22nd Czech and Slovak International Conference on Number Theory

Liptovský Ján, Slovakia

August 31 – September 4, 2015

22nd Czech and Slovak International Conference on Number Theory

Liptovský Ján, Slovakia

August 31 – September 4, 2015

Organized by

Mathematical Institute, Slovak Academy of Sciences

University of Ostrava

Scientific Committee

Karol Nemoga (Slovak Academy of Sciences)

Ladislav Mišík (University of Ostrava)

János Tóth (University J. Selye in Komárno)

Štefan Porubský (Academy of Sciences of the Czech Republic)

Radan Kučera (Masaryk University)

Organizing Committee

Ivana Geriaková (Slovak Academy of Sciences)

Zuzana Václavíková (University of Ostrava)

Jan Šustek (University of Ostrava)

Lukáš Novotný (University of Ostrava)

List of registered participants

Vladimír Baláž
Slovak University of Technology
Bratislava
Slovakia
vladimir.balaz@stuba.sk

Attila Bérczes
University of Debrecen
Debrecen
Hungary
berczesa@science.unideb.hu

Csanád Bertók
University of Debrecen, Institute of Mathematics
Debrecen
Hungary
bertok.csanad@science.unideb.hu

József Bukor
J. Selye University
Komárno
Slovakia
bukorj@ujs.sk

Michal Bulant
Masaryk university
Brno
Czech Republic
bulant@math.muni.cz

Peter Csiba
J. Selye University
Komárno
Slovakia
csibap@ujs.sk

Karl Dilcher
Dalhousie University
Halifax
Canada
dilcher@mathstat.dal.ca

Larry Ericksen
Millville
NJ, USA
LE22@cornell.edu

Judit Ferenczik
University of Debrecen
Debrecen
Hungary
jferenczik@gmail.com

Ferdinánd Filip
J. Selye University
Komárno
Slovakia
filipf@ujs.sk

István Gaál
University of Debrecen, Mathematical Institute
Debrecen
Hungary
gaal.istvan@unideb.hu

Marian Genčev
VŠB-TUO
Ostrava
Czech Republic
marian.gencev@vsb.cz

Kálmán Győry
University of Debrecen
Debrecen
Hungary
gyory@science.unideb.hu

Clemens Heuberger
Alpen - Adria - University of Klagenfurt
Klagenfurt
Austria
clemens.heuberger@aau.at

Stanislav Jakubec
Institute of Mathematics
Bratislava
Slovakia
jakubec@mat.savba.sk

Vítězslav Kala
University of Göttingen, Göttingen, Germany
Charles University, Prague, Czech Republic
vita.kala@gmail.com

Kamil Keprt
University of Ostrava
Ostrava
Czech Republic
kemil.keprt@seznam.cz

Katarína Korčeková
University of Ostrava
Ostrava
Czech Republic
quadratka@gmail.com

Juraj Kostra
University of Pardubice
Pardubice
Czech Republic
juraj.kostra@upce.cz

Piotr Krasoń
Szczecin University
Szczecin
Poland
krason@wmf.univ.szczecin.pl

Zuzana Krčmáriková
Czech Technical University
Praha
Czech Republic
zuzka.krcmarikova@gmail.com

Radan Kučera
Masaryk University
Brno
Czech Republic
kucera@math.muni.cz

Paolo Leonetti
Università Bocconi
Milano
Italy
leonetti.paolo@gmail.com

Stéphane Louboutin
IMM
Marseille
France
stephane.louboutin@univ-amu.fr

Diego Marques
University of Brasilia
Brasilia
Brazil
diego@mat.unb.br

Daniel C. Mayer
Austrian Science Fund
Graz
Austria
quantum.algebra@icloud.com

Ladislav Mišík
University of Ostrava
Ostrava
Czech Republic
ladislav.misik@osu.cz

Karol Nemoga
Institute of Mathematics
Bratislava
Slovakia
nemoga@mat.savba.sk

Lukáš Novotný
University of Ostrava
Ostrava
Czech Republic
lukas.novotny@osu.cz

Werner Georg Nowak
BOKU Wien
Vienna
Austria
nowak@boku.ac.at

Gábor Nyul
Institute of Mathematics, University of Debrecen
Debrecen
Hungary
gnyul@science.unideb.hu

Edita Pelantová
Czech Technical University
Prague
Czech Republic
edita.pelantova@fjfi.cvut.cz

Attila Pethő
University of Debrecen
Debrecen
Hungary
petho.attila@inf.unideb.hu

István Pink
University of Debrecen, Debrecen, Hungary
University of Salzburg, Salzburg, Austria
pinki@science.unideb.hu

Štefan Porubský
Institute of Computer Science
Prague
Czech Republic
sporubsky@hotmail.com

László Remete
University of Debrecen, Mathematical Institute
Debrecen
Hungary
remetel42@gmail.com

Andrzej Schinzel
IM PAN
Warszawa
Poland
schinzel@impan.pl

Lawrence Somer
Czech Academy of Sciences
Prague
Czech Republic
somer@cua.edu

Jörn Steuding
Department of Mathematics, Würzburg University
Würzburg
Germany
steuding@mathematik.uni-wuerzburg.de

Oto Strauch
Institute of Mathematics
Bratislava
Slovakia
oto.strauch@mat.savba.sk

Jan Šustek
University of Ostrava
Ostrava
Czech Republic
jan.sustek@osu.cz

Tímea Szabó
University of Debrecen
Debrecen
Hungary
szabo.timea@science.unideb.hu

Márton Szikszai
University of Debrecen
Debrecen
Hungary
szikszai.marton@science.unideb.hu

Yohei Tachiya
Hirosaki University
Hirosaki
Japan
tachiya@hirosaki-u.ac.jp

Szabolcs Tengely
University of Debrecen
Debrecen
Hungary
tengely@science.unideb.hu

János Tóth
J. Selye University
Komárno
Slovakia
tothj@ujs.sk

Salvatore Tringali
Texas A&M University
Doha
Qatar
salvo.tringali@gmail.com

Pavel Trojovský
University of Hradec Králové
Hradec Králové
Czech Republic
pavel.trojovsky@uhk.cz

Maciej Ulas
Jagiellonian University
Kraków
Poland
maciej.ulas@gmail.com

Abstracts of talks

Extremes of $\int_0^1 \int_0^1 F(x, y)\, d_x d_y g(x, y)$

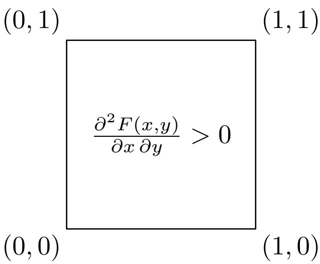
Vladimír Baláž

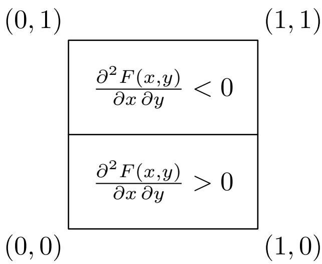
(joint work with M.R. Iacó, O. Strauch, R.F. Tichy, S. Thonhauser)

In uniform distribution theory the problem of optimizing the integral

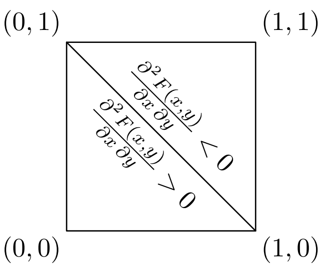
$$\int_0^1 \int_0^1 F(x,y)\, \mathrm{d}_x \mathrm{d}_y g(x,y) \tag{1}$$

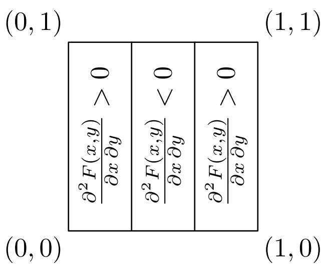
over copulas $g(x,y)$ is motivated by computing optimal limit points of the sequence $\frac{1}{N}\sum_{n=1}^{N} F(x_n, y_n)$, $N = 1, 2, \dots$ over uniform distribution sequences x_n and y_n, $n = 1, 2, \dots$. But problem of optimizing (1) is previously well-known as mass transportation problems. It turns out that the solution of the problem depends on sign of partial derivatives $\frac{\partial^2 F(x,y)}{\partial x\, \partial y}$. We have known a solution for the following Fig. 1 and a criterion for Fig. 2.





In this paper we solve maximum of (1) in a special Fig. 3 and a criterion for maximum in Fig. 4.





Effective results for division points on curves in $\mathbb{G}_m^2$

Attila Bérczes

Let $A := \mathbb{Z}[z_1, \ldots, z_r]$ be a finitely generated domain over $\mathbb{Z}$, and let K denote its quotient field, and denote by K^* the multiplicative group of non-zero elements of K. Let Γ be a finitely generated subgroup of K^*, and let $\overline{\Gamma}$ denote the division group of Γ. Let $F(X, Y) \in A[X, Y]$ be a polynomial. In 1960 S. Lang proved that the equation

$$F(x, y) = 0 \quad \text{in } x, y \in \Gamma \tag{1}$$

has only finitely many solutions, provided F is not divisible by any polynomial of the form

$$X^m Y^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n \tag{2}$$

for any non-negative integers m, n, not both zero, and any $\alpha \in \overline{K}^*$. The conditions imposed in Lang's theorem, i.e., that Γ be finitely generated and F not be divisible by any polynomial of type (2), are essentially necessary. Lang's proof of this result is ineffective. Lang also conjectured that the above equations has finitely many solutions in $x, y \in \overline{\Gamma}$ under the same condition (2). In 1974 Liardet proved this conjecture of Lang, however, the proof of Liardet is also ineffective.

An effective version of Liardet's Theorem in the number filed case is due to Bérczes, Evertse, Győry and Pontreau (2009), however, in the general case no effective result has been proved.

In the talk an effective version of the result of Liardet will be presented in the most general case. Our result is not only effective, but also quantitative in the sense that an upper bound for the size of the solutions $x, y \in \overline{\Gamma}$ is provided. This result implies that the solutions of the equation under investigation can be determined in principle.

In the proofs we combine effective finiteness results for these types of equations over number fields and over function fields, along with a specialization method developed by Győry in the 1980's and refined recently by Evertse and Győry.

On the equation $U_n = 2^a + 3^b + 5^c$

Csanád Bertók

(joint work with István Pink, Lajos Hajdu and Zsolt Rábai)

In the talk, first we propose a conjecture, similar to Skolem's conjecture, on a Hasse-type principle for exponential Diophantine equations. Namely, consider the equation

$$a_1 b_{11}^{\alpha_{11}} \cdots b_{1l}^{\alpha_{1l}} + \ldots + a_k b_{k1}^{\alpha_{k1}} \cdots b_{kl}^{\alpha_{kl}} = c$$

in non-negative integers $\alpha_{11}, \ldots, \alpha_{1l}, \ldots, \alpha_{k1}, \ldots, \alpha_{kl}$, where a_i, b_{ij}, are non-zero integers for every $i = 1, \ldots, k$ and $j = 1, \ldots, l$, and c is an integer. Our conjecture is that if the equation above has no solutions, then there exists an integer $m \geq 2$ such that the congruence

$$a_1 b_{11}^{\alpha_{11}} \cdots b_{1l}^{\alpha_{1l}} + \ldots + a_k b_{k1}^{\alpha_{k1}} \cdots b_{kl}^{\alpha_{kl}} \equiv c \pmod{m}$$

has no solutions in non-negative integers α_{ij}, $i = 1, \ldots, k$, $j = 1, \ldots, l$.

In the talk we present a result showing that in a sense, the conjecture is valid for "almost all" equations. Further, based upon the conjecture we propose a general method for the solution of exponential Diophantine equations, relying on a generalization of a result of Erdős, Pomerance and Schmutz concerning Carmichael's λ function.

Finally, we illustrate that our method works not only in $\mathbb{Z}$, but also in the ring of integers of $\mathbb{Q}(\alpha)$ (where α is a real algebraic number) by generalizing a result of D. Marques and A. Togbé and solving a problem of F. Luca and S. G. Sanchez. Let $U_n = A \cdot U_{n-1} + B \cdot U_{n-2}$ $(n \geq 2)$ with $A, B \in \mathbb{Z}$ and initial terms $U_0, U_1 \in \mathbb{Z}$ be a binary sequence. If a, b, c are non-negative integers, then we give all solutions of the equations

$$U_n = 2^a + 3^b,$$
$$U_n = 2^a + 3^b + 5^c,$$

in the case when $(A, B, U_0, U_1) = (1, 1, 0, 1)$, $(1, 1, 2, 1)$, $(2, 1, 0, 1)$, $(2, 1, 2, 2)$.

Statistical limit points and Baire category of sequences

József Bukor and János T. Tóth

The number λ is a statistical limit point of the sequence (x_n), if λ is the limit of a subsequence (x_{k_n}) such that the set of indices k_n has a positive upper asymptotic density.

Let $\mathbf{s}$ denote the Fréchet metric space of all real sequences. Denote by $\mathbf{s_0}$ the set of all real sequences, which statistical limit points is not equal to the set of all real numbers.

The main result of the talk is that $\mathbf{s_0}$ is a set of the first Baire category in the space $\mathbf{s}$.

Continued fractions and Stern polynomials

Karl Dilcher

(joint work with Larry Ericksen)

By using specific subsequences of two different types of generalized Stern polynomials, we obtain several related classes of finite and infinite continued fractions involving z^{t^j} in their partial numerators, where z is a complex variable and $t \geq 2$ an integer. The talk concludes with some additional related results.

Hyperbinary expansions and Stern polynomials

Larry Ericksen

(joint work with Karl Dilcher)

Two different types of generalized Stern polynomials $a_t(n;z)$ are obtained using recursions and generating functions. These polynomials in variable z reduce to the well-known Stern (diatomic) sequence $a(n)$ when $z=1$. A hyperbinary expansions of an integer n is an expansion of n as a sum of powers of 2, each power being used at most twice. Integers $a(n+1)$ in the Stern sequence count the number of hyperbinary expansions of n. In this talk, we derive the actual set of all hyperbinary expansions of n.

Properties of the Stern polynomials associated with these hyperbinary expansions are presented. The structures of certain Stern polynomials are given in terms of Jacobi polynomials. The talk concludes with an introductory analysis of the Stern polynomials being represented by continued fractions.

Equal values of Combinatorial numbers

Judit Ferenczik

(joint work with Ákos Pintér)

Let S_k^n be the Stirling number of the second kind with positive integer parameters n and k, i. e. S_k^n is the number of partition of n elements into k non-empty sets. We formulate the following conjecture concerning common values of Stirling numbers.

Conjecture. *Let $1<a<b$ fixed integers. Then all the solutions of equation $S_a^x = S_b^y$ with $x>a, y>b$ are $S_5^6 = S_2^5 = 15$ and $S_{90}^{91} = S_2^{15} = 4095$.*

We prove the conjecture for $\max(a,b) < 300$, extending our earlier result. The proof is based on Baker-method, elementary estimations and grid computational technique.

The structure of weighted densities

Ferdinánd Filip, Peter Csiba and János T. Tóth

Density is one of the possibilities to measure how large a subset of the set of positive integers is. The best known type of densities are weighted densities.

Let $f : \mathbb{N} \to (0, \infty)$ be a weight function such that the conditions

$$\sum_{n=1}^{\infty} f(n) = \infty$$

$$\lim_{n\to\infty} \frac{f(n)}{\sum_{i=1}^{n} f(i)} = 0$$

are satisfied.

For $A \subset \mathbb{N}$ function χ_A denote the characteristic function of the set A.

Define

$$\underline{d}_f(A) = \liminf_{n\to\infty} \frac{\sum\limits_{i=1}^{n} f(i)\chi_A(i)}{\sum\limits_{i=1}^{n} f(i)}, \quad \overline{d}_f(A) = \limsup_{n\to\infty} \frac{\sum\limits_{i=1}^{n} f(i)\chi_A(i)}{\sum\limits_{i=1}^{n} f(i)}$$

as the lower and upper f-densities of A. In the case when $\underline{d}_f(A) = \overline{d}_f(A)$ we say that A has f-density $d_f(A)$. The famous f-densities are the asymptotic and logarithmic density.

We present relations between weighted densities determined by several weight functions.

Solving Thue equations

István Gaál

Let $F(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree ≥ 3, irreducible over $\mathbb{Q}$, and let $0 \neq m \in \mathbb{Z}$. The Thue equation

$$F(x,y) = m \text{ in } x,y \in \mathbb{Z}$$

plays an important role in the theory and applications of Diophantine equations. The first general finiteness results on the number of solutions, the first applications of Baker's method, the first reduction algorithm etc. were all connected with Thue equations and were later successfully applied to other important classes of Diophantine equations.

In our talk we give a brief survey of these results and explain a new efficient algorithm to calculate "small" solutions of relative Thue equations. This method had already applications in describing generators of power integral bases in certain algebraic number fields.

A class of restricted sum formulas for the multiple Riemann $\zeta^\star$-values

Marian Genčev

In our contribution, we present a result that clarifies the evaluation of the so-called restricted sum formulas for the multiple $\zeta^\star$-values with general even arguments, i.e.,

$$\sum_{\substack{\sum_{j=1}^{K} c_j = c \\ c_j \in \mathbb{N}}} \zeta^\star(2sc_1, \ldots, 2sc_K), \tag{1}$$

where c, s, K are arbitrary positive integers with $c \geq K$, and

$$\zeta^\star(s_1, \dots, s_K) := \sum_{n_1 \geq n_2 \geq \dots \geq n_K \geq 1} \prod_{j=1}^{K} \frac{1}{n_j^{s_j}}$$

is the multiple Riemann $\zeta^\star$-function. This function is a naturally generalization of the usually Riemann ζ-function (it suffices to put $K = 1$ in the definition of $\zeta^\star(s_1, \dots, s_K)$). Our evaluation formulas for the restricted sums (1) involve only finite number of elementary terms like Bernoulli numbers, multinomial coefficients and the values of the cosine function.

Effective results for Diophantine equations over finitely generated domains

Kálmán Győry

(joint work with Jan-Hendrik Evertse and Attila Bérczes)

We present some recent effective finiteness results on unit equations, Thue equations, hyper- and superelliptic equations and discriminant equations.

Non-Adjacent Digit Expansions

Clemens Heuberger

Motivated by applications in cryptography, we consider redundant digit expansions to various bases. The redundancy allows to decrease the weight, i.e., the number of non-zero digits, and therefore the execution time for scalar multiplication algorithms in abelian groups such as the point group of an elliptic curve.

We discuss the questions of existence and optimality and analyse the expected weight.

Universal quadratic forms over number fields

Vítězslav Kala

A universal form is a positive definite quadratic form with integral coefficients which represents all positive numbers – a classical example over the integers is the sum of four squares $x^2 + y^2 + z^2 + w^2$. I shall discuss some recent results (joint with Valentin Blomer) concerning the number of variables required by a universal form over a real quadratic field. In particular, for a given positive integer n, one can use continued fractions to construct infinitely many such fields which admit no n-ary universal forms.

Arithmetic of Bethe Ansatz and Gaussian polynomials

Piotr Krasoń

(joint work with Jan Milewski)

We prove a congruence relation for the sums of coefficients of Gaussian polynomials. This calculation is in fact inspired by the famous model in physics of Bethe Ansatz and yields the number of elements in moduli classes of certain fibers of a natural fibration associated with this model. We show that, suitably interpreted, our calculation of number of elements in moduli classes of sums of restricted partitions is in fact equivalent to finding the number of elements in these special fibers. The calculation is done for prime numbers. We also give some generalizations of our main result

Finite beta-expansions with negative bases

Zuzana Krčmáriková

We consider positional numeration system with negative base $(-\beta)$ introduced by Ito and Sadahiro. We focus on aritmetical properties of such systems when β is a cubic Pisot unit. That means $\beta > 1$ is a root of polynomial

$$p(x) = x^3 - ax^2 - bx \pm 1,$$

where $|b-1| < a \pm 1$ and $(1-b) < \pm(1 \pm a)$. For these bases, we investigate when the set $\mathrm{Fin}(-\beta)$ of numbers with finite $(-\beta)$-expansion forms a ring. Moreover, we show that when the expansion of $-\frac{\beta}{\beta+1}$ is finite, then $\mathrm{Fin}(-\beta)$ is not a ring.

On a theorem of Thaine

Radan Kučera

Let K be a real abelian number field, $G = \mathrm{Gal}(K/\mathbb{Q})$ its Galois group, and p be a prime number. Let E be the group of units of the ring of integers of K and let C be the Sinnott group of circular units of K. Let $\mathrm{Cl}(K)$ be the ideal class group of K and let $(E/C)_p$ and $\mathrm{Cl}(K)_p$ be the p-Sylow subgroups of the corresponding $\mathbb{Z}[G]$-modules.

In 1988, Francisco Thaine proved that if $p \nmid [K : \mathbb{Q}]$ then

$$\mathrm{Ann}_{\mathbb{Z}[G]}((E/C)_p) \subseteq 2 \cdot \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Cl}(K)_p).$$

The aim of this talk is to describe a stronger variant of this theorem which can be proven by a modification of Thaine's method.

Upper and lower densities – Part II

Paolo Leonetti

An upper density (on $\mathbb{Z}$) is a real-valued set function $\mu^\star$ on the power set of $\mathbb{Z}$ that is monotonic, subadditive, (-1)-homogeneous, and translational invariant, and for which $\mu^\star(\mathbb{Z}) = 1$. In this talk, we will prove that the image of the density induced by an upper density is the whole interval $[0, 1]$, study if specific sets X of integers are *meager*, namely $\mu^\star(X) = 0$ for every upper density $\mu^\star$, and discuss various "structural properties" of upper and lower densities. If time permits, we will also present a list of open questions.

Explicit upper bounds for residues of Dedekind zeta functions

Stéphane Louboutin

Explicit bounds on the residues at $s = 1$ of the Dedekind zeta-functions of number fields (in terms of their degree and of the logarithm of the absolute value of their discriminant) have long been known. They date back to C. L. Siegel and E. Landau. The author gave a neat explicit bound in 2000, the best known bound until recently. In 2012 X. Li improved upon this bound. His results, although effective, were not explicit. Wee make one of his two bounds explicit and determine when it is the best known one.

On the Arithmetic Behavior of Transcendental Functions

Diego Marques

The study of the arithmetic behavior of transcendental functions at complex points has attracted the attention of many mathematicians for decades. The first result concerning this subject goes back to 1884, when Lindemann proved that the transcendental function e^z assumes transcendental values at all nonzero algebraic point. In 1886, Strauss tried to prove that an analytic transcendental function cannot be rational at all rational points in its domain. However, in 1886, Weierstrass supplied him with a counter-example and also stated (without proof) that there are transcendental entire functions which assume algebraic values at all algebraic points. This assertion was proved in 1895 by Stäckel who established a much more general result. Subsequent advances were made by Stäckel, Faber, Mahler, Van der Poorten, etc. In particular, Mahler (in his 1976 book and in a 1984 paper) raised some questions about this subject.

In this talk, we shall provide a brief overview of the classical results in this field as well as our advances related to these Mahler's questions (in particular, the solution for two of them). This is related to joint works with Moreira, Ramirez and Schleischitz.

New number fields with known p-class tower

Daniel C. Mayer

Denote by p a prime, by K a number field with p-class group $\mathrm{Cl}_p(K) \simeq (p, p)$, by $L_1, \ldots, L_{p+1}$ the unramified cyclic extensions of degree p of K, by $\varkappa(K)$ the p-capitulation type of K in $L_1, \ldots, L_{p+1}$, and by $\ell_p(K)$, resp. $G = \mathrm{Gal}(\mathrm{F}_p^\infty(K)|K)$, the length, resp. the group, of the p-class tower of K.

In the first two theorems, let $p = 3$, and let $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, be a real quadratic field.

Theorem 1. (Mayer) Suppose that $\mathrm{Cl}_3(L_1) \simeq (27, 9)$, and $\mathrm{Cl}_3(L_j) \simeq (9, 3)$ for $2 \le j \le 4$. Assume that $\varkappa(K)$ neither contains a total capitulation nor a 2-cycle. If there exists an unramified cyclic cubic extension M of some L_j, $2 \le j \le 4$, with $\mathrm{Cl}_3(M) \simeq (27, 3)$, resp. $\mathrm{Cl}_3(M) \simeq (9, 3)$, then $\ell_3(K) = 3$, $G \simeq \langle 729, 54\rangle - \#2; 2|4|6$ (e.g. $d = 342\,664$), resp. $\ell_3(K) = 2$, $G \simeq \langle 2\,187, 302|304|306\rangle$ (e.g. $d = 4\,760\,877$).

Theorem 2. (Mayer) Suppose that $\mathrm{Cl}_3(L_j) \simeq (3, 3, 3)$ for $1 \le j \le 3$, and $\mathrm{Cl}_3(L_4) \simeq (9, 3)$. Let $\tau^{(1)}(L_j) = [\tau_0(L_j); \tau_1(L_j)]$ be the IPAD (index-p abelianization data) of L_j for $1 \le j \le 4$. (See [1].)

If $\tau^{(1)}(L_1) = [1^3; (21^2, (1^3)^3, (1^2)^9)]$, $\tau^{(1)}(L_2) = [1^3; (21^2, (21)^{12})]$, $\tau^{(1)}(L_3) = [1^3; ((21^2)^4, (2^2)^9)]$, and $\tau^{(1)}(L_4) = [21; (21^2, (21)^3)]$, then $G \simeq \langle 2\,187, 273\rangle$ (e.g. $d = 957\,013$).

If $\tau^{(1)}(L_1) = [1^3; (21^2, (1^3)^3, (1^2)^9)]$, $\tau^{(1)}(L_j) = [1^3; (21^2, (21)^{12})]$ for $2 \le j \le 3$, and $\tau^{(1)}(L_4) = [21; (21^2, (31)^3)]$, then $G \simeq \langle 2\,187, 271|272\rangle$ (e.g. $d = 2\,023\,845$).

If $\tau^{(1)}(L_1) = [1^3; ((21^2)^4, (1^2)^9)]$, $\tau^{(1)}(L_j) = [1^3; (21^2, (21)^{12})]$ for $2 \le j \le 3$, and $\tau^{(1)}(L_4) = [21; (21^2, (21)^3)]$, then $G \simeq \langle 2\,187, 270\rangle$ (e.g. $d = 2\,303\,112$). In each of the three cases, $\ell_3(K) = 3$.

In the next two theorems, let $p = 5$.

Theorem 3. (Kishi, Mayer) Let $K = \mathbb{Q}((\zeta - \zeta^{-1})\sqrt{d})$ be a cyclic quartic field with $\zeta = \exp(\frac{1}{5} 2\pi i)$ and $d > 0$, $\gcd(d, 5) = 1$. If $\varkappa(K)$ is a 4-cycle (e.g. $d = 457$), resp. the identity permutation (e.g. $d = 581$), then $\ell_5(K) = 2$, and $G \simeq \langle 3\,125, 11\rangle$, resp. $G \simeq \langle 3\,125, 14\rangle$.

Theorem 4. (Ayadi, Oumazouz, Mayer) Let K be a cyclic quintic field with conductor f divisible by two primes p, q which are mutual quintic residues, and let γ be generator of a non-trivial primitive ambiguous principal ideal of K with norm $N_{K|\mathbb{Q}}(\gamma) = p^e q^u$. If $e = 0$ or $u = 0$, then $\ell_5(K) = 2$ (e.g. $f = 5\,921 = 31 \cdot 191$).

Reference. [1] D. C. Mayer, *Index-p abelianization data of p-class tower groups*, Adv. Pure Math. **5** (2015), no. 5, 286–313, DOI 10.4236/apm.2015.55029, Special Issue on Number Theory and Cryptography, April 2015.

Bounds for exponential sums combining Van der Corput's and Huxley's method

Werner Georg Nowak

The classic Van der Corput's method to estimate exponential sums consists of combining Poisson's formula followed by the asymptotic evaluation of exponential integrals ("A-step"), and a skillful application of Cauchy's inequality ("B-step"). In its simplest form it tells us what follows: Let be given throughout two real parameters $M \geq 1$ and $T > 0$ with $|\log T| \asymp \log M$, and a real function F on an interval I of length M, satisfying

$$F^{(j)} \asymp M^{-j} T \,, \tag{1}$$

with $j = 2$. Then it follows that, for any interval $I^* \subseteq I$,

$$E_{F,I^*} := \sum_{n \in I^*} e^{2\pi i F(n)} \ll T^{1/2} + M T^{-1/2} \,.$$

Applying *Van der Corput's differencing lemma* (also known as Weyl's B-step), it follows that (1) holding true for $j = 3$ implies that

$$E_{F,I^*} \ll M^{1/2} T^{1/6} + M T^{-1/6} \,.$$

Of course, the application of the B-step can be iterated.

More recently, M. Huxley and others developed an entirely new approach called the *Discrete Hardy-Littlewood method.* For the single exponential sum, its sharpest result says that

$$E_{F,I^*} \ll M^{1/2} T^{32/205+\epsilon} \,,$$

provided that (1) is true for $j = 2, 3, 4$ - however, under the restriction that the parameters satisfy

$$T^{141/328+\epsilon} \ll M \ll T^{181/328} \,. \tag{2}$$

In this talk it is described how both types of results can be combined to obtain sharp bounds for the single exponential sum. Under the conditions just stated, apart from (2), it can be proved that

$$M^{-\epsilon} E_{F,I^*} \ll M^{\frac{1}{2}}\, T^{\frac{32}{205}} + T^{\frac{751}{1968}} + M^{\frac{871}{1086}} + M\, T^{-1/2} \,.$$

Applying the differencing lemma once, one obtains

$$M^{-\epsilon} E_{F,I^*} \ll M^{\frac{679}{948}}\, T^{\frac{16}{237}} + M^{\frac{1}{2}}\, T^{\frac{751}{5438}} + M^{\frac{1957}{2172}} + M\, T^{-1/4}\,,$$

under the condition that (1) is true for $j = 3, 4, 5$. Again, the B-step can be iterated.

Finally, we mention a few applications; see also [3].

References

[1] W.G. Nowak, Higher order derivative tests for exponential sums incorporating the Discrete Hardy-Littlewood method. Acta Math. Hungarica **134**/1 (2012), 12-28.

[2] W.G. Nowak, Higher order derivative tests for exponential sums incorporating the Discrete Hardy-Littlewood method, II. In preparation.

[3] W.G. Nowak, A problem considered by Friedlander and Iwaniec and the Discrete Hardy-Littlewood method. Math. Slovaca, to appear.

A Ramsey type problem for linear recurrence sequences

Gábor Nyul

(joint work with Bettina Rauf and Csanád Bertók)

A well-known Ramsey type theorem of van der Waerden states that for any positive integers k and r, if we colour the positive integers with r colours, then there exists a strictly increasing monochromatic arithmetic progression of length k. In our talk, we investigate the similar problem for linear recurrence sequences.

H. Harborth and S. Maasberg studied this problem for sequences satisfying the Fibonacci recurrence. We extend their results for higher order linear recurrence sequences with positive integer coefficients, and we also study binary linear recurrences having coefficients of both signs.

Non-standard numeration systems: the algorithmic point of view

Edita Pelantová

We study algorithms for addition, multiplication and division on the set of numbers having finite representation in a positional numeration system defined by a base β in $\mathbb{C}$ and a finite digit set $\mathcal{A}$ of contiguous integers containing 0. For a fixed base β, we discuss the question of the alphabet allowing to perform addition in constant time independently of the length of representation of the summands. Such addition is a necessarry ingredient in on-line algorithms for multiplication and division. We focus on the properties of algebraic bases β which influence the efectivity of these on-line algorithms. Using the base $\beta = \frac{3+\sqrt{5}}{2}$ and the alphabet $\{-1, 0, 1\}$ we demonstrate that a system with an irrational base can be more suitable for computation than a system with an integer base.

On a clustering of the integers

Attila Pethő

Our talk is based on joint works with S. Akiyama (Tsukuba University, Japan) and L. Aszalós, and L. Hajdu (University of Debrecen).

Let A be a finite non-empty set, and let $\sim$ be a symmetric binary relation on A. Consider a partition P of A. Two distinct elements $a, b \in A$ are said to be in conflict with respect to the partition P either if they belong to the same class of P, but $a \nsim b$, or they belong to different classes of P, although $a \sim b$. The goal of correlation clustering is to find a partition with minimal number of conflicts.

First we show some general, density results. Next we concentrate on the case when A is the set of positive integers as well as the set of

S-integers with a finite set of primes, which are equipped with the coprimality relation. It turns out that the largest class of the correlation clustering behaves completely differently.

On the equation $1^k + 2^k + \ldots + x^k = y^n$ for fixed x

István Pink

We provide all solutions of the title equation in positive integers x,k,y,n with $1 \leq x < 25$ and $n \geq 3$. For these values of the parameters, our result gives an affirmative answer to a related, classical conjecture of Schäffer. In our proofs we combine several tools: Baker's method (in particular, sharp bounds for the linear combinations of logarithms of two algebraic numbers), polynomial-exponential congruences and computational methods.

Idempotents and number theory

Štefan Porubský

Idempotents (elements satisfying the identity $e \cdot e = e$) represent an important structural element in semigroups (algebraic structure endowed with an associative binary operation). Existence of idempotents is actually equivalent with the existence of subgroups in a given semigroup. More precisely, every identity elements of a subgroup is an idempotent, and conversely around every idempotents these lives at least one sub(semi)group of the given semigroup (e.g. the cyclic (semi)group generated by an element a power of which is the given idempotent). Though the complex of such subgroups and subsemigroups could be rich and mirrors arithmetic properties of connected algebraic structures, their role was studied very sporadically hitherto. For instance, in the semigroup of residue classes modulo n we have 2^r distinct idempotents and connected complexes of subgroups and subsemigroups, where

r is the number of distinct prime divisors of n. Besides the well-known group of the reduced residue classes connected with idempotent 1 and the semigroup of nilpotent residue classes around 0, there are additional ones provided $r > 1$. A typical demonstration example of their presence is the analysis of the classical Euler-Fermat theorem, Bauer identical congruence or Wilson Theorem given by Štefan Schwarz and enabling him to deduce many variants of these important elementary results in multiplicative semigroups of various matrix structures, of power sets of a finite set or of binary relations on a finite set. His approach is capable of a wide generalization giving a way to extend these results to more general commutative rings appearing in number theory as it was done by the author of this talk and M. Laššák. In this survey talk we show some of these applications as well some new ones, e.g. in a solution of a simple linear congruence $ax \equiv b \pmod{n}$.

Power integral bases in pure quartic number fields

László Remete

A number field K of degree n is *monogene* if there exist an integer $\vartheta \in K$ such that $\mathbb{Z}_K = \mathbb{Z}[\vartheta]$, that is $\{1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}\}$ is an integral basis (so called *power integral basis*) in K.

We consider the problem of monogenity and generators of power integral bases in pure quartic fields $K = \mathbb{Q}(\sqrt[4]{m})$ where m is a square free integer with $m \equiv 2, 3 \pmod{4}$. Set $\alpha = \sqrt[4]{m}$. For $1 < m < 10^7$ we determine all generators

$$\vartheta = a + x\alpha + y\alpha^2 + z\alpha^3$$

of power integral bases of K where $a, x, y, z \in \mathbb{Z}$ with

$$\max(|x|, |y|, |z|) < 10^{1000}.$$

This extensive computation was performed on a supercomputer.

We extended these results also to the relative case. Let d be one of $d = 3, 7, 11, 19, 43, 67, 163$, let $L = \mathbb{Q}(i\sqrt{d})$. Let $m \equiv 2, 3 \pmod{4}$, assume $(d, m) = 1$ and set $\alpha = \sqrt[4]{m}$. For $1 < m \leq 5000$ we calculate all generators $\vartheta = A + X\alpha + Y\alpha^2 + Z\alpha^3$ of *relative power integral bases* of K over L with $A, X, Y, Z \in \mathbb{Z}_L$ with $\max(\overline{|X|}, \overline{|Y|}, \overline{|Z|}) < 10^{500}$. We also proved that these octic fields K does not admit any generators of (absolute) power integral bases of the form

$$\vartheta = A + \varepsilon(X\alpha + Y\alpha^2 + Z\alpha^3)$$

where $A, X, Y, Z \in \mathbb{Z}_L$, ε a unit in L and

$$\max(\overline{|X|}, \overline{|Y|}, \overline{|Z|}) < 10^{500}.$$

On simple linear recurrences

Andrzej Schinzel

Let K be a number field and u_n a simple linear recurrence of order k defined over K. We shall consider for $k = 2, 3, 4$ the following problem: if for almost all prime ideals p of K there are elements u_n divisible by p, does it follow that $u_n = 0$ for a certain integer n?

Identically Distributed Second-Order Linear Recurrences Modulo p

Lawrence Somer

Let $w(a, -1)$ denote the second-order linear recurrence satisfying the recursion relation

$$w_{n+2} = aw_{n+1} - w_n\ ,$$

where a and the initial terms w_0, w_1 are all integers. Let p be an odd prime. The restricted period $h_w(p)$ of $w(a, -1)$ modulo p is the least positive integer r such that $w_{n+r} \equiv Mw_n \pmod{p}$ for all $n \geq 0$ and some nonzero residue M modulo p. We distinguish two recurrences, the

Lucas sequence of the first kind $u(a, -1)$ and the Lucas sequence of the second kind $v(a, -1)$, satisfying the above recursion relation and having initial terms $u_0 = 0$, $u_1 = 1$ and $v_0 = 2$, $v_1 = a$, respectively. We show that if $u(a_1, -1)$ and $u(a_2, -1)$ both have the same restricted period modulo p, or equivalently, the same period modulo p, then $u(a_1, -1)$ and $u(a_2, -1)$ both have the same distribution of residues modulo p. Similar results are obtained for Lucas sequences of the second kind.

Uniform Distribution and the Riemann Zeta-Function

Joern Steuding

Recent applications of uniform distribution theory to the Riemann zeta-function provide new insights in the analytic behaviour inside the critical strip. It has been shown that, for every fixed complex number a, the imaginary parts of the solutions to the equation $\zeta(s) = a$ (in ascending order) are uniformly distributed modulo one. Furthermore, it has been proved that the argument of $\zeta(1/2+it)$ for t from an arithmetic progression is uniformly distributed modulo π if there are not too many ordinates of zeta zeros in this arithmetic progression.

(Some of the results are joint work with Dr. Selin Selen Özbek from Antalya.)

Distribution functions of sequences

Oto Strauch

In this lecture we present three applications of distribution functions of sequences.

1. The sequence $\boldsymbol{\xi(3/2)^n}$ mod 1. Every distribution function $g(x)$ of $\xi(3/2)^n$ mod 1 satisfies

$$\begin{aligned} & g\Big(\frac{x}{2}\Big) + g\Big(\frac{x+1}{2}\Big) - g\Big(\frac{1}{2}\Big) \\ & \qquad = g\Big(\frac{x}{3}\Big) + g\Big(\frac{x+1}{3}\Big) + g\Big(\frac{x+2}{3}\Big) - g\Big(\frac{1}{3}\Big) - g\Big(\frac{2}{3}\Big), \qquad (1) \end{aligned}$$

for $x \in [0,1]$. The following solution $g(x)$ of (1)

$$g(x) = \begin{cases} 0 & \text{for } x \in [0, 1/6], \\ 2x - 1/3 & \text{for } x \in [1/6, 3/12], \\ 4x - 5/6 & \text{for } x \in [3/12, 5/18], \\ 2x - 5/18 & \text{for } x \in [5/18, 2/6], \\ 7/18 & \text{for } x \in [2/6, 8/18], \\ x - 1/18 & \text{for } x \in [8/18, 3/6], \\ 8/18 & \text{for } x \in [3/6, 7/9], \\ 2x - 20/18 & \text{for } x \in [7/9, 5/6], \\ 4x - 50/18 & \text{for } x \in [5/6, 11/12], \\ 2x - 17/18 & \text{for } x \in [11/12, 17/18], \\ x & \text{for } x \in [17/18, 1] \end{cases}$$

satisfies Mahler's conjecture in the following sense: K. Mahler (1968) conjectured that there exists no $\xi \in \mathbb{R}^+$ such that $0 \le \{\xi(3/2)^n\} < 1/2$ for every $n = 0, 1, 2, \ldots$ Mahler's conjecture follows from the conjecture: Let $g(x)$ be a distribution function satisfying (1). Then $g(x)$ is different of $g(x) = 1$ for $x \in (1/2, 1)$.

2. The first digit problem. Let $\lim_{i\to\infty}\{\log_q(N_i)\} = w$, then for integer sequence $n = 1, 2, \ldots$ we have

$$\begin{aligned} & \lim_{i\to\infty} \frac{\#\{n \le N_i\,;\ \text{first } s \text{ digits of } n \text{ are } k_1k_2\ldots k_s\}}{N_i} \\ & \qquad = g_w\big(\log_q k_1.k_2k_3\ldots(k_s+1)\big) - g_w\big(\log_q k_1.k_2k_3\ldots k_s\big) \end{aligned}$$

where

$$g_w(x) = \frac{1}{q^w}\frac{q^x - 1}{q - 1} + \frac{q^{\min(x,w)} - 1}{q^w}$$

is a distribution function of the sequence $\log_q n$ mod 1.

3. Four-dimensional Copula. Applying Weyl's limit relation we have

$$\begin{aligned}
&\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}F\big(\gamma_q(n),\gamma_q(n+1),\gamma_q(n+2),\gamma_q(n+3)\big)\\
&=\int_0^1\int_0^1\int_0^1\int_0^1 F(x,y,z,u)\,\mathrm{d}_x\mathrm{d}_y\mathrm{d}_z\mathrm{d}_u g(x,y,z,u)\\
&=\frac{1}{2}+\frac{3}{q}-\frac{6}{q^2},
\end{aligned}\tag{2}$$

where

- $\gamma_q(n)$ is the van der Corput sequence in base q,
- $g(x,y,z,u)$ is an asymptotic distribution function of

$$\big(\gamma_q(n),\gamma_q(n+1),\gamma_q(n+2),\gamma_q(n+3)\big),$$

- and $F(x,y,z,u)=\max(x,y,z,u)$.

Here the distribution function $g(x,y,z,u)$ is a new copula.

Comments. Result 1. is one of the first nontrivial applications of the distribution function theory. Result 2. is a unique solution of a problem that the sequence $n=1,2,3,\dots$ does not satisfy Benford's law. In Result 3. a referee described a general method for computing integral of the type (2), but 1. and 2. are given a basis for individual study of $g(x,y,z,u)$.

Power integral bases in quartic fields and quartic extensions

Tímea Szabó

The existence of power integral bases is a classical topic in algebraic number theory. It is well known that if a number field admits a power integral basis of type $(1,\theta,\dots,\theta^{n-1})$ then up to equivalence it admits only finitely many of them. There is an extensive literature of calculating power integral bases in special algebraic number fields. This problem is equivalent to solving diophantine equations, so called index form equations There are efficient algorithms for calculating power integral bases in lower degree (≤ 6) and in special higher degree $(6, 8, 9)$ number fields. The problem of power integral bases was also considered in relative extensions. Algorithms for calculating relative power integral bases were given in relative cubic and in relative quartic extensions. It is an especially delicate problem if we solve the index form equation not only in a specific number field but in an infinite parametric family of number fields, where the index form equation is given in a parametric form. Such results are known in certain parametric families of cubic, quartic and quintic number fields. Similar results for calculating relative power integral bases in infinite parametric families of relative extensions were not known before.

In this talk we present the resolution of the index form equations in two families of totally complex biquadratic fields depending on two parameters and prove that up to equivalence, they admit only one generator of power integral bases. Note that these are the first families of number fields with two parameters where all generators of power integral bases determined.

In the second half of my talk considering infinite parametric families of octic fields, that are quartic extensions of quadratic fields, we describe all relative power integral bases of the octic fields over the quadratic subfields and then we check if there exist corresponding generators of absolute power integral bases.

Perfect powers in products of terms of an EDS

Márton Szikszai

Let $B = (B_n)_{n=0}^{\infty}$ be an elliptic divisibility sequence and consider the diophantine equation

$$B_n B_{n+d} \dots B_{n+(k-1)d} = y^l$$

in variables n, d, k, y, l. In this talk we will discuss the solution of the above equation. Further, the working of our method will be presented through several concrete examples. Several comments on the efficient computation will also be given.

Linear independence results for the reciprocal sums of Fibonacci numbers associated with Dirichlet characters

Yohei Tachiya

(joint work with Hiromi Ei and Florian Luca)

We refine the methods of Chowla and Erdős who deduced the irrationality of certain Lambert series and give linear independence results for various infinite series; for instance, the numbers

$$1, \quad \sum_{n=1}^{\infty} \frac{\chi_j(n)}{F_n} \quad (j = 1, 2, \ldots)$$

are linearly independent over $\mathbb{Q}(\sqrt{5})$, where χ_j are certain nonprincipal real Dirichlet characters and $\{F_n\}_{n \geq 0}$ is the sequence of Fibonacci numbers. We also give irrationality results for the reciprocal sums of binary recurrences associated with another multiplicative functions.

Diophantine problems and arithmetic progressions

Szabolcs Tengely

In this talk we report on recent research related to three Diophantine problems. First we consider a special case of the so-called Erdős-Graham problem. Erdős and Graham asked if the Diophantine equation

$$\prod_{i=1}^{r} f(x_i, k_i, 1) = y^2$$

has, for fixed $r \geq 1$ and $\{k_1, k_2, \ldots, k_r\}$ with $k_i \geq 4$ for $i = 1, 2, \ldots, r$, at most finitely many solutions in positive integers $(x_1, x_2, \ldots, x_r, y)$ with $x_i + k_i \leq x_{i+1}$ for $1 \leq i \leq r - 1$. Skałba provided a bound for the smallest solution and estimated the number of solutions below a given bound. Ulas answered the above question of Erdős and Graham in the negative when either $r = k_i = 4$, or $r \geq 6$ and $k_i = 4$. Tengely proved that the only solution $(x, y) \in \mathbb{N}^2$ of

$$x(x+1)(x+2)(x+3)(x+k)(x+k+1)(x+k+2)(x+k+3) = y^2, \quad (1)$$

with $4 \leq k \leq 10^6$ is

$$(x, y) = (33, 3361826160)$$

with $k = 1647$. In this talk we provide more precise answer to this problem.

Zhang and Cai deal with the equations

$$(x-1)x(x+1)(y-1)y(y+1) = (z-1)z(z+1),$$
$$(x-b)x(x+b)(y-b)y(y+b) = z^2,$$

where b is a positive even number. In case of the first equation they prove that there exist infinitely many non-trivial positive integer solutions. In case of the second equation they obtain similar result. They also pose two questions related to the above equations.

Question 1. Are all the nontrivial positive integer solutions of $(x-1)x(x+1)(y-1)y(y+1) = (z-1)z(z+1)$ with $x \leq y$ given by $(F_{2n-1}, F_{2n+1}, F_{2n}^2)$, $n \geq 1$?

Question 2. Are there infinitely many nontrivial positive integer solutions of $(x-b)x(x+b)(y-b)y(y+b) = z^2$ if $b \geq 3$ odd?

We provide some partial results related to the above questions.

Upper and lower densities – Part I

Salvatore Tringali

We present an axiomatic theory of upper and lower densities on the integers that relies on a package of five axioms a real-valued set function $\mu^\star$ on the power set of $\mathbb{Z}$ is required to satisfy: monotonicity, subadditivity, (-1)-homogeneity, and translational invariance, together with the normalization condition $\mu^\star(\mathbb{Z}) = 1$. In particular, we will discuss and prove the mutual independence of these axioms, and provide a number of examples for which they are all satisfied (examples include the upper asymptotic, upper Banach, upper logarithmic, upper Buck, and upper analytic densities).

Primitive solutions of Diophantine equations involving squares and fifth powers

Maciej Ulas

We present some result concerning solvability in integers of the Diophantine equations of the form $T^2 = G(\overline{X})$, $\overline{X} = (X_1, \ldots, X_m)$, where $m = 3$ or $m = 4$ and G is a specific homogenous quintic form. First, we prove that if $F(x, y, z) = x^2 + y^2 + az^2 + bxy + cyz + dxz \in \mathbb{Z}[x, y, z]$ and $(b - 2, 4a - d^2, d) \neq (0, 0, 0)$, then for all $n \in \mathbb{Z} \setminus \{0\}$ the Diophantine equation $t^2 = nxyzF(x, y, z)$ has a solution in polynomials x, y, z, t with integer coefficients, with no polynomial common factor of positive degree. In case $a = d = 0, b = 2$ we prove that there are infinitely many primitive integer solutions of the Diophantine equation under consideration. As an application of our result we prove that for each $n \in \mathbb{Q} \setminus \{0\}$ the Diophantine equation

$$T^2 = n(X_1^5 + X_2^5 + X_3^5 + X_4^5)$$

has a solution in co-prime (non-homogenous) polynomials in two variables with integer coefficients. We also present a method which sometimes allows us to prove the existence of primitive integer solutions of more general quintic Diophantine equation of the form $T^2 = aX_1^5 + bX_2^5 + cX_3^5 + dX_4^5$, where $a, b, c, d \in \mathbb{Z}$. In particular, we prove that for each $m, n \in \mathbb{Z} \setminus \{0\}$, the Diophantine equation

$$T^2 = m(X_1^5 - X_2^5) + n^2(X_3^5 - X_4^5)$$

has a solution in polynomials which are co-prime over $\mathbb{Z}[t]$. Moreover, we show how a modification of the presented method can be used in order to prove that for each $n \in \mathbb{Q} \setminus \{0\}$, the Diophantine equation

$$t^2 = n(X_1^5 + X_2^5 - 2X_3^5)$$

has a solution in polynomials which are co-prime over $\mathbb{Z}[t]$.