

Devoir surveillé n°4

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

Le devoir est composé d'un unique problème sur l'équation diophantienne de PELL-FERMAT.
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

Problème - Equation de Pell-Fermat

On appelle équation de Pell-Fermat l'équation :

$$x^2 - dy^2 = m$$

où $d, m \in \mathbb{N}$ et où les inconnues x et y sont entières (on parle d'équation diophantienne dans ce cas).
On s'intéressera dans ce problème uniquement au cas où d n'est pas un carré parfait.

Selon l'idée originale de DIRICHLET, on considère alors

$$\mathbb{Z}[\sqrt{d}] = \{a + \sqrt{d} \times b; a, b \in \mathbb{Z}\} \quad (\text{ici noté } A_d)$$

Dans la partie A, nous étudions deux suites récurrentes. Elles réapparaîtront dans la partie C.
Dans la partie B, nous étudierons la structure algébrique de l'ensemble des solutions, paramétrée par d .

Dans la partie C, nous nous concentrerons sur le cas particulier $d = 2$.

Enfin en partie D, nous retournerons au cas général et chercherons un générateur du groupe.

Partie A - Etude d'un couple de suites imbriquées

/15

On considère deux suites numériques $(a_n)_n$ et $(b_n)_n$ telles que

$$\begin{cases} a_0 = 1 \\ \forall n \in \mathbb{N}, a_{n+1} = 2b_n + a_n \end{cases} \quad \begin{cases} b_0 = 0 \\ \forall n \in \mathbb{N}, b_{n+1} = a_n + b_n \end{cases}$$

1. Etudier la monotonie des suites (a_n) et (b_n) .
2. (a) Montrer que (a_n) et (b_n) vérifient

$$\begin{cases} a_0 = 1 \\ a_1 = 1 \\ \forall n \in \mathbb{N}, a_{n+2} = 2a_{n+1} + a_n \end{cases} \quad \begin{cases} b_0 = 0 \\ b_1 = 1 \\ \forall n \in \mathbb{N}, b_{n+2} = 2b_{n+1} + b_n \end{cases}$$

- (b) Donner, pour tout entier n , une expression explicite de a_n et de b_n .
- (c) En déduire que $a_n \sim \frac{1}{2}(1 + \sqrt{2})^n$ et $b_n \sim \frac{1}{2\sqrt{2}}(1 + \sqrt{2})^n$.

3. On cherche à donner une estimation pour tout $k \in \mathbb{N}$ de

$$r_k = \text{card}\{n \in \mathbb{N} \mid a_n \leq k \text{ et } b_n \leq k\}$$

On fixe $k \in \mathbb{N}$, $k \geq 2$.

- (a) Montrer que si $a_n \leq k$, alors $b_n \leq k$. Qu'en déduire pour r_k ?

- (b) On note $N_k = \left\lfloor \frac{\ln 2k}{\ln(1+\sqrt{2})} \right\rfloor$. Montrer que $a_n \leq k \iff n \leq N_k$.

On admettra que k est suffisamment grand pour pouvoir affirmer que

$$\epsilon_1 := \left\lfloor \frac{\ln(2k+1)}{\ln(1+\sqrt{2})} \right\rfloor - \left\lfloor \frac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor \leq \frac{1}{2} \text{ et } \epsilon_2 := \left\lfloor \frac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor - \left\lfloor \frac{\ln(2k-1)}{\ln(1+\sqrt{2})} \right\rfloor \leq \frac{1}{2}.$$

- (c) En déduire que la proportion des couples de $[0, k]^2$ qui sont des couples (a_n, b_n) est

$$s_k := \frac{1}{(k+1)^2} \left(\left\lfloor \frac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor + 1 \right)$$

- (d) Donner un équivalent simplifié (et sans partie entière) de (s_k) .

Soit $d \in \mathbb{N}$. On suppose que d n'est pas un carré parfait.

On note $A_d = \mathbb{Z}[\sqrt{d}]$

1. Unicité d'écriture.

(a) On souhaite montrer que $\sqrt{d}$ est irrationnel.

i. Montrer qu'il existe $s \in \mathcal{P}$, tel que $v_s(d)$ est impair.

ii. On suppose que $\sqrt{d} \in \mathbb{Q}$, et qu'il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $\sqrt{d} = \frac{p}{q}$.

En évaluant $v_s(p)$ et $v_s(q)$ montrer qu'on a une contradiction. Conclure

(b) Montrer que pour tout $z \in A_d$ il existe un unique couple $(a, b) \in \mathbb{Z}^2$ tel que $z = a + \sqrt{d}b$.

2. Structure algébrique de A_d .

(a) Montrer que $A_d \subset \mathbb{R}$ et que $1 \in A_d$.

(b) Montrer que pour tout $z_1, z_2 \in A_d$, $z_1 - z_2 \in A_d$.

(c) Montrer que pour tout $z_1, z_2 \in A_d$, $z_1 \times z_2 \in A_d$.

(d) Quelle est la nature algébrique de A_d ?

3. Morphisme c_d .

On note pour tout $z = a + \sqrt{d}b \in A_d$, $c_d(z) = a - \sqrt{d}b$ et $N_d(z) = z \times c_d(z)$.

(a) Montrer que $c_d : A_d \rightarrow A_d$. Que vaut $c_d(1)$?

(b) Exprimer pour tout $z_1, z_2 \in A_d$, $c_d(z_1 + z_2)$ et $c_d(z_1 \times z_2)$ en fonction de $c_d(z_1)$ et de $c_d(z_2)$.
Comment qualifier une telle application c_d ?

(c) Montrer que pour tout $z \in A_d$, $N_d(z) \in \mathbb{Z}$.

(d) Montrer enfin que pour tout $z_1, z_2 \in A_d$, $N_d(z_1 \times z_2) = N_d(z_1)N_d(z_2)$.

4. Inverses de A_d .

(a) Montrer que si z admet un inverse $z' \in A_d$ (i.e. z est inversible dans A_d), alors $N_d(z) = 1$ ou $N_d(z) = -1$.

(b) Réciproquement, montrer que si $|N_d(z)| = 1$, alors z est inversible. On donnera l'expression de z^{-1} .

Partie C - Cas particulier $n = 2$

/32

On considère ici $A_2 = \mathbb{Z} + \sqrt{2}\mathbb{Z} = \{z \in \mathbb{R} \mid \exists (a, b) \in \mathbb{Z}^2, z = a + \sqrt{2}b\}$.

On rappelle que $a + \sqrt{2}b$ est inversible dans A_2 ssi $N_2(z) = \pm 1$, ie ssi $|a^2 - 2b^2| = 1$

1. On cherche à résoudre ici l'équation de PELL-FERMAT pour $d = 2$ et m quelconque.

On considère alors l'ensemble $I = \{m \in \mathbb{Z} \mid \exists (a, b) \in \mathbb{Z}^2, m = a^2 - 2b^2\}$.

(a) Montrer que I est stable par produit. (On peut exploiter B.3.(d)).

(b) Donner la liste des carrés modulo 8.

(c) En déduire que 3 n'appartient pas à I .

Et plus généralement, donner l'ensemble des valeurs de K pour qu'on ait l'équivalence

$$m \in I \iff m \equiv K[8]$$

2. Densité de A_2 dans $\mathbb{R}$.

(a) Montrer que pour tout $p \in \mathbb{Z}$, et pour tout $n \in \mathbb{N}$, $p(\sqrt{2} - 1)^n \in A_2$

(b) En déduire que A_2 est dense dans $\mathbb{R}$.

On pourra prendre $x < y \in \mathbb{R}$ et exploiter la définition de $\lim(\sqrt{2} - 1)^n = 0$ avec $\epsilon = y - x$.

On note $\mathcal{H} = \{(x, y) \in \mathbb{R}^2 \mid |x^2 - 2y^2| = 1\}$ et $\pi : \mathcal{H} \rightarrow \mathbb{R}$, $(x, y) \mapsto x + \sqrt{2}y$.

Géométriquement, $\mathcal{H}$ est la réunion de deux hyperboles de $\mathbb{R}^2$.

Nous sommes maintenant amenés à définir un couple de suites (a_n, b_n) . A priori, il ne s'agit pas des mêmes suites que celles étudiées en A. Nous démontrerons en fait en 5. qu'il s'agit bien des mêmes suites. Nous gardons la même notation.

3. On note $\omega = 1 + \sqrt{2}$, un élément particulier de A_2 .

(a) Montrer que pour tout $n \in \mathbb{N}$, il existe un unique couple noté $(a_n, b_n) \in \mathbb{N}^2$ tel que :

$$\omega^n = a_n + \sqrt{2}b_n.$$

- (b) Montrer que pour tout $n \in \mathbb{N}$, $(a_n, b_n) \in \mathcal{H}$ (on a donc $\pi(a_n, b_n) = \omega^n$).
- (c) On considère l'application $\varphi : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$, $(x, y) \mapsto (x + 2y, x + y)$.
Montrer que φ est bijective et expliciter φ^{-1} .
- (d) Montrer que pour tout $n \in \mathbb{N}$, $(a_{n+1}, b_{n+1}) = \varphi((a_n, b_n))$.
- (e) En déduire que $\{\omega^n, n \in \mathbb{N}\} \subset \{a + \sqrt{2}b \text{ tel que } |a^2 - 2b^2| = 1 \text{ \& } a, b \in \mathbb{N}\}$
4. Réciproquement, on considère $(a, b) \in \mathbb{N}^2 \cap \mathcal{H}$
- (a) On suppose que $(x, y) \in \mathbb{N} \cap \mathcal{H}$ et $(x, y) \neq (1, 0)$.
Montrer alors que nécessairement : $0 \leq y \leq x < 2y$.
En déduire que $(2y - x, x - y) \in \mathbb{N}^2 \cap \mathcal{H}$.
- (b) On définit la suite $((x_n), (y_n))_{n \in \mathbb{N}}$ par $\begin{cases} (x_0, y_0) = (a, b) \\ \forall n \in \mathbb{N}, (x_{n+1}, y_{n+1}) = (2y_n - x_n, x_n - y_n) \end{cases}$.
En utilisant la question précédente, montrer qu'il existe $n \in \mathbb{N}$ tel que $(x_n, y_n) = (1, 0)$
- (c) Démontrer que les $(x, y) \in \mathbb{N}^2$ vérifiant l'équation $|x^2 - 2y^2| = 1$ sont les couples (a_n, b_n) avec $n \in \mathbb{N}$ (définies dans C.3.).
- (d) En déduire que $\pi(\{\mathbb{N}^2 \cap \mathcal{H}\}) = \{\omega^n; n \in \mathbb{N}\}$
5. On cherche une approximation du nombre de solutions $(a, b) \in \mathbb{Z}^2$ tel que $|a^2 - 2b^2| = 1$, ou plutôt une certaine fréquence.
On note $R_k = \{(a, b) \in \mathbb{Z}^2 \text{ tel que } |a^2 - 2b^2| = 1 \text{ \& } |a| \leq k, |b| \leq k\}$
et $R_k^+ = \{(a, b) \in \mathbb{N}^2 \text{ tel que } |a^2 - 2b^2| = 1 \text{ \& } a \leq k, b \leq k\}$.
- (a) Montrer que $\text{card}(R_k) = 4 \times \text{card}(R_k^+) - 2$.
- (b) Montrer que les suites (a_n) et (b_n) sont les mêmes suites que celles définies en partie A.
- (c) En déduire un équivalent simplifié de

$$\frac{\text{card}(R_k)}{(2k+1)^2}$$

la proportion des solutions de l'équation diophantienne $x^2 - 2y^2 = \pm 1$ parmi les nombres de valeurs absolues plus petite que k .

Partie D - Générateur de A_d

/27

On considère de nouveau d , un entier naturel non carré quelconque.

On rappelle que $\sqrt{d}$ est irrationnel.

- (a) Montrer qu'il existe une infinité de couples $(x, y) \in \mathbb{N}^2$ tels que $0 < |x^2 - dy^2| \leq 1 + 2\sqrt{d}$.
On pourra par exemple exploiter les fractions incluse dans $]\lfloor \sqrt{d} \rfloor, \lfloor \sqrt{d} \rfloor + 1[$.

(b) (*) Montrer qu'il existe un entier k non nul et deux couples (x, y) et $(x', y') \in \mathbb{N}^2$ tels que

$$x^2 - dy^2 = k = (x')^2 - d(y')^2 \quad \text{et} \quad x \equiv x'[k]; y \equiv y'[k]$$

(c) En considérant $(x' - \sqrt{d}y')(x + \sqrt{d}y)$ et $(x' + \sqrt{d}y')(x - \sqrt{d}y)$, montrer qu'il existe un couple $(u, v) \in \mathbb{Z}^2$ tels que $u^2 - dv^2 = 1$.
- On note $A_d = \{x + \sqrt{d}y \in \mathbb{R} \mid x, y \in \mathbb{Z} \text{ et } x^2 - dy^2 = 1\}$.

(a) On pose $G = A_d \cap \mathbb{R}_+^*$. Montrer que G est stable par produit et par passage à l'inverse.
On peut exploiter les résultats démontrés en partie B.

(b) En exploitant $c_d(z)$, montrer que tout élément $z \in G$ qui est strictement supérieur à 1 est supérieur ou égal à $1 + \sqrt{d}$.

(c) On note $\omega = \inf G \cap]1, +\infty[$.
Montrer que $[\omega, \omega + \frac{\sqrt{d}}{2}] \cap G$ ne possède qu'un seul élément. En déduire que $\omega \in G$.

(d) Montrer que pour tout $n \in \mathbb{Z}$, $\omega^n \in G$.

(e) Réciproquement montrer que $G \subset \{\omega^n, n \in \mathbb{Z}\}$.

(f) Montrer enfin l'unicité d'un tel nombre ω tel que $\omega > 1$ et $\langle \omega \rangle := \{\omega^n, n \in \mathbb{Z}\} = G$.

(g) Qu'en déduire pour A_d ?
- (a) On admet que ω est le nombre dont les coefficients x est le plus petit possible (et > 1).
Exprimer ω dans les deux cas $d = 2$ et $d = 3$.

(b) Expliciter les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 - 3y^2 = 1$