ABSTRACTS — FINNISH NUMBER THEORY DAYS 2023

Transcendence measure for roots of e

Anne-Maria Ernvall-Hytönen

Napier's constant e is a transcendental number. It means that if P is a polynomial with integer coefficients, then $P(e)$ is non-zero. A natural question is the following: how close to zero can the values of $P(e)$ get, if we let P be any polynomial with integer coefficients in some suitable family of polynomials? It is clear, that this must depend on the degree and height of the polynomial. This give rise to the transcendence measure of e. Studying the transcendence measure for e is a classical question. Transdence measures for powers or roots of e have been studied, but mostly as a by-product of something else, or as a corollary of more general results. We show that the roots of e have similar transcendence measures as e.

Two ways to predict asymptotics for moments in families of L-functions

Martin Čech

Since the work of Conrey, Farmer, Keating, Rubinstein and Snaith, we have precise conjectures for the asymptotic formulas of moments in different families of L-functions. For the Riemann zeta function and quadratic Dirichlet L-functions, similar formulas for the moments at the central point were obtained by Diaconu, Goldfeld and Hoffstein using multiple Dirichlet series.

In this talk, we will see that the two approaches usually not only give the same results, but there is a correspondence between the various terms that arise in the computations. We will extend the multiple Dirichlet series approach to other families and give an example of a family where the two predictions lead to different answers.

Grassmann algebra in transcendence

Tapani Matala-aho

The solutions to groups of integer equations with less equations than unknowns can be estimated by using the Thue-Siegel or Siegel's lemma, shortly. Let $\mathcal{V} \in \mathcal{M}_{M\times N}(\mathbb{Z})$ be a non-zero integer matrix, then the equation

$$\mathcal{V}\overline{x} = \overline{0}$$

has a small non-zero integer solution $\overline{x} = (x_1, \ldots, x_N)$ bounded with a non-trivial upper bound depending on the the matrix $\mathcal{V}$. Let $\overline{B}$ be the Grassmann vector of the matrix $\mathcal{V}$ and $\overline{R}$ be the primitive Grassmann vector of the orthogonal complement of the Kernel of $\mathcal{V}$. We will demonstrate that $\overline{B}$ is an integer multiple of $\overline{R}$. This shows that the upper bound of a small solution can be improved by the greatest common divisor of all the $M \times M$ minors of $\mathcal{V}$. Thus we arrive to a special case of the famous Bombieri-Vaaler version of Siegel's lemma.

Polynomial Learning with Errors / Ring Learning with Errors: Equivalence and attacks

Rahinatou Nchiwo

RSA is threatened by the rapid progress in quantum information, as such a need to protect our systems from post-quantum attacks, which leads us to Lattice Based Cryptography (LBC). Ring learning with error (RLWE), is one of the promising technology of LBC. We study the equivalence between the RLWE and Polynomial Learning with Errors (PLWE) problems for cyclotomic number fields, via polynomial noise increase. We give sharper bounds in the case where the conductor is divisible by at most six primes. We describe a decisional attack against a version of the PLWE in which the samples are taken from a certain proper sub-ring of large dimension of the cyclotomic ring $\mathbf{F}_q[x]/\Phi_{p^k}(x)$.

On Elliott's conjecture and applications

Joni Teräväinen

About 30 years ago, Elliott posed the conjecture that a bounded multiplicative function g should not correlate with their own shifts, unless g is "close to" a twisted Dirichlet character $\chi(n)n^{it}$. This conjecture includes Chowla's conjecture as a special case. I will discuss a recent work where we prove this conjecture "at almost all scales" for two-point correlations and for odd order correlations in case of real-valued functions, improving on previous results of Tao and myself. I will also discuss applications of these results e.g. to sign patterns of multiplicative functions.

This is joint work with O. Klurman and A. P. Mangerel.

Modular supercuspidal lifts of weight 2 and Langlands's functoriality

Iván Blanco-Chacón

Given a cusp form $f \in S_k(\Gamma_0(N))$ and a prime $p > k$ coprime to N, and assuming that its Deligne representation is absolutely irreducible and has large image, we find conditions over p and N such that there exists a p-supercuspidal modular lift of the residual Deligne representation. Our work follows a similar technique as our previous [1], where we focused on producing potentially diagonalisable modular lifts. In both cases we use a local-to-global construction due to Khare and Winterberger, but in the present case, the p-local deformation ring corresponds with potentially crystalline deformations, but restricted to the supercuspidal innertial type. After discussing construction, we address its application to Langlands's functoriality.

References

[1] Blanco-Chacón, I., Dieulefait, L.: Potentially diagonalizable modular lifts of large weight. *Journal of Number Theory* 228 (2021), 188-207.

On divisor bounded multiplicative functions in short intervals

Yu-Chen Sun

In 2016, the celebrated Matomäki–Radziwiłł theorem showed that there are cancellations for 1-bounded multiplicative functions in almost all short intervals. Our recent work proved that Matomäki–Radziwiłł theorem can be extended to divisor bounded multiplicative functions. Especially, we proved that for any sufficiently large X, $\epsilon > 0$ and $h \geq (\log X)^{(1+\epsilon)k\log k - k + 1}$, we have

$$\frac{1}{h}\sum_{x<n\leq x+h} d_k(n) - \frac{1}{x}\sum_{x<n\leq 2x} d_k(n) = o(\log^{k-1} x)$$

for almost all $x \in [X, 2X]$, where $d_k(n) = \sum_{m_1\cdots m_k = n} 1$.

Conditional estimates for logarithms and logarithmic derivatives in the Selberg class

Neea Palojärvi

The Selberg class consists of functions sharing similar properties to the Riemann zeta function. The Riemann zeta function is one example of the functions in this class. The estimates for logarithms of Selberg class functions and their logarithmic derivatives are connected to, for example, primes in arithmetic progressions.

In this talk, I will discuss about effective and explicit estimates for logarithms and logarithmic derivatives of the Selberg class functions when $\Re(s) \geq 1/2 + \delta$ where $\delta > 0$. All results are under the Generalized Riemann hypothesis and some of them are also under assumption of a polynomial Euler product representation or the strong λ-conjecture. The talk is based on a joint work with Aleksander Simonič (University of New South Wales Canberra).

Chasing universality: quadratic forms and number fields

Pavlo Yatsyna

This talk will address questions concerning quadratic forms representing integers in rings of integers of totally real number fields, with a particular focus on universal quadratic forms — forms that can represent all totally positive integers.

On the complexity of blocks of the indicator of the primes

Sebastian Zuniga Alterman

We will discuss the general theory of subshifts from a topological dynamics perspective and focus mainly on the subshift of primes, for which we will study its complexity. As it turns out, number theoretic tools like the large sieve and, assuming the Hardy–Littlewood conjecture, will be helpful. To do so, we follow an idea of T. Tao. If time allows, we will discuss the complexity of the subshift of almost primes.

Siegel zeros, twin primes, and Goldbach's conjecture

Kaisa Matomäki

The generalised Riemann hypothesis asserts that all non-trivial zeros of Dirichlet L-functions $L(s,\chi)$ satisfy $\Re s = 1/2$. However, for Dirichlet L-functions the known zero-free region is even weaker than for the Riemann zeta function. In particular we do not know how to rule out the possibility that, for a real character χ, there exists a real zero β which is very close to 1.

Such exceptional zeros are called Siegel zeros. There has been lot of research concerning what would follow if Siegel zeros existed. In the talk I will describe how Siegel zeros are related to twin primes, Goldbach's conjecture, and primes in almost all very short intervals. In particular I will be talking about my joint work with Jori Merikoski.