M2 2024-2025 : parcours d'arithmétique

Cours de remise à niveau

— Rappels d'algorithmique et de complexité.

— Rappels de géométrie algébrique/d'algèbre commutative ?

1 Cours fondamentaux

1.1 Corps locaux (Laurent Berger)

This course is an introduction to arithmetic and analysis in p-adic fields. Topics to be covered depend on the second semester courses, but will include some of the following : local fields and their extensions, Galois theory, ramification theory, p-adic analysis, p-adic Banach spaces, formal groups, Lubin-Tate theory, p-adic periods.

1.2 Courbes algébriques et courbes elliptiques (François Brunault)

Ce cours est une introduction aux courbes elliptiques, avec les points de vue analytique complexe et algébrique. On étudiera les propriétés des courbes elliptiques sur les corps locaux et sur les corps de nombres. En particulier, on démontrera le théorème de Mordell-Weil (le groupe des points rationnels d'une courbe elliptique sur un corps de nombres est finiment engendré). Enfin, on définira les courbes modulaires comme espaces de modules de courbes elliptiques, et expliquerons leurs modèles sur les corps de nombres.

Références

[DS05] Joseph Silverman. *The arithmetic of elliptic curves (Second edition)*, Grad. Texts in Math. volume 106, Springer-Verlag, 2009.

1.3 Formes modulaires (Sandra Rozensztajn)

L'objectif de ce cours est de donner une introduction à la théorie des formes modulaires.

Les fonctions modulaires sont des fonctions holomorphes définies sur le demi-plan de Poincaré, qui respectent certaines conditions de transformation sous l'action par homographies de $\mathrm{SL}_2(\mathbb{Z})$.

Cette définition en apparence analytique recouvre de nombreuses propriétés arithmétiques, concernant notamment les propriétés des coefficients de Fourier, que nous aborderons en partie dans ce cours.

Références

[DS05] Fred Diamond et Jerry Shurman. *A first course in modular forms*, GTM volume 228, 2005

[Miy89] Toshitsune Miyake. *Modular forms*, Springer-Verlag, 1989.

[Ser77] Jean-Pierre Serre. *Cours d'arithmétique*, PUF, 1977

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions.*, Princeton, 1971

2 Cours avancés

2.1 Formes modulaires p-adiques (Benjamin Schraen)

The course will be an introduction to the theory of p-adic families of modular forms. The goal will be to construct the eigencurve of p-adic modular forms and to give some example of applications, for instance to p-adic L-functions or to the completed cohomology of the tower of modular curves.

2.2 Arbre de Bruhat-Tits de SL(2) et géométrie non archimédienne / Bruhat-Tits tree of SL(2) and non-Archimedean geometry (Bertrand Rémy)

Les actions du groupe de matrices SL(2) sur des espaces adéquats permettent de mieux comprendre la structure et la théorie des représentations de celui-ci. Ce cours propose deux possibilités en matière d'espaces : d'une part les arbres de Bruhat-Tits, qui privilégient les structures métriques et permettent d'obtenir et d'interpréter des décompositions du groupes ; d'autre part les espaces analytiques au sens de Berkovich, qui fournissent un cadre plus riche. On expliquera le lien naturel entre les deux approches. Si le temps le permet, on évoquera un peu l'analyse harmonique bi-invariante sur ces espaces, et peut-être le cas plus général des groupes GL(n).

The actions of the matrix group SL(2) on suitable spaces provide a better understanding of the structure and the representation theory of the latter matrix group. This course proposes two possibilities in terms of spaces : on the one hand, the Bruhat-Tits trees, which emphasize metric structures and allow to obtain and interpret group decompositions ; on the other hand, analytic spaces in the Berkovich sense, which provide a richer framework. The natural link between the two approaches will be explained. If time permits, we will talk a little about the bi-invariant harmonic analysis on these spaces, and perhaps the more general case of the groups GL(n).

Références :

— V.G. Berkovich, *Spectral theory and analytic geometry over non-archimedean fields*. American Mathematical Soc., 1990.

— J.-P. Serre, *Arbres, amalgames,* $SL(2)$. Astérisque 46, Société Mathématique de France, 1977.

— J. Tits, *Reductive groups over local fields*. In Automorphic Forms, Representations and L-Functions (Part 1), American Mathematical Soc., 1979.

2.3 Elliptic curves in computational number theory (Benjamin Wesolowski)

This course will explore computational aspects of elliptic curves, and their many appli- cations. Computing with elliptic curves has long been of interest for an experimental approach to number theory and testing conjectures. Beyond such theoretical endeavors, the field has developed around important applications in information and communica- tion sciences : elliptic curves play a central part in ensuring the security of our everyday communications.

This course will cover :

(1) Fundamental aspects of the field : how to compute the group law, count points over finite fields, compute isogenies ;

(2) Applications to seemingly unrelated computational questions in number theory : how to factor integers, or prove that an integer is prime ;

(3) Applications in cryptography : how to design or break cryptosystems with elliptic curves and isogenies ;

(4) Along the way, various aspects of the theory of elliptic curves will be developed or revisited, including endomorphism rings, isogeny graphs and random walks, complex multiplication.