

La présentation, l'orthographe et la qualité de la rédaction seront prises en compte.

Les résultats devront être encadrés.

La recherche de l'intégralité du sujet est indispensable pour tous.

Cependant, vous rédigerez un devoir par binôme, avec relecture mutuelle. Bien sûr les écritures des deux signataires devront apparaître de manière significative dans la copie.

### Problème 1

Dans cet exercice, on pose  $a, b \in \mathbb{R}$  avec  $a < b$ .

## Un théorème d'analyse

Soit  $f$  et  $g$  deux fonctions continues sur  $[a, b]$  et dérivables sur  $]a, b[$ . On veut montrer qu'il existe  $c \in ]a, b[$  tel que  $(f(b) - f(a))g'(c) = (g(b) - g(a))f'(c)$ .

On pose

$$h : t \mapsto (f(b) - f(a))(g(t) - g(b)) - (g(b) - g(a))(f(t) - f(b)).$$

1. Montrer qu'il existe  $c \in ]a, b[$  tel que  $h'(c) = 0$ .
2. Conclure.

## Règle de l'Hôpital

Pour cette partie, soit  $f$  et  $g$  deux fonctions continues sur  $]a, b[$  et dérivables sur  $]a, b[$ . On suppose que  $g$  et  $g'$  ne s'annulent pas sur  $]a, b[$  et que les limites en  $a^+$  de  $f$  et  $g$  sont nulles.

Le but de cette partie est de montrer que si  $\frac{f'}{g'}$  admet une limite en  $a^+$ , alors  $\frac{f}{g}$  également et qu'on a

$$\lim_{x \rightarrow a^+} \frac{f'(x)}{g'(x)} = \lim_{x \rightarrow a^+} \frac{f(x)}{g(x)}.$$

3. Montrer que  $f$  et  $g$  sont prolongeables par continuité en  $a$  en donnant les valeurs de  $f(a)$  et  $g(a)$ .
4. D'après la première partie, montrer que pour tout  $0 < h < b - a$ , il existe  $c_h \in ]a, a + h[$  tel que

$$(f(a + h) - f(a))g'(c_h) = (g(a + h) - g(a))f'(c_h)$$

5. En déduire que pour tout  $0 < h < b - a$ , on a

$$\frac{f(a + h) - f(a)}{g(a + h) - g(a)} = \frac{f'(c_h)}{g'(c_h)}.$$

6. Donner la limite de  $c_h$  quand  $h$  tend vers 0.
7. Conclure.
8. **Exemple.** À l'aide de ce résultat, montrer que

$$\lim_{x \rightarrow 0} \frac{1 - \cos x}{x^2} = \frac{1}{2}.$$

## Problème 2

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 Prémiminaires

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. 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  $\mathcal{P}_{3,4} = \{p_i, i \in \llbracket 1, n \rrbracket\}$  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  $a \in \llbracket 1, p-1 \rrbracket$ , montrer qu'il existe un unique  $u \in \llbracket 1, p-1 \rrbracket$  tel que  $au \equiv 1 [p]$ .  
**On notera dans toute la suite cet inverse  $a^{-1}$ .**
5. En reprenant les notations de la question précédente, montrer qu'il existe un unique  $t \in \llbracket 1, p-1 \rrbracket$  tel que  $a+t \equiv 0 [p]$ .  
**On notera dans toute la suite cet opposé  $-a$ .**

**Remarque.** Les deux questions précédentes permettent de justifier que l'ensemble  $\llbracket 0, p-1 \rrbracket$  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 cette partie est de démontrer le lemme suivant.

### Lemme 1

L'équation  $s^2 \equiv -1 [p]$  d'inconnue  $s$  possède

- deux solutions appartenant à  $\llbracket 1, p-1 \rrbracket$  si  $p$  est premier congru à 1 modulo 4,
- aucune solution si  $p$  est premier congru à 3 modulo 4,
- une unique solution appartenant à  $\llbracket 1, p-1 \rrbracket$  si  $p = 2$ .

6. Démontrer le cas  $p = 2$ .

7. Soit  $p$  un nombre premier impair. On considère la relation binaire définie pour tous  $(x, y) \in \llbracket 1, p-1 \rrbracket^2$  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

- Montrer que  $\mathcal{R}$  est une relation d'équivalence.
  - Soit  $x \in \llbracket 1, p-1 \rrbracket$ . Justifier que la classe de  $x$  est  $\text{Cl}(x) = \{x, -x, x^{-1}, -x^{-1}\}$ .
  - Donner les classes d'équivalence dans le cas où  $p = 11$  puis dans le cas où  $p = 13$ .
8. Dans cette question, on cherche à préciser les cas où certains éléments de la classe de  $x$  sont égaux :
- Montrer que  $x = -x$  est impossible.
  - Montrer que  $x = x^{-1}$  équivaut à  $x = 1$  ou  $x = p-1$ .
  - Montrer que  $x = -x^{-1}$  possède 0 ou 2 solutions.
  - En déduire que l'ensemble  $\llbracket 1, p-1 \rrbracket$  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.
9. 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 cette partie  $\Gamma = \llbracket 0, \lfloor \sqrt{p} \rfloor \rrbracket$ .

- On pose  $\gamma = \text{Card}(\Gamma^2)$ . Donner  $\gamma$  et montrer que  $\gamma > p$ .
- Soit  $s \in \mathbb{Z}$  fixé.
  - Montrer qu'il existe deux couples distincts  $(x, y)$  et  $(x', y')$  de  $\Gamma^2$  tels que  $x - sy \equiv x' - sy' [p]$ .
  - On pose  $\hat{x} = |x - x'|$  et  $\hat{y} = |y - y'|$ . Montrer que  $(\hat{x}, \hat{y}) \in \Gamma^2$  et que  $\hat{x} \equiv \varepsilon s \hat{y} [p]$  avec  $\varepsilon \in \{-1, 1\}$ .
- En choisissant  $s$  de façon à utiliser le lemme 1, montrer que  $\hat{x}^2 + \hat{y}^2 = p$ .
- 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.

### Theorème 1

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 pourra penser à travailler dans  $\mathbb{C}$  pour éviter des calculs trop fastidieux.
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  $\frac{n}{p^2}$  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  $M_k = \left( \prod_{i=1}^k p_i \right)^2 + 2^2$ , 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.

**Remarque.** 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 ?

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