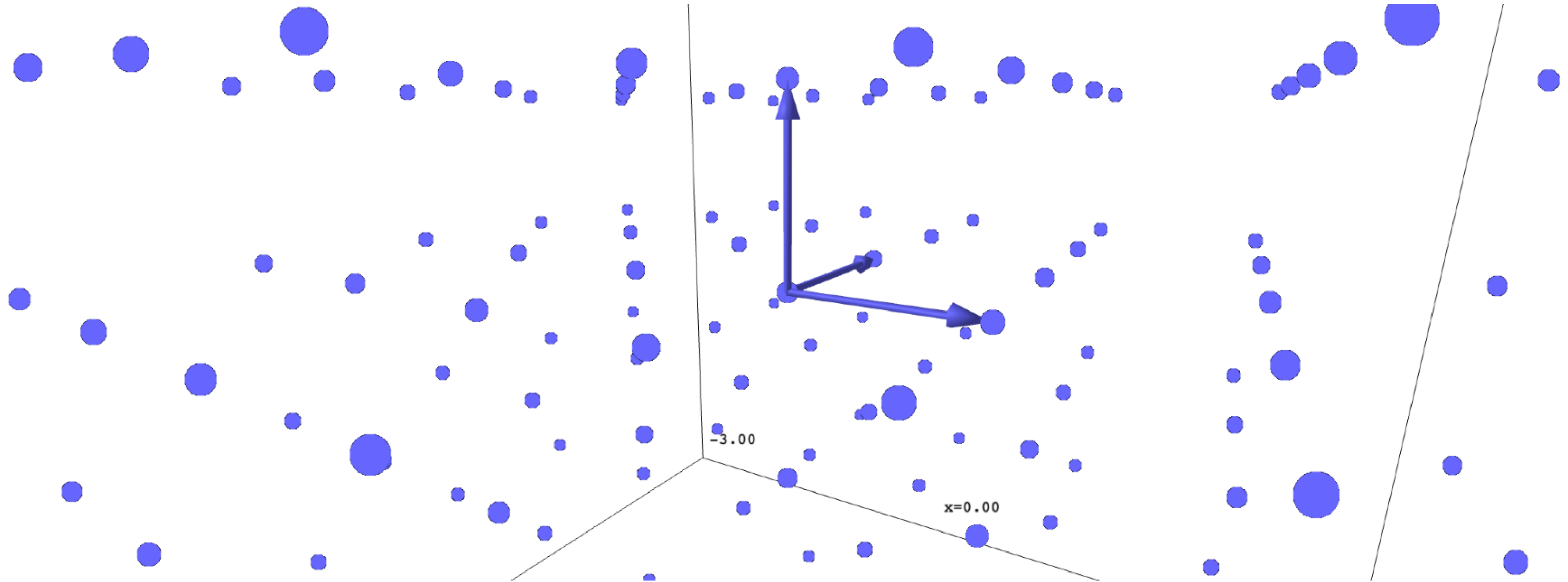


Réseaux Euclidiens

Exemple: \mathbb{Z}^3



Réseaux Euclidiens

Problème du vecteur le plus court

- SVP demande à trouver un $v \in L$ non nul tel que $\|v\| = \lambda$
 - [vEB, 1981] ? NP-Hard pour la norme uniforme
 - [Ajtai, 1998] NP-Hard (réduction randomisée) pour la norme Euclidienne
- SVP_γ demande à trouver un $v \in \Lambda$ non nul tel que $\|v\| \leq \gamma\lambda$
 - Algorithme LLL efficace pour un facteur d'approximation exponentiel