Numération : mathématiques et informatique

Rencontre organisée par :
Boris Adamczewski, Anne Siegel et Wolfgang Steiner

23-27 mars 2009

Boris Adamczewski, Anne Siegel, et Wolfgang Steiner

Présentation de la rencontre

Vol. 1, n° 1 (2009), p. 1-2.

<http://acirm.cedram.org/item?id=ACIRM_2009__1_1_1_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Actes des rencontres du C.I.R.M.
Vol. **1** n° 1 (2009) 1-2

Présentation de la rencontre

Boris Adamczewski, Anne Siegel, et Wolfgang Steiner

Les systèmes de numération, dont les représentations décimales, binaires ou en fractions continues sont des exemples emblématiques, permettent de représenter les éléments d'un ensemble donné (entiers naturels, nombres réels, nombres complexes, nombres p-adiques, séries formelles) de manière unifiée sous une forme combinatoire : leur suite de chiffres. De telles représentations apparaissent dans de nombreux domaines des mathématiques et de l'informatique, et sont source de problèmes ouverts difficiles.

A travers cette rencontre, nous avons souhaité aborder différents aspects des systèmes de numération, à la fois mathématiques et informatiques, afin notamment d'établir un contact entre des chercheurs français et étrangers provenant d'horizons très différents. La conférence s'est déroulée du 23 au 27 mars 2009 et a accueilli environ 80 participants, avec une représentation bien équilibrée entre chercheurs étrangers et français, débutants (doctorants, post-docs) et confirmés, mathématiciens et informaticiens. Cette rencontre a permis de présenter des survols et des contributions sur des sujets variés autour des systèmes de numération, allant des plus théoriques (théorie ergodique, théorie des nombres, géométrie) aux plus appliqués (cryptographie et géométrie discrète). Les cours et les exposés invités sur ces sujets ont été complétés par des exposés courts proposés par certains participants. Afin d'illustrer la richesse des problématiques liées aux systèmes de numérations, nous reprenons ci-dessous quelques thèmes actuels de recherches qui ont été abordés.

Du point de vue mathématique, une première question consiste à identifier les nombres ayant un développement fini, périodique ou ultimement périodique. Ainsi, d'après le classique théorème d'Euler–Lagrange, le développement en fraction continue d'un nombre réel est ultimement périodique si et seulement si ce dernier est un nombre quadratique irrationnel. Il est assez surprenant qu'une problématique en apparence aussi na¨ive conduise à des problèmes encore ouverts si l'on s'intéresse à d'autres représentations comme les β-numérations ou les fractions continues de Rosen. Les développements purement périodiques pour certaines β-numérations peuvent être caractérisés par des ensembles assez étranges à structure fractales qui sont intimement liés à des modèles de quasi-cristaux et des espaces de pavages auto-similaires. Les fractions continues de Rosen sont quant-à-elles liées à l'étude du flot géodésique sur certaines surfaces, comme la surface modulaire.

Un autre aspect mathématique des systèmes de numération vient de l'utilisation de la théorie ergodique, dont les outils permettent de déterminer les comportements statistiques des suites de chiffres pour différentes représentations. Ces résultats servent notamment de guide aux théoriciens de nombres et permettent de formuler de nombreuses conjectures sur les représentations des nombres algébriques ou de certaines périodes. Dans le cas des séries formelles à coeficients dans un corps fini, il est remarquable que l'on puisse décrire, suite aux travaux de Christol, la suite des chiffres des « nombres algébriques » : ce sont précisément ceux dont la suite de chiffres peut être engendré par un automate fini. Ce résultat a été récemment étendu par Kedlaya aux séries de Hahn à coeficients dans un corps finis $\mathbb{K}$, permettant ainsi de décrire complétement une clôture algébrique du corps des fonctions rationnelles $\mathbb{K}(T)$. Cela contraste avec un résultat d'Adamczewski et Bugeaud, lesquels montrent que la suite des chiffres de l'écriture décimale d'un nombre algébrique irrationnel comme $\sqrt{2}$ ne peut pas être produite par des machines de Turing aussi simples. Ce dernier résultat repose sur un théorème diophantien profond : le théorème du sous-espace de Schmidt.

Enfin, dans un registre différent, Mauduit et Rivat ont récemment démontré une conjecture de Gelfond sur la répartition des chiffres dans l'écriture des nombres premiers dans une base entière : asymptotiquement, 50 écrits dans la base 2. Dans ce cas, les principaux outils utilisés proviennent de la théorie analytique des nombres. Il y a bien sûr encore beaucoup d'aspects mathématiques des systèmes de numération que nous avons passés ici sous silence, comme certains problèmes de cryptographie, d'équirépartition...

D'un point de vue informatique, l'existence de différentes écritures est exploitée en arithmétique des ordinateurs et en cryptographie. Il est bien connu que l'utilisation de systèmes de numération redondants permet d'accélérer les algorithmes arithmétiques. En cryptographie, on distingue deux types d'opérations arithmétiques sur les courbes elliptiques que l'on souhaite optimiser : les formules d'addition et de doublement, et les algorithmes de multiplication scalaire (équivalent additif d'une exponentiation). Dans tous ces cas, des représentations comme la NAF (non-adjacent form) en base 2, ou le système à double base dans lequel tout nombre entier est représenté comme une somme de produits de puissances de 2 et de 3, ont permis des avancées significatives.

Géométriquement, l'algorithme des fractions continues permet de construire des approximations discrètes de droites dans le plan : le procédé d'engendrement est basé sur le développement de la pente de la droite. En dimension supérieure, une question naturelle consiste à engendrer un plan discret par un processus itératif. On cherche pour cela à utiliser le développement en fractions continues du vecteur normal au plan considéré. Même s'il n'existe pas de généralisation réellement naturelle des fractions continues unidimensionnelles, l'algorithme de Brun a récemment montré son intérêt, en particulier pour la reconnaissance des approximations de plans parmi les surfaces discrètes bornées (Berthé, Fernique).

Ce cadre des fractions continues multidimensionnelles est également riche d'un point de vue des approximations diophantiennes. En effet, de bonnes approximations rationnelles simultanées d'un vecteur en dimension d peuvent être obtenues grâce à l'algorithme LLL. Cependant, cette approche a pour défaut de ne pas être itérative : il est impossible de s'appuyer sur un résultat à l'ordre $1/q^d$ pour obtenir une approximation à l'ordre $1/(q+1)^d$. Lagarias a détaillé comment un flot sur l'ensemble des matrices de Minkowski réduites dans $GL(d+1,\mathbb{R})$ (jouant le rôle du demi-plan de Poincaré utilisé en dimension 1) permet de définir un développement en fraction continue et d'exhiber des meilleures approximations simultanées. Obtenir à partir de ces travaux un algorithme concret reste une tâche inachevée à ce jour.

Nous tenons à remercier ici l'ensemble des participants et des orateurs, les comités d'organisation et scientifque, ainsi que nos soutiens financiers (CIRM, ANR DyCoNum, GDR Informatique Mathématique, IRISA) pour avoir contribué à la pleine réussite de cette rencontre.

Université Claude-Bernard, Institut Camille-Jordan, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne CEDEX (France) • Boris.Adamczewski@math.univ-Lyon1.fr

IRISA, Campus de Beaulieu, 35042 Rennes CEDEX (France) • anne.siegel@irisa.fr

Université Denis-Diderot, LIAFA, Case 7014, 75205 Paris CEDEX 13 (France) • steiner@liafa.jussieu.fr