

Algorithme naïf

Énumération de tous les points dans une certaine borne

- Soit $\mathcal{L}(B)$ un réseau, on calcule la base du réseau dual $D = B^{-T} = d_1, d_2, \dots, d_n \in \mathbb{R}^n$
- Notons $w = \min_{b_i \in B} \|b_i\|$ la norme du plus petit vecteur de la base
- On peut donc borner les coefficients $|x_i| \leq \|d_i\|w$
- Puis énumérer $\left\{ \sum_{i=1}^n x_i b_i : x_i \in \mathbb{Z}, |x_i| \leq \|d_i\|w \right\}$, un nombre exponentiel en n de points

Optimisation

Coupure de l'espace de recherche en deux

- Puisque $\|v\| = \|-v\|$
- Il suffit de ne considérer, pour un i donné,
- Que les x_i positifs

