Luxembourg Number Theory Day 2017

18th December 2017, 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.

11:00 – 11:50 **Rene' Schoof** *Serre's Uniformity Conjecture*

12:00 – 12:50 **Vlad Serban** *p-adic Manin-Mumford and Bianchi modular forms*

12:50 – 13:30 (Sandwich Lunch Break)

13:30 – 14:20 **Chloe Martindale** *Isogeny graphs of abelian varieties and applications*

14:20 – 14:40 (Coffee Break)

14:40 – 15:30 **Wouter Castryck** *Counting quartic extensions of* $\mathbb{F}_q(t)$

ABSTRACTS

Wouter Castryck: *Counting quartic extensions of* $\mathbb{F}_q(t)$

There is a folklore conjecture stating that for a fixed integer $d > 1$ the amount of number fields K such that $[K : \mathbb{Q}] = d$ and $|\mathrm{Disc}(K)| < X$ equals $cX + o(X)$ for some constant $c > 0$. This is known up to $d \leq 5$, and in the cubic case it was moreover shown that there is a secondary term of the form $c'X^{5/6}$ for some other constant $c' < 0$. This was formerly known as the Roberts conjecture, now proven by Bhargava–Shankar–Tsimerman and Taniguchi–Thorne. In the quartic case it is believed that there is a similar error term $c'X^{5/6}$ but this is open. In his Ph.D. thesis Zhao demonstrated an analogue of the Roberts conjecture for cubic extensions of $\mathbb{F}_q(t)$. His proof gives a remarkable explanation for the exponent $5/6$, which shows up as a corollary to a well-known bound on the Maroni invariants e_1, e_2 of a trigonal curve. In this talk we will give a similar (but heuristic) derivation of the secondary term in the counting function for quartic extensions of $\mathbb{F}_q(t)$, where the lead role is now played by the Schreyer invariants b_1, b_2. As it turns out these satisfy a very similar bound, accounting for the appearance of the same exponent $5/6$. This is explained by Casnati's observation that $b_1 + 2, b_2 + 2$ are the Maroni invariants of Recillas' trigonal construction, which is the geometric equivalent of the cubic resolvent. This is joint work in progress with Yongqiang Zhao.

Chloe Martindale: *Isogeny graphs of abelian varieties and applications*

An isogeny graph is a graph whose vertices correspond to abelian varieties (with some structure) and whose edges correspond to isogenies of a certain degree. The structure of isogeny graphs for elliptic curves was first studied by David Kohel in his PhD thesis and has since been an essential tool in algorithmic number theory (for example to compute the endomorphism ring of an ordinary elliptic curve over a finite field) and cryptography (for example in the post-quantum cryptographic protocol SIDH). We present a structure theorem for isogeny graphs of ordinary abelian varieties, and explain how, under some heuristic assumptions, this can be applied to breaking the discrete logarithm problem for genus 3 curves and possibly some families of elliptic curves.

Rene' Schoof: *Serre's Uniformity Conjecture*

Serre's Uniformity Conjecture is a statement concerning the Galois action on torsion points of elliptic curves defined over number fields. In this talk, we formulate the conjecture and explain some of the difficulties in proving it.

Vlad Serban: *p-adic Manin-Mumford and Bianchi modular forms*

The Manin-Mumford Conjecture (a theorem by work of Raynaud et al.) states that a subvariety of a semiabelian variety containing a Zariski-dense set of torsion points must have a very special shape: it has to be the translate of a subgroup by a torsion point. We present an analogous result for suitable formal groups over a p-adic base and sketch an application to the study of p-adic families of cohomological automorphic forms for GL2 over an imaginary quadratic field.