OTKA NK104183 záró beszámolója
Mivel a részbeszámolókban szerepelnek az adott év eredményei, alább a 2017.02.01-2017.12.31-ig terjedő eredményekről adunk számot
Since the yearly reports contain the results of the given years here we present only the results of the last period, from 01.02.2017 until 31.12.2017

József Solymosi was working on Erdős-type problems in discrete geometry. He used combinatorial, algebraic, and probabilistic methods to improve various earlier results in the field. Probably the strongest results are in a paper with J. Balogh, where they applied the so-called Hypergraph Container Method to improve significantly some longstanding bounds.
In the work of Katalin Gyarmati the cross-combined measure (a natural extension of the cross-correlation measure) is introduced and important constructions of large families of binary lattices with optimal or nearly optimal cross-combined measures are presented.
These results are also strongly related to the one-dimensional case: An easy method is shown obtaining strong constructions of families of binary sequences with nearly optimal cross correlation measures based on the previous constructions of families of lattices. The important feature of this result is that so far there exists only one type of construction of very large families of binary sequences with small cross-correlation measure, and this only type of constructionwas based on one-variable irreducible polynomials.
However there are relatively fast algorithms to construct one-variable irreducible polynomials, still in certain applications these algorithms are too complicated or are not fast enough, thus it became necessary to show other types of constructions where the generation of sequences is much faster. Using binary lattices based on two-variable irreducible polynomials this problem can be avoided. (Since, contrary to one-variable polynomials, using the Schöneman-Eisenstein criteria it is possible to generate two-variable irreducible polynomials over F_p easily and very fast.)
András Sár közy, in a paper with Dartyge, and Gyarmati studied the irregularities of binary sequences relative to short arithmetic progressions, and they introduced a quantitative measure for this property. In this paper they give constructive bounds for the minimal value of this measure for binary sequences of a given length.
A few years ago new quantitative measures of pseudorandomness of binary sequences have been introduced. Since that these meaures and constructions applying them have been used in many papers. In a paper of Mérai, Rivat and SárkÖzy analyze the connection between the new measure and the NIST tests which are also used for studying pseudorandomness of binary sequences.
András Bíró reached important results concerning the hyperbolic circle problem for Fuchsian groups and on some integrals of hypergeometric functions.
Gergely Harcos and Peter Maga solved the sup-norm problem for spherical Hecke-Maass newforms of square-free level for the group GL(2) over a number field, with a power saving over the local geometric bound simultaneously in the eigenvalue and the level aspect.Their bounds feature a Weyl-type exponent in the level aspect, they reproduce or improve upon all known special cases, and over totally real fields they are as strong as the best known hybrid result over the rationals.
In further joint works with Blomer and Milicevic they established various basic analytic properties of spherical cusp forms on GL(n) over the rational numbers. They proved good pointwise upper bounds for these automorphic forms and their Whittaker functions, with a

particular emphasis on their global sup-norms. Their bounds are uniform in the Laplace eigenvalue and complement nicely the existing lower bounds. They also progressed understanding of the "essential support" of spherical cusp forms, i.e. the region outside which they decay exponentially.

Gyula Katona wrote a survey paper showing connections between the work of Levon Khachatrian, namely the Complete Intersection Theorem and the solution (given by the author and D.T. Nagy) of a problem of Körner asking for the maximum size of a family where certain unions are intersecting.

Ruzsa (joint with Horváth) studied additive and multiplicative combinatorial properties of integers. They improved the bound for the size of a sumset or difference set in the case when one of them is near to the possible maximal value. Improved some of the known sum-product estimates for the whole set or involving only pairs along a graph.

Endre Szemerédi (with coauthors Hladky, Piquet, Simonovits and Stein) proved an approximate form of the Loebl-Komlós-Sós conjecture.

Akiyama, Evertse and Pethő studied systematically nearly linear recursive sequences, i.e. sequences of complex numbers such that the difference of the n-th term and a linear combination of the preceding k terms is uniformly bounded. Such sequences appear frequently in the applications. They proved a Binet like formula, proved that its fluctuation can be arbitrary large, that the Skolem-Lech-Mahler theorem does not hold for them.

Pethő finished in 2017 two papers with Austrian coauthors. With J. Thuswaldner and M. Weitzer he studied shift radix systems with general parameters. Usually srs is bounded only if its eigenvalues lie inside or on the unit circle, but under special circumstances this is no longer true. We proved results in any dimension, but the focus of our interest were planary srs. Int hat case we characterized all exceptional cases up to a bounded small region.

In the second manuscript he, with J. Thuswaldner, generalized canonical number systems to relative extensions of algebraic number fields. Another innovativation is the definition of digit set with the application of fundamental domains. They were able to prove far reaching generalizations of old results of B. Kovács. They proved among others that usually the bases of GNS with finiteness property coinside up to finitely many exceptions, with bases of power integral bases.

Discriminant equations are of basic importance in Diophantine number theory. In their book "Discriminant Equations in Diophantine Number Theory" (Cambridge University Press, 2017) Győry with Evertse gave the first comprehensive treatment of the equations mentioned. The book contains many earlier and new results and applications of the authors and others. In a joint paper with Evertse, Győry proved new effective finiteness results on discriminant equations over the most general integral domains possible. Together with Bugeaud and Evertse Győry established general new results on the S-parts of values of univariate polynomials, binary forms and decomposable forms at integral points. Further, together with Bertók, Hajdu and Schinzel, he obtained several important results on certain generalizations of exceptional units in number fields.

András Bazsó together with István Mező showed that, for integers $\ell>1$, $m\neq 0$, r with $\gcd(m,r)=1$, the alternating sum $rn - (m+r)n + (2m+r)n - \ldots + (-1)\ell\text{-}1((\ell\text{-}1)m+r)n$ can be explicitly given in terms of Stirling numbers of the first kind and r-Whitney numbers of the second kind. Further, they proved that the coefficients of the polynomial extensions of the above sums are all integral if and only if m is even.

Bazsó, Bérczes, Hajdu and Luca investigated polynomial values of sums of products of consecutive integers. For the degree two case they gave effective finiteness results, while for the higher degree case they provided ineffective finiteness theorems. They further showed that the polynomials corresponding to the sums of products in consideration, are indecomposable.

Bérczes, Dujella, Hajdu and Tengely introduced the notion of, and prove finiteness results on so called (F,m)-Diophantine sets A, where F is a bivariate polynomial with integer coefficients such that for all distinct a,b from A the numbers F(a,b) are full m-th powers.

Bérczes, Pink, Savas and Soydan give upper bounds for n on the equation (x +1)^k+(x +2)^k+... +(2x)^k=y^n. Their results depend on assertions describing the precise exponents of 2 and 3 appearing in the prime factorization of the left hand side. Further, on combining Baker's method with the explicit solution of polynomial exponential congruences we show that for 1<x<14, k>0, y>1and n>2 the title equation has no solutions.

János Folláth together with Tamás Herendi further investigated their new discrete Gaussian sampler algorithm. The algorithm samples from the theoretical distribution directly in the same sense as Karney's sampler does, but is 24% faster. The main application is using it in the implementation of certain lattice based Post-Quantum cryptographic signature schemes.

Hajdu, Laishram and Tengely investigated power values of sums of products of consecutive integers. They gave general finiteness results, and also gave all solutions when the number of terms in the sum considered is at most ten.

Andrea Huszti with Norbert Oláh suggested a cryptographic protocol for identity verification and key exchange. Shared control among the cloud servers is provided by applying a Merkle-tree for storing one-time passwords distributed. A security analysis is carried out in case of external attacks. They show that their protocol fulfills typical security requirements of a key exchange protocol, i.e. authentication of the participants, key secrecy, key freshness and confirmation that both parties know the new key in the Dolev-Yao model.

Andrea Huszti with Zita Kovács provided a reductionist proof for sender anonymity of their asymmetric bilinear pairing based mixnet, called BILMIX. They give an experiment-based definition for anonymity and show that BILMIX possesses anonymity in the semi-honest model against static adversaries assuming that the co-Bilinear Diffie-Hellman Problem, the Matching Find-Guess Problem and the Matching Diffie-Hellman Problem are hard.

Á. Pintér and Cs. Rakaczki obtained several results on the decomposition of Euler polynomials. These can lead to applications in Diophantine equations. Á. Pintér with coauthors consider applications of mathematics in pharmacology.

Tengely studied composite rational functions having zeros and poles forming consecutive elements of an arithmetic progression. He gave a classification and as an application provided examples of composite rational functions having 3 or 4 zeros and poles. Tengely and Ulas considered a problem of Pethő related to existence of a quartic algebraic integer s for which t=4s^4/(s^4-1)-s/(s-1) is a quadratic algebraic number. By studying rational solutions of certain Diophantine system they proved that there are infinitely many quartic algebraic integers such that the corresponding t is quadratic. Moreover, they presented a description of quartic numbers such that the corresponding t is a quadratic real number.