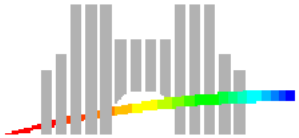
# L'algorithme LLL et certaines de ses applications

Nicolas Brisebarre
Arénaire, LIP, ENS Lyon
LArAl, Univ. St-Étienne

15 mai 2003


Si $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$, alors

$$(x|y) = x_1 y_1 + \cdots + x_n y_n.$$

On pose $||x|| = (x|x)^{1/2} = (x_1^2 + \cdots + x_n^2)^{1/2}$ et $||x||_\infty = \max_{1 \leq i \leq n} |x_i|$.

# Notion de réseau

**Définition .** *1. Un réseau est un sous-groupe-discret de* $\mathbb{R}^n$.

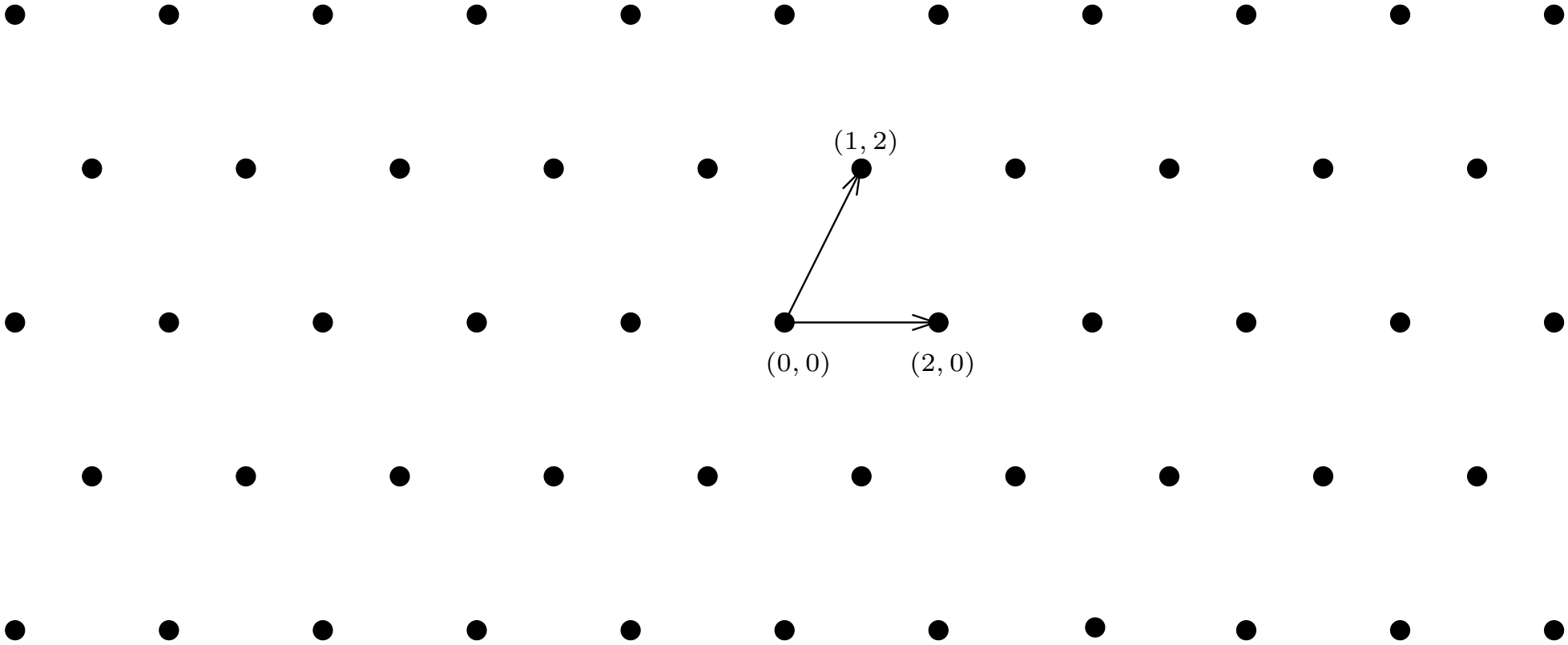
*2. Soit* $L$ *une partie non vide de* $\mathbb{R}^n$, $L$ *est un réseau ssi il existe des vecteurs* $b_1, \ldots, b_d$ $\mathbb{R}$*-linéairement indépendants tels que*

$$L = \mathbb{Z}.b_1 \oplus \cdots \oplus \mathbb{Z}.b_d.$$

$(b_1, \ldots, b_d)$ *est une base du réseau.*

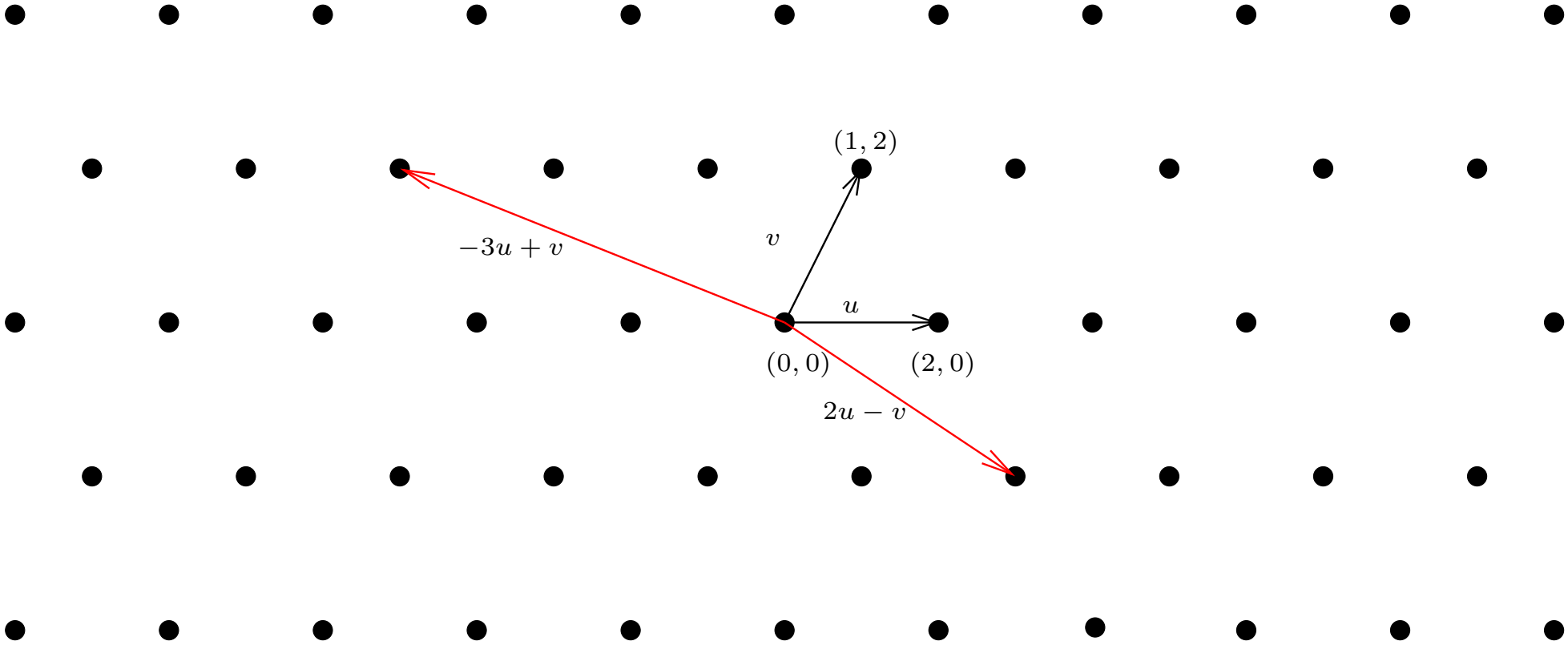
**Exemples.** $\mathbb{Z}^n$, tout sous-groupe de $\mathbb{Z}^n$.

**Remarque .** *On dit qu'un réseau* $L$ *est* entier *(resp.* rationnel*) lorsque* $L \in \mathbb{Z}^n$ *(resp.* $\mathbb{Q}^n$*).*




Le réseau $\mathbb{Z}(2,0) \oplus \mathbb{Z}(1,2)$.

**Proposition .** *Si* $(e_1, \ldots, e_k)$ *et* $(f_1, \ldots, f_j)$ *sont deux familles libres qui engendrent le même réseau, alors* $k = j$ *(rang du réseau) et il existe une matrice* $M$ *de dimension* $k \times k$*, à coefficients entiers, de déterminant* $\pm 1$ *telle que* $(e_i) = (f_i)M$*.*




Le réseau $\mathbb{Z}(2,0) \oplus \mathbb{Z}(1,2)$.

**Proposition .** *Si* $(e_1, \ldots, e_k)$ *et* $(f_1, \ldots, f_j)$ *sont deux familles libres qui engendrent le même réseau, alors* $k = j$ *(rang du réseau) et il existe une matrice* $M$ *de dimension* $k \times k$*, à coefficients entiers, de déterminant* $\pm 1$ *telle que* $(e_i) = (f_i)M$*.*

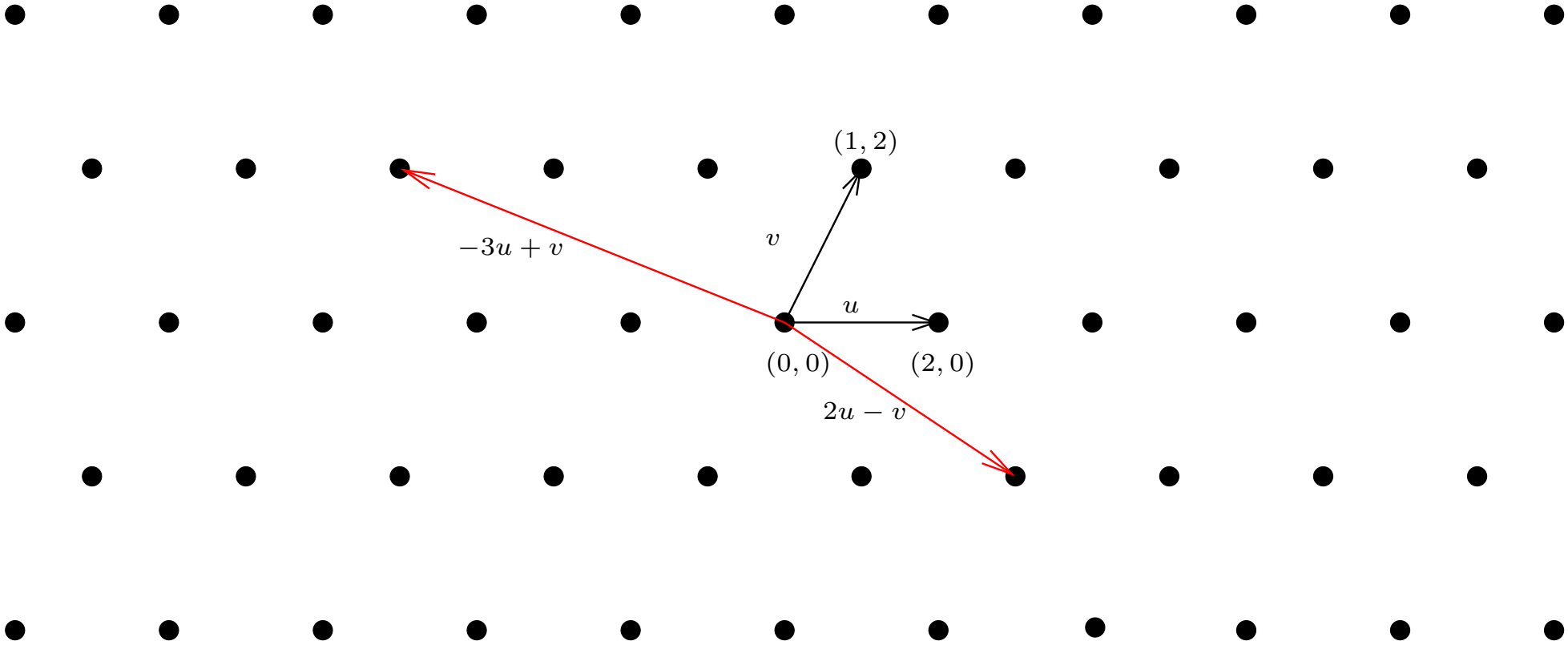
Il y a une infinité de bases mais certaines sont plus intéressantes que d'autres.

**Définition .** *Soit $L$ un réseau de $\mathbb{R}^n$, $(b_1, \ldots, b_d)$ une base de $L$. On appelle discriminant de $L$, et on note $\Delta(L)$ ou disc$(L)$ le déterminant de la matrice de Gram $(b_i|b_j)_{1\leq i,j\leq d}$. Le déterminant (ou volume) de $L$ noté $\det(L)$ est la racine carrée de $\Delta(L)$.*

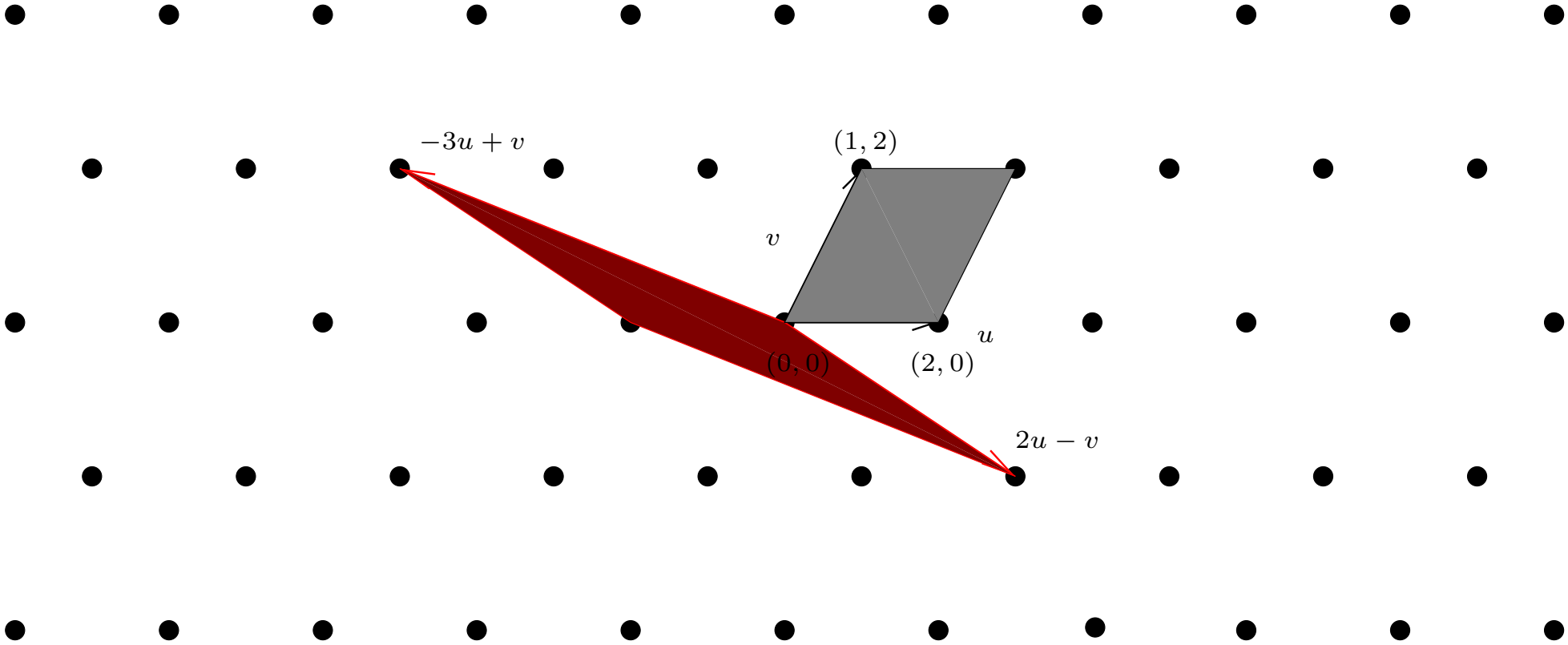
Lorsque $d = n$ ($L$ réseau total),

$$\det(L) = |\det(b_i)| = \text{ volume de } \left\{ \sum_{1\leq i\leq n} \alpha_i b_i, \alpha_i \in [0,1[ \right\},$$

le *parallélotope fondamental* du réseau.




Le réseau $\mathbb{Z}(2,0) \oplus \mathbb{Z}(1,2)$.




Le réseau $\mathbb{Z}(2,0) \oplus \mathbb{Z}(1,2)$.

# Vecteurs courts

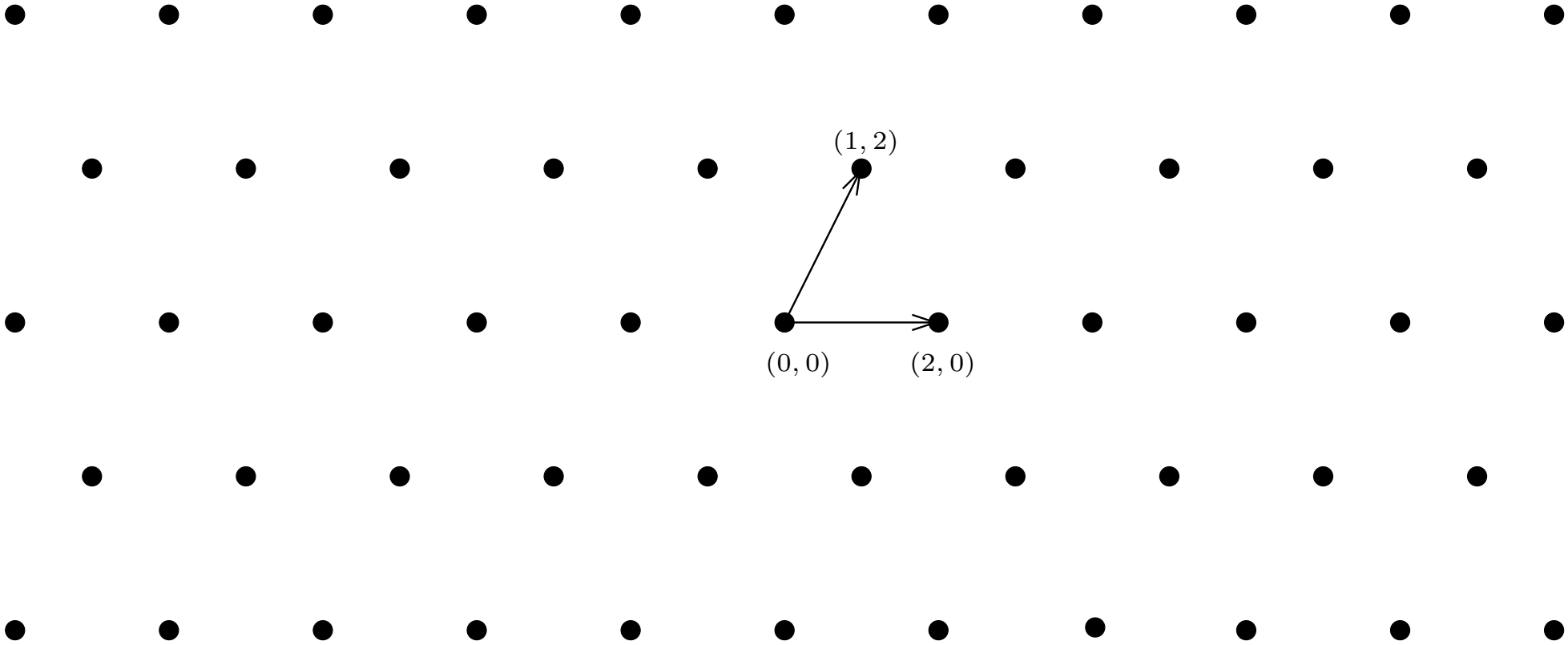
Soit $L$ un réseau de dimension $d$. $L$ est discret $\Rightarrow$ $L$ a au moins un plus court vecteur non nul. On note $||L||$ sa longueur : "norme du réseau". C'est le premier minimum $\lambda_1(L)$ du réseau.

Pour $k$ entre $1$ et $d$, le $k$-ème minimum de $L$

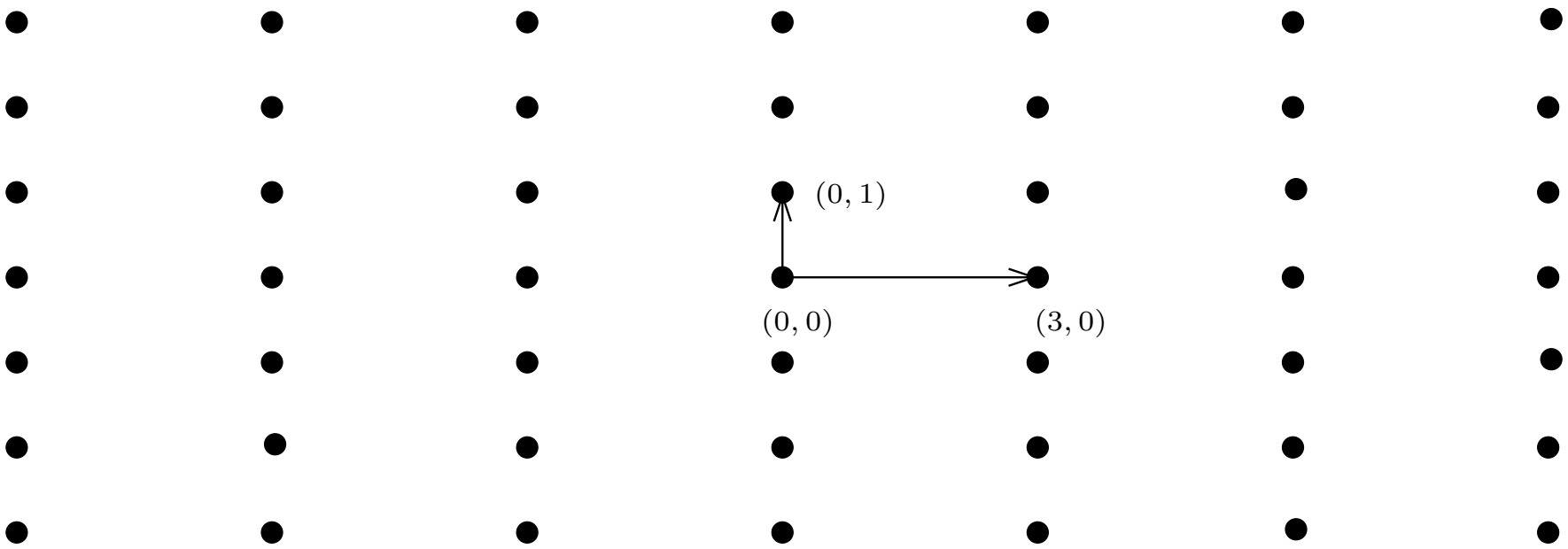
$$\lambda_k(L) := \inf\{\rho \in \mathbb{R}; \dim \mathrm{Vect}(L \cap B(0,\rho)) \geq k\}.$$

En d'autres termes, le $k$-ème minimum est le plus petit réel $\rho$ tel qu'il existe $k$ vecteurs $\mathbb{R}$-linéairement indépendants du réseau de norme au plus $\rho$.

Minkovski : $\lambda_1(L) \leq \sqrt{d}(\det(L))^{1/d}$.




Le réseau $\mathbb{Z}(2,0) \oplus \mathbb{Z}(1,2)$.




Le réseau $\mathbb{Z}(3,0) \oplus \mathbb{Z}(0,1)$.

Quand $L = \mathbb{Z}^2$, $\lambda_1(L) = \lambda_2(L) = 1$.

# Invariant d'Hermite

Soit $\gamma(L) = \left(\frac{\lambda_1(L)}{\det(L)^{1/\dim L}}\right)^2$ : invariant d'Hermite de $L$.

Minkovski : $\lambda_1(L) \leq \sqrt{d}(\det(L))^{1/d} \Longrightarrow$ Constante d'Hermite de rang $d$ :

$$\gamma_d = \sup_{L \text{ réseau de rang } d} \gamma(L).$$

**Remarque .** $\gamma_d$ *liée au problème des empilements réguliers de sphères.*

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\gamma_n^n$ | 1 | 4/3 | 2 | 4 | 8 | 64/3 | 64 | 256 |

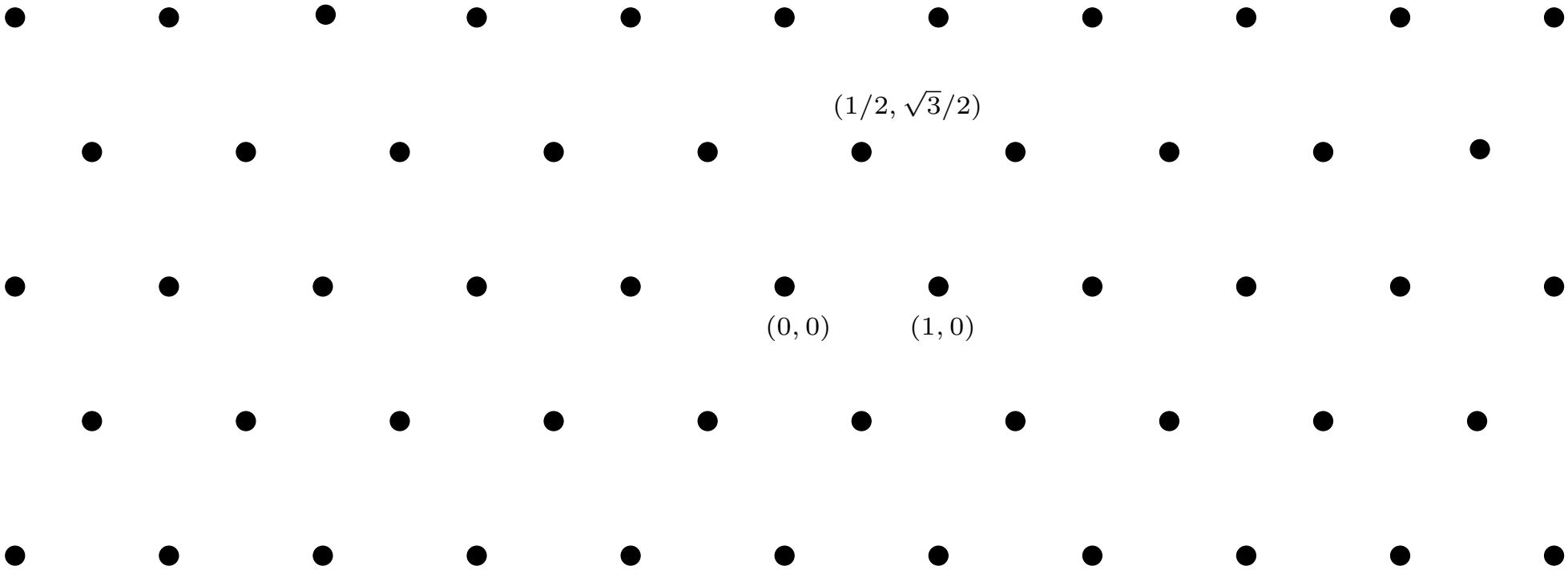
Constante d'Hermite de rang $d$ :

$$\gamma_d = \sup_{L \text{ réseau de rang } d} \left( \frac{\lambda_1(L)}{\det(L)^{1/\dim L}} \right)^2.$$

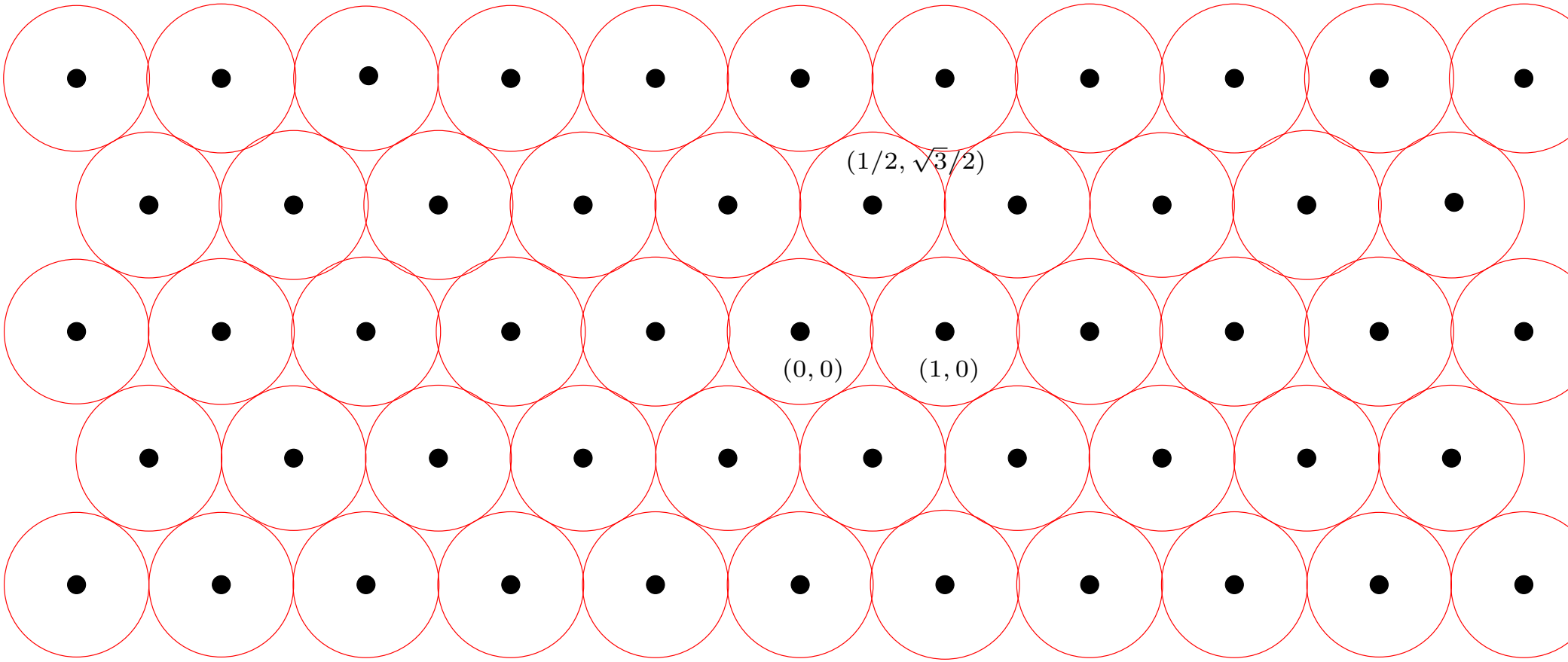
| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\gamma_n^n$ | 1 | $4/3$ | 2 | 4 | 8 | $64/3$ | 64 | 256 |

Actuellement,

$$\frac{d}{2\pi e} + \frac{\log(\pi d)}{2\pi e} + o(1) \leq \gamma_d \leq \frac{1.744d}{2\pi e}(1 + o(1)).$$




Le réseau $\mathbb{Z}(1,0) \oplus \mathbb{Z}\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.




Le réseau $\mathbb{Z}(1,0) \oplus \mathbb{Z}\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ réalise $\gamma_2 = 2/\sqrt{3}$.

# Vecteurs courts

**Théorème . (Minkovski)** *Pour tout réseau $L$ de dimension $n$, pour tout $r \leq d$, on a*

$$\prod_{i=1}^{r} \lambda_i(L) \leq \gamma_d^{r/2} (\det(L))^{r/d}.$$

*Pour $r = d$, on a*

$$1 \leq \frac{\prod_{i=1}^{d} \lambda_i(L)}{\det(L)} \leq \gamma_d^{d/2}.$$

# Base réduite

**Proposition .** *Soit $L$ un réseau de rang $\leq 4$, il existe une base formée de vecteurs réalisant les minima successifs de $L$.*

En dimension $\geq 5$, il n'est pas toujours possible de trouver une base formée de vecteurs réalisant les minima successifs.

En dimension $\geq 5$, il n'est pas toujours possible de trouver une base formée de vecteurs réalisant les minima successifs. Soit $L$ le réseau donné par

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Les minima successifs $= 2$ réalisés par $\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$.

# Orthogonalisation de Gram-Schmidt

**Données** : Une base $(b_i)$ de $\mathbb{R}^n$.

**Sortie** : Une base $(b_i^*)$ vérifiant
- $(b_i^*)$ est orthogonale ;
- $\mathrm{Vect}(b_1^*, \ldots, b_k^*) = \mathrm{Vect}(b_1, \ldots, b_k)$ pour tout $k$.

On pose $b_1^* = b_1$ et $b_k^*$ est le projeté orthogonal de $b_k$ orthogonalement au sous-espace $\mathrm{Vect}(b_1, \ldots, b_{k-1})$.

On cherche $b_k^*$ sous la forme $b_k + \sum_{i=0}^{k-1} m_{k,i} b_i^*$.

Nécessairement, $m_{k,i} = -(b_k | b_i^*)/\|b_i^*\|^2$.

**Remarques .**

- *On a* $\det L = \prod_{1 \leq i \leq n} ||b_i^*||$.
- *Pour tout* $i = 1, \ldots, d$, $||b_i^*|| \leq ||b_i||$.

**Lemme .** *Si* $(b_1, \ldots, b_d)$ *est une base d'un réseau* $L$, *alors, pour tout* $1 \leq i \leq d$,

$$\lambda_i(L) \geq \min_{i \leq j \leq d} ||b_j^*||.$$

# Défaut de longueur, défaut d'orthogonalité

**Remarque .** *Déterminant constant donc base formée de vecteurs courts va de pair avec base formée de vecteurs presque orthogonaux.*

**Définition .** *Soit* $L$ *un réseau de base* $b = (b_k)_{1 \leq k \leq d}$ *avec* $||b_1|| \leq ||b_2|| \leq \ldots \leq ||b_d||$. $i$*-ème défaut de longueur de* $b$ *:*

$$\mu_i(b) = \frac{||b_i||}{\lambda_i(L)} \geq 1.$$

**Définition .** *Le défaut d'orthogonalité d'une base* $(b_1, \ldots, b_d)$ *est*

$$\rho(b) = \prod_{i=1}^{d} \frac{\|b_i\|}{\|b_i^*\|} = \frac{\prod_{i=1}^{d} \|b_i\|}{\det(L)}.$$

Une base $b$ est orthogonale ssi $\rho(b) = 1$.

Théorème de Minkowski $\Rightarrow$

**Proposition .** *On a*

$$1 \leq \frac{\rho(b)}{\prod_{i=1}^{d} \mu_i(b)} \leq \gamma_d^d.$$

**Remarque .** *« base formée de vecteurs courts » et « base presque orthogonale » : notions voisines.*

# Diverses notions de réduction

**Définition .** *Une base* $(b_i)_{1\leq i\leq d}$ *d'un réseau* $L$ *est dite* réduite au sens de Minkowski *si pour tt* $1 \leq i \leq d$, $b_i$ *est un plus court vecteur t. q.* $(b_1, \ldots, b_{i-1}, b_i)$ *soit une famille libre pouvant être complétée en une base de* $L$.

**Définition .** *Une base* $(b_i)_{1\leq i\leq d}$ *d'un réseau* $L$ *est dite* réduite au sens de Korkine-Zolotarev *si*

- $(b_i)_{1\leq i\leq d}$ *est propre ;*
- $\forall i = 1, \ldots, d$, $b_i^*$ *est un élément de longueur minimale de* $proj_{<b_1,\ldots,b_{i-1}>^\perp} < b_1, \ldots, b_i >$.

**Remarques .**

- *On dit parfois* au sens de Hermite *au lieu d'*au sens de K-Z
- $||b_1||$ *: premier minimum du réseau.*
- *Pas d'algos polynomiaux pour ces deux notions de réduction. Helfrich (1985) : algos (non polynomiaux en la dimension).*

# La réduction faible

**Définition .** *Une base* $(b_i)$ *d'un réseau* $L$ *est dite* faiblement réduite *(ou* propre*) si les coefficients* $m_{i,j}$ *du procédé de Gram-Schmidt vérifient*

$$|m_{i,j}| \leq \frac{1}{2}.$$

Une base quelconque peut aisément être rendue propre, en faisant :

Pour $k$ de $2$ à $n$ faire
  Pour $j$ de $k-1$ à $1$ faire
    $b_k \leftarrow b_k - \lfloor (b_k | b_j^*) / \|b_j^*\|^2 \rceil b_j$

**Remarque .** $L$ *et* $(b_i^*)$ *sont inchangés.*

**Définition .** *Soit $s$ un paramètre réel positif supérieur à $2/\sqrt{3}$. Une base $(b_i)_{1\leq i\leq d}$ d'un réseau $L$ est dite* réduite au sens de $s$-Siegel *si*

- $(b_i)_{1\leq i\leq d}$ *est propre ;*
- $\forall i = 1, \ldots, d$, $\|b_{i+1}^*\| \geq \frac{1}{s}\|b_i^*\|$.

**Définition .** *Soit $t \in \left]\frac{1}{4}, 1\right[$. Une base $(b_i)_{1\leq i\leq d}$ d'un réseau $L$ est dite* réduite au sens de $t$-Lovász *ou* LLL-réduite à un facteur $t$ *si*

- $(b_i)_{1\leq i\leq d}$ *est propre ;*
- $\forall i = 1, \ldots, d-1$, $\|b_{i+1}^*\|^2 + m_{i+1,i}^2\|b_i^*\|^2 \geq t\|b_i^*\|^2$.

**Proposition .** *Une base $t$-Lovász réduite est $s$-Siegel réduite, avec $s = 1/\sqrt{t - 1/4}$.*

Preuve. La condition de réduction se récrit $\frac{\|b_{i+1}^*\|}{\|b_i^*\|} \geq \sqrt{t - m_{i+1,i}^2}$. Hyp. de propreté : $|m_{i,j}| \leq 1/2$. □

Les bases $s$-Siegel et $t$-Lovász réduites se calculent en temps polynomial !

**Théorème .** *Soit $(b_i)_{1\leq i\leq d}$ une base réduite au sens de $s$-Siegel d'un réseau de dimension $d$. Alors on a*

$$\mu_i(b) = \frac{||b_i||}{\lambda_i(L)} \leq s^{d-1}.$$

*et*

$$\rho(b) = \prod_{i=1}^{d} \frac{\|b_i\|}{\|b_i^*\|} = \frac{\prod_{i=1}^{d} \|b_i\|}{\det(L)} \leq s^{d(d-1)/2}.$$

**Remarque .** *En particulier, $\|b_1\| \leq s^{d-1}\lambda_1(L)$.*

*Initialement (et souvent), $t = 3/4$, soit $s = \sqrt{2}$.*

# Problèmes algorithmiques

On sait résoudre en temps polynomial les deux problèmes suivants

**Problème .** *On se donne une famille génératrice d'un réseau $L$. Déterminer une base de $L$.*

**Problème .** *Soit une base d'un réseau $L$ et $x$ un point de l'espace. Décider si $x$ appartient à $L$ et, si tel est le cas, donner la décomposition de $x$ selon la base.*

# Problème du plus court vecteur non nul

**Problème . (SVP)** *Étant donnée une base d'un réseau rationnel $L$ de dimension $n$, trouver $u \in L$ qui réalise le premier minimum de $L$. Problème d'approximation associé : trouver $v \in L \setminus \{0\}$ tel que $||v|| \leq k\lambda_1(L)$ où $k \in \mathbb{R}$ fixé.*

**Théorème .** *[Ajtai (1997), Miccianco (1998)] Le problème de trouver un vecteur $v$ tel que $\|v\| = \lambda_1(L)$ est NP-dur pour des réductions polynomiales probabilistes, et reste NP-dur si on tolère un facteur d'approximation $< \sqrt{2}$.*

Goldreich et Goldwasser : approcher SVP à un facteur $\sqrt{d/O(\log d)}$ n'est pas NP-dur.

Pas d'algo polynomial connu pour approcher SVP à un facteur $f(d)$ avec $f$ polynôme.

# Problème du vecteur le plus proche

**Problème . (CVP)** *Étant donnés une base d'un réseau rationnel* $L$ *de* $\mathbb{Q}^n$ *et* $x \in \mathbb{Q}^n$ *trouver* $y \in L$ *tel que* $||x - y|| = \mathrm{dist}(x, L)$. *Problème d'approximation associé : trouver* $y \in L \setminus \{0\}$ *tel que* $||x - y|| \leq k\mathrm{dist}(x, L)$ *où* $k \in \mathbb{R}$ *fixé.*

Emde Boas (1981) : CVP est NP-dur

Goldreich et al. : CVP ne peut pas être plus facile que SVP.

Goldreich et Goldwasser : approcher CVP à un facteur $\sqrt{d/O(\log d)}$ n'est pas NP-dur.

# Problème de la plus petite base

**Problème . (SBP)** *Étant donnée une base d'un réseau rationnel $L$ de dimension $n$, trouver une base $\{b_1, \ldots, b_n\}$ qui minimise le produit $||b_1|| \cdots ||b_n||$.*

Problème NP-dur.

# Cas de la dimension $2$ - L'algorithme de Gauss

Soit $L$ un réseau de rang $2$.

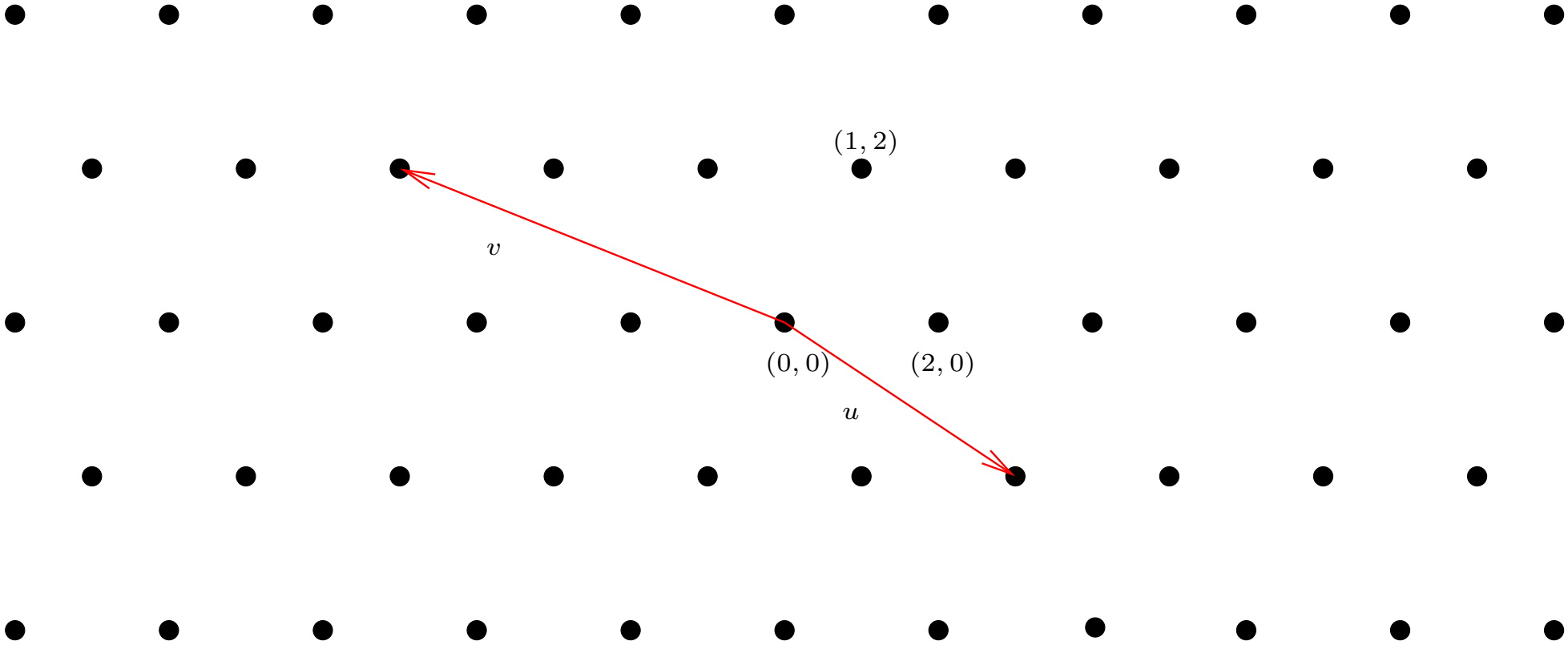
**Données** : $(u_0, v_0)$ base de $L$ avec $\|u_0\| \leq \|v_0\|$.

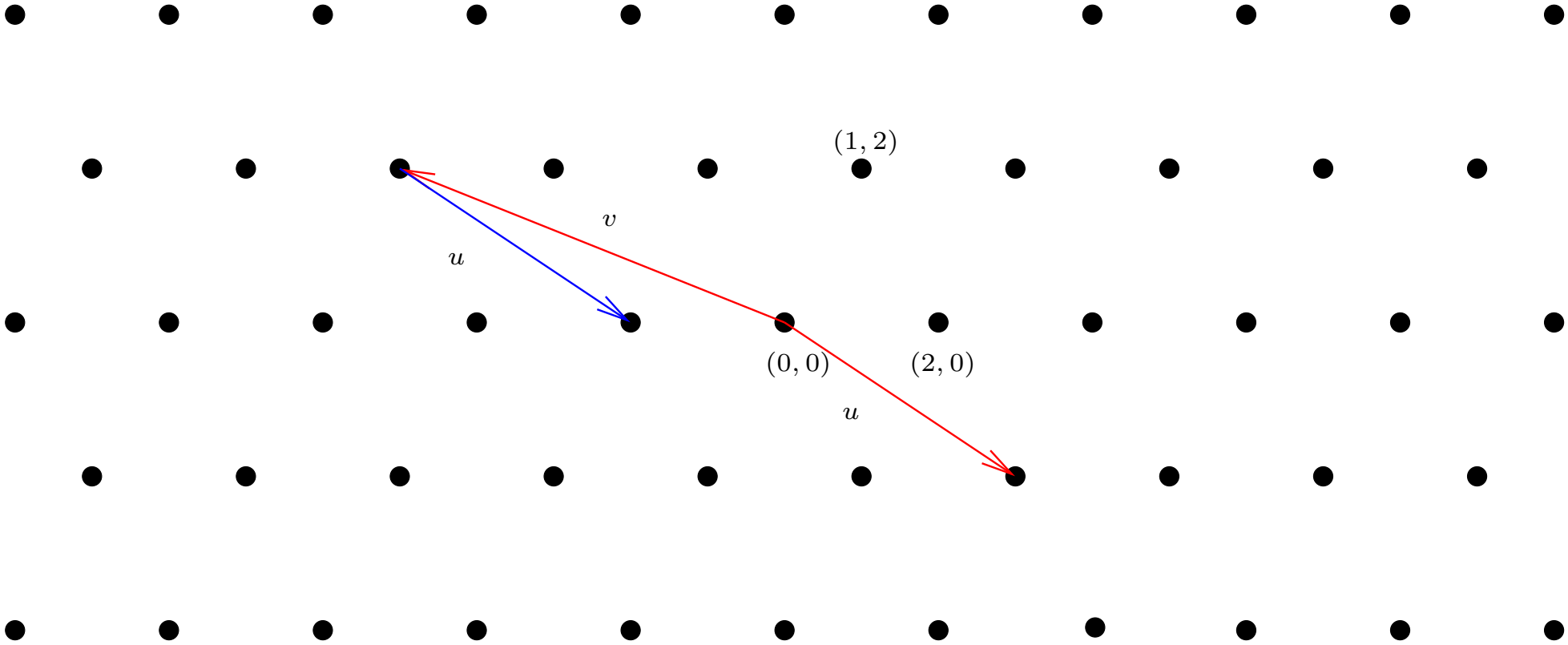
- $(u, v) \leftarrow (u_0, v_0)$.
- Répéter
  - $q = \lfloor (u|v)/\|u\|^2 \rceil$
  - $(u, v) \leftarrow (v - qu, u)$.

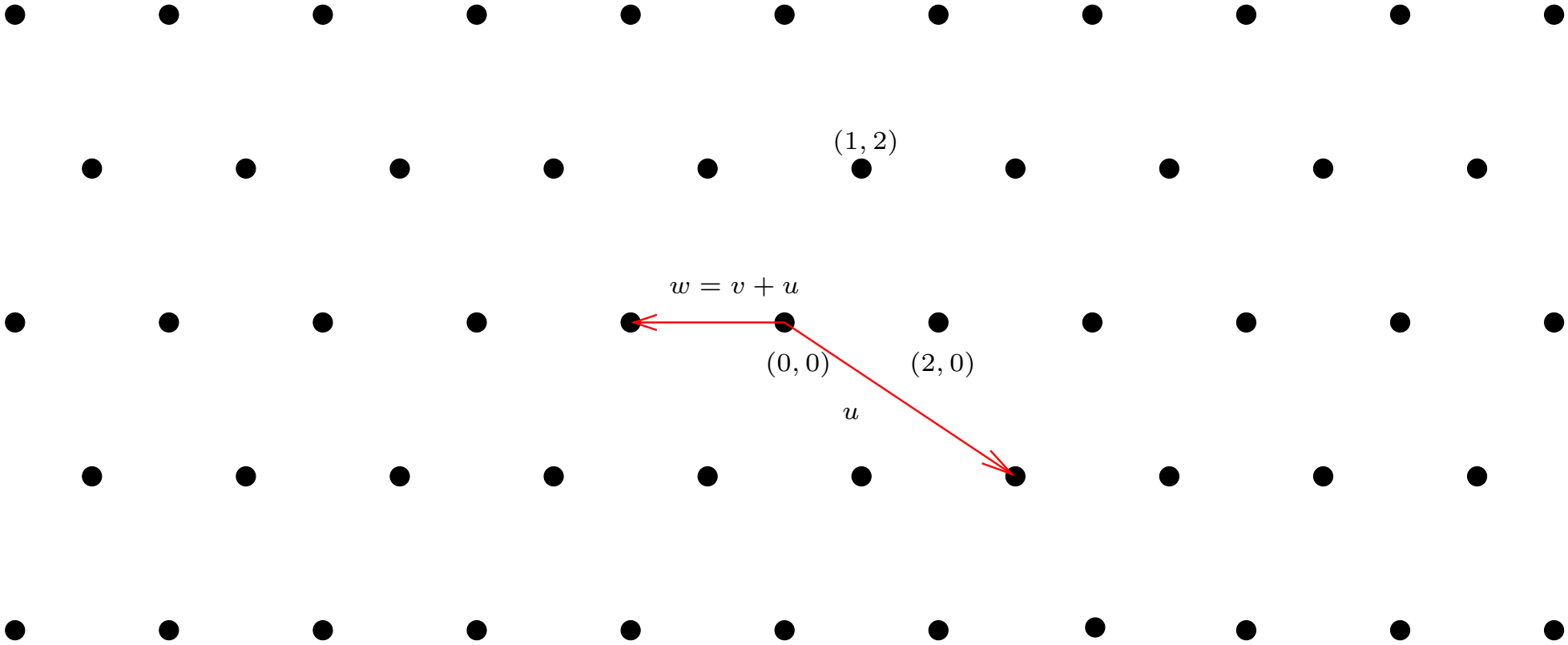
  jusqu'à ce que $\|v\| \leq \|u\|$
- Renvoyer $(u_1, v_1) = (v, u)$.

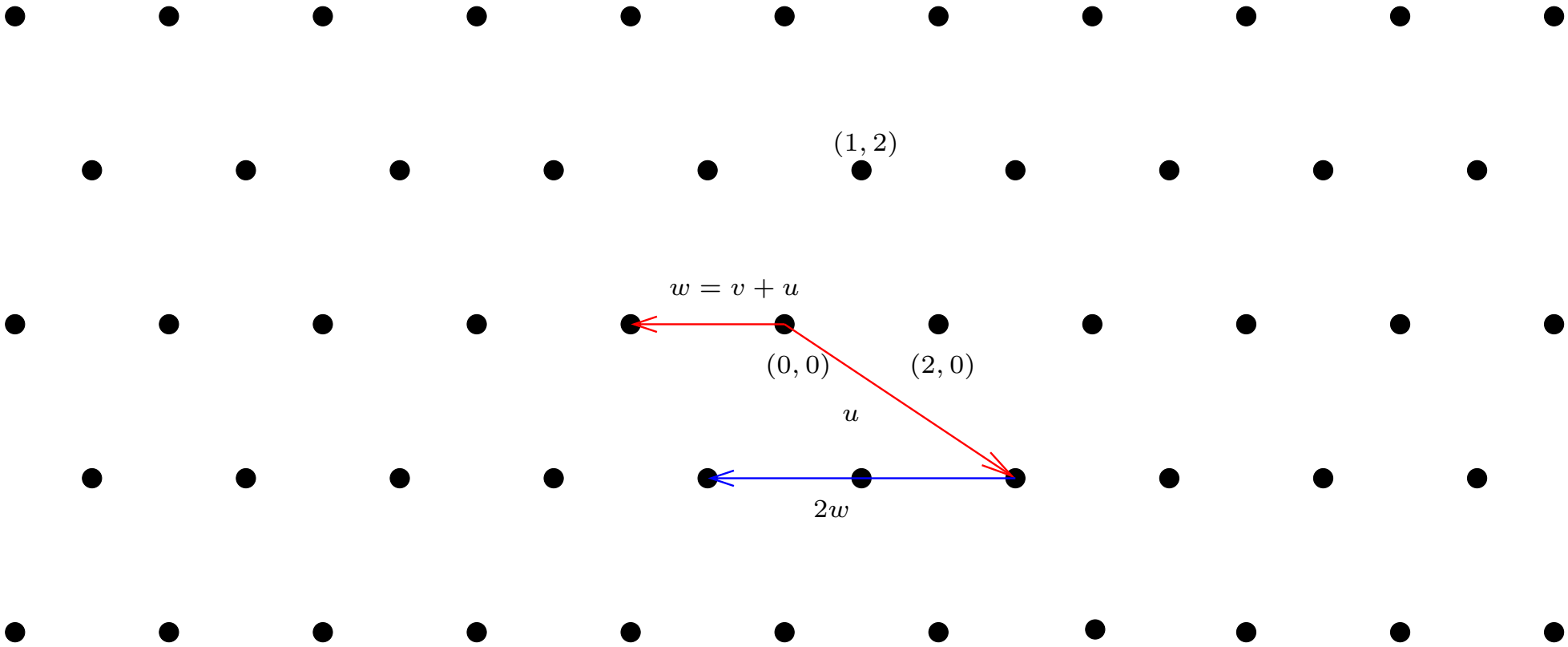
**Sortie** : une base réduite de $L$ réalisant $\lambda_1(L)$ et $\lambda_2(L)$.

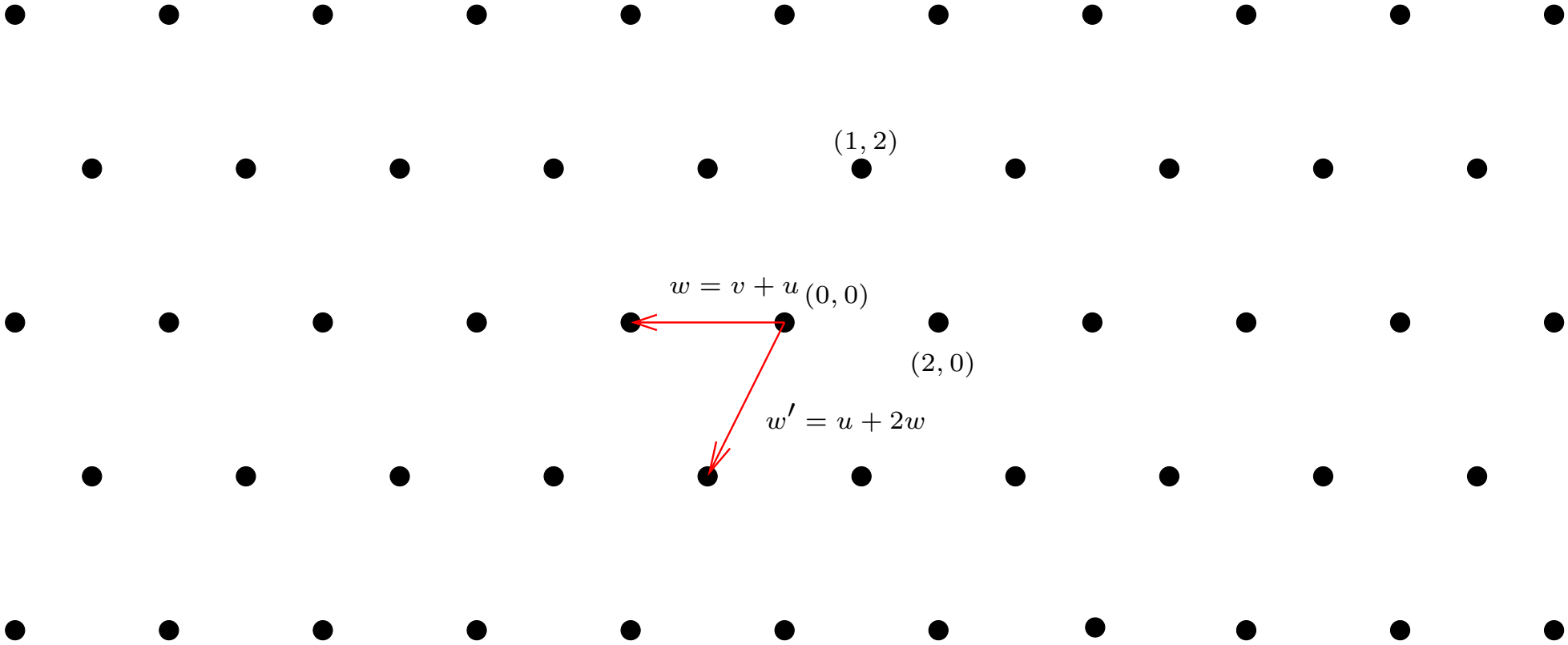
**Théorème .** *L'algorithme de Gauss termine en temps polynomial, renvoie une base du réseau $L$ de la forme $(u_1, v_1)$ avec $\|u_1\| \leq \|v_1\| \leq \|x\|$ pour tout $x \in L - < u_1 >$.*


$(1, 2)$
$v$
$(0, 0)$
$(2, 0)$
$u$


$(1,2)$
$v$
$u$
$(0,0)$
$(2,0)$
$u$


$(1,2)$
$w = v + u$
$(0,0)$
$(2,0)$
$u$


$(1,2)$
$w = v + u$
$(0,0)$
$(2,0)$
$u$
$2w$




Base réduite $(u + v, 2u + 3v)$.

# Algorithme de $t$-Gauss

Soient $L$ un réseau de rang $2$, $t$ un réel t.q. $1 < t \leq \sqrt{3}$.

**Données** : $(u_0, v_0)$ base de $L$ avec $\|u_0\| \leq \|v_0\|$.

- $(u, v) \leftarrow (u_0, v_0)$.
- Répéter
  - $q = \lfloor (u|v)/\|u\| \rceil$
  - $(u, v) \leftarrow (v - qu, u)$.

  jusqu'à ce que $\|v\| \leq t\|u\|$
- Renvoyer $(u_1, v_1) = (v, u)$.

**Sortie** : une base $(u, v)$ de $L$ t. q. deux des vecteurs $u$, $v$, $u - v$ réalisent $\lambda_1(L)$ et $\lambda_2(L)$.

# Complexité de l'algorithme de Gauss

Soient $(u, v)$ une base de $L$ avec $\max(||u||, ||v||) \leq M$, $t \in \mathbb{R}$ t.q. $1 < t \leq \sqrt{3}$.

$k(t)$ : nbre d'itérations de $t$-Gauss.

$k$ : nbre d'itérations de Gauss.

On a $k(t) \leq \log_t M + 1$.

Pour $1 < t \leq \sqrt{2}$, $k(t) \leq k \leq k(t) + 1$ : Gauss de complexité polynomiale.

Pire cas (B. Vallée) : $k(t) \leq \log_{1+\sqrt{2}} M + 3$.

# Cas de la dimension $3$

Soit $L$ un réseau de rang $3$, B. Vallée (1986) a donné un algorithme polynomial renvoyant une base du réseau $L$ atteignant les trois minima.

# Orthogonalisation de Gram-Schmidt

**Données** : Une base $(b_i)$ de $\mathbb{R}^n$.

**Sortie** : Une base $(b_i^*)$ vérifiant
- $(b_i^*)$ est orthogonale ;
- $\mathrm{Vect}(b_1^*, \ldots, b_k^*) = \mathrm{Vect}(b_1, \ldots, b_k)$ pour tout $k$.

On a $b_1^* = b_1$ et $b_k^*$ est le projeté orthogonal de $b_k$ orthogonalement au sous-espace $\mathrm{Vect}(b_1, \ldots, b_{k-1})$.

On cherche $b_k^*$ sous la forme $b_k + \sum_{i=0}^{k-1} m_{k,i} b_i^*$.

Nécessairement, $m_{k,i} = -(b_k | b_i^*)/\|b_i^*\|^2$.

# La réduction faible

**Définition .** *Une base $(b_i)$ d'un réseau $L$ est dite* faiblement réduite *(ou* propre*) si les coefficients $m_{i,j}$ du procédé de Gram-Schmidt vérifient*

$$|m_{i,j}| \leq \frac{1}{2}.$$

Une base quelconque peut aisément être rendue propre, en faisant :

Pour $k$ de $2$ à $n$ faire
  Pour $j$ de $k-1$ à $1$ faire
    $b_k \leftarrow b_k - \lfloor (b_k | b_j^*)/\|b_j^*\|^2 \rceil b_j$

**Remarque .** *$L$ et $(b_i^*)$ sont inchangés.*

# L'algorithme de Lenstra-Lenstra-Lovász

**Définition .** *Soit $\delta \in ]1/4, 1]$. Une base $(b_1, \ldots, b_d)$ de $L$ est dite LLL-réduite à un facteur $\delta$ si*

1. *elle est faiblement réduite ;*
2. *pour tout $1 < i \leq d$, $||b^*_{i+1} + m_{i+1,i} b^*_i||^2 \geq \delta ||b^*_i||^2$ (condition de Lovász).*

**Remarque .** *Initialement, $\delta = 3/4$.*

2. $\Leftrightarrow ||b^*_{i+1}||^2 \geq (\delta - m^2_{i+1,i}) ||b^*_i||^2$.

**Théorème .** *Soit $\delta \in ]1/4, 1]$, on pose $\alpha = 1/(\delta - 1/4)$. Soit $(b_1, \ldots, b_d)$ une base LLL-réduite à un facteur $\delta$ de $L$. Alors*

1. $||b_1|| \leq \alpha^{(d-1)/4} (\det L)^{1/d}$ ;
2. *Pour tout* $1 \leq i \leq d$, $||b_i|| \leq \alpha^{(d-1)/2} \lambda_i(L)$ ;
3. $\det L \leq ||b_1|| \cdots ||b_n|| \leq \alpha^{d(d-1)/4} \det L$.

LLL : **Entrée** : une base $(b_1, \ldots, b_d)$ d'un réseau $L$.

**Sortie** : La base $(b_1, \ldots, b_d)$ est LLL-réduite à un facteur $\delta$.

On suppose $(b_1, \ldots, b_k)$ LLL-réduite. On modifie $b_{k+1}$ pour que $(b_1, \ldots, b_k, b_{k+1})$ soit faiblement réduite.

Si $||b^*_{k+1}||^2 \geq (\delta - m^2_{k+1,k})||b^*_k||^2$ (condition de Lovász), on incrémente $k$.

Sinon, échange de $b_k$ et $b_{k+1}$, on décrémente $k$.

**Théorème .** *Soit $L$ un réseau de rang $d$. Si $\delta \in ]1/4, 1[$, LLL termine en au plus $O(d^6 \ln^3 B)$ opérations avec $B \geq ||b_i||^2$ pour tout $i$.*

Preuve : Soient $L_j = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_j$, $e_j =$ disc $L_j = \det((b_r|b_s)_{1\leq r,\, s\leq j})$, on pose

$$D := \prod_{j=1}^{d-1} e_j^2 = \prod_{j=1}^{d-1} \prod_{k=1}^{j} ||b_k^*||^2.$$

On a $D \leq B^{d(d-1)}$.

Test de Lovász : $||b_{i+1}^* + m_{i+1,i} b_i^*||^2 \geq \delta ||b_i^*||^2$.

Si vérifié, $D$ inchangé.

Sinon, échange de $b_i$ et $b_{i+1}$ :

- $b_i^*$ remplacé par $c_i^* = b_{i+1}^* + m_{i+1,i} b_i^*$
- $b_{i+1}^*$ remplacé par $c_{i+1}^* = b_i^* - m_{i+1,i} \dfrac{||b_i^*||^2}{||b_{i+1}^* + m_{i+1,i} b_i^*||^2} (b_{i+1}^* + m_{i+1,i} b_i^*)$.

$$D := \prod_{j=1}^{d-1} e_j^2 = \prod_{j=1}^{d-1} \prod_{k=1}^{j} ||b_k^*||^2.$$

Or, $||c_i^*||^2 = ||b_{i+1}^* + m_{i+1,i} b_i^*||^2 < \delta ||b_i^*||^2 \Rightarrow e_i^2$ remplacé par $e_i'^2 < \delta e_i^2$ et $d_j$ inchangé pour $i \neq j \Rightarrow D$ remplacée par $\delta D$.

$e_j$ inchangé pour $j \leq i-1$ : ok.

$e_j$ inchangé pour $j \geq i+1$ : calcul donne $||c_i^*||^2 ||c_{i+1}^*||^2 = ||b_i^*||^2 ||b_{i+1}^*||^2$.

Or, pour tout $i = 1, \ldots, d-1$, on a

$$e_i \geq \lambda_1(L)^{2i} \gamma_d^{-d}.$$

Preuve : Exercice 9, section 3.3.4. du vol. 2 de "The Art of Computer Programming" de D. Knuth.

$\Rightarrow D$ est minorée par une constante $K$ !

$\Rightarrow$ nombre fini de retours en arrière : $\frac{d(d-1)}{2}\log_t M - \frac{\log_t K}{2}$.

Nombre total d'étapes : $\frac{d(d-1)}{2}\log_t M - \frac{\log_t K}{2} + d - 1$. $\square$

**Remarques .**

- *LLL approche SVP à un facteur* $2^{\frac{d-1}{2}}$.
- *En pratique, la base renvoyée est de bien meilleure qualité et plus vite qu'attendu.*

# Variantes

- LLL entier : de Weger ;
- Versions flottantes : Schnorr, Schnorr et Euchner ;
- LLL sur des vecteurs non nécessairement linéairement indépendants.

# Algorithmes de Schnorr

LLL approche SVP à un facteur $2^{\frac{d-1}{2}}$.

Schnorr améliore le facteur : $2^{O(d(\log\log d)^2/\log d)}$.

Il définit une famille d'algos polynomiaux BKZ (blockwise Korkine Zolotarev). Variantes de BKZ : meilleurs algos de réduction en pratique.

En cryptanalyse, nécessité d'obtenir des bases de très bonnes qualité pour des réseaux de dimension jusqu'à plusieurs centaines.

Utilisation des algorithmes de Schnorr implantés dans bibliothèque NTL de V. Shoup publique, robuste et efficace.

Travaux récents de Koy et Schnorr, Schnorr.

# Algorithme de Kannan

SVP super exponentiel.

Soit $(b_1, \ldots, b_n)$ une base LLL-réduite d'un réseau $L$.

Soit $x = x_1 b_1 + \cdots + x_n b_n$, avec $x_i \in \mathbb{Z}$ et $x_n \in \mathbb{N}$, un plus court vecteur de $L$.

On a

$$x = \sum_{i=1}^{n} x_i b_i = \sum_{i=1}^{n} x_i \left( b_i^* + \sum_{j=1}^{i-1} m_{i,j} b_j^* \right) = \sum_{j=1}^{n} \left( x_j + \sum_{i=j+1}^{n} m_{i,j} x_i \right) b_j^*.$$

Comme $i \neq j \Rightarrow (b_i^* | b_j^*) = 0$, on a

$$||x||^2 = \sum_{j=1}^{n} \left( x_j + \sum_{i=j+1}^{n} m_{i,j} x_i \right)^2 ||b_j^*||^2.$$

$$||x||^2 = \sum_{j=1}^{n} \left( x_j + \sum_{i=j+1}^{n} m_{i,j} x_i \right)^2 ||b_j^*||^2.$$

$x$ plus court que $b_1$ d'où $0 \leq x_n < \dfrac{||b_1||}{||b_n^*||}$ et

$$\left( x_j + \sum_{i=j+1}^{n} m_{i,j} x_i \right)^2 ||b_j^*||^2 < ||b_1||^2 - \sum_{k=j+1}^{n} \left( x_j + \sum_{i=k+1}^{n} m_{i,k} x_i \right)^2 ||b_k^*||^2.$$

Recherche exhaustive. En théorie, au plus $n^{n/2+o(n)}$ possibilités.

# Applications de LLL

- Recherche de relations linéaires homogènes $\Rightarrow$ Polynôme minimal d'un nombre algébrique.
  $x = \sqrt{2} + \sqrt{3} \approx 3.1462...$. Théorie : $x$ est de degré $4$. On considère le réseau de $\mathbb{R}^5$ :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ [Cx^4] & [Cx^3] & [Cx^2] & [Cx] & C \end{pmatrix}$$

  avec $C$ un grand entier. Un vecteur du réseau est de la forme ${}^t(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_1[Cx^4] + \lambda_2[Cx^3] + \lambda_3[Cx^2] + \lambda_4[Cx] + C)$. Dernière coordonnée très proche de $C(\sum \lambda_i x^i)$.

- Recherche de relations linéaires simultanées.
- Recherche de relations linéaires inhomogènes.

# Factorisation de polynômes

Factorisations de polynômes multivariés (corps de base : $\mathbb{Q}$, corps fini, corps de nombres). Objet initial de LLL.

Cas d'une variable : $f \in \mathbb{Q}[X] \Rightarrow f \in \mathbb{Z}[X]$.

Trois algos : Berlekamp-Zassenhaus, LLL, Van Hoeij.

L'idée : prendre $p$ premier petit ne div. pas Rés$(f, f')$. On factorise $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[X]$.

Berlekamp : polynomial déterministe donnant $\bar{f} = f_1 \dots f_n$ avec $f_i \in \mathbb{Z}/p\mathbb{Z}[X]$

Hensel : $\bar{f} = f_1 \dots f_n$ avec $f_i \in \mathbb{Z}_p[X]$

Problème : retrouver les facteurs de $f$.

BZ : exponentiel en $n$.

LLL original : polynomial déterministe.

Van Hoeij : utilise LLL (vraiment efficace).

Berlekamp : polynomial déterministe donnant $\overline{f} = \overline{f_1} \dots \overline{f_n}$ avec $\overline{f_i} \in \mathbb{Z}/p\mathbb{Z}[X]$

LLL : on a un facteur $f_1 \in \mathbb{Z}[X]$ de degré $m$ t.q.
- $f_1 \bmod p$ irréductible dans $\mathbb{F}_p[X]$.
- $f_1 \bmod p$ divise $f \bmod p$ dans $\mathbb{F}_p[X]$.

Hensel : pour tout $l$, $f_1 \bmod p$ se relève en $f_1 \bmod p^l$.

Soit

$$L_l = \{\varphi \in \mathbb{Z}[X] \text{ de degré } q : \varphi = p^l b + a f_1 \text{ avec } a,\, b \in \mathbb{Z}[X]\}.$$

$L_l$ est un réseau admettant pour base

$$(p^l,\, p^l X,\, p^l X^2, \dots,\, p^l X^{m-1},\, f_1,\, f_1 X,\, f_1 X^2, \dots,\, f_1 X^{q-m}).$$

Vecteur court : donne $h \in \mathbb{Z}[X]$ t. q.
- $h$ facteur irréductible de $f$ dans $\mathbb{Z}[X]$.
- $h \bmod p^l$ multiple de $f_1 \bmod p^l$.

# Méthode de van Hoeij

Soit $f = \prod_{i=1}^{s} f_i$ avec $f_i \in \mathbb{Z}_p$, soient $v_1, v_2, \ldots, v_k \in \{0,1\}^s$ t. q. $\prod_{i=1}^{s} f_i^{v_{ji}}$ : facteurs de $f$ dans $\mathbb{Z}[x]$.

Remarque de van Hoeij : L'ensemble des vecteurs $w$ de $\mathbb{Z}^s$ t. q. $\prod_{i=1}^{s} f_i^{w_i} \in \mathbb{Q}(x)$ est un sous-réseau $L_f$ de $\mathbb{Z}^s$, engendré par les vecteurs $v_1, \ldots, v_k$.

# Conjecture de Mertens

Mise en défaut de la conjecture de Mertens.

Soit $M(x) = \sum_{n \leq x} \mu(n)$. Stieltjes affirme à Hermite (1885) que $M(x) = O(x^{1/2})$ ($\Rightarrow$ H. R.) et que probablement $|M(x)x^{-1/2}| \leq 1$. Conjecture (Mertens) : $|M(x)x^{-1/2}| < 1$ pour $x > 1$.

Non : Odlyzko et te Riele (1985) obtiennent grâce à LLL

$\limsup M(x)x^{-1/2} > 1.06$ et $\liminf M(x)x^{-1/2} < -1.009$.

# Cryptologie

Parmi de nombreuses applications :

- Cryptanalyse de protocoles à base de sac à dos.
- Attaque du générateur linéaire congruentiel.
- LLL intervient dans la dernière étape du crible algébrique.

# Recherche de petites racines modulo $N$

Travaux de Vallée, Girault, Toffin. Travaux de Coppersmith et Howgrave-Graham.

Soit $P \in \mathbb{Z}[X]$ unitaire, $N \in \mathbb{N}$, on recherche les $x_0$ entiers "petits" tels que $P(x_0) = 0 \bmod N$.

Procédé utilisant LLL répond efficacement quand $|x_0| < N^{1/\deg P}$.

Conséquences :

– Factorisation de nombres $N$ de la forme $p^r q$ : Travail de Boneh, Durfee et Howgrave-Graham.

Factorisation de $N$ en temps polynomial si $r \sim \log p$.

Factorisation de $N$ + rapide que par ECM si $r \sim \sqrt{\log p}$.

# Attaque de RSA avec petit exposant de déchiffrement

**Rappel** : Soient $p$ et $q$ premiers, on note $N = pq$.

Choix de $e$ premier avec $\phi(N) = (p-1)(q-1)$ et de $d$ t.q. $ed = 1 \bmod \phi(N)$.

Chiffrement : $x = m^e \bmod N$.

Déchiffrement : calcul de $x^d \bmod N = m \bmod N$.

$N$ et $e$ publics, $d, p, q$ secrets.

Exponentiation modulaire très coûteuse $\Rightarrow$ intérêt à prendre $d$ petit.

Boneh-Durfee : $d$ ne doit pas être pris trop petit.

**Conjecture .** *On peut retrouver facilement $d$ si $d < N^{0.5}$.*

Wiener (1990) : vrai si $d < N^{0.25}$.

Boneh et Durfee (1999) : vrai si $d < N^{0.292}$.

Verheul et Tilborg (1997) : on retrouve $d$ plus vite que par recherche exhaustive si $d < N^{0.5}$.

Soient $s = -(p+q)/2$ et $A = (N+1)/2$, il existe $k$ t. q.

$$k(A+s) = 1 \bmod e :$$

$A$ et $e$ sont connus, $k$ et $s$ sont inconnus. Hypothèse : $e$ de l'ordre de grandeur de $N$.

On pose $f(x,y) = x(A+y) - 1$. On cherche $(x_0, y_0)$ tel que $f(x_0, y_0) = 0 \bmod e$ avec $|x_0| \leq e^{\delta}$, $|y_0| < e^{0.5}$.

On pose $f(x,y) = x(A+y) - 1$. On cherche $(x_0, y_0)$ tel que $f(x_0, y_0) = 0 \bmod e$ avec $|x_0| \leq e^{\delta}$, $|y_0| < e^{0.5}$.

Version bivariée de la méthode de Coppersmith.

Soit $h(x,y) = \sum_{i,j} a_{i,j} x^i y^j$, on pose $||h(x,y)||^2 = \sum_{i,j} |a_{i,j}|^2$.

**Lemme .** *Soit $h(x,y) \in \mathbb{Z}[x,y]$, somme d'au plus $w$ monômes, tel que*

1. $h(x_0, y_0) = 0 \bmod e^m$ *pour un entier* $m$ *avec* $|x_0| < X$, $|y_0| < Y$ ;
2. $||h(xX, yY)|| < e^m/\sqrt{w}$ ;

*alors* $h(x_0, y_0) = 0$.

LLL donne $P_1$ et $P_2 \in \mathbb{Z}[x,y]$ t. q. $P_1(x_0, y_0) = 0$ et $P_2(x_0, y_0) = 0$ dans $\mathbb{Z}$.

Soit $R(y) = \text{Rés}_x(P_1, P_2)$, **heuristique** : $R \neq 0$.

$y_0 \in \mathbb{Z}$ racine de $R$ : détermination facile. Comme $y_0 = \frac{p+q}{2}$, on a $p$ et $q$.

On pose $f(x,y) = x(A+y) - 1$. On cherche $(x_0, y_0)$ tel que $f(x_0, y_0) = 0 \bmod e$ avec $|x_0| \leq e^{\delta}$, $|y_0| < e^{0.5}$.

Idée : construire à partir de $f$ un réseau $L$ engendré par des polynômes (vus comme des vecteurs de coordonnées les coefficients des polynômes dans une base formée des monômes impliqués).

Trouver des polynômes avec norme petite $=$ trouver des vecteurs courts de ce réseau.

**Rappel :** Soit $(b_1, \ldots, b_d)$ une base LLL-réduite de $L$ alors

$$||b_1|| \leq 2^{d/2}(\det L)^{1/d} \quad \text{et} \quad ||b_2|| \leq 2^{d/2}(\det L)^{\frac{1}{d-1}}.$$

Soient $g_{i,k} = x^i f^k(x,y) e^{m-k}$ et $h_{j,k} = y^j f^k(x,y) e^{m-k}$ avec $m$ entier.

$(x_0, y_0)$ est racine des $g_{i,k}$ et $h_{j,k}$ modulo $e^m$ pour $k = 0, \ldots, m$.

On considère le réseau engendré par les polynômes $g_{i,k}(xX, yY)$ et $h_{j,k}(xX, yY)$ (vus comme des vecteurs de coordonnées les coefficients des polynômes).

$f(x,y) = x(A+y) - 1$.

Exemple : réseau engendré par $g_{i,k} = x^i f^k(x,y) e^{m-k}$ et $h_{j,k} = y^j f^k(x,y) e^{m-k}$ pour $m = 3$, $k = 0, \ldots, 3$, $i = 0, \ldots, 3-k$ et $j = 0, 1$.

| | $e^3$ | $xe^3$ | $fe^2$ | $x^2e^3$ | $xfe^2$ | $f^2e$ | $x^3e^3$ | $x^2fe^2$ | $xf^2e$ | $f^3$ | $ye^3$ | $yfe^2$ | $yf^2e$ | $yf^3$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $1$ | $e^3$ | | $-$ | | | $-$ | | | | $-$ | | | | |
| $x$ | $0$ | $e^3X$ | $-$ | | $-$ | $-$ | | $-$ | $-$ | | | | | |
| $xy$ | $\vdots$ | $\ddots$ | $e^2XY$ | | | $-$ | | | | $-$ | | $-$ | $-$ | $-$ |
| $x^2$ | $\vdots$ | | $\ddots$ | $e^3X^2$ | $-$ | $-$ | | $-$ | $-$ | $-$ | | | | |
| $x^2y$ | $\vdots$ | | | $\ddots$ | $e^2X^2Y$ | $-$ | | | $-$ | $-$ | | | $-$ | |
| $x^2y^2$ | $\vdots$ | | | | $\ddots$ | $eX^2Y^2$ | | | | $-$ | | | $-$ | $-$ |
| $x^3$ | $\vdots$ | | | | | $\ddots$ | $e^3X^3$ | $-$ | $-$ | $-$ | | | | |
| $x^3y$ | $\vdots$ | | | | | | $\ddots$ | $e^2X^3Y$ | $-$ | $-$ | | | | $-$ |
| $x^3y^2$ | $\vdots$ | | | | | | | $\ddots$ | $eX^3Y^2$ | $-$ | | | | $-$ |
| $x^3y^3$ | $\vdots$ | | | | | | | | $\ddots$ | $X^3Y^3$ | | | | $-$ |
| $y$ | $\vdots$ | | | | | | | | | $\ddots$ | $e^3Y$ | $-$ | $-$ | $-$ |
| $xy^2$ | $\vdots$ | | | | | | | | | | $\ddots$ | $e^2XY^2$ | $-$ | $-$ |
| $x^2y^3$ | $\vdots$ | | | | | | | | | | | $\ddots$ | $eX^2Y^3$ | $-$ |
| $x^3y^4$ | $0$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $0$ | $X^3Y^4$ |

LLL donne deux vecteurs courts $P_1$ et $P_2$ de ce réseau : on aura $P_1(x_0, y_0) = 0$ et $P_2(x_0, y_0) = 0$ dans $\mathbb{Z}$.

**Rappel :** Soit $(b_1, \ldots, b_d)$ une base LLL-réduite de $L$ alors

$$||b_1|| \leq 2^{d/2}(\det L)^{1/d} \quad \text{et} \quad ||b_2|| \leq 2^{d/2}(\det L)^{\frac{1}{d-1}}.$$

Matrice triangulaire : RSA cassé dès lors que $d \leq N^{7/6-\sqrt{7}/3}$ avec $7/6 - \sqrt{7}/3 = 0.2847...$

Raffinement du choix de la famille de polynômes permet de casser RSA dès lors que $d \leq N^{1-1/\sqrt{2}}$ avec $1 - 1/\sqrt{2} = 0.29289....$

# Références

*Factoring Polynomials with Rational Coefficients*, A. K. Lenstra, H. W. Lenstra and L. Lovász, Math. Annalen **261**, 515-534, 1982.

*La réduction de réseaux en cryptographie*, A. Joux, Thèse de doctorat, 1993.

*La géométrie des nombres en cryptologie*, Phong Quang Nguyen, Thèse de doctorat, Université Paris 7, 1999.

*La réduction des réseaux. Autour de l'algorithme de Lenstra, Lenstra, Lovász*, B. Vallée, Informatique théorique et Applications, 1989.

*A Course in Computational Algebraic Number Theory*, H. Cohen, GTM **138**, Springer-Verlag, 1996.

*Réduction des réseaux et applications*, G. Hanrot, exposé disponible sur la page `http ://www-igm.univ-mlv.fr/~ejc2003/programme.html`

*Les réseaux parfaits des espaces euclidiens*, J. Martinet, Masson, 1996.