Projets pour l'enseignement d'approfondissement

Thématiques possibles :

— Arithmétique : projets 1, 2, 8.
— Géométrie : projets 3, 4, 5, 7.
— Algèbre effective : projets 6, 8.

Table des matières

1 Nombres premiers de la forme $x^2 + ny^2$ et multiplication complexe

Soit n un entier naturel non nul. Quels nombres premiers sont de la forme $x^2 + ny^2$? L'objectif de ce projet est de comprendre la preuve du théorème suivant :

Théorème. (th. 13.23 de [1]) Il existe un polynôme unitaire et irréductible à coefficients entiers f_n tel que, pour tout nombre premier p ne divisant pas $2n$, on a :

$$\exists x, y,\ p = x^2+ny^2 \Leftrightarrow \begin{cases} \text{la congruence } x^2 \equiv -n \mod p \text{ a une solution entière,} \\ \text{la congruence } f_n(x) \equiv 0 \mod p \text{ a une solution entière.} \end{cases}$$

De plus, il existe un algorithme permettant de calculer le polynôme f_n.

L'étude des courbes elliptiques à multiplication complexe est au coeur de la démonstration de ce résultat.

Principales références

[1] Cox D., Primes of the form $x^2 + ny^2$, Wiley, 2013.

[2] Silverman J., Advanced topics in the arithmetic of elliptic curves, Springer, 1999. Chapitre II.

[3] A. Borel et al., Seminar on complex multiplication, Springer Lecture Notes in Mathematics 21, 1966.

2 Autour du dixième problème de Hilbert

Existe-t'il un algorithme permettant de déterminer si une équation polynômiale à coefficients entiers admet une solution entière ? Cette question, qui constitue le dixième problème de Hilbert, a été résolue par Matjasevic à partir de travaux antérieurs de Davis, Putnam et Robinson ([1]).

Par la suite, d'autres auteurs se sont demandé ce qui se passe quand on remplace l'anneau des entiers $\mathbf{Z}$ par d'autres anneaux. L'objectif principal de ce projet consiste à comprendre la preuve du résultat suivant, dû à Denef :

Théorème. ([2]) Soit R un anneau intègre de caractéristique nulle. Il n'existe pas d'algorithme permettant de déterminer si une équation à coefficients dans $\mathbf{Z}[T]$ admet des solutions dans $R[T]$.

La preuve utilise de manière cruciale les courbes elliptiques.

Principales références

[1] Martin Davis. Hilbert's tenth problem is unsolvable. The American Mathematical Monthly, vol 80, no. 3, pages 233–269, March 1973.

[2] J. Denef. The diophantine problem for polynomial rings and fields of rational functions. Transactions of the American Mathematical Society, vol 242, pages 391–399, August 1978.

3 Uniformisation p-adique des courbes elliptiques

Le théorème d'uniformisation des courbes elliptiques complexes affirme que toute courbe elliptique sur $\mathbf{C}$ peut être vue comme le quotient de $\mathbf{C}$ par un réseau. Qu'en est-il des courbes définies sur des corps p-adiques ? Le but de ce projet est de comprendre comment Tate a réussi à répondre à cette question pour les courbes elliptiques dont le j-invariant est de valeur absolue > 1 (th. V.3.1 et V.5.3 de [2]).

Principales références

[1] J. H. Silverman. The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics, 106) 2nd ed. 2009. Chapitres IV et VI.

[2] J. H. Silverman. Advanced topic in the Arithmetic of Elliptic Curves (Graduate Texts in Mathematics, 151) 1994. Chapitre V.

4 Variétés abéliennes

L'objectif de ce projet consiste à étudier les variétés abéliennes, qui sont la généralisation naturelle des courbes elliptiques en dimension supérieure. Après avoir étudié les propriétés élémentaires des variétés abéliennes, on pourra par exemple se pencher sur les variétés abéliennes complexes (uniformisation des variétés abéliennes), sur les variétés abéliennes sur les corps finis (conjecture de Weil et nombre de points à valeurs dans un corps fini), ou encore sur les variétés abéliennes sur les corps de nombres (théorème de Mordell-Weil).

Principales références

[1] M. Hindry, J. H. Silverman. Diophantine Geometry, an introduction, Graduate Texts in Mathematics, Springer, New York, NY, 2000.

[2] J. S. Milne. Abelian Varieties, Chapter V of Arithmetic geometry (Storrs, Conn., 1984), 103–150, Springer, New York, 1986.

[3] J. S. Milne. Abelian varieties, course notes.

5 Vers les conjectures de Weil

Les conjectures de Weil (qui sont connues de nos jours grâce au travail de Deligne) portent sur le nombre de points d'une variété algébrique sur un corps fini. Dans le cours, nous parlerons de ces conjectures dans le cas particulier des courbes elliptiques. Un premier but de l'EA consisterait à comprendre comment démontrer ces conjectures pour les hyper-surfaces diagonales, c'est à dire pour les variétés projectives définies par une équation de la forme $a_0x_0^d+...+a_nx_n^d = 0$. S'il nous reste du temps après, nous pourrions regarder la preuve de Dwork de la rationalité de la fonction zêta pour toutes les variétés projectives lisses sur des corps finis.

Côté références, on pourrait commencer par utiliser [1]. Il s'agirait essentiellement de comprendre le chapitre 11 - notamment la section 3. Après, pour la deuxième partie de l'EA, si on a le temps, on peut utiliser le post [2] du forum de Terence Tao.

Principales références

[1] K. Ireland et M. Rosen. Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, Springer, New York, NY, 1990.

[2] Forum de T. Tao.
`https://terrytao.wordpress.com/2014/05/13/dworks-proof-of-rationality-of-the-zeta-function-over-finite-fields/`

6 Algorithme de Schoof

Un célèbre théorème de Hasse permet de borner le nombre de points d'une courbe elliptique définie sur un corps fini. Pour des applications pratiques (notamment en cryptographie), il est souvent important de savoir le nombre de points exact d'un telle courbe elliptique. L'objectif de cet EA consiste à comprendre un algorithme développé par Schoof pour répondre à cette question.

Principales références

[1] Schoof, R. Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44 (1985), 483-494.

[2] Schoof, R. Counting points on elliptic curves over finite fields, Journal de Théorie des Nombres de Bordeaux 7 (1995), 219-254.

7 Faisceaux et schémas

En cours, nous faisons de la géométrie algébrique classique, en définissant les variétés sur un corps K comme sous-ensembles de $\overline{K}^n$ ou $\mathbf{P}^n(\overline{K})$. L'objectif de cet EA consistera à s'introduire à la géométrie algébrique à la Grothendieck et donc au langage des faisceaux et des schémas. Si le temps le permet, on pourra également se pencher sur la cohomologie de Zariski.

Principales références

[1] I. Shafarevich. Basic Algebraic Geometry vol. 2, Springer-Verlag Berlin Heidelberg 2013.

[2] A. Holme. A Royal Road to Algebraic Geometry, Springer-Verlag Berlin Heidelberg 2012.

8 17ème problème de Hilbert

Le 17ème problème de Hilbert demande si toute fraction rationnelle $F \in \mathbf{R}(X_1, ..., X_n)$ positive est somme de carrés. Cette question a été résolue affirmativement par Artin et Lang, et l'objectif de cet EA serait d'en comprendre la preuve.

Principales références

[1] S. Lang. Algebra, Graduate Studies in Math, chap. XI.

[2] J. F. Fernando, J. M. Gamboa. Real algebra from Hilbert's 17th problem, `http://www.mat.ucm.es/~josefer/articulos/rgh17.pdf`.

9 Cryptographie via des courbes elliptiques

Les courbes elliptiques et les isogénies entre elles sont très utilisées en cryptographie. Dans cet EA, on pourra approfondir les méthodes cryptographiques fondées sur les courbes elliptiques au-delà de ce que nous verrons en cours. On pourra également s'introduire aux méthodes récentes exploitant les isogénies.

Principales références

[1] L. C. Washington. Elliptic Curves, number theory and cryptography, Chapman and Hall/CRC ; 2nd edition (2008). Chapitres 5 et 6.

[2] L. De Feo. Mathematics of Isogeny Based Cryptography, Lecture notes, 44 pp, 2017 (`https://arxiv.org/abs/1711.04062`).