Théorème de Fermat de Noël

Le but de ce problème est d'étudier la question posée et résolue par Pierre de Fermat : "quels sont les nombres entiers pouvant s'écrire comme somme de deux carrés d'entiers naturels ?"

Dans tout ce problème dire que l'entier naturel n est somme de deux carrés d'entiers naturels signifie :

$$\exists (x,y)\in\mathbb{N}^2,\ n=x^2+y^2$$

A-Préliminaires

1. Donner une décomposition de chaque entier entre 0 et 18 comme somme de deux carrés d'entiers naturels lorsque cela vous semble possible.
2. À l'aide d'un tableau de congruences, montrer qu'aucun entier congru à 3 modulo 4 n'est somme de deux carrés d'entiers naturels.
3. On note $\mathcal{P}_{3,4}$ l'ensemble des nombres premiers congrus à 3 modulo 4. Le but de cette question est de montrer que $\mathcal{P}_{3,4}$ est infini. On raisonne par l'absurde en supposant que $\mathcal{P}_{3,4}$ est fini et s'écrit $\mathcal{P}_{3,4}=\{p_i,\ i\in [\![1,n]\!]\}$ où $n\in\mathbb{N}^*$.
   (a) Justifier qu'un produit d'un nombre quelconque d'entiers naturels congrus à 1 modulo 4 est congru à 1 modulo 4.
   (b) On pose $M=\left(4\prod_{i=1}^{n}p_i\right)-1$.
      i. Montrer que M n'est pas premier.
      ii. Montrer que M possède au moins un diviseur premier congru à 3 modulo 4.
      iii. Conclure.

Remarque : *Plus généralement, si a et b sont deux entiers naturels non nuls et si on note $\mathcal{P}_{a,b}$ l'ensemble des nombres premiers congrus à a modulo b alors le théorème de la progression arithmétique de Dirichlet affirme que :*

$\mathcal{P}_{a,b}$ est infini si et seulement si a et b sont premiers entre eux

Ce théorème est très difficile à démontrer car la méthode vue pour $\mathcal{P}_{3,4}$ ne se généralise pas. Ce résultat n'intervient pas dans la suite du problème.

4. Soit p un nombre premier et $a\in [\![1,p-1]\!]$, montrer qu'il existe un unique $u\in [\![1,p-1]\!]$ tel que $au\equiv 1\ [p]$.
   On notera dans toute la suite cet inverse $\mathbf{a^{-1}}$.
5. En reprenant les notations de la question précédente, montrer qu'il existe un unique $t\in [\![1,p-1]\!]$ tel que $a+t\equiv 0\ [p]$.
   On notera dans toute la suite cet opposé $-\mathbf{a}$.

Remarque : *Les deux questions précédentes permettent de justifier que l'ensemble $[\![0,p-1]\!]$ muni de l'addition et de la multiplication modulo p est un corps. On le note usuellement $\mathbb{Z}/p\mathbb{Z}$.*

B-Une équation modulaire

Le but de ce paragraphe est de démontrer le lemme suivant :

Lemme 1 : L'équation $s^2 \equiv -1$ $[p]$ d'inconnue s possède :
- Deux solutions appartenant à $[\![1, p-1]\!]$ lorsque p est premier congru à 1 modulo 4.
- Aucune solution si p est premier congru à 3 modulo 4.
- Une unique solution appartenant à $[\![1, p-1]\!]$ si $p = 2$.

1. Démontrer le cas $p = 2$.
2. Soit p un nombre premier impair. On considère la relation binaire définie pour tous $(x, y) \in [\![1, p-1]\!]^2$ par :

$$x\mathcal{R}y \Leftrightarrow x = y \text{ ou } x = -y \text{ ou } x = y^{-1} \text{ ou } x = -y^{-1}$$

   Les notations $-x$ et x^{-1} sont celles introduites dans la partie A.

   (a) Montrer que $\mathcal{R}$ est une relation d'équivalence.

   (b) Soit $x \in [\![1, p-1]\!]$. Justifier que la classe de x est $\mathrm{Cl}(x) = \{x, -x, x^{-1}, -x^{-1}\}$.

   (c) Donner les classes d'équivalence dans le cas où $p = 11$ puis dans le cas où $p = 13$.

3. Dans cette question, on cherche à préciser les cas où certains éléments de la classe de x sont égaux :

   (a) Montrer que $x = -x$ est impossible.

   (b) Montrer que $x = x^{-1}$ équivaut à $x = 1$ ou $x = p - 1$.

   (c) Montrer que $x = -x^{-1}$ possède 0 ou 2 solutions.

   (d) En déduire que l'ensemble $[\![1, p-1]\!]$ est partitionné par les classes d'équivalence de la relation $\mathcal{R}$ en sous-ensembles ayant 4 éléments et un ou deux sous-ensembles ayant 2 éléments.

4. En déduire le lemme annoncé.

C-Nombres premiers somme de deux carrés

Le but de ce paragraphe est de démontrer le lemme suivant :

Lemme 2 : Tout nombre premier congru à 1 modulo 4 est somme de deux carrés d'entiers naturels.

Soit p un nombre premier congru à 1 modulo 4. On note dans ce paragraphe $\Gamma = [\![0, E(\sqrt{p})]\!]$ où E désigne la partie entière.

1. On pose $\gamma = $Card (Γ^2). Donner γ et montrer que $\gamma > p$.
2. Soit $s \in \mathbb{Z}$ fixé.

   (a) Montrer qu'il existe deux couples disctincts (x, y) et (x', y') de Γ^2 tels que $x - sy \equiv x' - sy'$ $[p]$.

   (b) On pose $\widehat{x} = |x - x'|$ et $\widehat{y} = |y - y'|$. Montrer que $(\widehat{x}, \widehat{y}) \in \Gamma^2$ et que $\widehat{x} \equiv \varepsilon s \widehat{y}$ $[p]$ avec $\varepsilon \in \{-1, 1\}$.

3. En choisissant s de façon à utiliser le lemme 1, montrer que $\widehat{x}^2 + \widehat{y}^2 = p$.
4. En déduire les nombres premiers qui sont somme de deux carrés d'entiers naturels.

D-Entiers somme de deux carrés

Nous allons dans cette partie démontrer le théorème suivant qui apporte la réponse au problème initial.

Théorème : Un entier naturel $n \geq 2$ peut s'écrire comme somme de deux carrés d'entiers naturels si et seulement si tous les facteurs premiers congrus à 3 modulo 4 dans la décomposition de n en facteurs premiers apparaissent à une puissance paire.

1. Montrer que si $m = x^2 + y^2$ et $n = t^2 + u^2$ avec m, n, x, y, t et u des entiers naturels, alors mn est également somme de deux carrés. On trouvera cette écriture explicitement grâce à une factorisation astucieuse.
2. Montrer que si $n \in \mathbb{N}$ est somme de deux carrés alors nz^2 où $z \in \mathbb{N}$ est également somme de deux carrés.
3. Montrer que si tous les facteurs premiers congrus à 3 modulo 4 dans la décomposition de n en facteurs premiers apparaissent à une puissance paire alors n s'écrit comme somme de deux carrés d'entiers naturels.
4. Montrons à présent la réciproque du théorème. Soit $n = x^2 + y^2$ avec $n \geq 2$ et $(x, y) \in \mathbb{N}^2$. Notons p un diviseur premier de n congru à 3 modulo 4.
   (a) Montrer que l'hypothèse $x \not\equiv 0\ [p]$ est contradictoire avec le lemme 1, on pourra utiliser x^{-1}.
   (b) En déduire que p^2 divise n.
   (c) Montrer que $\dfrac{n}{p^2}$ est également somme de deux carrés d'entiers naturels.
   (d) Conclure quant à la réciproque du théorème annoncé.
5. Voici une application du théorème : on note $(p_k)_{k\geq 1}$ la liste des nombres premiers impairs donnés dans l'ordre croissant. En considérant $M_k = \left(\displaystyle\prod_{i=1}^{k} p_i\right)^2 + 2^2$, montrer qu'il y a une infinité de nombres premiers congrus à 1 modulo 4.
6. Montrer qu'un entier congru à 7 modulo 8 ne peut être la somme de trois carrés d'entiers naturels.

Remarques : *Un théorème dû à Lagrange assure que tout entier naturel est somme de 4 carrés d'entiers naturels.*

E-Une dernière surprise

À l'aide de Python, déterminer le nombre moyen de décompositions d'un entier naturel n comme somme de deux carrés d'entiers **relatifs** pour n allant de 0 à 100000. Que peut-on conjecturer ? On fournira une impression des fonctions Python servant à répondre à cette question ou on enverra le programme par mail.

Vous pouvez bien sûr tenter de démontrer votre conjecture mais c'est facultatif pour ce devoir.

Théorème de Lagrange (pas de Noël)

Le but du problème est de démontrer le théorème de Lagrange et d'en étudier une application. Il s'énonce de la façon suivante :

Soit G un groupe fini et H un sous-groupe de G. Le cardinal de H divise le cardinal de G.

A-Démonstration du théorème

On considère G un groupe fini de cardinal $n \in \mathbb{N}^*$, on note e son élement neutre et on considère H un sous-groupe de G. On définit une relation binaire $\mathcal{R}$ sur G par :

$$\forall (x, y) \in G^2,\ x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. (a) Rappeler la définition de la classe d'équivalence d'un élément $a \in G$, pour la relation binaire $\mathcal{R}$. On note $\mathrm{Cl}(a)$ la classe de a.
   (b) Montrer que $\forall a \in G$, on a : $\mathrm{Cl}(a) = \{ax,\ x \in H\}$.
3. Pour tout $a \in G$, on considère l'application : $\gamma_a \ : \begin{array}{ccc} H & \to & \{ax,\ x \in H\} \\ x & \mapsto & ax \end{array}$
   (a) Montrer que γ_a est bien définie et que c'est une bijection.
   (b) En déduire que : $\forall a \in G$, $\mathrm{Card}(\mathrm{Cl}(a)) = \mathrm{Card}(H)$.
4. En déduire le théorème annoncé.
5. On suppose que le cardinal du groupe G est un nombre premier. Décrire les sous-groupes de G.

B-Une application du théorème

Soit G un groupe fini de cardinal $n \in \mathbb{N}^*$.

1. Soit $a \in G$, on considère l'application : $\varphi_a \ : \begin{array}{ccc} \mathbb{N} & \to & G \\ n & \mapsto & a^n \end{array}$
   (a) Justifier que φ_a n'est pas injective.
   (b) En déduire qu'il existe $k \in \mathbb{N}^*$ tel que $a^k = e$.
   (c) Si $a \in G$, on définit l'ordre de a de la façon suivante : $\mathrm{Ord}(a) = \min\{k \in \mathbb{N}^*,\ a^k = e\}$.
   Justifier que le minimum considéré dans la définition de $\mathrm{Ord}(a)$ existe.
2. (a) Soit $a \in G$, démontrer que $H_a = \{a^k,\ 0 \leq k \leq \mathrm{Ord}(a) - 1\}$ est un sous-groupe de G.
   (b) En déduire que $\mathrm{Ord}(a)$ est un diviseur de n.
3. Montrer que : $\forall a \in G,\ a^n = e$.
4. Montrer qu'un groupe de cardinal premier est commutatif.