CPGE MPSI
2016-2017

Le 03.12.16

Devoir Surveillé n°4

Durée de l'épreuve : 4 heures
La calculatrice est interdite

Le devoir est composé d'un exercice et d'un problème.
Lorsqu'une question est jugée, a priori, plus difficile, elle est précédée du symbole $(*)$ voire $(**)$
La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées**.

BON COURAGE

Exercice /10

Pour l'ensemble de cet exercice, on note $c = \cos 1$ et $s = \sin 1$.
On considère les suites (u_n) définie par récurrence par :

$$\forall\, n \in \mathbb{N}, u_{n+2} = 2c \times u_{n+1} - u_n$$

ainsi que deux conditions initiales ($u_0 = \dots$, $u_1 = \dots$), non précisées pour le moment.

1. Trouver une expression explicite de u_n en fonction de n.
2. Quelle valeur donnée à u_0 et de u_1 pour obtenir comme solution la suite $(v_n) = (\cos n)$ et quelle valeur donnée à u_0 et de u_1 pour obtenir comme solution la suite $(w_n) = (\sin n)$.
3. On suppose que (v_n) converge vers ℓ.
   (a) Montrer que nécessairement $\ell = 0$
   (b) En considérant la suite extraite (u_{2n}), montrer que la suite $(\sin^2(n))_n$ converge également vers 0.
   (c) En déduire, un contradiction, donc que (v_n) diverge.
4. De même montrer que (w_n) diverge.
5. Montrer que l'on peut extraire de (v_n), une suite convergente.
6. $(**)$ Montrer que pour tout $\ell \in [-1, 1]$, on peut trouver $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(v_{\varphi(n)})$ converge vers ℓ.

Problème

Dans ce problème, nous nous intéressons à un problème résolu par Fermat :

« Quels sont les nombres premiers (en partie C) ou les nombres entiers (en partie D) qui peuvent s'écrire comme la somme de deux carrés ? »

Pour résoudre ce problème, nous suivons la démarche proposée par Gauss. Il faut faire un détour dans $\mathbb{C}$ (!) et définir les entiers de Gauss. En partie A, nous voyons une image géométrique du produit dans $\mathbb{Z}[i]$, et dans la partie B, nous étudions nous étudions les propriétés arithmétiques de ces nombres particuliers...

Dans tout le problème, on note $\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}$. On appelle cet ensemble, l'anneau des entiers de Gauss.
On peut donc écrire :

$$z \in \mathbb{Z}[i] \iff \exists\ a, b \in \mathbb{Z} \text{ tels que } z = a + ib$$

A. Interprétation géométrique de la divisibilité dans $\mathbb{Z}[i]$ /3

Soit $z_0 = a_0 + ib_0 \in \mathbb{Z}[i]$. On note $\varphi_0 : \mathbb{C} \to \mathbb{C}$, $z \mapsto z_0 \times z$

1. Comment s'appelle la transformation géométrique φ_0 ?
   Quelles sont ces éléments caractéristiques ? Et que vaut $\varphi_0(1)$?
2. Montrer que φ_0 conserve les angles droits (si trois points forment un angle droit, leurs images forment un angle droit) et les alignements (si trois points sont alignés, leurs images sont alignés).
3. Montrer que φ_0 transforme les carrés en carrés.
   En particulier, quelle est l'image par φ_0 du carré $ABCD$, où les affixes des points A, B, C et D sont respectivement : 0, 1, $1 + i$ et i ?
4. Si $\mathbb{Z}[i]$ est représenté par un réseau de points réguliers, comme est représenté $z_0\mathbb{Z}[i]$.
   Faire une représentation graphique dans un plan $\mathbb{C}$ de $z_0\mathbb{Z}[i]$, avec $z_0 = 1 + 2i$.
   (La représentation graphique assez grande contiendra les points -6, 6, $-10i$ et $10i$).
   Où sont les multiples de z_0 sur le plan ?

B. L'anneau des entiers de Gauss /13,5

Dans cette partie, nous montrons que l'ensemble des entiers de Gauss a de nombreuses propriétés arithmétiques, comparables à celles dans $\mathbb{Z}$. Cela est une conséquence de l'existence d'une division euclidienne.

1. Montrer que si $z, z' \in \mathbb{Z}[i]$, alors $\overline{z}$, $z + z'$ et $z \times z' \in \mathbb{Z}[i]$.
   La stabilité de $\mathbb{Z}[i]$ assuré par ces deux dernières opérations explique ce nom d'anneau.
2. On note $N : \mathbb{Z}[i] \to \mathbb{N}, z \mapsto z\overline{z}$.
   Justifier que $N(\mathbb{Z}[i]) \subset \mathbb{N}$.
3. Montrer que $N(zz') = N(z)N(z')$
4. On note $\mathbb{Z}[i]^*$, l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ et dont l'inverse est dans $\mathbb{Z}[i]$.
   Autrement écrit : $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid \exists\ z' \in \mathbb{Z}[i], z \times z' = 1\}$.
   (a) Montrer que $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$
   (b) En déduire les quatre éléments de $\mathbb{Z}[i]^*$.
5. Dans cette question, nous allons montrer que $\mathbb{Z}[i]$ est un anneau euclidien.
   Autrement écrit, il existe « une »(sorte de) division euclidienne sur $\mathbb{Z}[i]$.
   (a) Soit $s \in \mathbb{C}$ (non forcément entier de Gauss).
   Montrer qu'il existe $z \in \mathbb{Z}[i]$ tel que $|z - s| \leqslant \dfrac{\sqrt{2}}{2}$.
   On pourra s'aider d'un dessin pour faire la démonstration
   (b) En déduire, en choisissant bien s, :

$$\forall\ x, y \in \mathbb{Z}[i], \exists\ (q, r) \in \mathbb{Z}[i] \text{ tel que } x = qy + r \text{ avec } 0 \leqslant N(r) < N(y)$$

   On dit que $\mathbb{Z}[i]$ est muni d'une division euclidienne, ou que $\mathbb{Z}[i]$ est un anneau euclidien.
   On notera que le couple (q, r) n'est pas unique
   (c) Faire la division euclidienne de $3 + 2i$ par $1 - i$.

6. On dit que $p \in \mathbb{Z}[i]$ est i-premier si
   — p n'est pas inversible
   — si, pour tout $a, b \in \mathbb{Z}[i]$, $p = ab$, alors a est inversible ou b est inversible
   (a) Cette définition généralise-t-elle celle des nombres premiers sur $\mathbb{N}$?
   (b) Montrer que si $N(p)$ est premier alors p est nécessairement i-premier.
   Donner un nombre i-premier.
   (c) En considérant $3 \in \mathbb{Z}[i]$, montrer que la réciproque de la proposition précédente est fausse.
   (d) Soit p un nombre i-premier .
   Montrer que, pour tout $a, b \in \mathbb{Z}[i]$, $p|a \times b \Longrightarrow p|a$ ou $p|b$ *(Lemme de Gauss)*
   (e) (*) Démontrer l'extension du théorème fondamentale de l'arithmétique :
   Tout entier de $\mathbb{Z}[i]$ est soit une unité, soit divisible par un nombre i-premier
   Puis :
   Tout nombre entier de $\mathbb{Z}[i]$ non inversible s'écrit comme un produit unique de nombres i-premiers.
   (sans tenir compte des inversibles, des nombres associés et de l'ordre du produit).

C. Un nombre premier comme somme de 2 carrés /11,5

Dans cette partie nous montrons que :

$p \in \mathbb{N}$ premier et $p \neq 2$ s'écrit sous la forme $a^2 + b^2$ si et seulement si $p \equiv 1[4]$.

Dans les questions 1. et 2., nous démontrons le sens direct de la proposition (condition nécessaire).
Dans la question 3., nous faisons un détour pour démontrer le théorème de Wilson.
Nous exploitons ce résultat dans la question 4., pour démontrer constructivement le sens indirect de la proposition (condition suffisante).

1. Montrer que si $p = 2$, il existe un seul couple $(a, b) \in \mathbb{N}$ tel que $p = a^2 + b^2$.
2. Soit p un nombre premier, différent de 2.
   Montrer que s'il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2$, alors $p \equiv 1[4]$
3. Soit q un entier premier.
   (a) Rappeler le petit théorème de Fermat avec comme hypothèse : q premier et $n \wedge q = 1$
   (b) On considère le polynôme $P(X) = (X^{q-1} - 1) - (X - 1)(X - 2) \cdots (X - (q - 1))$.
   Montrer que le degré de P est strictement inférieur à $q - 1$.
   On rappelle que le degré d'un polynôme est le plus grand coefficient k de X^k dans la combinaison linéaire définissant P.
   (c) Montrer que pour tout $k \in [\![1, q - 1]\!]$, $P(k) \equiv 0[q]$
   (d) En déduire le théorème de Wilson : $(q - 1)! \equiv -1[q]$.
   On admet le résultat suivant :
   Soit P de degré d à coefficients entiers, $P(X) = \sum_{k=0}^{d} a_k X^k$
   Si il existe $d+1$ valeurs entiers, $0 < a_0, \cdots < a_d \leqslant p-1$ tel que : $\forall\ i \leqslant d$, $P(a_i) \equiv 0[p]$, alors pour tout $k \in \{0, 1, \ldots d\}$, $a_k \equiv 0[p]$.
4. Nous allons démontrer l'application réciproque. Considérons p premier, tel que $p \equiv 1[4]$.
   (a) En exploitant le théorème de Wilson, montrer que
   $$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1[p]$$
   (b) En déduire qu'il existe $x \in \mathbb{N}$ tel que $p|(x + i)(x - i)$.
   (c) Par l'absurde montrer que p ne peut pas être i-premier.
   On exploitera le Lemme de Gauss dans $\mathbb{Z}[i]$
   (d) Conclure.
   (e) Application : Trouver $a, b \in \mathbb{N}$ tel que $a^2 + b^2 = 13$

D. Somme de deux carrés /14

Dans cette partie, nous généralisons le résultat de la partie précédente à tout entier n.
Nous démontrons en particulier :

$n \in \mathbb{N}$ s'écrit sous la forme $a^2 + b^2$ si et seulement si
chacun de ses facteurs premiers de la forme $4k + 3$ intervient à une puissance paire

Nous terminons cette partie en dénombrant le nombre de telle décomposition, selon la factorisation de n.

1. Soit $n = a^2 + b^2 \in \mathbb{N}$, avec $a, b \in \mathbb{N}$.
   On note $\delta = a \wedge b$ et a' et b' tels que $a = a'\delta$ et $b = b'\delta$.
   (a) Soit p diviseur premier impair de $(a')^2 + (b')^2$.
   Montrer que si p était i-premier (dans $\mathbb{Z}[i]$), alors p diviserait $2a'$ et $2b'$.
   En déduire une contradiction.
   On pourra utiliser le lemme de Gauss
   (b) Montrer alors que $p = z_1 z_2$, avec z_1 et z_2 non inversible.
   En déduire que $p = N(z_1)$ puis est la somme de deux carrés.
   (c) Conclure
2. Réciproquement, soit $n = 2^a \left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right)^2 q_1^{\beta_1} \cdots q_m^{\beta_m}$, avec $p_i \equiv 3[4]$ et $q_j \equiv 1[4]$
   (a) Montrer l'identité de Lagrange :
   $$\forall\ a, b, c, d \in \mathbb{Z} \qquad (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$
   (b) Montrer alors que :
   $$\exists\ A, B \in \mathbb{N} \qquad \text{tels que} \qquad 2^a q_1^{\beta_1} \cdots q_m^{\beta_m} = A^2 + B^2$$
   (c) En déduire que n peut s'écrire comme la somme de deux carrés.
3. Pour quel entier p, premier, a-t-on un triplet pythagoriciens $(a, b, p) \in \mathbb{N}$
   c'est-à-dire tel que $a^2 + b^2 = p^2$?
4. En reexploitant l'identité de Lagrange, trouver les 6 représentations distinctes comme somme de carrés de $2925 = 3^2 \times 5^2 \times 13$.
   On compte comme représentations disctinctes, les deux représentations A^2+B^2 et B^2+A^2 (si $A \neq B$). On considère $A, B \geqslant 0$.
5. (**) On note $r_2(n)$ le nombre de représentation distinctes sous la forme $n = a^2 + b^2$.
   Démontrer le théorème suivant :
   $$r_2(n) = \prod_{p \in \mathcal{P}_1} (v_p(n) + 1) \times \prod_{p \in \mathcal{P}_3} \left(\frac{1 + (-1)^{v_p(n)}}{2} \right)$$
   où $\mathcal{P}_1 = \{p \in \mathcal{P} \mid p \equiv 1[4]\}$ et $\mathcal{P}_3 = \{p \in \mathcal{P} \mid p \equiv 3[4]\}$.