UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n°6 : Équation de Pell-Fermat

Exercice 1

Soit θ un réel.

On considère les deux suites (a_n) et (θ_n) définies par récurrence de la façon suivante : $\theta_0 = \theta$, et pour tout $i \geq 0$, $a_i = \lfloor \theta_i \rfloor$, $\theta'_{i+1} = \theta_i - a_i$, de sorte que (a_n) est une suite d'entiers et (θ_n) une suite de réels. De plus, on définit, tant que θ'_{n+1} est non nul (ou de manière équivalente tant que θ_n n'est pas entier), $\theta_{n+1} = \frac{1}{\theta'_{n+1}}$. Par exemple si θ est un entier, $\theta_0 = \theta$ et θ_1 n'est pas défini. Remarquer que pour $i \geq 1$, $\theta_i > 1$ donc $a_i \geq 1$.

Si le processus s'arrête, c'est à dire si θ_n est entier pour un certain n, vérifier que

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}},$$

sinon, pour tout n on a

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{\theta_n}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}.$$

Cette écriture est appelée développement de θ en fractions continues. On la note aussi $\theta = [a_0, a_1, \ldots, a_{n-1}, a_n]$, respectivement $\theta = [a_0, \ldots, a_n, \ldots]$.

1. Montrer que le développement est fini si et seulement si θ est un nombre rationnel.
2. Donner le développement en fractions continues de $\frac{116}{27}$.
3. Quel est le nombre dont le développement en fractions continues est

$$5 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}?$$

4. Supposons θ irrationnel. On appelle réduite d'ordre n la fraction $[a_0, \ldots, a_n]$. Elle s'écrit de manière unique $\frac{p_n}{q_n}$, avec p_n et q_n entiers, calculés sans simplification. Vérifier que $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0a_1 + 1$ et $q_1 = a_1$ et que p_n comme q_n sont des polynômes en les $(a_i)_{0\leq i\leq n}$.
5. Pour $n \geq 2$, montrer que
$$p_n = a_n p_{n-1} + p_{n-2} \tag{1}$$
$$q_n = a_n q_{n-1} + q_{n-2}. \tag{2}$$
6. En déduire $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n+1}$ et $p_nq_{n-2} - p_{n-2}q_n = (-1)^n a_n$.
7. Montrer que pour tout n,
$$\theta = \frac{\theta_{n+1}p_n + p_{n-1}}{\theta_{n+1}q_n + q_{n-1}}. \tag{3}$$

Exercice 2

1. Soit $\theta = \frac{1}{2}(\sqrt{5} - 1)$. Montrer que θ est un entier algébrique et trouver le polynôme minimal de $\frac{1}{\theta}$. En déduire le développement en fractions continues de θ.
2. Écrire le développement en fraction continue de $3 + \sqrt{2}$, $2 + \sqrt{6}$ et $2 + \frac{\sqrt{15}}{5}$.
3. Le but de cette question est de calculer les trois premières réduites du développement en fractions continues de $\sqrt[3]{2}$. Montrer que $1,2 < \sqrt[3]{2} < 1,3$ et que $1,5 < \sqrt[3]{4} < 1,6$. Dans l'anneau $\mathbb{Q}[X]/(X^3 - 2)$ déterminer l'inverse de $X - 1$ et celui de $X^2 + X - 2$ dans la base $(1, X, X^2)$. Conclure.

Exercice 3

Montrer que pour $a, b \in \mathbb{N}$, $a \neq 0$, $b < 2a + 1$, on a
$$\sqrt{a^2 + b} = a + \cfrac{b}{2a + \cfrac{b}{2a + \cfrac{b}{\ddots}}}.$$
En déduire le développement en fraction continue de $\sqrt{5}$, $\sqrt{10}$, $\sqrt{17}$, $\sqrt{26}$, $\sqrt{37}$.

Exercice 4

On appelle nombre quadratique irrationnel un réel irrationel, qui est aussi un nombre algébrique de degré 2. On dit que le développement en fractions continues $[a_0, \ldots]$ du nombre irrationnel θ est finalement périodique s'il existe un entier $r \geq 0$ (penser rang) et un entier $m \geq 1$ (penser période) tel que pour tout $k \geq r$, $a_{k+m} = a_k$. Dans ce cas on note

$[a_0, \ldots] = [a_0, \ldots, \overline{a_r, \ldots, a_{r+m-1}}]$. On dit de plus que ce développement est purement périodique s'il est périodique avec $r = 0$. Les nombres quadratiques irrationnels sont exactement ceux dont le développement en fractions continues est finalement périodique. Le but de cet exercice est de montrer une inclusion.

Soit θ un nombre irrationnel dont le développement en fraction continue soit finalement périodique, *i.e.*

$$\theta = [a_0, \ldots, \overline{a_r, \ldots, a_{r+m-1}}]$$

Nous allons montrer que θ est un nombre algébrique de degré 2.

1. Soit $\beta = [\overline{a_r, \ldots, a_{r+m-1}}]$. Montrer que $\beta = [a_r, \ldots, a_{r+m-1}, \beta]$.
2. En déduire que β est solution d'une équation de degré 2 à coefficients rationnels.
3. Montrer que $\theta \in \mathbf{Q}(\beta)$ et en déduire que θ est un nombre algébrique de degré 2.

La réciproque de ce résultat est vraie, c'est le théorème de Lagrange. Dans le cas où $\alpha = \sqrt{d}$ avec d un entier sans facteur carré, on peut montrer que le développement de α est de la forme $[a_0, \overline{a_1, \ldots, a_n}]$, où n est le plus petit indice tel que $a_n = 2a_0$.

Exercice 5

1. Quel est le nombre dont le développement en fractions continues est $[\bar{1}]$?
2. Quel est le nombre dont le développement en fractions continues est $[\overline{4, 5}]$?
3. Montrer que le nombre dont le développement en fractions continues est $[\bar{a}]$ est $\frac{a+\sqrt{a^2+4}}{2}$.

Exercice 6

1. Soit d un entier sans facteur carré. Considérons l'équation de Pell-Fermat :

$$x^2 - dy^2 = 1.$$

   Soit (x_1, y_1) une solution de l'équation. Dans $\mathbb{Q}(\sqrt{d})$ considérons l'écriture $x_n + y_n\sqrt{d}$ de $(x_1 + y_1\sqrt{d})^n$ dans la $\mathbb{Q}$-base $(1, \sqrt{d})$. Montrer que (x_n, y_n) est une solution de l'équation de Pell-Fermat pour tout n.
   D'après le cours, il existe une solution (x_1, y_1) « minimale » et toutes les autres solutions s'en déduisent à l'aide de l'expression ci-dessus.

2. Cherchons maintenant une solution minimale (x_1, y_1) de l'équation.
   Montrer que si (p, q), avec p et q de même signe, est solution de l'équation, alors $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$.
   La fraction $\frac{p}{q}$ est donc une bonne approximation de $\sqrt{d}$. On peut déduire de cela que $\frac{p}{q}$ est nécessairement une réduite du développement de $\sqrt{d}$.

3. Soit T la période du développement de $\sqrt{d}$. Si T est impaire, on pose $n := 2T - 1$. Si Test pair, on pose $n = T - 1$. Dans tous les cas, $n + 1$ est le plus petit multiple paire de T. Nous allons montrer que la réduite $\frac{p_n}{q_n}$ de $\sqrt{d}$ fournit une solution (p_n, q_n) de l'équation de Pell-Fermat.
   On peut montrer que la solution obtenue est minimale.
4. On pose $\alpha = \sqrt{d}$ et on reprend les notations de l'exercice 1.
   Remarquer que $\frac{1}{\alpha_{n+2}} = \frac{1}{\alpha_1} = \alpha - a_0$.
5. En utilisant (3), montrer que $(q_{n+1} - a_0 q_n)\sqrt{d} + dq_n = p_n\sqrt{d} + (p_{n+1} - a_0 p_n)$.
6. En déduire avec (1) que $p_n^2 - dq_n^2 = (-1)^{n+1}$ et conclure.

Pour trouver les solutions de l'équation de Pell-Fermat $x^2 - dy^2 = 1$, on commence donc par chercher le développement en fraction continue de $\sqrt{d}$: $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_T}]$. La solution non neutre minimale est obtenue avec le numérateur et le dénominateur de la réduite d'indice n où $n + 1$ est le plus petit multiple pair de la plus petite période T. Toutes les autres solutions se déduisent à l'aide de la matrice M de la question (2).

Pour trouver les solutions de l'équation $x^2 - dy^2 = -1$, on commence par chercher le développement en fraction continue de $\sqrt{d}$: $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_T}]$. Les solutions sont obtenues avec le numérateur et le dénominateur des réduites d'indice n où $n + 1$ est un multiple impair de la plus petite période T. En particulier, si la période est paire, l'équation n'a pas de solution.

Application : solutions de l'équation de Pell-Fermat pour $d = 3, 5, 34, 37, 53$. (Indication : $\sqrt{34} = [5, \overline{1, 4, 1, 10}]$, $\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$.)

Exercice 7

Montrer que l'équation $x^2 + bxy + cy^2 = \pm 1$ est équivalente à une équation de la forme $X^2 - dy^2 = \pm 4$. (On déterminera un d convenable). L'équation $3x^2 + 2xy + 4y^2 = 1$ a-t-elle un nombre fini de solutions ?

Exercice 8

Le cours donne que le groupe des unités du corps de nombres $\mathbb{Q}(\sqrt{d})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Le facteur $\mathbb{Z}/2\mathbb{Z}$ correspond au signe : si u est une unité $-u$ aussi. Les réduites du développement en fractions continues de $\sqrt{d}$ ne donnent que les unités de la forme $a + b\sqrt{d}$ avec $a > 0$ et $b > 0$. En considérant les inverses, on obtient les $a - b\sqrt{d}$. Le facteur $\mathbb{Z}/2\mathbb{Z}$ permet d'obtenir aussi les $-a - b\sqrt{d}$ et $-a + b\sqrt{d}$.

Le facteur $\mathbb{Z}$ est un sous groupe monogène. Le cours dit qu'un générateur (l'unité fondamentale) est donné par $x_n + y_n\sqrt{d}$ où x_n/y_n est la réduite d'indice $n = T - 1$. Ici T est la plus petite période. La réduite x_2/y_2 par exemple est $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$.

Si la période T est paire l'équation $x^2 - dy^2 = -1$ n'a pas de solution. Aucune unité n'est de norme -1.

Si la période T est impaire, l'unité fondamentale (donnée par la réduite d'indice $n = T - 1$) est de norme -1 (i.e. vérifie $x_n^2 - dy_n^2 = -1$). La plus petite unité de norme 1 est $(x_n + y_n\sqrt{d})^2$ ou encore $x_{2T-1} + y_{2T-1}\sqrt{d}$.

Déterminer les unités de l'anneau des entiers des corps $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{7})$ et $\mathbb{Q}(\sqrt{5})$.

Exercice 9

Déterminer les unités de l'anneau $\mathbb{Z}[\sqrt{41}]$. Montrer que les unités de l'anneau des entiers de $\mathbb{Q}(\sqrt{41})$ sont en fait les unités de l'anneau $\mathbb{Z}[\sqrt{41}]$.

Pour un développement plus détaillé des fractions continues, on pourra consulter
`http://agreg-maths.univ-rennes1.fr/documentation/docs/fraccont.pdf`