Pethő Attilának az OTKA pályázatban megjelent és közlésre leadott dolgozatai az alábbi területekre koncentrálnak:

1. Parametrikus Thue egyenletek és Diofantikus egyenletek numerikus megoldása. Az első eredmény korábbi kutatásainak folytatása. [22]-ben megmutattuk, hogy ha t egy imaginárius másodfokú egész szám és ha $|t|$ vagy $\mathbb{Q}(t)$ diszkriminánsa elég nagy vagy $t = -1/2$, akkor az

$$x^3 - (t-1)x^2y - (t+2)xy^2 - y^3 = \mu$$

egyenlet, ahol μ egységgyök, minden $(x, y) \in \mathbb{Z}_{\mathbb{Q}(t)}$ megoldására $|x|, |y| \leq 1$ teljesül. Ez E. Thomas és M. Mignotte racionális egészekre vonatkozó eredményeinek az általánosítása.

A [13] és [14] cikkekben bebizonyítottuk, hogy egy normaforma egyenletnek általában csak véges sok olyan megoldása van, ahol a megoldások koordinátái egy számtani sorozatot alkotnak. Az eredmény azért érdekes, mert az általunk vizsgált normaforma egyenleteknek általában végtelen sok megoldása van. Példákat adtunk olyan tetszőlegesen nagy fokszámú normaforma egyenletekre is, amelyek megoldásai koordinátái számtani sorozatot alkotnak. [13]-ban az $\alpha^n = a$ tulajdonságú elemekkel definiált egyenletet oldottuk meg $0 < a \leq 100$ mellett, [14]-ben pedig a legegyszerűbb harmadfokú testek feletti normaforma egyenletet oldottuk meg ugyanezen feltétel mellett.

J.H.E. Cohn 2002-ben közölt egy dolgozatot az Acta Arithmeticaban, amelyben az $x^n = Dy^2 + 1$ diofantikus egyenlet megoldásait vizsgálta, ahol az ismeretlenek x, y és n. Azt - többek között - $0 < D \leq 100$-ra megoldotta, de hat eset nyitva maradt. Herrmannal és Járásival [21]-ben az elliptikus és a Thue egyenletekre korábban kidolgozott numerikus módszerek felhasználásával teljessé tettük Cohn eredményét.

S. Schmitt és H.G. Zimmer könyve [28] elliptikus görbékre vonatkozó algoritmusokról szól. Ehhez írtam egy 20 oldalas appendixet az A. Baker módszerén alapuló numerikus módszerekről diofantikus egyenletek megoldására.

2. Egyirányú függvények konstrukciója. A normaforma egyenleteket az elmúlt évtizedekben nagyon sokan (pl. W.M. Schmidt, H.P. Schlickewei, Győry Kálman, J.-H. Evertse, stb) és sokféle szempontból foglalkoztak. [12]-ben Bérczes és Ködmön egy korábbi dolgozatában foglaltakat tovább gondolva a $Norm_P(\mathbf{x}) \bmod s$ függvényt vizsgáltuk, ahol P $n \leq m$-ed fokú főpolinom, $Norm_P$ a P-hez tartozó m változós forma és s egy egész szám. Megmutattuk, hogy ha s két prímszám szorzata, akkor ez a függvény ütközésmentes és numerikus vizsgálatok valószínűsítik, hogy lavinahatással is rendelkezik.

3. Rekurzív sorozatok tulajdonságai. Itt két területen értem el eredményeket.

a. Legyen K egy algebrailag zárt test és $\{G_n\}_{n=0}^{\infty}$ a $K[x]$ egy d-ed rendű lineáris rekurzív sorozata. Legyen továbbá $P(x) \in K[x]$. [17]-ben a G_n kezdőértékeitől, az azt definiáló differenciaegyenlet együtthatóitól és P-től függő általános feltételek mellett sikerült megmutatni, hogy $d = 2$ mellett a

$$G_n(x) = G_m(P(x)) \tag{1}$$

egyenletnek csak véges sok $n \neq m$ megoldása lehet. Ezt az eredményt általánosítottuk [18]-ban tetszőleges $d \geq 2$-re. Mindkét esetben sikerült csak d-től függő felső korlátot bizonyítani (1) megoldásainak a számára. Eredményeinket általánosítottuk a

$$G_n(x) = cG_m(P(x))$$

egyenletre is, ahol $c \in K$ is ismeretlen. A [25] dolgozatban a [18] legfontosabb tételeit ismertettük.

Kutatásainkat folytatva [19]-ben általános feltételek mellett megmutattuk, hogy a $G_n(x) = G_m(y)$ egyenletnek csak véges sok n, m egész megoldása lehet feltéve, hogy x és y algebrailag függőek, amelyet a $Q(x, y) = 0$ egyenlet ír le. Felső becslést adtunk a megoldások számára is. Korábban azt az egyszerűbb esetet vizsgáltuk, amikor $Q(x, y) = y - P(x)$, ahol $P(x)$ egy polinom. [16]-ban megmutattuk, hogy ebben a speciális esetben nemcsak a megoldások számára lehet felső becslést adni, hanem effektív korlát adható $\max\{|n|, |m|\}$-re is.

b. Legyen a $G_n = G_n(a, b, \delta)$, $n \geq 0$ sorozat a $G_0 = 0$, $G_1 = 1$, $G_2 = a$, $G_3 = a^2 - b - \delta$ kezdőértékkel és a

$$G_{n+4} = aG_{n+3} - bG_{n+2} + \delta aG_{n+1} - G_n, \quad n \geq 0$$

rekurzióval definiálva. [26]-ban megmutattuk, hogy ez egy oszthatósági sorozat, azaz ha $d|n$, akkor $G_d|G_n$. Bebizonyítottuk továbbá, hogy G_n sorozat szoros kapcsolatban áll a $g_0 = 0$, $g_1 = 1$ kezdőértékekkel és

$$g_{n+2} = ag_{n+1} - (b - 2\delta)g_n, \quad n \geq 0$$

rekurzióval definiált másodrendű rekurzív sorozattal.

4. Általánosított számrendszerek. A tárgyalt időszakban itt végeztem a legtöbb kutatást.

a. A $1 \leq q \leq 2$ valós számot "univoque"-nak nevezzük, ha csak egyetlen olyan bináris c_i sorozat létezik, amelyre

$$1 = \frac{c_1}{q} + \frac{c_2}{q^2} + \frac{c_3}{q^3} + \dots$$

Komornik és Loretti 1998-ban bebizonyította, hogy van minimális "univoque" szám, q'. [23]-ban megmutattuk, hogy "univoque" algebrai számoknak van olyan sorozata, amelyik q'-höz tart.

b. K. Mahler bizonyította, hogy ha a tizedesvessző után írjuk a 2-hatványainak tizes számrendszerbeli alakját, akkor egy irracionális számot kapunk. Ezt az eredményt Bundschuh és Niederreiter általánosította kicserélve 2-t és 10-et tetszőleges multiplikatívan független egész számokra. [8]-ban több irányba is tovább általánosítottuk ezt az eredményt. Egyrészt a diadikus törtek helyett algebrai szám alapú β-előállításokat tekintettünk, másrészt a 2-hatványok helyett lineáris rekurzív sorozatok tagjait, végül ezek tizes számrendszer beli előállításai helyett a β-val definiált másik rekurzív sorozatot vettünk. A bizonnyításban fontos szerepet játszott a súlyozott S-egységtétel.

c. [1, 2] és [24] dolgozatokban a helyiértékes számrendszerek bizonyos általánosításainak a tulajdonságaival foglalkoztunk. Azt mondjuk, hogy az 1 főegyütthatós $P(x) \in \mathbb{Z}[x]$ polinom CNS, ha minden $A(x) \in \mathbb{Z}[x]$-hez vannak olyan $a_i \in \{0, \dots, |P(0)|\}$ egészek, hogy

$$A(x) \equiv \sum_{i=0}^{\ell} a_i x \pmod{P(x)}.$$

[1] fő eredménye annak a bizonyítása, hogy ha $|P(0)|$ elég nagy a többi együttható abszolút értékének összegéhez viszonyítva, akkor P CNS.

W.J. Gilbert 1982-ben megfogalmazott egy a harmadfokú CNS polinomokat karakterizáló sejtést. [2]-ben néhány esetben bebzonyítottuk a sejtést, de megmutattuk azt is, hogy az általában nem igaz. Néhány parametrizált harmadfokú számtestben megadtuk az összes CNS alapszámot is. [3] áttekintő dolgozat a CNS polinomokkal kapcsolatban, az utóbbi időben elért eredményekről.

[27] és [15] rokon problémával foglalkozik. Kovács Béla bizonyította 1986-ban, hogy egy számtest egészei gyűrűjében pontosan akkor van kanonikus számrendszer, ha van hatvány egész bázis. [27]-ben és [15]-ben meghatároztuk néhány negyedfokú, parametrikus számtestcsaládra az összes kanonikus számrendszer alapszámait.

A CNS tulajdonság fenti definíciója megengedi reducibilis polinomok vizsgálatát is. Kiderült és erről szól a [24] dolgozat, hogy egész számok szimultán helyiértékes reprezentációja, egész együtthatós polinomokkal való interpoláció és a CNS polinomok között szoros kapcsolat van.

Rényi 1957-ben vezette be a β-előállítások fogalmát. Ezek lényegében nem feltétlenül egész szám alapú számrendszereknek tekinthetőek. A β-előállítások és a kanonikus számrendszerek közös általánosításaként definiáltuk [4]-ben az eltolás alapú rendszereket (shift radix system, SRS). Legyen d egy pozitív egész és $r \in \mathbb{R}^d$. A $\tau_r : \mathbb{Z}^d \mapsto \mathbb{Z}^d$ leképezést, amely az $a = (a_1, \dots, a_d) \in \mathbb{Z}^d$ vektorhoz a

$$\tau_r(a) = (-\lfloor ra \rfloor, a_1, \dots, a_{d-1})$$

vektort rendeli SRS-nek nevezzük, ha minden $a \in \mathbb{Z}^d$ van olyan $k > 0$, hogy $\tau_r(a)^k = 0$. A d-dimenziós SRS-ek halmazát $\mathcal{D}_d^0$-al jelöltük. Bevezettük még a $\mathcal{D}_d$ halmazt is, amelybe azon $r \in \mathbb{R}^d$-ek tartoznak, amelyekre a $\{\tau_r^k(a)\}$ sorozat minden $a \in \mathbb{Z}^d$-re periódikus. [4]-ben megmutattuk, hogy $\mathcal{D}_d$ és $\mathcal{D}_d^0$ is Lebesgue mérhető, algoritmust adtunk annak eldöntésére, hogy adott $r \in \mathbb{R}^d$ benne van-e ezekben a halmazokban és bebizonyítottuk, hogy bármely $K > 0$-hoz van olyan $r \in \mathcal{D}_2^0$ és $a \in \mathbb{Z}^d$, hogy a $\{\tau_r^k(a)\}$ sorozat csak K-nál több lépés után éri el a 0-t.

[5]-ben részletesen tanulmányoztuk $\mathcal{D}_2$-t és $\mathcal{D}_2^0$-t. Az előbbi egy egyenlő oldalú háromszög, amelynek a csúcsai: $(-1, 0), (1, 2), (1, -2)$. Az $(1, 2), (1, -2)$ él kivételével a többi határoló élre illeszkedő pontokat is jellemezni tudtuk. Kiderült, hogy a $\mathcal{D}_2^0$ halmaz struktúrája igen bonyolult, de annak jelentős részét is jellemezni tudtuk. Elemzésünk választ ad arra, hogy miért nehéz a harmadfokú CNS polinomok, illetve azon harmadfokú β Pisot számok jellemzése, amelyekre a $\mathbb{Z}[1/\beta]$ minden elemének periódikus β-előállítása van.

A [7] dolgozatban az $(1,2),(1,-2)$ élre illeszkedő pontokat vizsgáltuk. Tulajdonképpen arról van szó, hogy az

$$0 \leq a_{n-1} + \lambda a_n + a_{n+1} < 1,$$

ahol $|\lambda| < 2$ nem lineáris rekurziónak eleget tevő, egész számokból álló a_n sorozatok tulajdonságát kellene leírni. Nyilvánvaló, hogy ha $\lambda = 0, -1, 1$, akkor az a_n sorozat periódikus. Számítógépes kisérletek azt mutatták, hogy ez mindíg így van. A nevezett dolgozatban ezt a sejtést vizsgáltuk. A sejtést be tudtuk bizonyítani akkor, ha $\lambda = \frac{1+\sqrt{5}}{2}$. A λ mindíg felírható $\omega + \bar{\omega}$ alakban, ahol ω az egységkörre esik. Megmutattuk, hogy adott λ-hoz tartozó pályák szerkezete lényegesen függ attól, hogy ω egységgyök-e. [6]-ben a fent ismertetett dolgozatok fő eredményeit foglaltuk össze.

[20]-ban Sárközy és szerzőtársai korábbi eredményeihez kapcsolódva megmutattuk, hogy az $\left(\frac{a_n}{p}\right)$ sorozat, ahol a_n egy lineáris rekurzív sorozat n-dik tagja, p pedig egy prímszám alkalmas feltételek mellett kriptográfiai szempontból jó tulajdonságú véletlen számsorozatnak tekinthető.

Bérczes Attila eredményei:

[9]-ben a korábbi idevágó eredményeket lényegesen élesítve illetve általánosítva felső korlátot adtak széteső polinom egyenletek megoldásszámára minden olyan esetben, amikor a megoldásszám véges. Ennek fő jelentősége abban áll, hogy a korlát egyrészt független a szóban forgó széteső polinom együtthatóitól, másrészt - a korábbi korlátokkal ellentétben - a polinom fokszámának csupán polinomiális függvénye.

[34]-ben a korábbi idevágó eredményeket igen jelentős mértékben általánosítva illetve élesítve felső korlátot adtak rögzített fokszámú és diszkriminánsú binér formák ekvivalencia osztályainak a számára. Bizonyos feltételek mellett szintén felső korlátot nyertek azon binér formák ekvivalencia osztályainak számára, melyek esetén a formához tartozó rend egy adott renddel izomorf. Megmutatták, hogy becsléseik a bennük szereplő paraméterek függvényében már élesek, illetve közel optimálisak.

[10] és [12]-ban vizsgálták norma formák kriptográfiai alkalmazásának lehetőségét, és javaslatot tettek egy ezen alapuló hash függvény használatára, melről belátták, hogy ütközésmentes.

[11]-ben [13]-ban és [14]-ben norma forma egyenletek számtani sorozatot alkotó megoldásaival kapcsolatban nyertek effektív eredményekett, illetve több parametrikus egyenletcsalád esetén az összes ilyen megoldást megkeresték.

Győry Kálmán eredményei:

Amint azt a közlemények jegyzéke mutatja, az ismertetésre kerülő eredmények egy része társszerzőkkel közösen elért eredmény.

1. Diofantikus egyenletek. Az [29, 35, 38] és [46] munkákban számos korábbi eredményt messzemenően általánosítva, mély és úttörő jellegű eredményeket ért el egy klasszikus, Fermat-ig és Euler-ig visszanyúló diofantikus témakörben, nevezetesen számtani sorozatokban található teljes hatványokra vonatkozóan. [46]-ban megmutatja, hogy csak véges sok olyan, különböző pozitív egészekből álló, $k \geq 4$ tagú számtani sorozat létezik, melynek tagjai korlátos kitevőjű teljes hatványok. Ezen kívül teljesen leírja a csak négyzetszámokból és köbszámokból álló relatív prím számtani sorozatokat. Erdős és Selfridge (1975) egy nevezetes tétele szerint egymásra következő pozitív egészek szorzata nem lehet teljes hatvány. Régi, sokat vizsgált, de sokáig megközelíthetetlen sejtés volt, hogy pozitív egészekből képzett, $k \geq 4$ tagú, $d > 1$ differenciájú számtani sorozat tagjainak a szorzata sem lehet teljes hatvány. [29] és [38]-ban $k < 12$-re bebizonyítja a sejtést. Az említett dolgozatokban a nevezett problémákat általánosított Fermat-típusú egyenletekre vezette vissza. Ezt követően a Fermat-sejtés bizonyítására kidolgozott ún. moduláris módszert esetenként továbbfejlesztve és más módszerekkel kombinálva, a kapott általános ternér egyenleteket megoldotta.

[45]-ben jelentős mértékben élesíti az S-egységegyenletek megoldásaira korábban nyert legjobb korlátokat. Ennek felhasználásával algebrai számtestek felett elsőként nyer a híres ABC-sejtésre vonatkozóan explicit eredményeket. [42]-ben a binom Thue egyenletek és az S-egységegyenletek egy közös általánosítására bizonyít effektív végességi tételt kvantitatív formában. Megmutatja, hogy ha a, b, c ismeretlen S-egységek, akkor az $ax^n - by^n = c$ egyenletnek csak véges sok és effektíve meghatározható $n \geq 3$, x, y, a, b, c egész megoldása van, melyekre az egyenlet tagjai relatív prímek. Analóg eredményeket nyer szuperelliptikus egyenletekre is. [44]-ben a tekintett egyenletet teljesen megoldja azokban az esetekben, amikor $c = 1$ és ab legfeljebb két, 13-nál nem nagyobb prímszámmal osztható. [47]-ben egy sokat vizsgált, szuperelliptikus egyenletekre vezető diofantikus problémakörben nyer úttörő jellegű eredményeket. Nevezetesen bebizonyítja, hogy (triviális esetektől eltekintve) az $1^k + 2^k + \cdots + n^k$, $n > 1$, $2 \leq k \leq 11$ összegek egyike sem lehet teljes hatvány. A bizonyításokban a modern diofantikus számelmélet szinte teljes arzenálját felhasználja, beleértve a Baker-módszert és a moduláris módszert is.

A [37] és [45] dolgozatokban folytatja a széteső forma egyenletekre vonatkozó kiterjedt vizsgálatait. [45]-ben általános végességi feltételek mellett jelentős mértékben élesíti a megoldásokra, valamint a széteső formák legnagyobb prímfaktorára korábban nyert felső illetve alsó korlátokat. [37]-ben végtelen sok megoldás mellet majdnem minden megoldás esetén explicit alsó korlátot ad a megoldások egy tetszőleges, de rögzített komponense legnagyobb prímfaktorának növekedésére.

1999-ben hatékony eljárást adott index forma egyenletek megoldására tetszőleges, $n \leq 5$ fokszámú számtestekben. [39]-ben most sikerült $n = 6$ esetén is működő numerikus eljárást kidolgoznia index forma egyenletek megoldására. A fő nehézség, hogy a fellépő egységegyenletekben az ismeretlenek száma elérheti a 14-et, amire a Wildanger-módszer már nem alkalmazható. [39] fő újdonsága Wildanger algoritmusának jelentős mértékű finomítása.

2. Polinomok és binér formák [30]-ban olyan újszerű eredményeket nyer kvantitatív formában, melyek azt mutatják, hogy egy egész együtthatós polinomot általában már "kevés" együtthatója meghatározza.

Ismeretes, hogy adott $n \geq 2$ fokszám és adott $D \neq 0$ diszkrimináns esetén unimoduláris transzformációtól eltekintve csak véges sok binér forma létezik. Ez effektív formában Evertse és Győry (1991) tétele. [43]-ban élesíti Evertse és Győry effektív és kvantitatív végességi eredményét. Továbbá rögzített felbontási test esetén [34]-ben uniform, a felbontási testtől független felső korlátot ad az n-edfokú és D diszkriminánsú binér formák ekvivalenciaosztályainak a számára. Az általánosabb formában, algebrai számtestek S-egészei felett kimondott és bizonyított tétel várhatóan sok alkalmazáshoz fog vezetni. [48]-ban hasonló eredményeket nyer adott rezultánsú binér forma párokra.

A [31, 41] és [48] dolgozatok áttekintő munkák a címükben feltüntetett témakörökről.

Tudományos eredményeiről meghívás alapján előadásokat tartott Grazban, Bécsben, Marseille-Luminyben, Szentpétervárott, Pozsonyban, Leidenben, Debrecenben, Minszkben, Torontóban, Campinasban (Brazília), Joanninaban (Görögország), Malenoviceben (Cseh Köztársaság), Bombayben nemzetközi konferenciákon, valamint Prágában, Szegeden, Thessalonikiben és Zürichben.

Herendi Tamás [49]-ben bebizonyítja, hogy ha u egy Dedekind-gyűrűbeli d-edrendű lineáris rekurzív sorozat, $s = (3d2 + 9d)/2 + 1$ és p egy prím normájú prímideál, akkor ha u egyenletes eloszlású moduló p^s, akkor egyenletes eloszlású moduló p^t, tetszőleges $t > 0$ esetén is. Az eredmény továbbfejlesztésével kidolgozott egy módszert, amellyel moduló 2^s egyenletes eloszlású nagy periódushosszú lineáris rekurzív sorozatokat lehet előállítani.

Horváth Géza eredményei:

A pályázatban szereplő témakörökben Horváth Géza egy dolgozatot készített. A [50] cikkben bemutatott új faktorizáló algoritmus ugyanazon feltételek esetén hatékony, amikor a klasszikus Fermat faktorizáció, ugyanakkor attól jelentős mértékben gyorsabb. Az újabb faktorizáló algoritmusnak megadtuk egy még gyorsabb változatát, ahol már kihasználjuk a rendelkezésre álló memóriát is.

Hivatkozások

[1] Sh. Akiyama and A. Pethő, *On canonical number systems*, Theor. Comp. Sci., 270 (2002), 921–933.

[2] Sh. Akiyama, H. Brunotte and A. Pethő, *Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert*, J. Math. Anal. and Appl., **281** (2003), 402–415.

[3] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. Thuswaldner, *On a generalization of the radix representation - a survey*, Fields Institute Communications, 41, 2004, 19-27., 2004.

[4] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. Thuswaldner, *Generalized radix representations and dynamical systems I*, Acta Math. Hungar., **108 (3)** (2005), 207 - 238.

[5] S. Akiyama, H. Brunotte, A. Pethő and J. M. Thuswaldner, *Generalized radix representations and dynamical systems II,* Acta Arith. **121** (2006), 21-61.

[6] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. Thuswaldner, *Basic properties of shift radix systems*, Acta. Math. Acad. Paed. Nyíregyháziensis, to appear.

[7] S. Akiyama, H. Brunotte, A. Pethő and W. Steiner, *Remarks on a conjecture on certain integer sequences*, Periodica Mathematica Hungarica, to appear.

[8] G. Barat, Ch. Frougny and A. Pethő, *On linear recurrent Mahler numbers*, Integers, **5** (2005) #A1, 17 pages. http://www.westga.edu/ integers/vol5-3.html

[9] A. Bérczes A, K. Győry, *On the number of solutions of decomposable polynomial equations,* Acta Arith, 2002; 101:171-187.

[10] A. Bérczes, J. Ködmön *Methods for the calculation of values of a norm form*, Publ. Math. Debrecen, 2003; 63: 751-768.

[11] A. Bérczes, A. Pethő, *On norm form equations with solutions forming arithmetic progressions*, Publ. Math. Debrecen, 2004; 65:281-290.

[12] A. Bérczes, J. Ködmön and A. Pethő, *A one-way function based on norm form equations*, Periodica Math. Hungar., **49**, 1-13, 2004.

[13] A. Bérczes and A. Pethő, *Computational experiences on norm form equations with solutions forming arithmetic progressions*, Glasnik Math., to appear

[14] A. Bérczes, A. Pethő and V. Ziegler, *Parameterized Norm Form Equations with Arithmetic progressions*, J. Théorie Nombres de Bordeaux, to appear.

[15] H. Brunotte, A. Huszti and A. Pethő, *Bases of canonical number systems in quartic algebraic number fields*, submitted.

[16] Cl. Fuchs and A. Pethő, *Effective bounds for the zeros of linear recurrences in function fields*, J. Théorie Nombres de Bordeaux, to appear

[17] Cl. Fuchs, A. Pethő and R.F. Tichy, *On the diophantine equation* $G_n(x) = G_m(P(x))$, Monatshefte Math., **137** (2002), 173–196.

[18] Cl. Fuchs, A. Pethő and R.F. Tichy, *On the Diophantine equation* $G_n(x) = G_m(P(x))$*: higher order recurrences*, Trans. Amer. Math. Soc., **355** (2003), 4657–4681.

[19] Cl. Fuchs, A. Pethő and R.F. Tichy, *On the diophantine equation* $G_n(x) = G_m(P(y))$ *with* $Q(x, y) = 0$, submitted

[20] K. Gyarmati, A. Sárközy and A. Pethő, *On linear recursion and pseudorandomness*, Acta Arith., **118** (2005), 359 - 374.

[21] E. Herrmann, I. Járási and A. Pethő, *Note on J.H.E. Cohn's paper "The Diophantine equation $x^n = Dy^2 + 1$"*, Acta Arith., to appear.

[22] C. Heuberger, A. Pethő and R.F. Tichy, *Thomas' family of Thue equations over imaginary quadratic fields*, J. Symbolic Comp., **34** (2002), 437-449.

[23] V. Komornik, P. Loretti and A. Pethő, *The smallest univoque number is not isolated*, Publ. Math. Debrecen, **62/3-4** (2003), 429–435.

[24] A. Pethő, *Notes on CNS polynomials and integral interpolation*, to appear.

[25] Pethő Attila, *Rekurzív polinomsorozatok*, a 2002 november 12.-én, tartott előadás szerkesztett változata.

[26] Pethő Attila, *Egy negyedrendű rekurzív sorozatcsaládról*, Acta Acad. Paed. Agriensis, submitted

[27] A. Pethő, *Connections between power integral bases and radix representations in algebraic number fields,* Proc. 2003 Nagoya Conf. Ÿokoi-Chowla Conjecture and Related Problems;̈ Eds.: S-i. Katayama, C. Levesque and T. Nakahara, Furukawa Total Pr. 2004, 115-125., 2004

[28] S. Schmitt and H.G. Zimmer, Elliptic Curves - A Computational Approach, with an Appendix by Attila Pethő, de Gruyter Studies in Mathematics: 31, 2003.

[29] K. Győry, L. Hajdu, N. Saradha, *On the diophantine equation* $n(n+d)\dots(n+(k-1)d) = by^l$, Canad. Math. Bull.47 (2004),373-388.

[30] K. Győry, L. Hajdu, A. Pintér, A. Schinzel, *Polynomials determined by a few of their coefficients*, Indag. Math.15(2004) 209-21

[31] K. Győry, *Perfect powers in products with consecutive terms from aritmetic progressions*, megjelenés alatt

[32] K. Győry A. Pintér, *On the equation* $1^k + 2^k + \dots + x^k = y^n$, Publ. Math Debrecen 62(2003)403-414

[33] K. Győry, *On some aritmetical properties of Lucas and Lehmer numbers II*, Acta Acad. Paed. Agriensis, Sect Math. 30(2003),67-73

[34] A. Bérczes, J.H. Evertse, K. Győry, *On the number of equivalence classes of binary forms of given degree and given discriminant*, Acta Arith.113(2004) 363-99.

[35] K. Győry A. Pintér, *Almost perfect powers in products of consecutive integers*, Monatsh. Math.145 (2005), 19-33

[36] Y Bugeaud, K. Győry, *On binominal Thue-Mahler equations*, Periodica Math. Hungarica49(2004),25-34.

[37] G. Everest, K. Győry, *On some aritmetical properties of solutions of decomposable form equations*, Math. Proc. Cambridge Philos. Soc.139(2005), 27-40

[38] M. Bennett,N. Bruin, K. Győry, L. Hajdu, *Powers from products of consecutive terms in aritmetic progression*, Proc. London Math. Soc..megjelenés alatt, 2004

[39] Y. Bilu, I. Gaál, K. Győry, *Index form equations in sextic fields: a hard computation*, Acta Arith 115, 85-96, 2004

[40] K. Győry, A. Pethő and Á. Pintér, *Béla Bridza (1958-2003)*, Publ. Math. Debrecen 65 (2004), 1-11.

[41] K. Győry, *Index form equations and their applications*, The Proc. of the Institute of Math. of NAN of Belarus, 13 (2005), 83-93.

[42] K. Győry, I. Pink and Á. Pintér, *Power values of polynomials and binomial Thue-Mahler equations*, Publ. Math. Debrecen 65 (2004), 341-362.

[43] K. Győry, *Polinomials and binary forms with given discriminant*, megjelenés alatt, 2004,

[44] M. Bennett, K. Győry, M. Mignotte, Á, Pintér, *Binomial Thue equatipons and polynomial powers*, Compositió Math., megjelenés alatt, 2004

[45] K. Győry, K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith.,2005

[46] N. Bruin, K. Győry, L. Hajdu and Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag Math, megjelenés alatt, 2005

[47] M. Bennett, K.Győry, A. Pintér, *On the Diophantine equation* $1^k + 2^k + \cdots + x^k = y^n$, Compositio Math. 140, 1417-1431., (2004)

[48] A. Bérczes, J.H. Evertse, K.Győry, *Diophantine problems related to discriminants and resultants of binary forms*, Diophantine Geometry, 2007

[49] T. Herendi *Uniform distribution of linear recurring sequences modulo prime powers*, Finite Fields and Their Applications 10 (2004) 1-23, 2004

[50] G. Horváth *A φ faktorizáló algoritmus*, Alkalmazott Matematikai Lapok 21, (2004), 253-262., 2004