A T48791 számú OTKA pályázat (2005–2008) zárójelentése

A kutatócsoport tagjai a számelmélet több területén értek el jelentős eredményeket, részben társszerzőkkel.

Bérczes Attila

Pethő Attilával közösen egy korábbi dolgozatban belátták, hogy egy normaforma egyenletnek csak véges sok olyan megoldása van, ahol a megoldások koordinátái egy számtani sorozatot alkotnak. Új eredményként az $x^n = a$ tulajdonságú elemekkel definiált norma foma egyenletek minden számtani sorozatot alkotó megoldását meghatározták $0 < a < 100$ mellett, illetve Pethővel és Zieglerrel közösen a legegyszerűbb harmadfokú testek feletti normaforma egyenletet oldották meg ugyanezen feltétel mellett.

Hajdu Lajossal és Pethő Attilával közösen folytatták a norma forma egyenletek számtani sorozatot alkotó megoldásainak vizsgálatát.

J.-H Evertsevel és Győry Kálmánal közösen vizsgálták rezultáns egyenletek megoldásszámát és komoly áttörést elérve olyan esetekben is sikerült a megoldáscsaládok számára felső korlátot adniuk, amely esetekben korábban csak kvalitatív végességi tételek születtek, és ezen esetekben idáig nem is látszott hogyan lehetne áttörést elérni.

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.

Két dolgozatban, Jan-Hendrik Evertse-vel, Győry Kálmánnal és részben Corentin Pontreau-val közösen effektív végességi vizsgálatokat végeztek tóruszok bizonyos részvarietásainak pontjaival kapcsolatban. A tekintett részvarietások olyanok, hogy lehetővé teszik a Baker-módszer alkalmazását.

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 az teljesen megoldották az $x^2 + p^{2k} = y^n$ egyenletet x, y, k, n változóiban, feltéve, hogy p egy 100-nál kisebb pozitív prím, $x > 0, y > 1, n > 2$ prím és $\gcd(x, y) = 1$.

Gaál István

Tovább folytatódott algebrai számtestek hatvány egész bázisainak vizsgálata, Robertsonnal közösen bizonyos körosztási testek esetén értek el újabb eredményeket.

Ebben az időszakban kezdődött el M. Pohst-tal közösen bizonyos típusú diofantikus egyenletek vizsgálata függvénytestek felett. Korábban számos szerző vizsgált hasonló problémákat 0 karakterisztikájú vagy prím karakterisztikájú esetekben is, algebrailag zárt konstans testeket vége. A mostani vizsgálatok alapvető újszerűsége abban áll, hogy az itt vizsgált függvénytestek valamely véges test feletti függvénytestek.

Ilyen típusú globális függvénytestek felett a diofantikus egyenletek megoldásának alapjául szolgáló egységegyenletek megoldásait sikerült leírni. Kétváltozós egységegyenletek esetén megmutatták, hogy az egységegyenlet minden megoldása vagy korlátos méretű, vagy ilyen megoldások p-edik hatványa (p karakterisztikában ha $x + y = 1$, akkor $x^p + y^p = 1$ és viszont). Ezt az eredményt globális függvénytestek feletti Thue egyenletekre és bizonyos típusú szétesők forma egyenletekre alkalmazták.

Ugyancsak M. Pohst-tal közösen megmutatták, hogy a $Res(f, g) = r$ rezultáns típusú egyenletek esetén, ha az egyik polinom ismert, akkor a másik polinom kiszámítása kétváltozós egységegyenlet megoldására vezet. Ezt felhasználva a számtest esetben és függvénytest esetben is algoritmust adtak egy polinom változós rezultáns típusú egyenletek megoldására.

Megmutatták továbbá, hogy globális függvénytestek feletti többváltozós egységegyenletek megoldása visszavezethető kevesebb változós egységegyenletek megoldására. Ezzel algoritmust nyertek többváltozós egységegyenletek megoldására globális függvénytestek felett. Ennek első alkalmazásaként bizonyos típusú többváltozós normaforma egyenletek megoldására adtak eljárást. Nyilvánvaló, hogy ennek az eredménynek számos további alkalmazása is lesz.

Hajdu Lajos

Diofantikus problémák. A "majdnem" teljes hatványokból álló számtani sorozatok irodalma rendkívül gazdag. Az egyik legfontosabb problémát az összes adott tulajdonságú sorozat meghatározása jelenti, rögzített tagszám esetén. Több szerző eredményeihez kapcsolódva, a korábbi idevágó eredményeket lényegesen javítva Bennettel, Bruinnal és Győryvel megmutatták, hogy $3 < k < 12$ 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 igényelte. Ezt az eredményt Győryvel és **Pintérrel** a pályázat utolsó évében sikeresen kiterjesztették a $3 < k < 35$ esetre. Ez a javítás nem csupán mennyiségi, hanem jelentős minőségi továbblépést is jelentett. Ekkora tagszám esetén ugyanis már 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. Részben önállóan, részben Bruinnal, Győryvel és Tengellyel közösen több eredményt nyert olyan számtani sorozatokkal kapcsolatban is, melyekben a tagok különböző kitevőjű hatványok is lehetnek. Leírták az összes olyan számtani sorozatot, melyek csupán négyzetszámokból és köbszámokból állnak. Ezen kívül sikerült jellemezni azon számtani sorozatokat, melyek tagjai teljes n-edik hatványok, illetve négyzetek vagy köbök. Az eredmények többek között Euler, Darmon és Merel bizonyos idevágó eredményeinek egyfajta továbbvitelét is jelentik. Ezen túl jellemezte az összes ún. "hatványgazdag" számtani sorozatot is. Végül, megmutatta, hogy ha X egy 2-nél nagyobb abszolút értékű teljes hatvány, akkor bármely, az X-et tartalmazó teljes hatványokból álló számtani sorozat hossza X segítségével korlátozható.

Sikerült csupán a 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, általános formában negatív választ adott M. Pohst egy prímszámok előállításával kapcsolatos problémájára. Az alaperedményt **Bérczes Attilával** és Pethő Attilával norma forma egyenletek megoldáshalmazában található számtani sorozatok hosszának korlátozására is alkalmazni tudták. Később az eredeti tételt Ádámmal és Lucával kvantitatív alakban is levezették.

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. Eljárásuk eredményeként a konkrét egyenletek megoldásához szükséges idő akár a korábbi idő 10-20 százalékára is olvadhat.

Polinomok. Bizonyos feltételek mellett Tijdemannal egy 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. Turi-Naggyal közösen számos tételt nyertek bizonyos speciális, de fontos polinomcsaládokhoz tartozó polinomok összegének gyökszerkezetével kapcsolatban. Eredményüknek több, diofantikus egyenletekre vonatkozó alkalmazását is adták.

Diszkrét tomográfia. Tijdemannal felkérésre egy könyvfejezetet készített korábbi valamint új diszkrét tomográfiai eredményeik felhasználásával. Az általuk lefektetett elméleti alapok összefoglalása mellett egy új kutatási irányt is kezdeményeztek, töröttvonalak (illetve még általánosabb görbék) mentén vett vonalösszegek vizsgálatával. Az ilyen típusú vizsgálatok gyakorlati szempontból is érdekesek lehetnek, például fénytörés esetén. Egy önálló cikkben bizonyos esetekben egyértelmű rekonstrukciót garantáló feltételeket adott.

Szomszédsági szekvenciák. Hajdu Andrással és Tijdemannal sikerült jellemezniük a metrikát generáló végperiodikus szomszédsági szekvenciákat $\mathbb{Z}^n$-en. Eredményeink lényegesen továbbviszik és kiterjesztik Yamashita és Ibaraki idevágó, a témakör alaperedményeinek számító tételeit. Hajdu Andrással, illetve Hajdu Andrással, Fazekassal és Tóthttal összegezte illetve továbbvitte az ún. oktagonális szomszédsági szekvenciák hálóstruktúrájával kapcsolatos vizsgálataikat.

Diszkrét függvényegyenletek. Több szerző eredményeihez kapcsolódva Hajdu Gabriellával meghatároztí az ún. Hosszú-féle függvényegyenlet összes megoldását a Gauss-egészek és az Eisenstein-egészek felett. Ezen kívül több, Ramanujan egy azonosságára vonatkozó eredmény kiterjesztését és általánosítását adták.

Liptai Kálmán

Florian Lucával, **Pintér Ákossal** és Szalay Lászlóval közösen általánosította a balansz szám fogalmát, és végességi állítást nyert az ehhez kapcsolódó

$f(x) = g(y)$ alakú szeparábilis diofantikus egyenlet megoldásainak számára.

Nyul Gábor

Gaál Istvánnal közös, 2006-ban megjelent cikkében az index forma egyenlet p-adikus változatának megoldásával foglalkozott. Eltekintve egy N. P. Smart által megoldott példától, ilyen egyenletet numerikusan eddig még nem oldottak meg. A bikvadratikus számtestek esetén vizsgálták ezeket az egyenleteket, és adtak a megoldásukra jól működő algoritmust. Az esetek jelentős részében a megoldást egy racionális egészek feletti S-egység egyenlet megoldására sikerült visszavezetni, ezekben az esetekben módszerük különösen hatékony. A kivételes esetben, amikor az egyenlet jobb oldalán szerepel olyan prímszám, mely a bikvadratikus számtest mindhárom másodfokú résztestében két különböző prímideál szorzatára bomlik, meg kell még oldani egy S-egység egyenletet a negyedfokú test felett is. Módszerüket több példán keresztül is szemléltették.

2007-ben benyújtotta és sikeresen megvédte PhD doktori értekezését. Ebben összefoglalta algebrai számtestek monogenitásával, hatvány egész bázisokkal, index forma egyenletekkel és testindexekkel kapcsolatos eredményeit. A testindexek (azaz az algebrai számtestbeli primitív algebrai egész elemek indexének legnagyobb közös osztója) meghatározásával foglalkozó részben parametrikus számtestcsaládokban vizsgálódunk. Egyrészt az ún. Kishi-féle harmadfokú számtesteknek adtuk meg egy egész bázisát, kiszámoltuk az ezekhez tartozó index formákat, és ezek vizsgálatával bebizonyítottuk, hogy a számtestcsalád minden tagjának testindexe 1. Másrészt a legegyszerűbb negyedfokú számtestek családjában igazoltuk, hogy a testindex 1 vagy 2, attól függően, hogy a testet meghatározó paraméter páros vagy páratlan. A disszertáció ezen fejezete egyelőre még nem lett publikálva, mivel további számtestcsaládok hasonló vizsgálata van még folyamatban, illetve tervezve.

Florian Lucaval közösen egy közlésre elfogadott cikkében egy korábban már vizsgált, binomiális együtthatókra vonatkozó oszthatósági problémával foglalkozik. Nevezetesen, rögzített k pozitív egész esetén keressük azokat az n értékeket, melyekre $nk \mid \binom{n}{k}$ teljesül. Korábban Nyul Gábor abban az esetben adott választ a problémára, amikor k prímszám vagy $k = 4$. Ebben a cikkben tetszőleges k esetén megoldották a problémát, sikerült leírni azt az m értéket, amire teljesül, hogy a megoldások halmaza bizonyos modulo m maradékosztályok uniója, továbbá prímhatvány k esetén pontosan le is írták

ezeket a maradékosztályokat. A gondolatmenetet követve bármilyen konkrét k esetén lehetséges a maradékosztályok meghatározása.

Olajos Péter

Orosz Erzsébettel közös cikkében a LaTeX programozási nyelv és a matematikai módszertan egy lehetséges kapcsolatát mutatja be. A dinamikus LaTeX alapú pdf fóliák megvalósítási lehetőségei a módszertani elveket nagy mértékben támogatják, ezzel segítve pl. akár diofantikus egyenletek megoldási lehetőségeinek, függvények ábrázolásának, tulajdonságainak szemléltetését. A cikkben számos stílus és módszer kerül bemutatásra.

Hajdu Lajossal, Liptai Kálmánnal és **Pintér Ákossal** közösen a balancing számok egy újabb általánosítását vizsgálja. Ebben több érdekes tulajdonság mellett azt is bizonyítja, hogy bizonyos feltételek mellett, csak egy olyan (a, b) tipusú balancing szám van, mely teljes hatvány. A bizonyítás során felhasználja Bennett és Skinner egy mély eredményét, továbbá az elliptikus és hiperelliptikus görbékre vonatkozó egész pont keresési algoritmusokat (pl. MAGMA program használata).

Liptai Kálmánnal közösen a korábban bevezetett (a, b) tipusú balancing számokra vonatkozóan vizsgálják meg azt a kérdést, hogy vannak-e azonos elemek különböző tipusú balancing számcsaládok között. A probléma szimultán Pell-egyenletek megoldására vezet vissza, melyeket Szalay egy új eredménye ill. a Baker-Davenport módszer segítségével oldanak meg.

Pink István

A kétváltozós polinomiális diofantikus egyenletek egy fontos osztályát képezik az ún. szuperelliptikus egyenletek. Legyen $f(x) \in \mathbb{Z}[x]$ egy legalább két különböző gyökkel rendelkező $d \geq 2$ fokú egész együtthatós polinom és legyenek $w \neq 0$ valamint $n \geq 2$ adott egész számok. Tekintsük az

$$f(x) = wy^n \tag{1}$$

ún. szuperelliptikus egyenletet, ahol az ismeretlenek az x, y racionális egészek.

Az elmúlt években sokan vizsgálták az (1) szuperelliptikus egyenletet abban a speciálisabb esetben, amikor az $f(x)$ egy adott negatív diszkriminánsú kvadratikus főpolinom sőt abban az általánosabb esetben is, amikor az $f(x)$ diszkriminánsának csak a prímosztói fixek. A jelenleg ismert

hatékony effektív módszerek (pl. Baker-módszer, moduláris módszer, Lucas-sorozatokban előforduló primitív prímosztók) alkalmazásával és kombinálásával sok esetben sikerült az (1) egyenlet összes megoldását megadni.

Ehhez a vizsgálatokhoz kapcsolódva, **Pink** az (1) egyenletet vizsgálta abban az esetben, amikor $w \in \{1, 4\}$ valamint $f(x)$ egy olyan kvadratikus főpolinom amelynek a diszkriminánsa nem rögzített, hanem adott prímekkel osztható. Bugeaud és Shorey egy eredményének gondolatmenetét kiterjesztve és ezt lokális módszerekkel kombinálva éles explicit korlátokat nyert az n kitevőre. A kapott becsléseket Cohn és de Weger bizonyos eredményeivel kombinálva megadta az

$$x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta = y^n$$

egyenlet összes olyan $x, y, n, \alpha, \beta, \gamma, \delta$ megoldását melyekben $\alpha \geq 1$. Ezzel jó néhány korábbi idevágó eredmény általánosítását nyerte.

Bérczes Attilával közösen írt dolgozatban az

$$x^2 + p^{2k} = y^n \tag{2}$$

egyenlettel foglalkozott, ahol $p < 100$ egy adott prím és bizonyos természetes feltételek mellett megadjuk a (2) egyenlet összes x, y, n, k megoldását.

Pintér Ákos

Pintér Ákos a diofantikus egyenletek két osztályával foglalkozott, és nyert a megoldásokra effektív és ineffektív végességi állításokat.

Győry Kálmánnal közösen folytatta az egymás után következő egész számok szorzataiban előforduló "'majdnem" teljes hatványok vizsgálatát. Bennettel, Győryvel és Mignotte-tal közösen tanulmányozta az

$$Ax^n - By^n = \pm 1$$

alakú, ismeretlen fokszámú, binomiális Thue-egyenleteket, ahol $n \geq 3$, x, y ismeretlen egészek, továbbá az együtthatók AB szorzatának is csak a prímfaktorai rögzítettek. A Compositio-ban megjelent cikkben a szerzők teljesen megoldották a fenti egyenletcsaládot, amikor AB-nek legfeljebb két különböző prímfaktora van, és azok egyike sem nagyobb 13-nál. A tétel bizonyításában a diofantikus számelmélet szinte valamennyi mély módszerét

kombinálták, így Baker algebrai számok logaritmusainak lineáris formáira vonatkozó effektív becsléseit, Wiles, Kraus, Bennett, Skinner és mások által kidolgozott, illetve a szerzők által továbbfejlesztett moduláris módszert, klasszikus, a körosztási testek segítségével nyert eredményeket és számítógépes eljárásokat. Később, Győry Kálmánnal közösen kiterjesztette ezt az eredményt arra az esetre, amikor a prímfaktorok 29-nél nem nagyobbak. A szerzők numerikus eredményeiket egy külön cikkben foglalták össze.

Pintér folytatta az $S_k(x) = 1^k+2^k+\ldots+(x-1)^k$ összeg hatványértékeinek vizsgálatát. A Baker módszer és a moduláris technika ötvözésével bebizonyította, hogy az $S_k(x) = y^n$ egyenletnek ($k \leq 169$, k páratlan, $n > 4$, n páros) csak triviális $(x, y) = (2, 1)$ megoldása van.

A másik kutatási irány az $f(x) = g(y)$ alakú, szeparábilis diofantikus egyenletek vizsgálata volt. Bilu és Tichy adott egy kritériumot annak eldöntésére, hogy az ilyen típusú diofantoszi egyenleteknek mikor van végtelen sok egész x, y megoldása, azonban konkrét esetekben ezt a tételt nehéz alkalmazni. Pintér ineffektív végességi állítást adott egy, a diszkrét geometriában fellépő diofantikus egyenlet megoldásaira.

Péter Gyöngyvérrel és Andrzej Schinzellel közösen, ugyancsak a Bilu-Tichy tételt alkalmazva, végességi tételt bizonyított trinomok közös értékeire.

Rakaczki Csaba

Cikkeiben Rakaczki számos új ineffektív, effektív és numerikus eredményt bizonyít binomiális együtthatókkal, illetve hatványösszegekkel kapcsolatosan.

Általános ineffektív állítást igazol az

$$F\left(\binom{x}{m}\right) = b\binom{y}{n}$$

alakú egyenletek $x \geq m$, $y \geq n$ egész megoldásaira vonatkozóan, ahol m, n adott pozitív egész számok, $F(x)$ pedig egy lineáris vagy prímfokszámú egész együtthatós polinom. Disszertációjában meghatározza mindazon m, n pozitív egészeket és $\lambda \neq 0$, l racionális paramétereket, amelyek mellett az

$$F(x, y) = x(x-1)\cdots(x-m+1) - \lambda y(y-1)\cdots(y-n+1) - l = 0$$

egyenlet csak véges sok x, y egész, illetve racionális megoldással rendelkezik.

Sikerült teljesen leírnia mindazon $(m, g(y))$ párokat, amelyek mellett az

$$S_m(x) = 1^m + 2^m + \ldots + x^m = g(y)$$

egyenletnek végtelen sok megoldása lehet, ahol m pozitív egész, $g(y) \in \mathbb{Q}[y]$ pedig egy legalább harmadfokú polinom.

Effektív felső korlátot nyert mindazon $x \geq m$, $y \geq n$ egészekre, amelyekre az

$$f(x) + g(x), \binom{x}{m}, \binom{y}{n}$$

számok valamilyen sorrendben számtani sorozatot alkotnak, ahol $f(x) \in \mathbb{Q}[x]$ egész értékű, legfeljebb $m-1$-ed fokú polinom, $g(x) \in \mathbb{Z}[x]$ tetszőleges polinom.

Végül meghatározta a

$$2\binom{x}{m} = \binom{y}{n} + k$$

egyenlet összes megoldását abban az esetben, amikor

$$(m, n) \in \{(2, 3), (2, 6), (3, 4), (4, 6)\}$$

és $0 \leq k \leq 10$.

Pintérrel közösen megmutatták, hogy ha egy $n \geq 5$ páratlan fokszámú $B_n(x)$ Bernoulli polinomot eltolva egy tetszőleges komplex b számmal, akkor az így kapott $B_n(x)+b$ polinom mindíg rendelkezik legalább három egyszeres gyökkel. $n \geq 8$ páros fokszám esetén azt sikerült igazolniuk, hogy legfeljebb egy olyan b komplex szám létezhet, amelyre az eltolt $B_n(x) + b$ Bernoulli polinomnak nincs három páratlan multplicitású gyöke.

Az előző, Bernoulli polinomokra nyert állítások egy analóg verzióját igazolta Euler polinomokra vonatkozóan. Ezen eredmények alkalmazásaként effektív végességi tételt bizonyított Euler polinomokat tartalmazó, algebrai egész együtthatós hiperelliptikus egyenletekre vonatkozóan.

Sikerült belátnia ortogonális polinomok egy családjáról, a $H_n(x)$ Hermite polinomokról, hogy $n \geq 7$ fokszám esetén a polinomcsalád $H_n(x) + b$ eltoltjainak van legalább három egyszeres gyöke bármely $b \in \mathbb{C}$ komplex szám esetén.

Részben a beszámolási időszak alatt elért eredményeket felhasználva, Rakaczki Csaba (2005), Pink István (2006) és Nyul Gábor (2007) elkészítette és megvédte PhD disszertációját, továbbá Bérczes Attila illetve Pintér Ákos 2009 februárjában beadta habilitációs illetve MTA doktori értekezését.