
Faster Lattice Basis Computation via a Natural Generalization of the Euclidean Algorithm

Kim-Manuel Klein^{*1} and Janina Reuter²

¹Universität zu Lübeck = University of Lübeck [Lübeck] – Allemagne

²Christian-Albrechts-Universität zu Kiel = Christian-Albrechts University of Kiel = Université Christian-Albrechts de Kiel – Allemagne

Résumé

The Euclidean algorithm is one of the oldest algorithms known to mankind. Given two integral numbers a_1 and a_2 , it computes the greatest common divisor (gcd) of a_1 and a_2 in a very elegant way. From a lattice perspective, it computes a basis of the sum of two one-dimensional lattices $a_1 \mathbb{Z}$ and $a_2 \mathbb{Z}$ as $\gcd(a_1, a_2) \mathbb{Z} = a_1 \mathbb{Z} + a_2 \mathbb{Z}$. In this paper, we show that the classical Euclidean algorithm can be adapted in a very natural way to compute a basis of a general lattice $L(A_1, \dots, A_n)$ given vectors $A_1, \dots, A_n \in \mathbb{Z}^d$ with $n > \text{rank}(a_1, \dots, a_d)$. Similar to the Euclidean algorithm, our algorithm is very easy to describe and implement.

^{*}Intervenant