ArithRand 22

Graz, 1-2 July 2022

scientific organisers: Christian Elsholtz and Thomas Stoll

Speaker: Kübra Benli *Institut Élie Cartan de Lorraine*

Title: Factor complexity along polynomial subsequences

Abstract:

For a sequence $\mathbf{u} = (u_n)_{n\geq 0}$ with members from a finite set Σ, the factor complexity is given by the map $p_{\mathbf{u}}(n) = \#\{(u_m, u_{m+1}, \dots, u_{m+n-1}) : m \geq 0\}$, $n \in \mathbb{N}$. In thi s talk, based on a joint work (in progress) with Thomas Stoll, we study $p_{\mathbf{u}}(H(n))$ for Fibonacci- Thue-Morse sequences where H a polynomial of degree at least 2.

Speaker: Pierre-Yves Bienvenu, *TU Graz*

Title: Metric decomposability theorems on sets of integers

Abstract:

A set $A \subset \mathbb{N}$ is called additively decomposable (resp. asymptotically additively decomposable) if there exist sets $B, C \subset \mathbb{N}$ of cardinality at least two each such that $A = B + C$ (resp. $A\Delta(B + C)$ is finite). If none of these properties hold, the set A is called totally primitive. We define $\mathbb{Z}$-decomposability analogously with subsets A, B, C of $\mathbb{Z}$. Wirsing showed that almost all subsets of $\mathbb{N}$ are totally primitive. In this talk, in the spirit of Wirsing, we study decomposability from a probabilistic viewpoint. First, we show that almost all symmetric subsets of $\mathbb{Z}$ are $\mathbb{Z}$-decomposable. Then we show that almost all small perturbations of the set of primes yield a totally primitive set. Further, this last result still holds when the set of primes is replaced by the set of sums of two squares, which is by definition decomposable.

Speaker: Rainer Dietmann, *Royal Holloway, University of London*

Title: Longer gaps between values of binary quadratic forms

Abstract:

In this talk I want to present some new results on large gaps between integers which are sums of two squares, or are represented by any binary quadratic form of discriminant D (this is joint work with Christian Elsholtz, Alexander Kalmynin, Sergei Konyagin and James Maynard): Let $s_1, s_2, \dots$ be the sequence of positive integers, arranged in increasing order, that are representable by *any* binary quadratic form of fixed discriminant D, then

$$\limsup_{n\to\infty} \frac{s_{n+1}-s_n}{\log s_n} \geq \frac{|D|-1}{2\varphi(|D|)(\log|D| + O((\log\log|D|)^3))},$$

where φ denotes Euler's totient function. This improves a lower bound of $\frac{1}{|D|}$ of Richards (1982). In the special case of sums of two squares, we improve Richards's bound of $\frac{1}{4}$ to $\frac{390}{449} = 0.868\ldots$. I also want to discuss another direction which generalizes this question to polynomial sequences of the form $c + x^d$.

Speaker: Michael Drmota, *TU Wien*
Title: Primes as Sums of Fibonacci Numbers, I

Abstract:

The purpose of these two talks is to discuss the relationship between prime numbers and sums of Fibonacci numbers. The main result says that for every sufficiently large integer k there exists a prime number that can be represented as the sum of k different and non-consecutive Fibonacci numbers. This property is closely related to, and based on, a prime number theorem for Zeckendorf sum-of-digits function z, which returns the number of summands in the representation of a nonnegative integer as sum of non-consecutive Fibonacci numbers. The proof of such a prime number theorem, combined with a corresponding local result, constitutes the central contribution. In the first part we present the background together and a (strong) central limit theorem for the Zeckendorf sum-of-digit function on primes. This is joint work with Clemens Müllner (TU Wien) and Lukas Spiegelhofer (MU Leoben). (For Part II, see Lukas Spiegelhofer's talk below).

Speaker: Florian Luca, *Wits, MPI-SWS, KAU*
Title: **Universal Skolem Sets**

Abstract:

The celebrated Skolem–Mahler–Lech theorem asserts that if $\mathbf{u} := (u_n)_{n\geq 0}$ is a linearly recurrent sequence of integers then the set of its zeros, that is the set of positive integers n such $u_n = 0$, form a union of finitely many infinite arithmetic progressions together with a (possibly empty) finite set. Except for some special cases, is not known how to bound effectively all the zeros of $\mathbf{u}$. This is called *the Skolem problem*. In this talk we present the notion of a *universal Skolem set*, which an infinite set of positive integers $\mathcal{S}$ such that for every linearly recurrent sequence $\mathbf{u}$, the solutions $u_n = 0$ with $n \in \mathcal{S}$ are effectively computable. We present a couple of examples of universal Skolem sets, one of which has positive lower density as a subset of all the positive integers.
This is joint work with Joël Ouaknine (Max–Planck Saabrücken) and James Worrell (Oxford).

Speaker: Péringuey Paul, *Institut Élie Cartan de Lorraine*
Title: **A generalization of Artin's primitive root conjecture among almost primes**

Abstract:

Artin's conjecture states that the set of primes for which an integer a different from -1 or a perfect square is a primitive root admits an asymptotic density among all primes. In 1967 C.Hooley proved this conjecture under the Generalized Riemann Hypothesis.
The notion of primitive root can be extended modulo any integer by considering then the elements of the multiplicative group generating subgroups of maximal size. I will discuss the set of almost primes for which a number a is a generalized primitive root, and prove, under GRH, results similar to Artin's conjecture for primitive roots.

Speaker: Andrei Shubin, *Postdoctoral project assistant, TU Wien*
Title: **Automatic sequences along Piatetski-Shapiro sequences** .

Abstract:

I will talk about some recent results on the distribution of values of automatic sequences along the numbers $\lfloor n^c \rfloor$ for non-integer c. In particular, we address the questions about prime number theorem for such sequences, Sarnak conjecture, and subword complexity estimates.

Speaker: Igor Shparlinski, *UNSW*
Title: **Equations and character sums with matrix powers, Kloosterman sums over small subgroups and quantum ergodicity**

Abstract:

We obtain a nontrivial bound on the number of solutions to the equation

$$\sum_{i=1}^{\nu} A^{x_i} = \sum_{i=\nu+1}^{2\nu} A^{x_i}, \qquad 1 \le x_i \le \tau,$$

with a fixed $n \times n$ matrix A over a finite field $\mathbb{F}_q$ of q elements of multiplicative order τ. We apply our result to obtain a new bound for additive character sums with a matrix exponential function, nontrivial beyond the square-root threshold. For $n = 2$ this equation has been considered by Kurlberg and Rudnick (for $\nu = 2$) and Bourgain (for large ν) in their study of quantum ergodicity for linear maps over residue rings. We use a new approach to improve their results and also obtain a bound on Kloosterman sums over small subgroups, of size below the square-root threshold.

Joint work with Alina Ostafe and Felipe Voloch

Speaker: Lukas Spiegelhofer, *MU Leoben*
Title: **Primes as Sums of Fibonacci Numbers, II**

The second part of the talk focuses on the central techniques underlying the proofs of our main theorems on prime numbers. In particular, we will be concerned with *very sparse arithmetic subsequences* of $z(n)$, which is also of independent interest. More precisely, we study the *level of distribution* of the related sequence $a_\vartheta(n) = \exp(2\pi i \vartheta z(n))$. This is based on a combination of the "Mauduit–Rivat–van der Corput method" for digital problems and an estimate of a *Gowers norm* of a_ϑ.

This is joint work with Michael Drmota and Clemens Müllner (TU Wien). (For part I see Michael Drmota's talk above.)

Speaker: Cathy Swaenepoel, *Université Paris Cité*
Title: **Integers with preassigned digits**

Abstract:

For an 'interesting' set $\mathcal{S}$ of non negative integers, we will discuss some properties of the integers in $\mathcal{S}$ with preassigned digits.

Speaker: Arne Winterhof, *Austrian Academy of Sciences*
Title: Pseudorandom sequences derived from automatic sequences

Abstract:

Many automatic sequences, such as the Thue-Morse sequence or the Rudin-Shapiro sequence, have some desirable features of pseudorandomness such as a large linear complexity and a small well-distribution measure. However, they also have some undesirable properties in view of certain applications. For example, the majority of possible binary patterns never appears in automatic sequences and their correlation measure of order 2 is extremely large.

Certain subsequences, such as automatic sequences along squares, may keep the good properties of the original sequence but avoid the bad ones.

In this survey talk we investigate properties of pseudorandomness and non-randomness of automatic sequences and their subsequences and present results on their behaviour under several measures of pseudorandomness including linear co mplexity, correlation measure of order k, expansion complexity and normality.

(This is joint work with László Mérai.)

L. Mérai, A. Winterhof, Pseudorandom sequences derived from automatic sequences, Cryptogr. Commun., to appear.
https://arxiv.org/abs/2105.03086.
https://link.springer.com/article/10.1007/s12095-022-00556-9