Devoir surveillé n°5

Durée : 3 heures, calculatrices et documents interdits

I. Suite de Fibonacci.

La suite (u_n) (**suite de Fibonacci**) est définie par

$$u_0 = 1\,; \quad u_1 = 1 \quad \text{et} \qquad \forall n \in \mathbb{N} \quad u_{n+2} = u_{n+1} + u_n\,.$$

1) Résoudre cette relation de récurrence et donner une expression de u_n en fonction de n.

Dans toute la suite on n'utilisera plus les résultats de la question précédente.

2) Montrer que pour tout $n \in \mathbb{N}$, $u_n \in \mathbb{N}^*$.

3) Montrer que la suite (u_n) est croissante.

4) Montrer que, pour tout $n \in \mathbb{N}$, $u_n \geqslant n$. Que peut-on en déduire quant à la limite de (u_n) ?

5) Démontrer que, pour tout $n \in \mathbb{N}$, $u_n u_{n+2} - u_{n+1}^2 = (-1)^n$.
Indication : On pourra introduire la suite $a_n = u_n u_{n+2} - u_{n+1}^2$ et montrer que, pour tout $n \in \mathbb{N}$, $a_{n+1} = -a_n$.

6) En déduire que pour tout $n \in \mathbb{N}$, u_n et u_{n+1} sont premiers entre eux.

7) Pour tout entier naturel n, on pose $v_n = \dfrac{u_{n+1}}{u_n}$, puis $x_n = v_{2n}$ et $y_n = v_{2n+1}$.

a) Démontrer la relation $v_{n+1} = 1 + \dfrac{1}{v_n}$ pour tout entier naturel n.

b) Démontrer la relation $v_{n+2} - v_n = \dfrac{(-1)^n}{u_n u_{n+2}}$ pour tout $n \in \mathbb{N}$.

c) En déduire que les suites (x_n) et (y_n) sont adjacentes.

d) En déduire que la suite (v_n) converge. Quelle est sa limite ?

II. Équation de Pell-Fermat

On appelle équation de Pell-Fermat toute équation de la forme $x^2 - dy^2 = 1$ où les inconnues x et y sont des entiers, et où $d \in \mathbb{N}$ n'est pas un carré parfait. Nous allons résoudre cette équation pour $d = 7$. Cette méthode pourrait se généraliser à n'importe quelle valeur de d.

On note $\mathbb{Z}[\sqrt{7}]$ l'ensemble $\left\{ a + b\sqrt{7} \;\middle|\; a, b \in \mathbb{Z} \right\}$.

1) **a)** Montrer que $\mathbb{Z}[\sqrt{7}]$ est un sous-groupe de $(\mathbb{R}, +)$.

b) Montrer aussi que $\mathbb{Z}[\sqrt{7}]$ est stable par la loi $\times$, puis en déduire que $(\mathbb{Z}[\sqrt{7}], +, \times)$ est un anneau commutatif.

2) **a)** Montrer que $\sqrt{7}$ est irrationnel.

b) Montrer

$$\forall x \in \mathbb{Z}[\sqrt{7}] \quad \exists!(a, b) \in \mathbb{Z}^2 \quad x = a + b\sqrt{7}$$

L'élément $a - b\sqrt{7}$ de $\mathbb{Z}[\sqrt{7}]$ est appelé *conjugué* de $x = a + b\sqrt{7}$ et est noté $\overline{x}$ (ne pas le confondre avec le conjugué complexe !).

c) On considère l'application $\varphi : \begin{array}{ccc} \mathbb{Z}[\sqrt{7}] & \to & \mathbb{Z}[\sqrt{7}] \\ x & \mapsto & \overline{x} \end{array}$. Montrer que φ est un endomorphisme d'anneaux.

3) Pour tout $x \in \mathbb{Z}[\sqrt{7}]$, on pose $N(x) = x\overline{x}$. Ce réel est appelé *norme* de x.

a) Montrer que pour tout $x \in \mathbb{Z}[\sqrt{7}]$, $N(x) \in \mathbb{Z}$.

b) Montrer que pour tout $x, x' \in \mathbb{Z}[\sqrt{7}]$, $N(xx') = N(x)N(x')$.

c) Soit $x \in \mathbb{Z}[\sqrt{7}]$. Montrer que x est inversible si et seulement si $N(x) = \pm 1$.

d) On pose $G = \left\{ x \in \mathbb{Z}[\sqrt{7}] \;\middle|\; N(x) = 1 \right\}$. Montrer que $(G, \times)$ est un groupe.

e) Expliquer en quoi la détermination des éléments de G est équivalente à la détermination des solutions entières de l'équation $x^2 - 7y^2 = 1$.

4) Soit $x \in G \cap]1, +\infty[$. On note $x = a + b\sqrt{7}$, avec $a, b \in \mathbb{Z}$.

a) Calculer $x + \overline{x}$ et en déduire que $a > 0$.

b) Montrer que $x^2 = 1 + 2bx\sqrt{7}$ et en déduire que $b > 0$.

c) Montrer que $b \geqslant 3$ et $a \geqslant 8$.

d) En déduire que $G \cap]1, +\infty[$ contient un plus petit élément $x_0 = a_0 + b_0\sqrt{7}$ pour l'ordre naturel sur $\mathbb{R}$.

e) Montrer qu'il existe un entier naturel n tel que $x_0^n \leqslant x < x_0^{n+1}$.

f) En déduire que $x = x_0^n$.

g) Montrer finalement que $G = \{ \pm x_0^n \mid n \in \mathbb{Z} \}$.

5) En déduire toutes les solutions de l'équation $x^2 - 7y^2 = 1$.

III. Formule d'inversion de Möbius.

On appelle $\mathscr{A} = \mathbb{C}^{\mathbb{N}^*}$ l'ensemble des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ (ensemble des fonctions *arithmétiques*).

Pour tout entier n non nul, on note $\mathscr{D}^+(n)$ l'ensemble des diviseurs positifs de n :

$$\mathscr{D}^+(n) = \{d \in \mathbb{N}^* \ , \ d \mid n\}\,.$$

Si $f, g \in \mathscr{A}$, on définit la fonction $f * g : \mathbb{N}^* \to \mathbb{C}$ par :

$$\forall n \in \mathbb{N}^*,\ (f*g)(n) = \sum_{d \in \mathscr{D}^+(n)} f(d) g\left(\frac{n}{d}\right).$$

On pourra remarquer que

$$\forall n \in \mathbb{N}^*,\ (f*g)(n) = \sum_{a,b \in \mathbb{N}^*,\ ab=n} f(a)g(b).$$

Cette opération $*$ est appelée *convolution de Dirichlet* et définit naturellement une loi de composition interne sur $\mathscr{A}$.

On définit deux éléments δ et $\mathbf{1}$ de $\mathscr{A}$ par :

$$\forall n \in \mathbb{N}^*,\ \delta(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$$

et

$$\forall n \in \mathbb{N}^*,\ \mathbf{1}(n) = 1.$$

I - Structure de $(\mathscr{A}, +, *)$.

1) Justifier que $*$ est associative sur $\mathscr{A}$.

2) La loi $*$ est-elle commutative sur $\mathscr{A}$?

3) Montrer que δ est un élément neutre pour $*$ dans $\mathscr{A}$.

4) Soit $f \in \mathscr{A}$ vérifiant $f(1) = 0$. Cet élément f est-il inversible ? Est-ce que $(\mathscr{A}, *)$ possède une structure de groupe ?

5) La réciproque du résultat précédent est-elle vraie ?

6) Montrer que $(\mathscr{A}, +, *)$ a une structure d'anneau.

7) Cet anneau est-il intègre ?

II - Fonction et formule d'inversion de Möbius.

On définit l'élément μ de $\mathscr{A}$ (fonction de Möbius) de la manière suivante : pour tout $n \in \mathbb{N}^*$:

— si n est divisible par le carré d'un nombre premier, $\mu(n) = 0$;

— si n s'écrit comme le produit de k nombres premiers distincts, $\mu(n) = (-1)^k$.

8) Soit I un ensemble fini non vide. Justifier que I possède autant de parties de cardinal pair que de parties de cardinal impair.

Remarque : on se rappellera que si $0 \leqslant k \leqslant n$, tout ensemble fini contenant n éléments possède exactement $\binom{n}{k}$ parties ayant k éléments.

9) En déduire que pour tout $n \in \mathbb{N}^*$ différent de 1 :

$$\sum_{d \in \mathscr{D}^+(n)} \mu(d) = 0.$$

10) Comment peut-on réécrire le résultat précédent, en fonction de **1** et au regard des objets introduits dans la première partie ?

11) En déduire la formule d'inversion de Möbius : pour tout $f, g \in \mathscr{A}$,

$$\left(\forall n \in \mathbb{N}^*,\ g(n) = \sum_{d \in \mathscr{D}^+(n)} f(d)\right) \Leftrightarrow \left(\forall n \in \mathbb{N}^*,\ f(n) = \sum_{d \in \mathscr{D}^+(n)} g(d)\mu\left(\frac{n}{d}\right)\right).$$

III - Une application.

Soit $n \in \mathbb{N}^*$. On note $\omega = \mathrm{e}^{\frac{2i\pi}{n}}$ et on rappelle que

$$\mathbb{U}_n = \left\{\omega^k,\ 0 \leqslant k \leqslant n-1\right\}.$$

Si $z \in \mathbb{U}_n$, on appelle *ordre* de z le plus petit entier $d \geqslant 1$ tel que $z^d = 1$.

Si $d \geqslant 1$, on note $\varphi(d)$ le nombre d'entiers de $[\![1, d]\!]$ premiers avec d :

$$\varphi(d) = \mathrm{Card}\left\{k \in [\![1, d]\!],\ k \wedge d = 1\right\}.$$

12) Soit $z \in \mathbb{U}_n$, montrer que l'ordre de z est bien défini, et qu'il divise n.

13) Soit $d \in [\![1, n-1]\!]$ tel que $d|n$. Montrer qu'il y a exactement $\varphi(d)$ éléments d'ordre d dans $\mathbb{U}_n$. *Indication :* avec $e \in [\![1, n-1]\!]$ tel que $d.e = n$, considérer ω^e.

14) En déduire que pour tout $n \geqslant 1$, $\varphi(n) = \sum_{\substack{a,b \in \mathbb{N}^* \\ ab=n}} a\mu(b)$.

— FIN —