21st Czech and Slovak International Conference on Number Theory

Ostravice, Czech Republic
September 2–6, 2013

21st Czech and Slovak International
Conference on Number Theory

Ostravice (Czech Republic), September 2–6, 2013

Organized by

Department of Mathematics, Faculty of Science,
University of Ostrava

Institute of Computer Science, Academy of Sciences
of the Czech Republic, Prague

Mathematical Institute, Slovak Academy of Sciences, Bratislava

University J. Selye in Komárno

Organizing committee

Jan Štěpnička
Jan Šustek
Zuzana Václavíková

Scientific committee

Jaroslav Hančl (University of Ostrava)
Ladislav Mišík (University of Ostrava)
Karol Nemoga (Slovak Academy of Sciences)
Štefan Porubský (Academy of Sciences of the Czech Republic)
János Tóth (University J. Selye in Komárno)

Abstracts of talks

Hilbert space with reproducing kernel and uniform distribution preserving maps

Vladimír Baláž, Jana Fialová, Oto Strauch

For Hilbert space H with reproducing kernel $K(\mathbf{x},\mathbf{y})$, we express the mean square worst-case error

$$\int_{[0,1]^s} \sup_{\substack{f\in H\\ ||f||\le 1}} \left| \frac{1}{N}\sum_{n=0}^{N-1} f(\Phi(\{\mathbf{x}_n+\boldsymbol{\sigma}\})) - \int_{[0,1]^s} f(\mathbf{x})\mathrm{d}\mathbf{x}\right|^2 \mathrm{d}\boldsymbol{\sigma}$$

as

$$\frac{1}{N^2}\sum_{n,m=0}^{N-1}\int_{[0,1]^s} K(\Phi(\mathbf{x}),\Phi(\mathbf{y}))\mathrm{d}_{\mathbf{x}}\mathrm{d}_{\mathbf{y}} g_{m,n}(\mathbf{x},\mathbf{y}) - \int_{[0,1]^{2s}} K(\mathbf{x},\mathbf{y})\mathrm{d}\mathbf{x}\mathrm{d}\mathbf{y}$$

where $\Phi(\mathbf{x})$ is a uniform distribution preserving map, $\mathbf{x}_0,\dots,\mathbf{x}_{N-1}\in[0,1)^s$, and $g_{m,n}(\mathbf{x},\mathbf{y})$ are copulas associated with points $\mathbf{x}_m$ and $\mathbf{x}_n$. Applying this, for dimension $s=1$, we find that the minimum of the mean square worst-case error is attained in the sequence $x_n=\frac{n}{N}$, for the kernel $K(x,y)=1-\max(x,y)$ and $\Phi(x)=x$.

Effective results for Diophantine equations over finitely generated domains

Attila Bérczes

(Joint work with J.-H. Evertse and K. Győry.)

Let A be an arbitrary integral domain of characteristic 0 that is finitely generated over $\mathbb{Z}$. We consider Thue equations $F(x,y)=\delta$ in $x,y\in A$, where F is a binary form with coefficients from A and δ is a non-zero element from A, and hyper- and superelliptic equations $f(x)=\delta y^m$ in $x,y\in A$, where $f\in A[X]$, $\delta\in A\setminus\{0\}$ and $m\in\mathbb{Z}_{\ge 2}$.

Under the necessary finiteness conditions we give effective upper bounds for the sizes of the solutions of the equations in terms of appropriate representations for A, δ, F, f, m. These results imply that the solutions of these equations can be determined in principle. Further, we consider the Schinzel-Tijdeman equation $f(x) = \delta y^m$ where $x, y \in A$ and $m \in \mathbb{Z}_{\geq 2}$ are the unknowns and give an effective upper bound for m.

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.

Representing integers as sums or differences of general power products

Csanád Bertók

Problems concerning representations of integers as linear combinations of power products has a large literature (see e.g. the corresponding papers of F. Luca, L. Hajdu, R. Tijdeman, V. S. Dimitrov and E. W. Howe, Zs. Ádám and the references given there). In the presentation we extend a result of Hajdu and Tijdeman concerning the smallest number which cannot be obtained as a sum of less than k power products of fixed primes.

Put $A'_{\pm} = A' \cup (-A')$. Define the function $F(k)$ $(k \in \mathbb{N})$ to be the smallest natural number which cannot be represented as the sum of less than k terms from A', and let $F_{\pm}(k)$ be the function defined similarly, except that A' is replaced by $A'_{\pm}$.

Nathanson asked for the growth properties of $F_{\pm}(k)$, in the particular case when the elements a_i $(i = 1, \ldots, l)$ of A are primes. Hajdu and Tijdeman proved several related theorems, both for $F(k)$ and $F_{\pm}(k)$. More precisely , they proved that for all $k > 1$

$$k^{C_0^* k} < F(k) < C_1^* (kl)^{(1+\varepsilon^*)kl} \text{ and } k^{C_0^* k} < F_{\pm}(k) < \exp((kl)^{C_2^*})$$

hold, where C_0^* and C_2^* are positive absolute constants, $\varepsilon^* > 0$ is arbitrary, and C_1^* is a positive constant depending only on ε^*.

In the presentation we consider the general case, where the elements a_i $(i = 1, \dots, l)$ of A are arbitrary positive integers. We note that it seems to be more natural to consider the problem under this condition mainly because since a part of the argument goes modulo m (with some appropriate m), the extra assumption that the numbers a_i $(i = 1, \dots, l)$ should be primes is irrelevant at many points. To prove our results, among other things we need to extend classical results of Tijdeman concerning the gaps in A' where the a_i are primes, to the case of arbitrary positive integers a_i $(i = 1, \dots, l)$.

On a modification of the group of circular units of a real abelian field

Michal Bulant, Radan Kučera

For a real abelian field K, Sinnott's group of circular units C_K is a subgroup of finite index in the full group of units E_K playing an important role in Iwasawa theory. Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension of K, and h_{K_n} be the class number of K_n, the n-th layer in K_∞/K. Then for $p \neq 2$ and n going to infinity, the p-parts of the quotients $[E_{K_n} : C_{K_n}]/h_{K_n}$ stabilize. Unfortunately this is not the case for $p = 2$, when the group $C_{1,K}$ of all units of K, whose squares belong to C_K, is usually used instead of C_K. But $C_{1,K}$ is better only for index formula purposes, not having the other nice properties of C_K. Our aim is to offer another alternative to C_K which can be used in cyclotomic $\mathbb{Z}_p$-extensions even for $p = 2$ still keeping almost all nice properties of C_K.

About the existence of the generalized Gauss composition of means

Peter Csiba

Let $I \subset \mathbb{R}$ be a non-void open interval. Let $M_i \colon I^2 \to I (i = 1, 2)$ be means on I and $a, b \in I$. Consider the sequences (a_n) and (b_n) defined by the Gauss iteration in the following way:

$$\begin{aligned} a_1 &:= a, & b_1 &:= b, \\ a_{n+1} &:= M_1(a_n, b_n), & b_{n+1} &:= M_2(a_n, b_n) \quad (n \in \mathbb{N}). \end{aligned}$$

If the limits $\lim_{n\to\infty} a_n$, $\lim_{n\to\infty} b_n$ exist and

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n \,,$$

than this common limit is called Gauss composition of the means M_1 and M_2 for the numbers a and b, and denoted by $M_1 \otimes M_2(a, b)$.

It is known, if M_1, M_2 are strict means on I, then $M_1 \otimes M_2(a, b)$ exist for every $a, b \in I$.

We generalised this result. We show that if means M_1, M_2 (not necessarily continuous) may be restricted by strict means, then their Gauss composition exists. We also show that the continuity of restrictive means is necessary.

Sums of reciprocals modulo composite integers

Karl Dilcher

(Joint work with John B. Cosgrave.)

In 1938, as part of a wider study, Emma Lehmer derived a set of four related congruences for certain sums of reciprocals of positive integers over various ranges, modulo squares of odd primes. These were

recently extended to congruences modulo squares of positive integers n, with certain restrictions on n. In this talk I will characterize those excluded n for which the congruences still hold, and find the correct reduced moduli in the cases in which the congruences do not hold.

Reducibility and irreducibility of Stern polynomials

Larry Ericksen

(Joint work with Karl Dilcher.)

The classical Stern (diatomic) sequence was extended by Dilcher and Stolarsky to the Stern polynomials $a(n;x)$ defined by $a(0;x) = 0$, $a(1;x) = 1$, $a(2n;x) = a(n;x^2)$, and $a(2n+1;x) = x\,a(n;x^2) + a(n+1;x^2)$. These polynomials $a(n;x)$ are Newman polynomials, as they have only 0 and 1 as coefficients. Numerous reducibility and irreducibility properties for these polynomials will be proven. Special attention will be given to the divisibility properties for Stern polynomials of the form $a(2^k \pm 1;x)$. Cyclotomic polynomials will be identified as factors of the reducible Stern polynomials.

Generalization of uniform distribution of sequences by using densities

Ferdinánd Filip and János T. Tóth

Let $\omega = \{x_n\}_{n=1}^{\infty}$ be a given sequence of real numbers. For a subset E of the unit interval $I = \langle 0, 1)$, let the set $A(E, \omega)$ be defined as

$$A(E, \omega) = \{n \in \mathbb{N} | \{x_n\} \in E\}\,.$$

Definition. *Let φ be a density. The sequence $\omega = \{x_n\}_{n=1}^{\infty}$ of real numbers is said to be φ-uniformly distributed modulo 1 if for every pair a, b of real numbers with $0 \le a < b < 1$ we have*

$$\varphi(A(\langle a, b), \omega)) = b - a\,.$$

In this talk we determine for what kind of φ densities there exsists a sequence which is φ-uniformly distributed modulo 1.

Elements of minimal index in the infinite family of simplest quartic fields

István Gaál

(The result is joint with G. Petrányi.)

It is a classical problem in algebraic number theory to consider *power integral bases* of type $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of number fields K. It is well known that α generates a power integral basis if and only if the *index* of α, that is

$$I(\alpha) = \left(\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+\right)$$

is equal to 1. There is an extensive literature about *calculating power integral bases* and deciding *monogenity* of specific number fields. If a number field does not admit elements of index 1, it is an important question to calculate *elements of minimal index* in the number field. Determining element of minimal index usually requires calculating elements of given index up to a certain bound, which is more complicated than just to determine elements of index 1.

It yields a challenge to consider this problem in *infinite parametric families* of number fields.

In the talk we consider the infinite parametric family of *simples quartic fields*, generated by a root of the polynomial

$$P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1$$

where $t \in \mathbb{Z}$, $t \neq 0, \pm 3$. *H.K. Kim and J.S. Kim* (2003) determined an integral basis in these fields. *P. Olajos* (2005) showed that power integral bases exist only for $t = 2, 4$. In the talk we describe all elements of minimal indices in this parametric family of number fields.

A note on the Diophantine equation $P(z) = m! + n!$

Maciej Gawron

We start with a short overwiew of Brocard-Ramanujan type Diophantine equations. As a main result we consider the equation $P(z) = n! + m!$, where P is a polynomial with rational coefficients. We show that the ABC Conjecture implies that this equation has only finitely many integer solutions when $d \geq 2$ and $P(z) = a_d z^d + a_{d-3} z^{d-3} + \cdots + a_1 x + a_0$.

A class of K-fold infinite series and their reduction

Marian Genčev

We present a result that enables the transformation of the general K-fold infinite series of the form

$$\sum_{1 \leq n_1 \leq n_2 \leq \cdots \leq n_K} \prod_{j=1}^{K} R(n_j),$$

$R(n)$ is a rational function satisfying some simple conditions, to a special ordinary (i.e., 1-fold) infinite series. We apply this result to the rational function

$$R(n) = \frac{1}{(n+a)^s + b^s}\,.$$

In this case we call the resulting K-fold sum the generalized multiple Hurwitz zeta-star function and denote it by $\zeta^\star(a; b; \{s\}_K)$. We construct a very effective algorithm which enables the complete evaluation

of $\zeta^\star(a;b;\{2s\}_K)$ for $a \in \{0,-1/2\}$, $b \in \mathbb{R}$ with $b \neq 0$, and $K, s \in \mathbb{N}$ are arbitrary. Several comments to the known evaluations of the ordinary multiple Riemann zeta-star function $\zeta^\star(0;0;\{2s\}_K) = \zeta^\star(\{2s\}_K)$ corresponding to $a = b = 0$ are given. Also a new identity for $\zeta^\star(\{3\}_K)$ is established.

An additive problem in cyclic groups

Georges Grekos

(Joint work with Jean-Marc Deshouillers.)

Let h, n be integers, $2 \leq h \leq n$. An h-basis for the "interval" $[n] := \{0, 1, \ldots, n-1\}$ is a subset A of $[n]$ such that

$$hA := \{x_1 + \cdots + x_h \ ; \ x_i \in A \ , \ 1 \leq i \leq h\}$$

contains $[n]$. An h-basis for the cyclic group $G_n := \mathbf{Z}/n\mathbf{Z}$ is a subset A of G_n such that $hA = G_n$.

A central question in additive number theory is to find "economical" h-bases, that is h-bases of minimal size (cardinality).

We present a construction which gives, in the case of G_n and for certain values of h, h-bases of cardinality much smaller than the known upper bound $hn^{1/h}$, bound due to Hans Rohr-bach [Ein Beitrag zur additiven Zahlentheorie. Math. Z. 42, 1-30 (1936)].

Perfect powers in products with terms from arithmetic progression – A survey

Kálmán Győry

By a celebrated theorem of Erdős and Selfridge, the product of consecutive positive integers is never a power. It is an old conjecture that more generally the equation

$$m(m+d)\ldots(m+(k-1)d) = y^n$$

has no solution in positive integers m, d, k, y, n with $\gcd(m, d) = 1$, $k \geq 3$, $n \geq 2$ and $(k, n) \neq (3, 2)$. This equation has been investigated by many people. In the last fifteen years the conjecture was confirmed for $k < 35$. In our talk we give a survey of these, and some related results and the methods utilized in the proofs.

Sets with perfect power shifted products

Lajos Hajdu

Diophantine sets, i.e. sets A with the property that $ab + 1$ is a perfect square for all distinct $a, b \in A$, have a long history and a broad literature. In the talk we present results concerning the related problem where for all distinct $a, b \in A$, the shifted products $ab + n$ should be perfect powers (possibly having different exponents) for some fixed value of n. Among others, we show that the size of a set A having this property cannot be bounded by an absolute constant. The new results presented are joint with Bérczes, Dujella and Luca.

Irrationality of infinite products

Ondřej Kolouch

(Joint work with Jaroslav Hančl.)

The talk deals with the criterium for the infinite product of infinite series of rational numbers to be the irrational number.

In 1975 Erdős proved that if $\{a_n\}_{n=1}^{\infty}$ is an increasing sequence of positive integers such that

$$\liminf_{n\to\infty} a_n^{\frac{1}{2^n}} = \infty$$

then the number $\sum_{n=1}^{\infty} \frac{1}{a_n}$ is irrational.

We follow this result and prove

Theorem. Let $\{a_n\}_{n=1}^{\infty}$ be an increasing sequence of positive integers with

$$\liminf_{n\to\infty} a_n^{\frac{1}{n!}} = \infty.$$

Then the number

$$\prod_{m=1}^{\infty}\left(1+\sum_{n=0}^{\infty}\frac{1}{a_{n+m}+n}\right)$$

is irrational.

Local to global principle for étale K-theory of curves

Piotr Krasoń

(Joint work with G. Banaszak.)

We investigate linear dependence over $\mathbb{Z}_l$ of elements in étale K-theory of curves. This is done via reduction maps. We discuss local to global principle in this context. The work is based on our previous result concerning linear independence over $\mathbb{Z}$ of elements in the Mordell-Weil group of an abelian variety defined over a number field.

On the class group of a cyclic field of odd prime power degree

Radan Kučera

(Joint work with Cornelius Greither.)

Let p be an odd prime and $K/\mathbb{Q}$ be a Galois extension of degree $\ell = p^k$ whose Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is cyclic. Let cl_K be the ideal class group of K and $h_K = |\,\mathrm{cl}_K\,|$ be the class number of K.

Let $p_1, \ldots, p_s$ be the primes which ramify in $K/\mathbb{Q}$, let e_j be the ramification index of p_j and g_j be the number of prime ideals of K

dividing p_j. We assume that $s > 1$ and that the primes $p_1, \ldots, p_s$ are ordered in such a way that $\ell = e_1 \geq e_2 \geq \cdots \geq e_s \geq p$.

Let C_K be the Sinnott group of circular units of K, which is a subgroup of the group E_K of all units of K of finite index defined by explicit generators. Sinnott's index formula for our field K gives that the index $[E_K : C_K] = 2^{\ell-1} \cdot h_K \cdot e_2^{-1}$.

The aim of this talk is to show that, if $s > 2$, we can enlarge the Sinnott group C_K by other explicit generators to a subgroup $\overline{C}_K$ of E_K having smaller index $[E_K : \overline{C}_K] = 2^{\ell-1} \cdot h_K \cdot p^n \cdot \prod_{j=1}^{s} e_j^{-g_j}$, where $n = \sum_{i=1}^{k} \max\{g_j \mid e_j \geq p^i\}$. This formula gives that h_K is divisible by $p^{-n} \cdot \prod_{j=1}^{s} e_j^{g_j}$, which is stronger than the usual divisibility result obtained by genus theory if and only if there are at least two ramified primes p_j having $g_j > 1$. Moreover, assuming that p does not ramify in $K/\mathbb{Q}$, by a modification of Thaine-Rubin machinery we can show that if $\alpha \in \mathbb{Z}[G]$ annihilates the p-Sylow subgroup of the quotient $E_K/\overline{C}_K$ then $(1 - \sigma^{\ell/p}) \cdot \alpha$ annihilates the p-Sylow subgroup of the class group cl_K, where σ is a generator of the Galois group G.

On the frequency of multiplicative properties in diophantine approximations of almost all real numbers

Pierre Liardet

Let E be a subset of the natural numbers and let $p_n(x)/q_n(x)$ be the n-th convergent of x related to its regular continued fraction expansion. What can be said about the set $E(x) := \{n \in E\,;\, q_n(x) \in E\}$? In the classical metric theory of continued fractions, P. Erdös (JNT 1970) proved that $\#E(x)$ is infinite for almost all x if and only if $\sum_{k \in E} \varphi(k)/k^2 = \infty$ where $\varphi(\cdot)$ is the Euler arithmetic function. A result which is closed to the Duffin-Schaeffer conjecture (that says for $\varepsilon : E \to (0, \infty)$ given, the inequality

$$\left| x - \frac{p}{q} \right| \leq \frac{\varepsilon(q)}{q}$$

holds for infinitely many p and q coprime with $q \in E$ if and only if

$$\sum_{q \in E} \frac{\varepsilon(q)\varphi(q)}{q} = \infty \,.$$

In this talk we first survey recent results about this conjecture and then pay more attention to sets E for which $E(x)$ has a fixed asymptotic density $\delta(E)$ for almost all x. This is precisely the case for sets E which are Buck measurable. We extend such a result to a wider class of sets E satisfying interesting multiplicative structures as, for example, the class of k-free integers. Extensions to other continued fractions in one or higher dimensions should be also discussed.

Fundamental units for orders generated by a unit

Stéphane Louboutin

Let ϵ be an algebraic unit. It is a natural question to ask wether ϵ belongs to some system of fundamental units of the order $\mathbf{Z}[\epsilon]$. We will show that this is indeed the case for some number fields $\mathbf{Q}(\epsilon)$ of small degrees. In our talk, we will restrict ourself to the case of cubic units, i.e. to the case that $\mathbf{Q}(\epsilon)$ is a cubic number field.

Spectra of quadratic Pisot units as cut-and-project sets

Z. Masáková, K. Pastirčáková, E. Pelantová

The spectrum of a real number $\beta > 1$ is the set of $p(\beta)$ where p ranges over all polynomials with coefficients restricted to a finite set of consecutive integers, in particular,

$$\begin{aligned} X^r(\beta) &= \Big\{ \sum_{j=0}^{n} a_j \beta^j : n \in \mathbb{N},\, a_j \in \mathcal{A} = \{0, 1, \ldots, r\} \Big\} \\ &= \{0 = x_0 < x_1 < x_2 < x_3 < \cdots \} \,. \end{aligned}$$

The study of such sets for $\beta \in (1,2)$ was initiated by Erdős et al. [1] and since then, many authors have contributed to the description of $X^r(\beta)$, especially in case that β is a Pisot number. A general result by Feng and Wen [2] states that for a Pisot number β and $r+1 > \beta$, the sequence of distances $x_{n+1} - x_n$ in $X^r(\beta)$ can be generated by a substitution. The alphabet of the substitution grows rapidly with r. However, neither the explicit prescription for the substitution, nor the values of distances and their frequencies are known in general. The only case of base β, for which the minimal distance in $X^r(\beta)$ is known for any r is when β is a quadratic Pisot unit [3]. For the same class of β, we show that recasting of the spectra in the frame of the cut-and-project scheme may bring new insight into the problem. We determine the values of all distances between consecutive points and their corresponding frequencies. We also show that shifting the set $\mathcal{A}$ of digits so that it contains at least one negative element, or considering negative base $-\beta$ instead of β, the generalized spectrum coincides with a cut-and-project sequence. As a consequence, we can show that the spectrum can be generated by a substitution over an alphabet at most five letters.

References

[1] P. Erdős, I. Joó, V. Komornik, *Characterization of the unique expansions* $1 = \sum_{i=1}^{\infty} q^{-n_i}$ *and related problems*, Bull. Soc. Math. France 118 (3) (1990), 377–390.

[2] D.-J. Feng, Z.-Y. Wen, *A property of Pisot numbers*, J. Number Theory, 97 (2) (2002), 305–316.

[3] T. Komatsu, *An approximation property of quadratic irrationals*, Bull. Soc. Math. France, 130 (1) (2002), 35–48.

About J-numbers, the solutions to the equation $\phi(\phi(n)(n-1)) = \phi(n)\phi(n-1)$ with ϕ the Euler ϕ-function.

V. Janitzio Mejía Huguet

In this talk we will prove the existence of infinitely many solutions of the equation $\phi(\phi(n-1)) = \phi(n)\phi(n-1)$. Such solution will be referred to simply as J-numbers. We discuss the problem of determining whether or not there exist infinitely many J-numbers having only two prime factors. Some consequences of this question would yield, concerning the well-known family of Sierpiński numbers, are mentioned too.

Some problems in arithmetics of dynamical systems

Władysław Narkiewicz

A family F of algebraic number fields will be defined, and the following result will be established:

Let n be an odd integer. If $K \in F$ and $f(X) = X^n + c$, where c is a non-integral element of K. If K does not contain any primitive root of unity of order p, with p being a prime divisor of n, then the length of cycles arising by iterating F in K is bounded by a constant $B(K, n)$, and if all prime divisors of n exceed 2^N with $N = [K : Q]$, then $B(K, n)$ depends only on N.

Some open problems will be also presented.

On expressible sets for products

Lukáš Novotný

For a sequence of real numbers $\{a_n\}_{n=1}^{\infty}$ we call the set

$$E_{\Pi}\{a_n\}_{n=1}^{\infty} = \left\{ \prod_{n=1}^{\infty} \left(1 + \frac{1}{a_n c_n}\right) : c_n \in \mathbb{Z}^+ \right\}$$

its Π-expressible set. We calculate $E_{\Pi}\{a_n\}_{n=1}^{\infty}$ under various hypothesis on $\{a_n\}_{n=1}^{\infty}$. Where this is not possible we give some partial information on its contents. This investigation can be considered a continuation of related investigations on the Σ-expressible sets of sums.

On the Masser-Gramain constant

W.G. Nowak

(based on joint work with Guillaume Melquiond (U. Paris-Sud) and Paul Zimmermann (Nancy))

As a two-dimensional analogue of the Euler-Mascheroni constant γ, the Masser-Gramain constant δ has been defined as

$$\delta = \lim_{N\to\infty} \left| \sum_{k=2}^{N} \frac{1}{\pi r_k^2} - \log N \right| .$$

Here r_k denotes the minimal radius of a compact circular disc in the Euclidean plane, with arbitrary center, which contains at least k points with integer coordinates. In 1985, F. Gramain conjectured that δ might be equal to

$$\delta^* = 1 + 2\gamma + \log\left(\frac{\pi^2}{2L^2}\right) = 1.822825\ldots ,$$

where $L = 2\int_0^1 (1-x^4)^{-1/2}\,\mathrm{d}x$ is known as Gauss' *lemniscate constant*. At that time, the only numerical information about δ was due to a computation by F. Gramain & M. Weber which furnished $1.81 < \delta < 1.9$. In this talk the history of δ is described briefly, and an account is given on a recent attack on the problem [1]: Using modern computing power and a tight approximation to the lattice discrepancy of a circular disc with arbitrary center, it has been calculated that, up to four decimal digits, $\delta \approx 1.8198$. This disproves Gramain's conjecture.

References

[1] G. Melquiond, W.G. Nowak, and P. Zimmermann, *Numerical approximation of the Masser-Gramain constant to four decimal digits:* $\delta = 1.819\ldots$, Math. Comp. **82**/282 (2013), 1235–1246.

Recent results on field indices

Gábor Nyul

The field index of an algebraic number field is the greatest common divisor of the indices of all primitive algebraic integer elements in the field. At a previous edition of this conference, we reported our research on field indices. We survey earlier results and present our recent results for some parametric families of number fields.

On the distribution of polynomials with real coefficients, a new application of the Selberg integral

Attila Pethő

My talk is based on joint work with Shigeki Akiyama, which is accepted for publication by Journal of the Math. Soc. Japan.

Let $\mathcal{E}_d \subset \mathbb{R}^d$ denote the set of coefficients of monic polynomials of degree d with roots inside or on the unit circle. This is a bounded set, which can be divided naturally into $\lfloor d/2 \rfloor + 1$ subsets according the signature of the polynomial, i.e., according the number of its real roots. Let $\mathcal{E}_d^{(r,s)} \subset \mathcal{E}_d$ denote the set with signature $(r,s), r+2s=d$. In the talk we answer questions like:

1. What is the probability that picking a point of $\mathcal{E}_d$ the corresponding polynomial is totally real?
2. More generally, what is the probability that picking a point of $\mathcal{E}_d$ the corresponding polynomial has signature (r,s)?
3. Arithmetical properties of these probabilities?

We prove that the volume of $\mathcal{E}_d^{(r,s)}$ can be computed by some generalization of the Selberg integral. It turns out that these numbers are rational, which are in the totally real case reciprocal of odd integers. We propose several open problems.

You can download the manuscripts at the URL:
`http://www.inf.unideb.hu/~pethoe/cikkek/realandint_poly_v5.pdf`
and `http://www.inf.unideb.hu/~pethoe/cikkek/int_poly_v8.pdf`

On the Diophantine inequality $\left|X^2 - cXY^2 + Y^4\right| \leq c+2$

Bo He, István Pink, Ákos Pintér, and Alain Togbé

Generalizing some earlier results, we find all the coprime integer solutions of the Diophantine inequality

$$\left|X^2 - cXY^2 + Y^4\right| \leq c+2, \quad (X,Y)=1\,,$$

except when $c \equiv 2 \pmod 4$, in which case we bound the number of integer solutions. Our work is based on the results on the Diophantine equation

$$AX^4 - BY^2 = C\,,$$

where A, B are positive integers and $C \in \pm\{1,2,4\}$.

Coprime solutions to $ax \equiv b \pmod{n}$

Štefan Porubský

It is well known that a congruence $ax \equiv b \pmod{n}$ has a solution iff $\gcd(a,n)|b$, and, if the condition is satisfied, the number of incongruent solutions equals $\gcd(a,n)$. In [1] the authors noticed the following result which seems not to appear previously explicitly in the literature: Given a non-zero $a \in \mathbb{Z}_n$, the ring of residues modulo n, such that $\gcd(a,n) = \gcd(b,n)$, there exists an invertible element $x \in \mathbb{Z}_n^*$ satisfying the congruence $ax \equiv b \pmod{n}$. They gave a very long elementary proof of this result which played a key role in a problem related to an electronic signature. In the talk we give a concise proof of this result, together with a closed formula for the number of incongruent solutions coprime to n as well. We also give a bound on the probability that this congruence, for randomly chosen $a, b \in \mathbb{Z}$, possesses at least one solution coprime to n. This talk is based on a joint paper [2] with O.Grošek (Bratislava).

References

[1] B. Alomair, A. Clark, and R. Poovendran. The power of primes: security of authentication based on a universal hash-function family. *J. Math. Cryptol.*, 4(2):121-148, 2010.

[2] O. Grošek and Š. Porubský. Coprime solutions to $ax \equiv b \pmod{n}$. *J. Math. Cryptol.*, to appear in 2013

Equal values of pyramidal numbers

Zsolt Rábai

A pyramidal number is a figurate number that represents a pyramid with a base and a given number of sides. The sequence of pyramidal

numbers is given by the formula

$$P(u,m) = \frac{u(u+1)((m-2)u+(5-m))}{6}.$$

We consider the equation $P(u,m) = P(v,n)$, or more precisely the equation

$$(m-2)u^3 + 3u^2 + (5-m)u = (n-2)v^3 + 3v^2 + (5-n)v$$

in positive integer unknowns m, n, u and v. We present a method, which yields an effective upper bound on the values of u and v (in terms of m and n), and also give the set of solutions for some small values of m and n. In the proofs we apply results from the theory of elliptic curves and elliptic logarithms. This is a joint work with Tünde Kovács.

Sidon basis

Eszter Rozgonyi

Let $\mathbb{N}$ denote the set of nonnegative integers. Let $\mathcal{A} = \{a_1, a_2, \dots\}$, $(a_1 < a_2 < \dots)$ be an infinite sequence of positive integers. For $h \geq 2$ integer let $R_h(\mathcal{A}, n)$ denote the number of solutions of the equation

$$a_{i_1} + a_{i_2} + \cdots + a_{i_h} = n, \quad a_{i_1} \in \mathcal{A}, \dots, a_{i_h} \in \mathcal{A}, \quad a_{i_1} \leq a_{i_2} \leq \dots \leq a_{i_h},$$

where $n \in \mathbb{N}$.

A (finite or infinite) set $\mathcal{A}$ of positive integers is said to be a Sidon set if all the sums $a+b$ with $a, b \in \mathcal{A}$, $a \leq b$ are distinct. In other words $\mathcal{A}$ is a Sidon set if for every n positive integer $R_2(\mathcal{A}, n) \leq 1$. We say a set $\mathcal{A} \subset \mathbb{N}$ is an asymptotic basis of order h, if every large enough positive integer n can be represented as the sum of h terms from $\mathcal{A}$, i.e., if there exists a positive integer n_0 such that $R_h(\mathcal{A}, n) > 0$ for $n > n_0$.

P. Erdős, A. Sárközy and V. T. Sós asked if there exists a Sidon set which is an asymptotic basis of order 3. It is easy to see that a Sidon

set cannot be an asymptotic basis of order 2. A few years ago J. M. Deshouillers and A. Plagne constructed a Sidon set which is an asymptotic basis of order at most 7. S. Kiss proved the existence of a Sidon set which is an asymptotic basis of order 5. We improve this result by proving that there exists an asymptotic basis of order 4 which is a Sidon set by using probabilistic methods.

In the talk I will try to give a short summarize about this result, which is joint work with Sándor Kiss and Csaba Sándor.

The Irrationality of Infinite Series of a Special Kind

Pavel Rucki

The contribution provides several criteria for certain infinite series of rational numbers to be irrational, transcendental or Liouville. They are based on the following Erdős Theorem [1]:

Theorem. *Let* $\{a_n\}_{n=1}^{\infty}$ *be a strictly increasing sequence of positive integers. Suppose that*

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_1 a_2 \dots a_n} = \infty.$$

Then the sum of the series

$$\sum_{n=1}^{\infty} \frac{1}{a_n}$$

is an irrational number.

Terms of the series will be constrained by specific reccurence relations. Several examples are included.

References

[1] Erdős, P.: *Problem 4321*, Amer. Math. Mothly, no **64**, (1957), p. 47.

An extension of three theorems of Nagell

Andrzej Schinzel

It will be proved that an algebraic sum of terms $1/(m + kn)$ $(k = 0, \ldots, x)$ is an integer only if $m = 1$, $x = 0$. Nagell in 1924 published the relevant theorem concerning the arithmetic sum.

A linear recurrence sequence of composite numbers

Jonas Šiurys

We prove that for each positive integer k in the range $2 \leq k \leq 10$ and for each positive integer $k \equiv 79 \pmod{120}$ there is a k-step Fibonacci-like sequence of composite numbers and give some examples of such sequences. This is a natural extension of a similar result of Graham[1] for the Fibonacci-like sequence.

References

[1] R.L. Graham, *A Fibonacci-like sequence of composite numbers*, Math. Mag. **37** (1964), 322–324.

Distribution functions of sequences

Oto Strauch

In this lecture we present two applications of distribution functions:

Three dimensional Copula. Applying Weyl's limit relation we compute

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}F(\gamma_q(n),\gamma_q(n+1),\gamma_q(n+2))$$
$$=\int_0^1\int_0^1\int_0^1 F(x,y,z)\mathrm{d}_x\mathrm{d}_y\mathrm{d}_x g(x,y,z)=\frac{q^4-3q^3+3q^2+2q+2}{4q^4+4q^3+4q^2},$$

where $\gamma_q(n)$ is the van der Corput sequence in base q, $g(x,y,z)$ is an asymptotic distribution function of $(\gamma_q(n),\gamma_q(n+1),\gamma_q(n+2))$, and $F(x,y,z)=xyz$. Here the distribution function $g(x,y,z)$ is a new copula, cf. [1].

Two-dimensional Benford's law. Let $x_n>0$, $y_n>0$, $n=1,2,\dots$ and $F_N(x,y)=\#\{n\le N;\{\log_b x_n\}<x \text{ and } \{\log_b y_n\}<y\}/N$ and express the integers K_1,K_2 in base b representation as $K_1=k_1^{(1)}k_2^{(1)}\dots k_{r_1}^{(1)}$, $K_2=k_1^{(2)}k_2^{(2)}\dots k_{r_2}^{(2)}$. Denote $u_1=\log_b\left(\frac{K_1}{b^{r_1-1}}\right)$, $u_2=\log_b\left(\frac{K_1+1}{b^{r_1-1}}\right)$, $v_1=\log_b\left(\frac{K_2}{b^{r_2-1}}\right)$, $v_2=\log_b\left(\frac{K_2+1}{b^{r_2-1}}\right)$. Then we have

$$\lim_{k\to\infty}\frac{\#\{x_n \text{ has first } r_1 \text{ digits } =K_1 \text{ and } y_n \text{ has first } r_2 \text{ digits } =K_2\}}{N_k}$$
$$=g(u_2,v_2)+g(u_1,v_1)-g(u_2,v_1)-g(u_1,v_2)\,,$$

if

$$\lim_{k\to\infty}F_{N_k}(x,y)=g(x,y)\,.$$

Thus to solve the problem of digits of (x_n,y_n) we need full description of the set of all distribution functions of $(\{\log_b x_n\},\{\log_b y_n\})$, see [2].

References

[1] R.B. Nelsen. *An Introduction to Copulas. Properties and Applications*, Lecture Notes in Statistics **139** Springer-Verlag, New York, 1999.

[2] O. Strauch, Š. Porubský. *Distribution of sequences: A Sampler*, `http://www.boku.ac.at/MATH/udt/`

k-block versus 1-block Parallel Addition in Non-standard Numeration Systems

Milena Svobodová

(Joint work with Christiane Frougny, Pavel Heller, Edita Pelantová.)

A positional numeration system is given by a base β in $\mathbb{C}$, $|\beta| > 1$, and a finite alphabet $\mathcal{A}$ of contiguous integers containing 0. We focus on the question whether, for a given numeration system, there exists a parallel algorithm performing addition of numbers with finite $(\beta, \mathcal{A})$-representations. By parallel algorithms we mean algorithms which perform the addition $x + y$ in constant time, independently of the lengths of the representations of x and y. This is equivalent to say that addition is a local function (or a sliding block code) from the alphabet $\mathcal{B} = \mathcal{A} + \mathcal{A}$ to $\mathcal{A}$. Recently, it has been shown that for any algebraic number β, $|\beta| > 1$, which has no conjugates of modulus 1, there exists an alphabet $\mathcal{A}$ allowing parallel addition. In general, the cardinality of $\mathcal{A}$ is unnecessarily large. In 1999, Kornerup suggested to consider a more general type of parallel algorithms, which, instead of treating each digit separately, manipulate blocks of digits of length $k \geq 1$. In that setting addition is a local function from $\mathcal{B}^k$ to $\mathcal{A}^k$.

In this talk we present an easy-to-check property of $(\beta, \mathcal{A})$ which guarantees the possibility of block parallel addition. We apply this result to the bases β which are Parry numbers, i.e., numbers whose Rényi expansion of unity $d_\beta(1) = t_1 t_2 t_3 \ldots$ is finite or eventually periodic. We show that if β additionally satisfies the property (F) or (PF), then block parallel addition is possible on the alphabet $\{0, \ldots, 2t_1\}$ or $\{-t_1, \ldots, t_1\}$. Specifically, we prove the usefulness of this concept on the d-bonacci base, where $\beta > 1$ is a root of the polynomial $f(X) = X^d - X^{d-1} - X^{d-2} - \cdots - X - 1$, by showing that k-block parallel addition is possible on the alphabets $\{0, 1, 2\}$ and $\{-1, 0, 1\}$ for some convenient k. However, if we require $k = 1$ (i.e., the standard parallel algorithm working with single digits), the cardinality of any alphabet allowing parallel addition in the d-bonacci base must be at least $d + 1$.

Power integral bases in infinite families of quartic fields

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 $(1, \theta, \ldots, \theta^{n-1})$ 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 relaive 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 our thesis we determine all power integral bases in infinite parametric families of certain quartic number fields and all relativ power integral bases in certain infinite families of quartic extensions of quadratic fileds. We utilize the algorithm known for determining power integral bases in quartic fields and its extension for calculating relative power integral bases in relative quartic extensions. The relative case has a similar formulation, but it is much more complicated technically. Both results reduce the index form equation in quartic fields (resp. relative quartic extensions) to a cubic and some corresponding quartic Thue equations (resp. relative Thue equations). In Chapter 2 of our thesis we describe all basic notions in algebraic number theory connected to power integral bases. In Chapter 3 we describe our results on infinite parametric families of quartic fields which appeared in a paper by I.Gaál and T.Szabó. In Chapter 4 we detail

our results on infinite parametric families of relative quartic extensions which are under publication in another paper by I. Gaál and T. Szabó.

On the equation $A!B! = C!$

Lajos Hajdu, Tamás Szakács

Suppose that $n! = a_1!a_2!\cdots a_r!, r \geq 2, a_1 \geq a_2 \geq \cdots \geq a_r \geq 2$. A trivial example is $a_1 = a_2!\cdots a_r! - 1, n = a_2!\cdots a_r!$. Dean Hickerson notes that the only nontrivial examples with $n \leq 410$ are $9! = 7!3!3!2!, 10! = 7!6! = 7!5!3!$ and $16! = 14!5!2!$ and asks if there are any others. Jeffrey Shallit and Michael Easter have extended the search to $n = 18160$ and Chris Caldwell has shown that any other n is greater than 10^6. We investigate the equation $A!B! = C!$, where $A, B, C \in \mathbb{N}^+$ and $A \leq B \leq C$.

Theorem. Let $B - A = k$ fixed. Then the equation $A!B! = C!$ has only finetly many solutions. $C < \alpha(k)$, where $\alpha(k)$ is an explicit constant only depending on k.

On the common factors in series of consecutive associated Lucas and Lehmer numbers

Márton Szikszai

We investigate a generalization of a problem originally stated by Pillai [1] concerning the greatest common divisors in sets of consecutive integers. We call an integer sequence $A = (A_n)_{n=0}^{\infty}$ Pillai if there exists a constant G_A such that for every $k \geq G_A$ one can find k consecutive terms of A such that none of these terms is coprime to all the others. This talk links up with previous works of Hajdu and the speaker [2, 3] in a sense that it continues the characterization of the Pillai property in specific recurrence sequences.

We show that in the case of non-degenerate associated Lucas and Lehmer sequences being a Pillai sequence depends on the parities of the corresponding parameters only. As a specific example we consider the well-known sequence of Lucas numbers and show that although it is not a Pillai sequence, one can find consecutive terms in it such that none of these terms is coprime to all the others. Further, we show that it takes at least 171 consecutive Lucas numbers to obtain such a string. We investigate the more general T-Pillai property as well.

References

[1] S. S. Pillai. *On M consecutive integers.* Proc. Indian Acad. Sci. **Sect. A 11** (1940), 6–12.

[2] L. Hajdu, M. Szikszai. *On the GCD-s of k consecutive terms of Lucas sequences.* J. Number Theory **132** (2012), 3056-3069.

[3] L. Hajdu, M. Szikszai. *On common factors within a series of consecutive terms of an elliptic divisibility sequence.* (submitted).

Irrationality of Lambert series associated with periodic sequence

Yohei Tachiya

This talk is based on a joint work with Florian Luca.

Let q be an integer with $|q| > 1$ and $\{a_n\}_{n\geq 1}$ be an eventually periodic sequence of rational numbers, not identically zero from some point on. Then the number $\sum_{n=1}^{\infty} a_n/(q^n-1)$ is irrational. In particular, if the periodic sequences $\{a_n^{(i)}\}_{n\geq 1}$ $(i=1,\dots,m)$ of rational numbers are linearly independent over $\mathbb{Q}$, then so are the following $m+1$ numbers:

$$1, \quad \sum_{n=1}^{\infty} \frac{a_n^{(i)}}{q^n-1}, \quad i=1,\dots,m.$$

This generalizes a result of Erdős who treated the case $m=1$ and $a_n^{(1)}=1$ $(n\geq 1)$.

On a problem of Erdős and Graham

Szabolcs Tengely

Erdős and Selfridge proved that the product of consecutive integers cannot be a perfect power. Later Erdős and Graham posed a related problem about product of two or more disjoint blocks of consecutive integers. In this talk we consider the Diophantine equation

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

where $x > 0, k > 0$. We note that there is a solution with $x = 33$ and $k = 1647$. Walsh gave an argument (based on the ABC conjecute) which provides reasonable support that the number of solutions is finite. We prove that if a solution exists, then $x \leq k + 1$. We also determine all solutions with $0 < k \leq 10^6$.

On a Generalization of a Problem of Erdős and Graham

Szabolcs Tengely, Nóra Varga

Let us define

$$f(x,k,d) = x(x+d)\cdots(x+(k-1)d)\,.$$

Erdős and independently Rigge proved that $f(x,k,1)$ is never a perfect square. A celebrated result of Erdős and Selfridge states that $f(x,k,1)$ is never a perfect power of an integer, provided $x \geq 1$ and $k \geq 2$. That is, they completely solved the Diophantine equation

$$f(x,k,d) = y^l$$

with $d = 1$.

In this talk we study the Diophantine equation

$$\frac{x(x+1)(x+2)(x+3)}{(x+a)(x+b)} = y^2;$$

where $a, b \in \mathbb{Z}$, $a \neq b$ are parameters. We provide bounds for the size of solutions and an algorithm to determine all solutions $(x, y) \in \mathbb{Z}^2$. We use this algorithm to resolve the above equation for $a, b \in \{-4, -3, -2, -1, 4, 5, 6, 7\}$. The method of proof is based on Runge's method.

Finally, we show some cases which are under examination.

On the properties of negative base number systems associated to confluent Pisot numbers

T. Vávra

(Joint work with Z. Masáková and D. Dombek.)

In positive base number systems many properties are specific for the class confluent Pisot bases, i.e. zeros of $x^k - mx^{k-1} - mx^{k-2} - \cdots - mx - n$, where $k \geq 1$, $m \geq n \geq 1$. The main aspect is that any integer combinations of non-negative powers of the base with coefficients in $\{0, 1, \ldots, \lceil \beta \rceil - 1\}$ is a β-integer, although a sequence of coefficients may be forbidden in the corresponding number system, in other words

$$X(\beta) := \Big\{ \sum_{i=0}^{n} a_i \beta^i \;\Big|\; n \in \mathbb{N}_0,\ a_i \in \{0, 1, \ldots, \lceil \beta \rceil - 1\} \Big\} = \mathbb{Z}_\beta. \quad (1)$$

Confluent Pisot bases are also among the only cases where an explicit prescription for the substitution generating the spaces in $X(\beta)$ has been provided. The question of description of $X(\beta)$ is a special case of the problem about spectra of real numbers introduced by Erdős et al. We concentrate on the analogy of (1) in negative base number systems introduced by Ito and Sadahiro. We show that any integer

combinations of non-negative powers of the base with coefficients in $\{0, 1, \ldots, \lfloor\beta\rfloor\}$ is a $(-\beta)$-integer, i.e.

$$X(-\beta) := \Big\{ \sum_{i=0}^{n} a_i \beta^i \;\; | \;\; n \in \mathbb{N}_0,\; a_i \in \{0, 1, \ldots, \lfloor\beta\rfloor\} \Big\} = \mathbb{Z}_{-\beta},$$

if and only if β is a zero of the above polynomial satisfying $m = n$ when k is even. It turns out that these are also precisely the bases, for which the infinite word $u_{-\beta}$ coding $(-\beta)$-integers has the same language as that of u_β. This fact implies some interesting properties of the corresponding system, e.g. that the language of $u_{-\beta}$ is closed under mirror image. For confluent Pisot bases, numbers with finite β-expansions form a subring of real numbers. On the other hand, for these bases (except the quadratic case) even the number $\lfloor\beta\rfloor + 1$ has no finite $(-\beta)$-representation over the alphabet $\{0, 1, \ldots, \lfloor\beta\rfloor\}$, hence the analogy does not hold. Also, as a consequence of our result, one can describe the structure of $X(-\beta)$.

Several problems on algebraic structures without choice

Eliza Wajch

Let ZW be more or less $(Z^- - [\text{Replacement}] - \text{Inf}) + [\text{Axioms of Logic}]$ where the notation for ZFC is taken from the excellent book "The Foundations of Mathematics" by K. Kunen. The purpose of my work is to define numbers in ZW and to investigate them as deeply as possible to apply the results obtained to physics. I reject Kunen's two extra assumptions of [2] that proper classes do not exist and that all elements of sets are sets. Similarly as in NBG or MK, I assume that every set is a class. In the light of my joint work with R. Pietrusiak, an ordinal number in the sense of Zermelo-von Neumann (in abbr. an ordinal number) can be defined as a set X of sets such that, for every non-void subset A of X, the set $\bigcap\limits_{x\in A} x$ is an element of $A \cap \mathcal{P}(X \setminus A)$. In my opinion, it is good to define Peano's set of natural numbers as an

ordered pair (N, f) where N is a set and f is an injection from N into N such that $N \setminus f(N) \neq \varnothing$ and N is the unique subset X of N such that $f(X) \subseteq X$ and $X \setminus f(N) \neq \varnothing$. A set is called T-infinite if it is not finite in the sense of Tarski. A set X is called uncountable if there is a T-infinite subset of X which is not equipollent with X. As usual, a set is called countable if it is not uncountable. Let ω be the class of all finite ordinal numbers, i.e. of all non-negative integers in the sense of von Neumann. Let ω_1 be the class of all countable ordinal numbers. It is neither true nor false in ZW that $\omega \neq \omega_1$. It is true in ZW that Peano's set of natural numbers exists if and only if there exists an uncountable set. Moreover, the following three conditions are equivalent in ZW+[Replacement]:(1) an uncountable set exists, (2) $\omega \neq \omega_1$, (3) ω_1 is a set. Other results strictly related to algebraic structures of numbers will be offered during my talk.

References

[1] H. Herrlich, *Axiom of Choice*,Springer-Verlag Berlin Heidelberg 2006 .

[2] K. Kunen, *The Foundations of Mathematics*,College Publications, London 2009. New York 1976.

[3] G. Priest, *An Introduction to Non-classical Logic*, Cambridge Univ. Press 2012.

Circular units of some real cyclic number fields

Milan Werl

Let K be a cyclic field whose genus field in the narrow sense is real and which is totally ramified at each ramifying prime. Then after a construction two explicit roots of circular units it is possible to find a basis for the group $C_W(K)$ of circular units of K defined by Washington. This basis enables us to compute the index of $C_W(K)$ in the group $E(K)$ of all units of K using Sinnott's formula for the index of the group of Sinnott's circular units in $E(K)$.