Algebraic and explicit methods in number theory

Laboratoire de mathématiques de Besançon
23-27 September 2013

Bruno Anglès, Université de Caen

Nombres de Bernoulli en caractéristique positive

À l'aide de certaines fonctions L à plusieurs variables introduites récemment par F. Pellarin, nous présenterons de nouvelles propriétés pour les nombres de Bernoulli-Carlitz. Cet exposé est basé sur un travail en commun avec F. Pellarin.

Werner Bley, Universität München

Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions

Let A be an abelian variety over a number field k and F a finite cyclic extension of k of p-power degree for an odd prime p. Under certain technical hypotheses, we obtain a reinterpretation of the equivariant Tamagawa number conjecture ('eTNC') for A, F/k and p as an explicit family of p-adic congruences involving values of derivatives of the Hasse-Weil L-functions of twists of A, normalised by completely explicit twisted regulators. This reinterpretation makes the eTNC amenable to numerical verification and furthermore leads to explicit predictions which refine well-known conjectures of Mazur and Tate.

This is a report on joint work with Daniel Macias Castillo.

Alberto Cámara, Université de Franche-Comté

Higher local fields and Functional Analysis

Jean-Marc Couveignes, Université Bordeaux 1

(Pseudo)-primality testing with ring extensions

Joint work with Tony Ezome. The ring $\mathbb{Z}/n\mathbb{Z}$ and its extensions have different properties depending on whether n is prime or composite. I will explain the role played by these extensions in the study of primality, following work by various authors.

Agnès David, Université du Luxembourg

Computing multiplicities in the Breuil-Mézard Conjecture

Let $\overline{\rho}$ be a 2-dimensional, modulo p, continuous representation of the absolute Galois group of a finite unramified extension of $\mathbb{Q}_p$.

The Breuil–Mézard Conjecture describes geometric properties of potentially semistable deformation rings of $\overline{\rho}$ in terms of representation theoretical data and some integers, called the modular multiplicities.

I will present a method and an algorithm to compute these modular multiplicities. Our first results for fields of small degree indicate new geometric phenomena.

This is a work in progress with X. Caruso and A. Mézard.

Chantal David, Concordia University

Groups of points of abelian surfaces over finite fields

Let A be an abelian surface over the finite field $\mathbb{F}_q$. The rational points on A over $\mathbb{F}_q$ form an abelian group $A(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}$. We are interested in determining which groups actually occur as the group of points of an abelian surface over $\mathbb{F}_q$. A characterization of these groups for abelian varieties of any dimension in terms of the characteristic polynomial of the Frobenius endomorphism was found recently by Rybakov. Using this characterization for the case of abelian surfaces, we show that "very split" groups (i.e. when n_1, n_2 are large compared to n_3, n_4) are less likely to occur, by relating this question to the uniform distribution modulo one of $n_2^{1/2}n_3n_4^{1/2}$. This is compatible with the general philosophy of the Cohen-Lenstra heuristics, which predict that random abelian groups naturally occur with probability inversely proportional to the size of their automorphism groups.

This is joint work with D. Garton, Z. Scherr, A. Shankar, E. Smith and L. Thompson.

Christine Huyghe, Université de Strasbourg

Some examples of computations of (φ, Γ)-modules coming from geometry

This is joint work with Nathalie Wach.

It is usually a difficult question to explicitely compute a (φ, Γ)-module attached to the p-adic tale cohomology of some scheme over a finite field. I will explain two families of examples where this can be achieved : the case of hyperelliptic curves, that uses a rigid cohomology computation due to Kedlaya, and the mod p case for Drinfeld curves, which uses Deligne-Illusie morphism.

Rafe Jones, Carleton College

Post-critically finite rational functions over number fields

Kristin Lauter, Microsoft Research, Cryptography Group

Genus 2 curves in cryptography

Henri Lombardi, Université de Franche-Comté

General Methods in Constructive Algebra for deciphering noneffective proofs

Nicolas Mascot, Université Bordeaux 1

Computing modular Galois representations

We will see how to quickly compute a coefficient of a newform by using a Galois representation. We will show how to do so in time polynomial in the level, by using a half-algebraic, half-numerical method.

Aurel Page, Université Bordeaux 1

Computing Kleinian modular forms

Kleinian modular forms are the analogues of classical modular forms when the hyperbolic half-plane is replaced with the hyperbolic half-space. We will describe an algorithm for computing spaces of such forms and explain their relations with automorphic forms for GL(2) over certain number fields.

Francesco Pappalardi, Università Roma Tre

Properties of reductions of groups of rational numbers

Let Γ be a multiplicative subgroup of $\mathbf{Q}^*$ and let p be a prime for which the valuation $v_p(x) = 0$ for every $x \in \Gamma$. Then the group $\Gamma_p = \{x \pmod p \ : \ x \in \Gamma\}$ is a well defined subgroup of $\mathbf{F}_p^*$. We will consider various properties of Γ_p as p varies and propose various results in analogy with the old Artin Conjecture for Primitive roots

---

Sandra Rozensztajn, UMPA, ENS de Lyon

Asymptotic modular multiplicities for GL_2 and the Breuil-Mézard conjecture

---

Peter Stevenhagen, Universiteit Leiden

Galois groups as arithmetic invariants

We discuss to which extent number fields are determined by their absolute abelian Galois group.

Lara Thomas, Université de Franche-Comté

Serre weights and ramification jumps for mod p Galois representations

---

Firmin Varescon, Université de Franche-Comté

Calcul de la $\mathbb{Z}_p$-torsion de $\mathfrak{X}$

Soient p un nombre premier et K un corps de nombres. On désigne par M la pro-p-extension abélienne non ramifiée en dehors de p, maximal de K. Dans cet exposé je vais étudier la torsion du $\mathbb{Z}_p$-module $\mathfrak{X} = \mathrm{Gal}(M/K)$ et présenter une méthode qui détermine effectivement les facteurs invariants de ce p-groupe fini. Ensuite je donnerai quelques résultats numériques et j'expliquerai comment les interpréter dans la philosophie des heuristiques à la Cohen-Lenstra.

Mark Watkins, University of Sidney

Ranks of quadratic twists of elliptic curves

Consider the family of quadratic twists: $y^2 = x^3 - D^2x$. Is the rank is this family bounded? There are competing conjectures, but one has to propose a growth rate to make an experimental test.

We report on a huge amount of experimental data that has been computed. We had three goals: find as many D up to 2^{60} with rank 6 or more, find as many D with rank 7 as possible, and to try to find a rank 8 example.

Gabor Wiese, Université du Luxembourg

On symplectic Galois representations and the inverse Galois problem

We give an account of joint work with Sara Arias-de-Reyna, Luis Dieulefait and Sug Woo Shin, in which we realise, for every even n and every d, the group $PGSp_n(\mathbb{F}_{p^d})$ or $PSp_n(\mathbb{F}_{p^d})$ as Galois group over the rationals, for p in a set of primes of positive density. The proof relies on compatible systems of automorphic Galois representations with special local properties.

In the beginning of the talk the overall strategy will be outlined, starting from previous joint work with Dieulefait on the 2-dimensional case. We will then explain the existence of a minimal global field such that almost all the residual representations of a compatible system can be defined projectively over its residue fields. Moreover, we shall present a very simple classification of symplectic representations containing a nontrivial transvection in their image. Finally, we shall report on the existence of the desired compatible system and how to use level lowering techniques to obtain our application to the inverse Galois problem.