Rapport à vague de Xavier Caruso

Période : décembre 2010 — décembre 2015

A. Rapport d'activités

1 Curriculum vitæ

Xavier Caruso
(né le 24 avril 1980 à Cannes)
IRMAR – Université Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
Tél : 02 23 23 58 92
E-Mail : xavier.caruso@normalesup.org
Page web : http://perso.univ-rennes1.fr/xavier.caruso/
Marié, deux enfants (nés pendant les dix derniers semestres)

Parcours scolaire et professionnel

2011 Habilitation à diriger les recherches soutenue le 3 juin à l'université de Rennes 1 durant le jury composé de Laurent Berger, Christophe Breuil, Pierre Colmez, Jean-Marc Fontaine et Michael Rapoport.

2009–2010 Mobilité d'une année au laboratoire Poncelet à l'Université Indépendante de Moscou

2006– Chargé de recherche au CNRS affecté à l'Université de Rennes 1.

2005 Thèse sous la direction de Christophe Breuil intitulée *Conjecture de l'inertie modérée de Serre* et soutenue le 7 décembre devant le jury composé de Ahmed Abbes, Pierre Berthelot (rapporteur), Lawrence Breen, Christophe Breuil (directeur de thèse), Michel Raynaud. Autre rapporteur : Mark Kisin.

2003–2006 Moniteur à l'université Paris 13.

1999–2003 Élève de de l'École normale supérieure de Paris

Responsabilités

2013– Rédacteur du journal en ligne *Images des mathématiques*

2012–2016 Membre élu du CoNRS (Comité National de la Recherche Scientifique)

2012–2016 Membre nommé du conseil de l'IRMAR (Institut de Recherche en Mathématiques de Rennes)

2009–2013 Coordinateur du projet ANR CETHop (Calculs effectifs en théorie de Hodge p-adique)

Divers

1997 Premier accessit au concours général de mathématiques.
Quatrième accessit au concours général de physique.
Participation aux olympiades internationales de mathématiques à Mar del Plata (Argentine). Obtention d'une *honourable mention*.

Langues : français (langue maternelle), anglais (parlé et écrit), russe (assez bonne connaissance)

2 RECHERCHE SCIENTIFIQUE

Durant les cinq dernières années, mes centres d'intérêt se sont grandement diversifiés : alors qu'initialement mon activité de recherche était concentrée sur la théorie de Hodge p-adique, elle s'étend désormais à une partie plus importante de la théorie des nombres ainsi qu'au calcul formel, à l'arithmétique des ordinateurs et, plus modestement, à la théorie des probabilités. Le fil directeur de mes recherches reste néanmoins l'étude des nombres p-adiques.

Dans toute la suite de cette présentation, la lettre p désigne un nombre premier fixé. On note $\mathbb{Q}_p$ le corps des nombres p-adiques. On en choisit une clôture algébrique $\bar{\mathbb{Q}}_p$ fixée une fois pour toutes. Toutes les extensions algébriques de $\mathbb{Q}_p$ que nous allons considérer seront implicitement supposés vivre à l'intérieur de $\bar{\mathbb{Q}}_p$.

2.1 Représentations galoisiennes p-adiques

Soit K et E deux extensions finies de $\mathbb{Q}_p$. Une représentation galoisienne locale p-adique est une représentation du groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ à coefficients dans E. De telles représentations interviennent couramment en géométrie arithmétique [1] et leur étude est devenue un sujet de recherche à part entière depuis les travaux fondateurs de Fontaine dans les années 1970 qui sont à l'origine de ce que l'on appelle maintenant la théorie de Hodge p-adique. Fontaine a dégagé en particulier les notions de représentations *cristallines* et *semi-stables* dont l'importance ne cesse de croître.

Mes recherches « traditionnelles » (directement issues de mes travaux de thèse) portaient sur ce domaine. Bien que mes centres d'intérêt aient évolué au cours des cinq dernières années, les problématiques de la théorie de Hodge p-adique sont encore fortement présentes dans mes recherches et, dans tout les cas, continuent de motiver la plupart de mes travaux.

2.1.1 Travaux antérieurs et habilitation à diriger les recherches

Références :
[1] X. Caruso, *Une contribution à la théorie de Hodge p-adique entière et de torsion*
[3] X. Caruso, *Représentations galoisiennes p-adiques et (φ,τ)-modules*
[10] X. Caruso, *Dimensions de certaines variétés de Kisin*

Durant les cinq dernières années ont été publiés les articles [3] et [10] qui correspondent à des travaux antérieurs. Par souci de concision, je ne les évoquerai pas davantage dans ce document. En juin 2011, j'ai soutenu mon habilitation à diriger les recherches à l'université de Rennes 1. À cette occasion, j'ai rédigé un document d'une soixantaine de pages [1] résumant mes principales contributions passées.

2.1.2 Réseaux dans les représentations semi-stables

Référence :
[11] X. Caruso, D. Lubicz, *Un algorithme de calcul de réseaux dans les représentations semi-stables*

Au fil de mes recherches, j'ai pu observer à plusieurs occasions que les calculs qui apparaissent en théorie de Hodge p-adique sont souvent laborieux, voire inextricables. C'est suite à cette constation que j'ai commencé à m'intéresser sérieusement aux aspects effectifs de la théorie. Dans cette optique, un premier travail que j'ai réalisé en collaboration avec David Lubicz a été la mise au point d'un algorithme de calcul de réseaux dans les représentations p-adiques semi-stables. Les principaux ingrédients qui apparaissent dans notre travail sont :

- d'une part, la théorie des modules de Breuil–Kisin qui donne une description des réseaux précédemment évoqués en termes d'objets d'algèbre semi-linéaire sur $\mathbb{Z}_p[[u]]$ et,
- d'autre part, une algorithmique efficace et prouvée pour la manipulation des séries p-adiques et des modules de type fini sur $\mathbb{Z}_p[[u]]$.

Cette algorithmique, dont il vient d'être question, a été développée pour l'occasion par nos soins et j'y reviendrai plus en détails au §2.2.1. Un résultat théorique intermédiaire qui joue un rôle central dans notre

1. La cohomologie des variétés algébriques en fournit par exemple un grand nombre.

travail est un théorème de surconvergence des modules de Breuil–Kisin qui me paraît intéressant en lui-même et pourrait être réutilisé et déboucher sur de nouvelles conséquences portant sur les représentations semi-stables.

Ce travail a donné lieu à une prépublication [11] ainsi qu'à une implémentation en SAGE qui, malheureusement, n'est pas aussi efficace que ce que nous l'aurions espéré *a priori*. Ce manque d'efficacité est, en grande partie, dû aux pertes de précision que nous majorons de façon trop brutale. C'est pour cette raison que, d'une part, que notre article est resté au stade de la prépublication et, d'autre part, que je me suis longuement intéressé par la suite à la gestion fine de la précision p-adique (voir §2.2.2).

2.1.3 Anneaux de déformations potentiellement Barsotti–Tate

Références :

[13] X. Caruso, A. David, A. Mézard, *Un calcul d'anneaux de déformations potentiellement Barsotti–Tate*

[14] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate*

En 2012, après avoir écouté un exposé d'Agnès David sur la question, j'ai entamé une collaboration avec Agnès David et Ariane Mézard sur la question du calcul explicite de certains anneaux de déformations galoisiennes, en lien avec les conjectures de type Breuil–Mézard qui sont l'une des pierres angulaires du programme de Langlands p-adique.

La situation que nous avons étudiée est la suivante. Soient f un entier naturel strictement positif et F l'unique extension non ramifiée de $\mathbb{Q}_p$ de degré f incluse dans $\bar{\mathbb{Q}}_p$. Soit $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}_p/F) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ une représentation de dimension 2. À $\bar{\rho}$ enrichi d'une donnée supplémentaire $\mathbf{t}$ que l'on appelle le *type galoisien*, on sait désormais associer une $\bar{\mathbb{Z}}_p$-algèbre $R(\mathbf{t}, \bar{\rho})$ qui « paramètre » les relevés $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/F) \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$ de $\bar{\rho}$ dont la restriction à un sous-groupe ouvert convenable provient d'un groupe p-divisible et qui vérifient une condition supplémentaire (qui s'exprime dans le langage de la théorie de Hodge p-adique) liée au type galoisien $\mathbf{t}$.

La compréhension fine des anneaux $R(\mathbf{t}, \bar{\rho})$ sus-mentionnés est importante pour les applications. Des présentations complètement explicites de ces anneaux avaient été obtenues par Breuil et Mézard dans le cas où le type galoisien $\mathbf{t}$ est *non ramifié* et la représentation $\bar{\rho}$ est *générique*. Avec Agnès et Ariane, nous sommes, pour la première fois, allés au-delà du cas générique. Dans un premier travail [13], nous avons obtenu des formules explicites pour $R(\mathbf{t}, \bar{\rho})$ en otant l'hypothèse de généricité sur $\bar{\rho}$ mais en nous restreignant, en contrepartie, au cas où $f = 2$ (*i.e.* $F = \mathbb{Q}_{p^2}$). Comme conséquence, nous avons réussi à calculer de nouvelles *multiplicités modulaires*, ce qui nous a permis de vérifier une conjecture de Kisin dans ce cas particulier.

À l'occasion de ce travail, nous avons constaté, que le cas non générique fait apparaître un lien manifestement très ténu entre les formules explicites obtenues $R(\mathbf{t}, \bar{\rho})$ et un autre objet géométrie : la *variété de Kisin* associée au couple $(\bar{\rho}, \mathbf{t})$. Poursuivant dans cette direction, nous avons calculé dans [14] les variétés de Kisin associées à tous les couples $(\bar{\rho}, \mathbf{t})$ comme ci-dessus. Le résultat obtenu s'exprime à l'aide d'un objet combinatoire simple que nous avons appelé le *gène* de $(\bar{\rho}, \mathbf{t})$. À partir du gène, nous proposons également une construction géométrique entièrement explicite — une suite d'éclatements et des complétés formels à partir d'un produit de copies de $\mathbb{P}^1$ — qui aboutit à une variété rigide p-adique qui, nous pensons, est un candidat sérieux pour être la fibre générique de Spf $R(\mathbf{t}, \bar{\rho})$. Afin d'asseoir notre conjecture sur de solides bases, nous sommes actuellement en train de vérifier sa compatibilité avec la conjecture de Breuil–Mézard (qui est démontrée dans le cas que nous considérons).

Le point de vue que nous avons adopté dans ce travail, qui met en avant les variétés de Kisin, a depuis été repris par plusieurs auteurs et a abouti, d'une part, à de nouveaux résultats explicites comparables à ceux que nous avons obtenu et, d'autre part, à une compréhension plus raffinée de la géométrie des espaces de déformations.

2.2 Algorithmique p-adique

Mon travail sur le calcul effectif de réseaux dans les représentations semi-stables (voir §2.1.2) m'a amené à m'intéresser à l'algorithmique des nombres et des structures p-adiques comme sujet à part entière. Et, de fait, je me suis rapidement rendu compte qu'il y avait beaucoup à dire sur le sujet, en tout cas beaucoup plus que je ne l'avais imaginé *a priori*.

Pour ne pas alourdir les notations, j'ai choisi de présenter tous les résultats de cette partie en me restreignant à $\mathbb{Q}_p$ mais tous s'étendent *verbatim* à un corps complet pour une valuation discrète. Dans tout ce qui suit, v_p désigne la valuation p-adique sur $\mathbb{Q}_p$.

2.2.1 Algorithmique des séries p-adiques

Références :
[4] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*,
[22] X. Caruso, D. Lubicz, *Algorithmics of $\mathfrak{S}_\nu$-modules*, librairie MAGMA
[23] X. Caruso, *Bounded series over ultrametric rings*, librairie SAGE

Directement en lien avec notre travail sur le calcul des réseaux dans les représentations semi-stables (voir §2.1.2), David Lubicz et moi-même nous sommes intéressés à concevoir une algorithmique efficace pour la manipulation des anneaux de séries p-adiques et des modules sur ceux-ci. Étant donné un nombre rationnel ν, notons $\mathfrak{S}_\nu$ l'anneau formé des séries $f(u) = \sum_{i=0}^{\infty} a_i u^i$ avec $a_i \in \mathbb{Q}_p$ et $v_p(a_i) \geqslant \nu i$. D'un point de vue rigide, $\mathfrak{S}_\nu$ (resp. $\mathfrak{S}_\nu[1/p]$) est l'anneau des séries convergentes et bornées par 1 (resp. convergentes et bornées) sur le disque ouvert D_ν de centre 0 et de rayon p^ν. Manipuler les éléments de $\mathfrak{S}_\nu$ présente quelques difficultés. En effet, représenter entièrement un tel élément demanderait de stocker un nombre infini de nombres p-adiques dans la mémoire d'un ordinateur, ce qui n'est manifestement pas possible. La solution la plus usuelle pour outrepasser cette difficulté est de travailler avec des approximations et c'est le point de vue que nous avons adopté dans notre travail.

Concrètement, nous avons choisi de représenter les éléments $\mathfrak{S}_\nu$ à l'aide de triplets de la forme $(\textit{approximation}, \textit{précision}, \textit{garantie})$. Les notions d'approximation et de précision sont classiques (pensez aux nombres réels !). La garantie, quant à elle, précise le comportement asymptotique des valuations des coefficients de la série lorsque l'indice i tend vers l'infini. Il s'agit, comme nous l'avons remarqué, d'une donnée indispensable à la mise en place d'une algorithmique. Avec cette représentation, nous avons démontré qu'il était possible d'effectuer les opérations arithmétiques élémentaires (addition, multiplication, division euclidienne, forme normale de Weierstrass) sur les éléments de $\mathfrak{S}_\nu$ et, plus généralement sur ceux de $\mathfrak{S}_\nu[1/p]$.

Forts de ces résultats, nous nous sommes ensuite intéressés à l'algorithmique des $\mathfrak{S}_\nu$-modules. Il nous est apparu rapidement qu'afin d'éviter une explosion exponentielle de la taille des objets, il était préférable de travailler à quasi-isomorphisme près, c'est-à-dire d'identifier deux modules $M_1 \subset M_2$ lorsque le quotient M_2/M_1 est de longueur finie. En effet, alors que les modules sur $\mathfrak{S}_\nu$ peuvent prendre des formes variées et complexes lorsqu'on les considère à isomorphisme près, ils se mettent à obéir à un théorème de structure relativement simple lorsqu'on ne les regarde qu'à quasi-isomorphisme près ; c'est, à peu de choses près, le théorème d'Iwasawa.

Continuant à travailler avec les approximations des éléments de $\mathfrak{S}_\nu$ introduites précédemment, nous avons conçu des algorithmes pour effectuer les opérations élémentaires (somme, intersection, *etc.*) sur les $\mathfrak{S}_\nu$-modules à quasi-isomorphisme près. Une conclusion intéressante de notre travail est qu'il n'est pas possible de travailler à ν fixé : chaque opération élémentaire oblige à diminuer ν d'une valeur strictement positive qui dépend de la précision et de la garantie que l'on a sur les entrées. En ce sens-là, le paramètre ν ne doit pas être considéré comme une donnée invariable du problème mais plutot comme une donnée de précision supplémentaire !

2.2.2 Une théorie de la précision p-adique

Références :
[6] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*,
[22] X. Caruso, D. Lubicz, *Algorithmics of $\mathfrak{S}_\nu$-modules*, librairie MAGMA
[21] X. Caruso, *p-adic precision*, librairie SAGE

J'ai expliqué précédemment que l'implantation des séries p-adiques sur ordinateur posaient des difficultés mais, plus fondamentalement, il en est déjà ainsi des nombres p-adiques eux-mêmes. En effet, ceux-ci sont composés d'une infinité de « chiffres » qui ne peuvent être stockés intégralement dans la mémoire d'un ordinateur. Ainsi, à l'instar des séries, il est d'usage dans les logiciels de calcul formel de

travailler avec des troncations qui prennent la forme $x + O(p^n)$ pour un certain entier n que l'on appelle la *précision absolue*. Ces troncations sont aisément manipulables. On a, par exemple :

$$\big(x_1 + O(p^{n_1})\big) + \big(x_2 + O(p^{n_2})\big) = x_1 + x_2 + O\big(p^{\min(n_1,n_2)}\big)$$

et il existe des formules analogues pour les autres opérations arithmétiques élémentaires : soustraction, multiplication, division. Cette manière de suivre la précision s'apparente à l'arithmétique d'intervalles utilisée avec les nombres réels et, malheureusement, elle surestime de la même manière les pertes de précision bien que la norme p-adique ne soit pas archimédienne.

Dans l'article [6], nous avons développé avec David Roe et Tristan Vaccon une alternative à cette approche qui a l'avantage décisif de l'optimalité. L'idée directrice de notre travail consiste à grouper les variables et à modéliser la précision sur un groupement de d variables non pas par un d-uplet $\big(O(p^{n_1}), O(p^{n_2}), \dots, O(p^{n_d})\big)$ comme on le ferait en « arithmétique d'intervalles » mais plutôt par un $\mathbb{Z}_p$-réseau dans $\mathbb{Q}_p^d$. On en vient ainsi à manipuler des quantités de la forme $\underline{x} + O(H)$ où $\underline{x} \in \mathbb{Q}_p^d$ et H est un $\mathbb{Z}_p$-réseau. Si maintenant $f : \mathbb{Q}_p^d \to \mathbb{Q}_p^n$ est une application de classe C^1 qui modélise une certaine opération d-aire, on définit l'image de $\underline{x} + O(H)$ comme étant $f(\underline{x}) + O(df_{\underline{x}}(H))$ où $df_{\underline{x}}$ désigne la différentielle de f en $\underline{x}$. Sous des hypothèses faibles, nous avons démontré que cette méthode aboutit à des résultats corrects mais, mieux encore, qu'elle aboutit à des résultats optimaux !

Cette approche différentielle a toutefois un inconvénient majeur puisque la donnée de précision $O(H)$ est devenue très volumineuse : il s'agit d'une matrice de taille $d \times d$ à coefficients dans $\mathbb{Q}_p$ [2] au lieu de seulement d (petits) entiers dans le cas de l'arithmétique d'intervalles. Les opérations que l'on effectue sur ces données de précision sont également beaucoup plus coûteuses ; ainsi, bien que notre approche théorique ait un parfum très prometteur au premier abord, il semblerait qu'elle soit *in fine* difficilement utilisable en pratique.

À ce problème, nous proposons une solution partielle. Il s'agit d'une méthode que nous avons appelée la *précision adaptative* qui, dans les bons cas, permet de conserver l'optimalité de l'approche différentielle ainsi que la souplesse et la simplicité de gestion de l'arithmétique d'intervalles. *Grosso modo*, l'idée est de mener les calculs comme on le ferait en arithmétique d'intervalles mais en s'autorisant en outre à augmenter arbitrairement la précision des variables à certaines étapes clés du calcul qui doivent être déterminées au préalable. En contrepartie, la méthode de la précision adaptative demande une étude théorique fine du problème posé qui peut s'avérer délicate dans certaines situations. Malgré tout, elle fonctionne de manière satisfaisante sur plusieurs exemples importants en algèbre linéaire (*e.g.* calcul de la décomposition LU) et en algèbre commutative (*e.g.* calcul de résultants et sous-résultants).

2.2.3 Algèbre linéaire p-adique

Références :
[7] X. Caruso, *Random matrices over a DVR and LU factorization*,
[9] X. Caruso, D. Roe, T. Vaccon, *p-adic stability in linear algebra*

Étude de la stabilité des opérations usuelles. À nouveau, avec David Roe et Tristan Vaccon, nous avons mis en application le cadre théorique développé dans [6] (voir §2.2.2) sur des exemples concrets issus de l'algèbre linéaire [9]. Nous avons, par exemple, étudié le comportement de la précision lors d'une suite de multiplications de matrices. Précisément, nous avons remarqué qu'une multiplication séquentielle de n matrices 2×2 aléatoires à coefficients dans $\mathbb{Z}_2$ conduit à une perte d'un nombre de chiffres significatifs qui est linéaire en n en moyenne pour un suivi sur le modèle de l'arithmétique d'intervalles tandis que celle-ci diminue à $O(\log n)$ lorsque l'on utilise un suivi de type différentiel. Dans ce cas particulier, la méthode différentielle présente un gain qui est donc tout à fait appréciable et justifie largement son utilisation malgré les complications qu'elle entraîne au niveau de la gestion de la précision (la taille en mémoire et la complexité ne sont multipliées que par un facteur constant, indépendant de n). Des phénomènes similaires se reproduisent dans plusieurs autres situations. Tel est le cas, par exemple, lorsque l'on calcule des intersections ou des sommes de sous-espaces vectoriels d'un certain $\mathbb{Q}_p$-espace vectoriel de dimension finie fixé. L'exemple de la décomposition LU traité plus en détails ci-dessous fait apparaître également le même type de comportement.

2. En pratique, il est possible de se ramener à $\mathbb{Z}/p^N\mathbb{Z}$ pour un entier N assez grand.

Un algorithme stable de factorisation LU. Un outil standard de l'algèbre linéaire effective est la factorisation LU. Elle se calcule usuellement à l'aide de l'algorithme du pivot de Gauss (ou de certaines variantes rapides mettant à profit les algorithmes de multiplication rapide des matrices). Malheureusement il se trouve que l'algorithme du pivot de Gauss est très instable dans le cadre p-adique. Précisément, j'ai démontré dans [7] que, dans le contexte d'un suivi de l'arithmétique d'intervalles, une exécution de cet algorithme sur des matrices aléatoires carrées de taille n à coefficients dans $\mathbb{Z}_p$ fait baisser la précision absolue de $\frac{n}{p-1}$ chiffres en moyenne ; autrement dit, si les coefficients de la matrice d'entrée sont tous connus à précision $O(p^N)$, certains coefficients des matrices L et U calculées par l'algorithme du pivot de Gauss ne seront connus qu'à précision $O(p^{N-c_1})$ avec $c_1 \approx \frac{n}{p-1}$.

En contrepartie, il existe des formules de type Cramer donnant une expression des coefficients de L et de U comme quotient de deux déterminants et il se trouve qu'en utilisant ces formules, on aboutit à une précision bien meilleure sur le résultat, à savoir $O(p^{N-c_2})$ avec $c_2 \approx \log_p n$. Malgré tout, cette approche n'est pas satisfaisante car l'évaluation de déterminants est coûteuse de sorte que l'algorithme résultant a une complexité inacceptable. Dans [7], je décris un nouvel algorithme pour le calcul de la décomposition LU qui combine les deux avantages : (1) une rapidité comparable à celle du pivot de Gauss (et même à ses variantes rapides) et (2) une stabilité numérique optimale démontrée. En un certain sens, mon algorithme peut être vu comme une variante de la méthode du pivot de Gauss sauf qu'il autorise, à chaque nouvelle réduction, le choix du pivot et permet d'éviter ainsi les pivots de petite norme qui nuisent à la stabilité.

2.2.4 Polynômes p-adiques

Références :
[15] X. Caruso, *Numerical stability of Euclide algorithm over ultrametric fields*
[16] X. Caruso, D. Roe, T. Vaccon, *Division and factorization of p-adic polynomials*

Division euclidienne et multiplication modulaire. De même que nous l'avions fait pour les matrices, nous avons étudié avec David Roe et Tristan Vaccon la stabilité des opérations usuelles sur les polynômes p-adiques et notamment celle de la division euclidienne et de la multiplication modulaire (c'est-à-dire la multiplication dans un anneau quotient $\mathbb{Q}_p[X]/M$ pour un certain polynôme M). D'une part, nous avons défini un modèle de précision construit à partir des polygones de Newton qui donne des résultats comparables à l'arithmétique d'intervalles mais permet une gestion plus rapide du suivi de précision : pour des polynômes de degré n en entrée, la complexité passe de $O(n^2)$ à $O(n \log n)$. D'autre part, de même que nous l'avions déjà fait avec les matrices, nous avons comparé les pertes de précision prédites par l'arithmétique d'intervalles aux pertes optimales données par la théorie de [6] dans le cadre de la multiplication modulaire. Les expériences que nous avons faites montrent une forte dépendance vis-à-vis du modulo M : lorsque M est un polynôme dont la réduction modulo p est irréductible ou lorsque M est un polynôme d'Eisenstein, l'arithmétique d'intervalles conduit à des résultats optimaux alors que ce n'est généralement pas du tout le cas pour les autres modulos. Cette observation justifie le fait (attendu) qu'il est largement souhaitable, lorsque l'on désire travailler dans une extension finie de $\mathbb{Q}_p$ de commencer par découper cette dernière en une première partie non ramifiée (donnée par un polynôme dont la réduction modulo p est irréductible) et une seconde partie totalement ramifiée (donnée par un polynôme d'Eisenstein).

Sur la stabilité de l'algorithme d'Euclide. Je me suis également intéressé à la stabilité de l'algorithme d'Euclide étendu pour le calcul du PGCD et des coefficients de Bézout. Le comportement que j'avais mis en évidence pour la factorisation LU (voir §2.2.3) se reproduit pratiquement à l'identique : d'une part, une exécution naïve de l'algorithme d'Euclide basée sur l'arithmétique d'intervalles conduit à des pertes de précision linéaires en le degré alors que, d'autre part, la théorie des résultants et sous-résultants fournit des formules explicites pour les coefficients du PGCD et des coefficients de Bézout qui, lorsqu'on les applique, conduisent à des pertes indépendantes du degré. Dans [15], j'étudie en détails ces phénomènes puis j'utilise la méthode de la précision adaptative développée dans [6] (voir §2.2.2) pour concevoir une version stabilisée de l'algorithme d'Euclide. Celle-ci combine deux avantages : celui de la rapidité (la complexité est identique à celle de l'algorithme d'Euclide classique) et celui de la stabilité (la précision sur les résultats calculés est quasi-optimale).

Un nouvel algorithme de factorisation par les pentes. La factorisation par les pentes — c'est-à-dire la factorisation relative aux pentes du polygône de Newton — des polynômes p-adiques est un outil classique et majeur autant d'un point de vue théorique qu'algorithmique. Elle a déjà fait l'objet de nombreuses études dans divers contextes mais, jusqu'à ce jour, tous les algorithmes rapides connus pour la calculer avaient l'inconvénient de devoir travailler, à un moment ou à un autre, dans une extension finie de $\mathbb{Q}_p$. Dans l'article [16] (encore en cours de rédaction), David Roe, Tristan Vaccon et moi-même avons proposé un nouvel algorithme qui évite cet écueuil mais conserve néanmoins la même complexité théorique et, du fait de sa simplicité, s'exécute légèrement plus rapidement en pratique. Il a en outre l'avantage d'être facilement adaptable à de nombreux autres contextes et, notamment, à un contexte non commutatif (voir §2.4.3 ci-après). Dans notre travail, nous avons également porté une attention particulière à l'analyse fine de la stabilité de notre algorithme dans le cadre de l'arithmétique d'intervalles puis dans celui de la précision différentielle. Nous comparons à nouveau les deux approches et concluons en expliquant comment utiliser la méthode de la précision adaptative pour bénéficier simultanément des avantages des deux approches.

2.3 Structures p-adiques aléatoires

Références :
[7] X. Caruso, *Random matrices over a DVR and LU factorization*
[15] X. Caruso, *Numerical stability of Euclide algorithm over ultrametric fields*
[19] X. Caruso, *Zeros of random p-adic polynomials*

Pour avoir une idée du comportement de mes algorithmes, j'ai souvent étudié leur complexité et leur stabilité moyennes lorsqu'ils sont appelés avec des entrées aléatoires. La notion d'aléatoire dans le cadre p-adique est facile à définir car $\mathbb{Z}_p$ est un groupe compact et hérite, par conséquent, d'une mesure de Haar qui est une mesure de probabilité. Concrètement, si les éléments de $\mathbb{Z}_p$ sont écrits sous la forme $\sum_{i=0}^{\infty} a_i p^i$ avec $a_i \in \{0, \dots, p-1\}$, les variables aléatoires a_i sont uniformément distribuées dans $\{0, \dots, p-1\}$ et indépendantes. Autrement dit, choisir un élément aléatoire de $\mathbb{Z}_p$ revient à choisir de manière indépendante chacun des a_i selon la mesure uniforme.

Dénominateurs dans la factorisation LU. Le premier exemple sur lequel je me suis attardé est celui de la factorisation LU en lien avec le travail que j'ai présenté au §2.2.3. Étant donnée une matrice carrée aléatoire M de taille n à coefficients dans $\mathbb{Z}_p$, je me suis demandé quelle était la plus petite valuation d'un coefficient d'un des deux facteurs intervenant dans la décomposition LU de M. J'ai obtenu une description alternative simple de cette variable aléatoire, à partir de laquelle j'ai pu démontrer que l'opposé de son espérance grandissait comme $\log_p n$ alors que son écart type était borné par une constante universelle (pouvant être choisie égale à 7). Ce résultat apparaît dans l'article [7] et est à l'origine des résultats sur les pertes de précision moyennes énoncés au §2.2.3.

Résultants de deux polynômes unitaires aléatoires. De manière similaire, afin d'étudier les pertes de précision lors de l'exécution de l'algorithme d'Euclide (étendu), je me suis intéressé aux variables aléatoires V_j donnant la valuation du j-ième sous-résultant scalaires de deux polynômes p-adiques aléatoires unitaires de degré fixé. J'ai réussi à reformuler cette question en termes purement combinatoires puis, à partir de là, à construire une famille de variables aléatoires secondaires W_j qui suivent la même moi que les V_j. En outre, les W_j possèdent une expression simple comme somme et infimum de variables aléatoires géométriques, ce qui permet d'accéder aisément à ses caractéristiques principales : moments, queue, *etc*. Cette étude constitue une part importante de l'article [15] où elle apparaît comme l'une des clés permettant de déterminer la complexité de la version stabilisée de l'algorithme d'Euclide que je propose dans *loc. cit*.

Répartition des racines des polynômes aléatoires. À la suite des deux travaux que je viens de présenter, j'ai commencé à m'intéresser aux polynômes p-adiques aléatoires pour eux-mêmes. C'est ainsi que j'ai étudié le nombre de zéros des polynômes aléatoires p-adiques ainsi que leur répartition. J'ai notamment démontré un analogue de la formule de Kac qui, dans le cadre p-adique, admet une formulation très simple et surprenante au premier abord : le nombre moyen de racines dans $\mathbb{Q}_p$ d'un polynôme p-adique

aléatoire de degré n à coefficients dans $\mathbb{Z}_p$ est 1, indépendamment de n et de p. De même que dans le cas réel, ce résultat peut être précisé de la manière suivante : on peut construire une densité ρ sur $\mathbb{Q}_p$ de manière à ce que, si Z_X désigne le nombre de racines dans X d'un polynôme aléatoire p-adique, on ait $\mathbb{E}[Z_X] = \int_X \rho(x)dx$ pour toute partie mesurable X de $\mathbb{Q}_p$. Les Z_X ne sont généralement pas indépendantes deux à deux mais j'ai mis au point une méthode générale pour étudier les corrélations entre elles. Tout ceci m'a permis d'étudier la répartition des zéros des polynômes aléatoires p-adiques en tant que processus. À ce niveau du travail, j'en suis venu à m'intéresser au comportement du processus sus-mentionné lorsque n tend vers l'infini et j'ai obtenu, à ce propos, un résultat de convergence faisant apparaître (sans grande surprise) une limite correspondant au processus donnant la répartition des zéros d'une série aléatoire p-adique. Enfin, lorsque p lui-même tend vers l'infini, j'ai démontré que le processus limite ci-dessus se rapproche (en un certain sens que l'on peut rendre précis) d'un processus de Poisson sur $\mathbb{Z}_p$ d'intensité 1.

2.4 Autour des polynômes de Ore

Les polynômes de Ore sont une variante non commutative des polynômes usuels : si R est un anneau muni d'un endomorphisme $\theta : R \to R$ et d'une θ-dérivation [3] ∂, l'anneau de Ore $R[X, \theta, \partial]$ est identique à l'anneau des polynômes usuels sur R sauf que la multiplication — non commutative, en général — est régie par la règle $Xa = \theta(a)X + \partial(a)$ pour $a \in R$. Ces polynômes interviennent en algèbre semi-linéaire et dans la théorie des équations différentielles linéaires au même titre que les polynômes usuels interviennent en algèbre linéaire. Leurs propriétés, et notamment leurs propriétés de factorisation, sont ainsi reliés à des résultats de décomposition (du type diagonalisation ou trigonalisation) concrets et directement exploitables.

2.4.1 Factorisation dans $\mathbb{F}_q[X, \theta]$

Références :
[12] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields*
[20] X. Caruso, *Skew polynomials over finite fields*, librairie SAGE

Soient $\mathbb{F}_q$ un corps fini de cardinal q et θ un automorphisme de $\mathbb{F}_q$. Concrètement, θ est une puissance du Frobenius : si $q = p^n$ (où p est un nombre premier et n est un entier), on a $\theta(x) = x^{p^s}$ où s est un entier défini modulo n. Dans la suite, on appelle r l'ordre de θ. Le sous-corps de $\mathbb{F}_q$ fixé par θ est ainsi $\mathbb{F}_{p^{n/r}}$; on le notera également $\mathbb{F}_q^{\theta=1}$ dans la suite. Avec Jérémy Le Borgne, nous avons étudié la factorisation dans l'anneau de Ore $\mathbb{F}_q[X, \theta, 0]$, que l'on notera plus simplement $\mathbb{F}_q[X, \theta]$ dans la suite. Notre motivation première était l'étude algorithmique des $\bar{\mathbb{F}}_p$-représentations galoisiennes d'un corps p-adique (*via* l'équivalence de catégories de Katz) mais les résultats que nous avons obtenus sortent largement de ce cadre et il nous a semblé nettement plus intéressant de les replacer et de les énoncer dans le langage des polynômes de Ore.

Nous avons dans un premier temps redécouvert un vieux théorème d'Ikehata qui affirme que $\mathbb{F}_q[X, \theta]$ est une algèbre d'Azumaya sur son centre $\mathbb{F}_q^{\theta=1}[X^r]$. Par la théorie générale des algèbres d'Azumaya, on dispose ainsi d'une norme réduite $\mathcal{N} : \mathbb{F}_q[X, \theta] \to \mathbb{F}_q^{\theta=1}[X^r]$. Nous avons établi un certain nombre de propriétés de $\mathcal{N}$ en lien avec la factorisation puis, en nous basant sur celles-ci, nous avons mis au point un algorithme probabiliste très rapide de factorisation dans $\mathbb{F}_q[X, \theta]$. Précisément, notre algorithme permet de se ramener à la factorisation dans le centre $\mathbb{F}_q^{\theta=1}[X^r]$ en temps *quasi-linéaire* en le degré d du polynôme d'entrée. Sachant que les meilleurs algorithmes connus pour la factorisation commutative ont actuellement une complexité quasi-linéaire en $d^{3/2}$, le goulot d'étranglement théorique se situe désormais à ce niveau.

Ce travail a donné lieu à la prépublication [12] (qui n'est pas encore publiée à cause des longueurs éditoriales excessives) qui inclut également, en guise de préliminaire, la description d'une algorithmique rapide pour l'arithmétique élémentaire dans l'anneau de Ore $\mathbb{F}_q[X, \theta]$; de nouveaux algorithmes pour la multiplication, la division euclidienne et le calcul de PGCD dans ce cadre non commutatif sont notamment proposés. J'ai également écrit une librairie SAGE [20] dans laquelle tous les algorithmes de l'article sont implantés. Nous avons pu constater que ceux-ci sont efficaces en pratique et permettent par exemple de factoriser en quelques minutes maximum des polynômes de degré 500 dans $\mathbb{F}_{5^3}[X, \theta]$ où $\theta : x \mapsto x^5$ est le Frobenius usuel.

3. Une θ-dérivation ∂ est une application additive vérifiant la règle de Leibniz tordue $\partial(ab) = \theta(a)\partial(b) + b\,\partial(a)$.

2.4.2 Sur la p-courbure des opérateurs différentiels

Références :
[5] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the characteristic polynomial of the p-curvature*
[8] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the p-curvature*
[17] A. Bostan, X. Caruso, É. Schost, *Computation of the similarity class of the p-curvature*

Si k est un corps de caractéristique p, l'anneau de Ore $k(x)[\partial, \mathrm{id}, \frac{d}{dx}]$ — noté plus traditionnellement $k(x)\langle\partial\rangle$ — jouït de propriétés analogues à $\mathbb{F}_q[X,\theta]$. Par exemple, ce sont tous les deux des algèbres d'Azumaya et ils sont en particulier tous les deux munis d'une norme réduite. Dans le cas différentiel, il s'agit d'une application multiplicative $\mathcal{N} : k(x)\langle\partial\rangle \to k(x^p)[\partial^p]$ qui possède à nouveau des propriétés agréables en lien avec la factorisation. Dans [5], nous avons démontré, avec Alin Bostan et Éric Schost, que $\mathcal{N}(L)$ s'identifie, à une renormalisation près, au polynôme caractéristique de la p-courbure du système différentiel associé à L. Nous avons en outre utilisé ce résultat pour concevoir un algorithme de calcul du polynôme caractéristique de la p-courbure dont la complexité vis-à-vis de p est quasi-linéaire en $\sqrt{p}$. Il s'agit d'un résultat remarquable car la taille de la p-courbure elle-même grandit généralement de manière linéaire par rapport à p (alors que celle de son polynôme caractéristique n'est qu'en $O(\log p)$) ; en particulier, notre algorithme évite le calcul de la p-courbure.

Avec les mêmes auteurs, nous nous sommes par la suite intéressés au calcul « complet » de la p-courbure et avons obtenu, pour ce problème, un algorithme quasi-optimal [8]. Notre méthode consiste à plonger $k(x)$ dans un anneau de séries formelles à puissances divisées sur lequel on dispose d'un analogue du théorème de Cauchy–Lipschitz. La p-courbure s'interprète alors en termes d'un système fondamental de solutions et peut-être calculée efficacement *via* une itération de Newton. Il est à noter que l'algorithme résultant est fortement parallélisable et s'étend sans diffilculté supplémentaire aux systèmes différentiels quelconques. Dans un troisième volet de ce travail qui est en cours de rédaction [17], nous avons adapté la méthode esquissée ci-dessus au calcul des invariants de similitude de la p-courbure. À l'instar du polynôme caractéristique, ceux-ci ont une taille qui ne grandit que logarithmiquement vis-à-vis de p et il est donc envisageable de pouvoir les calculer plus rapidement. Le résultat que nous avons obtenu est un algorithme résolvant ce problème pour un coût quasi-linéaire en $\sqrt{p}$.

2.4.3 Un théorème de factorisation par les pentes

Référence :
[18] X. Caruso, *Slope factorization of Ore polynomials*

Je me suis enfin intéressé à la factorisation des polynômes de Ore définis sur des corps valués complets (pour une valuation de rang 1). J'ai étendu la notion de polygone de Newton et ai obtenu un théorème de factorisation par les pentes dans cette généralité. La démonstration de ce dernier thèorème est effective dans le sens où elle fournit un algorithme de factorisation. J'ai étudié la stabilité de cet algorithme à l'aide des outils introduits au §§2.2.2–2.2.4 et j'en ai proposé, dans le cas où cela était nécessaire, des versions stabilisées. Plusieurs corollaires intéressants se déduisent de ce résultat selon les anneaux de Ore auxquels on l'applique. Par exemple, dans le cas de $\mathbb{Q}_q[X, \mathrm{Frob}]$, le théorème de factorisation n'est autre que le théorème classique de Dieudonné–Manin et l'algorithme correspondant peut être facilement utilisé pour calculer une décomposition de Dieudonné–Manin. De manière semblable, lorsque l'anneau de Ore $\mathbb{F}_p((u))[X,\theta]$ où θ envoie u sur u^p, le théorème de factorisation correspond *via* l'équivalence de catégorie de Katz à un théorème de décomposition des $\bar{\mathbb{F}}_p$-représentations galoisiennes du groupe de Galois absolu d'un corps p-adique et, à nouveau, l'algorithme de factorisation permet d'exhiber une telle décomposition. On retrouve comme ceci des résultats de la thèse de Jérémy Le Borgne que j'avais encadrée lors du quadriennal précédent. Pour appliquer le théorème dans le cas différentiel, le plus simple est de travailler sur le corps résiduel du point générique d'une courbe de Berkovich. Le théorème de factorisation s'instancie alors en un théorème effectif de décomposition des équations différentielles p-adiques selon le rayon de convergence. Une analyse de la démonstration permet en outre de relever cette décomposition sur un voisinage explicite du point générique considéré. Dans le même contexte, le théorème de factorisation peut également être utilisé pour éviter l'explosion rapide des degrés dans un algorithme de Pulita du calcul des rayons de convergence d'une équation différentielle p-adique ; avec cette modification, la complexité de l'algorithme de Pulita devient polynomiale alors qu'elle était exponentielle dans sa version initiale.

3 Enseignement, formation et diffusion de la culture scientifique

Enseignement et formation

Cours de M1

En 2011-2012 et 2012-2013, j'ai donné le cours d'*Algorithmique de base* du M1 du master cryptographie de Rennes. Cela a été pour moi l'occasion de compléter ma formation en algorithmique qui était restée, malgré tout, relativement superficielle.

En 2013-2014, j'ai donné le cours d'*Algèbre commutative* et d'*Introduction à la géométrie algébrique* du M1 de recherche en mathématiques de Rennes.

J'ai participé également occasionnellement à la préparation à l'agrégation en étant jury dans des oraux blancs.

Stages de M2

En 2010-2011, j'ai encadré les stages de M2

- de Tristan Vaccon : le sujet, très classique, consistait à comprendre et à exposer la théorie du corps de classes
- de Cao Tung Pham : le sujet, également très classique, consistait à comprendre et à exposer, la théorie de vecteurs de Witt et son application à la théorie de Artin-Schreier-Witt

Direction de thèse

La thèse de Jérémy Le Borgne. Avec David Lubicz, nous avons codirigé la thèse de Jérémy Le Borgne de septembre 2009 à avril 2012. Sa thèse portait sur l'étude algorithmique des φ-modules ou des (φ, Γ)-modules sur les anneaux de séries formelles et sur les applications aux représentations galoisiennes de corps p-adiques.

La thèse de Tristan Vaccon. J'ai encadré la thèse de Tristan Vaccon de septembre 2011 à juillet 2015. Sa thèse portait sur l'algorithmique des nombres p-adiques. Elle se découpe en deux parties : la première met en place un cadre théorique pour le suivi de la précision p-adique et le met en application dans plusieurs situations concrètes simples tandis que la seconde est focalisée sur l'étude des bases de Gröbner sur un corps p-adique.

La thèse de Charles Savel. J'ai encadré la thèse de Tristan Vaccon de septembre 2011 à octobre 2015. Sa thèse portait sur l'étude de certaines variétés de Kisin. Son travail a consisté à étendre les résultats de mon article [10] au cas du groupe réductif $\mathrm{Res}_{k/\mathbb{F}_p}\mathrm{GL}_n$ où k est une extension finie de $\mathbb{F}_p$.

Le séminaire Mathematic Park

En janvier 2010, j'ai été l'instigateur du séminaire *Mathematic Park* et en suis depuis le principal organisateur. Le séminaire, qui se réunit en moyenne une fois par mois (hors vacances scolaires) à l'IHP, est destiné aux étudiants en mathématiques de la première année à la thèse. Les exposés sont donnés par des chercheurs en mathématiques reconnus et portent sur des thèmes variés. Le séminaire connaît un succès appréciable : entre 50 et 150 participants à chaque séance, sachant que certains périodes de l'année sont plus propices que d'autres. Le programme du séminaire est disponible sur le site :

http://www.ihp.fr/fr/seminaire/mathematic-park

dont je suis le webmaster. Depuis 2013, les exposés sont filmés par l'IHP et déposés sur Youtube. Chaque exposé compte entre 1000 et 7000 vues.

Pendant deux ans, entre 2011 et 2013, j'ai organisé une réplique rennaise du séminaire Mathematic Park au lycée Chateaubriand pour les élèves de classes préparatoires. Depuis l'an dernier, cette réplique a été déplacée à l'université de Rennes 1 et placée sous la tutelle du centre Henri Lebesgue ; elle s'adresse

désormais aux étudiants de l'université et s'appelle à présent *Mathematic World*. Depuis cette modification, les exposés sont également filmés.

Bicentenaire de la naissance de Galois

En 2011, j'ai participé au comité d'organisation des célébrations en l'honneur du bicentenaire de la naissance d'Évariste qui ont eu lieu à l'IHP. En particulier :

- j'ai été webmaster du site http://galois.ihp.fr/
- j'ai rédigé trois articles de vulgarisation pour le site ci-dessus dont voici les titres :
  (1) [26] *Les imaginaires de l'arithmétique*
  (2) [30] *De l'ambiguité des puzzles aux idées de Galois* (avec B. Teheux)
  (3) [31] *À propos de l'image du mug*
  et en ai sollicité trois autres dont voici les titres :
  (4) *Galois et le jeu de taquin* (par M. Coste)
  (5) *Résolution des équations de degré* 3 *et* 4 (par A. Marrakchi)
  (6) *Représentations galoisiennes et théorème de Fermat-Wiles* (par B. Edixhoven)
- j'ai donné plusieurs interviews.

Rédacteur à *Images des Mathématiques*

En janvier 2013, je suis entré dans le comité de rédaction de la revue en ligne *Images des Mathématiques* (IdM) en tant que responsable de la rubrique *L'IHP, une maison de sciences pour tous*. Le premier événement que j'ai couvert dans ce cadre est le festival *Futur en Seine* de 2013. Dans ce cadre, j'ai préparé deux animations et ai rédigé un article pour expliquer chacune d'elle :

(1) [32] *Au feu les pompiers — L'algorithme de Ford–Fulkerson* (avec L. Fourquaux)

(2) [34] *Qui est-ce ? — Le codage de Hamming*

J'ai depuis rédigé et sollicité plusieurs autres articles dans ce cadre [35, 36, 37].

Les semestres du Centre Henri Lebesgue

Le centre Henri Lebesgue est un LabEx regroupant les laboratoires de mathématiques des universités de Rennes, Nantes, Angers et Brest et de l'ÉNS Rennes. Chaque année, il organise un semestre thématique et j'ai été nommé coordinateur avec Michele Bolognesi et Christophe Mourougane de celui de géométrie qui s'est déroulé de mars à septembre 2014. Huit événements qui ont réuni, au total, plus de 500 participants ont été organisés dans le cadre de ce semestre.

En plus de la supervision générale du semestre, j'ai pris la charge d'organiser avec François Charles, Michel Gros et Christophe Mourougane une école de printemps sur les théories de Hodge classique et p-adique. Elle s'est déroulée sur deux semaines à Rennes et a réuni plus d'une centaine de participants venant de nombreux pays du monde entier.

À l'issue de ce semestre, j'ai écrit un logiciel — un module DRUPAL précisément — pour aider à la gestion des semestres à venir et des événements individuels organisés dans le cadre du CHL [25]. Mon logiciel est relativement complet : il s'occupe de la création et de la mise à jour de la page web, il gère les inscriptions avec très peu d'intervention extérieure, il émet les ordres de mission et intervient enfin dans les paiements en ligne et la facturation. Il est désormais utilisé couramment et est, je pense, très apprécié de tous les acteurs, enseignants-chercheurs et gestionnaires, intervenant dans l'organisation d'un semestre.

Les 5 minutes Lebesgue

Depuis novembre 2015, je suis le cofondateur et le coorganisateur avec San Vũ Ngọc du séminaire hebdomadaire « Les 5 minutes Lebesgue ». Il s'agit d'un séminaire d'un genre particulier puisque les exposés ne durent que cinq minutes mais sont filmés puis mis en ligne sur le site du CHL et sur Youtube.

Je me suis, moi-même, très récemment essayé à l'exercice en donnant un exposé dans ce cadre sur les nombres p-adiques.

Autres

Voici quelques autres activités auxquelles je participe mais pour lesquelles je suis, de fait, relativement peu impliquées :

- les journées Louis-Antoine à Rennes : mon rôle se limite essentiellement à réserver les pauses café ;
- le stage MathC2+ qui a lieu tous les ans à Ker-Lann : j'ai proposé plusieurs sujets et ai participé une fois au café des métiers ;
- le festival des sciences à Rennes où j'ai encadré plusieurs animations.

4 Transfert technologique, relations industrielles et valorisation

5 Encadrement, animation et management de la recherche

Projets ANR

De 2009 à 2013, j'ai été le coordinateur du projet ANR CETHop. À ce titre, j'ai écrit le site web http://cethop.cnrs.math.fr/. Outre le contenu standard — liste des membres de l'ANR, liste des publications réalisées dans le cadre de l'ANR, *etc.* — ce site héberge un « SAGE Notebook », *i.e.* un serveur sur lequel n'importe qui peut demander un compte lui permettant d'utiliser en ligne les librairies MAGMA et SAGE développées dans le cadre du projet. Toujours dans ce cadre, j'ai également organisé plusieurs événements internationaux d'une semaine chacun :

- une à l'ENS de Lyon en juin 2011 qui s'intitulait « Théorie de Hodge p-adique, équations différentielles p-adiques et leurs applications » et qui a réuni environ 60 participants ;
- une à Luminy en avril 2013 qui s'intitulait « Représentations galoisiennes et théorie de Hodge p-adique : aspects théoriques et effectifs » et qui a réuni environ 50 participants.
- Des SAGE *Days* en septembre 2013 portant sur le développement des nombres p-adiques qui ont réuni environ 15 participants.

Très récemment, en octobre 2015, avec l'aide d'Ariane Mézard, nous avons monté une nouvelle équipe et, ensemble, nous avons déposé un nouveau préprojet ANR intitulé « Correspondance de Langlands p-adique : une approche constructive et algorithmique » (CLap–CLap) dont je suis pressenti pour être le coordinateur.

Membres de conseils/comités

Je suis, ou j'ai été, membre de plusieurs comités ou conseils, à savoir :

- le conseil de l'IRMAR (Institut de Recherche en Mathématiques à Rennes),
- le comité scientifique du séminaire de cryptographie de Rennes,
- le comité de pilotage du master cryptographie de Rennes,
- le comité de culture scientifique de l'IHP.

Concrètement, pour chacun de ces items, il s'agit de quelques réunions par an (entre 2 et 4).

Comité National de la Recherche Scientifique (CoNRS)

Depuis septembre 2012, comme vous le savez, je suis membre élu du CoNRS. Dans ce cadre, j'ai en particulier participé comme expert à l'évaluation du l'*Institut Mathématique de Bordeaux* en 2014 et du *Laboratoire de Mathematiques Nicolas Oresme* à Caen en 2015.

B. Objectifs

Comme je l'ai expliqué dans mon rapport d'activités, mes centres d'intérêt se sont beaucoup diversifiés au cours des cinq dernières années. Après cette période d'ouverture thématique, je pense que le temps de la stabilisation et de l'approfondissement est arrivé. C'est ainsi que, pour les dix prochains semestres, j'envisage pour l'essentiel de poursuivre mes recherches récentes au sein des quatre directions évoquées dans mon rapport d'activités, à savoir (1) les espaces de déformations de représentations galoisiennes, (2) l'algorithmique et précision p-adiques, (3) les structures aléatoires p-adiques et (4) les polynômes de Ore et leurs applications aux équations différentielles linéaires. Ci-après je détaille, pour chacun de ces items séparément, quelques questions et quelques problèmes sur lesquels je projette de me pencher.

Espaces de déformations de représentations galoisiennes

Il s'agit ici de poursuivre le travail que j'ai entamé avec Agnès David et Ariane Mézard qui est encore loin d'être achevé. En effet, comme je l'ai expliqué au §2.1.3 de mon rapport d'activités, notre dernier article [14] se concluait par la construction explicite de candidats potentiels à être la fibre générique (au sens des variétés rigides) de certains espaces de déformations. Toutefois, nous n'avons pour l'instant que très peu étudié cette construction ; en particulier, nous ne disposons pas actuellement de formule explicite pour les candidats sur lesquels notre construction débouche (ni même pour leurs réductions modulo p) et ne savons pas davantage démontré qu'ils possèdent les propriétés attendues (ni même seulement certaines d'entre elles). Un premier travail envisagé consiste donc à trouver des réponses satisfaisantes à ces questions.

Une fois que cela sera fait, j'aimerais me concentrer sur d'autres questions connexes allant au delà des cas particuliers que nous avons considéré jusqu'alors. La première d'entre elles concerne à oter une limitation génante de notre approche, à savoir l'hypothèse de ramification modérée que nous avons sur le type galoisien. Le souci principal dans cette affaire est que la théorie de Breuil–Kisin fonctionne assez mal pour des représentations potentiellement semi-stables qui ne deviennent semi-stables qu'après restriction à une extension sauvagement ramifiée. J'aimerais améliorer la théorie sur ce point afin d'en déduire, dans un second temps, de nouveaux calculs explicites d'anneaux de déformations. Par certains aspects, ce projet est lié à certains résultats récents de Laurent Berger ; voilà pourquoi j'envisage comme possibilité de lui proposer de travailler avec moi sur ce sujet.

Une seconde question, qui est d'apparence plus technique, mais qui me semble tout aussi importante est celle de la stratification des variétés de Kisin. En effet, à deux reprises et dans deux contextes *a priori* différents, un ingrédient essentiel dans mon travail a consisté à définir par des méthodes *ad hoc* une stratification appropriée sur certaines variétés de Kisin. La question se pose ainsi naturellement de savoir si l'on peut unifier les méthodes et construire, ce faisant, des stratifications intéressantes sur toutes les variétés de Kisin. Récemment Cariani et Levin se sont penchés sur cette question mais je n'ai pas encore d'étudier leur travail avec l'attention qu'il mérite.

J'ai récemment déposé, en tant que coordinateur, le préprojet ANR « Correspondance de Langlands p-adique : une approche constructive et algorithmique » (CLap–CLap) dans lequel j'évoque (entre autres) les questions mentionnées ci-dessus.

Algorithmique et précision p-adiques

Il est apparu, dans mon rapport d'activités, que la majeure partie de ma recherche de ces cinq dernières années a été consacrée à l'étude des problèmes de stabilité numérique dans un contexte p-adique (ou plus généralement ultramétrique). Il s'agit, en fait, d'une thématique nouvelle que j'ai, semble-t-il, été le premier à étudier de manière systématique. Afin que celle-ci ne soit pas laissée à l'abandon, je compte m'y investir encore de manière importante dans les années à venir. Il demeure notamment un certain nombre de questions que j'aimerais étudier ; tel est le cas, par exemple, du calcul stable et efficace du polynôme caractéristique d'une matrice p-adique ; ceci me semble particulièrement intéressant pour les applications potentielles (*e.g.* algorithmes de comptage de points à la Kedlaya, bases de Grobner).

Comme objectif à plus long terme, qui pourrait être considéré en un certain sens comme un aboutissement de tout ce travail, je me propose d'améliorer (grandement !) la stabilité numérique de mon algorithme (développé conjointement avec David Lubicz) de calcul de réseaux dans les représentations semi-stables dans l'espoir de le rendre utilisable en pratique sur des exemples de taille raisonnable.

Finalement, afin de sensibiliser les algorithmiciens aux avantages du p-adique et, en même temps, de les familiariser à l'analyse ultramétrique, j'ai le projet d'écrire un livre complet sur le thème de la précision p-adique. J'ai été invité à donner un cours sur ce sujet aux *Journées nationales de calcul formel* en 2017 ; cela sera certainement l'occasion de me plonger entièrement dans ce projet.

Structures aléatoires p-adiques

Mes travaux sur les matrices et polynômes p-adiques aléatoires m'ont fait prendre goût à ce sujet dans lequel, à l'aide de méthodes souvent élémentaires, on aboutit à des résultats à la fois simples, précis, élégants et parfois même surprenants. Une question qui m'intéresse particulièrement en ce moment est celle de comprendre la loi d'un produit d'un grand nombre de matrices aléatoires à coefficients p-adiques. Ma principale motivation pour cela est une meilleure compréhension du comportement des pertes de précision lors de l'exécution d'un algorithme « générique » mais il est clair que la portée de la question posée dépasse cette application particulière : elle devrait par avoir aussi des conséquences en dynamique p-adique et aller vers une meilleure compréhension des exposants de Liapounov dans ce contexte.

Polynômes de Ore et équations différentielles

Lors de mes récents travaux avec Alin Bostan et Éric Schost, nous avons introduit de nouvelles méthodes pour calculer efficacement (les principaux invariants de) la p-courbure des opérateurs différentiels de $k(x)\langle\partial\rangle$ (où k est un corps de caractéristique p). Or, aussi bien du point de vue théorique qu'algorithmique, la p-courbure est classiquement utilisée comme un ingrédient primordial à la factorisation. Il paraît donc naturel que nous nous intéressions à présent au problème de la factorisation des opérateurs différentiels en caractéristique p. En combinant les techniques que nous avons introduites avec celles de l'article [12] que j'ai coécrit avec Jérémy Le Borgne, nous pensons pouvoir aboutir à un algorithme complet de factorisation dont la complexité serait quasi-linéaire vis-à-vis du paramètre p. Une difficulté majeure est toutefois attendue : l'utilisation des techniques sus-mentionnés demandera certainement d'étendre notre cadre d'étude à des opérateurs différentiels définis sur des courbes générales (et non plus uniquement sur la droite projective). À première vue, cela ne semble pas poser problème du point de vue théorique. Il n'en va pas de même cependant de l'algorithmique car, de ce point de vue, cela fait une différence notable de travailler dans le corps $k(x)$ ou dans l'une de ses extensions finies possiblement sauvagement ramifiées.

Un autre thème que j'aimerais aborder dans mes recherches futures est la continuation de mon travail (encore en cours de rédaction) sur la factorisation par les pentes de polynômes de Ore [18]. Jusqu'à présent, je me suis limité au cas où le corps de base est valué complet (pour une valuation de rang 1). Or, les corps valués complets apparaissent comme les points de la géométrie de Berkovich. En utilisant des arguments géométriques d'extension à un voisinage et de recollement, j'ai bon espoir de pouvoir étendre mon théorème à des espaces géométriques « globaux » comme, par exemple, des courbes analytiques p-adiques. Un tel résultat pourrait avoir plusieurs applications intéressantes. Dans le contexte des équations différentielles, premièrement, il redonnerait un théorème de décomposition globale des équations différentielles p-adiques (selon le polygone de Newton des rayons de convergence) et, de surcroît, le complèterait par un algorithme calculant cette décomposition. Deuxièmement, appliqué dans un contexte d'algèbre semi-linéaire, il donnerait un théorème effectif de décomposition des fibrés sur (certains ouverts de) la courbe de Fargues–Fontaine qui s'inscrirait dans la continuité des travaux de Fargues, Fontaine, Kedlaya, Liu, Scholze...

Je conclus en mentionnant que les deux sujets que je viens de présenter me semblent suffisamment mûrs et complets pour donner lieu à de bons sujets de thèse. J'envisage donc la possibilité — sans pour autant m'être fermement décidé pour l'instant — de les proposer à des étudiants.

MA BIBLIOGRAPHIE DES DIX DERNIERS SEMESTRES

Mémoire écrit pendant les 10 derniers semestres

[1] X. Caruso, *Une contribution à la théorie de Hodge p-adique entière et de torsion*, mémoire d'habilitation (2011), 62 pages

Articles de recherche publiés pendant les 10 derniers semestres

[2] X. Caruso, *Application des fractions continues à la construction des gammes musicales*, RMS 123-1 (2012), 11 pages
[3] X. Caruso, *Représentations galoisiennes p-adiques et (φ, τ)-modules*, Duke Math. J. **162** (2013), 2525–2607
[4] X. Caruso, D. Lubicz, *Linear Algebra over $\mathbb{Z}_p[[u]]$ and related rings*, LMS J. Comput. Math. **17** (2014), 302–344
[5] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the characteristic polynomial of the p-curvature*, proceddings de la conférence ISSAC 2014
[6] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*, LMS J. Comput. Math. **17** (2014), 274–294
[7] X. Caruso, *Random matrices over a DVR and LU factorization*, J. Symbolic Comput. **71** (2015), 98–123
[8] A. Bostan, X. Caruso, É. Schost, *A fast algorithm for computing the p-curvature*, proceddings de la conférence ISSAC 2015
[9] X. Caruso, D. Roe, T. Vaccon, *p-adic stability in linear algebra*, proceddings de la conférence ISSAC 2015
[10] X. Caruso, *Dimensions de certaines variétés de Kisin*, à paraître à J. reine angew. Math.

Prépublications écrites pendant les 10 derniers semestres et travaux en cours

[11] X. Caruso, D. Lubicz, *Un algorithme de calcul de réseaux dans les représentations semi-stables*, prépublication (2013), 35 pages
[12] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields*, prépublication (2013), 32 pages
[13] X. Caruso, A. David, A. Mézard, *Un calcul d'anneaux de déformations potentiellement Barsotti–Tate*, prépublication (2014), 57 pages
[14] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate* prépublication (2015), 44 pages
[15] X. Caruso, *Numerical stability of Euclide algorithm over ultrametric fields*, prépublication (2015), 22 pages
[16] X. Caruso, D. Roe, T. Vaccon, *Division and factorization of p-adic polynomials*, en préparation
[17] A. Bostan, X. Caruso, É. Schost, *Computation of the similarity class of the p-curvature*, en préparation
[18] X. Caruso, *Slope factorization of Ore polynomials*, en préparation
[19] X. Caruso, *Zeros of random p-adic polynomials*, en préparation

Logiciels écrits pendant les 10 derniers semestres

[20] X. Caruso, *Skew polynomials over finite fields*, librairie SAGE (2013), $\sim$ 8000 lignes[4]
[21] X. Caruso, *p-adic precision*, librairie SAGE (2013), version préliminaire, $\sim$ 5000 lignes
[22] X. Caruso, D. Lubicz, *Algorithmics of $\mathfrak{S}_\nu$-modules*, librairie MAGMA (2013), $\sim$ 2000 lignes
[23] X. Caruso, *Bounded series over ultrametric rings*, librairie SAGE (2013), version non documentée, $\sim$ 3000 lignes
[24] X. Caruso, *Lattices in semi-stable representations*, librairie SAGE (2013), version préliminaire $\sim$ 1500 lignes
[25] X. Caruso, *Utilitaire pour la gestion des conférences et des semetres du CHL*, librairie DRUPAL (2014), $\sim$ 5000 lignes

Articles de vulgarisation écrits pendant les 10 derniers semestres

[26] X. Caruso, *Les imaginaires de l'arithmétique*, Images des Mathématiques (2011)
[27] X. Caruso, *Logiciels de topologie et de géométrie*, Images des Mathématiques (2011)
[28] X. Caruso, *Mathematic Park*, Images des Mathématiques (2011)
[29] X. Caruso, B. Teheux, *De l'ambiguité des puzzles aux idées de Galois*, Images des Mathématiques (2011)
[30] X. Caruso, B. Teheux, *Quel est ce nombre ?*, Images des Mathématiques (2011)
[31] X. Caruso, *À propos de l'image du mug*, disponible à http://www.galois.ihp.fr/ressources/vie-et-oeuvre-de-galois/les-mathematiques-de-galois/a-propos-de-limage-du-mug/
[32] X. Caruso, L. Fourquaux, *Au feu les pompiers — L'algorithme de Ford-Fulkerson*, Images des Mathématiques (2013)
[33] X. Caruso, *Qui est-ce ? — Le codage de Hamming*, Images des Mathématiques (2013)
[34] X. Caruso, *Brainpop français*, Images des Mathématiques (2013)
[35] X. Caruso, *Des mathématiques à la photographie numérique : bruit, dynamique*, Images des Mathématiques (2014)
[36] X. Caruso, *À la conquête du nord-est*, Images des Mathématiques (2014)
[37] X. Caruso, *L'IHP fait son ciné-club*, Images des Mathématiques (2014)

4. Pour une comparaison avec un article, on peut compter 100 lignes pour une page.