

# Réseaux Euclidiens

## Algorithme de Lenstra–Lenstra–Lovász

- Soit  $B = b_1, \dots, b_n \in \mathbb{R}^n$  la base d'un réseau  $L(B)$  et  $0.25 < \delta < 1$
- [Lenstra, 1982]  $B^*$  une base  $\delta$ -LLL réduite de  $L(B)$  est telle que

$$\|b_1^*\| \leq \frac{2^{n-1}}{\sqrt{4\delta - 1}} \lambda$$

- Résout  $SVP_\gamma$  pour  $\gamma$  exponentiel en temps polynomial

# Apprentissage avec erreurs

