Réseaux euclidiens et applications

Question 1 : On considère le réseau engendré par les lignes de :

$$B = \begin{pmatrix} 11 & 1 & & \\ 19 & & 1 & \\ 29 & & & 1 \end{pmatrix}$$

Trouver un vecteur court (de norme 2) dans ce réseau.

Question 2 : On considère le réseau engendré par les lignes de :

$$B = \begin{pmatrix} 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 \\ & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \\ & & 5 & 10 & 15 & 20 & 25 & 30 & 35 \\ & & & 7 & 14 & 21 & 28 & 35 & 42 \\ & & & & 11 & 22 & 33 & 44 & 55 \\ & & & & & 13 & 26 & 39 & 52 \\ & & & & & & 17 & 34 & 51 \\ & & & & & & & 19 & 38 \\ & & & & & & & & 23 \end{pmatrix}$$

Quel est son volume ? Que peut-on en déduire sur la norme de son vecteur le plus court ? Essayer d'exhiber un vecteur à petits coefficients dans le réseau (indice : il faut se concentrer sur les premières lignes).

Question 3 : Quel est le volume du réseau engendré par

$$B = \begin{pmatrix} 1 & & a \\ & 1 & b \end{pmatrix}$$

Proposez une généralisation en taille n.

Équations diophantiennes linéaires

En cours, on a affirmé qu'on pouvait ramener la résolution de problèmes linéaires sur les entiers du type :

$$\begin{cases} a_1 x_1 + \cdots + a_n x_n = 0 \mod p \\ |x_i| \leq B_i \\ (x_1, \ldots, x_n) \neq (0, \ldots, 0) \end{cases}$$

au calcul d'un vecteur court dans un réseau euclidien.

Question 4 : Montrer qu'on peut, sans perte de généralité, supposer que $a_n = 1$.

Question 5 : En supposant que $a_n = 1$, donner la base d'un réseau (de rang plein) de dimension n dont les points sont exactement les solutions de l'équation ci-dessus.

Question 6 : Modifier cette base pour qu'une solution de l'équation corresponde à un point du réseau modifié dont toutes les coordonnées sont à peu près de l'ordre de $B_1 \times \cdots \times B_n$.

Question 7 : Supposons que $n^{n/2} p \leq m$. La borne de Minkowksi garantit l'existence d'un vecteur « court » dans le réseau. Démontrez que ceci garantit l'existence d'une solution.

Applications (non-crypto) « amusantes »

Question 8 : Soit p un nombre premier. On considère un entier $0 < a < p$. Démontrer qu'il existe deux entiers x, y tels que $a \equiv x/y \bmod p$ (p un nombre premier) avec $x, y \approx \sqrt{p}$.

Version effective d'un résultat de Fermat

Soit p un nombre premier tel que $p \equiv 1 \bmod 4$. Pierre de Fermat a démontré au 17ème siècle que p peut s'écrire comme une somme de deux carrés.

Défi : trouver a, b tels que $10^{400} + 69 = a^2 + b^2$.

Question 9 : Montrer que, comme $p \equiv 1 \bmod 4$, il existe α tel que $-1 \equiv \alpha^2 \bmod p$ (-1 est un carré modulo p !).

Question 10 : Montrer que si $p = a^2 + b^2$, alors le couple (a, b) qu'on cherche appartient au réseau engendré par les lignes de On trouve donc que (a, b) appartient au réseau $\mathcal{L}$ engendré par les lignes de :

$$B = \begin{pmatrix} \alpha & 1 \\ p & 0 \end{pmatrix}$$

Question 11 : En déduire un algorithme (efficace) qui permet d'écrire p comme une somme de deux carrés.

Défi : trouver a, b tels que $10^{400} + 69 = a^2 + b^2$.

Autour de RSA et de l'attaque de Wiener

On part d'une paire de clefs RSA, c'est-à-dire de e, d et $N = pq$ tels que $ed \equiv 1 \bmod \phi(N)$, où $\phi(N) = (p-1)(q-1)$. On sait donc que $\phi(N) = N - t$ avec $t \approx 2\sqrt{N}$.

Question 12 : Pour empêcher l'attaque de Wiener, on peut remplacer e par $e' := e + x\phi(N)$ — cela ne change pas le fait que $e'd \equiv 1 \bmod \phi(N)$, donc élever puissance e' et d sont bien des opérations réciproques. Quelle taille de x garantit que l'attaque de Wiener ne marchera pas ?

Pour simplifier, on peut imposer que $x \leq N^\beta$.