# Az OTKA K75566 számú pályázatának zárójelentése

A kutatócsoport tagjai elsősorban számelméleti, azon belül diofantikus egyenletekkel kapcsolatos vizsgálatokat folytattak. Több fontos egyenletosztály megoldására nyertek effektív, ineffektív és numerikus eredményeket, korábbi módszereket nem-triviális módon továbbfejlesztve és általánosítva. A kutatócsoport több tagja végzett alkalmazott számelméleti (diszkrét tomográfia és kriptográfia)i kutatásokat. Több eredmény született különböző klasszikus polinomok és polinomcsaládok gyökstruktúrájával és összetételével kapcsolatban.

A pályázat ideje alatt, a pályázat támogatásával elért eredmények alapján 3 PhD (Bazsó, Huszti, Kovács) , 1 habilitáció (Bérczes) és 2 MTA Doktora (Hajdu, Pintér) fokozat született.

## Bazsó András eredményei

Bazsó általánosította és kiterjesztette Győry és Pintér binom Thue-egyenletekre vonatkozó eredményeit.Különböző szignatúrájú, Fermat-típusú ternér egyenletek ismeretlen kitevőjére adott éles felső korlátokat abban az általános esetben, amikor az egyenlet együtthatói ismeretlen S-egységek, jelentősen általánosítva ezzel Bennett, Győry, Mignotte és Pintér, valamint Győry és Pintér ilyen irányú eredményeit. Eredményei alkalmazásaként hasonló eredményt bizonyított S-egyég együtthatójú, ismeretlen fokszámú binom Thue-egyenletekre, amivel az ismert korábbi eredményeket kiterjesztette.

2010-ben Bazsó András benyújtotta és megvédte doktori értekezését, így PhD fokozatot szerzett.

Faulhaber klasszikus tételéből következik, hogy egy b, a+b, 2a+b, …, a(n-1)+b számtani sorozat páratlan hatványösszegei felírhatók (n-1)b + n(n-1)a/2 polinomjaként. Társszerzőkkel megmutatta, hogy az $S^k_{a,b}(n) = b^k + (a+b)^k + (2a+b)^k + \ldots + (a(n-1)+b)^k$ (ahol n>1 pozitív egész) hatványösszeg Bernoulli polinomokon keresztül kiterjeszthető tetszőleges valós x értékre. Továbbá meghatározta az $\boldsymbol{S}^k_{a,b}(x) = b^k + (a+b)^k + (2a+b)^k + \ldots + (a(x-1)+b)^k$ polinom összes lehetséges felbontását.

Legyenek a,b,c,d,k,l olyan adott egész számok, melyre a és b ill. c és d relatív prímek, és $k \neq l$. Társszerzőkkel megmutatta, hogy a $b^k + (a+b)^k + (2a+b)^k + \ldots + (a(x-1)+b)^k = d^l + (c+d)^l + (2c+d)^l + \ldots + (c(y-1)+d)^l$ diofantikus egyenletnek bizonyos feltételek mellett csak véges sok x, y egész megoldása lehet. Ineffektív végességi tételt bizonyított a $2 \leq k < l$ esetre. A k=1, l≠1,3,5; illetve a k=3, l≠1,3,5 esetekben megmutatta, hogy effektív felső korlát adható a megoldások abszolút értékére.

Vizsgálta a $T^k_{a,b}(n) = b^k - (a+b)^k + (2a+b)^k - \ldots + (-1)^{n-1} (a(n-1)+b)^k$ (n>1 pozitív egész) alternáló hatványösszeg polinom-kiterjesztéseit felbonthatóság szempontjából. Az $E_k(x)$ Euler polinomok felhasználásával a $T^k_{a,b}(n)$ hatványösszeg az n paritásától függően kiterjeszthető a $\boldsymbol{T}^{k+}_{a,b}(x) = a^k (E_k(b/a) + E_k(x+b/a))/2$ ill. $\boldsymbol{T}^{k-}_{a,b}(x) = a^k (E_k(b/a) - E_k(x+b/a))/2$ polinomokká. A cikkben meghatározta ekvivalencia erejéig a fenti polinomok összes lehetséges felbontását. Ezzel Faulhaber tételének egy analógját adta alternáló hatványösszegekre.

# Bérczes Attila eredményei

Bérczes Attila társszerzőkkel effektív végességi vizsgálatokat végzett tóruszok bizonyos részvarietásainak pontjaival kapcsolatban. A tekintett részvarietások olyanok, hogy lehetővé teszik a Baker-módszer alkalmazását. Először kétdimenziós esetben lineáris polinom által meghatározott részvarietásokat tekintett. Így lényegében az $a_1 x_1 + a_2 x_2 = 1$ alakú kétismeretlenes egységegyenletekre vonatkozó korábbi eredményeket élesítette és általánosította, ahol $a_1$, $a_2$ adott algebrai számok. Előbb a fenti egyenlet olyan $(x_1, x_2)$ megoldásainak magasságára nyert effektív felső korlátot, melyek egy végesen generált csoportból valók, majd társszerzőkkel nyert eredményeit általánosította azon megoldások esetére, melyek a fenti csoport divíziócsoportjából, a divíziócsoport körüli „hengerből", illetve a divíziócsoport körüli „csonkakúpból" valók. Az általánosítások esetén a teljesen effektív eredmény eléréséhez szükség volt korlátozni a megoldások fokszámát is, mivel ezek a megoldások nem feltétlenül elemei egy előre megadott számtestnek. A fokszámokra nyert korlátok igazolásához a varietásokban található kis magasságú pontok számára adott becslések szükségesek. További vizsgálataiban tetszőleges dimenziós tóruszok olyan X részvarietásait tekintette, melyek binomok és trinomok segítségével definiálhatók. Előbb az X részvarietás és egy végesen generált csoport metszetéhez tartozó pontokra nyert effektív végességi eredményt, majd ezt általánosította arra esetre is, amikor a fenti csoport helyett annak divíziócsoportja, a divíziócsoport körüli „henger", illetve a divíziócsoport körüli „csonkakúp" szerepel. Szintén effektív eredményeket bizonyított a fenti halmazokra abban az esetben amikor X egy síkbeli görbe.

Foglalkozott index formák kriptográfiai alkalmazásának lehetőségével. Ez a munka egy korábbi, Pethő Attilával és Ködmön Józseffel közös, norma formákkal kapcsolatos kriptográfiai vizsgálat egyenes folytatása. Most javaslatot tett egy index formára alapozott hash függvény használatára, melyről belátják, hogy ütközésmentes. Az általuk javasolt hash függvény lavina hatását számítógépes kísérletekkel vizsgáltuk. A szerzők folytatják a kutatócsoport korábbi hash függvényekkel kapcsolatos vizsgálatait. Korábbi dolgozataikban olyan hash függvényeket dolgoztak ki, melyek norma illetve index formákra voltak alapozva. Mint kiderült, az, hogy ezek a formák homogének, több technikai problémát is okozott. Ezért jelen dolgozatukban, az ilyen típusú problémákat megelőzendő, 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. Jelen algoritmus a korábbi javasolt algoritmusoknál sokkal gyorsabb, ugyanis ebben az esetben a biztonságot nem veszélyezteti az, ha egy véges prímtest felett dolgozunk.

Bérczes Attila választ ad Ruzsa Imre egy problémájára is. Egy 2004-ben Debrecenben tartott előadásán Ruzsa Imre azt kérdezte, hogy mennyi lehet az elemszáma egy véges, 1-nél nagyobb pozitív kvóciensű mértani sorozatot tartalmazó halmaz összeghalmazának. A kérdés nyilvánvalóan három-, illetve négytagú polinomok közös gyökeinek vizsgálatára vezethető vissza. Bérczes Attila belátja, hogy két $X^n-X^m-X^k+1$ alakú polinomnak, illetve egy $X^n-X^m-X^k+1$ alakú és egy $X^n-2X^m+1$ alakú polinomnak, néhány expliciten megadott esettől eltekintve, nincs olyan közös gyöke, mely nem egységgyök. Megjegyzendő, hogy az összeghalmaz szempontjából pont azok a legérdekesebb esetek, amikor van ilyen közös gyök.

Bérczes Attila társszerzőkkel belátja, hogy egy triviális esettől eltekintve nincs olyan egészekből álló $R_n$ másodrendű rekurzív sorozat, mely definiáló polinomjának diszkriminánsa pozitív, és amely valamilyen $n>1$, $k>0$ egész esetén teljesíti az

$$R_1+R_2+\ldots+R_{n-1} = R_{n+1} +R_{n+2}+\ldots+ R_{n+k}$$

egyenletet.

A diofantikus egyenletek elméletének egyik intenzíven fejlődő ága az explicit módszerek alkalmazása egyenletek teljes megoldására. Pink Istvánnal közösen teljesen megoldják az

$$x^2+d^{2l+1}=y^n$$

egyenletet abban az esetben mikor a Q(\sqrt{-d}) test ideálosztályszáma 2 vagy 3 és d 8-cal való osztási maradéka nem 7.

Foglalkozott a Pell egyenletek megoldáshalmazában található mértani sorozatokkal, számos effektív és kvantitatív eredményt nyerve, továbbá teljesen leírja a Lucas sorozatokban található mértani sorozatokat.

Bebizonyította, hogy adott algebrai számtestben legfeljebb véges sok olyan monogén rend van, mely három egymással nem ekvivalens algebrai egésszel is generálható a racionális egészek felett. Eredményüket ennél lényegesen általánosabban, Z felett végesen generált tartományok feletti rendek esetén is bizonyítják.

## Gaál István eredményei

Gaál István foglalkozik globális függvénytestek feletti diofantikus egyenletekkel. Társszerzőkkel eljárást ad globális függvénytestek feletti többváltozós egységegyenletek megoldására. Ezt a módszert alkalmazza normaforma egyenletek megoldásainak kiszámítására. Globális függvénytestek felett algoritmust ad rezultáns típusú egyenletek megoldására, ahol az egyik polinom adott, a másik ismeretlen, továbbá algoritmust ad adott normájú elemek megkeresésére. Az eredmény az egységegyenletek megoldásán alapul. Globális függvénytestek felett eljárást ad homogén binér formák közös értékeinek megkeresésére, valamint megoldja az

$$x_1+x_2=y^k$$

típusú egyenletet, ahol x_1 és x_2 ismeretlen S-egységek, y S-egész és a k kitevő is ismeretlen.

Gaál István vizsgálta továbbá harmadfokú gyökbővítésekben a hatvány egész bázis létezését és a minimális indexek viselkedését és negyedfokú számtestek két paramétertől függő végtelen családjaiban határozza meg a hatvány egész bázisokat.

## Győry Kálmán eredményei

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.

**Általános effektív végességi tételek** (részben Bérczes Attilával közös eredmények). 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. A Thue egyenletek, szuperelliptikus egyenletek és egységegyenletek centrális szerepet játszanak a diofantikus számelméletben. A számtest esetben Thue, illetve Siegel, majd általánosabban Mahler, Parry, LeVeque és Lang bizonyították a nevezett egyenletek megoldásszámának a végességét. Ezek az eredmények azonban ineffektivek voltak. Számtest esetben ezekre később Baker, Győry, Schinzel és Tijdeman adtak effektív bizonyítást. Újabban Győry egységegyenletek esetén Evertsevel, Thue és szuperelliptikus egyenletekre Bérczessel és Evertsevel közösen a lehető legáltalánosabb formában, Z felett végesen generált tartományok felett nyert effektiv végességi tételeket. Kvantitatív formában nyert eredményei új fejezetet nyitottak a számelméletben és számos alkalmazáshoz vezettek.

**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 $k \geq 2$ egymásra következő egész szorzata nem lehet teljes hatvány. Egy általános sejtés szerint – mely $k = 3$ esetén egészen Fermat-ig nyúlik vissza- az általánosabb (2) $x(x+d) \ldots (x+(k-1)d) = y^n$ 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 (2)-at visszavezették (3) $Ax^n + By^n = Cz^q$, $q \in \{2, n\}$ 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 (3) 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) $Ax^n-By^n=C$ 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 (3) 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 binér formák** (Bérczes Attilával közös eredmények). Az adott diszkriminánsú 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. Az említett eredményekhez szorosan kapcsolódva megmutatták, hogy adott algebrai számtestben legfeljebb véges sok olyan monogén rend van, mely három egymással nem ekvivalens algebrai egésszel külön-külön is generálható a racionális egészek gyürűje felett. Eredményüket ennél lényegesen általánosabban, Z felett végesen generált tartományok feletti rendek esetén is bizonyítják.

## Hajdu Lajos eredményei

Benyújtotta és megvédte akadémiai doktori értekezését. Disszertációjában különböző multiplikatív tulajdonságú halmazokban található számtani sorozatokra vonatkozó eredményeit összegezte.

***Diofantikus problémák.*** 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. Tengellyel közösen éles korlátot nyert az n-edik hatványokból valamint négyzetekből, illetve köbökből álló számtani sorozatok hosszára. Korábban sikerült csak természetes paraméterektől függő felső korlátot adnia S-egységek összegeiből álló halmazokban található számtani sorozatok hosszára. 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 és kiterjesztették, választ adva Nathanson egy kapcsolódó kérdésére. Dombekkel és Pethővel több eredményt bizonyított algebrai számtestek egészei gyűrűinek egységek lineáris kombinációjával történő reprezentációjával kapcsolatban. Zieglerrel véges sok, explicit módon megadott kivételtől eltekintve meghatározták az összes olyan totálisan komplex negyedfokú algebrai számtestet, melyekben minden algebrai egész előállítható különböző egységek összegeként. 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-egység egyenletek esetében hasonló irányba tett lépéseket: olyan S-alapegység rendszer létezését igazolta konstruktív módon, amely az LLL-módszer alkalmazásakor a legnagyobb hatékonyságot teszi lehetővé. Kováccsal, Pethővel és Pohsttal általánosították a duális rács fogalmát a nemteljes rácsok esetére. Hatékony algoritmusokat adtak egy kapcsolódó rácselméleti problémára is.

***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.

***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. Szikszaival több eredményt is igazolt Pillai fenti k egymást követő egész szám legnagyobb közös osztóira vonatkozó kérdésének Lucas- és általánosabb rekurzív sorozatokra való kiterjesztésével kapcsolatban. Többek között megmutatták, hogy bármely k>24 esetén található k darab egymást követő Fibonacci szám melyek egyike sem relatív prím a többiek mindegyikéhez. Hasonló eredményeket nyertek úgynevezett elliptikus oszthatósági sorozatok egymást követő tagjaira vonatkozóan is. 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. Kovács Lászlóval, Tomán Henriettával, Jónás Ágnessel és Hajdu Andrással különböző algebrai és egyéb eszközök felhasználásával igazolták egy újszerű kombinált rendszer hatékonyságát bizonyos típusú, orvosi jellegű képfeldolgozási problémák kezelésére.

## Huszti Andrea eredményei

Az elektronikus választási sémák az alkalmazott kriptográfiai technikák alapján három fő kategóriába sorolhatók: mix-net modell, vak aláíráson alapuló modell és a homomorf titkosításon alapuló sémák. Az irodalomban több olyan választási protokoll is ismert, mely rendelkezik az alapvető elvárásokkal (ellenőrizhetőség, jogosultság, egyszer-szavazhatóság, titkosság stb.) de nem visszaigazolás-mentes, a legtöbb visszaigazolás-mentes séma lehallgathatatlan csatornát vagy szavazó fülke csatornát használ, ami nem gyakorlatias. Huszti Andrea kidolgoz egy olyan visszaigazolás-mentes homomorf választási sémát, mely nem a

szavazó fülke vagy lehallgathatatlan csatornát, hanem a gyakorlatias, anonim válasz csatornát alkalmazza. Nem tételezzük fel egyik szervezetről sem, hogy teljesen megbízható, az egyetlen feltételezés az, hogy a Szavazó Bizottságok között az osztott kulcsgenerálás és dekódolás során legalább egy megbízható.
Az elektronikus szavazó és az elektronikus vizsgáztatási rendszerek kriptográfiai protokollja a sok közös elvárás miatt szoros kapcsolatban állnak. Huszti Andrea több dolgozatában olyan e-vizsgáztatási rendszereket mutat be, melyek garantálják valamennyi alapvető biztonsági elvárást, melyekkel a hagyományos papír alapú rendszerek rendelkeznek, illetve biztosítják mind a vizsgázó, mind a javító anonimitását. Például az egyik nem tételezi fel teljesen megbízható fél részvételét, egy másik pedig *experiment-based* definíciókat is ad az alapvető biztonsági jellemzőkre és igazolja, hogy a javasolt rendszer rendelkezik ezekkel az elvárásokkal.
Huszti Andrea megad egy olyan általános kriptográfiai protokollt, mely megfelel valamennyi közös biztonsági kritériumnak, és alkalmas elektronikus vizsgáztatásra, közvélemény-kutatásra, aukcióra, pályáztatásra és szavazásra is. Az előbb felsorolt rendszerek fontos közös kritériumai az anonimitás, jogosultság, adatintegritás, titkosság, ellenőrizhetőség. Speciálisan a vizsgáztatás, a pályáztatás és az aukció esetén szükség van olyan anonimitásra, amely ─ kizárólag a kiértékelés után ─ visszaállítható, azaz a résztvevő személyazonossága visszanyerhető. A javasolt rendszer a fenti elvárásokat több kriptográfiai eszközzel valósítja meg. Az anonimitást vak aláírás és egy anonim szerver garantálja, mely a szükséges esetekben lehetőséget biztosít a visszaállíthatóságra. A bizalmas adatokat továbbításához a digitális boríték technikát alkalmazzuk. Az ellenőrizhetőséget digitális hirdetőtábla segítségével valósítjuk meg.

Formális módszerrel vizsgálta a PayWord mikrofizetési rendszert, melyet Ronald L. Rivest és Adi Shamir fejlesztett ki 1997-ben. Megadta (társszerzőkkel) a rendszer formális leírását Spi kalkulusban, melyet tipikusan kriptográfiai protokollok formalizálására fejlesztettek ki. Egy fizetési rendszer használatánál reklamációk, vitás helyzetek merülhetnek fel, melyek költségét a bolt állja. Mikrofizetési rendszerek esetén a Payment Technologies for E-commerce című könyv szerint $150 is meghaladhatja, miközben a vásárlás során a felhasználó mindössze néhány dollárt fizetett. Egyik munkájában a PayWord mikrofizetési rendszer olyan kiterjesztését adta meg, mely kriptográfiai eszközökkel növeli a rendszer biztonságát, azaz minimalizálja a vitás helyzetek, kockázatok, visszaélések számát. Mindezt vásárlásonként egy MAC alkalmazásával érték el, mely nem növelte a rendszer időbonyolultságát jelentősen. A kiterjesztett protokollt formálisan is elemezte api kalkulusban.

## Kovács Tünde eredményei

2011-ben benyújtotta Combinatorial Diophantine equations címmel doktori értekezését. 2011. november 25-én volt a doktori védése, melyet követően 2012. január 23-i dátummal PhD fokozatot szerzett.

A fenti időszakban több, különböző témában folytatott tudományos kutatómunkát. Másodrendű lineáris rekurzív sorozatokban található kombinatorikus számokkal kapcsolatban mind effektív végességi, mind explicit tételeket sikerült bizonyítania.

Általánosított, ún. (a,b)-balansz számokkal kapcsolatban Liptai Kálmánnal és Olajos Péterrel közösen folytatott vizsgálatokat. Több effektív végességi és explicit eredményt sikerült nyerniük. A bizonyításoknál a Baker-módszert, Bennett egy fontos eredményét, a Chabauty-módszert és az elliptikus görbék elméletét is alkalmazták.

Péter Gyöngyvérrel és Varga Nórával közösen folytatott vizsgálatokat azonos jegyekből álló számok (repdigit numbers) polinomértékeivel kapcsolatban. Több effektív végességi és explicit eredményt sikerült belátnunk. A bizonyításoknál Schinzel és Tijdeman egy fontos eredményét, az elliptikus görbék elméletét alkalmaztuk, számolásainkhoz pedig a Magma programcsomagot, annak eljárásait illetve Kovács egy Magmában implementált programját használtuk.

## Mező István eredményei

Mező István különböző kombinatorikus hátterű számsorozatokkal, azok kiterjesztéseivel és generátorfüggvényeivel foglalkozott. Új karakterizációját adta a Fibonacci sorozatnak. Vizsgálta a hiperharmonikus sorok és a Hurwitz zeta függvény kapcsolatát, valamint általánosította a diszkrét matematikában nagy szerepet játszó másodfajú Stirling szám fogalmát. Új formulát adott a Bernoulli polinomokra, általánosította a Bell számok fogalmát és vizsgálta ezen általánosítás tulajdonságait.

Más irányú vizsgálatai a Vilenkin csoportokhoz és a Jacobi theta függvényekhez kötődnek.

## Nyul Gábor eredményei

B. M. Landman nem rögzített együtthatós másodrendű lineáris rekurziót kielégítő három sorozatcsalád esetén adott felső korlátot a van der Waerden-típusú számokra, ha a színek száma kettő. A. Robertsonnal közös könyvükben vetették fel hasonló sorozatcsaládok esetén ugyanennek a kérdésnek a vizsgálatát. Rauf Bettinával közös cikkben megadták az összes lehetséges hasonló sorozatcsaládot, és mindegyik esetén a megfelelő felső korlátokat. Egy másik közös cikkben konstans együtthatós, tetszőleges rendű lineáris rekurziót teljesítő sorozatcsaládok esetén bizonyítottak a van der Waerden-típusú számok létezésére és nem létezésére vonatkozó tételeket.

Másodfajú Stirling-számok és Bell-számok gráfokra vonatkozó általánosítását B. Duncan és R. Peele definiálták. Kereskényiné Balogh Zsófiával közös cikkben ezeknek a számoknak a tulajdonságait vizsgálták. Ezek segítségével egyúttal a másodfajú r-Stirling-számok és az r-Bell-számok újfajta megközelítését kapták. Hasonló, gráfokra vonatkozó változat vizsgálata más kombinatorikus számok esetén is folyamatban van.

Gyimesi Eszterrel együtt azt az észrevételt fogalmazták meg és bizonyították, hogy a pozitív racionális számok különböző egységtörtek összegeként való előállítására szolgáló Golomb-módszer és a lánctört módszer mindig ugyanazt az eredményt adja.

Kvaterniók szorzása leírható háromdimenziós vektorok skaláris és vektoriális szorzata segítségével. Ezen megállapítás által motivált függvényegyenleteket oldottak meg Nyul Balázzsal közösen.

## Pink István eredményei (részben ismertetve Bérczes Attila eredményeinél)

Pink István Rábai Zsolttal közös cikkben megadja az $x^2+5^k17^l=y^n$ diofantikus egyenlet összes olyan (x,y,k,l,n) egész megoldását, amelyre x>=1, y>=1, n>=3, k>=0, l>= 0 és lnko(x,y)=1. A bizonyítás során n>=5 esetén felhasználják Bilu, Hanrot és Voutier, egy Lucas-sorozatok primitív prímosztóira vonatkozó mély eredményét és megmutatják, hogy ebben az esetben a fenti egyenletnek nincs megoldása. Az n=3,4 esetben Cohn és Holzer tételeit kombinálva a problémát visszavezetik bizonyos elliptikus görbék S-egész pontjainak a megkeresésére, ahol S={5,17}. A felmerülő egyenletek S-egész pontait ezután a MAGMA programcsomagban implementált eljárással oldják meg.
Tekintsük az $|ax^n -by^n n|=c$ binom Thue egyenletet, ahol az ismeretlenek olyan (a,b,x,y,n) egészek, amelyekre 1<= a < b, x>=1, y>= 1. Bennett megmutatta, hogy c=1 esetén a fenti egyenletnek minden a,b, n>=3 esetén legfeljebb egy (x,y) megoldása van. Ebben a cikkben a szerzők kiterjesztik Bennett fenti eredményét az $|ax^n-by^n|<=3$ esetre vonatkozóan és megmutatják, hogy az (a,b,n)=(1,3,n), (2,5,n) esetektől eltekintve a fenti egyenlőtlenségnek minden a,b, n>=3 esetén legfeljebb egy (x,y) megoldása van. A bizonyítás során a hipergeometrikus módszert kombinálják a kétváltozós Baker-módszerrel.

## Pintér Ákos eredményei (részben ismertetve Bazsó András, Bérczes Attila, Győry Kálmán és Hajdu Lajos eredményeinél)

Alf van der Poortennel közösen alsó becslést adott rekurzív sorozattal definiált polinomok egyszeres gyökeinek a számára, felhasználva Mason függvénytestek feletti abc-tételét. Török társszerzőkkel és Florian Lucával közösen, természetes feltételek mellett, megoldotta az

$$x^2 +2^a11^b=y^n$$

egyenletet, ahol x,a,by,n ismeretlenek. Varga Nórával közösen redukciós módszerek nélkül oldott meg egy olyan diofantikus egyenletet, ahol a megoldásokra kapott korlát igen nagy. Módszerük a Pell egyenletek megoldásainak hézagosságán alapszik. Egy másik PhD hallgatójával és Andrzej Schinzellel közösen tanulmányozta a trinomok lehetséges közös értékeit. Ugyancsak tanítványaival közösen vizsgálta egy a binomiális együtthatók lehetséges közös értékeivel analóg problémát, másodfajú Stirling számokra vonatkozóan. Volker Zieglerrel közösen új karakterizációját adta a Fibonacci sorozatnak, nevezetesen megmutatták, hogy lényegében a Fibonacci sorozat az egyetlen olyan másodrendű rekurzív sorozat, amely végtelen sok háromtagú számtani sorozatot tartalmaz. Srivastavával közösen, egy korábbi cikkükhöz kapcsolódóan, addíciós formulákat nyert Appell polinomokra. Dujellával és Győry Kálmánnal közösen vizsgálta a piramidális számok hatványértékeit. A Biluval, Fuchsszal és Lucával közös, 2013 elején megjelent cikkükben tanulmányozták különböző kombinatorikus számok lehetséges egyenlő értékeit, továbbá egy finomítását bizonyították a szeparábilis f(x)=g(y) típusú diofantikus egyenletek megoldásaira vonatkozó Bilu-Tichy tételnek. Koreai társszerzőkkel közösen megfogalmazott és megoldott poligonális

számokkal kapcsolatos diofantikus problémákat, kiterjesztve néhány korábbi klasszikus eredményt. Tengely Szabolccsal közösen a Korteweg-de Vries parciális differenciálegyenlet soliton megoldásaihoz kapcsolódó diofantikus problémákat vizsgált.

## Rakaczki Csaba eredményei

Rakaczki Csaba klasszkis polinomcsaládok (Hermite, Euler és Bernoulli polinomok) gyökstruktúrájával kapcsolatban ért el eredményeket és alkalmazta ezeket a fenti polinomokkal kapcsolatos diofantikus problémákra. Kiemelendő az Acta Arithmeticában megjelent, a Schaffer egyenlet általánosításával foglalkozó eredménye.