Szakmai zárójelentés az OTKA-67580 (2007-2011) pályázatról

A pályázati téma a korábbi OTKA-42985 (2003-2006) téma folytatása volt.

Az elmúlt 40 évben a diofantikus egyenletek elméletében rendkívül jelentős előrehaladás történt. Születtek igen általános, de ineffektív végességi tételek; explicit felső korlátokat nyertek a megoldásszámra; effektív módszereket dolgoztak ki fontos egyenletosztályokra, melyek az összes megoldás megkeresését teszik elvileg lehetővé; olyan hatékony algoritmusokat is kidolgoztak, melyek bizonyos típusú egyenletek esetén lehetővé teszik konkrét egyenletek összes megoldásának a tényleges megkeresését számítógép felhasználásával; végül a nyert módszereknek és eredményeknek számos fontos alkalmazása született, egyebek között az algebrai számelméletben és a rekurzív sorozatok elméletében. Kutatócsoportunk az OTKA 67580 sz. pályázati támogatással mind az öt fő vizsgálati irányban, nemzetközi viszonylatban is igen jelentősnek minősített eredményeket ért el. Kutatásainkat a szerződésben megfogalmazott munkatervnek megfelelően végeztük. Eredményeinket 90 tudományos dolgozatban publikáltuk, s igen sok előadást tartottunk nemzetközi fórumokon.

Eredményes tudományos együttműködést folytattunk számos külföldi matematikussal. Közös cikkeket publikáltunk amerikai, angol, ausztrál, francia, holland, horvát, indiai, japán, kanadai, mexikói, lengyel, német, osztrák és török matematikusokkal. Munkáinknak jelentős a nemzetközi visszhangja, a publikációinkra való hivatkozások száma meghaladja a 3000-et. Vizsgálatainkhoz sokan kapcsolódtak, eredményeinket, módszereinket sokan felhasználták kutatásaikban.

Tudományos eredményeinkért számos elismerésben részesültünk. Újabb OTKA pályázatunk mindhárom opponense úgy nyilatkozott, hogy a „témavezető korábbi pályázatai kiemelkedően eredményesek voltak". Győry Kálmán a Debreceni Egyetem Díszérme kitüntetésben (2010) részesült. 2008 és 2011 között az European Research Council meghívására részt vett az EU-s tudományos pályázatok elbírálásában. Pethő Attilát az MTA levelező tagjává (2010), az MTA Matematikai Tudományok Osztálya pedig osztályelnök helyettessé választotta. Pintér Ákos 2010-ben, Hajdu Lajos 2011-ben akadémiai doktori címet szerzett. Bérczes Attila 2009-ben habilitált. A csoportvezető kutatói állandó meghívottjai és felkért előadói szakterületük nemzetközi konferenciáinak. Egy nemzetközi konferenciát és több workshopot rendeztek.

Az OTKA 67580 sz. pályázat keretében végzett kutatások legfontosabb eredményeinek rövid összefoglalása

Számos jelentős effektív, kvantitatív és numerikus eredmény született egy sor alapvető fontosságú diofantikus problémával kapcsolatban. Az eredmények elsősorban szétesző forma egyenletekre, egységegyenletekre, szuperelliptikus és binom Thue egyenletekre, általánosított Fermat-típusú egyenletekre, szeparábilis egyenletekre, valamint rekurzív sorozatokra, adott diszkriminánsú, illetve adott rezultánsú binér formákra, általánosított számrendszerekre és alkalmazásaikra vonatkoznak. Az alábbiakban ismertetjük a legfontosabb eredményeket. A legkiemelkedőbb eredményeket a rövid összefoglalóban is felsoroljuk. A kutatócsoport tagjainak a közös eredményeit csak egyetlen (az alábbi sorrendben az első) helyen fogjuk ismertetni.

Győry Kálmán eredményei: Győry Kálmán a projekt keretében 17 tudományos dolgozatot publikált. Az alábbiakban részletezzük a legfontosabb eredményeit.

Általános effektív végességi tételek (részben Bérczes Attilával és Pintér Ákossal közös eredmények). A diofantikus számelméletben középponti szerepet játszanak az egységegyenletek és a szétesző forma egyenletek. Egységegyenletekre, általánosabban S- egységegyenletekre és szétesző forma egyenletekre Győry Kálmán nyerte az első effektív eredményeket, explicit korlátokat adva a megoldásokra. Ezeket a korlátokat később lényegesen élesítette és eredményeinek számos alkalmazását adta. Minden eddiginél jobb effektív egyenlőtlenségeket sikerült bizonyítania az algebrai számtestek feletti híres ABC-sejtés irányában.

A diofantikus approximációk elméletének egy klasszikus, igen sokat vizsgált területén nyert jelentős új eredményeket Bérczes Attilával és J. H. Evertsével közösen. Effektív eredményeket nyert adott algebrai számoknak egy végesen generált multiplikatív csoport elemeivel való approximációjáról. A nyert explicit alsó korlátok jelentősen pontosítják Bombieri, Cohen, Bugeaud és Gubler nevezetes eredményeit, és fontos alkalmazásokhoz vezettek diofantikus egyenletekre vonatkozóan.

Bérczes Attilával, J. H. Evertsével (és részben C.Pontreauval) közösen elsőként nyertek effektív korlátokat algebrai görbék és bizonyos egyéb sokaságok olyan pontjaira, melyek "közel" vannak egy algebrai számokból álló végesen generált multiplikatív csoporthoz, illetve még általánosabban annak divíziocsoportjához.

Számos diofantikus probléma vezethető vissza (1) Ax^n-By^n=C alakú binom Thue-egyenletekre, ahol $x, y \neq 0$, $n \geq 3$ ismeretlen egészek, A, B, C pedig rögzített, 0-tól különböző egészek. A Baker-módszer felhasználásával x és y abszolút értékére és n-re egy , A, B, C-től függő explicit felső korlát adható. Győry Kálmán és Pintér Ákos az (1) alakú egyenletek és az S –egységegyenletek közös általánosítására nyert effektív végességi tételeket. Megmutatták, hogy ha A, B, C is ismeretlenek, de csak adott $p_1, \ldots, p_s$ prímekkel oszthatók és Ax, By, C relatív prímek, úgy Ax, By, és C abszolút értékére csupán $Q = p_1, \ldots, p_s$-től függő effektív felső korlát adható. A nyert eredmény közös általánosítását adja az S- egységegyenletekre és a binom Thue-egyenletekre korábban nyert kvalitatív effektív végességi eredményeknek.

Klasszikus, sokat vizsgált egyenlet a (2) $f(x) = wy^n$ alakú szuperelliptikus egyenlet, ahol $f(X) \in Z[X]$ adott főpolinom, $w \neq 0$ rögzített egész x, y és $n \geq 3$ pedig ismeretlen egészek. Sokan nyertek effektív felső korlátot a megoldásokra, melyek azonban függnek az w-tól, az f fokszámától, valamint az f magasságától vagy diszkriminánsától. Győry és Pintér megmutatták, hogy bizonyos természetes feltételek mellett a megoldásokra olyan effektív korlát is adható, ami csupán az f fokszámától, valamint az w és az f általánosított diszkriminánsa különböző prímosztóinak szorzatától függ. A nyert eredmény már véglegesnek tekinthető abban az értelemben, hogy a korlátokban a nevezett paraméterektől való függés tovább már nem gyengíthető.

A számtestek feletti egységegyenletekre és S-egységegyenletekre vonatkozó végességi eredményeket Lang 1960-ban messzemenően általánosította a Z felett végesen generált integritástartományok esetére. Azonban a számtest esettel ellentétben Lang eredménye ineffektív. 50 év elteltével Győrynek Evertsével közösen sikerült Lang tételére effektív bizonyítást adnia, ráadásul kvantitatív formában. Az eredménynek számos fontos alkalmazása lesz.

Teljes hatványok számtani sorozatokban (Hajdu Lajossal és Pintér Ákossal közös eredmények) Ezzel a klasszikus témakörrel a 17. század óta rendkívül sokan foglalkoztak, közöttük Fermat, Euler, Liouville, Sylvester, Erdős és Siegel. Egy másfél évszázados sejtést bizonyítva Erdős és Sejfridge (1975) megmutatta, hogy $k \leq 2$ egymásra következő egész szorzata nem lehet teljes hatvány. Egy általános sejtés szerint – mely $k = 3$ esetén egészen Fermat-ig nyúlik vissza- az általánosabb (3) $x(x+d) \ldots (x+(k-1)d) = y^n$ egyenlet relatív prím x, d és $(k,x) \neq (3,2)$ mellett sem megoldható. Számos részeredmény után az első áttörést Győry (1999) érte el, aki a sejtést $k = 3$-ra bebizonyította. Ezt az eredményt Győry és Hajdú (társszerzőkkel közösen) kiterjesztette a $k < 12$ esetre, újabban pedig Győry, Hajdu és Pintér a $k < 35$ esetre. A bizonyításaik során (3)-at visszavezették (4) $Ax^n + By^n = Cz^q$, $q \in \{2, n\}$ alakú egyenletekre, majd számos mély, klasszikus és modern eredményt és módszert, közöttük a Frey görbék, Galois reprezentációk és moduláris formák módszerét használták fel a kapott (4) típusú egyenletek kezelésére.

Binom Thue egyenletek és szuperelliptikus egyenletek explicit megoldása (Pintér Ákossal és részben Bérczes Attilával közös eredmények) A $C = 1$ esetben Győry és Pintér szisztematikusan elkezdte (1) alakú egyenletek teljes megoldását korlátos A és B mellett, s max $(|A|, |B|) = 20$-ra az összes megoldást meghatározták. Újabban Bazsó Andrással és Bérczes Attilával közösen kiterjesztették (1)-re vonatkozó eredményeiket arra az estre, amikor az A, B, C pozitív együtthatók értéke legfeljebb 30, C=1 mellett legfeljebb 50, $A = C = 1$ mellett pedig legfeljebb 400. Néhány kivételtől eltekintve a tekintett egyenleteket teljesen megoldották.

A szerzők a bizonyítások során a modern diofantikus számelmélet szinte valamennyi fontos módszerét kombinálták, beleértve a Baker-módszert, a hipergeometrikus módszert, a lokális módszert, a modern számítógépes módszereket, valamint a Fermat-sejtés bizonyítására kidolgozott módszernek a szerzők által továbbfejlesztett változatát. $C = 1$ és $q \in \{3,n\}$ esetén $n \geq 13$ prímekre a (4) alakú egyenletek egy széles osztályát megoldották. Eredményük az $A = B = C = 1$ esetben $n \geq 13$-ra tartalmazza Wiles híres tételét a Fermat-féle egyenletre vonatkozóan.

Adott fokszámú és adott diszkriminánsú, illetve adott rezultánsú binér formák (Bérczes Attilával közös eredmények) Győry Kálmán a 70-es évek elején számos alkalmazással járó effektív végességi tételeket nyert adott diszkriminánsú egész együtthatós főpolinomokról. Később végességi eredményeket publikált adott fokszámú és adott rezultánsú egész együtthatós főpolinomokról is. Az eredmények a "monic" binér formák nyelvén is megfogalmazhatók. Birch és Merriman – Győrytől függetlenül- analóg, de ineffektív tételt nyert adott diszkriminánsú binér formákról, mely azonban nem

adja ki speciális estként a "monic" estben nyert végességi állításokat. Evertse és Győry (1991) kvantitatív formában effektivizálta a Birch-Mirriman tételt.

Az adott diszkriminánsú illetve adott rezultánsú binér formák természetes módon ekvivalenciaosztályokba sorolhatók. Bérczessel és Evertsével közösen adott felbontási testtel rendelkező binér formák esetén explicit és egyben uniform felső korlátokat adtak az említett ekvivalenciaosztályok számára. Alkalmazásként fontos új eredményt nyertek Thue-Mahler egyenletek megoldásszámára vonatkozóan. Az említett eredményekhez szorosan kapcsolódva megmutatták, hogy adott algebrai számtestben legfeljebb véges sok olyan monogén rend van, mely három egymással nem ekvivalens algebrai egésszel is generálható a racionális egészek gyűrűje felett. Eredményüket ennél lényegesen általánosabban, Z felett végesen generált tartományok feletti rendek esetén is bizonyítják.

Aritmetikai gráfok: A végesen generált integritástartományokon korábban Győry által bevezetett aritmetikai gráfok számos alkalmazáshoz vezettek. Újabban olyan általános kvantitatív eredményeket nyert az említett gráfokra vonatkozóan, melyek fontos új alkalmazásokat eredményeztek rezultáns egyenletek és diszkriminánsegyenletek vonatkozásában.

Pethő Attila eredményei: Pethő Attila 2007 és 2011 között 19 tudományos dolgozatot készített az OTKA pályázat támogatásával.

Akiyamaval, Brunotteval és Thuswaldnerrel tovább folytattuk a shift radix rendszerek tulajdonságainak a tanulmányozását. Cikksorozatunk 3. részében meghatároztuk az adott fokszámú és adott korlát alatti konstans tagú CNS polinomok eloszlását. A vizsgálatot tovább folytattuk a 4. részben, ahol a Pisot polinomok számára is sikerült aszimptotikus formulát bizonyítani, sőt a maradéktag nagyságrendjére is adtunk becslést. Ugyanebben a dolgozatban az F-tulajdonságú Pisot polinomok számára is tudtunk aszimptotikus formulát bizonyítani, de maradéktag nélkül. Utóbbi dolgozat gondolatmenetét követve Madritsch-csal lényegesen javítottuk az egész együtthatós kontraktív polinomok
eloszlására vonatkozó eredményünket. Akiyamaval és Brunotteval jellemeztük a harmadfokú, reducibilis CNS polinomokat. Hasonló eredmény az általános esetben nem várható, mint azt korábbi munkáink mutatják.

Foglalkoztunk a valós együtthatós kontraktív polinomok határának vizsgálatával is. Ekkor fontos probléma a határpontok osztályozása abból a szempontból, hogy egy hozzájuk rendelt majdnem lineáris leképezés pályái ciklikusak-e vagy van közöttük divergens. Beláttam, hogy ha a polinomnak nincsenek az egységgyököktől különböző gyökei a komplex egységkörön és azok is egyszeresek, akkor az SRS leképezéssel definiált sorozat növekménye egyenletesen korlátos. Ez bizonyos esetekben algoritmust ad a pontok osztályozására. Kirschenhoferrel és Thuswaldnerrel a háromdimenziós határhalmaznak egy az aranymetszéssel definiált pontját elemeztük. Szoros kapcsolatot találtunk az így definiált sorozat periódikussága, illetve divergenciája illetve a kezdőtagok Zeckendorff előállítása között.

A kétdimenziós eset határát az $(1, y)$, ahol $-2 < y < 2$, szakasz kivételével korábban teljesen leírtuk és megfogalmaztuk azt a sejtésünket, hogy az ezekhez a pontokhoz tartozó pályák is periódikusak. Legyen $y = 2 \cos z$. Akiyamaval, Brunotteval és Steinerrel beláttuk, hogy sejtésünk igaz, ha a $\cos z + i \sin z$ komplex szám másodfokú algebrai szám. Ezen felül leírtuk a lehetséges periódushosszakat is. Kirschenhoferrel és Thuswaldnerrel példákat mutattunk arra, hogy háromdimenziós esetben a határhalmaz pontjainak tulajdonságai a sorozat kezdőértékétől is függhetnek.

Zieglerrel a Pell egyenlet olyan megoldásait vizsgáltuk, amelyek valamely koordinátában számtani sorozatot alkotnak. Az ilyen sorozatok legnagyobb elemére és így hosszára is explicit felső korlátot adtunk. Megmutattuk azt is, hogy minden háromtagú számtani sorozathoz végtelen sok $x^2 - dy^2 = m$ Pell egyenlet található, amelyek megoldásai között az y koordinátában ez a sorozat előfordul. Beláttuk, hogy öttagú számtani sorozatokra már csak véges sok Pell egyenlet létezik hasonló tulajdonsággal. Négytagúak esetén találtunk mindkét alternatívára példát. Dujellával és Tadiccsal megmutattuk, hogy a Zieglerrel talált – 0, 1, 2, 3 - négytagú számtani sorozat jelenti az egyetlen kivételt. Bérczessel és Hajduval ezen eredmények egy részét általánosítottuk normaforma egyenletekre. Érdekes, hogy a normaforma egyenletekre illeszkedő számtani sorozatok hosszára vonatkozó becslésünk csak a forma fokszámától és a konstans tagtól függ.

Zannier 2008-ban jellemezte az összes olyan polinomot, amelyeknek rögzített számú nem nulla együtthatója van és felbonthatatlan a függvények kompozíciójára nézve. Fuchssal ugyanezt a problémát vizsgáljuk, azonban nem a 0-tól különböző együtthatók, hanem a gyökök számát rögzítjük.

Megmutattuk, hogy ha egy racionális törtfüggvény gyökei és pólusai számát rögzítjük, akkor néhány triviális esettől eltekintve csak véges sok, effektíven meghatározható, felbontható racionális törtfüggvény létezik.

Az algebrai számelmélet egyik klasszikus problémája algebrai számtestek testindexének meghatározása. Pohsttal meghatároztuk a trikvadratikus számtestek testindexének lehetséges értékeit. Ezen felül megmutattuk, hogy bármely p prímszámhoz és n természetes számhoz p^n osztja azon multikvadratikus számtest testindexét, amelyet elég sok, multiplikative független négyzetszám adjungálásával kapunk Q-ból.

Husztival egy biztonságos vizsgáztató rendszert írunk le. Biztonságos abban az értelemben, hogy mind a vizsgázó, mind a vizsgáztató anonim marad a regisztráció után, de a vizsga befejezése után a vizsgázó egyértelműen azonosítható, így az érdemjegyét hozzá tudjuk rendelni. Bérczessel és Folláthal olyan hash függvényt definiálunk, amelyik nem invertálható egyszerű próbálgatással és megmutatjuk, hogy biztonságos, ha az egész számok faktorizációjának problémája nehéz. A konstrukció többváltozós, hiányos polinomokat használ.

Gaál István eredményei: Gaál István a projekt keretében 10 dolgozatot publikált.

M. Pohsttal közösen megmutatta, hogy rezultáns típusú egyenletek esetén, ha az egyik polinom adott és a másik polinom ismeretlen, akkor az egyenlet megoldása kétváltozós egységegyenletek megoldására vezethető vissza. Ezt fölhasználva függvénytestek és algebrai számtestek esetén is algoritmust adott az egyenlet megoldására. Ugyanezen észrevétel vezetett a rezultáns típusú egyenletek megoldásszámára adott eddig ismert korlátnak a javításához is. Véges testek feletti függvénytestek esetén algoritmust adott többváltozós egységegyenletek megoldására. Ennek számos további alkalmazása lesz, elsőként normaforma egyenletek megoldásának kiszámítására használták fel.

M. Pohsttal közösen a globális függvénytestek feletti egy illetve két polinom változós rezultáns típusú egyenleteket visszavezették két-illetve háromváltozós egységegyenletekre. Felhasználva az egységegyenletekre vonatkozó korábbi tételeiket, hatékony eljárást adtak rezultáns tipusú egyenletek megoldására globális függvénytestek felett.

M. Pohsttal közösen eljárást adtak általános normaforma egyenletek megoldására globális függvénytestek felett, felhasználva a többváltozós egységegyenletek megoldására kifejlesztett módszerüket. Továbbá általános feltételek mellett az F(x,y)=G(x,y) egyenlet összes megoldásának kiszámítására adtak algoritmust a Q(x) függvénytest felett.

M. Pohsttal közösen hatékony eljárást adtak függvénytestek felett az összes olyan teljes hatvány meghatározására, melyek két S-egység összegei. Továbbá C. Fiekerrel és M. Pohsttal közösen hatékony algoritmust adtak a függvénytestek feletti Mordell-egyenlet megoldására. A módszer számtestek felett is alkalmazható.

Szabó Tímeával közösen kiszámította több ezer harmadfokú gyökbővítés minimális indexét. Eredményük mutatja, hogy a diszkrimináns abszolút értékének növekedésével a minimális index tendenciájában nő.

Pintér Ákos eredményei: Pintér Ákos a projekt keretében 18 tudományos közleményt publikált. Benyújtotta és megvédte az akadémiai doktori értekezését, melyben a binom Thue egyenletekre, ternér egyenletekre és polinomok hatványértékeire vonatkozó, már publikált eredményeit foglalta össze.

A Bilu-Tichy tétel felhasználásával ineffektív végességi állításokat nyert kombinatorikus geometriai hátterű diofantikus egyenletek megoldásszámára. Társszerzőkkel közösen megoldotta az x^2+2^a11^b=y^n egyenletet.

Társszerzőkkel közösen a balansz számok egy általánosítását adta, effektív és ineffektív tételeket nyert ezen általánosított balansz számok számára. Vizsgálták az f(x)=g(y) egyenletet , ahol az f és g polinomok trinomok. Végességi állítást nyertek a megoldások számára. Alsó becslést adott rekurzív sorozattal meghatározott polinomok egyszeres és különböző gyökeinek számára.

Korábbi vizsgálatait kiterjesztette binom Thue-egyenletek egy széles osztályának teljes megoldására. Egy speciális hézagelv segítségével egy Runge-tipusú diofantikus egyenlet összes megoldását meghatározta,

Számtani sorozatokkal kapcsolatos karakterizációját adta a klasszikus Fibonacci sorozatnak. Alsó becslést adott bizonyos másodrendű rekurziót kielégítő polinomcsaládok egyszeres gyökeinek a számára.

Számtani sorozat tagjainak k-adik hatvány összegét, mint polinomot tekintve megadta a polinom más polinomokkal való összetételét (decompositio-ját).

Hajdu Lajos eredményei: Hajdu Lajos az OTKA pályázat keretében 25 tudományos dolgozatot publikált. Benyújtotta és megvédte akadémiai doktori értekezését. Disszertációjában különböző multiplikatív tulajdonságú halmazokban található számtani sorozatokra vonatkozó eredményeit összegezte.

Diofantikus problémák. A „majdnem" teljes hatványokból álló számtani sorozatok irodalma rendkívül gazdag, a területet többek között Fermat, Euler, Erdős neve fémjelzi. A korábbi idevágó eredményeket lényegesen javítva, Győryvel és Pintérrel megmutatták, hogy $3<k<35$ esetén egy számtani sorozat k egymást követő tagjának szorzata nem lehet teljes hatvány. Az eredmény bizonyítása többek között mély kombinatorikus megfontolásokat, illetve a Fermat-egyenlet megoldásában is kulcsszerepet játszó moduláris módszer alkalmazását igényli. A bizonyítás a korábbiakhoz képest nem csupán mennyiségi, hanem jelentős minőségi továbblépést is jelent. Ekkora tagszám esetén ugyanis nem használhatók a korábbi kombinatorikus megfontolások, az egymást követő számok prímtényezőivel kapcsolatos összefüggéseknek (illetve számos más módszernek) az eddigieknél lényegesen mélyebb, pontosabb megértésére és használatára volt szükség.

Társszerzőkkel a köbök illetve ötödik hatványok esetében a fenti területen lényeges előrelépést ért el, megmutatva, hogy $3<k<39$, illetve $3<k<54$ esetén sem lehet egy számtani sorozat k darab egymást követő elemének szorzata teljes harmadik, illetve ötödik hatvány. E hatványokra korábban csak klasszikus eszközök álltak rendelkezésre. Nekik sikerült először modern algebrai geometriai eszközöket (elliptikus görbék, Chabauty-módszert) alkalmazniuk ezekre az esetekre is.

Több tételt bizonyított különböző hatványokból álló számtani sorozatokról. Megmutatta, hogy egy ilyen sorozat hossza valamely tagja, illetve a differencia függvényében is korlátozható. Sikerült jellemeznie az úgynevezett „hatványgazdag" számtani sorozatok lehetséges tagszámait. Tengellyel közösen éles korlátot nyert az n-edik hatványokból valamint négyzetekből, illetve köbökből álló számtani sorozatok hosszára.

Sikerült csak természetes paraméterektől függő felső korlátot adnia S-egységek összegeiből álló halmazokban található számtani sorozatok hosszára. Tételét Green és Tao prímekből álló számtani sorozatokkal, kapcsolatos eredményével kombinálva, negatív választ adott Pohst egy prímszámok előállítására vonatkozó kérdésére. Később az eredeti tételt Lucával kvantitatív alakban is levezette.Részben a fenti eredmény alkalmazásával, Bérczes Attilával és Pethő Attilával több végességi eredményt igazoltak norma forma egyenletek megoldáshalmazában található számtani sorozatok hosszára vonatkozóan.

Ádámmal és Lucával megmutatták, hogy bármely k-hoz található olyan m, hogy bármely k darab szám hatványainak adott lineáris kombinációi csak „kevés" maradékosztályt érintenek modulo m. Ezt az eredményt később Tijdemannal pontosították, választ adva Nathanson egy kapcsolódó kérdésére.

Bérczessel, Dujellával és Lucával több újszerű tételt igazolt olyan diofantikus halmazokra vonatkozóan, ahol az elemek eltolt szorzata különböző hatvány is lehet.

Párhuzamosan több Mordell-Weil bázist használva Kováccsal kidolgoztak egy olyan eljárást, amely az elliptikus egyenletek megoldására szolgáló, Gebel-Pethő-Zimmer illetve Stroeker-Tzanakis eredményein alapuló Ellog algoritmus javítását szolgáltatja. Az S-egységegyenletek esetében hasonló irányba tett lépéseket: olyan S-alapegység rendszer létezését igazolta konstruktív módon, amely az LLL-módszer alkalmazásakor a legnagyobb hatékonyságot teszi lehetővé.

Polinomok. Győryvel és Tijdemannal közösen több új eredményt bizonyított Schur- valamint Pólya-típusú irreducibilitási kérdésekkel kapcsolatban. Eredményeik több klasszikus tétel kiterjesztését, élesítését jelentik. Az általuk igazolt új összefüggések több fontos (például algebrai számelméleti) alkalmazását is adták.

Bizonyos feltételek mellett Tijdemannal jellemzését adták azon polinomoknak, melyek végtelen sok k-tagú polinomot osztanak. Eredményük a kapcsolódó, Posner és Rumsey illetve Győry és Schinzel nevéhez fűződő sejtéssel illetve problémával kapcsolatban is új információkkal szolgál.

Egész számok legnagyobb közös osztóival kapcsolatos eredmények. Recaman egy 1978-ban megfogalmazott problémája a következő: határozzuk meg azokat a p prímszámokat, melyekre az első p darab prím teljes maradékrendszert alkot modulo p. A kérdéssel, illetve a kapcsolódó témakörrel rengetegen foglalkoztak. Saradhával megmutatták, hogy a Recaman problémájában szereplő tulajdonság egyedül $p=2$ esetén teljesül. Saradhával és Tijdemannal a probléma egy általánosabb, Pomerance-tól származó alakját is eredményesen vizsgálták, sőt a Riemann hipotézist feltételezve

teljesen meg is oldották azt. A fenti kérdések vizsgálata során az egy adott n szám illetve egy adott intervallumban szereplő egészek legnagyobb közös osztójával kapcsolatos Jacobsthal függvény is fontos szerephez jut. Saradhával megcáfolták Jacobsthal egy 1962-ben a j(n) függvény viselkedésével kapcsolatban megfogalmazott sejtését. A bizonyítások során több különböző prímszámelméleti eredmény és szitamódszer felhasználása mellett hatékony szitáló algoritmusok kidolgozására is szükségük volt.

Saradhával több eredményt is nyert Pillai egy adott intervallumban található egészek legnagyobb közös osztóival kapcsolatos problémájára vonatkozóan. Egyrészt sikerült a problémában kulcsszerepet játszó paramétert (a vizsgált intervallum hosszát) sok részestben meghatározniuk, másrészt a probléma különböző általánosításait is kezelni tudták.

Schinzellel és Skalbával közösen megmutatták, hogy (bizonyos speciális kivételektől eltekintve) bármely szám „elég sok" osztóját kiválasztva mindig találunk három olyan osztót, melyek szorzata teljes négyzet. Eredményüknek bizonyos halmazok sűrűségére vonatkozó több fontos alkalmazását is adták.

Diszkrét tomográfia. A diszkrét tomográfia alapproblémája: határozzuk meg egy bináris mátrix elemeit, pusztán a mátrix bizonyos vonalösszegeinek (például sor- és oszlopösszegeinek) ismeretében. Egy korábbi eredményükben Tijdemannal megmutatták, hogy a kérdés tárgyalása során a probléma legrövidebb valós megoldása fontos szerepet játszik. Társszerzőkkel közösen újszerű, általános eredményeket nyert a legrövidebb megoldás előállításával kapcsolatban. Eredményeiknek több fontos **alkalmazását** is adták, például az azonos vonalösszegű mátrixok távolságára vonatkozóan.

Digitális képfeldolgozás. Hajdu Andrással és Tijdemannal több speciális, de fontos esetben sikerült meghatározniuk a négyzetrácson az Euklideszi metrikát legjobban approximáló szomszédsági sorozatot.

Különböző algebrai és egyéb eszközök felhasználásával igazolták egy újszerű kombinált rendszer hatékonyságát bizonyos típusú, orvosi jellegű képfeldolgozási problémák kezelésére.

Bérczes Attila eredményei. Bérczes Attila a projekt keretében 16 tudományos dolgozatot publikált.

A diofantikus egyenletek elméletének egyik intenzíven fejlődő ága az explicit módszerek alkalmazása egyenletek teljes megoldására. Ezen belül az egyik népszerű irány a Ramanujan-Nagell egyenlet különféle általánosításainak vizsgálata. Pink Istvánnal közösen teljesen megoldottak két fontos általánosított Ramanujan-Nagell egyenletet.

A debreceni számelméleti kutatócsoport kezdeményező szerepet töltött be a norma forma egyenletek megoldáshalmazában található számtani sorozatok vizsgálatában. Bérczes Attila Hajdu Lajossal és Pethő Attilával közösen jelen pályázat keretei között is folytatta ezen kutatásokat. Több kvalitatív és kvantitatív végességi eredményt értek el abban az esetben, amikor a számtani sorozat a megoldáshalmazban a megoldások egy rögzített koordinátájában jelenik meg. Ugyanezen kutatási területen Zieglerrel közösen Pell egyenletek megoldáshalmazában található mértani sorozatokkal kapcsolatban értek el eredményeket, továbbá meghatározták a Lucas sorozatokban található összes mértani sorozatot.

Választ adott Ruzsa Imre egy problémájára. Egy 2004-ben Debrecenben tartott előadásán Ruzsa azt kérdezte, hogy mennyi lehet az elemszáma egy véges, 1-nél nagyobb pozitív kvóciensű mértani sorozatot tartalmazó halmaz összeghalmazának. A kérdés három-, illetve négytagú polinomok közös gyökeinek vizsgálatára vezethető vissza.

Liptai Kálmánnal és Pink Istvánnal közösen belátták, hogy egy triviális esettől eltekintve nincs olyan egészekből álló R_n másodrendű rekurzív sorozat, mely kísérőpolinomjának diszkriminánsa pozitív, és amely valamilyen n>1, k>0 egész esetén teljesíti az R_1+R_2+...+R_{n-1} = R_{n+1} +R_{n+2}+...+ R_{n+k} egyenletet.

Lucaval közösen a nevezetes Bernoulli számok számlálójának legnagyobb prímtényezőjére, illetve a számláló számjegyeinek összegére vonatkozó eredményeket nyertek

Járási Istvánnal közösen a kutatócsoport elméleti kutatásainak közvetlen gazdasági-társadalmi hasznosíthatóságát is alátámasztva, index formák kriptográfiai alkalmazásának lehetőségét vizsgálták. Ez a munka Pethő és Bérczes egy korábbi, norma formákkal kapcsolatos kriptográfiai vizsgálatának egyenes folytatása. Dolgozatukban javaslatot tesznek egy index formára alapozott egyirányú hash függvény használatára, melyről matematikailag belátták, hogy ütközésmentes. Az általuk javasolt hash függvény lavina hatását számítógépes kísérletekkel vizsgálták. A vizsgálatok azt mutatják, hogy az általuk javasolt függvény ebből a szempontból is jól viselkedik és biztonságosan működik.

A norma illetve index formákra alapozott hash függvények a formák homogenitása miatt több technikai problémát is okoztak. Ezért egy újabb dolgozatban, az ilyen típusú problémákat megelőzendő, társszerzőkkel közösen olyan hash függvényre tesznek javaslatot, melyek alapjául egy olyan többváltozós polinom szerepel, mely két különböző fokszámú homogén polinom összege, melyek közül a magasabb fokszámúban minden változó szerepel a polinom fokszámával megegyező fokszámon is. Az ezek segítségével definiált hash függvényről a szerzők belátják, hogy ütközésmentes. Jelen algoritmus a korábbi javasolt algoritmusoknál sokkal gyorsabb, ugyanis ebben az esetben a biztonságot nem veszélyezteti az, ha egy véges prímtest felett dolgozunk.

.