Plan de l'exposé

- **Définition**
  - Réseau d'espace vectoriel Euclidien
  - Problème du plus court vecteur
  - Algorithme d'énumération naïf
- **Optimisation**
  - Coupure de l'espace en deux
  - Coupure par mise à jour des bornes (B&B)
  - Traitement par lots
  - Approximation par réduction de base (**LLL**)
- **Benchmarks**
  - Réseau arbitraire
  - Petite instance difficile
  - Grande instance difficile
- **Ressources**
  - Code
  - Références

Réseau d'un espace vectoriel Euclidien

a.k.a. a lattice, a discrete subgroup of $\mathbb{R}^n$

- Soient $n \in \mathbb{N}, B \in GL_n(\mathbb{R})$ avec colonnes $b_1, \ldots, b_n \in \mathbb{R}^n$
- Alors le réseau $\mathscr{L}$ engendré par la base B se note

$$\mathscr{L}(B) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\} \subseteq \mathbb{R}^n$$

- Ex $\mathbb{Z}^2$: