Quelques problèmes classiques d'arithmétique
Parimaths - Niveau avancé

Diego Izquierdo

2 novembre 2013

Le but de cette séance est de donner des preuves de certains théorèmes classiques d'arithmétique que vous connaissez peut-être déjà.

1 La loi de réciprocité quadratique

1.1 Introduction

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 $x^2 \equiv a \mod m$. Le but de ce problème est de déterminer une méthode assez performante pour savoir si a est un résidu quadratique modulo m. Avant de commencer, on remarquera que, si a et b sont congrus modulo m, alors a est un résidu quadratique modulo m si, et seulement si, b l'est aussi.

1. Quels sont les résidus quadratiques modulo m pour $2 \leq m \leq 8$?

2. On note $m = p_1^{\alpha_1}...p_r^{\alpha_r}$ la décomposition de m en produit de facteurs premiers. Montrer que a est un résidu quadratique modulo m si, et seulement si, a est un résidu quadratique modulo $p_i^{\alpha_i}$ pour chaque i.

3. L'entier 604 est-il un résidu quadratique modulo 840 ? Et l'entier 636 ?

4. Que pensez-vous de l'assertion : "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 pour chaque i".

Malgré la question précédente, 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 :

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

On remarquera immédiatement que, si $a \equiv b \mod p$, alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

5. Calculer $\left(\frac{a}{p}\right)$ pour $p = 2, 3, 5, 8$.

Dans toute la suite, on supposera que $p \neq 2$.

1.2 Caractère quadratique de -1

Dans cette section, on cherche à calculer $\left(\frac{-1}{p}\right)$ en fonction du nombre premier p.

1. Montrer que, si -1 est un résidu quadratique modulo p, alors $p \equiv 1 \mod 4$.

2. (a) Soit $X = \{1, 2, ..., p-1\}$. Pour $x \in X$, rappeler pourquoi il existe un unique $y \in X$ tel que $xy \equiv 1 \mod p$. On note $y = x^{-1}$.
(b) Pour chaque $x \in X$, calculer le cardinal de $\{x, x^{-1}, p-x, p-x^{-1}\}$.
(c) En déduire que, si $p \equiv 1 \mod 4$, alors -1 est un résidu quadratique modulo p.

3. Conclure.

4. Supposons que $p \equiv 1 \mod 4$. Montrer que $x = \left(\frac{p-1}{2}\right)!$ vérifie $x^2 \equiv -1 \mod p$.

1.3 Le critère d'Euler

Dans cette section, on cherche à établir une relation fondamentale vérifiée par le symbole de Legendre : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

1. Montrer que, si $\left(\frac{a}{p}\right) = 1$, alors $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

2. (a) Montrer que, pour tout entier x, $x^{\frac{p-1}{2}}$ est congru à 0, 1 ou -1 modulo p.
(b) Soit P un polynôme à coefficients dans $\mathbb{Z}$ de degré d. Montrer qu'il existe $a_0, ..., a_d \in \mathbb{Z}$ tels que $P(X) = a_0 + a_1(X-1) + a_2\frac{(X-1)(X-2)}{2} + ... + a_d\frac{(X-1)(X-2)...(X-d)}{d!}$.
(c) Soit P un polynôme à coefficients dans $\mathbb{Z}$ tel que, pour tout entier x, p divise $P(x)$ si, et seulement si, p ne divise pas x. Montrer que le degré de P est au moins $p-1$.
(d) En déduire qu'il existe un entier x_0 tel que $x_0^{\frac{p-1}{2}} \equiv -1 \mod p$.
(e) *(Critère d'Euler)* Par un argument combinatoire, utiliser les questions précédentes pour montrer que $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

3. Déduire de ce qui précède que $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. Comment aurait-on pu obtenir cette relation sans utiliser le critère d'Euler ?

4. Déduire que $\left(\frac{2}{p}\right) = 1$ dès que $p \equiv 1 \mod 8$.

1.4 Le caractère quadratique de 2 et la loi de réciprocité de Gauss

Dans cette partie, nous allons d'abord calculer le symbole $\left(\frac{2}{p}\right)$ pour chaque premier p, puis nous allons établir la **loi de réciprocité quadratique**, qui permet de relier les symboles $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$ pour p et q deux nombres premiers impairs distincts.

1. *(Lemme de Gauss)* Supposons que p ne divise pas a. Notons $S = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{2ka}{p}\right]$. Montrer que $\left(\frac{a}{p}\right) = (-1)^S$.

2. *(Caractère quadratique de 2)* Calculer $\left(\frac{2}{p}\right)$ en fonction de p.

3. (a) Soient p et q deux nombres premiers impairs distincts. On note $S(p,q) = \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{pk}{q}\right]$. Calculer $S(p,q) + S(q,p)$ en fonction de p et q.
(b) *(Loi de réciprocité de Gauss)* En déduire la relation :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

1.5 Conclusion

1. À l'aide de tout ce qui précède, donner une méthode "rapide" pour déterminer si un entier a est un résidu quadratique modulo un nombre premier p ou pas.

2. L'entier 814 est-il un résidu quadratique modulo 2011 ?

2 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 $|a_1b_2 - a_2b_1|$.

2.1 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 tels O, A, B ne sont pas alignés. 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 compris entre 0 et 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 ?

5. (a) Soient C et D deux points de V tels que O, C, et D ne sont pas alignés. Montrer que $R(A, B) = R(C, D)$ si, et seulement si, il existe quatre entiers c_A, c_B, d_A et d_B tels que $C = c_A A + c_B B$, $D = d_A A + d_B B$ et $|c_A d_B - c_B d_A| = 1$.
(b) En déduire 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.
(c) Deux réseaux ayant même covolume sont-ils forcément égaux ?

2.2 Le théorème de Minkowski

Soient X une partie de V d'aire $\mathcal{A}(X)$ et R un réseau de V de covolume $\mathrm{Covol}(R)$. 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 $\mathcal{A}(X) > \mathrm{Covol}(R)$, alors il existe deux points distincts A et B de X tels que $A + (-B) \in R$.

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 $\mathcal{A}(X) > 4\mathrm{Covol}(R)$, 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) Si R est un réseau, montrer qu'une partie bornée du plan (c'est-à-dire une parrtie contenue dans un disque) ne peut contenir qu'un nombre fini de points de R.
(b) Montrer que tout réseau R contient un point A différent de l'origine tel que la longueur OA est majorée par $2\sqrt{\frac{\text{Covol}(R)}{\pi}}$.
(c) Montrer que tout réseau R contient un point B différent de l'origine tel que l'abscisse de B est majorée par $\sqrt{\text{Covol}(R)}$.
(d) Montrer que tout réseau R contient un point $C(c_1, c_2)$ différent de l'origine tel que $|c_1| + |c_2| \leq \sqrt{2\text{Covol}(R)}$.

3 Applications

3.1 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 premiers problèmes, 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.

3.2 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** :

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

3.2.1 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 $(-1, 0)$.

3.2.2 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 $x^2 - 11y^2 = 5$?

3.3 Principe local-global

On admet le **théorème de Dirichlet** : si a et b sont deux entiers non nuls premiers entre eux, alors la suite arithmétique $x_n = an + b$ contient une infinité de nombres premiers. 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.

———————————————FIN———————————————