Titre du slide

Theorem (Correction)

L'algorithme BasisReduction (LLL) calcule une base réduite de $\mathscr{L}$.

Algorithme 1 : *Proprification de g_i*

$g_i := g_i - \lceil \mu_{ij} \rfloor \cdot g_j$;
Mettre à jour $(B^*, U) := \mathrm{GSO}(B)$;

Lemma

1. *Soit $G, G^*, M \in \mathbb{Q}^{n \times n}$ et $H, H^*, N \in \mathbb{Q}^{n \times n}$ les matrices des g_k, g_k^*, μ_{kl} avant et après Proprification de g_i. Soit $E = I_n - \lceil \mu_{ij} \rfloor E_{ij} \in \mathbb{Z}^{n \times n}$, où E_{ij} désigne la matrice élémentaire.*
   Alors
   $$H = EG, \quad N = EM, \quad H^* = G^*.$$
2. *Avant Proprification de g_i, on a :*