Quelques problèmes classiques d'arithmétique II
Parimaths - Niveau avancé

Diego Izquierdo

8 mars 2014

Cette séance est la suite de celle du 2 novembre 2013. Il n'est pas nécessaire d'avoir été présent le 2 novembre pour suivre la séance d'aujourd'hui : tous les résultats utiles sont rappelés dans la partie 2.1.

1 La théorie de Minkowski

0. *(Question préliminaire)* Soient $A(a_1, a_2)$ et $B(b_1, b_2)$ deux points du plan. Soit C le point de coordonnées $(a_1 + b_1, a_2 + b_2)$. Montrer que l'aire du parallélogramme $OACB$ est $|a_1b_2 - a_2b_1|$.

1.1 Réseaux

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. Considérons $A(a_1, a_2)$ 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). 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 $R(A, B)$**.

1. Dessiner le réseau engendré par $A(1, 0)$ et $B(0, 1)$ ainsi que sa maille élémentaire. Comment caractériser les points appartenant à ce réseau ? Et que vaut le covolume ?

2. 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.

3. 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 $R(A, B)$?

4. 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.

1.2 Le théorème de Minkowski

Soient X une partie de V d'aire $\mathcal{A}(X)$ et $R = R(A, B)$ un réseau de V de covolume $\text{Covol}(R)$. 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.

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

2. *(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 $\mathcal{A}(X) > 4\text{Covol}(R)$, alors X contient un point de R différent de l'origine. Pourrait-on remplacer 4 par une constante plus petite dans l'inégalité $\mathcal{A}(X) > 4\text{Covol}(R)$?

3. (a) Montrer que, si $R(A, B) = R(C, D)$, alors les covolumes de $R(A, B)$ et $R(C, D)$ sont égaux. Par conséquent, le covolume ne dépend que de l'ensemble $R(A, B)$ et non des points A et B.
(b) Deux réseaux ayant même covolume sont-ils forcément égaux ?

4. (a) Si R est un réseau, montrer qu'une partie bornée du plan (c'est-à-dire une partie contenue dans un disque) ne peut contenir qu'un nombre fini de points de R.
(b) Montrer que tout réseau R contient un point C différent de l'origine tel que la longueur OC est majorée par $2\sqrt{\frac{\text{Covol}(R)}{\pi}}$.
(c) Montrer que tout réseau R contient un point D différent de l'origine tel que l'abscisse et l'ordonnée de D sont majorées en valeur absolue par $\sqrt{\text{Covol}(R)}$.
(d) Montrer que tout réseau R contient un point $E(e_1, e_2)$ différent de l'origine tel que $|e_1| + |e_2| \leq \sqrt{2\text{Covol}(R)}$.

2 Applications

2.1 Rappels : La loi de réciprocité quadratique

La séance du 2 novembre a été consacrée à l'étude des résidus quadratiques modulo un nombre premier et à la preuve de la loi de réciprocité quadratique. Nous rappelons ici les résultats que nous avons prouvés. Ils pourront être librement utilisés dans la suite.

Considérons a un entier relatif et m un entier naturel supérieur ou égal à 2. On dit que a est un **résidu quadratique** modulo m s'il existe un entier x tel que $x^2 \equiv a \mod m$. Lors de la séance du 2 novembre, on a montré que, si $m = p_1^{\alpha_1}...p_r^{\alpha_r}$ est la décomposition de m en produit de facteurs premiers, alors a est un résidu quadratique modulo m si, et seulement si, a est un résidu quadratique modulo $p_i^{\alpha_i}$ pour chaque i. Par contre, on a vu que cela n'équivaut pas à dire que a est un résidu quadratique modulo p_i pour chaque i. Malgré cette observation, il est toujours intéressant de traiter le cas m premier. Dans la suite, on remplace donc l'entier m par un nombre premier p. Dans ce contexte, on définit le **symbole de Legendre** par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p|a \\ 1 & \text{si } p \nmid a \text{ et } a \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } p \nmid a \text{ et } a \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

Pour $p \neq 2$, les propriétés fondamentales que nous avons établies sur le symbole de Legendre sont les suivantes :

- *(Caractère quadratique de -1)* On a $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
- *(Critère d'Euler)* Pour chaque entier a, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.
- *(Multiplicativité)* Pour a et b entiers, on a $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
- *(Caractère quadratique de 2)* On a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
- *(Loi de réciprocité de Gauss)* Si q est un nombre premier impair différent de p, on a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

1. *(Cette question a déjà été traitée le 2 novembre.)* L'entier 814 est-il un résidu quadratique modulo 2011 ?

2.2 Sommes de deux carrés

On cherche à déterminer quels entiers naturels s'écrivent comme somme de deux carrés.

1. Soient a et b deux entiers qui s'écrivent comme somme de deux carrés. Montrer que ab s'écrit aussi comme somme de deux carrés.

2. En utilisant les deux premières parties, montrer qu'un nombre premier impair s'écrit comme somme de deux carrés si, et seulement si, il est congru à 1 modulo 4.

3. En déduire quels sont les entiers naturels qui s'écrivent comme somme de deux carrés.

A l'aide d'une généralisation du théorème de Minkowski, il est possible de montrer par une méthode similaire le **théorème des quatre carrés** : tout entier naturel est somme de quatre carrés parfaits.

2.3 Équations de Pell-Fermat

Soit $d \geq 2$ un entier sans facteurs carrés (c'est-à-dire qu'il n'existe pas de nombre premier p tel $p^2|d$). On cherche à trouver tous les entiers x et y vérifiant l'**équation de Pell-Fermat** :

$$x^2 - dy^2 = 1.$$

2.3.1 Existence de solutions non évidentes

Soit $\mathcal{S}$ l'ensemble des réels de la forme $a+b\sqrt{d}$ avec a et b entiers. Pour $z = a+b\sqrt{d} \in \mathcal{S}$, on note $\overline{z} = a - b\sqrt{d}$ et $N(z) = a^2 - db^2 = z\overline{z}$.

1. Montrer que la fonction $\mathcal{S} \to \mathbb{R}^2, z \mapsto (z, \overline{z})$ est injective. Notons R son image.

2. Montrer que R est un réseau de $\mathbb{R}^2$. Calculer son covolume.

3. Soient $t > 0$ et $r > 0$. Dans $\mathbb{R}^2$, on considère l'ensemble $X_{t,r}$ défini par l'inégalité $t^2x^2 + \frac{y^2}{t^2} \leq r$. Dessiner l'allure de $X_{t,r}$.

4. Montrer que $X_{t,r}$ convexe et symétrique par rapport à l'origine.

5. On admet que l'aire de $X_{t,r}$ est indépendante de t. Calculer cette aire en fonction de r.

6. En utilisant le théorème de Minkowski, montrer qu'il existe un entier M tel que l'équation $N(z) = M$ a une infinité de solutions avec $z \in \mathcal{S}$.

7. En déduire que l'équation de Pell-Fermat possède au moins une solution différente de $(1, 0)$ et de $(-1, 0)$.

2.3.2 Résolution de l'équation

1. Montrer que l'équation de Pell-Fermat admet une solution (x_1, y_1) telle que :
- $x_1 > 0$ et $y_1 > 0$.
- pour toute solution (x, y) de l'équation telle que $x > 0$ et $y > 0$, on a $x_1 + y_1\sqrt{d} \leq x + y\sqrt{d}$.

On note $z_1 = x_1 + y_1\sqrt{d}$.

2. Montrer que, pour tout entier relatif n, si x_n et y_n sont des entiers tels que $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, alors (x_n, y_n) est une solution de l'équation de Pell-Fermat.

3. Montrer que les solutions de l'équation de Pell-Fermat sont exactement les couples (x_n, y_n) et les couples $(-x_n, -y_n)$.

4. Calculer les solutions de l'équation $x^2 - 11y^2 = 1$. Sauriez-vous résoudre l'équation $x^2 - 11y^2 = 5$?

2.4 Théorème de Dirichlet et principe local-global

1. Montrer qu'il existe une infinité de nombres premiers.

2. Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

3. Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Les résultats précédents sont des cas particuliers d'un théorème fondamental en arithmétique, le **théorème de Dirichlet** : si a et b sont deux entiers strictement positifs premiers entre eux, alors la suite arithmétique $x_n = an + b$ contient une infinité de nombres premiers.

4. En admettant le théorème de Dirichlet, montrer qu'un entier naturel a est un carré si, et seulement si, c'est un résidu quadratique modulo p pour tout nombre premier p.

Ce résultat est un cas particulier d'un théorème fondamental en arithmétique, le **théorème de Hasse-Minkowski**. Soit $n > 0$ un entier naturel et donnons-nous un entier a_{ij} pour chaque couple (i, j) d'entiers compris entre 1 et n. Considérons la fonction $f : \mathbb{R}^n \to \mathbb{R}, (x_1, ..., x_n) \mapsto \sum_{i,j} a_{ij} x_i x_j$. Le théorème de Hasse-Minkowski affirme alors que l'équation $f(x_1, ..., x_n) = 0$ admet une solution entière non nulle si, et seulement si, elle admet une solution réelle non nulle et une solution modulo m non nulle pour chaque m.

5. Soient d et N deux entiers non nuls. On suppose que d n'est pas un carré et que, si $N < 0$, alors $d > 0$. En admettant le théorème de Hasse-Minkowski, montrer que si pour chaque entier naturel non nul m la congruence $x^2 - dy^2 \equiv N \mod m$ a une solution, alors l'équation $x^2 - dy^2 = N$ a une solution rationnelle.

——————————————————FIN——————————————————