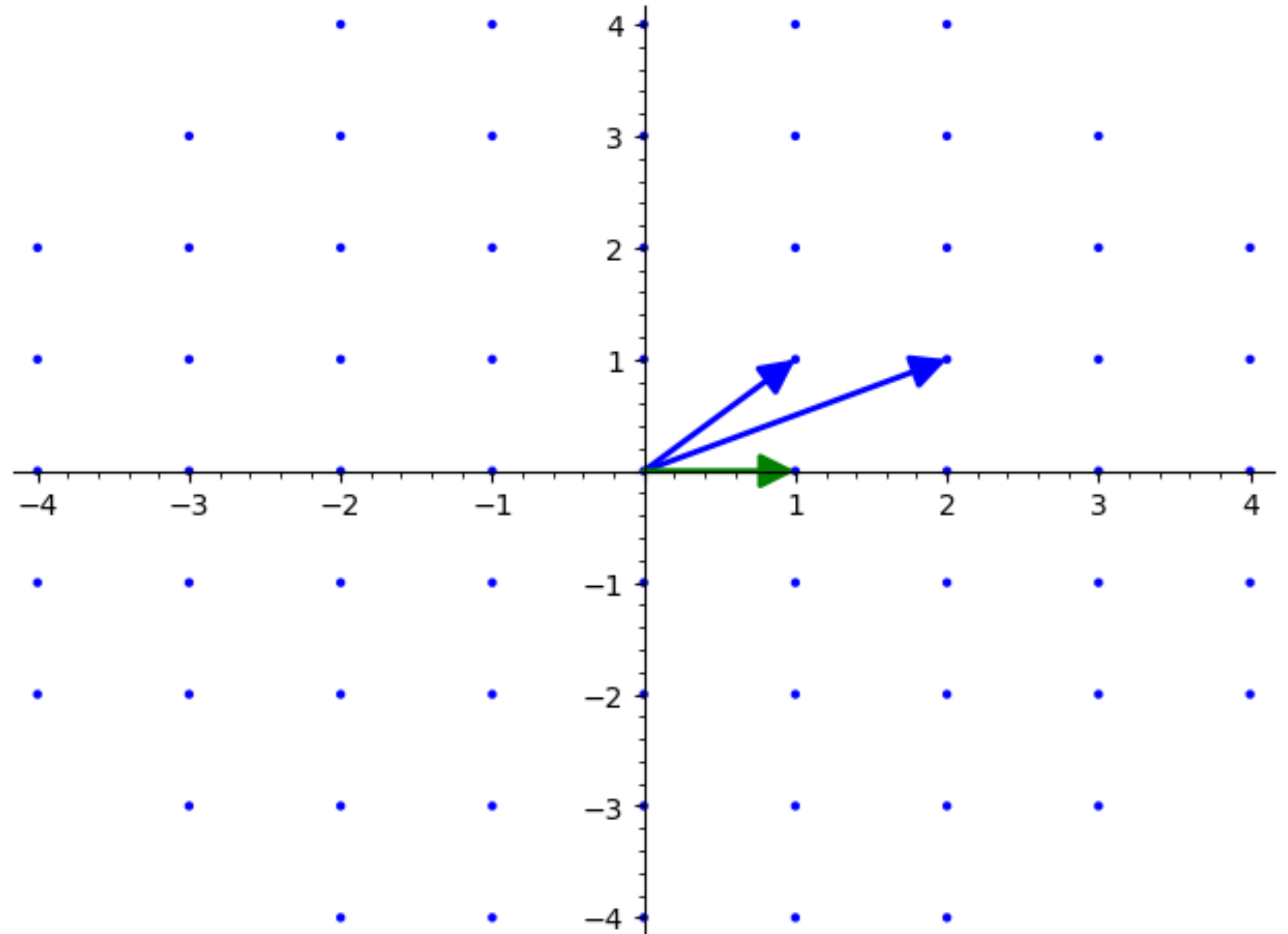


Réseaux Euclidiens

Vecteur le plus court

- Soit $B = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$
- Le réseau engendré est \mathbb{Z}^2
- Le vecteur le plus court est
 - $v = (0, \pm 1)$ ou $v = (\pm 1, 0)$
 - $\lambda = 1$



Réseaux Euclidiens

Recherche du vecteur le plus court: énumération

- Soit $D = B^{-T} = d_1, \dots, d_n \in \mathbb{R}^n$ la base du réseaux dual de $L(B)$

D est telle que $b_i d_j = \delta_{i,j}$ (1 si $i = j$ et 0 sinon)

- Soit $w = \min_{b_i \in B} \|b_i\|$ la norme du plus petit vecteur de la base
- On peut borner les coefficients du plus court vecteur $v = \sum_{i=1}^n x_i b_i$ par

$$|x_i| \leq \|d_i\| w$$