Zárójelentés a "Számítógépes számelmélet" c. OTKA pályázathoz

Témavezető: Járai Antal
OTKA szám: T0 43657

1. A publikációk rövid ismertetése

Az OTKA jelentésben mellékelt publikációs jegyzékben található munkákról itt csak rövid ismertetést adunk, mivel azokban úgyis nagy részletességgel szerepelnek a közlésre szánt eredmények. Részletesebben kívánunk majd foglalkozni olyan munkákkal, amelyek könyvekben, vagy folyóiratcikkekben csak érintőlegesen szerepelnek. Ilyenek például a kutatás során folytatott sikeres projektek, fejlesztett szoftverek, illetve elért világrekordok.

Megjegyezzük még, hogy a kutatási tervben kiemelt három terület, nevezetesen **prímszámtesztek, szitamódszerek, általánosított számrendszerek,** szorosan összefügg, amit a nagy prímszámok utáni hajszában jól nyomon követhetünk. Ahhoz, hogy eredményesen keressünk nagy prímszámokat, illetve prímkombinációkat, mint például k **hosszúságú Cunningham-láncok, Sophie Germain, vagy ikerprímek**, először "szitálni" kell, amely az eratosztenészi szitán alapuló nagy mennyiségű prímszám előállítására utal, illetve az úgynevezett általános szita eljárásra, amely során kiszűrjük egy intervallumból azon számokat, amelyeknek biztosan van egy adott határnál kisebb prímosztója. A szitálás után már csak a maradék számokra (kandidátusok) kell elvégeznünk a prímszámteszteket. Manapság a gyakorlati életben a leggyorsabbnak számítanak az úgynevezett **elliptikus görbés prímtesztek**, amelyek egyúttal jól példázzák a fent említett három kutatási terület összefonódását, hiszen az általánosított számrendszerek vizsgálatának része kvadratikus testek algebrai egészeinek vizsgálata. Felmerül a kérdés, hogy mi köze ezeknek a prímteszteléshez. Tekintsük tehát az **Atkin-tesztet**. Itt az alapgondolat az, hogy prímteszteléskor először

nem az elliptikus görbét választjuk ki, hanem a rendjét. Ezt egy képzetes kvadratikus test algebrai egészei segítségével tesszük. Ha ezek közt találunk olyan ν-t, amelyre $\mid \nu \mid^2 = n$, akkor érdemes olyan m számmal kísérletezni, amelyre $m = \mid \nu \pm 1 \mid^2$, azért, mert ha van ilyen és megfelelő módon faktorizálni is lehet, akkor a megfelelő $E(\mathbb{Z}/n\mathbb{Z})$ elliptikus görbe viszonylag könnyen megtalálható. Megfelelő alatt azt értjük, hogy a csoport rendje m, azaz $\mid E(\mathbb{Z}/n\mathbb{Z}) \mid = m$. A felhasznált kvadratikus testben nem mindegy, hogy hogyan választjuk meg az úgynevezett D alapdiszkriminánst, mivel D negatív egésznek rendelkeznie kell a következő tulajdonságokkal: $D \equiv 0 \pmod 4$, vagy $D \equiv 1 \pmod 4$, minden $k > 1$ egészre D/k^2 nem alapdiszkrimináns, $D < -7$. Adott n esetén és a hozzá megtalált D értékkel kiszámíthatjuk az úgynevezett **Hilbert-polinomot,** amelynek tetszőleges $\pmod n$ vett gyökének segítségével megadhatunk két elliptikus görbét, amelyek rendje $m = \mid \nu \pm 1 \mid^2$.

Bui Minh Phong kutatásai elméleti jellegűek, aritmetikai függvények jellemzése bizonyos tulajdonságaik alapján. Az OTKA pályázat elmúlt négy évében saját eredményein kívül M. V. Subbarao, I. Kátai, I. Joó, C. Spiro és J. M. DeKonnick e témakörre vonatkozó néhány eredményét általánosította és javította. Az elméleti eredményeinek eléréséhez számítógépes segítségre is szükség volt, amelyben jól hasznosíthatóak voltak a kutatócsoport által fejlesztett gyors aritmetikai rutinok. Gondolhatunk itt a páros és páratlan Goldbach sejtésre, amelyek igaz voltának ellenőrzése bizonyos határig egyenlőre csak számítógéppel lehetséges.

Kátai Imre professzor kutatásai főleg az analitikus számelmélettel kapcsolatosak. Az elmúlt négy évben számos publikációja küzül többek közt a q-additív függvényekkel, az Euler-féle φ-fügvény k-adik iteráltjával és additív függvények eloszlásaival foglalkozó cikkei kapcsolódnak OTKA pályázatunk témájához. Kifimomult módszereit és technikáit eredményesen tudtuk felhasználni számítógépes számelméleti vizsgálatokban is.

Annak, hogy az első látásra különbözőnek tűnő kutatási területek mégis összhangban vannak, jó példája a 2006 decemberében Vietnamban tartott számelméleti konferencia, ahol három kutatónk (Bui Minh Phong, Farkas Gábor és Kátai Imre) az OTKA pályázat jóvoltából résztvehetett és nagysikerű előadásokat tarthatott saját témájában.

2. Projektleírások

A számítógépes számelmélet célja az elméleti kutatások mellett az is, hogy ezeket felhasználja szoftverek fejlesztésére, tökéletesítésére. Valamint fordítva, komputeres támogatást nyújtani matematikai vizsgálatokhoz. Számítógépes projektjeink alapját egy olyan gyors aritmetikai programcsomat képezi, amely fejlesztését Járai Antal kezdte évekkel ezelőtt. Itt olyan rutinokra kell gondolnunk, amelyek segítségével kedvezőbb futási időt érhetünk el bizonyos nagy számításigényű és pontosságú programfuttatásoknál. Célunk tehát egyrészt az, hogy már jól ismert algoritmusokat úgy implementáljunk, hogy sokkal hatékonyabb szoftvert kapjunk, másrészt, hogy új algoritmusokat találjunk ki, azaz kicsit merész szóhasználattal élve, "elméleti úton" gyorsítsuk fel a programokat.

Az elmúlt években kutatásaink fókuszában, a kutatási tervünknek megfelelően, a prímszámok álltak, külös tekintettel az úgynevezett prímkombinációkra. Az ikerprímekkel kapcsolatban mind a mai napig sok nyitott probléma van, gondoljunk csak arra a tényre, hogy még azt sem tudjuk bizonyítani, hogy végtelen sok van belőlük. Azt tudjuk, hogy az ikerprímek reciprokösszege konvergál az úgynevezett **Brun konstanshoz**, amelynek minél pontosabb meghatározása szintén kihívásnak számít a számítógépes számelméletben.

Egy p pozitív prímszám Sophie Germain prím, ha $2p+1$ is prím. k hosszúságú elsőfajú Cunningham láncról beszélünk olyan k darab prímből álló sorozat esetén, ahol minden szám az előző kétszerese plusz egy, másodfajú láncot kapunk, ha az előbbi sorozatban plusz egy helyett mínusz egyet veszünk. A Sophie Germain prímekkel például a kriptográfiában találkozhatunk. Tekintsünk például egy RSA nyilvános kulcsú kriptográfiai algoritmust, ahol p és q páratlan prímek, $n = pq$, továbbá e relatív prím $\varphi(n)$-hez. Ekkor a p és q legoptimálisabb választása, ha ők úgynevezett dupla Sophie Garmain prímek, valamint e primitív gyök $\pmod{p-1}$ és $\pmod{q-1}$. Úgy is fogalmazhattunk volna p és q választásánál, hogy legyen mindkettő egy-egy 3 hosszúságú elsőfajú Cunningham lánc kezdő eleme.

Első prímszámkereső projektünket 2005 nyarán folytattuk. Célunk az volt, hogy bizonyítandó a fent említett gyors aritmetikai rutinok "erejét", relatíve rövid idő alatt megtaláljuk a világ legnagyobb ismert ikerprímjét, vagy Sophie Germain prímjét. Első lépésként választanunk kellett egy pozitív egészekből álló intervallumot (H halmaz), amely elemeinek segítségével egy megfelelően nagy számokból álló sorozatot generáltunk. Ennek a sorozatnak az elemei között kerestük a prímkombi-

nációkat. Az intervallumunkat természetesen úgy kellett választanunk, hogy ne legyen túl hosszú, mert az növeli a program futásidejét, de túl rövid sem lehetett, mert ez lecsökkenti annak valószínűségéz, hogy tartalmaz a sorozat iker, vagy Sophie Germain prímet. Az optimális hosszat a **Bateman–Horn sejtés** segítségével tudtuk megbecsülni, úgy hogy munkánk sikere nem a szerencsén múlott és beleférтünk az amúgy szűkre szabott CPU időbe.

Bateman–Horn sejtés. *Legyenek $f_1(x), f_2(x), \ldots, f_s(x)$ egész együtthatós irreducible polinomok pozitív főegyütthatóval. Ha $\pi(r)$ jelöli azon $1 < n < r$ egészek számát, amelyekre $f_1(n), f_2(n), \ldots, f_s(n)$ egyszerre prím, akkor*

$$\pi(r) \approx C_{f_1,\ldots,f_s} \cdot \frac{1}{deg(f_1(x)) \cdots deg(f_s(x))} \cdot \sum_{n=2}^{r} \frac{1}{(ln(n))^s},$$

ahol

$$C_{f_1,\ldots,f_s} = \prod_{p \in P} \left(1 - \frac{w(p)}{p}\right) \cdot \left(1 - \frac{1}{p}\right)^{-s},$$

ahol $w(p)$ jelöli az

$$f_1(x) \cdots f_s(x) \equiv 0 \pmod{p}$$

kongruencia x megoldásainak a számát.

Fenti, 1962-ben publikált, sejtés ugyan a mai napig bizonyítatlan, de a gyakorlati életben nagyon jól hasznosítható. Végül 2^{33} egész számot használtunk fel a H halmaz létrehozásához, amelyekből az úgynevezett "hármas szita" módszerrel próbáltuk kiszűrni azokat, amelyek a következő három polinom valamelyikébe helyettesítve biztosan összetett számot eredményeznek.

$$f_1(x) = (h_0 + c \cdot x) \cdot 2^e - 1,$$

$$f_2(x) = (h_0 + c \cdot x) \cdot 2^e + 1,$$

$$f_3(x) = (h_0 + c \cdot x) \cdot 2^{e+1} - 1.$$

A h_0, c, e paramétereket úgy választottuk, hogy egy H-beli elemet helyettesítve körülbelül 51780 jegyű számot kapjunk, amely új világcsúcsot jelentett úgy iker, mint Sophie Germain prímeknél. A hármas szita

lényege, hogy egyszerre szitálunk mindkét típusú kombinációra. Így a szitálás tömörítő hatása nagyobb lesz, de marad esélyünk a sikeres keresésre. A szitálás folyamata egy bizonyos ponttól kezve jól párhuzamosítható, így több processzoron egyidejűleg futhat. Ehhez mi az Amsterdamban (Hollandia) található SARA központ szuperszámítógépét vehettük igénybe. Mivel a szitáláshoz egyre nagyobb prímeket használunk, egy idő után már ez az eljárás nem hatékony. Ekkor következik a H halmaz maradék elemeinek, az úgynevezett kandidátusoknak a prímtesztje, pontosabban az általuk generált számoké. Ekkor valószínűségi tesztet végeztünk, amely futása gyorsabb, mint az egzakt teszté. Ez a művelet már nem igényel nagy teljesítményű gépeket és nagy operatív memóriát, így használhattuk az egyetemi gridet. Az egzakt teszt futtatására háromszor két alkalommal volt szükség, hiszen végül két ikerprím párt illetve egy Sophie Germain prímet találtunk. Tehát sorrendben a következő világrekordokat jegyeztük:

A legnagyobb ismert ikerprím pár:

$$16869987339975 \cdot 2^{171960} \pm 1,$$

51779 számjegy.

A legnagyobb ismert Sophie Germain prím:

$$137211941292195 \cdot 2^{171960} - 1,$$

51780 számjegy.

A legnagyobb ismert ikerprím pár:

$$100314512544015 \cdot 2^{171960} \pm 1,$$

51780 számjegy.

3. Kiegészítés a gazdasági jelentéshez

Az OTKA pályázat pénzügyi zárójelentéséhez annyi kiegészítést szeretnénk fűzni, hogy a költségtervtől történő jelentősebb eltérés nincs. Az utolsó évben jelentkezik egy olyan mértékű eltérés, amely nem haladja meg az összköltségvetés 0,6 százalékát, tehát elenyésző, ráadásul nem túlköltésről van szó, csak átcsoportosításról. Megjegyezzük, hogy erre

a jelentéktelen változtatásra is igen nyomós indokunk volt. A tervek szerint három kutatónk (Kátai Imre, Bui Minh Phong és Farkas Gábor) 2006 decemberében Hanoiban vettek volna részt egy számelméleti konferencián. Azonban a nagy érdeklődésre való tekintettel további előadások tartására kérték fel őket a Saigoni egyetemen. Annak érdekében, hogy eleget tegyenek a felkéréseknek meghosszabbítottuk utazásukat, így a napidíj keretet átléptük kb 50 ezer forinttal, amely összeg az utazási keretből fedezhető. Mivel a konferencia a záró év december végén volt, előre nem volt időnk az OTKA irodától keretátcsoportosítást kérni. Összegezve, ennek a minimális tranzakciónak köszönhetően további kiváló lehetőséghez jutottunk eredményeink nemzetközi publikálásában, amely remélhetőleg javára válik a magyar tudományos életnek és így összhangban van az OTKA szellemiségével.