Colloque Jeunes Chercheurs en Théorie des Nombres

Bordeaux, 11-12-13 Juin 2014

Titres et résumés : Séances Plénières.

***

Le problème ternaire de Goldbach

Harald Helfgott (ENS Paris)

La conjecture ternaire de Goldbach (1742) affirme que tout nombre impair plus grand que 5 est la somme de trois nombres premiers. À la suite des pionniers (Hardy et Littlewood), Vinogradov prouva (1937) que tout nombre impair plus grand qu'une certaine constante C satisfaisait la conjecture. Durant les trois quarts de siècle suivants, il y a eu une succession de résultats réduisant C, mais seulement à des niveaux beaucoup trop grands pour qu'une vérification mécanique jusqu'à C soit possible ($C > 10^{1300}$). (Par ailleurs, les travaux de Ramaré et Tao ont résolu des problèmes correspondants avec six et cinq nombres premiers au lieu de trois.)

Nous verrons comment une nouvelle approche du problème, combinant des techniques modernes avec des nouvelles idèes, amène à de grandes améliorations dans les bornes de la partie analytique. Ceci ramène C à 10^{27}; or, une vérification jusqu'à 10^{27} n'est qu'un petit calcul. La conjecture ternaire de Goldbach est donc prouvée.

Nous discuterons les idées centrales de la preuve, avec un accent sur des outils d'intérêt général dans l'analyse et la théorie analytique des nombres.

Cryptographie reposant sur les réseaux euclidiens

Damien Stehlé (ENS Lyon)

La cryptographie reposant sur les réseaux euclidiens est une alternative récente et prometteuse aux approches classiques pour construire des cryptosystèmes à clé publique. Ses deux propriétés les plus attrayantes sont, d'une part, ses garanties de sécurité inégalées et, d'autre part, la grande richesse des primitives qu'elle permet de construire.

Dans ce cours introductif au domaine, je me restreindrai au problème *Learning With Errors* (LWE), introduit par Oded Regev en 2005, et prouvé au moins aussi difficile à résoudre que certains problèmes portant sur les réseaux euclidiens. Je montrerai en particulier comment obtenir un chiffrement à clé publique sûr à partir de LWE.

Le principal défaut de LWE est l'inefficacité des primitives cryptographiques en découlant. Pour remédier à cela, des variantes plus "structurées" de LWE ont été introduites : cette structure additionnelle permet d'obtenir des primitives cryptographiques plus efficaces. L'une de ces variantes, appelée Ring-LWE, est au moins aussi difficile à résoudre que certains problèmes portant sur les réseaux, si l'on se restreint à des réseaux correspondant à des idéaux d'anneaux d'entiers de corps de nombres. Dans la seconde partie du cours, je décrirai le problème Ring-LWE, ce qu'il apporte en termes d'efficacité, et ce qu'il fait perdre en termes de sécurité.

Enfin, je montrerai comment utiliser LWE pour construire un schéma de chiffrement homomorphe, c'est-à-dire un chiffrement permettant de calculer sur des données en ne manipulant que des messages chiffrés leur correspondant. Cette primitive a été réalisée pour la première

fois par Craig Gentry en 2009, et, à ce jour, toutes les constructions reposent sur les réseaux euclidiens.

Bibliographie.

- Daniele Micciancio and Oded Regev. Lattice-based Cryptography. Book chapter in "Post-quantum Cryptography", D. J. Bernstein and J. Buchmann (eds.), Springer (2008). Available at `http://www.cims.nyu.edu/~regev/`.
- Oded Regev. The Learning with Errors Problem. Invited survey in CCC 2010. Available at `http://www.cims.nyu.edu/~regev/`.
- Fabien Laguillaumie, Adeline Langlois et Benot Libert. Chiffrement avanc partir du problme *Learning With Errors*. Chapitre de l'ouvrage "Informatique Mathmatique, une photographie en 2014", Presses Universitaires de Perpignan. Disponible depuis `http://perso.ens-lyon.fr/damien.stehle/EJCIM.html`.
- Boaz Barak and Zvika Brakerski. The Swiss Army Knife of Cryptography. Guest blog post on homomorphic encryption. In Windows on Theory, 2012. Part I available at `http://windowsontheory.org/2012/05/01/the-swiss-army-knife-of-cryptography/`. Part II available at `http://windowsontheory.org/2012/05/02/building-the-swiss-army-knife/`.

Introduction à la théorie du corps de classes supérieur

Olivier Wittenberg (ENS Paris)

La théorie du corps de classes, qui connut son essor dans la première moitié du 20ème siècle, vise à donner une description interne de l'ensemble des extensions abéliennes d'un corps local ou global. Elle fut étendue aux corps de dimension supérieure dans les années 1970 et 1980, à l'aide d'outils K-théoriques élaborés. Aujourd'hui, un nouveau point de vue, introduit par Wiesend en 2006, permet une approche simplifiée, et plus élémentaire, de la théorie du corps de classes en dimension supérieure. C'est à la présentation de la théorie du corps de classes supérieur selon Wiesend que cette série d'exposés sera consacrée, après des rappels sur la théorie classique et sur le groupe fondamental abélien en géométrie algébrique.

Iwasawa theory past and present

Ted Chinburg (University of Pennsylvania)

Classical Iwasawa theory has to do with the rate of growth of ideal class groups in towers of number fields. In this talk I'll survey some of the history of the subject. This includes various Main Conjectures which link the above growth rates to analytically defined invariants such as p-adic L-series. By the end of the talk I'll describe how previous Main Conjectures are about first Chern classes. The theory of higher Chern classes suggests a new direction for the subject.

Colloque Jeunes Chercheurs en Théorie des Nombres

Bordeaux, 11-12-13 Juin 2014

Titres et résumés : Sessions parallèles.

***

Le théorème de Schanuel dans les espaces adéliques hermitiens

Thomas Ange (Université de Bordeaux)

Le théorème de Schanuel fournit une estimation asymptotique du nombre de points de hauteur (de Weil) bornée dans $\mathbb{P}(K^n)$ où K est un corps de nombres. Je présenterai une version totalement explicite de ce théorème dans le cadre d'un espace adélique hermitien sur K (on se limitera au cas pur), structure qui permet une certaine souplesse au niveau du choix de la hauteur. Je mettrai ensuite celui-ci en relation avec une estimation du nombre d'idéaux entiers de K de norme bornée (problème de Dedekind-Weber).

The fourth moment of automorphic L-functions at prime power level

Olga Balkanova (University of Bordeaux)

Behavior of automorphic L-functions at the critical point is an important study in analytic number theory. Subconvexity bounds and a question of vanishing (or non-vanishing) are problems of particular interest. A possible way to analyse them is the method of moments and its variations: mollification and amplification. Given techniques proved to be extremely effective in the past years. However, the majority of results are known under the assumption that a level of L-function is either prime or square-free number. Recently, Rouymi considered a level of the form p^ν, where p is a fixed prime number and $\nu \to \infty$. He computed the asymptotics of the first three moments and established a positive proportion of non-vanishing L-functions at the critical point. In this talk we give an asymptotic formula for the fourth power moment of automorphic L-functions at prime power level.

Rareté des points algébriques de certaines fonctions spéciales

Etienne Besson (Institut Fourier)

L'investigation des propriétés arithmétiques des valeurs prises par les fonctions analytiques intéressantes (fonction zêta de Riemann, fonction Gamma d'Euler, fonctions elliptiques...) est un problème d'approximation diophantienne naturel, mais souvent très difficile. Généralement, on conjecture que d'importantes relations d'indépendance algébrique peuvent être énoncées. Je propose de montrer comment, dans certains cas, on peut énoncer une propriété de rareté pour la situation où un nombre algébrique aurait pour image un autre nombre algébrique. La démonstration est basée sur une stratégie proposée en 2011 par David Masser.

Formule de Poisson motivique

Margaret Bilu (ENS / Université Paris Sud)

La formule sommatoire de Poisson est un outil notoirement efficace pour établir les propriétés de méromorphie de diverses fonctions zêta et de leurs généralisations, et en particulier de fonctions zêta des hauteurs telles qu'elles apparaissent par exemple dans les conjectures de Manin. Le développement récent de l'intégration motivique a donné lieu à des perspectives de ce genre dans un cadre plus géométrique en remplaçant les coefficients réels de ces fonctions zêta par des coefficients dans un anneau appelé anneau de Grothendieck des variétés. Nous donnerons une introduction à ce contexte motivique, nous focalisant sur la formule de Poisson motivique de Hrushovski et Kazhdan qui a déjà connu des applications analogues à celles de ses pendants plus classiques.

Number systems with negative base

Salma Dammak (Université de Sfax)

A venir.

Densité des points rationnels sur les surfaces de Del Pezzo

Julie Desjardins (Institut Mathématiques de Jussieu)

Soit X une surface de Del Pezzo de degré d. Si $d \geq 3$, il suffit que X contienne un point rationnel pour que $X(\mathbb{Q})$, l'ensemble de ceux-ci, soit dense. Dans le cas $d = 2$, il faut de plus que ce point se trouve en dehors de certaines courbes explicites. Lorsque $d = 1$, la surface X est automatiquement pourvue d'un point rationnel, mais la question de densité de $X(\mathbb{Q})$ est largement ouverte. Cet exposé présentera une méthode pour répondre partiellement à cette question.

En éclatant le point de base anticanonique de X, surface de Del Pezzo de degré 1, on obtient $\mathcal{E}$ une surface elliptique rationnelle. Une étude de la variation du signe des fibres de $\mathcal{E}$ peut mener à des résultats intéressants sur la densité des points rationnels de X grâce à la conjecture de parité. Cependant, lorsque la surface considérée est isotriviale, il peut arriver que le signe soit constant.

Critère explicite pour l'égalité de fonctions L d'Artin

Charlotte Euvrard (Laboratoire de Mathématiques de Besançon)

Soit L/K une extension galoisienne de groupe de Galois G. Pour un caractère χ de degré d associé à une représentation (ρ, V) de G, on peut écrire la fonction L d'Artin sous la forme

$$L(s, \chi, L/K) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \prod_{i=1}^{d} \left(1 - \alpha_{i,\rho}(\mathfrak{p}) \mathrm{N}(\mathfrak{p})^{-s}\right)^{-1},$$

où les complexes $(\alpha_{i,\rho}(\mathfrak{p}))_{1 \leq i \leq d}$ sont appelés les paramètres locaux en $\mathfrak{p}$ de $L(s, \chi, L/K)$.

Nous nous intéresserons ici à l'explicitation, dans le cadre particulier des fonctions L d'Artin, d'un théorème dû à Henryk Iwaniec et Emmanuel Kowalski démontrant l'existence d'un nombre fini de paramètres locaux permettant de distinguer deux fonctions L de même degré.

Cohomologie de certaines variétés de Shimura et critères de semi-simplicité

Karam Fayad (Université Paris 6 - IMJ)

Soient G un groupe réductif défini sur $\mathbb{Q}$ et $\mathcal{X} \subset \mathrm{Hom}(\mathbb{S}, G_{\mathbb{R}})$ une $G(\mathbb{R})$-classe de conjugaison de morphismes. On considère la donnée de Shimura $(G, \mathcal{X})$, et pour $K \subset G(\widehat{\mathbb{Q}})$ un sous-groupe ouvert compact, on note $Sh_K(G, \mathcal{X})$ la variété de Shimura correspondante, définie sur E, le corps réflexe de $(G, \mathcal{X})$.

Soit $\mathcal{L}_{\xi,l}$ le $\overline{\mathbb{Q}}_l$-faisceau d'espaces vectoriels, associé à une représentation $\xi_l : G_{\overline{\mathbb{Q}}_l} \to GL(N)_{\overline{\mathbb{Q}}_l}$, et défini sur $Sh_K(G, \mathcal{X})$. On a:

$$H^*_{et}(Sh(G,\mathcal{X}) \otimes_E \overline{\mathbb{Q}}, \mathcal{L}_{\xi,l}) = \varinjlim_K H^*_{et}(Sh_K(G,\mathcal{X}) \otimes_E \overline{\mathbb{Q}}, \mathcal{L}_{\xi,l}) = \bigoplus_{\pi^\infty} V(\pi^\infty) \otimes \pi^\infty$$

où $V(\pi^\infty) \otimes \pi^\infty$ est une représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}/E) \times G(\widehat{\mathbb{Q}})$. On s'intéresse à étudier la semi-simplicité de la représentation $V(\pi^\infty)$ de $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$.

Si $\mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_r$ (par exemple, dans le cas quaternionique, i.e. $G = \mathrm{Res}_{F/\mathbb{Q}}(B^*)$ où B est une algèbre de quaternions sur un corps totalement réel F), les relations d'Eichler-Shimura généralisées nous conduisent à traiter, dans un contexte plus général, la question suivante: soient Γ un groupe profini, et $\rho, \rho_1, ..., \rho_r$ des représentations continues de dimension finie de Γ, à coefficients dans $\overline{\mathbb{Q}}_l$, tels que

$$\forall\ g \in \Gamma,\ P_{(\rho_1 \otimes \ldots \otimes \rho_r)(g)}(\rho(g)) = 0$$

où P désigne le polynôme caractéristique, alors sous quelles hypothèses supplémentaires a-t-on la semi-simplicité de ρ?

Preuves géométriques d'inégalités de Brauer-Siegel

Richard Griffon (Université Paris 7 - Jussieu)

Le théorème de Brauer-Siegel décrit la croissance du nombre de classes $h(K)$ et du régulateur $R(K)$ d'un corps de nombres K lorque le discriminant D_K tend vers l'infini (à degré $[K : \mathbb{Q}]$ fixé) : plus précisément, il dit que $\log \sqrt{D_K} \ll \log(h(K) \cdot R(K)) \ll \log \sqrt{D_K}$. La démonstration usuelle passe par une étude analytique fine de la fonction zeta au voisinage de son pôle, le point difficile étant la preuve de la minoration (qui reste ineffective) de l'encadrement.

Dans cet exposé, j'expliquerai comment on peut retrouver la majoration de ce théorème grâce à des considérations géométriques et un calcul de volume. Je montrerai aussi comment retrouver une version faible (mais effective) à l'aide de minoration de hauteurs.

Nombres de Salem, polynômes expansifs et fractions continues de Stieltjes.

Christelle Guichard (Université de Grenoble I)

On considère une réciproque à la Construction de Salem (1945) de suites convergentes de nombres de Salem en termes d'association entre polynômes de Salem et de quotients d'Hurwitz par l'intermédiaire de polynômes expansifs de petite mesure de Mahler. Cette association utilise le Théorème A (1995) de Bertin-Boyd d'entrecroisement de conjugués sur le cercle unité ; dans ce contexte, un nombre de Salem est produit et codé par un m-uplet de nombres rationnels strictement positifs caractérisant la fraction continue de Stieltjes (SITZ) du quotient (alternant) d'Hurwitz correspondant. Le sous-ensemble des fractions continues de Stieltjes au-dessus d'un polynôme de Salem à racines simples, ne s'annulant pas en ± 1, provenant de polynômes expansifs unitaires de terme constant égal à leur mesure de Mahler, admet une structure de semi-groupe. Cette structure de semi-groupe se transporte sur les ensembles de nombres de Garsia généralisés correspondants.

Pluri-canonical systems on arithmetic surfaces

Yi Gu (Université de Bordeaux)

Let S be a Dedekind scheme, $f : X \to S$ be a minimal arithmetic surface of arithmetic genus $g > 1$, and $X' \to C$ be the canonical model of f. It is well known that $\omega_{X'/C}$ is relatively ample, so the question is for which $n \in \mathbb{N}$ such that $\omega_{X'/C}^{\otimes n}$ is very ample. In this talk we will prove when S has equal characteristic and perfect residue fields, then the answer is $n \geq 3$. The idea is first to reduce to the case where S is a curve over an algebraic closed field, then apply Reider's Method.

Non-annulation des coefficients fondamentaux de Fourier des formes modulaires de Siegel

Marzec Jolanta (University of Bristol)

Nous allons étudier les coefficients fondamentaux de Fourier propres aux formes modulaires de Siegel de genre 2. Ceux qui présentent un intérêt particulier sont ceux déterminés par des matrices de discriminant fondamental. Chaque fois que nous sommes en mesure de dire que l'un d'eux ne s'annule pas, nous obtenons - grâce à la conjecture généralisée de Böcherer - la non-annulation des valeurs centrales de fonctions L. Nous allons discuter plusieurs cas de sous-groupes de congruence $\Gamma_0(N)$ et $\Gamma^{\text{para}}(N)$ avec N sans facteur carré.

Problème inverse de Galois et conditions locales

Francois Legrand (Université Lille 1)

On s'intéressera dans cet exposé aux extensions galoisiennes de $\mathbb{Q}$ obtenues par spécialisation d'extensions galoisiennes de $\mathbb{Q}(T)$ (la lettre T désignant une indéterminée). Plus précisément, on cherchera à imposer le groupe de Galois et le groupe d'inertie des spécialisations en un nombre fini de nombres premiers fixés au préalable. Les liens avec certaines questions classiques de la théorie inverse de Galois seront évoqués.

Open image theorems for abelian varieties

Davide Lombardo (Université Paris-sud)

To any abelian variety over a number field K it is possible to attach a system of representations of the absolute Galois group of K, indexed by the rational primes. It is conjectured that, with the exception of a finite number of primes, the image of these representations should be 'as large as possible', in a very precise sense. In this talk I will try to introduce the problem and describe some of the known results in this direction, focusing on the case of elliptic curves.

Modular forms of arbitrary real weight and Eichler cohomology

Michael O. Neururer (Univ. Nottingham)

The interpretation of modular forms as elements in certain cohomology groups goes back to Eichler in 1957. The theory he and others developed has many applications in the computational theory of modular forms and the study of special values of their L-functions.

I will present a new proof of a theorem by Knopp and Mawi that identifies modular forms of arbitrary real weight as elements of Eichler cohomology groups.

Calculs de formes automorphes pour GL_2

Aurel Page (Université de Bordeaux)

Les formes automorphes pour GL_2 sont des généralisations à un corps de nombre F des formes modulaires classiques, et interviennent par exemple si on veut tabuler les courbes elliptiques sur F. J'esquisserai un algorithme permettant de calculer des espaces de telles formes automorphes. Les ingrédients seront de la géométrie hyperbolique, des algèbres de quaternions, et de la cohomologie des groupes.

Explicit lower bounds for heights related to elliptic curves

Linda Raabe (TU Darmstadt)

After shortly introducing heights and elliptic curves we will look at the torsion points E_{tor} of an elliptic curve E over $\mathbb{Q}$ and adjoin their coordinates to $\mathbb{Q}$. What we get is $\mathbb{Q}(E_{\mathrm{tor}})$ which is a Bogomolov field. In a Bogomolov field, the height of a nonzero number which is not a root of unity is bounded from below by a positive constant. We will compute this bound explicitly.

Frobenius and Logarithmic ramification

Stéphanie Reglade (Université de Bordeaux)

Given $K_\mathfrak{p}$ a finite extension of $\mathbb{Q}_p$, we study the ℓ-adification of the multiplicative group of our local field $\mathcal{R}_{K_\mathfrak{p}}$ endowed with the logarithmic valuation introduced by Jaulent [2]. Compared to the previous article [4], we replace here the maximal abelian unramified pro-ℓ-extension of $K_\mathfrak{p}$ by the $\mathbb{Z}_\ell$-cyclotomic one, and the usual valuation by the logarithmic one. We show that it is possible to use Neukich's abstract theory [1] in this context. Thus, it allows to define a logarithmic local symbol and a logarithmic Frobenius. The interesting point is that usual and logarithmic Frobenius coincide when usual and logarithmic ramification are the same. The goal of our presentation is to explain the notion of logarithmic ramification, and how we generalize the notion of Frobenius in this framework.

References

[1] J. Neukirch, *Class Field Theory*, Springer-Verlag, GTM 280, (1986)

[2] J.-F Jaulent, *Classes logarithmiques d'un corps de nombres*, J. Théor. Nombres Bordeaux, **6**, (1994), 301–325.

[3] J.-F. Jaulent, *Théorie ℓ-adique du corps des classes*, J. Théor. Nombres Bordeaux, **10**, fasc.2 (1998), 355–397.

[4] S.Reglade, *A formal approach "à la Neukirch" of ℓ-adic class field theory*, submitted.

[5] S.Reglade, *Frobenius et ramification logarithmique*, preprint.

[6] C.Brighi, *Capitulation des classes logarithmiques et tude de certaines tours de corps de nombres*, thèse, Publ. Math. Fac. Sci. Metz, Théor. Nombres (2007), 1–67.

Algèbres graduées des formes modulaires

Nadim Rustom (Université de Copenhague)

Soit N un entier naturel. Nous étudions les algèbres graduées $M(G, A)$ engendrées par les formes modulaires à coefficients dans l'anneau A et pour le groupe G au cas où $A = \mathbb{Q}, \mathbb{Z}[\frac{1}{N}]$ ou $\mathbb{Z}$, et $G = \Gamma_0(N)$ ou $\Gamma_1(N)$. Avec quelques conditions imposées sur N, nous présentons des bornes supérieures pour les poids des formes modulaires dans un ensemble minimal de générateurs, et aussi pour les degrés des relations entre eux, ce qui nous permet de décrire un algorithme qui calcule explicitement la structure des $M(G, A)$. Nous présentons aussi des résultats numériques explicites concernant la structure des $M(G, A)$.

Le douzième problème de Hilbert et la conjecture de Stark

Coline Wiatrowski (ICJ - Université de Lyon 1)

Dans cet exposé, on s'intéresse au douzième problème de Hilbert qui conjecture une généralisation du théorème de Kronecker-Weber aux extensions abéliennes de tout corps de nombres. On verra ici comment la conjecture abélienne de rang 1 de Stark permet de fournir des générateurs d'une telle extension.

Chebotarev explicite

Bruno Winckler (Université de Bordeaux)

Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G; le fameux théorème de Chebotarev énonce, grossièrement, que les automorphismes de Frobenius associés aux idéaux premiers de K se répartissent "uniformément" parmi les classes de conjugaison de G. Pour des applications arithmétiques, il est parfois utile de pouvoir préciser cette répartition. L'objectif de cet exposé est de montrer, dans les grandes lignes, comment obtenir une version effective de ce résultat; on reviendra particulièrement sur l'importance des résultats de densité et de répartition des zéros des fonctions L, afin de comprendre comment améliorer le terme d'erreur du théorème de Chebotarev.

Une formule de type Riemann-Hurwitz pour les revêtements sous μ_{p^n}

Gabriel Zalamansky (IMJ Paris 6)

Soit $f : X \to Y$ un morphisme de courbes lisses. Si f est génériquement séparable alors la formule de Riemann-Hurwitz établit un lien entre le lieu des points où f n'est pas étale et les faisceaux de différentielles des courbes X et Y.

Les torseurs sous des groupes infinitésimaux sont génériquement inséparables. Cependant, si $f : X \longrightarrow Y$ est un μ_{p^n}-revêtement qui est génériquement un torseur, on définira à l'aide de l'action de μ_{p^n} sur X un diviseur qui coïncidera avec le lieu des points où f n'est pas un torseur et on prouvera une formule analogue à celle de Riemann-Hurwitz dans ce cadre.