Barcelona Fall Workshop on NUMBER THEORY II

ABSTRACTS

Isomorphisms of modular Galois representations and graphs

Samuele Anni (Univ. Aix-Marseille)

In this talk I will explain how to effectively test whether two modular Galois representations of the absolute Galois group of the rationals are isomorphic. In particular, I will present sharp bounds on the number of traces to test, as well as a database of modular Galois representations. In the end, as an application, I will briefly discuss about graphs of isomorphisms and the related results on Hecke algebras.

Dihedral Galois representations and CM forms.

Nicolas Billerey (Univ. Clermond-Ferrand)

Starting from congruences modulo 23 of Ramanujan's tau function, we discuss the question to decide whether a given dihedral mod l Galois representation arises from a CM form with prescribed optimal type. Joint work with Filippo Nuccio.

Formal theorem proving with a view towards Diophantine equations.

Sander R. Dahmen (VU Amsterdam)

Proof assistants, such as Coq, Isabelle, or Lean, are software tools which assist in rigorously expressing mathematical statements and their proofs in a formal logical language. The mathematics that has been formalized this way ranges from purely theoretical results to algorithmic ones. We will discuss several such results, including recent joint work with Hölzl and Lewis on the formalization of the Cap Set Problem in Lean. We also turn to effective methods for solving Diophantine equations, and discuss the desirability and possibilities to formalize aspects of these.

A geometric Serre weight conjecture.

Fred Diamond (King's College London)

Serre's Conjecture, now a theorem of Khare and Wintenberger, asserts that every odd, irreducible two-dimensional mod p representation of the absolute Galois group of Q arises from a modular form, and the "weight part" of the conjecture determines the minimal weight of such a form. More general Serre weight conjectures have been formulated for Galois representations associated to automorphic forms, but only in the context of regular algebraic weights. I'll discuss a geometric variant for Hilbert modular forms that allows irregular weight. I'll explain some new features, and the reason a naive version of the conjecture is false. I'll also discuss the proof in some cases involving partial weight one, and some connections with the geometry of Hilbert modular varieties. This is joint work with Shu Sasaki.

Implementing Algorithms to Compute Elliptic Curves Over $\mathbb{Q}$.

Adela Gherga (UBC Vancouver)

Let S be a set of rational primes and consider the set of all elliptic curves over $\mathbb{Q}$ having good reduction outside S and bounded conductor N. Currently, using modular forms, all such curves have been determined for $N \leq 500000$, the bulk of this work being attributed to Cremona.

Early attempts to tabulate all such curves often relied on reducing the problem to one of solving a number of certain integral binary forms called Thue-Mahler equations. These are Diophantine equations of the form $F(x, y) = u$, where F is a given binary form of degree at least 3 and u is an S-unit. A theorem of Bennett-Rechnitzer shows that the problem of computing all elliptic curves over $\mathbb{Q}$ of conductor N reduces to solving a number of Thue-Mahler equations. To resolve all such equations, there exists a practical method of Tzanakis-de Weger using bounds for linear forms in p-adic logarithms and various reduction techniques. In this talk, we describe our refined implementation of this method and discuss the key steps used in our algorithm.

Congruences for sporadic sequences and modular forms for non-congruence subgroups.

Matija Kazalicki (University of Zagreb)

In 1979, in the course of the proof of the irrationality of $\zeta(2)$ Apéry introduced numbers $b_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}$ that are, surprisingly, integral solutions of recursive relations

$$(n+1)^2 u_{n+1} - (11n^2 + 11n + 3)u_n - n^2 u_{n-1} = 0.$$

Zagier performed a computer search on first 100 million triples $(A, B, C) \in \mathbb{Z}^3$ and found that the recursive relation generalizing b_n

$$(n+1)u_{n+1} - (An^2 + An + B)u_n + Cn^2 u_{n-1} = 0,$$

with the initial conditions $u_{-1} = 0$ and $u_0 = 1$ has (non-degenerate i.e. $C(A^2 - 4C) \neq 0$) integral solution for only six more triples (whose solutions are so called sporadic sequences) .

Stienstra and Beukers showed that the for prime $p \geq 5$

$$b_{(p-1)/2} \equiv \begin{cases} 4a^2 - 2p \pmod{p} \text{ if } p = a^2 + b^2, \text{ a odd} \\ 0 \pmod{p} \text{ if } p \equiv 3 \pmod{4}. \end{cases}$$

Recently, Osburn and Straub proved similar congruences for all but one of the six Zagier's sporadic sequences (three cases were already known to be true by the work of Stienstra and Beukers) and conjectured the congruence for the sixth sequence (which is a solution of recursion determined by triple $(17, 6, 72)$.

In this talk we prove that remaining congruence by studying Atkin and Swinnerton-Dyer congruences between Fourier coefficients of certain cusp form for non-congruence subgroup.

Quadratic Chabauty for nonsplit Cartan modular curves.

Samuel Le Fourn (Univ. Grenoble Alpes)

In a famous recent paper, Balakrishnan, Dogra, Müller, Tuitman and Vonk managed to prove that the modular curve $X_{ns}^{+}(13)$ did not have non-CM rational points, through so-called quadratic Chabauty method. This method requires sophisticated conditions to effectively be applied (in particular, complete knowledge of the rank of the rational points of the Jacobian). In this talk, I will explain a joint work with Netan Dogra allowing to weaken the hypotheses of quadratic Chabauty and to apply it unconditionally in the context of nonsplit Cartan modular curves, leading in itself to an explicit bound on the number of their rational points.

Images of residual Galois representations of elliptic curves without CM.

Pedro Lemos (University College London)

It is a fact that when p is a prime larger than 37, the image of the Galois representation modulo p of an elliptic curve defined over the rationals and without complex multiplication is either the whole of $\mathrm{GL}_2(\mathbb{F}_p)$, or is contained in the normaliser of a non-split Cartan subgroup. In this talk, I will show that, in the case where the representation is not surjective, this image must, in fact, be the whole normaliser of a non-split Cartan subgroup. This is joint work in progress with Samuel Le Fourn.

Uniform Kummer theory for elliptic curves over $\mathbb{Q}$.

David Lombardo (Univ. di Pisa)

Let K be a number field and $\alpha \in K^{\times}$. Kummer theory shows that the Galois group G_n of $K(\zeta_n, \sqrt[n]{\alpha})$ over $K(\zeta_n)$ is canonically isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$; moreover, if α is not a root of unity, the index $(\mathbb{Z}/n\mathbb{Z} : G_n)$ is uniformly bounded as n varies. Equivalently, there exists a constant $d(K, \alpha) > 0$ such that for all $n \geq 1$ we have $[K(\zeta_n, \sqrt[n]{\alpha})/K(\zeta_n)] \geq d(K, \alpha) \cdot n$. The nature of the constant $d(K, \alpha)$ is well-understood in terms of arithmetical properties of α.

A natural generalisation of Kummer theory can be obtained by considering a commutative algebraic group $\mathcal{A}$ defined over K, a rational point $\alpha \in \mathcal{A}(K)$, and the tower of extensions $K \subseteq K(\mathcal{A}[n]) \subseteq K(\mathcal{A}[n], \frac{1}{n}\alpha)$: this reduces to the classical case by taking $\mathcal{A} = \mathbb{G}_m$. In this talk I will discuss the case where $\mathcal{A}$ is an elliptic curve E, and show that if E is defined over $\mathbb{Q}$ we have

$$[\mathbb{Q}(E[n], \frac{1}{n}\alpha) : \mathbb{Q}(E[n])] \geq cn^2,$$

where c is now an *absolute* constant, independent of E and α, provided only that α is not divisible by any $k > 1$ in the free abelian group $E(\mathbb{Q})/\text{torsion}$.

This is joint work with Sebastiano Tronto (Université du Luxembourg).

Modularity of elliptic curves over totally real cubic fields.

Filip Najman (University of Zagreb)

We will prove that all elliptic curves over totally real cubic fields are modular and explain the ingredients that go into this proof. This is joint work with Maarten Derickx and Samir Siksek.

Diophantine applications of Serre's modularity conjecture.

George Turcas (IMAR Bucharest)

Successful resolutions of Diophantine equations over $\mathbb{Q}$ via Frey elliptic curves and modularity rest on three pillars: Mazur's isogeny theorem, modularity of elliptic curves defined over $\mathbb{Q}$ and Ribet's level-lowering theorem. One can replace the last two with Serre's modularity conjecture over $\mathbb{Q}$, now a theorem due to Khare and Wintenberger. For general number fields K, there's no analogue of Mazur's isogeny theorem, but there is a formulation of Serre's modularity conjecture. In this talk, we will show how one can use the latter for showing that certain Diophantine equations do not have solutions in K.

Integral presentations of $GL(n) * GL(2)$ ***Rankin-Selberg L-functions and applications.***

Jeanine van Order (Univ. Bielefeld)

Central and critical values of Rankin-Selberg L-functions for $GL(n)*GL(2)$ (for $n \geq 2$) play a major underlying role in arithmetic geometry, starring in the conjectures Birch-Swinnerton-Dyer, Iwasawa-Greenberg, and Deligne, not to mention various open conjectures in the analytic theory of automorphic forms. I would like to explain how several features of the underlying representation theory, particularly the surjectivity of the archimedean local Kirillov map and a certain classical projection operator (used e.g. to establish converse theorems) lead to novel integral presentations of these values as the constant coefficients of certain L^2-automorphic forms on the mirabolic subgroup of $GL(2)$. Making a suitable extension to $GL(2)$ then gives a convenient re-interpretation of such values, for instance to study central critical values in families. In this latter setting, I will explain a novel approach to deriving nonvanishing estimates via spectral decompositions of Eisenstein series, as well as the relation to recent progress on Deligne's conjecture for automorphic motives, and (if time permits) the potential to give new constructions of p-adic interpolation series.

POSTERS

Quadratic points on modular curves, Josha Box

Torsion groups of elliptic curves defined over number fields with rational j-invariant, Tomislaw Gužvić.

Effective irreducibility of residual Galois representations of abelian surfaces with RM over $\mathbb{Q}$ computationally., Timo Keller

Torsion groups of elliptic curves over infinite Abelian extensions of $\mathbb{Q}$, Ivan Krijan

Local obstructions to S-unit equations, Eduardo Soto.

Torsion subgroups of elliptic curves over cubic number fields, Antonella Trbović

Torsion groups of rational elliptic curves over some cyclotomic fields, Borna Vukorepa

More information on the program at http://stnb.cat.