Représentation des nombres comme somme de deux carrés

Parimaths, 23 novembre 2013

Problème 1 : Le corps $\mathbb{F}_p$

Soit p un nombre premier. On note $\mathbb{F}_p$ l'ensemble $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p. Ces ensembles, outre la particularité de pouvoir faire des additions, soustractions et multiplications sur eux, ont la propriété d'admettre une *division* (bien entendu, pour tout élément non nul). Un ensemble ayant ces quatre propriétés est appelé un *corps* et, puisque $\mathbb{F}_p$ n'a qu'un nombre fini d'éléments, un *corps fini*.

1. Soit $a \in \mathbb{F}_p$ un élément non nul (i.e. la classe d'un des entiers $1, 2, \ldots, p-1$). Montrer en utilisant le théorème de Bézout qu'il existe une *unique* classe $a' \in \mathbb{F}_p$ telle que $aa' = \bar{1}$. En déduire la notion d'*inverse multiplicatif* d'une classe $a \in \mathbb{F}_p$.
2. À partir de cela, donner pour des classes $a, b \in \mathbb{F}_p$ avec $b \neq \bar{0}$ une classe $c \in \mathbb{F}_p$ qui serait un bon candidat pour représenter l'expression $\frac{a}{b}$.
3. Soit maintenant $n \geq 2$ un nombre composé. Donner une classe dans $\mathbb{Z}/n\mathbb{Z}$ n'admettant pas d'inverse multiplicatif. En déduire que $\mathbb{Z}/n\mathbb{Z}$ ne peut pas être muni d'une structure de corps.

Problème 2 : Autour de $\mathbb{F}_p$

Soit p un nombre premier impair. On veut montrer le résultat suivant :

Lemme 1. *L'équation $x^2 = \overline{-1}$ admet des solutions si et seulement si $p \equiv 1[4]$. Dans ce cas, il admet exactement deux solutions.*

Pour ce faire, on définit une relation R sur $\mathbb{F}_p^*$ de la façon suivante : pour $a, b \in \mathbb{F}_p^*$, on a aRb si et seulement si l'une des quatre égalités suivantes est vérifiée :

$$a = b, \qquad a = -b, \qquad a = b^{-1}, \qquad a = -b^{-1}.$$

1. Montrer que R est un relation d'équivalence.
2. Montrer que toute classe d'équivalence a deux ou quatre éléments. Exhiber une classe à deux éléments.
3. Conclure que si $p \equiv 1[4]$ il doit y avoir une deuxième classe à deux éléments.
4. Montrer qu'il ne peut pas y avoir plus de deux classes à deux éléments et que la deuxième classe contient les solutions de l'équation $s^2 = \overline{-1}$.
5. Conclure en montrant que pour $p \equiv 3[4]$ une telle classe n'existe pas.

Problème 3 : Nombres premiers comme sommes de carrés

1. Démontrer que tout nombre premier p de la forme $p \equiv 3[4]$ ne peut pas être écrit comme la somme de deux carrés. *Indication : on regardera la congruence des carrés modulo 4.*
2. Montrer que 2 est bien une somme de deux carrés.
3. On veut démontrer maintenant la proposition suivante :

   Proposition 1. *Tout nombre premier p de la forme $p \equiv 1[4]$ peut être exprimé comme la somme de deux carrés.*

   (a) Soit P l'ensemble des paires d'entiers $0 \leq x, y \leq \sqrt{p}$. Montrer que P a plus de p éléments.

   (b) Soit $s \in \mathbb{Z}$. Montrer qu'il existe deux paires $(x_1, y_1), (x_2, y_2) \in P$ *distinctes* et telles que $x_1 - sy_1 \equiv x_2 - sy_2[p]$.

(c) En posant $x := |x_1 - x_2|$, $y := |y_1 - y_2|$, en déduire que $(x, y) \in P$ et que $x \equiv \pm sy[p]$.

(d) On suppose maintenant que p est de la forme $p \equiv 1[4]$ et que s est tel que $\bar{s}$ est une solution dans $\mathbb{F}_p^*$ de l'équation $x^2 = \overline{-1}$ (qui existe d'après l'exercice précédent). Montrer que l'on a alors $x^2 \equiv -y^2[p]$.

(e) Montrer que $0 < x^2 + y^2 < 2p$ et conclure.

Problème 4 : Une preuve en une ligne de la proposition 1
Vérifier toutes les affirmations implicites dans la preuve de Don Zagier de la proposition 1.

Problème 5 : Nombres entiers comme sommes de carrés
Le but de cet exercice est de démontrer le théorème plus général

Théorème 1. *Soit n un entier positif ≥ 2. Alors n s'écrit comme somme de deux carrés si et seulement si, dans sa factorisation en puissances de nombres premiers, tout nombre premier p de la forme $p \equiv 3(4)$ a un exposant pair.*

Un tel nombre sera désormais appelé *représentable.*

1. Montrer l'égalité

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2.$$

   En déduire que le produit de deux nombres représentables est représentable.
2. Montrer que le produit d'un nombre représentable et d'un carré est représentable.
3. En déduire, en utilisant tout ce qu'on a fait, qu'un nombre dont la décomposition en facteurs premiers est comme dans l'énoncé est représentable.

   Il s'agit maintenant de démontrer que tout nombre représentable est effectivement de cette forme-là.
4. Soit p un nombre premier congru à $3[4]$. Montrer que si p divise un nombre représentable $n = x^2 + y^2$, alors p divise x et y. *Indication : on pourra regarder l'équation $x^2 + y^2 = n$ modulo p, puis supposer que p ne divise pas x et utiliser l'inverse multiplicatif de $\bar{x}$ dans $\mathbb{F}_p^*$*
5. En déduire que p^2 divise n et conclure la démonstration par récurrence.