Réseaux et aires
Parimaths - Niveau débutant

Diego Izquierdo

6 décembre 2014

Plaçons-nous dans le plan V, muni d'un système de coordonnées, de telle sorte que V est identifié à $\mathbb{R}^2$ l'ensemble des couples de nombres réels. On note O l'origine. Dans V, on appelle R le réseau des points réticulaires, c'est-à-dire l'ensemble des points à coordonnées entières.

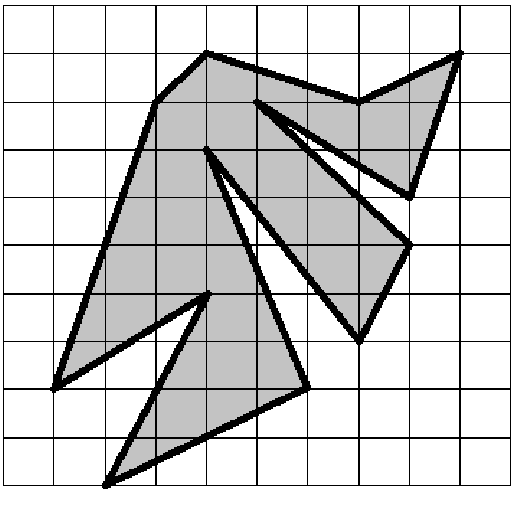
But de la séance : étant donnée une partie X du plan V, établir des liens entre l'aire de X et le nombre de points de R contenus dans X.

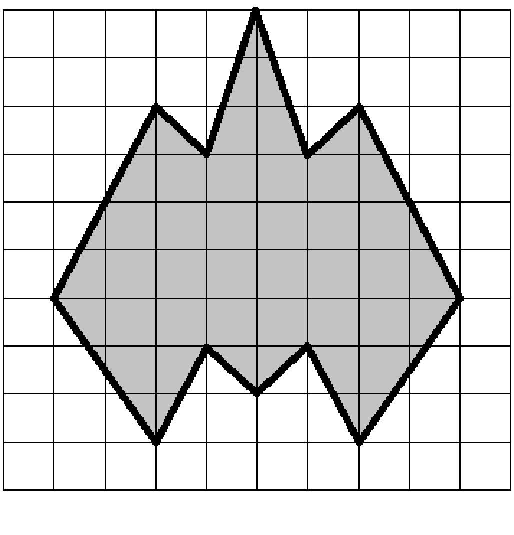
0. (a) Soit N un entier naturel. Existe-t'il un réel positif S tel que toute partie X de V d'aire supérieure S contient au moins N points de R ?
(b) Soit S un réel positif. Existe-t'il un entier naturel N tel que toute partie X de V contenant au moins N points de R est d'aire supérieure à S ?

1 Le cas où X est un polygone : la formule de Pick

Soit X un polygone (plein) non croisé dont les sommets sont des points du réseau R. Soit $I(X)$ (resp. $F(X)$) le nombre de points de R à l'intérieur de X (resp. sur la frontière de X). Dans cette partie, nous allons exprimer l'aire $\mathcal{A}(X)$ de X en fonction de $I(X)$ et $F(X)$.

1. En faisant appel à des exemples bien choisis, conjecturer une expression de $\mathcal{A}(X)$ en fonction de $I(X)$ et $F(X)$. Vérifier la conjecture sur les deux polygones suivants :





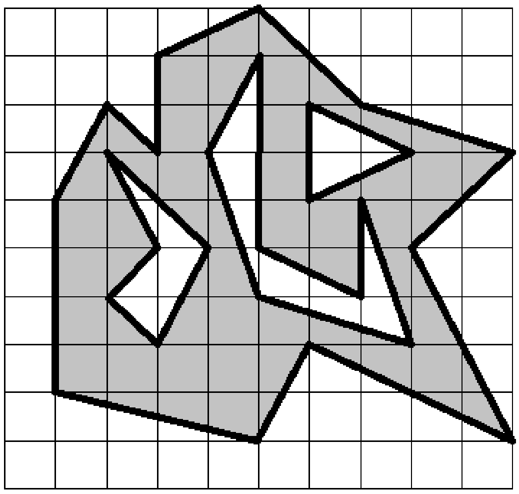
2. Montrer la formule pour les rectangles dont les côtés sont parallèles aux axes de coordonnées.

3. Montrer la formule pour les triangles rectangles dont les côtés de l'hypothénuse sont parallèles aux axes de coordonnées.

4. Montrer la formule pour les triangles.

5. En déduire la formule en toute généralité.

6. Comment modifier la formule dans le cas où X est un polygone "à g trous" ? Voici un exemple de polygone à 3 trous :



2 Le cas où X est un disque

Soit X le disque de centre O et de rayon r. Soit $N(r)$ le nombre de points de R qui sont à l'intérieur ou sur la frontière de X.

1. Calculer $N(5)$.

2. Donner sans preuve une estimation de $N(r)$ quand r est très grand.

3. Montrer que, pour tout réel positif r, on a : $\pi\left(r-\sqrt{2}\right)^2 \leq N(r) \leq \pi\left(r+\sqrt{2}\right)^2$. Cet encadrement confirme-t'il l'estimation précédente ?

4. En déduire que : $\left(\sqrt{N(r)}-\sqrt{2\pi}\right)^2 \leq \mathcal{A}(X) \leq \left(\sqrt{N(r)}+\sqrt{2\pi}\right)^2$.

5. *(Une application arithmétique)* Pour tout entier naturel n, on note $T(n)$ le nombre d'entiers naturels $m \leq n$ tels que l'équation $x^2+y^2=m$ n'a pas de solutions entières. Déduire des questions précédentes que pour tout $n>0$, on a $T(n)>\frac{n}{5}$.

3 Le cas où X est convexe : la théorie de Minkowski

Soient X une partie de V d'aire $\mathcal{A}(X)$. Le but de cette partie est d'établir le **théorème de Minkowski**, qui affirme que, *sous de bonnes hypothèses*, si $\mathcal{A}(X)$ est assez grande, alors X contient des points de R. Pour ce faire, il est utile d'introduire quelques notations : étant donnés $A(a_1, a_2)$ et $B(b_1, b_2)$ deux points de V, on note $A + B$ le point de coordonnées $(a_1 + b_1, a_2 + b_2)$, $-A$ le point de coordonnées $(-a_1, -a_2)$ et, pour s un réel, sA le point de coordonnées (sa_1, sa_2).

1. Dans le cas où $A(1, 2)$ et $B(3, -3)$, dessiner $C = A + B$, $D = -A$, $E = A + (-B)$ et $F = (2A) - (\frac{1}{3}B)$.

2. *(Lemme de Blichtfeld)* Montrer que, si $\mathcal{A}(X) > 1$, alors il existe deux points distincts C et D de X tels que $C + (-D) \in R$.

3. *(Théorème de Minkowski)* Supposons que X soit convexe (c'est-à-dire que si deux points sont dans X, alors le segment qu'ils définissent est entièrement contenu dans X) et symétrique par rapport à l'origine. Montrer que, si $\mathcal{A}(X) > 4$, alors X contient un point de R différent de l'origine. Pourrait-on remplacer 4 par une constante plus petite dans l'inégalité $\mathcal{A}(X) > 4$?

4 Généralisation aux réseaux quelconques

Considérons $A(a_1, a_2)$ et $B(b_1, b_2)$ deux points de V.

1. Montrer que l'aire du triangle OAB est $\frac{1}{2}|a_1b_2 - a_2b_1|$.

Supposons maintenant que O, A, B ne sont pas alignés. On rappelle qu'un tel triplet de points permet de définir un repère (O, A, B), c'est-à-dire que chaque point de V s'écrit de manière unique sous la forme $sA + tB$ avec s et t réels. On appelle **réseau de V engendré par A et B** l'ensemble des points C tels qu'il existe deux entiers m et n tels que $C = mA + nB$, et on le note $R(A, B)$. On appelle **maille élémentaire de $R(A, B)$** l'ensemble des points C tels qu'il existe des nombres réels s et t dans $[0, 1[$ vérifiant $C = sA+tB$. Son aire est appelée **covolume de $R(A, B)$**.

2. Reconnaître le réseau engendré par $A(1, 0)$ et $B(0, 1)$. Dessiner sa maille élémentaire. Que vaut le covolume ?

3. Dessiner le réseau engendré par $A(2, -1)$ et $B(3, 1)$, ainsi que sa maille élémentaire. Montrer que $R(A, B)$ est constitué des points (x, y) tels que x et y sont entiers et $x \equiv 3y \mod 5$. Calculer le covolume.

4. Soient m un entier relatif et n un entier naturel. Trouver deux points A et B tels que l'ensemble des points de coordonnées entières (x, y) vérifiant $x \equiv my \mod n$ soit le réseau engendré par A et B. Quel est le covolume de $R(A, B)$?

5. Comment modifier les résultats des trois premières sections si l'on remplace R par un réseau quelconque ?

6. Que dire des réseaux engendrés par les points suivants ?
(i) $A_1(1,0)$ et $B_1(0,1)$.
(ii) $A_2(1,1)$ et $B_2(0,1)$.
(iii) $A_3(1,1)$ et $B_3(1,2)$.
(iv) $A_4(2013,-2012)$ et $B_4(-2014,2013)$.
Et que dire de leurs covolumes ? Émettez une conjecture. Donnez-en trois preuves à l'aide de la question 5.

5 Retour au théorème de Minkowski pour un réseau quelconque

La théorie de Minkowski (section 3) pour un réseau quelconque (section 4) a d'importantes applications en arithmétique, comme le **théorème des quatre carrés**, qui affirme que tout entier naturel est somme de quatre carrés, ou l'étude des solutions entières de l'équation $x^2 - dy^2 = 1$ dite de **Pell-Fermat**. Voici une application plus accessible :

Application. Soit p un nombre premier congru à 1 modulo 4. On admet qu'il existe un entier x tel que $x^2 \equiv 1 \mod p$. Montrer que p est somme de deux carrés.

——————————————FIN——————————————