2019-01488 - Post-Doctoral Research Visit F/M (BN19) Algorithms for rigid analytic geometry

Type de contrat : CDD de la fonction publique
Niveau de diplôme exigé : Thèse ou équivalent
Fonction : Post-Doctorant

A propos du centre ou de la direction fonctionnelle

Team presentation
The LFANT team researches algorithms in number theory and arithmetic geometry. We cover all aspects from complexity theory over optimised implementations up to cryptologic applications.

Research themes
The LFANT team has the goal of making an inventory of the major number theoretic algorithms, with an emphasis on algebraic number theory and arithmetic geometry, and of carrying out complexity analyses. So far, most of these algorithms have been designed and tested over number fields of small degree and scale badly. A complexity analysis should naturally lead to improvements by identifying bottlenecks, systematically redesigning and incorporating modern asymptotically fast methods.

Reliability of the developed algorithms is a second long term goal of our team. Short of proving the Riemann hypothesis, this could be achieved through the design of specialised, slower algorithms not relying on any unproven assumptions. We would prefer, however, to augment the fastest unreaden algorithms with the creation of independently verifiable certificates. Ideally, it should not take longer to check the certificate than to generate it.

All theoretical results are complemented by concrete reference implementations in Pari/Gp, which allow to determine and tune the thresholds where the asymptotic complexity kicks in and help to evaluate practical performances on problem instances provided by the research community. Another important source for algorithmic problems treated by the LFANT team is modern cryptology. Indeed, the security of all practically relevant public key cryptosystems relies on the difficulty of some number theoretic problem; on the other hand, implementing the systems and finding secure parameters require efficient number theoretic algorithms.

Contexte et atouts du poste
Job environnement
The research will be conducted in the LFANT term located at Institut Mathématiques de Bordeaux. The LFANT team is the main developer of the software PARI/GP and it has a strong international recognition in Number Theory.

Scientific priorities
My proposal ts with the priority Algorithmes et programmation of the Plan stratégique scientifique of INRIA. Indeed, the objective of the project is to design efficient algorithms for algebraic computations with expected impact on Geometry, Number Theory and Cryptography. Moreover, we plan to pay particular attention to prove the correction of our algorithms, taking into account the uncertainty of our initial data (which are p-adic numbers, necessarily given by approximations).

Scientific Research context
In many questions arising in Number Theory and Geometry, the concept of analytic functions is a notion of first importance. This observation is supported by a myriad of examples. The most two significant of them are probably:
(1) the Riemann zeta function (and its avatars) which has become the most powerful tool for understanding the distribution of prime numbers and
(2) the Weierstrass elliptic p function which allows for a complete understanding of elliptic curves over C.
Both of them have important applications in Computer Science, in particular in Cryptography.

For many arithmetical applications, the completion Qp (the field of p-adic numbers) of Q is often as relevant as R or C. The theory of analytic p-adic functions has been developed throughout the 20th century and is now well understood at least from the theoretical point of view. For instance, the Riemann zeta function and the Weierstrass elliptic p function do have p-adic analogues. Related to this is the notion of p-adic analytic geometry: it has emerged after Tate's works in the 1970's and is now at the heart of the most recent achievements in Arithmetic Geometry (for which Peter Scholze received the Fields Medal in 2018).

Keywords
Computer algebra, Gröbner bases, p-adic numbers, Algebraic geometry

Main references
Mission confiée

Work description

In many concrete situations, being able to carry out explicit computations in p-adic analytic geometry would be a decisive asset. However, this aspect has not been much developed so far, except a first step which was concretised recently by Vaccon, Verron and myself in [1]: we designed a theory of Gröbner bases for Tate algebras. The main objective of the present project is to go further in this direction. Below is a list of tasks we propose to work on.

1. Improve the complexity of the algorithms of [1]

The work of [1] is a proof of concept and no special attention has been payed to efficiency and complexity. In particular, the division algorithm used is naive and slow. The first task of this postdoc will be to revisit all algorithms of [1] and drastically improve their efficiency/complexity. Several lines of research will be explored. First, although the context is different, we plan to import ideas from the world of standard bases and especially Mora's division algorithm. A second option will be to design analogues of Faugère's F5 algorithm in the framework of Tate's algebras.

2. Create a complete toolbox for formal schemes and rigid varieties

Tate algebras are the building blocks of formal schemes and rigid varieties (two types of p-adic analytic varieties) as polynomial algebras are the building blocks of algebraic varieties (or, more generally, schemes). The second task of the postdoc will be to design a complete toolbox working with formal schemes and rigid varieties, including optimized algorithms for performing all standard meaningful constructions on these geometric objects (e.g. blow-ups, tubes...).

3. Explore applications

If time permits, we also plan to explore applications to Number Theory. Several options are possible in this direction, depending on the wishes and the skills of the candidate. Here are some ideas: explicit computations with elliptic curves over Qp (in the Tate curve model), explicit Iwasawa theory, explicit computations of deformations spaces of Galois representations...

Principales activités

Summary of the main activities:

1. Design and implement fast algorithms for computing Gröbner bases over Tate algebras
2. Create a complete toolbox for formal schemes and rigid varieties
3. Explore applications to Number Theory

Compétences

The candidate must hold a PhD thesis in Mathematics or Computer Algebra. Other prerequisites include:

- a good knowledge of classical algorithms in Symbolic Computation, including Gröbner bases algorithms
- a good knowledge of Python and C/C++

Besides, some familiarity with p-adic numbers and Algebraic Geometry will be highly appreciated.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération

2653€ / month (before taxes)

Informations générales

- **Thème/Domaine** : Algorithmique, calcul formel et cryptologie
  Calcul Scientifique (BAP E)
- **Ville** : Talence
- **Centre Inria** : CRI Bordeaux - Sud-Ouest
- **Date de prise de fonction souhaitée** : 2019-09-02
- **Durée de contrat** : 12 mois
- **Date limite pour postuler** : 2019-03-31

Contacts

- **Equipe Inria** : LFANT
A propos d'Inria

Inria, l'institut national de recherche dédié aux sciences du numérique, promeut l'excellence scientifique et le transfert pour avoir le plus grand impact. Il emploie 2400 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3000 scientifiques pour relever les défis des sciences informatiques et mathématiques, souvent à l'interface d'autres disciplines. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 160 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

Essential qualities in order to fulfil this assignment are feeling at ease in an environment of scientific dynamics and wanting to learn and listen.

Consignes pour postuler

Thank you to send :

- CV
- Cover letter
- Support letters (mandatory)
- List of publication

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.