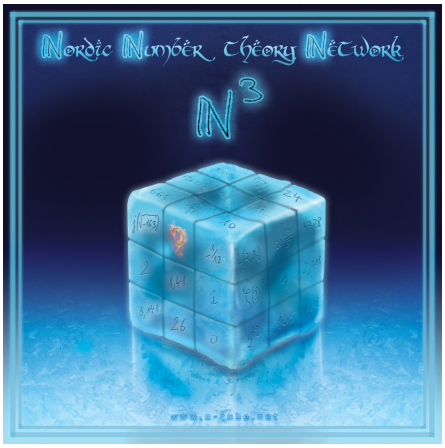
Nordic Number theory Network Days XIX

Copenhagen University,
November 17 – 18, 2023
organised by Jasmin Matz (KU), Fabien Pazuki (KU), Tim With Berland (KU).



Program

	Friday 17.11			Saturday 18.11
11:00-11:10	*Foreword*	◇		
11:10-12:00	**Hultberg**	◇		
12:00-13:00	*Lunch break*	◇		
13:00-13:50	**Södergren**	◇	09:10-10:00	**Nardi**
14:00-14:20	*Coffee break*	◇	10:00-10:30	*Coffee break*
14:20-15:10	**Müller**	◇	10:30-11:20	**Steiner**
15:20-16:10	**Wieser**	◇	11:30-12:20	**Kwan**
16:20-16:40	*Coffee break*	◇	12:30	*Farewell*
16:40-17:30	**Nelson**	◇		
18:30	*Social event*			

All talks will take place in Auditorium 5, HCØ-building, Universitetsparken 5, 2100 Copenhagen; see here for directions. *Registration* will take place in front of Auditorium 5 from around 10:45 on Friday.

Abstracts

SPEAKER: **Nuno Hultberg** (University of Copenhagen).
TITLE: *A linear AFL for quaternion algebras.*
ABSTRACT:The relative trace formula approach to the Beilinson-Bloch height conjectures aims to reduce the equality of certain arithmetic intersection numbers on Shimura varieties and derivatives of L-functions to local statements. Arithmetic fundamental lemmas are instances of such local statements. After giving an introduction to the Beilinson-Bloch conjectures I will present a particular instance of an AFL proven in joint work with Andreas Mihatsch.

SPEAKER: **Chung-Hang Kwan** (University College London).
TITLE: *Moments and Periods for* GL(3).
ABSTRACT:Moments of L-functions have been important in number theory and are well-motivated by a variety of arithmetic applications. In this talk, we will begin with two elementary counting problems of Diophantine nature, followed by a survey of techniques in the past and the present. The main goal is to demonstrate how period integrals (after Jacquet-Piatetskii-Shapiro-Shalika, Reznikov, and Michel-Venkatesh) can be used to study moments of automorphic L-functions and uncover the interesting underlying structures, some of which can be modeled by the theory of multiple Dirichlet series and the random matrix theory. If time permits, we will discuss some ongoing works and generalizations.

SPEAKER: **Werner Müller** (University of Bonn)
TITLE: *On the growth of torsion in the cohomology of arithmetic groups.*
ABSTRACT:There are deep connections between cohomology of arithmetic groups, the theory of automorphic forms and number theory. This concerns the cohomology with complex coefficients. Recent developments indicate that torsion classes may play a similar role. In the light of this a basic question is what is the size of torsion that one can expect in the cohomology of a given arithmetic group. A natural approach is to consider a decreasing sequence of congruence subgroups of a given arithmetic group with trivial intersection and investigate the growth of torsion in the cohomology of the congruence subgroups if the index of the subgroup tends to infinity. This is similar to the limit multiplicity problem in the theory of automorphic forms. Starting with a review of the work of Bergeron and Venkatesh, who treated the case of co-compact arithmetic groups, I will discussÂ various aspects of the growth of torsion in the cohomology of locally symmetric spaces of finite volume, associated to arithmetic groups. The method is analytic and is based on the study of the Ray-Singer analytic torsion of the locally symmetric spaces. Â I will review some of the recent results and discuss some open problems.

SPEAKER: **Jade Nardi** (Universite de Rennes).
TITLE: *Goppa–like AG codes from $C_{a,b}$ curves and the dimension of the square of their dual.*
ABSTRACT: McEliece cryptosystem is one of the last code-based candidates for standardization of postâquantum cryptrographic to the NIST competition since the third round. It guarantees the smallest ciphertexts among all the candidates, but it suffers from the largest public keys. Over the past forty years, there were many attempts in replacing the family of binary Goppa codes by other structured families of codes in order to reduce the key size.

In this talk, we will interest in a family of well-studied linear codes, namely algebraic geometry (AG) codes, and their subfield subcodes. As evaluation of functions of bounded "degree", algebraic geometry codes can easily be distinguished from random codes by computing

their Schur square, i.e. the vector space spanned by the component-wise product of its element. While Goppa codes are subfield subcodes of Reed-Solomon codes, the dimension of their Schur square is likely to be equal to the one of a random codes.

Recently, Mora and Tillich established a bound for the dimension of the Schur square dual of Goppa codes, which for high rate Goppa codes is abnormally small compared to random codes. This makes high rate Goppa codes distinguishable from random ones, which does not threaten the McEliece cryptosystem but is likely to break the code-based CFS signature.

After an introduction about linear codes, code-based cryptography and the Schur square, we will introduce a new family of codes that can be used in this context, called *Goppa–like AG codes*. These codes generalize Goppa codes and can be constructed from any curve of genus $\mathfrak{g} \geq 0$. We will get the grasp of Mora and Tillich's strategy to bound the dimension of the dual of classical Goppa codes and discuss how it generalizes to a family of Goppa-like AG codes from $C_{a,b}$ curves. We propose numerical experiments to measure how much our bound is sharp.

The talk is based a joint work with Sabira El Khalfaoui and Mathieu Lhotel. The preprint is available on ArXiv: https://arxiv.org/abs/2303.08687

SPEAKER: **Paul Nelson** (Aarhus University)).
TITLE: *Subconvex bounds for unitary groups in horizontal aspects.*
ABSTRACT:We'll describe some of the main ideas from the paper https://arxiv.org/abs/2309.06314 (joint with Yueke Hu), which establishes subconvex bounds for unitary groups in some new aspects. We'll begin by illustrating, in the setting of general linear groups over finite fields, how the methods developed in our earlier work with Venkatesh https://arxiv.org/abs/1805.07750 give rise to useful test vectors for the integral representations of L-functions furnished by known cases of the Ichino–Ikeda conjecture. We'll then discuss the geometric problems that arise when averaging this integral representation in an amplified relative trace formula.

SPEAKER: **Anders Södergren** (Chalmers).
TITLE: *Non-vanishing at the central point of the Dedekind zeta functions of non-Galois cubic fields.*
ABSTRACT:It is believed that for every S_n-number field, i.e. every degree n extension of the rationals whose normal closure has Galois group S_n, the Dedekind zeta function is non-vanishing at the central point. In the case $n = 2$ Soundararajan established, in spectacular work improving on earlier work of Jutila, the non-vanishing of the Dedekind zeta function for at least 87.5% of the fields in certain families of quadratic fields. In this talk, I will present joint work with Arul Shankar and Nicolas Templier, in which we study the case $n = 3$. In particular, I will discuss some of the main ideas in our proof that the Dedekind zeta functions of infinitely many S_3-fields have non-vanishing central value.

SPEAKER: **Raphael Steiner** (Zürich).
TITLE: *Fourth moments of automorphic forms and an application to diameters of hyperbolic surfaces.*
ABSTRACT:In joint work with Ilya Khayutin and Paul Nelson, we demonstrate how theta functions may be used to derive geometric expressions for fourth moments of automorphic forms on hyperbolic surfaces. By carefully estimating a second moment matrix count, we obtain a sharp pointwise bound on the fourth moment in the weight and level aspect. As a consequence, we significantly improve the sup-norm bounds in these aspects and give an unconditional upper bound on the diameter of hyperbolic surfaces of the same strength as if one were to assume the

Selberg eigenvalue conjecture.

SPEAKER: **Andreas Wieser** (Hebrew University of Jerusalem).
TITLE: *Equidistribution of subspaces and their shapes.*
ABSTRACT:Given a k-dimensional rational subspace of n-dimensional Euclidean space, one may associate to it two shapes: the shape of the integer lattice in the subspace and in the orthogonal complement. Moreover, one may measure the arithmetic complexity of a rational subspace by its discriminant which is the square of the covolume of the integer lattice in the subspace. Following work of Maass, Roelcke, and Schmidt it is conjectured that the set of triples consisting of a subspace L and the two shapes is equidistributed in the appropriate product space when L varies with fixed discriminant D and D goes to infinity. In this talk, we first recall known results towards this conjecture and then discuss new work joint with Aka, Einsiedler, Luethi, and Michel in which an effective variant of the conjecture is established for most dimensions. The proof uses a bootstrapping technique based on effective mixing as well as a discrepancy trick and will be discussed in a model case.