Acronyme	**CETHop**
Titre du projet en français	Calculs effectifs en théorie de Hodge p-adique
Titre du projet en anglais	Effective computations in p-adic Hodge theory
CSD Principale	5. Mathématiques et interactions
CSD Secondaire (si interdisciplinarité)	

Aide totale demandée	238 789 €	**Durée du projet**	48 mois

Sommaire

1 Contexte et positionnement du projet / *Context and positionning of the proposal*

Notre projet a pour but d'introduire l'outil algorithmique dans la théorie de Hodge p-adique, qui pour l'instant est essentiellement développée d'un point de vue théorique.

La théorie de Hodge p-adique est une branche de l'arithmétique qui s'est développée depuis les années 70 principalement en France sous l'impulsion de Jean-Marc Fontaine. Elle a pour but d'étudier les représentations p-adiques du groupe de Galois absolu d'un corps p-adique, et notamment les représentations obtenues *via* la cohomologie étale des variétés, parfois qualifiées de « géométriques ». Les premiers travaux de Fontaine étaient à l'origine motivés par la compréhension des groupes de cohomologie étale qui ont la vertu de coder une très grande quantité d'information concernant la variété, notamment au travers des fonctions L et ζ. Aujourd'hui, la théorie a pris un essor considérable et son champ d'application s'étend à une partie importante de l'arithmétique. Elle intervient par exemple de façon centrale dans l'étude des formes modulaires (sur laquelle repose en particulier la démonstration par Andrew Wiles du grand théorème de Fermat), ou la correspondance de Langlands p-adique initiée récemment par Christophe Breuil, et à l'avenir très prometteur (voir [119]). Il faut savoir à ce sujet que la correspondance de Langlands usuelle revêt une importance de tout premier plan dans notre domaine, comme en témoigne la médaille Fields décernée en 2002 à Laurent Lafforgue.

Ce développement fulgurent de la théorie de Hodge p-adique s'est accompagné d'une multiplication et d'une complexification des objets, à tel point qu'il devient très difficile aujourd'hui de faire des calculs concrets, et même d'exhiber des exemples. C'est ce manque que nous souhaitons combler par l'intermédiaire de ce projet. Précisément, nous nous proposons de mettre au point — et d'implémenter — des algorithmes dont le but sera de jongler efficacement avec les diverses structures qui interviennent en théorie de Hodge p-adique. Ces algorithmes pourront en outre être utilisés clé en main par tout un chacun, et seront utiles aussi bien à l'utilisateur occasionnel (qui n'a peut-être pas envie de comprendre tous les rouages de la théorie pour avoir accès au résultat qui l'intéresse) qu'à l'expert (qui pourra les utiliser efficacement dans son travail quotidien).

Comme nous venons de l'expliquer, le point de vue par lequel nous souhaitons aborder la théorie de Hodge p-adique — à savoir le point de vue algorithmique — est tout à fait original en ce sens qu'il n'a jamais encore été adopté de manière systématique. Nous pensons toutefois que cela est tout à fait crucial. D'une part, comme nous l'avons déjà expliqué, pour aider au développement à venir de la théorie elle-même. Mais aussi, d'autre part, pour entrevoir d'éventuelles applications, en particulier à la cryptographie tant les problèmes de comptage de points sur les variétés demandent à manipuler un certain nombre d'objets complexes liés à la théorie de Hodge p-adique (voir par exemple [105], [109], [110], [111]). Au final, nous pensons que notre projet est suffisamment original pour ne pas entrer en concourrence directe avec d'autres projets aussi bien dans le domaine de l'arithmétique que celui de l'algorithmique, mais que les résultats escomptés ont toutes les chances par ailleurs d'apporter de nouvelles idées ou de nouvelles bases de travail à chacun de ces deux domaines.

Au niveau du contexte international, la théorie de Hodge p-adique a une tradition française très marquée : Fontaine, père fondateur de la théorie, a formé un certain nombre de mathématiciens au sujet, et a su par là-même créer une école française performante dont la renommée internationale est indiscutable. Rapidement, toute une école japonaise rassemblée autour de Kazuya Kato et Takeshi Tsuji s'est également intéressée aux aspects géométriques de la théorie. La partie plus algébrique (essentiellement liée à la classification et l'étude des représentations galoisiennes p-adiques), quant à elle, est restée plus longtemps confinée à l'hexagone mais s'étend aussi aujourd'hui largement au delà de nos frontières, principalement parce qu'elle fournit des outils incontournables pour un grand nombre d'arithméticiens. En résumé, la théorie de Hodge p-adique est un produit de qualité de l'école française de mathématiques qui a su s'imposer sur le plan international, et contribue par le fait à la fierté de la recherche française. Il nous apparaît donc tout à fait nécessaire, surtout en cette période de concurrence difficile, de poursuivre notre investissement dans cette direction afin de ne pas céder notre rôle de précurseur dans le domaine.

2 Description scientifique et technique / *Scientific and technical description*

2.1 État de l'art / *Backgroup, state of the art*

Fixons p un nombre premier, K une extension finie[1] de $\mathbb{Q}_p$, et appelons G_K le groupe de Galois absolu de K.

La théorie rationnelle Les premiers travaux de Fontaine ont consisté à définir une hiérarchie dans la catégorie vaste des représentations p-adiques de G_K : on distingue essentiellement les représentations cristallines, semi-stables et de de Rham. Cette hiérarchie est d'ordre géométrique dans le sens où Fontaine conjecture[2] que la cohomologie étale p-adique des variétés propres et lisses sur K fournissent toujours des représentations de de Rham ; en outre si la variété a bonne réduction (resp. réduction semi-stable), alors la représentation devrait être cristalline (resp. semi-stable).

Le travail de Fontaine ne s'arrête pas là, puisque ce dernier, avec l'aide de Pierre Colmez, arrive aussi à décrire par des objets d'algèbre linéaire, appelés *φ-modules filtrés (faiblement) admissibles* (resp. *(φ, N)-modules filtrés (faiblement) admissibles*), les représentations cristallines (resp. semi-stables). Géométriquement, ces objets correspondent à la cohomologie cristalline ou log-cristalline des variétés correspondantes, mais un des points importants de la théorie consiste à remarquer que l'on peut faire abstraction de la cohomologie, et retenir simplement qu'*une large classe de représentations p-adiques est entièrement comprise en terme de structures d'algèbre linéaire d'apparence beaucoup plus simple.* Une bonne référence concernant toutes ces questions est le recueil d'articles [118]. Il serait injuste de ne pas aussi citer à ce sujet [99], où les auteurs montrent que les notions d'admissibilité et de faible admissibilité coïncident.

[1] On peut travailler dans une situation plus générale, mais cela n'apportera rien de plus pour cette petite introduction.

[2] Depuis, ces conjectures ont été complètement démontrées, grâce aux travaux de nombreux mathématiciens. Voir par exemple [100], [102], [116], [117].

À côté de cela, dans [103], Fontaine propose une théorie parallèle pour décrire simultanément *toutes* les représentations p-adiques. Elle est incarnée par ce que l'on appelle les *(φ, Γ)-modules (étales)* et, contrairement à ce qui précède, a la particularité d'être complètement déconnectée de la géométrie. Ainsi, l'énorme avantage des (φ, Γ)-modules est de fournir un cadre uniforme pour mener à terme les calculs (essentiellement, lorsque l'on fait des opérations sur les représentations, on n'a pas besoin de se demander constamment si on reste dans le cadre semi-stable) ; le prix à payer, en contrepartie, est une complexité accrue dans la manipulation des objets, additionnée au fait que l'on oublie complètement la géométrie et donc que l'on ne distingue plus les représentations « intéressantes » des autres.

Il restait à faire le lien entre les deux théories concurrentes que nous venons de présenter. C'est dans [3] que Laurent Berger a accompli cette tâche en donnant des recettes (théoriques) pour reconnaître parmi les (φ, Γ)-modules ceux qui conduisent à des représentations cristallines, semi-stables ou de de Rham. Dans les deux premiers cas, il a également expliqué comment obtenir le φ-module filtré (ou (φ, N)-module filtré) correspondant à la représentation. Nous n'insistons pas sur la construction de Berger, mais nous contentons de signaler qu'elle passe par un objet intermédiaire appelé *équation différentielle p-adique*, dont l'étude connaît aussi actuellement un développement rapide.

Réseaux À côté de cela, on commençait à s'intéresser aux réseaux dans les représentations p-adiques, ainsi qu'à leur réduction modulo p. Une des raisons en est que ces questions interviennent de façon centrale dans l'étude des déformations des représentations p-adiques, qui s'est considérablement développée depuis que Wiles les a utilisées de façon tout à fait spectaculaire pour démontrer (une grosse partie de) la conjecture de Taniyama-Shimura-Weil puis le fameux théorème de Fermat.

Les premiers pas dans cette étude ont été accomplis par Fontaine et Guy Laffaille dans [101] et ne s'appliquaient qu'avec certaines restrictions importantes : leur théorie ne fonctionnait qu'avec une extension K non ramifiée de $\mathbb{Q}_p$ et n'englobait que les représentations cristallines dont les poids de Hodge-Tate[3] étaient compris entre 0 et $p-2$. Il a fallu attendre les travaux de Breuil et de Tong Liu (voir notamment [94], [96] et [112]) pour démêler la situation et voir apparaître une première description des réseaux dans le cas des représentations semi-stables, sans restriction sur la ramification de K. Encore une fois, cela s'incarne par la définition de nouveaux objets d'algèbre linéaire qui viennent inlassablement s'ajouter aux précédents ; ils s'appellent cette fois-ci les *modules fortement divisibles*.

Cependant, encore une fois, la théorie est mise en échec lorsque les poids de Hodge-Tate sont trop grands. Breuil était bien conscient de ce problème et a proposé très tôt, dans [97], un palliatif aux modules fortement divisibles, ou du moins à une version un peu batarde de ceux-ci. Ces nouveaux modules n'ont vraiment été étudiés intensivement que récemment par Mark Kisin (voir [106]) qui a effectivement établi une correspondance avec des « pseudo-réseaux[4] » dans les représentations semi-stables. Encore plus récemment, Liu en a proposé une version améliorée

[3] Il s'agit d'un invariant usuel associé à certaines représentations p-adiques, et notamment aux représentations de de Rham (et donc en particulier aux représentations cristallines).

[4] Un peu plus précisément, on ne demande pas à ces réseaux d'être stables par tout le groupe de Galois G_K mais seulement par un sous-groupe assez gros.

à partir de laquelle il arrive à classifier les réseaux dans les représentations semi-stables sans aucune restriction (voir [113]).

2.2 Objectifs et caractère ambitieux/novateur du projet / *Rationale highlighting the originality and novelty of the proposal*

La description que l'on vient de faire, et notamment la multiplication des notions introduites (φ-modules filtrés, (φ, N)-modules filtrés, (φ, Γ)-modules, équations différentielles p-adiques, modules fortement divisibles, *etc.*) prouve on ne peut mieux que la théorie de Hodge p-adique connaît de nos jours un essor considérable, qui ne cesse en outre de s'accroître.

À vrai dire, on est même un peu désarmé devant le développement que la théorie a connu ces dernières années. En effet, bien que l'on sache *théoriquement* relativement bien jongler entre les divers points de vue, des problèmes souvent très délicats se posent lorsque l'on souhaite faire fonctionner *pratiquement* la machine : les formules ou les équations théoriques dont on dispose sont en général très difficiles à appliquer ou à résoudre. Les réponses à ces questions « effectives » manquent et ce sont elles que nous souhaitons développer par l'intermédiaire de ce projet ANR. Plus précisément, notre objectif est de mettre au point des algorithmes qui permettraient, dans bon nombre de situations, d'expliciter complètement les liens encore mystérieux qu'entretiennent tous les aspects de la théorie de Hodge p-adique. Typiquement, nous souhaitons fournir des algorithmes qui établissent de façon concrète les liens entre les divers objets répertoriés en 2.1 (et notamment calculent des réseaux), mais aussi qui permettent d'accéder aux invariants numériques classiquement associés à ces objets : nous pensons notamment aux poids de Hodge-Tate, au polygone de Newton, au conducteur de Swan, aux facteurs ε, à l'irrégularité p-adique, *etc.*

Bien entendu, disposer de telles méthodes de calcul serait un atout majeur aussi bien pour les « utilisateurs » de la théorie que pour les « développeurs » : les premiers pourraient mener à bien beaucoup plus rapidement et facilement les calculs dans la situation qui les intéresse, alors que les seconds pourraient émettre et tester de façon beaucoup plus fiable leurs conjectures. L'enjeu de notre projet apparaît d'autant plus clairement lorsque l'on voit l'importance que prend aujourd'hui la théorie de Hodge p-adique dans des domaines de l'arithmétique de plus en plus nombreux et variés.

Les méthodes de calcul que nous allons développer nous permettront par la suite d'étudier *complètement*[5] de nombreux exemples de représentations cristallines et semi-stables. Il faut savoir qu'au-delà de la dimension 2 (qui est encore loin d'être entièrement traitée), peu de choses sont connues à ce sujet, et que ces lacunes apparaissent quotidiennement comme un frein au développement de la théorie. S'appuyant sur les algorithmes que nous allons développer, nous voulons dans un premier temps terminer l'étude en dimension 2 avant de nous attaquer à la dimension 3 qui nous apportera certainement une « faune » bien plus diversifiée, et sans doute aussi bien plus intéressante. Ceci nous permettra de fournir une base de données de représentations p-adiques à partir de laquelle les mathématiciens pourront beaucoup plus aisément formuler ou tester des conjectures. En particulier, les exemples en dimension 3 que nous souhai-

[5]Nous entendons par là que nous avons pour but de calculer tous les invariants classiques associés à ces représentations.

tons obtenir intéresseront certainement ceux qui travaillent à la correspondance de Langlands p-adique.

Nous voulons également nous concentrer sur une question plus théorique. Il s'agirait de trouver une condition nécessaire et/ou suffisante, simple à tester, pour qu'un module muni d'une action d'un opérateur de Frobenius φ admette une action supplémentaire du groupe Γ qui en fasse un (φ, Γ)-module. La même question peut se poser en terme de modules fortement divisibles, et revient essentiellement au niveau des représentations à se demander lorsqu'une représentation d'un certain sous-groupe de G_K peut se prolonger à tout le groupe de Galois. Cette interrogation revient en fait de façon récurrente lorsque l'on s'intéresse à construire des (φ, Γ)-modules (ou des modules fortement divisibles) : pour cela, on commence par construire le φ, et on veut savoir à quelle condition il est effectivement possible d'ajouter une action de Γ. Nous espérons en réalité que la condition recherchée puisse s'exprimer simplement en terme de certains invariants numériques classiques associés aux représentations que nous évoquions plus haut. Il est alors clair que la base de données que nous nous proposons d'établir nous apporterait une aide cruciale pour formuler une conjecture.

Notre projet est certainement novateur dans le sens où pour l'instant personne ne s'est attaqué de façon aussi systématique à décrire explicitement les représentations galoisiennes p-adiques. Certes, plusieurs p-adiciens (notamment Breuil, Mézard et Savitt) ont exploré de larges familles d'exemples en dimension 2, mais sans jamais s'aider de l'outil informatique, ni présenter leurs résultats de façon très structurée. Pour illustrer le caractère ambitieux de notre projet, j'aimerais dire que notre objectif est un peu d'éclairer simultanément un grand nombre de ponts (entre les divers aspects de la théorie, donc) qui ont été découverts il y a peu de temps, que l'on n'a pas encore réussi à fouler avec beaucoup d'assurance, et qui en effraient encore plus d'un. On aimerait, qu'au terme de notre recherche, ces ponts deviennent de véritables autoroutes que tout un chacun pourrait emprunter en toute sécurité.

3 Programme scientifique et technique, organisation du projet / *Scientific and technical program, project management*

3.1 Programme scientifique et structuration du projet / *Scientific program, specific aims of the proposal*

Nous avons choisi de concentrer nos efforts sur quatre grands thèmes importants pour lesquels l'algorithmique aura certainement un rôle central à jouer. Ceux-ci constituent les quatre premières tâches de notre projet et sont intitulées comme suit :

1. Calcul des invariants associés aux $\mathbb{Q}_p$-représentations p-adiques.
2. Réseaux dans les représentations semi-stables et réduction modulo p.
3. Prolongement de l'action d'un sous-groupe de G_K.
4. Aspect géométrique de la théorie de Hodge p-adique.

Le contenu scientifique de chacun des thèmes sera détaillé dans la partie 3.3 ; nous n'insistons pour l'instant pas plus sur cela. Nous aimerions quand même souligner qu'il s'agit selon nous de quatre questions *a priori* disjointes (notamment, elles mettent en jeu, chacune, leurs propres objets) mais qui ont cependant de grandes chances d'entretenir des rapports étroits et complexes. Ainsi, il est probable que les progrès effectués dans l'une des tâches aient des conséquences inattendues (et importantes) dans un autre tâche. C'est la raison pour laquelle nous pensons qu'il est fondamental de mener de front l'étude de ces quatre thématiques.

Dans un second temps, nous nous interrogerons sur la manière la plus efficace pour mettre à disposition nos résultats de la manière la plus efficace possible. Pour le moment, nous entrevoyons deux possibilités complémentaires : d'une part, l'intégration de nos algorithmes au logiciel `magma` *via* l'écriture d'une libraire, et d'autre part la création d'une page web à partir de laquelle tout un chacun pourra soit soumettre le calcul qui l'intéresse à nos algorithmes, soit consulter la base de données d'exemples que nous aurons étudier. Ce dernier travail de regroupement et de mise à disposition est l'objet de la dernière tâche qui s'intitule

5. Regroupement et mise en place d'une base de données

On se reportera à la partie 3.3 pour une description plus détaillée.

3.2 Coordination du projet / *Project management*

Nous prévoyons de distinguer deux grands temps dans la réalisation de notre projet. Le premier, qui occupe grosso modo les trois premières années, est celui dans lequel nous traiterons les quatre premières tâches. Comme nous l'avons déjà expliqué, il nous apparaît essentiel de mener leur étude de façon simultanée, car il n'est pas facile de décider à l'avance quels résultats obtenus dans l'une seront utiles pour une autre. Au contraire, en ce qui concerne les personnes impliquées, nous prévoyons un découpage *a priori* en fonction des compétences de chacun. Malgré tout, afin de ne pas nous perdre dans une organisation trop complexe et de favoriser la discussion permanente entre nous, nous avons décidé d'isoler trois sous-équipes de notre projet qui se présentent comme des unités indivisibles pour la répartition des tâches. Nous avons trouvé intéressant de baser la constitution de ces sous-équipes sur des critères géographiques (deux membres travaillant dans la même université auront certainement plus de facilité à communiquer au quotidien). Concrètement, il y a :

– l'équipe de Rennes comprenant Xavier Caruso, Michel Gros, Jérémy Le Borgne, Bernard Le Stum et David Lubicz ;
– l'équipe de Strasbourg comprenant Adriano Marmora, Christine Noot-Huyghe et Nathalie Wach ;
– l'équipe de Lyon/Montpellier comprenant Laurent Berger et Andrea Pulita.

Le tableau de la figure 1 indique la répartition qui a été retenue. Bien sûr, en complément de cela, il est aussi nécessaire de mettre en place une coordination transversale d'une part en offrant la possibilité à deux équipes différentes travaillant sur la même tâche (ou sur des tâches ayant un lien pressenti) de mettre en commun leur avancées, et d'autre part en organisant régulièrement des rencontres générales pour tenir au courant tous les membres du projet des résultats.

Tâche	Participants impliqués			Année 1		Année 2		Année 3		Année 4	
	Ren.	Str.	L/M	6	12	18	24	30	36	42	48
1. Invariants Resp. : A. Marmora	√	√	√	√	√	√	√	√	√		
2. Réseaux Resp. : X. Caruso	√	√	√	√	√	√	√	√	√		
3. Prolongement Resp. : L. Berger	√		√	√	√	√	√	√	√		
4. Géométrie Resp. : C. Noot-H.	√	√		√	√	√	√	√	√		
5. Base de données Resp. : D. Lubicz	√								√	√	√
Rapports d'avancement				☆		☆			☆		★

Légende :

☆	Rapport d'avancement annuel
★	Rapport de synthèse
Ren.	Rennes (regroupe les membres de l'IRMAR impliqués dans le projet)
Str.	Strasbourg (regroupe les membres de l'IRMA impliqués dans le projet)
L/M	Lyon et Montpellier (regroupe Laurent Berger et Andrea Pulita)

Fig. 1 – Coordination des tâches

Pour le premier point, nous prévoyons d'offrir la possibilité à chacun d'entre nous de se déplacer une fois par semestre dans le laboratoire d'accueil d'un autre membre du projet. Il serait souhaitable, afin de ne pas trop saccader le rythme de travail, que ces déplacements soient de courte durée (environ une semaine). Pour le second point, nous prévoyons d'organiser deux ou trois mini-séminaires. La première rencontre pourrait avoir lieu à Lyon assez rapidement après le mise en place du projet et aura pour but principal d'échanger nos connaissances et nos points de vue sur les questions que nous souhaitons résoudre. En ce qui concerne la suite, le programme reste à fixer, mais on pourrait envisager une autre rencontre à mi-parcours aux alentours du 18ème et une dernière vers le 36ème mois dans laquelle on pourrait commencer à établir un bilan des résultats obtenus, puis à discuter des modalités pratiques de l'exécution de la dernière tâche. À l'issue de chacun de ces séminaires, nous rendrons un rapport d'avancement dans lequel nous discuterons les progrès accomplis et ceux espérés avant la prochaine rencontre.

La dernière tâche, donc, qui est celle de regroupement et de mise à disposition de nos travaux devrait débuter à partir du 36ème mois (peut-être un peu après). Elle sera accomplie dans les locaux de l'IRMAR (à Rennes) sous la direction de David Lubicz. Afin de faciliter ce dernier travail, nous pensons installer dès le commencement du projet un serveur informatique à Rennes auquel tous les membres du projet auront accès et sur lequel ils pourront déposer leur travail au fur et à mesure de leur réalisation. Ce même serveur sera ensuite utilisé pour l'hébergement de la page web que nous souhaitons mettre à disposition de la communauté.

Le tableau de la figure 1 récapitule de façon synthétique les choix que nous venons de justifier.

3.3 Description des travaux par tâche / *Detailed description of the work organised by tasks*

Ci-dessous, nous détaillons le contenu scientifique des cinq tâches que nous avons isolées en 3.1. Nous renvoyons au tableau de la figure 1 pour ce qui concerne les responsables tâche par tâche, le détail des personnes impliquées et le calendrier.

• **Tâche 1 : Calcul des invariants associés aux $\mathbb{Q}_p$-représentations p-adiques**

Comme le titre l'indique, cette tâche se focalise sur la partie rationnelle (*i.e.* à coefficients dans $\mathbb{Q}_p$ — ou éventuellement une extension algébrique de $\mathbb{Q}_p$) de la théorie de Hodge p-adique. Les invariants dont il est question sont de deux natures. Il s'agit d'une part des structures algébriques qui ont été sommairement présentées en 2.1 (c'est-à-dire φ-modules filtrés, (φ, N)-modules filtrés, (φ, Γ)-modules et équations différentielles p-adiques) et d'autre part d'invariants numériques associés à ces objets. Ces derniers prennent souvent l'aspect de nombres rationnels, ou de collection de nombres rationnels qu'il est alors souvent commode de représenter sous forme de polygone.

Sans trop rentrer dans les détails, citons les principaux invariants numériques susceptibles de nous intéresser (faire une liste exhaustive serait déraisonnable pour cette présentation). Il y a tout d'abord ceux que l'on lit sur les φ-modules filtrés ; ce sont :

- les sauts de la filtration, qui correspondent au signe près à ce que l'on appelle les *poids de Hodge-Tate* et qui donnent naissance au *polygone de Hodge* ;
- les pentes de l'action de φ, qui donnent naissance au *polygone de Newton*.

Les φ-modules filtrés sont les structures qui correspondent aux représentations cristallines. On peut s'intéresser plus généralement aux représentations dites *potentiellement cristallines* qui sont celles qui deviennent cristallines en restriction à un sous-groupe ouvert (*i.e.* d'indice fini) de G_K. Ces représentations sont classifiées par des φ-modules filtrés munis d'une action résiduelle d'un groupe fini. À ces objets, il est associé une *représentation de Weil*, à partir de laquelle on fabrique un nombre entier appelé *conducteur de Swan*, ou aussi, de façon plus précise, une collection de nombres regroupés dans le *polygone de Swan*. Pour le cas semi-stable, des analogues définis à partir d'un (φ, N)-module filtré existent.

Au niveau des équations différentielles p-adiques, plusieurs invariants ont également été introduits. Lorsque celles-ci sont munies d'une structure de Frobenius, il y a les pentes de ce dernier, définies par Kedlaya. Nous pensons aussi à l'*irrégularité p-adique* qui peut encore une fois prendre la forme d'un unique nombre, ou au contraire de tout un polygone. Finalement, remarquons que les (φ, Γ)-modules ne semblent pas aussi riches de ce point de vue. Toutefois, il est évident que ceux-ci restent d'une importance capitale car ce sont eux qui réalisent les ponts entre les différentes théories et qui, par le fait, interviennent de façon essentielle pour comprendre les relations entre toutes les quantités que nous avons présentées. C'est par exemple grâce à eux qu'Adriano Marmora a prouvé, dans [84], une formule reliant conducteur de Swan et irrégularité p-adique.

L'objectif de cette première tâche est de proposer des solutions pratiques pour manipuler toutes les structures et toutes les quantités que nous venons de passer en revue, mais aussi — et surtout — de jongler entre celles-ci. Certes, nous nous demanderons comment décider si un φ-module filtré est, oui ou non, admissible. Et, le cas échéant, nous chercherons à calculer son polygone de Newton et son polygone de Hodge. Certes, nous chercherons à concrétiser au maximum les travaux de Kedlaya sur les équations différentielles p-adiques avec structure de Frobenius pour programmer une routine qui en calcule les pentes. Mais une grande partie de notre travail résidera dans l'interaction de tous ces objets. Typiquement, voici les questions générales sur lesquelles on aimerait progresser :

- Comment calculer l'équation différentielle p-adique associée à un (φ, Γ)-module ?
- Comment reconnaître si la représentation galoisienne associée à un (φ, Γ)-module est cristalline/semi-stable/de de Rham ? Le cas échéant, comment calculer le module filtré correspondant ?

Comme nous l'expliquerons plus en détail par la suite, aussi bien les (φ, Γ)-modules que les équations différentielles p-adiques et les modules filtrés charient une quantité infinie d'information. Ainsi, il est absolument déraisonnable d'espérer un algorithme qui calcule complètement ces objets ; il pourra au mieux les calculer avec une précision arbitraire définie à l'avance. Plutôt, donc, que de vouloir calculer la structure algébrique dans sa globalité, il semble judicieux de s'attacher (au moins dans un premier temps) à décrire seulement les invariants numériques associés que nous avons introduits, surtout que ceux-ci donnent une information sur la représentation souvent plus directement exploitable.

Évidemment, au lieu de débuter avec un (φ, Γ)-module, on peut se poser des questions analogues lorsque la représentation avec laquelle on travaille est donnée par son φ-module filtré (ou son (φ, N)-module filtré) éventuellement muni d'une action complémentaire d'un groupe fini si elle est seulement potentiellement cristalline/semi-stable.

Comme nous y avons déjà fait allusion précédemment, une difficulté algorithmique attendue réside dans le fait que les objets que l'on souhaite manipuler sont très souvent des modules sur des anneaux des séries (convergentes, surconvergentes, formelles, cela dépend), qu'il faudra savoir tronquer correctement afin de les représenter en machine. Ainsi faut-il chercher à évaluer *a priori* un rang à partir duquel lesdits coefficients n'interviennent pas dans le calcul qui nous intéresse. Qui plus est, ces coefficients eux-mêmes sont en général des éléments de $\mathbb{Q}_p$ (ou d'un corps p-adique plus général) qu'il est à nouveau nécessaire de tronquer pour pouvoir manipuler. Dès lors, on constate que les problèmes pratiques que nous souhaitons résoudre s'accompagnent immanquablement de questions d'apparence plus théorique. De façon légèrement plus précise, si X est l'indéterminée des séries que nous évoquions tantôt, une de ces questions peut être :

> Soit M un (φ, Γ)-module associé à une représentation semi-stable V. Existe-t-il des entiers m (précision arithmétique) et n (précision analytique) pour lequel les poids de Hodge-Tate de V sont entièrement déterminés par la réduction de M modulo l'idéal (p^m, X^n) ? Le cas échéant, peut-on donner une formule explicite pour les calculer ?

Il va de soi que la même interrogation vaut pour les pentes du Frobenius, le conducteur de Swan, *etc.* à la place des poids de Hodge-Tate. Bien sûr, pour résoudre ce type de questions, l'outil algorithmique fournit un préliminaire tout à fait intéressant. En effet, il est pertinent d'attaquer le problème en commençant par écrire une routine qui travaille avec une précision fixée, puis d'exécuter celle-ci avec différentes valeurs. Une étude des résultats permettrait alors d'émettre une conjecture précise.

Nous attacherons bien évidemment un soin particulier à optimiser les précisions arithmétique et analytique puisque celles-ci ont une influence directe sur la complexité des algorithmes. Nous nous demanderons par exemple quels sont les paramètres pertinents qui doivent être pris en compte pour le calcul de ces constantes. On peut d'ores et déjà penser que la dimension de la représentation et le degré du corps K sur $\mathbb{Q}_p$ (ou peut-être seulement son indice de ramification) interviendront de façon centrale. En outre, dans certaines situations plus particulières (par exemple liées aux représentations cristallines ou semi-stables), on peut facilement imaginer que d'autres quantités (à piocher parmi les invariants que nous avons décrits) auront leur rôle à jouer. L'écart entre le plus grand et le plus petit poids de Hodge-Tate a par exemple toutes les caractéristiques d'un bon candidat. Dans tous les cas, nous nous efforcerons de concevoir des familles d'algorithmes dont nous évaluerons soigneusement la complexité en fonction des paramètres qui nous paraissent significatifs. Pour obtenir les meilleures complexités asymptotiques nous utiliserons des résultats récents ou classiques relatifs à des algorithmes efficaces de manipulation de séries formelles [91], [93], [114], [92].

• Tâche 2 : Réseaux dans les représentations semi-stables et réduction modulo p

Si V est une représentation p-adique, un fait remarquable est que la semi-simplifiée de L/pL, où $L \subset V$ est un réseau stable par l'action de Galois, ne dépend pas du choix de L, mais que de V. Ainsi, cette représentation annulée par p est canoniquement associée à V et, par ailleurs, beaucoup plus facile à décortiquer. L'espoir est qu'elle conserve néanmoins un soupçon d'information sur V. Notre fil directeur, ici, est en quelque sorte de comprendre comment tout cela s'instancie pour les représentations semi-stables, en passant par les objets d'algèbre linéaire associés. Un premier essai sur la question est réalisé dans [27].

Comme nous l'avons expliqué en 2.1, les réseaux dans les représentations semi-stables sont classifiés par les modules fortement divisibles lorsque les poids de Hodge-Tate sont petits, et par des d'autres structures récemment introduites par Liu dans le cas général. Pour cette tâche, en tout cas au moins dans un premier temps, nous pensons nous restreindre aux petits poids de Hodge-Tate (et donc aux modules fortement divisibles) car la théorie de Liu n'est pas encore bien comprise — théoriquement, s'entend — à ce jour[6]. Il faut savoir, avant tout, que ces modules fortement divisibles vivent dans ce que Breuil appelle des *modules filtrés sur* S_{K_0}, ces derniers étant directement reliés aux (φ, N)-modules filtrés. Un premier problème que l'on devra élucider sera donc de rendre cette correspondance complètement explicite.

Par un argument général de compacité, on sait que toute représentation p-adique[7] admet un réseau ; ainsi, par traduction, dans tout module filtré sur S_{K_0}, il y a au moins un réseau fortement divisible. Malgré tout, en construire n'est généralement pas chose facile. Dans [96],

[6] Il se peut malgré tout que cela évolue rapidement, auquel cas nous reviendrons peut-être sur notre point de vue.

[7] La semi-stabilité est sans importance à ce niveau.

Breuil propose une méthode pour cela. Hélas, celle-ci n'est pas tout à fait algorithmique dans le sens où elle travaille avec des modules sur des anneaux infinis et demande par deux fois de considérer des intersections infinies. En outre, Breuil ne parvient à prouver que la méthode fonctionne seulement dans le cas où les poids de Hodge-Tate sont « très petits[8] ». Il semble donc intéressant pour commencer d'approfondir le travail de Breuil en le rendant complètement opérationnel. Nous sommes en fait déjà en train de faire ce travail sur une version plus simple de l'algorithme dû à Laffaille (voir [108]) qui ne s'applique que dans le cas des représentations cristallines avec $e = 1$. Les résultats partiels que nous avons obtenus sont déjà très prometteurs.

Les principales difficultés sont, comme dans la tâche 1, d'obtenir des bornes sur la précision requise, qui à nouveau dépendront de paramètres qu'il reste à déterminer. Pour cette dernière interrogation, les deux premiers paramètres auxquels on pense sont les poids de Hodge-Tate et l'indice de ramification absolu de K, puisque ceux-ci interviennent déjà abondamment dans la théorie. Mieux encore, lorsque les seuls poids de Hodge-Tate sont uniquement 0 et 1, la théorie laisse croire que les algorithmes eux-mêmes puissent se simplifier. Il semble donc tout à fait indiqué de traiter en priorité ce cas (d'autant plus qu'il suffit déjà pour beaucoup d'applications), et même de continuer à le traiter à part dans la suite. Par ailleurs, ce travail sera aussi l'occasion de se demander dans quelle généralité la méthode de Breuil fournit des résultats (*i.e.* de quelle hypothèse a-t-on vraiment besoin sur les poids de Hodge-Tate ?)

D'autres questions sur les réseaux se posent d'elles-mêmes. Par exemple, l'ensemble des réseaux L à l'intérieur d'une représentation p-adique (semi-stable) fixée est naturellement muni de deux opérations binaires qui sont la somme et l'intersection. Comment celles-ci s'effectuent-elles au niveau des modules fortement divisibles ? Ceci nous amène directement à une autre interrogation plus générale : comment construire le plus petit tel réseau qui contient une partie donnée (ou réciproquement le plus grand inclus dans une partie donnée) ? Des variantes de la méthode de Breuil devraient pouvoir encore s'appliquer ici, et c'est un point sur lequel nous voulons travailler.

La prochaine étape est d'étudier les réductions modulo p des modules fortement divisibles. Celles-ci vivent naturellement dans une catégorie d'objets de torsion définie par Breuil. Ce sont des objets finis que l'on peut donc représenter avec des structures de données adaptées. Il conviendra d'écrire des algorithme efficaces pour les manipuler. Plusieurs invariants numériques leur sont naturellement associés (poids de Hodge-Tate modulo p, poids de l'inertie modérée) auxquels on aimerait pouvoir accéder facilement. En réalité, nous pensons même qu'il est envisageable, au moins dans le cas des objets annulés par p, de déterminer efficacement et complètement la représentation galoisienne associée : cela revient en effet à résoudre un système d'équations polynômiales à coefficients dans $\mathcal{O}_K$ (pour lequel les bases de Grobner devrait être un outil adéquat) puis à manipuler des groupes de Galois d'extensions finis de K. Pour ce dernier point, il ne semble étrangement pas y avoir de références disponibles, mais le problème analogue sur $\mathbb{Q}$ (à la place de K) a été beaucoup étudié (voir par exemple [104], [115], ainsi que leur bibliographie) et les idées développées pour ce faire devraient s'étendre à notre situation.

Par ailleurs, les résultats de [32] montrent que les catégories de Breuil possèdent une structure riche qu'il pourrait être intéressant de mieux appréhender *via* l'algorithmique.

Concluons le descriptif de cette tâche en revenant au fil directeur que nous présentions

[8]Précisément, lorsque ceux-ci sont strictement inférieurs à $\frac{p-1}{e}$, e étant l'indice de ramification absolu de K.

au début. Forts de ce qui précéde, il sera l'heure d'émettre des conjectures sur d'éventuels liens qu'entretiendraient les invariants associés aux objets de torsion avec ceux associés à la représentation semi-stable dont nous sommes partis. À la lumière de [27], il nous paraît par exemple pertinent de comparer les poids de Hodge-Tate modulo p avec le polygone de Newton de la représentation.

• **Tâche 3 : Prolongement de l'action d'un sous-groupe de G_K**

Comme son nom l'indique, un (φ, Γ)-module est un module (libre sur un anneau de séries) muni simultanément d'un endomorphisme φ (le Frobenius) et d'une action d'un groupe (procyclique) Γ, ces deux actions étant astreintes à commuter. Une problématique importante de la théorie des représentations galoisiennes p-adiques est la construction explicite de familles assez vastes de (φ, Γ)-modules. Une façon naturelle d'appréhender le problème est de partir d'un φ-module (c'est-à-dire d'un module libre muni simplement d'un endomorphisme φ), et de se demander s'il existe une condition simple pour que celui-ci admette de surcroît une action compatible de Γ.

En réalité, cette approche est d'autant plus intéressante qu'elle a une interprétation simple au niveau des représentations. Pour l'expliquer, introduisons l'extension cyclotomique K_∞ : c'est celle obtenue en ajoutant à K toutes les racines p^n-ièmes de l'unité ($n \geq 1$). Comme K_∞ est une extension galoisienne de K, son groupe de Galois absolu G_∞ s'identifie à un sous-groupe distingué de G_K. Nous avons signalé tantôt que la donnée d'un (φ, Γ)-module est équivalente à celle d'une représentation p-adique de G_K ; en fait, le Frobenius détermine complètement sa restriction à G_∞, alors que l'action de Γ est ce qui permet de la prolonger à tout G_K. Ainsi, la question que nous posions en terme d'algèbre linéaire dans l'alinéa précédent revient à se demander s'il existe une condition simple pour qu'une représentation p-adique de G_∞ (donnée par l'intermédiaire de son φ-module) se prolonge en une représentation de G_K tout entier.

Malheureusement, il ne semble pas évident qu'une telle condition existe en toute généralité. Toutefois, on peut espérer que ce soit le cas pour une classe plus réduite de représentations (*e.g.* cristallines, semi-stables), et qu'alors elle puisse s'exprimer en terme d'invariants numériques standards. On voit alors que les algorithmes permettant d'accéder à ces invariants que nous voulons développer dans la tâche 1 auront certainement un rôle crucial à jouer ici. Malgré tout, ils ne sauraient à eux seuls régler complètement le problème, puisque l'on aura également besoin d'algorithmes décisionnels qui, à partir d'un φ-module, seraient capables de déterminer si, oui ou non, il existe une action compatible de Γ. La mise au point de ces derniers apparaît alors comme une étape importante à développer dans cette tâche.

Il est à noter que les questions esquissées précédemment se posent en des termes très proches au niveau des modules fortement divisibles. En effet, un module fortement divisible est un module libre muni d'un Frobenius φ (défini sur un sous-module) et d'un opérateur de monodromie N, astreints à certaines compatibilités. Là encore, la donnée du Frobenius (et du sous-module) détermine, à elle seule, la restriction de la représentation galoisienne associée à un certain sous-groupe G'_∞ de G_K, tandis que l'opérateur de monodromie n'est utilisé que pour la prolonger à tout G_K. La problématique qui apparaît ici est donc celle du prolongement d'un quasi-module fortement divisible (*i.e.* un module fortement divisible sans le N) en module fortement divisible, et est donc tout à fait similaire à celle que nous avons détaillée précédemment : *grosso modo*, on a remplacé Γ par N. À nouveau, nous aimerions interpréter ce problème de prolongement en termes d'invariants usuels, et nous avons besoin pour cela de disposer d'un certain nombre d'exemples, hélas pratiquement inexistants à ce jour.

Soulignons pour finir qu'une bonne compréhension d'une réponse à la question du prolongement que nous venons de présenter devrait avoir des répercussions importantes sur la compréhension des réseaux (voir tâche 2). En effet, un des principaux résultats de la théorie développée par Kisin dans [107] est la classification des réseaux dans les représentations semi-stables invariants par l'action du sous-groupe G'_∞ qui apparaît dans l'alinéa précédent. Ainsi, il ne fait aucun doute que la connaissance de critères de prolongement de cette action à tout G_K constituera un pas essentiel, sinon décisif, pour l'étude des réseaux invariants par tout le groupe de Galois.

- **Tâche 4 : Aspect géométrique de la théorie de Hodge p-adique**

Étant donné que les structures de la théorie de Hodge p-adique ont été introduites comme abstraction de certains groupes de cohomologie, il est naturel de croire que les exemples les plus intéressants d'objets de la théorie sont ceux qui s'obtiennent par voie cohomologique à partir d'une donnée géométrique (typiquement une variété) sur un corps p-adique. Dans cette tâche, nous nous proposons de calculer explicitement les groupes de cohomologie (cristalline, rigide, *etc.*) associés à certaines classes de variétés.

Pour décrire plus précisément ce que nous souhaitons faire, commençons par fixer quelques notations. On rappelle que K est une extension finie de $\mathbb{Q}_p$. On note π une uniformisante, $\mathcal{O}_K$ son anneau des entiers et $k = \mathcal{O}_K/\pi$ son corps résiduel. Donnons-nous X une variété propre et lisse sur K. Si X a bonne réduction (resp. réduction semi-stable), la cohomologie cristalline (resp. log-cristalline) de la fibre spéciale (resp. munie de la log-structure adéquate) d'un modèle lisse (resp. semi-stable) de X est l'exemple naturel de φ-module filtré (resp. de (φ, N)-module filtré). Nous nous proposons dans cette tâche de calculer ces groupes de cohomologie sur plusieurs exemples. Le cas des variétés à bonne réduction ayant déjà été abordé par plusieurs auteurs, notamment pour ses applications à la cryptographie *via* le comptage de points, nous voulons nous concentrer essentiellement sur le cas semi-stable. Les premiers exemples qui viennent à l'esprit sont les courbes elliptiques, typiquement $y^2 = x^2(x-1)+p$. De façon légèrement plus générale, on pourra considérer le cas des courbes hyperelliptiques définies par l'équation $y^2 = P(x)$ où P est un polynôme de degré éventuellement supérieur à 3.

Entrons à présent légèrement dans les détails. Puisque X est semi-stable, il admet par définition un modèle $\mathcal{X}$ défini sur $\mathcal{O}_K$ qui est propre, régulier et dans lequel la fibre spéciale définit un diviseur à croisements normaux. Ceci définit une log-structure sur $\mathcal{X}$ et en fait un log-schéma log-lisse sur la base $\mathcal{O}_K$ munie de la log-structure associée à $\mathbb{N} \to \mathcal{O}_K, 1 \mapsto \pi$. Les premières structures qui nous intéressent sont les groupes de cohomologie log-cristalline (munis de l'action du Frobenius et de l'opérateur de monodromie) de la fibre spéciale de $\mathcal{X}$ par rapport à $\mathcal{O}_K$. Comme nous travaillons dans une situation relevée, le calcul des modules et du Frobenius se ramène à celui de la cohomologie d'un complexe de de Rham logarithmique. C'est donc pour l'instant en un sens assez proche de ce que l'on sait déjà faire dans certaines situations à bonne réduction (avec, bien entendu, des complications inévitables liées à la manipulation des log-structures). La difficulté essentielle semble résider dans le calcul de l'opérateur de monodromie, dont la définition fait intervenir la cohomologie de variétés de plus grande dimension, et donc plus compliquées.

La cohomologie log-cristalline permet également de faire le lien avec les modules fortement divisibles de Breuil. Pour cela, on travaille sur une nouvelle base définie comme suit. Soient $W = W(k)$ et $W[u]$ l'anneau des polynômes à coefficients dans W en l'indéterminée u. Soit S l'enveloppe à puissances divisées de $W[u]$ par rapport à l'idéal noyau de la projection $W[u] \to \mathcal{O}_K$, $u \mapsto \pi$. On munit $E = \operatorname{Spec} S$ de la log-structure associée au morphisme de monoïdes $\mathbb{N} \to S$, $1 \mapsto u$. Par composition par l'épaississement (compatible aux log-structures) $\operatorname{Spec} \mathcal{O}_K \to E$, $u \mapsto \pi$, $\mathcal{X}$ apparaît comme un E-log-schéma. C'est la partie « sans p-torsion » de la cohomologie log-cristalline de $\mathcal{X}$ par rapport à cette nouvelle base qui, au moins conjecturalement[9] fournit des modules fortement divisibles. On s'intéressera à les calculer explicitement sur certains exemples de courbes elliptiques ou hyperelliptiques. Aux difficultés algorithmiques récurrentes viennent alors s'ajouter d'autres problèmes liés au fait que l'on ne dispose *a priori* pas de schéma log-lisse sur E dans lequel la fibre spéciale de $\mathcal{X}$ se plonge[10]. Il faudra donc, dans une étape préalable, construire explicitement de tels relevés.

Le cas du premier groupe de cohomologie semble particulièrement intéressant à étudier car il fournit des modules fortement divisibles à poids de Hodge-Tate dans $\{0, 1\}$ qui, comme nous l'avons déjà sous-entendu tantôt, ont une structure bien plus simple que les modules fortement divisibles généraux. Il est donc probable que l'on puisse alors disposer d'algorithmes particuliers, à la fois plus simples et plus efficaces. Signalons en outre que Breuil a montré dans [94] que les modules fortement divisibles à poids de Hodge-Tate dans $\{0, 1\}$ entretiennent aussi un lien très étroit avec les schémas en groupes sur $\mathcal{O}_K$. Il serait là encore intéressant de comprendre mieux cette correspondance en le décrivant explicitement sur des familles d'exemples.

• Tâche 5 : Regroupement et mise en place d'une base de données

Le but de cette dernière tâche est dans un premier temps de regrouper et d'unifier les méthodes et les algorithmes qui auront été développés lors de du projet ANR, ceci afin de former un tout cohérent, facile d'utilisation, qui pourra alors être diffusé auprès de la communauté.

Pour cette diffusion, nous envisageons principalement deux moyens. Le premier consiste en la création d'une interface web à partir de laquelle l'utilisateur pourrait questionner directement nos procédures sur les exemples qui l'intéressent. Le second, quant à lui, serait l'intégration d'une bibliothèque de calcul sur les représentations p-adiques au logiciel `Magma`, utilisé par beaucoup de nos confrères. Ces moyens nous semblent essentiels tous les deux, car complémentaires et s'adressant à des publics différents. L'aspect « page web » serait plutôt utile au théoricien qui a besoin épisodiquement de faire un calcul pour asseoir son intuition ou tester une conjecture. L'aspect « intégration à `Magma` », quant à lui, constituerait par contre un ingrédient important au développement d'autres projets explicites en arithmétique ; nous pensons notamment à certaines questions tournant autour des formes modulaires, ou des valeurs spéciales de fonctions L dans lesquelles la théorie de Hodge p-adique est de plus en plus présente.

[9]Précisément, on conjecture dans [98] que c'est le cas pour les r-ièmes groupes de cohomologie avec $r < p-1$. On sait le prouver (voir [95] et [26]) lorsque $er < p-1$ où e est l'indice de ramification absolu de K.

[10]Dans le cas de la base $\mathcal{O}_K$, on pouvait prendre le log-schéma $\mathcal{X}$ lui-même.

En plus de cela, nous comptons utiliser nous-mêmes ces algorithmes pour fournir une base de données d'exemples de représentations galoisiennes p-adiques. Il s'agirait donc d'établir des listes de telles représentations (principalement en dimension 2 et 3) et de donner explicitement pour chacune d'entre elles tout ce que la théorie lui associe (aussi bien les structures d'algèbre linéaire, que les divers invariants numériques). Bien entendu, ce sera aussi l'occasion de faire le lien avec la géométrie : certaines de ces représentations apparaissent comme la cohomologie étale de variétés, et la base de données se devra de signaler quand cela se produit accompagné, le cas échéant, d'une description explicite de la variété correspondante.

La mise à disposition de cette base de données se ferait simplement par l'intermédiaire d'une page web pouvant être interrogée à distance. Nous comptons d'ailleurs porter une attention particulière aux modes d'interrogation proposés pour qu'ils répondent le plus fidèlement possible aux problèmes quotidiens des arithméticiens.

Finalement, nous aimerions développer des ponts entre l'aspect « calcul en ligne » et celui « base de données ». Typiquement, on voudrait faire en sorte que les résultats des calculs soumis en ligne viennent automatiquement alimenter notre base de données. Bien entendu, réciproquement, avant d'entamer un calcul demandé par l'utilisateur, il serait logique de consulter la base de données pour voir si la réponse n'est pas déjà répertoriée. Aussi, chaque résultat pourra être accompagné d'un lien vers certaines entrées de la base de données qui semblent en relation (selon certaines heuristiques qu'il faudra développer). Il ne fait aucun doute que, si cela fonctionne correctement, ce serait une aide inestimable pour la mise en évidence de nouveaux liens, et la formulation de nouvelles conjectures.

3.4 Calendrier des tâches, livrables et jalons / *Planning of tasks, deliverables and milestones*

Voir tableau figure 1 (page 9).

4 Stratégie de valorisation des résultats et mode de protection et d'exploitation des résultats / *Data management, data sharing, intellectual property and results exploitation*

Bien entendu, notre première stratégie de valorisation reste la publication dans des revues scientifiques à comité de lecture. Mais, en plus de cela, nous souhaitons valoriser notre travail d'une part en intégrant les algorithmes que nous allons implémenter au logiciel de calcul formel `Magma`, et d'autre part en mettant en ligne sur Internet la base de données de représentations p-adiques que nous souhaitons développer. Nous comptons comme ceci nous imposer rapidement auprès de la communauté comme les spécialistes incontournables des questions effectives en théorie de Hodge p-adique.

D'un point de vue pratique, la base de données sera hébergée sur un serveur dédié qui sera très probablement entreposé et administré à Rennes.

5 Organisation du partenariat / *Consortium organisation and description*

5.1 Description, adéquation et complémentarité des participants / *Relevance and complementarity of the partners within the consortium*

Le projet que nous souhaitons développer a pour objectif d'expliciter de nombreux liens en théorie de Hodge p-adique. Il nous fallait donc regrouper des experts (que nous avons choisi parmi les jeunes[11] chercheuses et chercheurs) d'une part dans les différents aspects de la théorie, et d'autre part en algorithmique.

Commençons par l'algorithmique. C'est David Lubicz qui incarne cette compétence au sein de notre projet. En effet, en ayant beaucoup travaillé sur des algorithmes de comptage de points sur les courbes elliptiques (pour des applications à la cryptographie), il est devenu très familier avec la manipulation sur machine des nombres p-adiques et des séries formelles (ou convergentes), qui sont les objets principaux qui interviennent en théorie de Hodge p-adique. Par ses compétences, il est donc certain qu'il saura apporter une contribution déterminante à l'ensemble des recherches que nous désirons poursuivre. C'est également lui qui sera en charge de coordonner la tâche 5 qui revêt un aspect algorithmique qu'il maîtrise certainement.

En ce qui concerne la compréhension des liens entre la théorie initiale de Fontaine et les équations différentielles p-adiques (qui apparaissent notamment dans la tâche 1), la participation de Laurent Berger s'imposait d'elle-même. C'est en effet lui qui a mis en lumière ces liens inattendus dans [3] et les a utilisés pour démontrer un certain nombre de résultats importants. Dans sa thèse, Adriano Marmora a lui aussi contribué à éclaicir ces liens en donnant une formule qui relie le conducteur de Swan d'une représentation potentiellement semi-stable à l'irrégularité p-adique de l'équation différentielle associée. Il est donc certain qu'il maîtrise les subtilités de la construction de Berger et sera un ajout majeur pour notre projet. À côté de cela, le projet nécessitait aussi bien sûr un expert des équations différentielles p-adiques, maîtrisant simultanément les incarnations théorique et pratique de la théorie. Il est certain qu'Andrea Pulita est le jeune chercheur adapté à la situation puisqu'il s'est longuement penché dans sa thèse sur la résolution explicite d'équations différentielles p-adiques en rang 1.

L'étude des réseaux dans les représentations galoisiennes et des quotients de ceux-ci (que nous souhaitons étudier dans la tâche 2) repose sur la compréhension précise de la théorie de Breuil, domaine dont est spécialiste Xavier Caruso comme en témoigne ses travaux passés. C'est donc tout naturellement que celui-ci trouve sa place dans le projet et est nommé responsable de la tâche 2. Le travail de Jérémy Le Borgne, qui débute actuellement sa thèse sous la direction de Caruso et Lubicz, concerne l'étude effective des modules de torsion issus de la théorie de Breuil et donc s'intègre parfaitement au projet. Par l'introduction des modules de Wach, Nathalie

[11] Il est vrai que certains de nos membres ont déjà dépassé — et parfois de beaucoup — l'âge charnière de 38 ans. Malgré tout, la moyenne d'âge de notre projet reste peu élevée puisque, pondérée par les pourcentages d'implication, elle atteint à peine 32,7 ans. Ainsi, nous pensons que notre candidature trouve tout à fait sa place dans le *Programme jeunes chercheuses et jeunes chercheurs*.

Wach a également grandement contribué à l'étude des représentations cristallines de torsion et trouve donc naturellement sa place ici.

Christine Noot-Huyghe, Michel Gros, Bernard Le Stum sont, quant à eux, des spécialistes des cohomologies p-adiques, c'est-à-dire des aspects géométriques que nous évoquions dans la tâche 4. Il est donc certain qu'ils apporteront une contribution importante aux recherches que nous souhaitons entreprendre.

Pour la bibliographie et les indicateurs numériques concernant les différences personnes impliquées dans le projet, on pourra se reporter respectivement aux annexes 7.1 et 7.2.

5.2 Qualification du coordinateur du projet / *Qualification of the project coordinator*

Le coordinateur du projet, Xavier Caruso, a déjà malgré son jeune âge une certaine expérience de l'organisation et de l'encadrement.

Avant même d'entrer dans le monde de la recherche, il a été un des organisateurs ou un des responsables scientifiques de nombreux stages de préparation aux olympiades internationales de mathématiques. Dans un registre assez proche, il a également organisé pendant trois ans à l'École normale supérieure de Paris un groupe de travail destiné à de brillants élèves de lycée. Pendant la même période, il a aussi été avec Farouk Boucekkine et François Gaudel l'inititiateur puis l'organisateur d'un tutorat mettant en relation les étudiants de l'ÉNS avec des élèves volontaires issus de lycées défavorisés de banlieue parisienne.

Pendant sa thèse, Caruso a été le fondateur puis l'organisateur d'un séminaire des doctorants à l'université Paris 13. Depuis qu'il travaille à Rennes, il a mis un place un séminaire interne qui regroupe chaque semaine une grande partie des membres des trois équipes de géométrie de l'IRMAR (le laboratoire de mathématiques de l'université de Rennes 1).

Toutes ces initiatives montrent bien que Caruso aime s'impliquer dans la vie collective d'une équipe, et qu'il est tout à fait capable de gérer un petit groupe avec assurance et brio.

5.3 Qualification, rôle et implication des participants / *Contribution and qualification of each project participant*

Nom	Prénom	Emploi actuel	Unité de rattachement et lieu	Personne × mois	Rôle/reponsabilité dans le projet
Berger	Laurent	Prof.	UMPA (ÉNS Lyon)	19,2	• Responsable de la tâche 3 • Expert sur la théorie de Berger
Caruso	Xavier	CR	IRMAR (Rennes)	38,4	• Coordinateur du projet • Responsable de la tâche 2 • Expert sur la théorie de Breuil

Nom	Prénom	Emploi actuel	Unité de rattachement et lieu	Personne × mois	Rôle/reponsabilité dans le projet
Gros	Michel	CR	IRMAR (Rennes)	12	• Calcul de réseaux fortem[t] divisibles (tâche 2) • Implication dans l'étude géométrique (tâche 4)
Le Borgne	Jérémy	Thésard	IRMAR (Rennes)	36	• Algorithmique des modules de Breuil en torsion (tâche 3)
Le Stum	Bernard	MCF	IRMAR (Rennes)	14,4	• Implication dans l'étude géométrique (tâche 4) • Expert en cohomologies p-adiques
Lubicz	David	Ingénieur recherche	IRMAR (Rennes)	19,2	• Responsable de la tâche 5 • Référent sur les questions algorithmiques
Marmora	Adriano	MCF	IRMA (Strasbourg)	14,4	• Responsable de la tâche 1 • Implication dans l'étude géométrique (tâche 4)
Noot-Huyghe	Christine	CR	IRMA (Strasbourg)	12	• Responsable de la tâche 4 • Expert en cohomologies p-adiques
Pulita	Andrea	MCF	IMMM (Montpellier)	24	• Expert en équations différentielles p-adiques
Vienney	Mathieu	Thésard	UMPA (ÉNS Lyon)	12	• Étude en caractéristique p • Applications à la correspondance de Langlands p-adique
Wach	Nathalie	MCF	IRMA (Strasbourg)	12	• Implication dans l'étude géométrique (tâche 4) • Expert en modules de Wach et représentations cristallines de torsion

Pour les biographies, on se reportera à l'annexe 7.2.

6 Justification scientifique des moyens demandés / *Scientific justification of the requested budget*

Il semble délicat de répartir les moyens demandés en fonction des tâches comme cela est demandé puisque la plupart des investissements que nous souhaitons faire ne sont certainement pas spécifiques à une tâche particulière mais plutôt transversaux. Un exemple typique est celui des séminaires puisqu'ils ont pour but essentiel de réunir les personnes impliquées dans les diverses tâches. Nous avons donc choisi une solution de simplicité pour remplir le document de soumission A qui consiste à diviser simplement la somme globale demandée par le nombre de tâches. Toutefois, nous avons préféré comptabiliser le serveur de calcul entièrement dans la tâche 5 (bien qu'il sera également utile pour les autres tâches) car il s'agit d'un unique achat pour lequel il nous semblait plus simple d'avoir tout le budget sur le même compte.

Tous les prix indiqués dans cette section sont *hors taxes*.

6.1 Équipement / *Large equipment*

Notre projet étant centré sur l'algorithmique, nous aurons besoin pour le mener à bien dans les meilleures conditions d'acquérir un serveur de calcul (lame de calcul).

Celui-ci sera utilisé dans un premier temps comme machine de calcul lors de la conception et du développement des algorithmes et, dans un second temps, comme hébergeur de l'interface Web et de la base de données que nous voulons mettre en ligne.

Coût estimé : **10 000 €**

6.2 Missions / *Travels*

Bien qu'en apparence plutôt isolées, il ne fait aucun doute que les tâches que nous avons définies dans la description du programme scientifique (partie 3.1) vont entretenir des relations étroites et subtiles. Afin de nous donner les outils pour comprendre le plus rapidement et le plus profondément possible ces relations, nous souhaitons favoriser au maximum les échanges entre les membres de l'équipe. Pour cela, nous voulons donner la possibilité à chacun d'entre nous de se déplacer deux fois par an durant une courte période (environ une semaine) dans le laboratoire d'accueil d'un autre partenaire de l'ANR.

Coût estimé : $(300 + 400) \times 11$ pers. $\times$ 8 semestres = **61 600 €**

Il est également très important, afin de ne pas nous cloisonner, que nous puissions rencontrer des mathématiciens extérieurs à l'ANR (éventuellement des étrangers). À cette fin, nous prévoyons un budget pour que chacun d'entre nous ait les moyens d'inviter une fois tous les deux ans pour une durée allant d'une à deux semaines quelqu'un de son choix.

Coût estimé : $(700 + 800) \times 11$ pers. $\times$ 2 invitations = **33 000 €**

Nous voulons également organiser trois mini-séminaires, comme cela a été discuté en 3.2.

Coût estimé : 9000×3 séminaires = **27000 €**

Pour clore le projet, nous souhaitons organiser un congrès sur Rennes. Celui-ci s'étalerait sur une semaine et réunirait au moins une cinquantaine de participants.

Coût estimé : **17 920 €**

Nous prévoyons finalement d'organiser un séminaire mensuel, ceci afin de pouvoir nous tenir bien informés des progrès parallèles de la théorie, et de ses applications.

Coût estimé : 400×10 mois $\times$ 4 ans = **16 000 €**

6.3 Décharges d'enseignement / *Research Teaching relief*

Notre projet rassemble plusieurs jeunes enseignants-chercheurs, souvent submergés par les charges d'enseignement qui demandent un investissement considérable surtout les premières années. Afin de permettre à ces jeunes talents de s'impliquer complètement dans le projet (et accessoirement de pouvoir se libérer plus facilement pour les rencontres que nous souhaitons organiser), il nous serait très utile de disposer de décharges d'enseignement à hauteur d'un semestre par an.

Coût estimé : 10 000 × 4 ans = **40 000 €**

6.4 Autres dépenses de fonctionnement / *Other expenses*

Pour le fonctionnement quotidien, et notamment pour équiper les membres de notre équipe en petite fourniture, livres et ordinateur portable, nous prévoyons un budget de 1500 € par personne pour toute la durée du projet.

Coût estimé : 1500 × 11 pers. = **16 500 €**

Finalement, pour mener à bien notre projet et développer des librairies pour `Magma`, nous avons besoin d'acheter des licences pour ce logiciel.

Coût estimé : **2000 €**

7 Annexes

7.1 Références bibliographiques / *References*

Bibliographie des membres du projet

[1] D. Benois, L. Berger, *Théorie d'Iwasawa des représentations cristallines II*, Comment. Math. Helv. **83** (2008), 603–677.

[2] L. Berger, *L'approximation par des polynômes à coefficients entiers.*, Gaz. Math. **84** (2000), 35–40

[3] L. Berger, *Représentations p-adiques et équations différentielles.* Invent. math. **148** (2002), 219–284

[4] L. Berger, *Bloch and Kato's exponential map : three explicit formulas.*, Doc. Math. (2003) Extra Vol. : Kazuya Kato's Fiftieth Birthday, 99–129

[5] L. Berger, H. Li, H. J. Zhu, *Construction of some families of 2-dimensional crystalline representations.*, Math. Ann. **329** (2004), 365–377

[6] L. Berger, *An introduction to the theory of p-adic representations.*, Geometric Aspects of Dwork Theory, 255–292, Walter de Gruyter, Berlin, 2004

[7] L. Berger, *Limites de représentations cristallines.* Compositio Math. **140** (2004), 1473–1498

[8] L. Berger, *Représentations de de Rham et normes universelles.*, Bull. Soc. Math. France **133** (2005), 601–618

[9] L. Berger, *Construction de (φ, Γ)-modules : représentations p-adiques et B-paires.*, Algebra & Number Theory **2** (2008), 91–120

[10] L. Berger, P. Colmez, *Familles de représentations de de Rham et monodromie p-adique.*, à paraître dans Astérisque

[11] L. Berger, C. Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbf{Q}_p)$., à paraître dans Astérisque

[12] L. Berger, *Représentations modulaires de* $\mathrm{GL}_2(\mathbf{Q}_p)$ *et représentations galoisiennes de dimension* 2., à paraître dans Astérisque

[13] L. Berger, *Équations différentielles p-adiques et (φ, N)-modules filtrés.*, à paraître dans Astérisque

[14] L. Berger, *Presque $\mathbf{C}_p$-représentations et (φ, Γ)-modules.*, à paraître dans JIMJ

[15] L. Berger, *On some modular representations of the Borel subgroup of* $\mathrm{GL}_2(\mathbf{Q}_p)$., preprint (2008)

[16] R. Carls, D. Kohel, D. Lubicz, *Higher-dimensional* 3*-adic CM construction*, J. Algebra **319** (2008), 971–1006

[17] R. Carls, D. Lubicz, *A p-adic quasi-quadratic point counting algorithm*, Int. Math. Res. Not. (2008)

[18] G. Chatel, D. Lubicz, *A point counting algorithm using cohomology with compact support*, preprint (2008)

[19] B. Chiarellotto, B. Le Stum, *Sur la pureté de la cohomologie cristalline* C. R. Acad. Sci. Paris, **326** (1998), 961–963

[20] B. Chiarellotto, B. Le Stum, *F-isocristaux unipotents*, Compositio Math. **116** (1999) 81–110

[21] B. Chiarellotto, B. Le Stum, *Pentes en cohomologie rigide et F-isocristaux unipotents*, Manuscripta Math. **100** (1999), 455–468

[22] B. Chiarellotto, B. Le Stum, *A comparison theorem for weights*, J. Reine u. Angew. Math. **546** (2002) 159–176

[23] X. Caruso, *Représentations semi-stables de torsion dans le cas $er < p - 1$*, J. reine angew. Math. **594** (2006), 35–92

[24] X. Caruso, *Dualité de Cartier et modules de Breuil*, preprint (2006)

[25] X. Caruso, *Schémas en groupes et poids de Diamond-Serre*, preprint (2007)

[26] X. Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), 629–699

[27] X. Caruso, D. Savitt, *Polygones de Hodge, de Newton et de l'inertie modérée des représentations semi-stables*, à paraître dans Math. Ann.

[28] X. Caruso, D. Savitt, *Poids de l'inertie modérée de certaines représentations cristallines*, preprint (2008)

[29] X. Caruso, T. Liu, *Quasi-semi-stable representations*, à paraître dans Bull. Soc. Math. France

[30] X. Caruso, T. Liu, *Some bounds for ramification of p^n-torsion semi-stable representations* preprint (2008)

[31] X. Caruso, *Sur la classification de quelques ϕ-modules simples*, preprint (2008)

[32] X. Caruso, *$\mathbb{F}_p$-représentations semi-stables*, preprint (2008)

[33] C. Doche, D. Lubicz, *Algebraic background*, Handbook of elliptic and hyperelliptic curve cryptography, 19–37, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[34] J.-C. Faugère, D. Lubicz, *Computing modular correspondance for abelian varieties*, preprint (2008)

[35] P. Gaudry, D. Lubicz, *The arithmetic of characteristic 2 Kummer surface*, preprint (2007)

[36] M. Gros, *Classes de Chern et classes de cycles en cohomologie de Hodge-Witt logarithmique*, Mém. Soc. Math. France **21** (1985)

[37] M. Gros, *Sur la partie p-primaire du groupe de Chow de codimension deux*, Comm. Algebra **13** (1985), 2407–2420

[38] M. Gros, *Quelques résultats sur l'homologie cyclique des algèbres en caractéristique positive*, C. R. Acad. Sci. Paris Sér. I. Math. **304** (1987), 139–142

[39] M. Gros, *0-cycles de degré 0 sur les surfaces fibrées en coniques*, J. Reine Angew. Math. **373** (1987), 166-184

[40] M. Gros, N. Suwa, *La conjecture de Gersten pour les faisceaux de Hodge-Witt logarithmique*, Duke Math. J. **57**, (1988), 615–628

[41] M. Gros, N. Suwa, *Application d'Abel-Jacobi p-adique et cycles algébriques*, Duke Math. J. **57** (1988), 579–613

[42] M. Gros, *Régulateurs syntomiques et valeurs de fonctions L p-adiques I*, Inv. Math. **99** (1990), 293–320

[43] M. Gros, *Régulateurs syntomiques et valeurs de fonctions L p-adiques II*, Inv. Math. **115** (1994), 61–79

[44] M. Gros, *Sur les (K_0, φ, N)-structures attachées aux courbes de Mumford*, Rend. Sem. Mat. Univ. Padova **103** (2000), 233–260

[45] M. Gros, *Monodromie archimédienne d'une courbe complexe*, Rend. Sem. Mat. Univ. Padova **103** (2000), 251–260

[46] M. Gros, L. Narvaez-Macarro, *Cohomologie évanescente p-adique : calculs locaux*, Rend. Sem. Mat. Univ. Padova **104**, 71–90

[47] M. Gros, *Caractères des groupes réductifs finis et D-modules*, Rend. Sem. Mat. Univ. Padova **106** (2001), 1–19

[48] M. Gros, *Sur le D-module associé au complexe des cycles proches et ses variantes p-adiques*, Rend. Sem. Univ. Padova **112** (2004), 77–95

[49] M. Gros, *Opérations différentiels globaux sur une courbe elliptique*, preprint (2008)

[50] M. Gros, *Un scindage de l'application de Frobenius sur toute l'algèbre des distributions de $SL(2)$*, preprint (2008)

[51] M. Gros, B. Le Stum, A. Quirós, *A Simpson correspondence in positive characteristic*, preprint (2008)

[52] C. Huyghe, *Interprétation géométrique sur l'espace projectif des $A_N(K)^\dagger$-modules cohérents*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), 587–590

[53] C. Huyghe, *Transformation de Fourier des $\mathscr{D}^\dagger_{\mathscr{X},\mathbb{Q}}(\infty)$-modules*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), 759–762

[54] C. Huyghe, *Théorème d'acyclicité pour les $\mathscr{D}^\dagger_Q$-modules sur l'espace projectif*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), 453–455

[55] C. Huyghe, *$\mathscr{D}^\dagger$-affinité de l'espace projectif* avec un appendice de P. Berthelot, Compositio Math **108** (1997), no. 3, 277–318

[56] C. Huyghe, *$\mathscr{D}^\dagger$-affinité des schémas projectifs*, Ann. Inst. Fourier **48** (1998), no. 4, 913–956

[57] C. Huyghe, *Un théorème de comparaison entre les faisceaux d'opérateurs différentiels de Berthelot et de Mebkhout-Narvaez-Macarro*, J. Algebraic Geom. **12** (2003), no. 1, 147–199

[58] T. Lange, D. Lubicz, A. Weigl, *Random numbers generation and testing*, Handbook of elliptic and hyperelliptic curve cryptography, 715–735, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[59] J. Le Borgne, *Détermination de la constante optimale dans le théorème d'Ax-Sen-Tate*, en préparation

[60] B. Le Stum, *Cohomologie rigide et variétés abéliennes*, thèse de troisième cycle (1985) et C. R. Acad. Sc. Paris, t. 303, Série I, n° 20 (1986)

[61] B. Le Stum, *Applications of Rigid Cohomology to Arithmetic Geometry*, thèse de Ph. D. (1988)

[62] B. Le Stum, J.-Y. Étesse, *Fonctions L associées aux F-isocristaux surconvergents I, Interprétation cohomologique*, Math. Ann. **296** (1993), 557–576

[63] B. Le Stum, *Filtration par le poids sur la cohomologie de de Rham d'une courbe projective non-singulière*, Rend. Sem. Mat. Univ. Padova **93** (1995), 43-85

[64] B. Le Stum, *La structure de Hyodo-Kato pour les courbes*, Rend. Sem. Mat. Univ. Padova, **94** (1995), 279–301

[65] B. Le Stum, J.-Y. Étesse, *Fonctions L associées aux F-isocristaux surconvergents II, Zéros et pôles unités*, Invent. Math. **127** (1997), 1–31

[66] B. Le Stum, A. Quirós, *Transversal Crystals of Higher Level*, Ann. Inst. Fourier, Grenoble **47** (1997) 69–100

[67] B. Le Stum, A. Quirós, *The exact Poincaré lemma in crystalline cohomology of higher level*, Journal of Algebra **240** (2001), 559–588

[68] B. Le Stum, F. Trihan, *Log-cristaux et surconvergence*, Ann. Inst. Fourier, Grenoble **5** (2001), 1189–1207

[69] B. Le Stum, *Frobenius action, F-isocrystals and slope filtration*, Geometric aspects of Dwork theory. Vol. I, II, Walter de Gruyter GmbH & Co. KG, Berlin (2004), 837–843

[70] B. Le Stum, *The overconvergent site I. Coefficients*, preprint (2006)

[71] B. Le Stum, *Rigid Cohomology, Cambridge tracts in Mathematics*, Cambridge University Press (2007)

[72] B. Le Stum, *The overconvergent site II. Cohomology*, preprint (2007)

[73] B. Le Stum, A. Quirós, *The filtered Poincaré lemma in higher level (with applications to algebraic groups)*, à paraître dans Nagoya Mathematical Journal (2008)

[74] R. Lercier, D. Lubicz, *Counting points in elliptic curves over finite fields of small characteristic in quasi quadratic time*, Advances in cryptology, EUROCRYPT 2003, 360–373, Lecture Notes in Comput. Sci. **2656**, Springer, Berlin, 2003.

[75] R. Lercier, D. Lubicz, F. Vercauteren, *Point counting on elliptic and hyperelliptic curves*, Handbook of elliptic and hyperelliptic curve cryptography, 407–453, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006

[76] R. Lercier, D. Lubicz, *A quasi quadratic time algorithm for hyperelliptic curve point counting*, Ramanujan J. **12** (2006), 399–423

[77] D. Lubicz, *Une description de la cohomologie du complément à un diviseur non réductible de P^2*, Bull. Sci. Math. **124** (2000), 447–458

[78] D. Lubicz, *Sur les pinceaux de courbes définis par une fonction régulière*, Bull. Sci. Math. **125** (2001), 139–160

[79] D. Lubicz, *Background on p-adic numbers*, Handbook of elliptic and hyperelliptic curve cryptography, 39–44, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[80] D. Lubicz, *On a classification of finite statistical tests*, Adv. Math. Commun. **1** (2007), 509–524

[81] D. Lubicz, F. Vercauteren, *Cohomological background on point counting*, Handbook of elliptic and hyperelliptic curve cryptography, 133–141, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[82] D. Lubicz, T. Sirvent, *Attribute-Based Broadcast Encryption Scheme Made Efficient*, Proc. of Advances in Cryptology-Africacrypt'08 (2008), Casablanca

[83] D. Lubicz, T. Sirvent, *Pseudo-random groups and related problems*, Identity-Based Cryptography, M. Joye et G. Neven, Cryptology and Information Security Series, IOS Press

[84] A. Marmora, *Irrégularité et conducteur de Swan p-adiques*, Doc. Math. **9** (2004), 413–433

[85] A. Marmora, *Facteur epsilon p-adiques*, Compos. Math. **144** (2008), 439–483

[86] C. Noot-Huyghe, *Transformation de Fourier des $\mathscr{D}$-modules arithmétiques. I.*, Geometric aspects of Dwork theory. Vol. I, II, 857–907, Walter de Gruyter GmbH & Co. KG, Berlin, 2004

[87] C. Noot-Huyghe, *Finitude de la dimension homologique d'algèbres d'opérateurs différentiels faiblement complètes et à coefficients surconvergents*, J. Algebra **307** (2) (2007)

[88] C. Noot-Huyghe, F. Trihan, *Sur l'holonomie de $\mathscr{D}$-modules arithmétiques associés à des F-isocristaux surconvergents sur des courbes lisses*, Ann. Fac. Sci. Toulouse Math. (6) **16** (2007), 611–634

[89] N. Wach, *Représentations cristallines de torsion*, Compositio Math. **108** (1997), no. 2, 185–240

[90] N. Wach, *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France **124** (1996), no. 3, 375–400

Autres références bibliographiques utilisées dans le document

[91] A. V. Aho, K. Steiglitz, J. D. Ullman, *Evaluating polynomials at fixed sets of points* SIAM J. Comput. **4** (1975), 533–539

[92] A. Bostan, F. Chyzak, F. Ollivier, B. Salvy, É. Schost, A. Sedoglavic, *Fast computation of power series solutions of systems of differential equations*, in *SODA* (2007), 1012–1021

[93] A. Bostan, B. Salvy, É. Schost, *Power series composition and change of basis*, in David J. Jeffrey, editor, *ISSAC'08*. ACM Press, to appear.

[94] C. Breuil, *Construction de représentations p-adiques semi-stables*, Ann. Scient. ENS. **31** (1997), 281–327

[95] C. Breuil, *Cohomologie étale de p-torsion et cohomologie cristalline en réduction semi-stable*, Duke mathematical journal **95** (1998), 523–620

[96] C. Breuil, *Représentation semi-stables et modules fortement divisibles*, Invent. math. **136** (1999), 89–122

[97] C. Breuil, *Une application du corps des normes*, Compos. Math. **117** (1999), 189–203

[98] C. Breuil, *Integral p-adic Hodge theory*, Advanced studies in pure mathematics **36** (2002), 51–80

[99] P. Colmez, J.-M. Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), 1–43

[100] G. Faltings, *Crystalline cohomology and p-adic Galois representations*, Journal of algebraic geometry **1** (1992), 61–82

[101] J.-M. Fontaine, G. Laffaille, *Construction de représentations p-adiques*, Ann. Scient. ENS. **15** (1982), 547–608

[102] J.-M. Fontaine, W. Messing, *p-adic periods and p-adic étale cohomology*, Contemporary math. **67** (1987), 179–207

[103] J.-M. Fontaine, *Représentations p-adiques des corps locaux*, Grothendieck Festschrift II, (1991), 249–309

[104] A. Hulpke, *Techniques for the computation of Galois groups* in *Algorithmic Algebra and Number Theory*, Springer, Heidelberg (1999), 65–77

[105] K. S. Kedlaya. *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338

[106] M. Kisin, *Crystalline representations and F-crystals*, Algebraic Geometry and Number Theory, Drinfeld 50th Birthday volume, 459–496

[107] M. Kisin, *Crystalline representations and F-crystals*, Algebraic Geometry and Number Theory, Drinfeld 50th Birthday volume, 459–496

[108] G. Laffaille, *Groupes p-divisibles et modules filtrés : le cas peu ramifié*, Bull. Soc. math. France **108** (1980), 187–206

[109] A. G. B. Lauder, D. Wan, *Computing zeta functions of Artin-Schreier curves over finite fields*, LMS J. Comput. Math. **5** (2002), 34–55 (electronic)

[110] A. G. B. Lauder, D. Wan, *Computing zeta functions of Artin-Schreier curves over finite fields II*, J. Complexity, **20** (2004), 331–349

[111] A. G. B. Lauder. *Deformation theory and the computation of zeta functions*, Proc. London Math. Soc. (3) **88** (2004), 565–602

[112] T. Liu, *On lattices in semi-stable representations : a proof of a conjecture of Breuil*, Compos. Math. **144** (2008), 61–88

[113] T. Liu, *A note on lattices in semi-stable representations*, preprint

[114] M. S. Paterson and L. J. Stockmeyer, *On the number of nonscalar multiplications necessary to evaluate polynomials*, SIAM J. Comput. **2** (1973), 60–66

[115] G. Renault, *Introduction à la théorie de Galois effective*, cours aux Journées de Calcul Formal à Luminy (2008)

[116] T. Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. math. **137** (1999), 233–411

[117] T. Tsuji, *Semi-stable conjecture of Fontaine-Jannsen : a survey*, Astérisque **279**, Soc. math. France (2002), 323–370

[118] *Periodes p-adiques*, Astérisque **223**, Soc. math. France (1994)

[119] Astérisque, 3 volumes, à paraître

7.2 Biographies / *CV, Resume*

Laurent Berger

- *Âge* : 31 ans
- *Genre* : masculin
- *Situation actuelle* : professeur à l'ENS Lyon
- *Cursus* :

2007 –	Professeur à l'ENS Lyon
2006	Habilitation à diriger les recherches
2005 – 2008	PCCEI (« petites classes ») à l'École Polytechnique
2004 – 2007	Chargé de recherche au CNRS (Orsay et IHÉS)
2002 – 2004	*Benjamin Peirce Assistant Professor* à l'université de Harvard
2001 – 2002	Service national
1998 – 2001	Thèse à l'université Paris 6 sous la direction de Pierre Colmez
1995 – 1999	Élève à l'École normale supérieure de Paris

- *Encadrement doctoral* :

2008 – Mathieu Vienney, *Représentations galoisiennes modulo p et correspondance de Langlands*

- *Liste des cinq publications les plus significatives* :

[1] L. Berger, *Représentations p-adiques et équations différentielles*, Invent. Math. **148** (2002), no. 2, 219–284

[2] L. Berger, *Bloch and Kato's exponential map : three explicit formulas*, Kazuya Kato's fiftieth birthday. Doc. Math. 2003, Extra Vol., 99–129

[3] L. Berger, *Limites de représentations cristallines*, Compos. Math. **140** (2004), no. 6, 1473–1498

[4] L. Berger, L. Hanfeng, Z. Hui June, *Construction of some families of 2-dimensional crystalline representations*, Math. Ann. **329** (2004), no. 2, 365–377

[5] L. Berger, *Construction de* (φ, Γ)*-modules : représentations p-adiques et B-paires*, Algebra & Number Theory, **2** (2008), no. 1, 91–120

- *Nombre total de publications* : 13

Xavier Caruso, coordinateur du projet

- *Âge* : 28 ans
- *Genre* : masculin
- *Situation actuelle* : chargé de recherche au CNRS
- *Cursus* :

2006 – Chargé de recherche au CNRS affecté à l'IRMAR

2002 – 2005 Thèse à l'université Paris 13 sous la direction de Christophe Breuil

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

- *Encadrement doctoral* :

2008 – Jérémy Le Borgne, *Méthodes effectives pour la théorie de Hodge p-adique*

- *Liste des cinq publications les plus significatives* :

[1] X. Caruso, *Conjecture de l'inertie modérée de Serre*, à paraître dans Invent. Math.

[2] X. Caruso, *Représentations semi-stables de torsion dans le cas* $er < p-1$, J. reine angew. Math. **594** (2006), 35–92

[3] X. Caruso, T. Liu, *Quasi-semi-stable representations*, à paraître dans Bull. Soc. Math. France

[4] X. Caruso, D. Savitt, *Polygones de Hodge, de Newton et de l'inertie modérée des représentations semi-stables*, à paraître dans Math. Ann.

[5] X. Caruso, $\mathbb{F}_p$*-représentations semi-stables*, preprint (2008)

- *Nombre total de publications* : 4
- *Expérience antérieure en coordination* :

2006 –	Organisation d'un séminaire interne à l'université de Rennes 1
2004 – 2006	Organisation du séminaire des doctorants de l'université Paris 13
2004 – 2006	Organisation d'un groupe de travail pour brillants lycéens et élèves de prépa

Michel Gros

- *Âge* : 52 ans
- *Genre* : masculin
- *Situation actuelle* : chargé de recherche à l'IRMAR
- *Cursus* :

1994	Habilitation à diriger les recherches
1994	Thèse de Ph. D. à l'université Paris XI sous la direction de Luc Illusie
1988 –	Chargé de recherche au CNRS affecté à l'IRMAR
1983	Thèse de troisième cycle à l'Université Paris XI sous la direction de Luc Illusie

- *Liste des cinq publications les plus significatives* :

[1] M. Gros, L. Narvaez-Macarro, *Cohomologie évanescente p-adique : calculs locaux*, Rend. Sem. Mat. Univ. Padova **104**, 71–90

[2] M. Gros, *Sur le D-module associé au complexe des cycles proches et ses variantes p-adiques*, Rend. Sem. Univ. Padova **112** (2004), 77–95

[3] M. Gros, *Opérations différentiels globaux sur une courbe elliptique*, preprint (2008)

[4] M. Gros, *Un scindage de l'application de Frobenius sur toute l'algèbre des distributions de $SL(2)$*, preprint (2008)

[5] M. Gros, B. Le Stum, A. Quirós, *A Simpson correspondence in positive characteristic*, preprint (2008)

- *Nombre total de publications* : 13

Jérémy Le Borgne

- *Âge* : 23 ans
- *Genre* : masculin
- *Situation actuelle* : thésard à l'IRMAR
- *Cursus* :

2008 –	Thèse à l'IRMAR sous la direction de Xavier Caruso et David Lubicz
2008	Master 2 de mathématiques de l'université de Rennes 1 : *Algèbre et Géométrie*. Mention Bien, rang 2
2008	Agrégation de mathématiques, rang 31
2005 – 2009	Élève de l'École normale supérieure de Cachan, antenne de Bretagne

- *Liste des cinq publications les plus significatives* :

  [1] J. Le Borgne, *Détermination de la constante optimale dans le théorème d'Ax-Sen-Tate*, en préparation

- *Nombre total de publications* : 0

Bernard Le Stum

- *Âge* : 49 ans
- *Genre* : masculin
- *Situation actuelle* : maître de conférences à l'IRMAR
- *Cursus* :

1994	Habilitation à diriger les recherches
1988 –	Maître de conférences à l'IRMAR
1985 – 1988	*Teaching Assistant* puis *Teaching Associate* au département de mathématiques de l'université du Minnesota
1985 – 1988	Thèse de Ph. D. à l'université du Minnesota sous la direction de William Messing
1982 – 1985	Thèse de troisième cycle à l'Université Rennes 1 sous la direction de Pierre Berthelot

- *Encadrement doctoral* :

2006 –	Viviana Delanoy, *Différentielles de niveau supérieur et supersingularité*
2002 – 2007	Gweltaz Chatel, *Comptage de points : méthodes cristallines*
1998 – 2002	Daniel Caro, *Fonctions L et D-modules arithmétiques*
1992 – 1996	Fabien Trihan, *Théorie de Dieudonné cristalline de niveau m*
1992 – 1996	Rachid Lamjoun, *Géométrie rigide et espaces de Berkovich*

- *Liste des cinq publications les plus significatives* :

  [1] B. Le Stum, F. Trihan, *Log-cristaux et surconvergence*, Ann. Inst. Fourier (Grenoble) **5** (2001), no. 5, 1189-1207

  [2] B. Chiarellotto, B. Le Stum, *A comparison theorem for weights*, J. Reine Angew. Math. **546** (2002), 159–176

  [3] B. Le Stum, *Frobenius action, F-isocrystals and slope filtration*, Geometric aspects of Dwork theory. Vol. I, II, 837–843, Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

  [4] B. Le Stum, *Rigid cohomology*, Cambridge Tracts in Mathematics, **172**, Cambridge University Press, Cambridge, 2007

  [5] B. Le Stum, A. Quirós, *The filtered Poincaré lemma in higher level (with applications to algebraic groups)*, à paraître dans Nagoya Mathematical Journal (2008)

- *Nombre total de publications* : 14

David Lubicz

- *Âge* : 37 ans
- *Genre* : masculin
- *Situation actuelle* : Ingénieur de recherche au CELAR
- *Cursus* :

2008	Habilitation à diriger les recherches
2008 –	Chercheur associé à l'IRMAR
2001 –	Responsable du séminaire de cryptographie de l'IRMAR
2000 –	Ingénieur de recherche au laboratoire de cryptographie du CELAR (DGA)
1996 – 1999	Thèse à l'université de Bordeaux sous la direction de Alexandru Dimca

- *Encadrement doctoral* :

  2008 – Jérémy Le Borgne, *Méthodes effectives pour la théorie de Hodge p-adique*

- *Liste des cinq publications les plus significatives* :

  [1] D. Lubicz. *Une description de la cohomologie du complément à un diviseur non irréductible de* $\mathbb{P}^2$, Bull. Sci. Math. **125** (2001), no. 2, 139–160

  [2] D. Lubicz. *Sur les pinceaux de courbes définis par une fonction régulière*, Bull. Sci. Math. **125** (2001), no. 2, 139–160

  [3] R. Lercier, D. Lubicz. *Counting points on an hyperelliptic curves over finite fields in quadratic time*, Ramanujan Journal of Mathematics, 2007

  [4] R. Carls, D. Kohel, D. Lubicz. *Higher dimensional* 3*-adic CM construction*, Journal of Algebra, 2008

  [5] D. Lubicz. *On a classification of finite statistical tests*, Advances in Mathematics of Communications, 2007

- *Nombre total de publications* : 13

Adriano Marmora

- *Âge* : 31 ans
- *Genre* : masculin
- *Situation actuelle* : maître de conférences à l'IRMA
- *Cursus* :

2008	Organisation de la conférence *Recent Progress in Arithmetic D-modules theory* avec Christine Huyghe
2007 –	Maître de conférences à l'IRMA
2007	Diplôme d'honneur de docteur de l'université Paris 13
2006 – 2007	Stage postdoctoral (3 mois) à *University of Tokyo* avec une bourse JSPS (Japan Society of Promotion of Science)
	Stage postdoctoral (13 mois) au CRM (Centre de Recherche Mathématiques) à l'Université de Montréal et à *Concordia University* (Montréal, Canada)

2003 – 2006	Thèse à l'université de Paris 13 sous la direction de Ahmed Abbes

- *Liste des cinq publications les plus significatives* :

[1] A. Marmora, *Irrégularité et conducteur de Swan p-adiques*, Doc. Math. **9** (2004), 413–433

[2] A. Marmora, *Facteur epsilon p-adiques*, Compos. Math. **144** (2008), 439–483

- *Nombre total de publications* : 2

Christine Noot-Huyghe

- *Âge* : 40 ans
- *Genre* : féminin
- *Situation actuelle* : chargée de recherche au CNRS
- *Cursus* :

2008	Organisation de la conférence *Recent Progress in Arithmetic D-modules theory* avec Adriano Marmora
2003 –	Chargée de recherche au CNRS affectée à l'IRMA
1995 – 2003	Chargée de recherche au CNRS affectée à l'IRMAR
1992 – 1995	Thèse à l'université de Rennes 1 sous la direction de Pierre Berthelot
1988 – 1992	Élève de l'École normale supérieure de Lyon

- *Liste des cinq publications les plus significatives* :

[1] C. Huyghe, *$\mathscr{D}^\dagger$-affinité de l'espace projectif* avec un appendice de P. Berthelot, Compositio Math **108** (1997), no. 3, 277–318

[2] C. Huyghe, *$\mathscr{D}^\dagger$-affinité des schémas projectifs*, Ann. Inst. Fourier **48** (1998), no. 4, 913–956

[3] C. Huyghe, *Un théorème de comparaison entre les faisceaux d'opérateurs différentiels de Berthelot et de Mebkhout-Narvaez-Macarro*, J. Algebraic Geom. **12** (2003), no. 1, 147–199

[4] C. Noot-Huyghe, *Transformation de Fourier des $\mathscr{D}$-modules arithmétiques. I.*, Geometric aspects of Dwork theory. Vol. I, II, 857–907, Walter de Gruyter GmbH & Co. KG, Berlin, 2004

[5] C. Noot-Huyghe, *Finitude de la dimension homologique d'algèbres d'opérateurs différentiels faiblement complètes et à coefficients surconvergents*, J. Algebra **307** (2) (2007)

- *Nombre total de publications* : 9

Andrea Pulita

- *Âge* : 31 ans
- *Genre* : masculin
- *Situation actuelle* : maître de conférences à l'université de Montpellier 2

- *Cursus* :

2008 –	Maître de conférences à l'université de Montpellier 2
2006 – 2008	Stage postdoctoral à l'université de Bielefeld dans le cadre du *Sonderforschungsbereich 701 : Spektrale Strukturen und Topologische Methoden in der Mathematik*
2002 – 2005	Thèse à l'université Paris 6, en collaboration avec *l'Università degli Studi di Padova* sous la direction de Gilles Christol et Bruno Chiarellotto

- *Liste des cinq publications les plus significatives* :

[1] A. Pulita, *Frobenius structure for rank one $p-$adic differential equations.*, Contemp. Math. **384** (2005)

[2] A. Pulita, *Rank One Solvable $p-$adic Differential Equations and Finite Abelian Characters via Lubin-Tate Groups.*, Math. Ann. **337** (2007), 489–555

[3] A. Pulita, B. Chiarellotto, *Arithmetic and Differential Swan conductors of rank one representations with finite local monodromy*, preprint (2008)

[4] A. Pulita, *Infinitesimal deformation of ultrametric differential equations*, preprint (2008)

- *Nombre total de publications* : 2

Mathieu Vienney

- *Âge* : 23 ans
- *Genre* : masculin
- *Situation actuelle* : thésard à l'UMPA

- *Cursus* :

2008 –	Thèse à l'UMPA sous la direction de Laurent Berger
2007	Master 2 de mathématiques de l'université de Paris 11 : *Analyse, arithmétique et géométrie*
2006	Agrégation de mathématiques, rang 59
2004 – 2008	Élève de l'École normale supérieure de Paris

- *Nombre total de publications* : 0

Nathalie Wach

- *Âge* : 41 ans
- *Genre* : féminin
- *Situation actuelle* : maître de conférences à l'IRMA

- *Cursus* :

1995 –	Maître de conférences à l'IRMA
1994 – 1995	*Adjunct Assistant Professor* à l'Université de Californie, Los Angeles (UCLA)
1990 – 1994	Thèse à l'université Paris 13 sous la direction de Jean-Marc Fontaine
1987 – 1991	Élève de l'École normale supérieure de Paris

- *Liste des cinq publications les plus significatives* :

[1] N. Wach, *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France **124** (1996), no. 3, 375–400

[2] N. Wach, *Représentations cristallines de torsion*, Compositio Math. **108** (1997), no. 2, 185–240

- *Nombre total de publications* : 2

7.3 Implication des personnes dans d'autres contrats / *Involvement of project participants to other grants, contracts, etc.*

Part.	Nom de la personne participant au projet	Personne × mois	Intitulé de l'appel à projet Source de financement Montant attribué	Titre du projet	Nom du coordinateur	Date début & Date fin
No 1	David Lubicz	18	Programme blanc (en cours de soumission)	Courbes hyperelliptiques, isogénies et comptage	David Lubicz	2009 – 2012
No 2	Andrea Pulita	24	Programme jeunes chercheuses et jeunes chercheurs (en cours de soumission)	Aspects algébriques et analytiques des équations aux q-differences	Lucia Di Vizio	2009 – 2013