

*Research project CGREC***Computing Galois representations attached to elliptic curves**

Supervisor 1 Peter Stevenhagen
E-mail `psh@math.leidenuniv.nl`
Institution Universiteit Leiden

Supervisor 2 Karim Belabas
E-mail `Karim.Belabas@math.u-bordeaux1.fr`
Institution Université Bordeaux 1

Research project short description:

An elliptic curve E defined over a number field K naturally gives rise to a Galois representation of the absolute Galois group G_K of K on the group E_{tors} of torsion points of E . By a theorem of Serre, the image of G_K in the full automorphism group $\text{Aut}(E_{tors})$ of this group is for most (more precisely, the non-CM) elliptic curves E a subgroup of finite index. The full group $\text{Aut}(E_{tors})$ has a well-known structure: it is a profinite limit of 2-dimensional matrix groups. Thus, it is in principle possible to describe the Galois representation attached to E "in finite terms".

In the special case of CM-elliptic curves, the Galois representations are of a different, and more classical nature. In this case, an explicit concise description of the image of G_K can in principle also be given.

The project focuses on theoretical and algorithmic aspects of determining, on input of E and K , the exact Galois representation attached to E . There are various questions of a theoretical, algorithmic and practical nature that the candidate can try to answer. These pertain to exhibiting explicit upper bounds on the image of Galois in $\text{Aut}(E_{tors})$, finding algorithms that, in theory and/or in practice, compute the image of Galois, and analyzing the run time of such algorithms.

References:

- J.-P Serre: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, *Inventiones mathematicae* **15**, 259–331 (1972)
S. Lang, H. Trotter: *Frobenius Distributions in GL_2 -Extensions*, Springer, 1974.