Finding short vectors in ideal lattices using subfields

A lattice is a subset of \( \mathbb{R}^m \) consisting of all integer linear combinations of a set of linearly independent vectors \( \mathbf{b}_1, \cdots, \mathbf{b}_n \in \mathbb{R}^n \). The set of vectors \( \{\mathbf{b}_i\} \) is called a basis of the lattice.

Algorithmic problems related to lattices have been used to construct cryptographic primitives. One of their advantages, compared to other algorithmic problems such as factorization or discrete logarithm, is that they are supposed to be hard to solve even with a quantum computer. Hence, cryptographic constructions built from these problems (supposedly) enjoy post-quantum security (which is not the case of the RSA algorithm for instance).

The main algorithmic problem on lattices considered for cryptography is the shortest vector problem (SVP). It consists, given any basis of a lattice, in finding a non-zero vector of the lattice as small as possible (for the euclidean norm). The complexity of the best algorithms we know to solve this problem increases exponentially in the dimension \( n \) of the lattice.

In order to improve efficiency of the schemes, recent cryptographic constructions use structured lattices, such as ideal lattices. Adding structure to the lattice enables the constructions to reduce significantly the size of the keys and ciphertexts. This might however weaken the security of the construction, since the extra structure might also help an attacker in solving the shortest vector problem in the lattice.

The objective of this internship is to study the hardness of the shortest vector problem in the special case of ideal lattices. An ideal lattice is a lattice which can also be seen as an ideal in some number field of large degree \( K \). It is known that when \( K \) has sufficiently many subfields, then some computations on \( K \) (like for instance computing the units of \( K \)) can be accelerated, by doing a recursion in the subfields of \( K \). The objective of this internship would be to use similar ideas in order to improve the algorithms computing short vectors in ideal lattices when the underlying field \( K \) has many subfields.

The algorithms which find short vectors in lattices are often heuristic. Hence, a non-negligible part of the internship would consist in implementing parts of the algorithms, in order to check that they indeed behave as we expect them to behave.

**Foreknowledge:** basic knowledge of number theory would be an advantage (number fields, ring of integers, algebraic norm), as well as basic knowledge of programming (in Python or Sagemath for instance). No knowledge about lattice reduction is required.
Practicalities

Supervisor: Alice Pellet-Mary  \texttt{alice.pellet-mary@math.u-bordeaux.fr}
Nature of the work: 30% literature, 40% theoretical work, 30% implementation (experimental work)
Where: Institut de mathématiques de Bordeaux
351 cours de la Libération, Talence
Duration: from 3 to 6 months

References
