Luxembourg Number Theory Day 2019

17th December 2019, University of Luxembourg

LOCATION & SCHEDULE

The workshop will take place in the Seminar Room B on 6th Floor of the Maison du Nombre, Campus Belval.

10:30 – 11:20 **Valentijn Karemaker** *Arboreal Galois representations*

11:20 – 11:40 (Coffee Break)

11:40 – 12:30 **Pieter Moree** *The elusive Bernoulli numbers*

12:30 – 13:30 (Sandwich Lunch Break)

13:30 – 14:20 **Manfred G. Madritsch** *Diophantine inequalities, intersective sets and exponential sums*

14:20 – 14:40 (Coffee Break)

14:40 – 15:30 **Claus Fieker** *On Class Groups and Class Fields*

ABSTRACTS

Claus Fieker: *On Class Groups and Class Fields*

Class groups are one of the most important and mysterious invariants of number fields with many applications in cryptography, coding theory as well as in general computational number theory. The actual computation of class groups follows the "usual" index-calculus approach: starting from a (small) set of prime ideals (the generators), we search for smooth elements (the relations) until the group can be determined. The run-time analysis is heuristic and yields results similar to the analysis of algorithms for factoring or to compute discrete logarithms.

In this talk I will explain (briefly) what a class group is and how we can compute them. The analysis of the algorithm will also show the limitations of the current ideas which renders computations in fields of degree > 500 completely impossible.

One of the applications I am interested is the computation of class fields: a suitably modified class group uniquely determined an abelian extension of the number field - the classical example would be that cyclotomic fields are determined by their Galois group given as $\mathbb{Z}/n\mathbb{Z}^*$. I will explain how we can, in practice compute defining equations from the ideal data.

Recent applications are the automatical computation of fields with a given solvable Galois group.

Valentijn Karemaker: *Arboreal Galois representations*

Arboreal Galois representations are useful to describe the Galois theory of iterates of rational maps over number fields. These representations were introduced in the 1980s to study the prime divisors of non-linear recurrences (also called dynamical sequences). We study so-called dynamical Belyi maps; for these rational maps, we fully determine their arboreal Galois representations, and prove a result about the density of prime divisors of the corresponding dynamical sequences.

This is joint work with Irene Bouw and Özlem Ejder.

Manfred G. Madritsch: *Diophantine inequalities, intersective sets and exponential sums*

Dirichlet's approximation theorem states that for any real ξ and any $N > 0$ there exists $1 \leq n \leq N$ such that $\|\xi n\| \leq N^{-1}$, where $\|\cdot\|$ denotes the distance to the nearest integer. This was generalized, among others, by Heilbronn (1948), who proved that for any real ξ and any integer $N > 0$ there exists $1 \leq n \leq N$ such that $\|\xi n^2\| \leq N^{-\frac{1}{2}+\varepsilon}$.

We start the talk by presenting the connection of these questions with uniform distribution and intersective sets. In recent joint work with Robert Tichy we investigate pseudo polynomials, *i.e.* functions $f(x) = \alpha_1 x^{\theta_1} + \cdots + \alpha_d x^{\theta_d}$ such that $1 < \theta_1 < \cdots < \theta_d$ and at least one $\theta_j \notin \mathbb{Z}$. In particular, we show that for any real ξ and any integer N there exist $\sigma, \eta > 0$ depending only on f such that

$$\min_{1\leq n\leq N} \|\xi \lfloor f(n) \rfloor\| \ll N^{-\sigma} \quad \text{and} \quad \min_{\substack{1\leq p\leq N \\ p \text{ prime}}} \|\xi \lfloor f(p) \rfloor\| \ll N^{-\eta},$$

where the implied constant depends only on f.

Pieter Moree: *The elusive Bernoulli numbers*

Due to their unpredictable nature, Bernoulli numbers tend not to be a grateful topic of study. Over the years I took some care to avoid them, but did not quite manage. I will discuss three of my projects where they do appear (involving around 10 different coauthors).
-The irregularity of primes p for the (integers) $2(1-2^n)B_n$, which arise in a result a la Kummer (who did this for B_n) on the p-divisibility of certain class numbers (here methods used to study the Artin primitive root conjecture can be applied)
-Properties of the Bernoulli denominator D_n; the smallest positive integer so that multiplied with the nth Bernoulli polynomial $B_n(x)$ gives rise to a polynomial in $\mathbb{Z}[x]$.
-The integrality of ratios of consecutive power sums

The latter two projects were inspired by conjectures due to Bernd Kellner.