ÉQUATIONS DE PELL-FERMAT ET THÉORÈME DE STØRMER

Deux niveaux de difficulté/longueur :

— Piste rouge : partie **1**.

— Piste noire : tout le devoir.

Pour tout $n \in \mathbb{N}^*$, on appelle *n-nombre* tout entier naturel non nul dont les diviseurs premiers divisent n. Par exemple, les 2-nombres sont les entiers 2^k, k décrivant $\mathbb{N}$, et les 6-nombres sont les entiers $2^i 3^j$, i et j décrivant $\mathbb{N}$, dont les premiers sont 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48… On a représenté ci-dessous les 6-nombres inférieurs à 1000 et ils paraissent d'autant plus rares qu'ils sont grands. Cette raréfaction suggère que les 6-nombres sont de plus en plus éloignés les uns des autres à l'échelle collective, mais elle n'empêche pas a priori qu'il puisse exister une infinité de couples (x,y) de 6-nombres pour lesquels $x-y=1$ ou $x-y=2$ par exemple.

On souhaite prouver le résultat suivant.

Théorème **(Théorème de Størmer)** Soient $p_1,\dots,p_r \in \mathbb{P}$ distincts.
Les équations $x-y=1$ (resp. $x-y=2$) dont l'inconnue (x,y) est un couple de $p_1\dots p_r$-nombres possède au plus 3^r solutions.

Ce théorème du mathématicien norvégien Carl Størmer (1874-1957) date de 1897 et repose sur l'analyse préalable d'une famille importante d'équations diophantiennes dites *de Pell-Fermat*.

1 ÉQUATIONS DE PELL-FERMAT

On appelle *équation de Pell-Fermat* toute équation de la forme $x^2-ny^2=1$ d'inconnue $(x,y)\in\mathbb{Z}^2$ dans laquelle l'entier naturel non nul n est fixé. La résolution complète de ces équations est tout à fait possible en MPSI, mais le théorème de Størmer exige un peu moins.

Soit $n\in\mathbb{N}^*$ fixé. On pose $E_n = \left\{(x,y)\in\left(\mathbb{N}^*\right)^2 \mid \quad x^2-ny^2=1\right\}$.

1) Déterminer E_n sous l'hypothèse que n est un carré parfait.

Dans les questions **2)** à **4)**, on suppose que n n'est pas un carré parfait, mais aussi que E_n est non vide. Dans ces conditions, $\sqrt{n}$ est irrationnel et l'application $(x,y)\longmapsto x+y\sqrt{n}$ est injective sur $\mathbb{Z}^2$. Ces résultats ont été démontrés en TD, assurez-vous que vous savez les redémontrer.

2) On pose $G_n = \left\{x+y\sqrt{n} \mid \quad (x,y)\in E_n\right\}$.

a) Montrer que pour tous $(x,y),(x',y')\in E_n$: $\quad x\leqslant x' \iff x+y\sqrt{n}\leqslant x'+y'\sqrt{n}$.

b) En déduire que G_n possède un plus petit élément $a+b\sqrt{n}$ avec $(a,b)\in E_n$, $a\wedge n=1$ et $a\geqslant 2$.

c) Montrer que G_n est *stable par produit*, i.e. que $gg'\in G_n$ pour tous $g,g'\in G_n$.

d) Montrer que pour tous $(x,y),(x',y')\in E_n$, si $x'<x$, alors $\dfrac{x+y\sqrt{n}}{x'+y'\sqrt{n}}\in G_n$.

e) En déduire que $G_n = \left\{\left(a+b\sqrt{n}\right)^i \mid \quad i\in\mathbb{N}^*\right\}$.

3) Pour tout $i \in \mathbb{N}^*$, on note (a_i, b_i) l'unique couple de E_n pour lequel $\left(a + b\sqrt{n}\right)^i = a_i + b_i\sqrt{n}$.

a) Montrer que pour tous $i, j \in \mathbb{N}^*$, si $i \mid j$, alors $b_i \mid b_j$.

En particulier, pour tout $i \in \mathbb{N}^*$, on peut noter c_i l'unique entier pour lequel $b_i = bc_i$.

b) Exprimer c_i en fonction de a, b et n pour tout $i \in \mathbb{N}^*$, puis montrer que si c_i est un n-nombre, alors c_i est aussi un i-nombre.

c) Montrer que $c_i \geqslant 2$ pour tout $i \geqslant 2$.

4) Soit $k \in \mathbb{N}^*$. On suppose que b_k est un n-nombre.

a) Exprimer c_2 en fonction de a, puis montrer que k n'est pas divisible par 2.

b) Exprimer de même c_3 en fonction de a, puis montrer que k n'est pas divisible par 3.

c) Soit $p \in \mathbb{P} \setminus \{2,3\}$. Montrer que si $p \mid k$, alors $p \mid n$ et $c_p \equiv pa^{p-1} \left[p^2\right]$, puis dénicher une contradiction.

5) Montrer que pour tout $n \in \mathbb{N}^*$, E_n contient au plus un élément dont la deuxième composante est un n-nombre.

2 Théorème de Størmer

Soient $p_1, \dots, p_r \in \mathbb{P}$ distincts.

6) On note S l'ensemble des $p_1 \dots p_r$-nombres de la forme $x^2 - 1$ avec $x \geqslant 2$ entier et on pose :

$$D = \left\{ p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r} \mid \quad \varepsilon_1, \dots, \varepsilon_r \in [\![0,2]\!] \right\}.$$

a) Soit $x \geqslant 2$ un entier pour lequel $x^2 - 1 \in S$. Montrer qu'il existe un entier $n \in D$ et un n-nombre y pour lesquels $(x, y) \in E_n$.

b) En déduire que S est fini de cardinal au plus 3^r.

7) On note enfin U_1 (resp. U_2) l'ensemble des solutions de l'équation $x - y = 1$ (resp. $x - y = 2$) dont l'inconnue (x, y) est un couple de $p_1 \dots p_r$-nombres.

a) Montrer que $(2y+1)^2 - 1$ est un $p_1 \dots p_r$-nombre pour tout $(x, y) \in U_1$, puis en déduire que U_1 est fini de cardinal au plus 3^r.

b) Montrer de même que U_2 est fini de cardinal au plus 3^r.