

École Doctorale des Sciences Fondamentales

Title of the thesis: Galois representations, linear forms in logarithms and applications to Diophantine equations

Supervisor : Nicolas Billerey

Laboratory : Laboratoire de mathématiques Blaise Pascal, UMR 6620

University : Université Clermont-Auvergne

Email and Phone : nicolas.billerey@uca.fr 0473407632

Possible co-supervisor : Éric Gaudron (eric.gaudron@uca.fr)

Laboratory : Laboratoire de mathématiques Blaise Pascal, UMR 6620

University : Université Clermont-Auvergne

Summary :

Solving Diophantine equations is an old yet very active research area in Number Theory. Current approaches to these problems usually combine methods from various branches of fundamental mathematics. Among these, the most fruitful ones, lay on the use of both the theory of linear forms in logarithms and modularity results for certain types of Abelian varieties and Galois representations. In many situations, getting or improving such a Diophantine result strongly relies on our ability of making effective the statements used.

In this Ph.D. thesis, we will focus on proving effective results that can be used in concrete situations. We now explain in more details the topics involved in this project.

Let A be a commutative algebraic group defined over the field of rational numbers \mathbb{Q} . For the complex Lie group $A(\mathbb{C})$, there is an exponential map defined on the tangent space at the origin $t_A(\mathbb{C})$ which is surjective and takes values in $A(\mathbb{C})$. Given a rational point p on A , it is thus possible to consider a preimage $u \in t_A(\mathbb{C})$ of the rational point p under this exponential map. Such a vector u is called a logarithm of p . The goal of the theory of linear forms in logarithms is to study the distance between such a logarithm u and a subspace of t_A , defined over \mathbb{Q} (in these questions, the field \mathbb{Q} can be replaced by a number field). In particular, we seek for a (non-zero) lower bound of this quantity. When A is a product of elliptic curves, we have a very powerful result proved by S. David in 1995 (Mémoires de la Société Mathématique de France) which is often used when one tries to solve Diophantine equations with the method of the elliptic logarithms (introduced in the late 90's). What counts here, is the smallness of the numerical constants in the lower bound. One goal of this Ph.D. project will be to establish new lower bounds in the elliptic case which are better than those of S. David and which take into account the recent theoretical progress made since then. In particular, the modern techniques from Arakelov geometry will be of great help to achieve this goal.

Another fruitful approach to solve Diophantine equations arises from the method, now known as the modular method, used by A. Wiles in his 1995 proof of Fermat's Last Theorem. It is based on deep results on the arithmetic of points of finite order on rational elliptic curves and establishes a profound link between certain Abelian varieties or Galois representations and

École Doctorale des Sciences Fondamentales

the theory of modular forms. Extending this method to other Diophantine equations (for instance following the ambitious Darmon's program) requires to develop tools and results adapted to these new situations. In this direction, one can cite recent work (2015, *Inventiones mathematicae*) of N. Freitas, B.V. Le Hung and S. Siksek who proved the modularity of all elliptic curves defined over real quadratic fields. One can also mention the development of new irreducibility criteria for elliptic Galois representations allowing the use of the modular method in situations where generalizations of B. Mazur's theorem are not known.

In all of these questions, the concept of congruences between modular forms plays a fundamental role. One goal of this Ph.D. project will be to study certain specific aspects of this notion, in particular in the case of reducible representations. The questions around level lowering and level raising then involve properties of Eisenstein ideals in the Hecke algebra that will have to be studied in details. These problems can also be addressed with benefit in the context of Hilbert modular forms which arise naturally in extensions of the modular method.

In addition to the contributions of this Ph.D. project to the fundamental research in Arithmetic Geometry, the study of these topics will give to the student a rather broad view on the techniques used to solve Diophantine equations and help her/him to develop her/his own tools, a rather rare skill in the community.