaud és Győry Kálmán (1996) bizonyította, hogy:

$$\max\{|x|, |y|\} < \exp\left\{3^{3(n+9)} n^{18(n+1)} H^{2n-2} (\log H)^{2n-1} \log^* |m|\right\},$$

ahol $\log^* |m| = \max\{\log |m|, 1\}$ és $H = \max\{1, |a_0|, \ldots, |a_{n-1}|\}$.

A nagyon egyszerűnek számító

$$x^4 - ax^3y - x^2y^2 + axy^3 + y^4 = 1$$

egyenletre $a = 4$ mellett Bugeaud és Győry felső korlátja $\max\{|x|, |y|\} < 10^{10^{78}}$.
M. Mignotte, Pethő, R. Roth (1996) szétosztott számítással mégis meg tudta mutatni, hogy $a \neq \pm 4$ - re nincs más megoldás, mint

$$(x, y) = \pm(0, 1), (1, 0), (1, 1), (-1, 1), (a, 1), (-1, a).$$

A Saarvidéki Egyetem 42 számítógépe 3 héten keresztül dolgozott a problémán.

Eredmények elliptikus egyenletekre

L.J. Mordell, K. Weierstraß, S. Lang eredményeinek felhasználásával J. Gebellel és H.G. Zimmerrel 1994-ben numerikus módszert adtunk az

$$y^2 = x^3 + ax + b$$

elliptikus egyenlet megoldására.

Az eljárás során valós számok közelítő értékét kell kiszámítani több ezer tizedes jegy pontossággal.

• J. Gebellel és H.G. Zimmerrel (1998) megoldottuk az $y^2 = x^3 + k$ egyenletet a $k = 7823$ érték kivételével minden $|k| < 10\ 000$-re és bizonyos feltételek mellett $|k| < 100\ 000$-re is. Néhány évvel később Manfred Stoll a $k = 7823$ értéket is elintézte.

• Az algoritmust Emanuel Herrmann implementálta a MAGMA programcsomagban és így a Thue egyenletekre vonatkozó hasonló eljárással együtt a diofantikus egyenletek kutatásával foglalkozó tudósok mindennapos segédeszközévé vált.

Köszönöm a megtisztelő figyelmet!