Algebraic number theory
Théorie algébrique des nombres
(Org: **Imin Chen** (Simon Fraser), **Nuno Freitas** (Barcelona) and/et **Beth Malmskog** (Colorado))

ALEX BARRIOS, Carleton College
Elliptic curves with non-trivial isogeny

Let K be a field and suppose E and E' are isogenous non-isomorphic elliptic curves defined over K. Then there is an isogeny $\pi : E \to E'$ defined over K such that $\ker \pi \cong \mathbb{Z}/n\mathbb{Z}$ for some integer $n > 1$. In particular, the pair $(E, \ker \pi)$ is a non-cuspidal K-rational point of $X_0(n)$. When $n \geq 2$ and $X_0(n)$ has genus 0, we have the Klein-Fricke parameterizations which parameterize the j-invariants of the K-rational points of $X_0(n)$. By using these parameterizations, Cremona, Watkins, and Tsukazaki gave an algorithm to compute the isogeny class of an elliptic curve $E/\mathbb{Q}$. In this talk, we discuss an improvement of this algorithm by means of an explicit classification of isogeny graphs for elliptic curves $E/\mathbb{Q}$ that admit a non-trivial isogeny. We conclude by discussing joint work with Chimarro, Roy, Sahajpal, Tobin, and Wiersema, which uses this explicit classification to investigate how the Kodaira-Néron types of elliptic curves change under 2- or 3-isogeny.

ALINA COJOCARU, University of Illinois at Chicago
Bounds for the distribution of the Frobenius traces associated to abelian varieties

In 1976, Serge Lang and Hale Trotter conjectured the asymptotic growth of the number $\pi_A(x,t)$ of primes $p < x$ for which the Frobenius trace a_p of a non-CM elliptic curve $A/\mathbb{Q}$ equals an integer t. Even though their conjecture remains open, over the past decades the study of the counting function $\pi_A(x,t)$ has witnessed remarkable advances. We will discuss generalizations of such studies in the setting of an abelian variety $A/\mathbb{Q}$ of arbitrary dimension and we will present non-trivial upper bounds for the corresponding counting function $\pi_A(x,t)$. This is joint work with Tian Wang (University of Illinois at Chicago).

NIRVANA COPPOLA, Vrije Universiteit Amsterdam
Reduction types of genus 3 curves

The goal of this talk is to give a classification of the reduction of genus-3 curves whose automorphism group contains a subgroup isomorphic to the Klein group. We will first compute all possible reduction types, and then characterise when each case is attained in terms of invariants attached to the equation of a normalised model of the curve. This is joint work with I. Bouw, P. Kılıçer, S. Kunzweiler, E. Lorenzo García and A. Somoza Henares.

LASSINA DEMBELE, University of Luxembourg
Explicit Inertial Langlands correspondence for GL_2 and arithmetic applications

In this talk we will describe an algorithm for computing automorphic inertial types for GL_2. Then, we will give several arithmetic applications of this. (This is joint work with Nuno Freitas and John Voight.)

FRED DIAMOND, King's College London
Hecke correspondences and Kodaira-Spencer isomorphisms on Hilbert modular varieties

Kodaira-Spencer isomorphisms on classical modular curves relate differentials on the curve to those on the universal elliptic curve over it. I'll present a generalization that describes dualizing sheaves of integral models of Hilbert modular varieties with Iwahori level at p. I'll also describe properties of the associated degeneracy maps to prime-to-p level, including a relative cohomological vanishing result, with applications to the construction and properties of Hecke operators at p, mod p Galois representations, and integral models of Hilbert modular varieties.

LUIS DIEULEFAIT, Universitat de Barcelona
Potentially diagonalizable modular lifts of arbitrarily large weight

I will begin this talk by recalling the notion of "potential diagonalizability", and its role in Automorphy Lifting Theorems. Then I will present the main result of this talk, which is joint work with Iván Blanco: existence of modular lifts of arbitrarily large weight (of a given residual modular Galois representation) which are potentially diagonalizable. In the non-ordinary case, the proof of this result requires a combination of local and global results for Galois deformation rings, a local to global principle due to Böckle and a potential variant of the result we want to prove due to Barnet-Lamb, Gee, Geraghty and Taylor.

VALENTIJN KAREMAKER, Utrecht University
Polarisations of abelian varieties over finite fields via canonical liftings

In this talk we will give a widely applicable and computable description of polarisations of abelian varieties over finite fields. More precisely, we will describe all polarisations of all abelian varieties over a finite field in a fixed isogeny class corresponding to a squarefree Weil polynomial, when one variety in the isogeny class admits a canonical lifting to characteristic zero. The computability of the description relies on applying categorical equivalences between abelian varieties over finite fields and fractional ideals in étale algebras.

This is joint work with Jonas Bergström and Stefano Marseglia.

BENJAMIN MATSCHKE, Boston University
Proofs by several examples and stable combinatorial Nullstellensätze

The numerical Nullstellensatz (M. 2019) states in an explicit and practical manner that a polynomial vanishes on a non-empty irreducible variety if and only if it almost vanishes on a sufficiently generic point close to the variety. This yields the foundation of a valid proof by example method for algebraic statements. In this talk we present various extensions thereof based on a conceptual notion of when a set of examples is sufficiently generic. Besides theoretical and algorithmic criteria for sufficient genericity, we obtain several new types of Nullstellensätze in the spirit of the combinatorial Nullstellensatz and the Schwartz-Zippel lemma, also for varieties.

DAVID MCKINNON, University of Waterloo
Rational curves and rational points

Amongst curves, the mighty genus zero boasts the largest number of rational points. Can it be that these curves are always present when rational points are found in abundance?

It can.

In the talk, I'll discuss a number of cases in which we can actually prove statements like this, and a whole bunch more where we're pretty sure we *could* prove it, if only we were smarter.

FILIP NAJMAN, University of Zagreb
Quadratic points on bielliptic modular curves $X_0(n)$

Bruin and Najman, Ozman and Siksek and Box described all the quadratic points on the modular curves of genus $2 \leq g(X_0(n)) \leq 5$. Since all the hyperelliptic curves $X_0(n)$ are of genus ≤ 5 and as a curve can have infinitely many quadratic points only if it is either of genus ≤ 1, hyperelliptic or bielliptic, the question of describing the quadratic points on the bielliptic modular curves $X_0(n)$ naturally arises; this question has recently also been posed by Mazur.

We answer Mazur's question completely and describe the quadratic points on all the bielliptic modular curves $X_0(n)$, for which this has not been done already. The values of n that we deal with are $n = 60, 62, 69, 83, 89, 92, 94, 95, 101, 119$ and 131; the curves $X_0(n)$ are of genus up to 11. The two main methods we use is Box's relative symmetric Chabauty and an application of a moduli description of $\mathbb{Q}$-curves of degree d with an independent isogeny of degree m, which reduces the problem to finding the rational points on several quotients of modular curves. This is joint work with Borna Vukorepa.

RACHEL NEWTON, King's College London
Evaluating the wild Brauer group

The local-global approach to the study of rational points on varieties over number fields begins by embedding the set of rational points on a variety X into the set of its adelic points. The Brauer-Manin pairing cuts out a subset of the adelic points, called the Brauer-Manin set, that contains the rational points. If the set of adelic points is non-empty but the Brauer-Manin set is empty then we say there's a Brauer-Manin obstruction to the existence of rational points on X. Computing the Brauer-Manin pairing involves evaluating elements of the Brauer group of X at local points. If an element of the Brauer group has order coprime to p, then its evaluation at a p-adic point factors via reduction of the point modulo p. For p-torsion elements this is no longer the case: in order to compute the evaluation map one must know the point to a higher p-adic precision. Classifying p-torsion Brauer group elements according to the precision required to evaluate them at p-adic points gives a filtration which we describe using work of Bloch and Kato. Applications of our work include addressing Swinnerton-Dyer's question about which places can play a role in the Brauer-Manin obstruction. This is joint work with Martin Bright.

EKIN OZMAN, Bogazici University
Quadratic Points on Modular Curves and Fermat-type Equations

Understanding solutions of Diophantine equations over rationals or more generally over any number field is one of the main problems of number theory. By the help of the modular techniques used in the proof of Fermat's last theorem by Wiles and its generalizations, it is possible to solve other Diophantine equations too. Understanding quadratic points on the classical modular curve plays a central role in this approach. In this talk, I will mention some recent results about these notions.

ANWESH RAY, University of British Columbia
Rational points on algebraic curves in infinite towers of number fields

We study a natural question in the Iwasawa theory of algebraic curves of genus > 1.

Let X be a smooth, projective, geometrically irreducible curve X defined over a number field K of genus $g > 1$, such that the Jacobian has good ordinary reduction at the primes above p. Fix an odd prime p and for any integer $n > 1$, let K_n denote the degree-p^n extension of K contained in $K(\mu_{p^{n+1}})$. We prove explicit results for the growth of $\#X(K_n)$ as $n \to \infty$. When the Jacobian of X has rank zero and the associated adelic Galois representation has big image, we prove an explicit condition under which $X(K_n) = X(K)$ for all n. We show that this condition is satisfied for 100% of primes p at which the Jacobian of X has good ordinary reduction.

RENATE SCHEIDLER, University of Calgary
Constructing Imaginary Quadratic Fields with Large n-Class Rank

Constructing imaginary quadratic fields whose ideal class groups have large n-rank is a challenging practical problem, due in part because heuristically and experimentally such examples are very rare. One of the most successful methods for producing many fields of relatively small discriminant with large 3-class rank is due to Diaz y Diaz dating back to the 1970s. His technique formed the basis of the approach used by Quer in 1987 to find three fields with 3-class rank equal to 6, which still stands as the current record. We describe generalizations to this method to allow the construction of fields with large n-class rank for any positive odd integer n. An extensive search using our new algorithm in conjunction with a variety of further practical improvements produced billions of fields with non-trivial p-class rank for the primes $p = 3, 5, 7, 11$ and 13, and a large volume of fields with high p-class ranks and unusual p-class group structures. Our numerical results include a field with 5-class rank equal to 4 with the smallest absolute discriminant discovered to date and the first known examples of imaginary quadratic fields with 7-rank equal to 4. This is joint work with Christian G. Bagshaw, Michael J. Jacobson, Jr. and Nickolas Rollick.

PADMAVATHI SRINIVASAN, University of Georgia

Computing nonsurjective primes associated to Galois representations of abelian surfaces

Let A be a principally polarized abelian surface over the rational numbers. Serre proved that there are finitely many primes ℓ for which the Galois action on the ℓ-torsion points of A is not surjective on to the group of symplectic similitudes $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Dieulefait showed that this finite set is effectively computable, conditional on Serre's conjecture (now a theorem of Khare and Wintenberger). I will report on ongoing joint work with Banwait, Brumer, Kim, Klagsbrun, Mayle and Vogt where we implement this algorithm and use it to compute nonsurjective primes for all genus 2 curves in the LMFDB.