# Report on the scientific achievements supported by the OTKA-115479 (1 January, 2016 – 31 December, 2021)

This project can be regarded as a continuation of our previous project OTKA-100339 (2012-2015). In the frame of the present project many significant qualitative, quantitative and numerical results and some important breakthroughs have been established in Diophantine number theory, mostly in international cooperation. The results led to very important applications in algebraic number theory, Diophantine approximation and Diophantine geometry. The results have been published in 3 books and 117 research papers, and were presented at many international conferences and seminars.

During the period of the project KÁLMÁN GYŐRY has been elected a member of the Polish Academy of Science and Art (2016) and the European Academy (2016). He has been awarded honorary doctorate by the Selye University of Komarno (2016). ATTILA BÉRCZES defended (2017) and SZABOLCS TENGELY submitted (2021) their academic doctor's dissertations.

We now briefly summarize the most important results of the research group. In our report, the joint results of the participants will be mentioned only at one place.

RESULTS OF Kálmán GYŐRY: In the frame of the project GYŐRY published 2 books and 16 research papers.

Since the 1970s, several general effective finiteness theorems have been obtained by GYŐRY for discriminant equations, including monic polynomials and algebraic integers with given discriminant. These led to important applications to index from equations and power integral bases, and provided the solutions of some old problems. Since the 1980s, Evertse and GYŐRY have established significant results on the number of solutions of the equations under consideration and on binary forms of given discriminant. Later, a great number of numbertheorists joined these investigations. In their book „Discriminant equations in diophantine number theory", published in 2017 at Cambridge University Press, Evertse and GYŐRY gave the first comprehensive account of discriminant equations and their applications to algebraic number theory, diophantine approximation and diophantine geometry. The book contains several new results as well. Recently, the authors extended their effective results to equations over integral domains, finitely generated over Z, that are not necessarily integrally closed. The proofs are mainly based on the diophantine results of the authors concerning unit equations.

The so-called S-unit graphs play a very important role in the theory of Diophantine equations: for example, such graphs are the basic objects behind the proofs of several deep, classical theorems of GYŐRY concerning unit equations and decomposable form equations. GYŐRY and HAJDU, together with Tijdeman earlier initiated the systematic study of such graphs, proving several basic results about representability questions. In the frame of the project, they have extended these results to the algebraic number field case. In their proofs, beside classical ineffective and effective finiteness theorems concerning S-unit equations (due to GYŐRY and others), they have used novel ideas of combinatorial nature.

There is an extensive literature on arithmetical properties of values of univariate polynomials, binary forms and decomposable forms at integral points. GYŐRY, jointly with Bugeaud and Evertse, have established several deep results on the S-parts of values of these polynomials and forms, where S denotes a finite set of fixed primes. They proved in a quantitative form that the S-parts of the values cannot be large compared with the values under consideration. Their ineffective results are already best possible. Density results, weaker but effective versions and some applications to discriminants of algebraic integers are also given.

Unit equations and in particular exceptional units have been investigated by many authors, and they have important applications. GYŐRY, together with Bertók, HAJDU and Schinzel proved several interesting results concerning a generalization of exceptional units. For a number field K, denote by L(K) the smallest integer n≥3 such that the unit equation e_1+...+e_n=0 is solvable in units e_1, ..., e_n of K. When such an n exists, they gave an explicit upper bound for L(K), and proved various properties of L(K), including its magnitude and parity. As an application, they dealt with the representability of cycles in certain arithmetic graphs.

Number systems have been intensiven studied among others in algebraic number fields. Recently, GYŐRY and PETHŐ together with Evertse and Thuswaldner have extended several earlier results to a class of general integral domains.

S-unit equations and decomposable form equations play an extremely important role in Diophantine number theory. GYŐRY was the first to give explicit upper bounds for the solutions of such equations. These bounds were later improved by himself and others. Recently, he considerably improved upon, in terms of S, the best known effective bounds for the solutions of such equations. These led to several significant applications, for example towards the ABC-conjecture over number fields.

GYŐRY (1983,1984) initiated to extend effective Diophantine finiteness results over number fields to the finitely generated case over Z when the ground domain may have transcendental elements, too. He developed an effective specialization method, reducing the initial equations to the number field and function field case, and using the corresponding effective results over number fields and function fields, he derived effective bounds for the solitions of the initial equations. In 2013, Evertse and GYŐRY refined Győry's method. By means of this general method every effective Diophantine finiteness theorem concerning integral solutions of polynomial equations over number fields can be extended in an effective way to the finitely generated case, provided that an effective analogue over function fields is at our disposal. Using this method, several people, including the authors, have estableshed general effective finiteness theorems in quantitative form for many classical equations over finitely generated domains.These led to several applications. The recent book of Evertse and GYŐRY (2022) provides the first comprehensive and up-to-date treatment of effective results and methods for Diophantine equations over finitely generated domains.

RESULTS OF Attila PETHŐ: PETHŐ published 6 papers.

He finished one paper with L. HAJDU and Cs. Bertók. They used the method of Akiyama and PETHŐ to expresse the volume of the set of coefficient vectors of real polynomials of degree d, signature s and lying in the unit square. They deduced an asymptotic formula for the number of polynomials of integral coefficients, of degree d and signature s. This improves considerably an earlier result of A. Dubickas. With Akiyama and Evertse, PETHŐ investigated nearly linear recursive sequences (nlrs), i.e. sequences whose terms satisfy a linear recursive relation with a bounded error term. They proved a Binet-like formula and that such sequences may have arbitrarily large fluctuation. Moreover, they proved that nlrs have completely different arithmetical properties than lrs. For example, the Skolem-Lech-Mahler theorem does not satisfy for them and they may have infinitely many common terms.

PETHŐ with J. Thuswaldner and M. Weitzer 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. They proved results in any dimension, but the focus of their interest were planary SRS. In that case they characterized all exceptional cases up to a bounded small region. Further PETHŐ, with J. Thuswaldner, generalized canonical number systems to relative extensions of algebraic number fields. Another innovation 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 coincide up to finitely many exceptions, with bases of power integral bases.

RESULTS of István GAÁL: He published 1 book and 17 papers.

He considered monogenity of algebraic number fields. His results in this area were summarized in the new and considerably extended edition of his book Diophantine equations and power integral bases, Theory and algorithms.

Together with Remete and Szabó they investigated the calculation of generators of power integral bases by using the relative indices. An application of this method was given by him and Remete for some infinite families of octic fields. With Remete they investigated integral bases and monogenity of pure number fields of degees 3 to 9. This results initiated a series of results on the monogenity of pure fields of various degrees.

In many cases one can construt a linear combination of the factors of the index form that is divisibly by certain constants. This can be used to exclude monogenity in some number fields. Usng this method he and Remete characterized monogenity in the family of simplst sextic fields. With Jadrijevic he described elements of minimal indices in a family of quartic fields.
Using the factors of the index form, with Remete he considered monogenity in composites of quadratic fields with simplest cubic fields, pure cubic fields etc.
It turned out that the resolution of totally real relative Thue equations over imaginary quadratic fields can be reduced to the resolution of absolute Thue equations. This idea was applied to solve all simplest quartic and simplest sextic relative Thue equations over imaginary quadratic fields. It made possible to consider monogenity of totally complex sextic fields much more efficiently then formerly.

Using Kummer theory and class field theory with M.C.Pohst and M.E. Pohst he constructed an efficient method to calculate solutions of Mordell type equations $y^2=x^3+k$. This made possible to extend the range $|k|<10^7$ to about $|k|<10^{15}$.

Using the factors of the index form with Remete he described an efficient algorithm to calculate generators of power integral bases in cubic and quartic extensions of totally real quadratic fields.

Extending former methods for relative quartic extensions, he gave an algorithm to calculate generators of power integral bases in in totally complex quartic extensions of real fields. The method uses Baker's method and reduction.

Using LLL basis reduction algorithm an efficient mehtod was given by him to find "small" solutions (say, with absolute values less than $10^{100}$) of relative Thue equations. This can be applied e.g. to find generators of relative power integral bases in sextic fields with a quadratic subfield. It was shown by him that also relative index form equations of totally real extensions of imaginary quadratic fields can be reduced to absolute index form equations. He investigated monogenity in an infinite family of sextic fields. The corresponding family of sextic polynomials was found to be monogenic formerly. In the paper all generators of power integral bases are calculated.

RESULTS of Ákos PINTÉR: He published 7 papers.

Together with Adédjia, BoHe and AlainTogbé they considered the extensibility of the Diophantine triple $\{a,b,c\}$, where $a<b<c$ with $a=3b$, and proved that such a set cannot be extended to an irregular Diophantine quadruple. As corollary, they proved that any Diophantine quadruple which contains the pair $\{a,3a\}$ is regular. They showed that by considering the case $b=8a$ one obviously obtain similar results.

The Bernoulli and Euler numbers/polynomials play an important role in Diophantine number theory. Of particular importance are the results concerning the indecomposability of such polynomials. PINTÉR together with Rakaczki have obtained remarkable results more generally on the indecomposability of linear combinations of Bernoulli and Euler polynomials. Their results have important applications to various Diophantine problems.

RESULTS of Lajos HAJDU: HAJDU obtained important results in several topics of the project. We mention only the most important directions and results. He published 49 papers.

***Exponential Diophantine equations and their applications.*** A famous conjecture of Skolem states that (under certain simple, necessary assumptions) if an exponential Diophantine equation has no solutions, then it has no solutions modulo m with an appropriate m. Beside being interesting in itself, the validity of this conjecture would have an extremely important impact on the theory of exponential Diophantine equations. Earlier, based upon their related results, HAJDU together with Bertók worked out a heuristic method, for finding all solutions of exponential Diophantine equations with integral bases. During the project they extended their results over number fields. The importance of their method is that by the present tools such equations can be explicitely solved only if the number of (nonzero) terms is at most two. Skolem's conjecture is still open: so far only the one-term case has been proved by Schinzel. BÉRCZES and HAJDU, together with Luca and Tijdeman (in a series of papers) could make a breakthrough: they were able to prove Skolem's conjecture for exponential Diophantine equations of the form a^x-tb_1^{y_1}… b_k^{y_k}=\pm 1 and a^n-tb^n=c^n. In particular, Fermat's equation (with a,b,c fixed) is included in the new result.

The Diophantine equation 1^k+...+x^k=y^n is one of the most classical Diophantine equations, and has been studied by several mathematicians. By a well-known conjecture of Schaffer, this equation has only certain long known solutions. BÉRCZES, HAJDU and PINK, together with Miyazaki, has found all solutions of the equation for x<25. This theorem is of novel nature: earlier (up to a preceeding result of HAJDU) the equation was investigated only for fixed k and/or n.

***Polynomial Diophantine equations.***

The Diophantine equation x(x+d)…(x+(k-1)d)=by^n has a long history going back to Fermat and Euler, and has been studied by eminent mathematicians. There ara also many results concerning the more general equation when the right hand side is replaced by an arbitrary polynomial g(y) having rational coefficients. In these results the root structure f(x) ont he left hand side of the equation is heavily used. In the frame of the project HAJDU initiated the study of the question that how far one can 'perturb' the symmetry of the roots such that finiteness results for the solutions are still available. First, as special (but already nontrivial) cases, together with Varga and Papp they studied tha cases when one term is added to or removed from f(x), respectively (with generaly right hand side g(y)). Then, together with Papp and Tijdeman, they have described cases when 'many' terms are deleted. Finally, together with Tijdeman they took up the case when f(x) is arbitrary with rational roots. They could link the question to the famous Prouhet-Tarry-Escott problem, and could obtain precise results for the possible degrees of f,g when the equations have infinitely many solutions.

***Irreducibility of Diophantine sets.*** The additive and multiplicative irreducibility of certain arithmetic sets is an old problem, with many deep and intersting result, and with several open questions and conjectures. One of the most famous open conjectures is due to Ostmann, which states that the set of primes cannot be decomposed into the som of two sets, in the asymptotic sense. In the frame of the project, in a series of papers, HAJDU together with Sárközy studied the additive and multiplicative irreducibility (indecomposability) of value sets of polynomials with integer coefficients. Among others, they were able to obtain sharp results for the additive irreducibility of subsets of shifted squares, and they proved a multiplicative analogue (for the

shifted case) of a classical theorem of Sárközy and Szemerédi concerning the additive irreducibility of the set of squares, when a certain number of elements are allowed to be changed. In fact, all these result concern the asymptotic case, i.e. provide 'total irreducibility'. In the proofs of their results, they needed to combine deep tools from the theory of polynomial Diophantine equations, by methods from additive and multiplicative number theory and graph theory.

GYŐRY and HAJDU, together with Sárközy in a series of papers studied the additive and multiplicative irreducibility (in the asymptotic sense) of sets of smooth numbers and sets of integers composed of a 'narrow' set of primes and their shifts. They could considerably sharpen several results from the literature, and they could provide theorems of new types, as well. They also demonstrated that their results cannot be extended to arbitrary situations (or, in other words, that the conditions in their theorems cannot be omitted): if the function y(n) in the definition of smooth numbers grows too rapidly, or the underlying set of primes is 'too thick', then the obtained sets will be reducible. In the proofs of their results, they needed to combine deep tools from the theory of exponential Diophantine equations (S-unit equations), by methods from additive and multiplicative number theory and graph theory.

RESULTS of Attila BÉRCZES: He published 10 papers.

With HAJDU, PINK and Miyazaki they completely solved the equation 1+x^a+z^b=y^n in the positive unknowns n≥4,a,b,y, for all integers values of x,z of with different parity.and with 1≤ x,z≤ 50. In the proof a very sharp Baker-type estimate is combined with local considerations.

In 2016 BÉRCZES submitted his academic doctoral thesis to the Hungarian Academy of Sciences.

With Luca, PINK and Ziegler they study trinomials of the form X^n-BX+A with integral S-unit coefficients A, B having a quadratic factor. For n>30 they describe all such polynomials, which in fact belong to four families, two finite and two infinite ones. Excluding the two infinite families for n >2 we also provide effective finiteness result for the rest of the polynomials with the above property. In the case S={2,3,5,7} they determine explicitly all polynomials in question.

With BAZSÓ, HAJDU and Luca they investigate polynomial values of sums of products of consecutive integers. For the degree two case we give effective finiteness results, while for the higher degree case we provide ineffective finiteness theorems. For the latter purpose, we also show that the polynomials corresponding to the sums of products we investigate are indecomposable.

With PINK, Savas and Soydan they give upper bounds for n on the title equation. 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.

With Bilu and Luca he proves an effective finiteness result for the equation u_n u_(n+1)…u_(n+k)=±u_m^2, where u_n is a second order recurrence sequence, whose characteristic polynomial has free term equal to 1 or -1. Similar results have been established in the case when u_n is a Lucas-sequence. In that case the question of large indices is easily handled using the powerful and famous result of Bilu, Hanrot and Voutier on primitive prime divisors of Lucas sequences. They consider such recurrence sequences u_n which are not Lucas sequences, so the above mentioned powerful tool cannot be used. This is the first effective result in the literature on the equation in title which has been achieved without the use of the primitive prime divisor theorem.

Erdős and Graham made a systematic study of the problem of products of factorials being a square, but left open the question concerning higher powers. With Dujella, HAJDU, Saradha and Tijdeman, he proves several results for products of factorials being a perfect power.

With coauthors, he uses tools from discrete mathematics to analize the database of patients who suffered haemorrhagic stroke in Hungary in a given timeframe.

RESULTS of Szabolcs TENGELY: He published 18 papers.

There are many questions in a monograph of Erdős and Graham related to representations of rational numbers $n/2^n$ as a sum. Some of these questions were already answered by Borwein and Loring. TENGELY, Ulas and Zygadlo extended these results and investigated other aspects of the problem.

TENGELY and Ulas extended a result by Nemes and PETHŐ related to the Diophantine equation $P(x)=R_n$, where $R_n$ is a recurrent sequence and $P(x)$ is a polynomial. They proved the existence of a polynomial $P_k(x)$ of degree 2k-1 such that the equation $P_k(x)=F_m$ has infinitely many solutions in positive integers (x,m), here $F_m$ denotes the Fibonacci sequence.

Hashim, Szalay and TENGELY provided a general argument to deal with Markoff-Rosenberger equations, where the solutions are elements of certain generalized Lucas sequences.

HAJDU and TENGELY investigated the function describing the number of *l*-th powers among the first N terms of an arithmetic progression ax+b. They completely described the arithmetic progressions containing the most *l*-th powers asymptotically.

ITRU cryptosystem is a public key cryptosystem and one of the known variants of NTRU cryptosystem. They claimed that ITRU has better features comparing to the classical NTRU, such as having a simple parameter selection algorithm, invertibility, and successful message decryption, and better security. Hashim, Molnár and TENGELY presented an attack technique against the ITRU cryptosystem.

Hashim and TENGELY generalized a result presented by Marques and Togbé in which they found all the Fibonacci numbers with only one distinct block of digits of length up to 10 in its decimal expansion. Also some general finiteness results were obtained and in case of Fibonacci and Pell numbers the argument was applied to completely solve the problem in some numeral systems.

Denote by P_A(n) the number of partitions of an integer n into parts from the set A. If A is the set of natural numbers, then P_A(n) is the famous partition function introduced by Euler and extensively studied by Ramanujan. Tengely and Ulas proved several results related to Diophantine equations of the form P_A(x)=P_B(y).

TENGELY and Ulas presented results of computations of all integer points on certain one parametric curves of genus 1 and 3, related to cubic and quartic fields, respectively. Their approach is based on Gröbner basis techniques and they do numerical experiences based on it.

RESULTS of István PINK: He published 5 papers.

Earlier HAJDU together with PINK have completely solved the Diophantine equation 1+2^a+x^b=y^n for x<50 (with a,b,y,n being unknown integers). In the frame of the project Pink together with BÉRCZES, HAJDU and Miyazaki could make a step further by finding all solutions of the Diophantine equation 1+x^a+z^b=y^n, where x,z<50 are integers of different parities, and a,b,y,n are unknown integers with n>3.

Together with Bertók, HAJDU and Rábai, he proved several results concerning common elements of recurrence sequences. Among others, extending results of Togbe, Luca and others, they completely described all Fibonacci numbers of the form 2^a+3^b+5^c.

Together with BÉRCZES, HAJDU and Rout, he gave various finiteness results concerning terms of recurrence sequences U_n representable as a sum of S-units with a fixed number of terms. They proved that under certain (necessary) conditions, the number of indices n for which

U_n allows such a representation is finite, and can be bounded in terms of the parameters involved.

Jointly with Miyazaki, they investigated the Diophantine equation a^x+b^y=c^z (1), where a,b,c are positive integers with min(a,b,c)>1 and gcd(a,b,c)=1. There are many papers in the literature dealing with the number of solutions (x,y,z) of (1). In 2019 Hu and Le proved that if max(a,b,c)>10^62 then (1) has at most two solutions (x,y,z). Together with Miyazaki, PINK improved this result by proving that (1) has at most two solutions (x,y,z) except if (a,b,c) is in {(3,5,2), (5,3,2)} in which case equation (1) possesses exactly three solutions. Note that this result is sharp and definitive. In the reporting period, the authors have made some important improvements for specific values of a,b,c, confirming a conjecture of Scott and Styer.

RESULTS of Gábor NYUL: He published 10 papers.

NYUL worked mainly in the field of combinatorial numbers. Stirling and Bell type numbers count permutations/partitions of a finite set with a fixed or an arbitrary number of cycles/blocks. He introduced and studied several variants and generalizations of such numbers together with his PhD students, including Eszter Gyimesi, Gabriella Rácz and Zsófia Kereskényi-Balogh. Since it plays a crucial role in these investigations, they defined the r-generalization of these numbers where r distinguished elements have to belong to distinct cycles/blocks.

Beside the above, NYUL also wrote a paper about some variants of Stirling and Bell numbers interpreting them through the combinatorics of rhyme schemes, and a popularizing article for secondary school students about diophantine number sets.

Together with Tímea Arnóczki, GÁBOR NYUL strengthened an almost forty-year-old result of Nakahara stating that the set of minimal indices of bicyclic biquadratic number fields with field index 1 is unbounded. They proved that there exist infinitely many totally complex bicyclic biquadratic number fields having field index 1 and minimal index equal to an arbitrarily fixed positive integer. Moreover, they achieved similar results for all the other possible values (2,3,4,6,12) of the field index.

NYUL submitted his habilitation thesis in 2019, and succesfully defended it in 2020.