Fabrizio Andreatta (Milan)

Nearly overconvorgent forms and p-adic L functions

In this talk I will present the approach proposed by A. Iovita and myself for the construction of the p-adic analogue of the nearly holomorphic elliptic modular forms. I will provide applications to the constructions of p-adic L-functions.

Alex Bartel (Glasgow)

The Cohen–Lenstra–Martinet heuristics on class groups of "random" number fields

In the 1980s Cohen and Lenstra proposed a probabilistic model for class groups of quadratic number fields. A few years later, Cohen and Martinet extended that model to much more general families of number fields. To date, only very few instances of these heuristics have been proven. In this talk I will present joint work with Hendrik Lenstra, in which we disprove the Cohen–Martinet heuristics in two different ways and propose corrections.

Laurent Berger (Lyon)

Iterated extensions and p-adic dynamical systems

Let K be a p-adic field and let P be a polynomial with coefficients in K. Consider the extension of K obtained by adjoining a compatible sequence of roots of the iterates of P (for example, the cyclotomic extension of K is obtained in this way). I will discuss the arithmetic of some of these extensions. Along the way, we'll see a generalization of Coleman power series, as well as some p-adic dynamical systems.

Pierre Charollois (Jussieu)

Felder-Varchenko modular forms and applications to cubic fields

We prove a variant of a modular identity of Felder-Varchenko (2005) owing its origin to mathematical physics. We will explain why the new class of functions that occurs should be promoted as some kind of "modular units for SL3(Z)", as was anticipated by Eisenstein as early as 1844.

Huayi Chen (Paris 7)

Comparison between slopes and minima

The successive minima are classic invariants in the geometry of numbers. The successive slopes are invariants of Euclidean lattices (or more generally Hermitian vector bundles), which are constructed in inspiring by the geometry of vector bundles on a projective curve. In this talk, I will explain the comparison of these invariants, based on the $\mathbb{R}$-filtration approach.

Vladimir Dokchitser (KCL)

Parity of the Mordell-Weil rank of an abelian surface

The Birch-Swinnerton-Dyer conjecture famously predicts that the rank of an elliptic curve or of an abelian variety agrees with the order of the zero at s=1 of its L-function. I will explain that the conjecture correctly gives the parity of the rank in the case of semistable abelian surfaces, assuming finiteness of the Tate-Shafarevich group and the analytic continuation and functional equation of the L-function. This is joint work with Celine Maistret.

Sary Drappeau (Aix-Marseille)

Combinatorial identities and Titchmarsh's problem for multiplicative functions

In joint work with B. Topacogullari (Lausanne) we discuss the extent to which generalized divisor functions can be brought within the scope of combinatorial methods. We apply this to Titchmarsh's divisor problem of estimating the shifted convolution sum $\sum_{p\leq x} d(p+1)(d(n)$ being the number of divisors of n), replacing primes by other sets of arithmetic interest.

Tom Fisher (Cambridge)

Computing the Cassels-Tate pairing

Computing the n-Selmer group of an elliptic curve gives an upper bound for its Mordell-Weil rank. This upper bound coming from n-descent may not be sharp if the elliptic curve has non-trivial Tate-Shafarevich group. Computing the Cassels-Tate pairing on the n-Selmer group improves the upper bound for the rank from that coming from n-descent to that coming from n^2-descent. An efficient method for computing the pairing on 2-Selmer groups was found and implemented in Magma by Steve Donnelly. I will report on ongoing work attempting to generalise his methods to 3-Selmer groups. One problem that arises in this context is the following: Given two 9-dimensional central simple algebras over Q (specified by structure constants) that are known to be isomorphic, how can we find such an isomorphism explicitly?

Dimitris Koukoulopoulos (Montréal)

Is a random polynomial irreducible?

Given a "random" polynomial over the integers, it is expected that, with high probability, it is irreducible and has a big Galois group over the rationals. Such results have been long known when the degree is bounded and the coefficients are chosen uniformly at random from some interval. Less is known when the coefficients are bounded and the degree goes to infinity, with the prototypical example being polynomials with plus-minus 1 coefficients. In this talk, I will discuss the history around these problems, and I will present some recent progress towards them, joint with Lior Bary-Soroker and Gady Kozma.

Holly Krieger (Cambridge)

A dynamical approach to common torsion points

Bogomolov-Fu-Tschinkel conjectured that there is a uniform upper bound on the number of common torsion points of two nonisomorphic elliptic curves (more precisely, on the number of common images of torsion points when the curve is presented as a double cover of the Riemann sphere). I will discuss a dynamical approach to this conjecture via Lattès maps of the Riemann sphere associated to an elliptic curve. I will report on recent progress on this dynamical approach (joint with Laura DeMarco and Hexi Ye) and formulate a more general dynamical conjecture.

Youness Lamzouri (York)

On the distribution of the maximum of exponential and Kloosterman sums

In this talk, we shall present recent results concerning the distribution of the maximum of partial sums of certain cubic exponential sums, commonly known as "Birch sums". The proofs use a blend of probabilistic methods, Fourier analytic techniques, and deep tools from algebraic geometry. We also discuss ongoing work with D. Bonolis, where we obtain similar results for the maximum of partial sums of Kloosterman sums. As an application, we exhibit large values of partial sums of Birch and Kloosterman sums, which we believe are best possible.

Jaclyn Lang (Max Planck)

Images of GL2-type Galois representations

There is a general philosophy that the image of a Galois representation should be as large as possible, subject to the symmetries of the geometric object from which it arose. This can be seen in Serre's open image theorem for non-CM elliptic curves, Ribet and Momose's work on Galois representations attached to modular forms, and recent work of the speaker and Conti, Iovita, Tilouine on Galois representations attached to Hida and Coleman families of modular forms. Recently, Bellaiche developed a way to measure the image of an arbitrary Galois representation taking values in GL2 of a local ring A. Under the assumptions that A is a domain and the residual representation is not too degenerate, we explain how the symmetries of such a representation are reflected in its image. This is joint work with Andrea Conti and Anna Medvedovsky.

Robert Lemke Oliver (Tufts)

Counting finite towers of number fields

From work of Bhargava and Cohen–Diaz y Diaz–Olivier, it follows that while "most" quartic extensions of the rationals have Galois group S_4, roughly 20% have the smaller Galois group D_4 when ordered by discriminant. This can be explained by the fact that a D_4 quartic field arises as the generic relative quadratic extension of a quadratic field. Klüners generalized this by counting fields that arise as the relative quadratic extension of any class of number fields that is not unexpectedly large when ordered by discriminant.

In joint work with Jiuya Wang and Melanie Matchett Wood, we generalize this idea further, counting fields that arise either as relative abelian or relative cubic extensions of any not unexpectedly large family of number fields. This verifies many new cases of Malle's conjecture and, in some cases, provides new classes of counterexamples. We also indicate how our approach may be used to obtain nontrivial bounds on the average sizes of specified torsion in class groups.

Florian Luca (Witwatersrand)

Variations on the largest prime factor of Fibonacci numbers

Let $\{F_n\}_{n\geq 0}$ be the Fibonacci sequence. For an integer m, let $P(m)$ be the largest prime factor of m (with $P(0) = P(\pm 1) = 1$). Carmichael showed in **1913** that $P(F_n) \geq n-1$. This was improved exactly 100 years later by C. L. Stewart who proved that $P(F_n) > n\exp(\log n/(104\log\log n))$ for n sufficiently large, which in particular settled a conjecture of Erdős. In my talk, I will look at the largest prime factor of expressions involving Fibonacci numbers and variations of them such as $P(F_n + m!)$, $P(F_m + F_n)$, $P(F_n^{(k)})$ and $P(F_m^{(k)} + F_n^{(k)})$, where $\{F_n^{(k)}\}_{n\geq 0}$ is the k-order linear recurrence having the first $k-1$ terms equal to 0 and the kth term equal to 1 and in which each term is the sum of the previous k terms. These results have been obtained jointly with my former Ph.D. students J. J. Bravo, C. A. Gómez and S. Gúzman.

Steven Miller (Williams College)

From the Manhattan Project to Elliptic Curves

Physicists developed Random Matrix Theory (RMT) in the 1950s to explain the energy levels of heavy nuclei. A fortuitous meeting over tea at the Institute in the 1970s revealed that similar answers are found for zeros of L-functions, and since then RMT has been used to model their behavior. The distribution of these zeros is intimately connected to many problems in number theory, from how rapidly the number of primes less than X grows to the class number problem to the bias of primes to be congruent to 3 mod 4 and not 1 mod 4. We report on recent progress on understanding the zeros near the central point, emphasizing the advantages of some new perspectives and models. We end with a discussion of elliptic curves. We'll mix theory and experiment and see some surprisingly results, which lead us to conjecture that a new random matrix ensemble correctly models the small conductor behavior.

Yiannis Petridis (UCL)

Arithmetic Statistics of modular symbols

Modular symbols have been a useful tool to study the space of holomorphic cusp forms of weight two, and the homology of modular curves. They have been the object of extensive investigations by many mathematicians including Birch, Manin, and Cremona. Mazur, Rubin, and Stein have recently formulated a series of conjectures about statistical properties of modular symbols in order to understand central values of twists of elliptic curve L-functions. Two of these conjectures relate to the asymptotic growth of the first and second moments of the modular symbols. In joint work with Morten S. Risager we prove these on average using analytic properties of Eisenstein series twisted with modular symbols. We also prove another conjecture predicting the Gaussian distribution of normalized modular symbols ordered according to the size of the denominator of the cusps.

Siddarth Sankaran (Manitoba)

Green forms for special cycles

This is joint work with Luis Garcia. We use Quillen's superconnection formalism to construct natural families of Green forms for special cycles on Shimura varieties of orthogonal or unitary type, and study their basic properties. In addition, for certain Shimura varieties, we identify the integral of a Green form as the non-holomorphic part of the derivative of an Eisenstein series evaluated at a special point; this confirms the "non-holomorphic" part of Kudla's conjectural formula for the arithmetic volumes of special cycles in arithmetic Chow groups.

Will Sawin (Columbia/Clay)

L-functions of Dirichlet character twists over function fields

This talk will give an introduction to L-functions over function fields and their unusual properties. Specifically, I will discuss their connection to (random) unitary matrices. I will conclude with new results on the L-functions of elliptic curves (and other Galois representations) over function fields twisted by Dirichlet characters ramified at a single place.

Damaris Schindler (Utrecht)

Diophantine inequalities for ternary diagonal forms

We discuss small solutions to ternary diagonal inequalities of any degree where all of the variables are assumed to be of size P. We study this problem on average over a one-parameter family of forms and discuss a generalization of work of Bourgain on generic ternary diagonal quadratic forms to higher degree. In particular we discuss how these Diophantine inequalities are related to counting rational points close to varieties.

Arul Shankar (Toronto)

Heuristics for counting number fields

A foundational question in arithmetic statistics is: how many degree-n field extensions of $\mathbb{Q}$ exist with discriminant bounded by X? This question has been answered for $n = 3$ by Davenport and Heilbronn and for $n = 4$ and 5 by Bhargava. Furthermore, conjectures of Malle and Bhargava posit an answer for all integers n, at least when we restrict to number fields whose normal closure have Galois group S_n over $\mathbb{Q}$.

In this talk, we will present joint work with Jacob Tsimerman, which gives new theoretical evidence towards this conjecture. Along the way, we also give an elementary proof of the Davenport–Heilbronn result on counting cubic fields.

Vinayak Vatsal (UBC)

Uniqueness of theta series

I describe work in progress with Dimitar Jetchev and Jon Hanke on a proof of a result due to Schiemann, which states that a ternary integral quadratic form is determined by its representation numbers. The argument uses a detailed analysis of Waldspurger's correspondence to produce relations amongst theta series and Mumford's theory of algebraic theta functions to recover the quadratic form, once enough relations are obtained.

Stefano Vigni (Genova)

On Kolyvagin's conjecture and the Bloch-Kato formula for modular forms

A few years ago, Wei Zhang proved (under certain assumptions) Kolyvagin's conjecture on the non-triviality of his system of cohomology classes built out of the Euler system of Heegner points on a rational elliptic curve. This led him to a proof of the p-part of the Birch and Swinnerton-Dyer formula in analytic rank one. In this talk I will describe an analogue of Kolyvagin's conjecture for Heegner cycles on Kuga-Sato varieties and state the p-part of the Bloch-Kato formula for higher (even) weight modular forms in analytic rank one. Time permitting, I will briefly sketch our strategy of proof of these results. This is joint work (in progress) with Matteo Longo and Daniele Masoero.

Michel Waldschmidt (Jussieu)

Generalization of the Landau–Ramanujan constant for sums of two squares to other binary forms

Let $F \in \mathbb{Z}[X, Y]$ be a binary form with integer coefficients, non-zero discriminant, and degree d. As $N \to \infty$, the number of integers $m \in \mathbb{Z}$, $|m| \leq N$ which are representable by F is asymptotically $C_F N(\log N)^{-1/2}$ if $d = 2$ and $C_F N^{2/d}$ if $d \geq 3$ (Stewart – Yao Xiao). For the quadratic form $F(X, Y) = X^2 + Y^2$, the constant C_F is the so–called Landau–Ramanujan constant.

In a joint work with Etienne Fouvry and Claude Levesque, we consider cyclotomic binary forms, which are the homogeneous versions of the cyclotomic polynomials.

David Zywina (Cornell)

Computing ℓ-adic monodromy groups

Fix a prime ℓ and an abelian variety A over a number field. The Galois action on the torsion points of A can be described by an ℓ-adic Galois representation. The Zariski closure G of its image is called the ℓ-adic monodromy group of A. The group G encodes a lot of the arithmetic/geometry of A. For example, the Sato–Tate distribution of A can conjecturally be determined from G.

We will discuss approaches to studying and computing these monodromy groups.