BARANGOLÁS A SZÁMOLÁSTECHNIKA HATÁRVIDÉKEIN

PETHŐ ATTILA

1. Bevezetés

Az igen megtisztelő felkérés, hogy a Magyar Tudományos Akadémia frissen megválasztott levelező tagjaként én tartsak előadást a DAB 2011-es közgyűlésén, nehéz feladatot tűzött ki számomra. "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." írja Timothy Ferris [9]. Egyetértek vele abban, hogy a matematika egy antientropikus képződmény, a matematikusokra azonban ez már nem igaz. A matematika ugyanis Eukleidesztől kezdve, de különösen a XIX. század közepétől, a formális logika szabályait követve, szigorúan deduktív módon épül fel. Ugyanezt az utat utat járja a számítástudomány is, hiszen a számítógépeink bitekből építik fel a legbonyolultabb virtuális tereket is. Ehhez pedig, végső soron, csak néhány nagyon egyszerű utasítást: értékadás, adatok mozgatása és, ami a legfőbb erőt adja, a ciklikus utasítást használhatnak.

Az előadásomhoz tehát olyan témát kellett választanom, amelyben fel tudom villantani azt a tudományos eredményt, amely miatt az Akadémia levelező tagjai sorába választottak, de mindezt oly módon, hogy az más tudósok számára is érdekes legyen.

Legfontosabbnak tartott eredményeim diofantikus egyenletek numerikus megoldásával kapcsolatosak. Egyrészt olyan eljárásokat dolgoztam ki, amelylyel ilyen egyenleteket meg lehet oldani, másrészt konkrét esetekben bizonyítottam, hogy az eljárások tényleg használhatóak, sőt azt mások is használni tudják. A számítások során igen nagy, több ezer tizedes jegy, pontossággal kell műveleteket végezni, így természetes módon adódott, hogy a számolástudományról beszéljek. A témának azonban nemcsak tudományos, hanem mindennapos gyakorlati vonatkozásai is vannak. Itt elsősorban az internetes kommunikáció biztonságát emelem ki. Ha például egy banki tranzakciót hajtunk végre, akkor a bizalmas adatforgalmat igen nagy számokon végzett műveletekkel biztosítják.

2. Bibliai népszámlálás

"A gyors számolás vágya egyidős a számolással.[...] Ezen a területen az első igazi ugrást a helyi értékes számírás feltalálása hozta.", írja Sain

Márton [27]. Az Európai matematika fejlődését az ókori görög matematika határozta meg, amely elsősorban a geometriára koncentrált. A helyi értékes ábrázolás elemei megjelentek Babilonban, de Indiában teljesedtek ki. A ókori számítási teljesítményre szép pédát találunk Mózes IV. könyve 1. és 2. részében: "Vegyétek számba Izráel fiainak egész gyülekezetét, az ő nemzetségeik szerint, az ő atyáiknak háznépe szerint, a neveknek száma szerint, minden férfiút főről-főre." [5]

A bibliai népszámlálás során megállapították az egyes törzsek létszámát. Ezek után összegezték a Júda, Rúben, Efraim és Dán táborába tartozók létszámát, végül kiszámolták Izráel fiainak lélekszámát. Matematikai szempontból öt, bonyolult összeadást kellett végrehajtani.

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

Az összeadások pontos elvégzése komoly intellektuális teljesítményt jelentett a Biblia kétésfél-háromezer évvel ezelőtt élt szerzőjének. Feladatát nehezítette, hogy nem a ma használt tizes számrendszerben írta fel a számokat, hanem szöveggel. Az alapműveletek végrehajtásának ősi technikáival alig foglalkozik a tudománytörténet. Valószínűnek tartom azonban, hogy a törzsek létszámának összegzése az akkori számolástudomány egyik csúcsteljesítménye volt.

A számok tizes számrendszerben való felírása csak a kora középkorban, miután Kr.u. 500 körül feltalálták a nullát, vált lehetővé. Károlyi Gáspárnak a XVI. században már nem okozott gondott elvégezni a Bibliában megfogalmazott műveleteket és széljegyzeteiben meg is magyarázta a szövegben szereplő adatok és az összeadás eredménye közötti eltéréseket.

3. Nagy prímszámok

A számolástudomány fejlődését nagyon jól lehet követni az ismert Mersenne féle prímszámok növekedésével. Ezeknek a számoknak a története visszanyúlik az ókori görög matematikusokhoz. Egy számot tökéletesnek nevezünk, ha valódi osztóinak összege megegyezik magával a számmal. Például

a 6 és a 28 tökéletes számok, mert a valódi osztóik $1, 2, 3$, illetve $1, 2, 4, 7, 14$ és $1 + 2 + 3 = 6$, illetve $1 + 2 + 4 + 7 + 14 = 28$. Eukleidész bebizonyította, hogy egy páros szám csak akkor lehet tökéletes, ha $2^{p-1}(2^p - 1)$ alakú, ahol p és $2^p - 1$ is prímszámok. Az előző példáknál maradva, 2 és $2^2 - 1 = 3$, illetve $2^3 - 1 = 7$ prímszámok, így $2(2^2 - 1) = 6$, illetve $2^2(2^3 - 1) = 28$ tökéletes számok. Néhány értékre $p = 7, 13, 17$ és 19-re direkt számolással ellenőrizték $2^p - 1$ prím tulajdonságát. L. Euler felismerte, hogy a Mersenne számok esetleges osztói speciális alakúak és ezt felhasználva 1772-ben megmutatta, hogy $2^{31} - 1 = 2147483647$ is prímszám.

Peter Barlow, korának egy jelentős tudósa, a következőt írta Euler felfedezéséről [4]:" [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

- F.E.A. Lucas francia matematikus 1876-ban felfedezett egy nagyon hatékony módszert Mersenne számok prímtulajdonságának tesztelésére,
- a XX. század közepétől kezdve az elektronikus számítógépeken a Lucas féle tesztet hatékonyan lehetett implementálni,
- A. Schönhage és V. Strassen [28] a véges Fourier transzformáció felhasználásával, a hagyományos szorzási algoritmusnál sokkal gyorsabb szorzási eljárást dolgoztak ki. Megjegyezzük, hogy nemcsak a szorzást, hanem az osztást is lehet sokkal hatékonyabban végezni, mint azt hagyományosan tesszük;
- a szuperkomputerek, illetve az internettel összekötött számítógépek (cloud computing) igen nagy számítási erőt szolgáltatnak.

Ma már 47 Mersenne prímszámot ismerünk, a legnagyobb $2^{43\ 112\ 609} - 1$, amelyik egy 12 978 189 decimális jegyű szám és a GIMPS [14] (Great Internet Mersenne Prime Search) csoport szoftverével 2008-ban találták. Ez ma a legnagyobb olyan egész szám, amelynek valamilyen nem triviális tulajdonságát bizonyítani lehetett. Látható, hogy Mersenne prímszámok elég ritkán fordulnak elő, de a szakértők többsége mégis azt gondolja, hogy végtelen sokan vannak.

A Kossuth Lajos Tudományegyetemen 1967-ben alakult a Számoló Központ. Gesztelyi Ernő és Jékel Pál [13] 1976-ban tetszőleges nagyságú egész számokkal való számolásra dolgoztak ki algoritmust, amely párhuzamosan számítja ki a művelet eredményének számjegyeit, majd standardizálják az eredményt. Módszerükkel az akkor rendelkezésre álló ODRA 1204-es számítógépen kiszámították $n!$ értékét $1 \leq n \leq 1003$-ra.

Ha p és $p + 2$ is prímszámok, akkor őket ikerprímeknek nevezzük. Néhány példa ilyen számpárra: $3, 5$; $5, 7$ és $2027, 2029$. Ikerprímekből álló párok sokkal gyakoribbak, mint a Mersenne prímszámod, de ezekről sem tudjuk, hogy végtelen sokan vannak-e. Magyar tudósok nagyon eredményesek

nagy ikerprímszámok meghatározásában. Járai Antal, az ELTE professzora, több kutatócsoporttal, 1994-től kezdve többször is vezette a legnagyobb ikerprímek listáját [19]. A legnagyobb általuk talált ikerprímek: $194772106074315 \cdot 2^{171960} \pm 1$, amelyeknek 51780 számjegye van. Ezt 2007-ben találták, de 2009-ben a PrimeGrid csoport átvette a vezetést a 100355 decimális jegyű $65516468355 \cdot 2^{333333} \pm 1$ ikerprímmel. A verseny tovább folytatódik...

4. Kriptográfiai alkalmazások

A Mersenne- és az ikerprímekre vonatkozó eredmények komoly intellektuális eredmények, de közvetlen hasznuk nincs. A számelméletet és ezen belül a prímszámok elméletét egészen a legutóbbi évtizedekig a tiszta matematika mintapéldájának tartották. Godfrey Hardy, a XX. sz. első felének egyik legnagyobb számelméletésze büszke volt erre a státuszra. 1940-ben megjelent könyvében [16] írja: "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." Mekkora OTKA támogatásra számíthatna ma egy tudós ilyen attitüddel? Az 1950-ben megjelent nekrológban is csak egy esetleges kivételt említenek meg, mégpedig a Hardy-Weinberg féle népességgenetikai szabályt [7].

1976-ban azonban drámai változás történt. Ebben az évben fogalmazta meg Whitfield Diffie és Martin E. Hellman [8] a nyilvános kulcsú titkosítás elvét, amely alapvető szerepet tölt be a modern algoritmikus adatvédelemben. Az elv lényege az, hogy ha valaki bizalmas üzenetet küldene Aladárnak, akkor azt Aladár nyilvános kulcsával titkosítva továbbítja a nyilvános csatornán, például az interneten. A kódolásnak olyannak kell lenni, hogy hiába tudja valaki Aladár nyilvános kulcsát és kerül birtokába a kódolt üzenet, azt ne legyen képes megfejteni. Ezzel szemben Aladár meg tudja fejteni az üzenetet a csak általa ismert titkos kulccsal, ami természetesen a nyilvános kulcs párja.

Diffie és Hellman csak a nyilvános kulcsú titkosítás elvét fogalmazta meg. Nem sokat váratott magára azonban olyan algoritmusok publikálása sem, amelyek megfeleltek az első ránézésre teljesíthetetlen követelményeknek. Ronald Rivest, Adi Shamir és Leonard Adleman 1978-ban közölte a ma széles körben alkalmazott RSA algoritmusról szóló cikkét [26]. Ez és az elmúlt évtizedekben kidolgozott több mint 300 nyilvános kulcsú titkosításra alkalmas algoritmus többsége nehéz számelméleti problémákon alapszik.

Az RSA-t például azért fogadjuk el biztonságosnak, mert nagy számokat igen nehéz prímszámok szorzatára bontani. Aladárnak tehát keresni kell két nagy prímszámot: p, q. Ezeket összeszorozva kapja az $n = pq$ számot. Ezen kívül kiszámítja a $\varphi(n) = (p-1)(q-1)$ értéket és keres egy olyan $1 < e < \varphi(n)$ számot, amelynek $\varphi(n)$-nel nincs 1-től különböző közös osztója.

Ezek után ki kell még számolnia egy olyan $1 < d < \varphi(n)$, 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.

Amikor Kriszta az M bizalmas üzenetet akarja küldeni Aladárnak, akkor először M-et bináris számmá alakítja, majd kiszámítja M^e maradékét n-nel osztva, amit jelöljön T. Ezek után elküldi T-t Aladárnak, aki az üzenetet megkapva kiszámolja T^d maradékét n-nel osztva és így visszanyeri M-et.

Az eljárás minden egyes lépése gyorsan elvégezhető. Ehhez azonban számítógépre van szükségünk, mert a paraméterek igen nagy számok. Ma ugyanis csak azt az RSA implementációt tekinthetünk biztonságosnak, amely legalább 1024 bites n értékkel számol. Tekintettel arra, hogy az e és d számok hasonló méretűek, így az RSA kulcsok legalább 256 karakterből, 3 gépelt sorból, álló jelszónak felelnek meg, amelyet a legtöbb ember képtelen memorizálni.

A kriptográfia eredményei ma mindennapjaink részévé váltak. Ezek teszik lehetővé, hogy 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. Az Informatikai Kar tanácsának tagjai 2005 óta saját fejlesztésű RSA azonosító használatával érhetik el a bizalmas dokumentumokat [10].

5. Tizedes törtek

Eddig nagy szám alatt mindíg egész számot értettünk. Sokkal gyakrabban találkozhatunk azonban nagy pontosságú számokkal, azaz olyan tizedes törtekkel, amelyek a tizedes vessző után sok számjegyig pontosak. Az ókorban csak törtekkel számoltak, bár már a görög matematikusok is tudták, hogy például egy egységoldalú négyzet átlójának hossza, $\sqrt{2}$, nem fejezhető ki két egész szám hányadosaként, azaz összemérhetetlen az oldalhosszal.

Sain Márton [27] szerint Al-Kási Dzsamidsid Gijászaddin, iráni tudós 1427-ben megjelent *Az aritmetika kulcsa* "könyve az első írásos ismertetés a tizedes törtekkel való számolás szabályairól". Al-Kási 2π közelítését számította ki 16 tizedes jegy pontossággal, $2\pi \approx 6,283\,185\,307\,179\,586\,5$.

Európában a tizedes törtek Simon Stevin 1585-ben megjelent *A tizedes egység* című könyvének hatására terjedtek el. John Napier (1550-1617) 20 évig dolgozott azon a táblázaton, amelyben 0°-tól 90°-ig 1'-es ugrásokkal növekvő szögek szinuszai logaritmusát számította ki 8 tizedes jegy pontossággal. Az általa használt logaritmus alapszáma $(1 - 1/m)^m$ volt, ahol $m = 10^7$. Ez gyakorlatilag a természetes logaritmus alapszámának a reciproka, azaz $1/e$. A tizes alapú logaritmust Henry Briggs (1561-1630) vezette be, aki az 1624-ben megjelent *Arithmetica logarithmica* című könyvében $1 - 20\,000$ és $90\,000 - 100\,000$ intervallumokban számolta ki az egész számok 10-es alapú logaritmusát 14 tizedes jegy pontossággal. A logaritmus táblázatok és azok mechanikus változata a logarléc évszázadokon keresztül a

mérnökök elmaradhatatlan eszköze volt, az 1980-as évektől kezdve azonban fokozatosan kiszorították őket a kalkulátorok.

Ahogy a minél nagyobb egész számok kiszámításáért, ugyanúgy az érdekes valós számok minél pontosabb közelítéséért is verseny folyik. 2010 augusztus 2-án jelentette be például A.J. Yee és S. Kondo [30], hogy π-t $5 \cdot 10^{12}$ tizedes jegy pontossággal határozták meg. A számítás és az ellenőrzés 90 napig tartott egy asztali számítógépen. S. Kondo valamivel korábban ugyanilyen pontossággal meghatározta e-t valamint 10^{12} tizedes pontossággal $\sqrt{2}$-t. Egyetemünk PTI BSc hallgatója, Kovács Gábor [20], grafikus kártyát használva néhány perc alatt ki tudta számolni π-t 1 millió tizedes jegy pontossággal. Ez persze még távol van a világrekordtól, de a programja még javítható.

Ezeknek a számításoknak nemcsak technikai érdekessége van, de felvilágosítást ad a számjegyek és számjegycsoportok eloszlásáról is. Egy nagyon nehéznek tartott sejtés szerint ugyanis a fent említett számok *normálisak*, azaz tizedes tört felírásukban a számjegyek és a számjegycsoportok egyenletesen oszlanak el. A számítások a sejtést megerősítik, de előfordult már, hogy egy tulajdonság igaz volt a numerikusan elérhető tartományban, de általában nem teljesül.

6. A Pentium FDIV hiba

Ha egy statikus mérnök pontatlanul méretezi a tető teherbíró képességét, akkor az beszakad, mint arra az utóbbi években több példát is láttunk. A számítógépes program írása közben vétett hiba rendszerint gyorsan kiderül, mert az eredmények különböznek a várt értéktől. A programozó gyorsan megtanulja, hogy ilyenkor ő követte el a hibát, a gép csak azt hajtotta végre, amit ő előírt.

Thomas R. Nicely, a Lynchburg College matematika professzora az 1990-es évek elején a $6.4 \cdot 10^{15}$-nél kisebb prímszámok, ikerprímek, prímhármasok és -négyesek leszámlálásával valamint ezen számok reciprokai összegének kiszámításával foglalkozott. 1994 júniusában egy új, Pentium processzoros gépet is beállított a munkába. Azt vette azonban észre, hogy az új számítógép más eredményt ad, mint a régiek. Hónapokon keresztül kereste a hibát a saját maga és mások által írott programokban. Több hibát is talált és ki is javított, de az eredményeket ez nem befolyásolta. Végül az új számítógép Pentium processzorának működésében sikerült lokalizálnia a probléma okát. Kiderült, hogy a processzorban az osztást gyorsító néhány paraméter rosszul volt beállítva, ami miatt bizonyos értékekre hibásan végezte el a műveletet. Egy ilyen hibás osztás:

$$\begin{aligned} 4195835.0/3145727.0 &= 1.3338204491362410025 \quad (\textit{helyes érték}) \\ 4195835.0/3145727.0 &= 1.3337390689020375894 \quad (\textit{hibás Pentium}). \end{aligned}$$

A processzort gyártó Intel konszern csak hónapokkal később ismerte be a hibát és végül visszahívta a hibás egységeket. A pontatlanul beállított proceszorok kijavítása és cseréje 100 millió $-ba került a gyártónak. További részletek Nicely [23] honlapján olvashatóak.

7. Diofantikus egyenletek

Egy egyenletet diofantikusnak nevezünk, ha a megoldásait az egész számok körében keressük. Előfordulhat, hogy egy ilyen egyenletnek

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

David Hilbert 1900-ban a 2. Matematikus Kongresszuson, Párizsban 23 problémát fogalmazott meg a XX. század matematikusai számára [18]. Ezek többségét megoldották, de például a Riemann sejtés máig támadhatatlannak tűnik.

A 10. probléma következőképpen hangzott [17]: *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.*

Ő tehát egy olyan eljárás megadását tűzte ki célul, amellyel minden diofantikus egyenletről el lehet dönteni, hogy megoldható-e. A keresett eljárás mai szóhasználattal élve egy algoritmus, de annak pontos fogalmát csak 30 évvel később Kurt Gödel adta meg és rögtön be is bizonyította, hogy vannak algoritmussal megoldhatatlan problémák. 1970-ben Jurij Matiyasevich szovjet matematikus bizonyította be, hogy diofantikus egyenletek megoldására sem létezik általános eljárás.

Ugyanakkor diofantikus egyenletek széles osztályait meg lehet oldani algoritmussal. Ezt Alan Baker angol matematikusnak az 1960-as évek elején algebrai számok logaritmusaiból álló lineáris formákra adott híres alsó becslései [1] teszik lehetővé. Baker ezért az eredményéért Fields díjat kapott, ami a matematikusok Nobel díja. A legfontosabb egyenletek, amelyekre a Baker módszer használható:

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

Az első három típusra Baker [2, 3], a negyedikre Győry Kálmán [15] bizonyította az algoritmikus megoldhatóságot. Eredményeik azonban csak elvben teszik lehetővé az egyenletek megoldását, mert módszerükkel csak olyan nagy felső korlátot lehet bizonyítani, amely nem teszi lehetővé a maradék véges tartományba eső pontok tesztelését. A Thue egyenletre vonatkozó

ma ismert legélesebb felső korlátot Y. Bugeaud és Győry Kálmán [6] bizonyította:

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

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

$$x^4 - 4x^3y - x^2y^2 + 4xy^3 + y^4 = 1$$

egyenletre Bugeaud és Győry felső korlátja $\max\{|x|,|y|\} < 10^{10^{78}}$. Ez bizony sokkal nagyobb szám, mint a legnagyobb ismert Mersenne prím, pedig azt is extrém nagynak találtuk. Az A.K. Lenstra, H.W. Lenstra és Lovász László [24] bázisredukciós algoritmusát használva mégis be tudtam bizonyítani [25], hogy az előző egyenletet csak az

$$(x,y) = \pm(0,1),(1,0),(1,1),(-1,1),(4,1),(-1,4),(8,7),(-7,8)$$

számpárok elégítik ki. Valamivel később M. Mignotteval és R. Rothtal [22] azt is megmutattuk, hogy az

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

egyenletnek egyetlen egész $a \neq \pm 4$-re sincs más megoldása, mint

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

A Baker módszert az akkor elosztott, ma felhő, számításnak nevezett technikával kombináltuk, amely az utóbbi egyik első alkalmazása volt.

8. A redukciós technika

Baker lineáris forma tétele minden algebrai számra igaz, konkrét esetben azonban esetleg javítható. Ez a gondolat áll azon redukciós technikák mögött, amelyek lehetővé teszik a kezdeti igen nagy felső korlát lényeges csökkentését, majd az egyenlet megoldását. Thue egyenletekre Y. Bilu és G. Hanrot, indexforma egyenletekre pedig Gaál István, részben M. Pohsttal és velem dolgozta ki a módszer részleteit. A technika fő lépéseit Gebel, Pethő és Zimmer [11], illetve Stroeker és Tzanakis [29] nyomán az elliptikus egyenletre mutatjuk be.

Legyen tehát a $P = (x,y) \in \mathbb{Z}^2$ az

$$y^2 = x^3 + ax + b. \tag{1}$$

egyenlet egy megoldása. Két lépésben fogjuk bővíteni az (1) görbére illeszkedő pontok koordinátáinak a halmazát azért, hogy a halmazok valamilyen használható struktúrával rendelkezzenek. Először csak a racionális számok $\mathbb{Q}$ halmazára terjesztjük ki figyelmünket.

Jelölje tehát $E(\mathbb{Q})$ az (1) görbére illeszkedő racionális koordinátájú pontok halmazát, kiegészítve egy - Henri Poincaré által bevezetett - végtelen távoli ponttal. Már a XVII. sz.-ban élt Claude Bachet is ismerte a metsző-érintő eljárást. Legyen adva két különböző pont P_1, P_2 az (1) görbén. Az őket összekötő egyenes egy harmadik pontban metszi a görbét. Ennek az x-tengelyre

vonatkozó tükörképét P_3 - ami persze szintén rajta van a görbén - nevezzük a P_1 és P_2 összegének. Íly módon két ismert pontból általában végtelen sokat tudunk előállítani. Ettől több is igaz; az $E(\mathbb{Q})$ Abel csoportot alkot. Louis Mordell 1921-ben még azt is bebizonyította, hogy $E(\mathbb{Q})$ végesen generált, azaz vannak olyan $P_1, \ldots, P_r \in E(\mathbb{Q})$, hogy minden $P \in E(\mathbb{Q})$ felírható

$$P = n_1 P_1 + \ldots n_r P_r \tag{2}$$

alakban, ahol $n_1, \ldots, n_r$ egész számok.

Most még tovább bővítjük a megengedett koordináták halmazát, mégpedig a komplex számokra. Így kapjuk az $E(\mathbb{C})$ halmazt. Karl Weierstraß bizonyította be, hogy az $(x, y) \in E(\mathbb{C})$ pontok parametrizálhatóak a Weierstraß féle $\wp$ függvények segítségével, azaz bármely $(x, y) \in E(\mathbb{C})$-hez van olyan $t \in \mathbb{C}$, hogy $(x, y) = (\wp(t), \wp'(t))$. Persze minden elliptikus görbéhez más Weierstraß függvény tartozik. Weierstraß ezeket a függvényeket az első- és masodfajú elliptikus integrálokból származtatta, amelyek például az ellipszis ívhosszának kiszámítására is használhatóak. Innen származik az egyenletek elnevezése is. Azt is érdemes megjegyezni, hogy a $\wp$ függvények két, független irányban periódikus függvények. A két irány a komplex számsíkon egy paralellogrammát Λ határoz meg és teljesül, hogy bármely $(x, y) \in E(\mathbb{C})$-hez van olyan, most már egyértelműen meghatározott $t \in \Lambda$, hogy $(x, y) = (\wp(t), \wp'(t))$. Ezt a t értéket nevezzük a $P = (x, y)$ pont *elliptikus logaritmusának* és $u(P)$-vel jelöljük. Megmutatható, hogy az elliptikus logaritmus és az összeadás felcserélhető, így (2)-ből következik

$$u(P) = n_1 u(P_1) + \cdots + n_r u(P_r) \bmod \Lambda.$$

Ezen hosszú előkészítés után visszatérhetünk az eredeti problémánkhoz. Minket csak az elliptikus görbére illeszkedő egész pontok érdekelnek. Ezekre belátható, hogy csak olyan $n_1, \ldots, n_r$ egész számok jöhetnek szóba, amelyekre

$$|n_1 u(P_1) + \cdots + n_r u(P_r)| < \exp(-cN^2), \tag{3}$$

ahol c egy nem nagy konstans és $N = \max(|n_1|, \ldots, |n_r|)$. Ennek az egyenlőtlenségnek még lehet végtelen sok megoldása, de Baker típusú tételek segítségével N-re kiszámítható felső korlát, N_0, adható. Mint korábban már említettem N_0 nagyon nagy, legalább 10^{30}. Az $u(P_1), \ldots, u(P_r)$ számok megfelelő pontosságú, ami esetünkben néhány ezer tizedes jegy, közelítésének ismeretében az LLL algoritmussal numerikus alsó korlátot lehet kiszámítani $|n_1 u(P_1) + \cdots + n_r u(P_r)|$-re. Az alsó korlát ismeretében (3)-ból új, az eredetinél lényegesen kisebb felső korlát következik N-re. Szükség esetén a redukció iterálható addig, amíg a felső korlát tovább nem csökkenthető.

A redukciós eljárás azért működik, mert a diofantikus approximáció elméletének eredményei alapján várható, hogy az $|n_1 u(P_1) + \cdots + n_r u(P_r)|$ lineáris formára érvényes alsó korlát N-ben polinomiális. Ezt ma még nem tudjuk bizonyítani, de konkrét esetben ellenőrizni tudjuk, ami nagyon sok

diofantikus egyenlet megoldását teszi lehetővé. J. Gebellel és H.G. Zimmerrel [12] megoldottuk például 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 általunk kidolgozott 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.

A technikai fejlődésnek árnyoldalai is vannak. A kalkulátort használó kisdiákok nem tanulnak meg fejben vagy papíron számolni. Fiatal kollégáim csak beírják a MAGMA-ba a diofantikus egyenlet adatait és várják a számítógép válaszát. Általában megkapják az eredményt, de ha nem, akkor csak annyit mondanak, hogy a feladatot a számítógép sem tudta megoldani. Az igazi intellektuális kihívást pedig az jelenti, hogy olyan problémát is meg akarunk és tudunk oldani, amire a számítógép nem képes!

Hivatkozások

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers I, II, II, IV*, Mathematica, **13** (1966), 204–216; **14** (1967), 102–107; 220-228; **15** (1968), 204-216.

[2] A. Baker, *Contribution to the theory of Diophantine equations*, Philos. Trans. Roy. Soc. London Ser. A, **263** (1968), 173–208.

[3] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc., **65** (1969), 439–444.

[4] Peter Barlow, An Elementary Investigation of the Theory of Numbers, London, 1811.

[5] Szent Biblia, azaz Istennek ó és új testamentumában foglalt egész Szent Írás, Magyar nyelvre fordította Károlyi Gáspár, A Magyarországi Református Egyház Egyetemes Konventje az Evangélikus Egyház és a Szabad Egyházak Szövetségének Közreműködésével, Budapest, 1958.

[6] Y. Buegaud, K. Győry, *Bounds for the solutions of Thue-Mahler equations and norm form equations,* Acta Arith., **74** (1996), 273–292.

[7] Dr. Czeizel Endre, A magyarság genetikája, Galenus Kiadó, Budapest, 2003.

[8] Whitfried Diffie and Martin Hellman, *New direction in cryptography*, IEEE Trans. on Information Theory, **22** (1976), 644-654.

[9] Timothy Ferris, A világmindenség Mai kozmológiai elméletek

[10] J. Folláth, A.Huszti and A. Pethő, *DESignIn asymmetric authentication system*, ICAI 2007, 55-64.

[11] J. Gebel, A. Pethő and H.G. Zimmer, *Computing integral points on elliptic curves,* Acta Arith. **68** (1994), 171–192.

[12] J. Gebel, A. Pethő and H.G. Zimmer, *On Mordell's equation*, Compositio Math., **110** (1998), 335–367.

[13] Gesztelyi Ernő és Jékel Pál, *Tetszőleges nagy egész számokkal való pontos számolás számítógéppel*, MTA Számítástechnikai és Automatizálási Kutató Intézete, Közlemények, 16/1976, 53–84.

[14] GIMPS home page: http://www.mersenne.org/default.php

[15] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné III.*, Publ. Mat. Debrecen, **23** (1976), 141–165.

[16] Godfrey Hardy, *A Mathematician's Apology* Cambridge: University Press, 1940.

[17] D. Hilbert, Entscheidung der Lösbarkeit einer Diophantischen Gleichung. Akad. Wiss. Göttingen 1900, 276.
[18] Mathematical developments arising from Hilbert problems. Proceedings of the Symposium in Pure Mathematics of the American Mathematical Society held at Northern Illinois University, De Kalb, Ill., May, 1974. Edited by Felix E. Browder. Proceedings of Symposia in Pure Mathematics, Vol. XXVIII. American Mathematical Society, Providence, R. I., 1976.
[19] Járai Antal, *Word records in computational number theory*, http://compalg.elte.hu/ ajarai/worldr.htm
[20] Kovács Gábor, *Az e kiszámítása*, TDK dolgozat, Debreceni Egyetem, 2010.
[21] Yu. V. Matiyasevič, *The Diophantineness of enumerable sets.* (Russian) *Dokl. Akad. Nauk SSSR*, **191** (1970), 279–282.
[22] M. Mignotte, A. Pethő and R. Roth, *Complete solutions of quartic Thue and index form equations,* Math. Comp. **65** (1996), 341–354.
[23] Thomas R. Nicely, *Pentium FDIV flaw*, http://www.trnicely.net/pentbug/pentbug.html
[24] A.K. Lenstra, H.W. Lenstra, L. Lovász, *Factoring Polynomials with Rational Coefficients*, Math. Ann. **261** (1982), 515–534.
[25] A. Pethő, *Complete solutions to a family of quartic diophantine equations*, Math. Comp. **57** (1991), 777-798.
[26] Ronald Rivest, Adi Shamir and Leonard Adleman, *A method for obtaining digital signature and public-key cryptosystems*, Communications of the ACM, 21 (1978), 120-126.
[27] Sain Márton, Nincs királyi út! Matematikatörténet, Gondolat, Budapest, 1986.
[28] A. Schönhage und V. Strassen, *Schnelle Multiplikation großer Zahlen*, Computing **7** (1971), 139-144.
[29] R.J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arithm. 67 (1994),177-196.
[30] Alexander J. Yee and Shigeru Kondo, *5 Trillion Digits of Pi - New World Record*, http://www.numberworld.org/misc_runs/pi-5t/announce_en.html

Pethő Attila
Debreceni Egyetem, Informatikai Kar,
MTA-DE Számelméleti Kutatócsoport
Debreceni Egyetem
H-4010 Debrecen, Pf. 12.
E-mail address: Petho.Attila@inf.unideb.hu