Théorie des Nombres et Applications

CIRM

10 mars - 14 mars 2014

Résumés

Eva Bayer
Euclidean number fields and Euclidean minima
This is a joint work with Piotr Maciak. The study of Euclidean number fields and Euclidean minima is a classical topic of number theory. The aim of this talk is to give a (brief) survey of this subject, to present some new results and perspectives, especially concerning upper bounds for Euclidean minima. In particular, joint results with Piotr Maciak concerning Euclidean minima of abelian number fields of prime power conductor will be presented.

Laurent Berger
Sen theory and locally analytic vectors
I will explain how the theory of locally analytic vectors allows us to generalize Sen theory to extensions whose Galois group is a Lie group of any dimension (joint work with Pierre Colmez).

Nicolas Billerey
Sur la modularité des représentations galoisiennes réductibles
Dans cet exposé, je donnerai un résultat de modularité concernant les représentations galoisiennes réductibles. Par analogie avec le cas des représentations irréductibles, j'énoncerai dans ce contexte plusieurs questions concernant la caractérisation et l'optimisation des différents types de formes modulaires attachées à une représentation donnée. Enfin, je donnerai une application de ces résultats à la détermination d'une borne inférieure explicite pour le degré maximal du corps de coefficients des formes modulaires nouvelles de niveau premier et de caractère trivial. Il s'agit d'un travail en collaboration avec Ricardo Menares.

Francois Brunault
Valeurs non critiques de fonctions L de variétés abéliennes modulaires
Dans cet exposé, j'expliquerai l'énoncé et les ingrédients de la preuve d'une version équivariante des conjectures de Beilinson pour les valeurs non critiques des fonctions L des variétés abéliennes modulaires. La preuve utilise le théorème de Beilinson pour une courbe modulaire convenable et un résultat de modularité pour l'algèbre des endomorphismes d'une telle variété abélienne. Je mentionnerai également les conséquences de ce théorème pour les Q-courbes.

Alberto Camara
Functional analysis on arithmetic two-dimensional local fields
The two-dimensional local fields arising from an arithmetic surface always come equipped with an embedding of a local field into them. We will discuss the resulting vector space from the point

of view of the theory of p-adic locally convex spaces. We will also discuss what new phenomena appear and some new approaches to the study of higher local fields.

Xavier Caruso
Sur quelques espaces de déformations potentiellement Barsotti-Tate
Les espaces de déformations galoisiennes jouent un rôle central dans la résolution de nombreuses questions de géométrie arithmétique (en lien, notamment, avec les théorèmes de modularité qui entrent dans la lignée directe des travaux de Wiles). Cependant, hormis dans certains cas particuliers, il est généralement très difficile de déterminer explicitement ces espaces de déformations. Dans cet exposé, je présenterai une méthode, basée sur la théorie de Hodge p-adique, pour calculer les espaces de déformations qui paramètrent certaines classes de représentations p-adiques de dimension 2 du groupe de Galois absolu de $\mathbb{Q}_{p^f}$ qui sont « modérément potentiellement Barsotti–Tate » dans le sens où elles proviennent d'un groupe p-divisible sur une extension finie modérément ramifiée. Il s'agit d'un travail en cours avec Agnès David et Ariane Mézard.

Pierre Charollois
Cocycles sur GL_n et valeurs spéciales de fonctions zêta p-adiques
En raffinant un travail antérieur de Sczech, nous construisons un cocycle explicite à valeurs entières sur GL_n. Il nous permet d'étudier l'ordre d'annulation en $s = 0$ des fonctions L p-adiques de Cassou-Noguès et Deligne-Ribet. En particulier, nous retrouvons un résultat de Wiles (1990) en direction de la conjecture de Gross. Nous proposons également une seconde construction, basée cette fois sur la méthode de Shintani, dont nous démontrons qu'elle conduit à un cocycle cohomologue au précédent. C'est un travail en commun avec S. Dasgupta et M. Greenberg.

Brian Conrey
Moments and zeros of L-functions
We give a new proof, based on random matrix theory, of the combinatorial identity in the Rudnick-Sarnak paper on the n-correlation of zero of L-functions. This proof offers insight into the structure of moments of families of L-functions.

Gabriel Dospinescu
Réduction modulo p des réseaux dans les représentations de Banach unitaires de $GL_2(Q_p)$
Dans ce travail en collaboration avec Pierre Colmez et Vytautas Paskunas, nous décrivons les réductions modulo p (à semi-simplification près) des réseaux $GL_2(Q_p)$-invariantes dans les représentations unitaires, irréductibles, admissibles de $GL_2(Q_p)$ sur des espaces de Banach p-adiques. Ceci a des applications directes à la correspondance de Langlands locale p-adique pour $GL_2(Q_p)$, qui joue d'ailleurs un rôle crucial dans les arguments.

Daniel Fiorilli
A conditional determination of the average rank of elliptic curves
A famous conjecture of Goldfeld asserts that in families of quadratic twists of elliptic curves, the average rank is 1/2. In this talk we show how to deduce Goldfeld's Conjecture from a hypothesis which is only slightly stronger than the Riemann Hypothesis. As a corollary we obtain that under this hypothesis, the Birch and Swinnerton-Dyer Conjecture holds for almost all curves

in our family, and that asymptotically one half of these curves have algebraic rank 0, and the remaining half 1. We also discuss results in the family of all elliptic curves.

Eduardo Friedman

Anomaly of regularized products

The regularized product $\widehat{\prod}_n \lambda_n := \exp(-f'(0))$, obtained through the analytic continuation of the Dirichlet series $f(s) := \sum_n \lambda_n^{-s}$, is important in number theory and mathematical physics. Barnes' and Shintani's multiple Γ-functions are examples of regularized products appearing in analogues of the Kronecker limit formulas. In physics, regularized products are called ζ-regularized determinants and denoted by $\det_\zeta$. They are attached to (suitable) operators A by taking $\{\lambda_n\}_n$ to be set of non-zero eigenvalues of A. Regularized determinants are well-known to fail to be multiplicative, i.e. in general $\det_\zeta(AB) \neq \det_\zeta(A)\det_\zeta(B)$. This has lead to the study of the multiplicative anomaly

$$M_2(A,B) := \frac{\det_\zeta(AB)}{\det_\zeta(A)\det_\zeta(B)}$$

attached to two operators. The anomaly M_2 is often a far simpler quantity than the individual regularized products. I will discuss the n-fold multiplicative anomaly,

$$M_n(A_1,...,A_n) := \frac{\det_\zeta\Big(\prod_{i=1}^n A_i\Big)}{\prod_{i=1}^n \det_\zeta(A_i)} \qquad (*)$$

attached to n (suitable) operators $A_1,...,A_n$. Recently we showed that when the A_i are commuting pseudo-differential elliptic operators, then their joint multiplicative anomaly M_n reduces to a product of pairwise multiplicative anomalies. Namely

$$M_n(A_1,...,A_n)^{m_1+\cdots+m_n} = \prod_{1\leq i<j\leq n} M_2(A_i,A_j)^{m_i+m_j},$$

where m_j is the order of A_j. I will sketch the proof, which relies on Wodzicki's 1987 formula for the pairwise multiplicative anomaly $M_2(A,B)$ of commuting elliptic operators. In the number-theoretic formulation, an n-fold anomaly is associated to n (suitable) polynomials in several variables. I will begin by describing the formula (*) in this simpler case. This is joint work with Victor Castillo-Garate and Marius Mantoiu.

Kevin Henriot

Extensions quantitatives du théorème de Roth

Le théorème de Roth affirme l'existence de progressions arithmétiques de longueur 3 dans tout sous-ensemble dense des entiers. Dans cet exposé, nous nous intéressons à des extensions de ce résultat, avec une emphase particulière sur les aspects quantitatifs. Précisément, étant donné un sous-ensemble A de $\{1,\dots,N\}$, on sait grâce aux travaux de Sanders que A contient une progression arithmétique dès lors que $|A| \geq N(\log N)^{-1+o(1)}$. Le premier objectif de cet exposé est de montrer comment étendre ces résultats au cas où A est un sous-ensemble fini d'un groupe abélien quelconque, sujet uniquement à la condition $|A+A| \leq (\log|A|)^{1-o(1)}|A|$. Remarquons aussi que le théorème de Roth concerne l'existence de solutions non-triviales à l'équation $x+y=2z$ avec $x,y,z \in A$, et l'on peut considérer plus généralement un système d'équations linéaires invariantes par translation. Nous considérons alors le probl'eme d'obtenir des bornes

de qualité logarithmique pour la plus large classe possible de systèmes d'équations pour laquelle une méthode d'analyse harmonique est disponible.

David Kohel
On the quaternion ℓ-isogeny path problem
Let $\mathcal{O}$ be a maximal order in a quaternion algebra $B/\mathbb{Q}$ of prime discriminant p, and let $\ell \neq p$ be a small prime. We describe a probabilistic algorithm, which for a given left $\mathcal{O}$-ideal I, computes a representative $J = I\alpha$, for $\alpha \in B^*$, in its left ideal class of ℓ-power norm. Subject to average distribution of primes in short intervals, this algorithm runs in expected polynomial time. The motivation for this problem is an explicit equivalence of categories between left $\mathcal{O}$-ideals and supersingular elliptic curves over $\bar{\mathbb{F}}_p$. In the latter, geometric, category, the analogous problem of finding an isogeny of ℓ-power degree appears difficult, and is the basis for a hash function of Charles-Goren-Lauter. The efficient algorithm in the algebraic category breaks the analogous problem in the quaternion analog of the CGL construction and has security implications for original function.

Srilakshmi Krishnamoorthy
On the Fourier coefficients of a Cohen-Eisenstein series
In the first part of this talk, we present a formula for the coefficients of a weight 3/2 Cohen-Eisenstein series of squarefree level N. This formula generalizes a result of Gross and in particular, it proves a generalization of a conjecture of Quattrini. In the second part, we explain the proof of this formula and we discuss some additional applications.

Nicolas Mascot
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.

Djordjo Milovic
The infinitude of $\mathbb{Q}(\sqrt{-p})$ with class number divisible by 16
The density of primes p such that the class number h of $\mathbb{Q}(\sqrt{-p})$ is divisible by 2^k is conjectured to be 2^{-k} for all positive integers k. The conjecture is true for $1 \leq k \leq 3$ but still open for $k \geq 4$. For primes p of the form $p = a^2 + b^4$ with b even, we find the 8-Hilbert class field of $\mathbb{Q}(\sqrt{-p})$ in terms of a and b. We then use a theorem of Iwaniec and Friedlander to show that there are infinitely many primes p for which h is divisible by 16, and also infinitely many primes p for which h is divisible by 8 but not by 16.

Ramon Moreira-Nunes
On the distribution of square-free numbers in arithmetic progressions

Let $\mu(n)$ be the Möbius function. We exhibit an asymptotic formula for the square mean

$$\sum_{a(q)}^{*} \left| \sum_{n \leq X, n \equiv a(q)} \mu^2(n) - MT \right|^2,$$

uniformly for $q \geq X^{31/41+\epsilon}$ and where MT stands for the expected main term. Moreover, we can show an upper bound that improves previous results on the larger domain $q \geq X^{8/13+\epsilon}$.

Aurel Page

The principal ideal problem in quaternion algebras

A crucial step in the computation of the Hecke operators for quaternionic automorphic forms is to find a generator for certain principal ideals. Given a maximal order in an indefinite quaternion algebras over a number field, testing whether two right ideals are equivalent reduces to the same problem over the base field by Eichler's theorem. However, computing a generator of a given right ideal that is known to be principal is much harder. We describe a new probabilistic algorithm using factor bases techniques that computes a generator of such an ideal. Assuming heuristics of good distribution and the generalized Riemann hypothesis, the algorithm runs in subexponential time. It performs well in practice.

Fabien Pazuki

Bounds for the number of rational points on curves over global fields

Rational points on smooth projective curves of genus $g \geq 2$ over number fields are in finite number thanks to a theorem of Faltings from 1983. The same result was known over function fields of positive characteristic since 1966 thanks to a theorem of Samuel. The aim of the talk is to give a bound as uniform as possible on this number for curves defined over such fields. In a first part we will report on a result by Rémond concerning the number field case and on a way to strengthen it assuming a height conjecture. During the second part we will focus on function fields of positive characteristic and describe a new result obtained in a joined work with Pacheco.

Antonella Perucca

The order of the reductions of points on algebraic groups

Let G be a commutative algebraic group defined over a number field K and let R be a K-point on G. For almost all primes p of K the reduction $(R \bmod p)$ is a point on the reduction of G modulo p. The order of $(R \bmod p)$ by varying p provides a family of natural numbers that contains information on R and G. We will consider the density of primes p such that the order of $(R \bmod p)$ is divisible by some fixed prime number. We will illustrate results of Jones and Rouse and a work in progress with Debry.

Gabor Wiese

Applying automorphic Galois representations in the inverse Galois problem

In the talk, I will report on recent results on the inverse Galois problem based on compatible systems of Galois representations coming from modular and automorphic forms. The focus will be on ideas and strategies as well as the obstacles that are preventing us from proving much stronger theorems. In this context, the role of coefficient fields will be particularly highlighted.

Han Wu

Subconvexity Problem for $\mathrm{GL}_2 \times \mathrm{GL}_1$

After introducing the generalization of the L-functions associated with a modular form and twisted by a Dirichlet character into the adelic picture, we present a proof of a Burgess-like bound for this type of L-functions based on an idea originated from P.Sarnak combined with the method of amplification. This is a part of my thesis.

Nadav Yesha

The Divisor Function in Short Intervals and Arithmetic Progressions

We discuss the behavior of sums of the divisor function in both short intervals and arithmetic progressions. We will describe recent work on the former problem, in which in short intervals of certain length, we show that these sums have a Gaussian limiting distribution. The latter case of arithmetic progressions was studied by É. Fouvry, S. Ganguly, E. Kowalski, and Ph. Michel, who proved a Gaussian limiting distribution, but only for smoothed sums ; we will discuss an analogue of their result with a sharp cut-off. Joint work with Steve Lester.