Approximate-GCD problem and variants

The approximate-GCD (AGCD) problem is an algorithmic problem used in cryptography. The problem is the following: given many approximate multiples \( b_i = p \cdot q_i + e_i \) of a secret prime number \( p \) (with small “noise” \( e_i \ll p \)), the objective is to recover the secret integer \( p \).

This problem is believed to be hard to solve and has been used extensively to construct homomorphic encryption schemes. Many variants of this problem are also being considered:

- \( p \) can be replaced by a product of prime numbers
- a unique exact multiple \( p \cdot x_0 \) may be known
- the integers may be replaced by polynomials (modulo \( X^n + 1 \) for instance)

The hardness of these variants of the AGCD problem is sometimes much less studied than the hardness of the original AGCD problem. The objective of this internship would be to study some of these variants in order to determine how hard they actually are. Multiple approaches can be taken (depending on the length of the internship and the will of the intern student).

**Reductions.** It is known that a small variant of the original AGCD problem is at least as hard as the learning with error problem (see [1]). It would be interesting to see if other variants of the AGCD problem also enjoy similar hardness guarantees (maybe using algebraic variants of the learning with error problem instead of the plain learning with error).

**Attacks.** On the other hands, it would also be interesting to study the known attacks on the AGCD problem and see if they can be extended in order to solve some of the variants more efficiently than what is actually known.

**Foreknowledge:** No knowledge on lattices or on the approximate-GCD problem is required.

**Practicalities**

- Supervisor: Alice Pellet-Mary [alice.pellet-mary@math.u-bordeaux.fr](mailto:alice.pellet-mary@math.u-bordeaux.fr)
- Nature of the work: 40% literature, 60% theoretical work
- Where: Institut de mathématiques de Bordeaux
  351 cours de la Libération, Talence
- Duration: from 3 to 6 months

**References**
