Développement d'un réel en fractions continues

Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

M. Couchouron

Introduction et commentaires

Ce document a été écrit pour les étudiants préparant l'agrégation interne.
Ce qui suit est une présentation de l'algorithme des fractions continues et deux applications :

- la première, très naturelle, porte sur le problème de meilleure approximation des réels par des rationnels. Le lecteur pourra consulter le livre de Roger Descombes, pour un exposé bien plus complet, mais plus difficile ;
- la seconde est une application à l'équation de Pell-Fermat. Il s'agit de résoudre, en nombres entiers, les équations de la forme
$$x^2 - dy^2 = 1$$
où d est un entier naturel, qui n'est pas le carré d'un entier. Ce qui revient à déterminer les inversibles de l'anneau $\mathbb{Z}[\sqrt{d}\,]$, de norme 1. La difficulté est de montrer que cette équation possède une solution non triviale. C'est une conséquence d'un théorème plus général que l'on peut trouver, par exemple, dans le livre de Pierre Samuel. De ce point de vue, la démonstration repose sur le lemme de Minkowski qui suppose connu un minimum de théorie de la mesure. La démonstration proposée dans la suite est plus élémentaire, et de plus elle fournit un algorithme qui détermine toutes les solutions. Je me suis très fortement inspiré d'un livre de Alan Baker. Voir la bibliographie.

Il s'agit d'un codage des nombres réels, donné par un algorithme. Ce codage établit une bijection de l'ensemble des irrationnels sur l'ensemble des suites $(a_0, a_1, a_2, \dots)$ d'entiers où $a_1, a_2, \dots$ sont strictement positifs. Les rationnels sont en bijection avec l'ensemble des suites finies d'entiers $(a_0, a_1, \dots, a_n)$ où $a_1, \dots, a_n$ sont strictement positifs et $a_n \geqslant 2$ lorsque n est non nul.

§ 1. Fractions continues formelles

Soient n un entier et $X_0, X_1, , \dots, X_n$ des variables.
— si $n = 0$ on considère la fraction rationnelle
$$F_0 = X_0$$
— si $n = 1$ on considère la fraction rationnelle
$$F_1 = X_0 + \frac{1}{X_1}$$
— si $n = 2$ on considère la fraction rationnelle
$$F_2 = X_0 + \cfrac{1}{X_1 + \cfrac{1}{X_2}}$$
— D'une manière générale, on considère la fraction rationnelle

(1)
$$F_n = X_0 + \cfrac{1}{X_1 + \cfrac{1}{\ddots \; + \cfrac{1}{X_{n-2} + \cfrac{1}{X_{n-1} + \cfrac{1}{X_n}}}}}$$

De manière plus formelle, on peut définir F_n par récurrence par

$$F_{n+1}(X_0,\dots,X_n,X_{n+1}) = F_n(X_0,\dots,X_{n-1},X_n+\frac{1}{X_{n+1}})$$

Notations. De manière évidente ces écritures sont rapidement trop lourdes et inexploitables.

Dans la suite la fraction rationnelle F_n ci-dessus sera notée

$$F_n = [X_0, X_1, , \dots , X_n] \tag{2}$$

Parfois, cette fraction rationnelle F_n est aussi notée $F_n = X_0 + \frac{1}{X_1 +|}\ \frac{1}{X_2 +|}\ \cdots\ \frac{1}{|X_n}$

Proposition 0.0.1 *Il existe une suite (P_n) de polynômes telle que pour tout entier $n \geqslant 0$, le polynôme P_n ne dépende que des variables $X_0,\dots,X_n$ et telle que les conditions suivantes soient vérifiées.*

1. $P_0 = X_0 \quad P_1 = X_0X_1 + 1$

2. Pour tout entier $n \geqslant 2$: $\quad P_n = X_nP_{n-1} + P_{n-2}$

— Il existe une suite (Q_n) de polynômes telle que pour tout entier $n \geqslant 0$, le polynôme Q_n ne dépende que des variables $X_1,\dots,X_n$ et telle que les conditions suivantes soient vérifiées :

1. $Q_0 = 1 \quad Q_1 = X_1$

2. Pour tout entier $n \geqslant 2$: $\quad Q_n = X_nQ_{n-1} + Q_{n-2}$

— Les coefficients de P_n et de Q_n sont des entiers naturels.

Pour tout entier n : P_n est un polynôme de degré $n+1$, dont la partie homogène de degré $n+1$ est réduite au monôme $X_0X_1\dots X_n$ et Q_n est un polynôme de degré n, dont la partie homogène de degré n est réduite au monôme $X_1\dots X_n$.

Démonstration: □ La vérification se fait par récurrence. □

Théorème 0.0.2 *Pour tout entier $n \geqslant 0$:*

$$F_n = [X_0, X_1, , \dots , X_n] = \frac{P_n}{Q_n}$$

Démonstration: □ La démonstration se fait par récurrence sur n.

Pour $n = 0$ c'est évident car $F_0 = X_0$, $P_0 = X_0$ et $Q_0 = 1$

Pour $n = 1$: dans ce cas $F_1 = X_0 + \frac{1}{X_1}$, $P_1 = X_0X_1 + 1$ et $Q_1 = X_1$. L'égalité $F_1 = \frac{P_1}{Q_1}$ est bien vraie.

Soit $n \geqslant 2$ un entier et supposons que pour tout entier $k \leqslant n$ l'égalité $F_k = \frac{P_k}{Q_k}$ soit vraie.

On a donc, en utilisant la définition des polynômes P_n et Q_n :

$$F_n = [X_0, X_1, , \dots , X_n] = \frac{P_n}{Q_n} = \frac{X_nP_{n-1} + P_{n-2}}{X_nQ_{n-1} + Q_{n-2}}$$

et donc :

$$\begin{aligned}[X_0, X_1, , \dots , X_{n+1}] &= \left[X_0\,, X_1, , \dots , X_{n-1}\,, X_n + \frac{1}{X_{n+1}}\right] \\ &= \frac{(X_n + \frac{1}{X_{n+1}})\,P_{n-1} + P_{n-2}}{(X_n + \frac{1}{X_{n+1}})\,Q_{n-1} + Q_{n-2}}\end{aligned}$$

D'où en multipliant le numérateur et le dénominateur par X_{n+1} :

$$[X_0, X_1, , \dots , X_{n+1}] = \frac{X_{n+1}\,(X_n\,P_{n-1} + P_{n-2}] + P_{n-1}}{X_{n+1}\,(X_n\,Q_{n-1} + Q_{n-2}) + Q_{n-1}}$$

Compte tenu de la définition des polynômes P_n et Q_n :

$$[X_0, X_1, , \dots, X_{n+1}] = \frac{X_{n+1}\,P_n + P_{n-1}}{X_{n+1}\,Q_n + Q_{n-1}} = \frac{P_{n+1}}{Q_{n+1}}$$

Ce qui démontre le théorème. □

§ 2. Algorithme des fractions continues

Soit θ un nombre réel.

On considère sa partie entière $a_0 = [\theta]$.

— Si θ est un entier $\theta = a_0$ et l'algorithme s'arrête.

— Sinon θ n'est pas un entier $\theta - a_0$ est un réel tel que $0 < \theta - a_0 < 1$. Il s'écrit donc sous la forme $\dfrac{1}{\theta_1}$, avec $\theta_1 > 1$. Dans ce cas on a donc :

$$\theta = a_0 + \frac{1}{\theta_1}$$

Dans ce cas le procédé se réitère en remplaçant θ par θ_1 : soit a_1 la partie entière de θ_1.

— Si θ_1 est un entier donc égal à a_1, l'algorithme s'arrête, et on a l'égalité :

$$\theta = a_0 + \frac{1}{a_1}$$

— Sinon θ_1 n'est pas un entier et $\theta_1 - a_1$ est un réel qui s'écrit sous la forme $\dfrac{1}{\theta_2}$, avec $\theta_2 > 1$. Dans ce cas le même procédé s'applique à θ_2.

Ce processus s'arrête au cran n si et seulement si θ_n est un entier, égal à sa partie entière a_n. Dans ce cas on a l'égalité :

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} \tag{3}$$

Lemme 0.0.3 *Réciproquement si θ est un nombre rationnel, l'algorithme des fractions continues s'arrête après un nombre fini d'itérations, et que de plus si $\theta = p/q$ les calculs des nombres a_k peuvent se faire par des divisions euclidiennes successives, comme dans l'algorithme d'Euclide.*

Démonstration: □ La démonstration est laissée en exercice. □

Si θ n'est pas rationnel, il existe donc une suite (a_n) d'entiers qui, sauf peut-être le premier a_0, sont supérieurs ou égaux à 1 et une suite $(\theta_n)_{n\geqslant 1}$ de réels strictement plus grands que 1 vérifiant les relations :

$$\theta_n = a_n + \frac{1}{\theta_{n+1}} \tag{4}$$

De plus pour tout entier n on a :

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{n-2} + \cfrac{1}{a_n + \cfrac{1}{\theta_{n+1}}}}}} \tag{5}$$

Dans la suite on suppose que, dans l'algorithme des fractions continues, n itérations sont possibles, et produisent donc des entiers $a_0, a_1, \ldots, a_n$, qui à l'exception de a_0 sont strictement positifs, et des réels $\theta_1, \ldots, \theta_n, \theta_{n+1}$ strictement plus grands que 1. Dans la fraction rationnelle F_n, définie en (1), on peut donc substituer $(a_0, \ldots, a_n)$ à $(X_0, \ldots, X_n)$.

Notations. Dans la suite, si $x_0, x_1, \ldots, x_n$ sont des nombres tels que $F_n(x_0, x_1, \ldots, x_n)$ soit définie, on notera

$$[x_0, x_1, \ldots, x_n] = F_n(x_0, x_1, \ldots, x_n).$$

Lorsque θ est un nombre rationnel, l'égalité (3) s'écrit donc :

$$\theta = [a_0, a_1, \ldots, a_n]$$

De même, l'égalité (5) se notera aussi :

$$\theta = [a_0, a_1, \ldots, a_n, \theta_{n+1}] \tag{6}$$

Définition 0.0.4 *En conservant les notations précédentes et en supposant $a_0, a_1, \ldots, a_n$ définis :*

1. Pour tout entier $k \leqslant n$, a_k s'appelle le quotient incomplet de θ d'indice k et θ_k s'appelle le quotient complet de θ d'indice k.

2. Le nombre rationnel $[a_0, a_1, \ldots, a_k]$ s'appelle la réduite d'indice k.

En substituant $(a_0, a_1 \ldots, a_n)$ à $(X_0, X_1 \ldots, X_n)$ dans les polynômes P_n et Q_n, on obtient des nombres qui seront notés p_n et q_n respectivement. Comme ces polynômes sont à coefficients entiers, les nombres p_n et q_n sont eux-mêmes des entiers. De plus, pour tout entier k tel que $1 \leqslant k \leqslant n$ on a $a_k \geqslant 1$ et donc : $q_k \geqslant q_{k-1} + q_{k-2}$.

D'autre part, pour tout entier $n \geqslant 2$, les suites d'entiers (p_n) et (q_n) vérifient les relations suivantes.

$$p_n = a_n p_{n-1} + p_{n-2} \tag{7}$$

$$q_n = a_n q_{n-1} + q_{n-2} \tag{8}$$

Ceci résulte de la définition même des polynômes P_n et Q_n. Il en résulte par une récurrence immédiate que pour tout entier n : $q_n \geqslant$ **fu1-6l9'-**

Démonstration: □ On a l'égalité : $\theta = [a_0, a_1, \ldots, a_n, \theta_{n+1}] = F_{n+1}(a_0, a_1, \ldots, a_n, \theta_{n+1})$, qui s'obtient à partir de l'égalité formelle

$$F_{n+1}(X_0, X_1, \ldots, X_n, X_{n+1}) = \frac{P_{n+1}}{Q_{n+1}} = \frac{X_{n+1}P_n + P_{n-1}}{X_{n+1}Q_n + Q_{n-1}}$$

en substituant $(a_0, a_1, \ldots, a_n, \theta_{n+1})$ à $(X_0, X_1, \ldots, X_n, X_{n+1})$ dans F_{n+1}. □

§ 3 Meilleure approximation

Dans la suite on considère un nombre réel θ irrationnel.
On notera (a_n) la suite des quotients incomplets et (θ_n) la suite des quotients complets. On conviendra parfois que $\theta_0 = \theta$.
Les nombres p_n et q_n désigneront toujours les entiers définis précédemment.

Lemme 0.0.8 *Pour tout entier $n \geqslant 1$, on a la relation :*

$$(\theta - p_n$$

Théorème 0.0.12 (Meilleure approximation.) *Quel que soit l'entier $n \geqslant 1$, pour tout entier p et tout entier q tel que $0 < q < q_{n+1}$ on a :*

$$| q\theta - p | \geqslant | q_n\theta - p_n | \tag{12}$$

De plus l'inégalité est une égalité si et seulement si $p = p_n$ et $q = q_n$.

Démonstration: □ Il existe deux entiers u et v tels que

$$\begin{aligned} p &= up_n + vp_{n+1} \\ q &= uq_n + vq_{n+1} \end{aligned}$$

Ceci résulte du fait que ce système d'inconnues (u, v) a comme déterminant $(-1)^n$, qui est inversible dans $\mathbb{Z}$.

Si $u = 0$ la seconde équation se réduit à $q = vq_{n+1}$ qui est incompatible avec l'hypothèse $0 < q < q_{n+1}$. Donc u est non nul.

Si $v = 0$ alors $p/q = p_n/q_n$ qui correspond au cas d'égalité.

On suppose donc dans la suite u et v non nuls. Montrons que dans ce cas ils sont de signes contraires. Ceci découle de l'hypothèse $0 < q < q_{n+1}$. En effet, elle s'écrit $uq_n + vq_{n+1} < q_{n+1}$, soit : $uq_n < (1 - v)q_{n+1}$.

— Donc si $v \geqslant 1$: $uq_n < 0$ et donc u est strictement négatif.

— Sinon v est négatif on nul et donc strictement négatif, et l'hypothèse $q > 0$, qui s'écrit $uq_n + vq_{n+1} > 0$, ce qui implique $u > 0$.

Un calcul immédiat montre que

$$q\theta - p = \theta(uq_n + vq_{n+1}) - (up_n + vp_{n+1}) = u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})$$

Comme u et v sont de signes contraires, et que $(q_n\theta - p_n)$ et $q_{n+1}\theta - p_{n+1})$ sont également de signes contraires, on a

$$\begin{aligned} | q\theta - p | &= | u(q_n\theta - p_n) | + | v(q_{n+1}\theta - p_{n+1}) | \\ &> | (q_{n+1}\theta - p_{n+1}) | \end{aligned}$$

car v est non nul, et que $u(q_n\theta - p_n)$ est également non nul. □

Proposition 0.0.13 *Pour tout entier l'une des réduites $f_n = p_n/q_n$ ou $f_{n+1} = p_{n+1}/q_{n+1}$ satisfait à :*

$$| \theta - p/q | < 1/2q^2$$

Démonstration: □ La proposition (0.0.11) montre que $q_n\theta - p_n$ et $q_{n+1}\theta - p_{n+1}$ sont de signes contraires. Donc, on a les égalités :

$$\begin{aligned} \left| \theta - \frac{p_n}{q_n} \right| + \left| \theta - \frac{p_{n+1}}{q_{n+1}} \right| &= \left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| \\ &= \frac{1}{q_n q_{n+1}} \end{aligned}$$

Or, si a et b sont deux réels distincts : $2ab < a^2 + b^2$. Donc : $\dfrac{1}{q_n q_{n+1}} < \dfrac{1}{2q_n^2} + \dfrac{1}{2q_{n+1}^2}$. Ce qui, compte tenu de l'inégalité précédente démontre le résultat voulu. □

Cette proposition admet une réciproque qui sera utilisée dans la résolution de l'équation de Pell-Fermat.

Proposition 0.0.14 *Soient p et $q > 0$ deux entiers. La relation $|\,\theta - p/q\,| < 1/2q^2$ implique que p/q est une réduite de θ.*

Démonstration: □ Il existe un entier n tel que $q_n \leqslant q < q_{n+1}$.

Or, en utilisant l'inégalité triangulaire :

$$\begin{aligned}\left|\frac{p}{q} - \frac{p_n}{q_n}\right| &\leqslant \left|\theta - \frac{p}{q}\right| + \left|\theta - \frac{p_n}{q_n}\right| \\ &= \frac{1}{q}|\,q\theta - p\,| + \frac{1}{q_n}|\,q_n\theta - p_n\,| \\ &\leqslant (\frac{1}{q} + \frac{1}{q_n})|\,q\theta - p\,| \quad \text{D'après (0.0.12).}\end{aligned}$$

D'où en chassant les dénominateurs :

$$\begin{aligned}|\,pq_n - qp_n\,| &\leqslant (q + q_n)|\,q\theta - p\,| \\ &< 2q \times \frac{1}{2q^2} = \frac{1}{q} \leqslant 1\end{aligned}$$

D'où finalement : $|\,pq_n - qp_n\,| < 1$. Comme $pq_n - qp_n$ est un entier, ceci implique $pq_n - qp_n = 0$ et donc $\frac{p}{q} = \frac{p_n}{q_n}$. □

§ 4. Nombres algébriques quadratiques

Rappelons qu'un nombre complexe θ est dit algébrique de degré 2 s'il existe un polynôme de degré 2, à coefficients rationnels, irréductible sur $\mathbb{Q}$, dont θ est une racine. Autrement dit : θ n'est pas rationnel et il existe des rationnels $a \neq 0$, b et c tels que $a\theta^2 + b\theta + c = 0$. Après avoir réduit a, b, c au même dénominateur, on peut supposer en fait que a, b, c sont des entiers. Dans ce cas on dit aussi que θ est quadratique. Les exemples standards sont i, $j = e^{\frac{2i\pi}{3}}$, ainsi que tous les nombres réels de la forme $\sqrt{d}$ où d est un entier qui n'est pas le carré d'un entier. Dans la suite ce sont ces nombres qui seront envisagés.

Le but est de démontrer que θ étant un nombre réel, le développement de θ en fraction continue est périodique à partir d'un certain rang si et seulement si θ est quadratique.

Notations et définitions. Soit θ un nombre réel, non rationnel, et (a_k) la suite de ses quotients partiels. Le développement de θ en fraction continue est dit périodique à partir d'un certain rang, si il existe deux entiers $r \geqslant 0$ et $m \geqslant 1$ tels que $a_{m+k} = a_k$ pour tout entier $k \geqslant r$. Dans ce cas, on notera $\theta = [a_0, \ldots, a_{r-1}, \overline{a_r \ldots, a_{r+m-1}}]$. On dira que le développement de θ est purement périodique si il existe un entier $m \geqslant 1$ tel que pour tout entier k : $\quad a_{m+k} = a_k$.

Proposition 0.0.15 *Soit θ un réel non rationnel. Si le développement de θ en fraction continue est périodique à partir d'un certain rang, θ est quadratique.*

Démonstration: □ Supposons dans un premier temps que le développement soit purement périodique. Soit donc $\varphi = [\overline{a_0 \ldots, a_{m-1}}]$.

On a donc l'égalité :

$$\varphi = [a_0 \ldots, a_{m-1}, \varphi]$$

Donc, en se souvenant des notations du premier paragraphe, en supposant $m \geqslant 2$:

$$\varphi = F_{m-1}(a_0 \ldots, a_{m-1}, \varphi)$$

Cette dernière fraction étant égale à

$$F_{m-1}(a_0 \ldots, a_{m-1}, \varphi) = \frac{P_{m-1}(a_0 \ldots, a_{m-1}, \varphi)}{Q_{m-1}(a_0 \ldots, a_{m-1}, \varphi)} = \frac{\varphi\, p_{m-1} + p_{m-2}}{\varphi\, q_{m-1} + q_{m-2}}$$

Donc, dans le $m \geqslant 2$, φ est bien racine d'un polynôme de degré 2. Dans le cas où $m < 2$, nécessairement $m = 1$ et dans ce cas $\phi = [\overline{a_0}]$ qui vérifie donc $\varphi = a_0 + 1/\varphi$ et est encore racine d'un polynôme de degré 2.

Dans le cas général où $\theta = [a_0, \ldots, a_{r-1}, \overline{a_r \ldots, a_{r+m-1}}]$, notons $\varphi = [\overline{a_r \ldots, a_{r+m-1}}]$ qui est donc racine d'un polynôme de degré 2 à coefficients entiers. Or θ est une fonction homographique de φ, à coefficients entiers. Il est immédiat de vérifier que θ est aussi racine d'un polynôme de degré 2 à coefficients entiers. □

Théorème 0.0.16 *Soit θ un nombre irrationnel, algébrique de degré 2 sur $\mathbb{Q}$. Alors son développement en fraction continue est périodique à partir d'un certain rang.*

Démonstration: □ Soient a, b, c des entiers non tous nuls tels que $a\theta^2 + b\theta + c = 0$. On considère la forme quadratique de deux variables définie par

$$f(x, y) = ax^2 + bxy + cy^2$$

Par hypothèse, on a donc : $f(\theta, 1) = 0$

Si n est un entier, on considère la forme quadratique f_n définie par

$$f_n(x, y) = f(xp_n + yp_{n-1}, xq_n + yq_{n-1})$$

Cette forme quadratique s'écrit sous la forme

$$f_n(x, y) = a_n x^2 + b_n xy + c_n y^2$$

En se souvenant des formules démontrées au début, il est clair que $f_n(\theta_{n+1}, 1) = f(\theta, 1) = 0$.

La démonstration du théorème consiste à montrer que les formes quadratiques f_n sont en nombres fini. Dans ce cas il y a un nombre fini de nombres φ tels que $f_n(\varphi, 1) = 0$ donc un nombre fini de quotients complets, ce qui implique le résultat. Pour démontrer ceci, on montre dans un premier temps que les entiers (a_n) forment une suite bornée.

On a la relation $a_n = f_n(1, 0) = f(p_n, q_n) = q_n^2 f(p_n/q_n, 1)$. Or, comme $f(\theta, 1) = 0$, on a aussi :

$f(p_n/q_n, 1) = f(p_n/q_n, 1) - f(\theta, 1) = (p_n/q_n - \theta)\big(a(p_n/q_n + \theta) + b\big)$

D'autre part, pour tout entier n : $|\, p_n/q_n - \theta \,| \leqslant 1$. (Revoir éventuellement la proposition (0.0.9) page 5). Et donc $\big|\, \big(a(p_n/q_n + \theta) + b\big) \,\big| \leqslant |\, a \,|(2|\, \theta \,| + 1) + |\, b \,|$. Notons K cette constante.

D'après ce qui précède on a donc :

$$|\, a_n \,| \leqslant q_n^2 |\, p_n/q_n - \theta \,| \times K$$

Or la même proposition montre que $|\, p_n/q_n - \theta \,| \leqslant 1/q_n^2$. On a donc montré finalement que

$$|\, a_n \,| \leqslant |\, a \,|(2|\, \theta \,| + 1) + |\, b \,|.$$

Il en résulte bien que la suite (a_n) ne prend qu'un nombre fini de valeurs.

La définition de f_n montre que $c_n = f(p_{n-1}, q_{n-1}) = a_{n-1}$. Donc la suite (c_n) ne prend également qu'un nombre fini de valeurs.

Pour démontrer que la suite (b_n) ne prend qu'un nombre fini de valeurs, le résultat essentiel est que les deux formes quadratiques f et f_n ont même discriminant, à savoir que l'on a l'égalité :

$$b^2 - 4ac = b_n^2 - 4a_n c_n$$

Cette égalité se démontre par un petit calcul. On peut également remarquer que si A et A_n désignent les matrices respectives des formes quadratiques f et f_n, il suffit de montrer que les matrices A et A_n ont même déterminant. Or f_n se déduit de f par changement de base. La

matrice P de changement de base est de déterminant $(-1)^{n+1}$. La relation $A_n = P^t A P$ montrent que A et A_n ont même déterminant.

Donc la suite (b_n) ne prend également qu'un nombre fini de valeurs.

Il en résulte que la suite de formes quadratiques (f_n) ne prend également qu'un nombre fini de valeurs et donc que la suite $(\theta)_n$ ne prend qu'un nombre fini de valeurs. Il existe donc deux entiers distincts r et s tels que $\theta_r = \theta_s$, ce qui implique que la suite (a_n) est périodique à partir d'un certain rang. □

Définition 0.0.17 *Soit θ un nombre quadratique et f son polynôme minimal qui est donc de degré deux. On appelle conjugué de θ l'autre racine de f. Cette autre racine sera notée θ'.*

Lemme 0.0.18 *Soit θ un nombre quadratique strictement plus grand que 1 et $f(x) = x^2+\alpha x+\beta$ son polynôme minimal. Soient a la partie entière de θ et φ le nombre réel tel que $\theta = a + 1/\varphi$. Alors φ est quadratique, strictement plus grand que 1 et son conjugué est donné par la formule suivante :*

$$\varphi' = \frac{1}{\theta' - a}$$

Démonstration: □ On considère le changement de variable : $x = a + 1/y$. Il est clair que $g(y) = y^2\, f(a + 1/y)$ est un polynôme en y de degré deux, à coefficients rationnels et que $g(\varphi) = 0$. Comme φ n'est pas rationnel, g est irréductible sur $\mathbb{Q}$. □

Proposition 0.0.19 *Soit θ un nombre quadratique. Les conditions suivantes sont équivalentes.*

1. *Le développement de θ est purement périodique.*
2. *Le nombre θ vérifie les deux relations : $\theta > 1$ et $-1 < \theta' < 0$.*

Démonstration: □ Démontrons l'implication 1) $\Longrightarrow$ 2). Supposons donc que $\theta = [\overline{a_0 \ldots, a_{m-1}}]$, où m est supérieur ou égal 1. Comme $a_0 = a_m$ on a donc $a_0 \geqslant 1$ et donc $\theta > 1$. Supposons dans un premier temps que m soit supérieur ou égal à 2. On a alors l'égalité : $\theta = [a_0 \ldots, a_{m-1}, \theta]$ et donc

$$\theta = \frac{\theta\, p_{m-1} + p_{m-2}}{\theta\, q_{m-1} + q_{m-2}}$$

et θ vérifie donc l'équation :

$$q_{m-1}\, \theta^2 + (q_{m-2} - p_{m-1})\theta - p_{m-2} = 0$$

Notons $f(x) = q_{m-1}\, x^2 + (q_{m-2} - p_{m-1})x - p_{m-2}$. L'une des racines de f est θ et l'autre θ'. Le produit des racines est $-p_{m-2}/q_{m-2}$ qui est strictement négatif. Donc $\theta' < 0$. De plus $f(0) < 0$ et il est immédiat de vérifier que la suite de terme général $p_n + q_n$ est strictement croissante et donc que $f(-1) > 0$. Il en résulte que $-1 < \theta' < 0$. Dans le cas où la période est $m = 1$ on a $\theta = a_0 + \dfrac{1}{\theta}$ avec $a_0 \geqslant 1$, et donc $\theta^2 - a_0\theta - 1 = 0$ ce qui implique $-1 < \theta' < 0$.

La réciproque est plus délicate. Supposons donc que le nombre θ vérifie les deux relations : $\theta > 1$ et $-1 < \theta' < 0$. Soit (θ_k) la suite des quotients complets de θ, et (a_k) la suite des quotients incomplets. Le lemme précédent permet de montrer par récurrence que pour tout entier k, le conjugué θ'_k est dans $]-1, 0[$ et que de plus on a la relation

$$\theta'_{k+1} = \frac{1}{\theta'_k - a_k}$$

Cette égalité implique

$$\frac{-1}{\theta'_{k+1}} = a_k - \theta'_k$$

comme $-\theta'_{k+1}$ appartient à $]0,1[$ cette égalité montre que a_k est la partie entière de $\dfrac{-1}{\theta'_{k+1}}$.

Comme θ est quadratique, il existe deux entiers m et n distincts tels que $\theta_n = \theta_m$. On a donc également $\theta'_n = \theta'_m$, et donc $\dfrac{-1}{\theta'_n} = \dfrac{-1}{\theta'_m}$, ce qui implique $a_{n-1} = a_{m-1}$ d'après ce qui précède. Mais les deux égalités $a_{n-1} = a_{m-1}$ et $\theta_n = \theta_m$ impliquent que $\theta_{n-1} = \theta_{m-1}$. Il en résulte, en supposant par exemple $m > n$ que $\theta_{m-n} = \theta_0$ et donc que le développement de θ est purement périodique. □

§ 5. L'équation de Pell-Fermat

Dans toute la suite d désigne un entier naturel qui n'est pas le carré d'un entier, ce qui implique $d \geqslant 2$.

Il s'agit de trouver les solutions, en nombres entiers, de l'équation

(Pell-Fermat) $$x^2 - dy^2 = 1$$

Lemme 0.0.20 *Soit $d \geqslant 2$ un entier naturel qui n'est pas le carré d'un entier naturel. Le développement en fractions continues de $\sqrt{d}$ est périodique à partir du rang 1, c'est à dire de la forme*

$$\sqrt{d} = [a_0, \overline{a_1, \ldots, a_m}]$$

Démonstration: □ Notons a_0 la partie entière de $\sqrt{d}$, et φ le premier quotient complet de $\sqrt{d}$. On a donc $\sqrt{d} = a_0 + 1/\varphi = [a_0, \varphi]$. Il suffit donc de montrer que φ, qui est quadratique, est purement périodique. Il est clair que $\varphi > 1$. Un calcul immédiat montre que φ est racine du polynôme $P(X) = (a_0^2 - d)X^2 + 2a_0X + 1$. D'autre part on a $P(0) = 1$ et $P(-1) = (a_0 - 1)^2 - d < 0$. Donc P a une racine dans l'intervalle $]-1, 0[$ et il, suffit d'appliquer la proposition précédente (0.0.19)). □

Lemme 0.0.21 *Soit (x, y) un couple d'entiers naturels solution de l'équation de Pell-Fermat. Alors si y est non nul, x/y est une réduite de $\sqrt{d}$.*

Autrement dit, en conservant les notations habituelles, il existe un entier n tel que $x = p_n$ et $y = q_n$.

Démonstration: □ L'égalité $x^2 - dy^2 = 1$ montre que $x > y\sqrt{d} > y$. De plus cette égalité implique les relations suivantes :

$$\left| x - y\sqrt{d} \right| = x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}} < \frac{1}{2y}$$

et donc :

$$\left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{2y^2}$$

La proposition (0.0.14) montre que x/y est une réduite de $\sqrt{d}$. Comme de plus x et y sont premiers entre eux ceci implique le résultat. □

Dans la suite, pour retrouver les notations des paragraphes précédents, on note $\theta = \sqrt{d}$ et $\sqrt{d} = [a_0, \overline{a_1 \ldots, a_m}]$ le développement en fraction continues de $\sqrt{d}$. On a donc $a_{m+k} = a_k$ et $\theta_{m+k} = \theta_k$ pour tout entier $k \geqslant 1$. On supposera également que m est la plus petite période.

Théorème 0.0.22 *Soient d un entier naturel qui n'est pas un carré et m la plus petite période du développement de $\sqrt{d}$ en fraction continue. Soient n un entier naturel non nul et $f_n = p_n/q_n$ une réduite de $\sqrt{d}$. Pour que (p_n, q_n) soit solution de l'équation de Pell-Fermat il faut et il suffit que les deux conditions suivantes soient réalisées :*

1. *L'entier n est impair.*
2. *L'entier $n+1$ est un multiple de m.*

Démonstration: □ Soit donc $f_n = p_n/q_n$ une réduite de $\sqrt{d}$.

Si (p_n, q_n) est solution de l'équation de Pell-Fermat, on a $p_n > q_n\sqrt{d}$. La réduite f_n est donc strictement plus grande que $\sqrt{d}$. Donc n doit être impair. Voir éventuellement la proposition (0.0.9).

On a déjà utilisé souvent la relation

$$\sqrt{d} = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n(\theta_{n+1}q_n + q_{n-1})}$$

et donc :

$$\theta_{n+1}\,(p_n - q_n\sqrt{d}) = q_{n-1}\sqrt{d} - p_{n-1}$$

En multipliant cette égalité par $(p_n + q_n\sqrt{d})$ et en tenant compte du fait que (p_n, q_n) est solution on obtient

$$\theta_{n+1} = \sqrt{d}(p_nq_{n-1} - p_{n-1}q_n) + b$$

où b est un entier. Compte tenu de l'égalité $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n+1}$ et du fait que n est impair on a donc :

$$\theta_{n+1} = \sqrt{d} + b$$

où b est un entier. Or on a également les relations

$$\theta_{n+1} = a_{n+1} + \frac{1}{\theta_{n+2}} \quad \text{et} \quad \sqrt{d} = a_0 + \frac{1}{\theta_1}$$

L'égalité précédente s'écrit donc :

$$a_{n+1} + \frac{1}{\theta_{n+2}} = a_0 + b + \frac{1}{\theta_1}$$

Ce qui implique $a_{n+1} = a_0 + b$ et $\theta_{n+2} = \theta_1$. L'entier m étant la plus petite période la dernière égalité implique que $n+2$ est de la forme $km+1$, autrement dit que n est de la forme $km-1$.

Réciproquement, si ces deux conditions sont vérifiées, les calculs ci-dessus se remontent : si n est de la forme $km-1$, ceci signifie que $\theta_{n+2} = \theta_1$ et donc :

$$\frac{1}{\theta_{n+2}} = \frac{1}{\theta_1} = \sqrt{d} - a_0$$

On a donc les égalités :

$$\sqrt{d} = \frac{p_{n+1}\theta_{n+2} + p_n}{q_{n+1}(\theta_{n+2}q_{n+1} + q_n)} = \frac{p_{n+1} + \dfrac{p_n}{\theta_{n+2}}}{q_{n+1} + \dfrac{q_n}{\theta_{n+2}}}$$

$$= \frac{p_{n+1} + \dfrac{p_n}{\theta_1}}{q_{n+1} + \dfrac{q_n}{\theta_1}} = \frac{p_{n+1} + p_n(\sqrt{d} - a_0)}{q_{n+1} + q_n(\sqrt{d} - a_0)}$$

Ce qui montre que

$$(q_{n+1} - a_0q_n)\sqrt{d} + dq_n = p_n\sqrt{d} + (p_{n+1} - a_0p_n)$$

ce qui implique les relations :

$$q_{n+1} - a_0q_n = p_n$$
$$p_{n+1} - a_0p_n = dq_n$$

Par combinaison linéaire de ces deux équations on obtient donc :

$$p_n^2 - dq_n^2 = -(p_{n+1}q_n - p_nq_{n+1}) = -(-1)^{n+2} = (-1)^{n+1}$$

et comme n est impair, on a donc

$$p_n^2 - dq_n^2 = 1.$$

□

L'équation $x^2 - dy^2 = -1$.

Contrairement à la précédente cette équation ne possède pas toujours de solution entières. Une condition nécessaire évidente : si cette équation possède une solution dans $\mathbb{Z}^2$, -1 est un carré modulo d. Cette condition n'est pas suffisante. Il est immédiat de montrer que l'équation $x^2 - 5^2y^2 = -1$ ne possède pas de solutions entières, bien que $7^2 = -1$ modulo 5^2. Évidemment 5^2 est un carré. Après avoir vu le théorème suivant, il est facile de montrer que l'équation $x^2 - 34y^2 = -1$ ne possède pas de solutions entières, bien que $13^2 = -1$ modulo 34.

Théorème 0.0.23 *Soient d un entier naturel qui n'est pas un carré et m la plus petite période du développement de $\sqrt{d}$ en fraction continue.*

1. *Si m est un entier pair l'équation $x^2 - dy^2 = -1$ ne possède pas de solution dans $\mathbb{Z}^2$.*

2. *Si m est un entier impair l'équation $x^2 - dy^2 = -1$ possède une infinité de solutions dans $\mathbb{Z}^2$. Plus précisément, si n est un entier naturel non nul et $f_n = p_n/q_n$ une réduite de $\sqrt{d}$, pour que (p_n, q_n) soit solution de l'équation $x^2 - dy^2 = -1$ il faut et il suffit que les deux conditions suivantes soient réalisées :*

i) L'entier n est pair.

ii) L'entier $n + 1$ est un multiple de m.

Démonstration: □ Soit (x, y) une solution de l'équation $x^2 - dy^2 = -1$. Quitte à changer x en $-x$ et y en $-y$ on peut supposer que x et y sont des entiers naturels. Il est clair que y est non nul et donc supérieur ou égal à 1. Dans ce cas, d'après la proposition 0.0.14, le nombre $\frac{x}{y}$ est une réduite du développement de $\sqrt{d}$.

Ces remarques étant faites, la démonstration est tout à fait analogue à celle du théorème précédent.

Soit n un entier naturel. Si (p_n, q_n) est solution de l'équation de $x^2 - dy^2 = -1$, on a $p_n < q_n\sqrt{d}$. La réduite f_n est donc strictement plus petite que $\sqrt{d}$. Donc n doit être pair. Voir éventuellement la proposition (0.0.9). D'autre part, on a

$$\theta_{n+1}\,(p_n - q_n\sqrt{d}) = q_{n-1}\sqrt{d} - p_{n-1}$$

En multipliant cette égalité par $(p_n + q_n\sqrt{d})$ et en tenant compte du fait que (p_n, q_n) est solution on obtient

$$-\theta_{n+1} = \sqrt{d}(p_nq_{n-1} - p_{n-1}q_n) + c = (-1)^{n+1}\sqrt{d} + c$$

où c est un entier. Comme n est pair, cette relation se réduit à

$$\theta_{n+1} = \sqrt{d} - c$$

Comme dans la démonstration précédente, on en déduit la relation

$$a_{n+1} + \frac{1}{\theta_{n+2}} = a_0 - c + \frac{1}{\theta_1}$$

Ce qui implique $a_{n+1} = a_0 - c$ et $\theta_{n+2} = \theta_1$. L'entier m étant la plus petite période la dernière égalité implique que $n+2$ est de la forme $km+1$. L'entier n étant pair, cette égalité n'est jamais réalisée si la période m est paire.

Donc, si m est pair, il n'existe pas de réduite $\frac{p_n}{q_n}$ telle que (p_n, q_n) soit solution de l'équation $x^2 - dy^2 = -1$. Les remarques préliminaires montrent que si m est pair, cette équation ne possède pas de solution dans $\mathbb{Z}^2$.

Supposons donc que la période m est impaire. Pour que (p_n, q_n) soit solution de l'équation $x^2 - dy^2 = -1$ il faut donc que l'entier n soit de la forme $km - 1$.

Réciproquement, en supposant m pair, si n est un entier pair et si $n + 1$ est un multiple de m, comme dans la démonstration du théorème précédent, les calculs ci-dessus se remontent et donc dans ce cas (p_n, q_n) est une solution de l'équation $x^2 - dy^2 = -1$. (Le détail des calculs est laissé au lecteur). □

§ 6. Quelques exemples numériques

Les calculs effectifs concernant les développements en fraction continue sont rapidement pénibles bien qu'élémentaires. Le logiciel Maple possède un module qui fait tous ces calculs.

1. On considère l'équation $x^2 - 34y^2 = 1$. Le développement en fraction continue de $\sqrt{34}$ est

$$\sqrt{34} = [5, \overline{1, 4, 1, 10}]$$

La plus petite période est donc $m = 4$. Le théorème précédent montre que l'équation $x^2 - 34y^2 = -1$ ne possède pas de solution dans $\mathbb{Z}^2$, bien que -1 soit un carré modulo 34 car $13^2 + 1 = 170 = 34 \times 5$.

2. On considère l'équation $x^2 - 31y^2 = 1$. Maple donne le développement de $\sqrt{31}$ en fraction continue :

$$[5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

Donc la plus petite période est $m = 8$. Le théorème 0.0.22 montre que les solutions dans $\mathbb{N}^2$, autres que $(1, 0)$, sont données par les numérateurs et dénominateurs des réduites f_n où l'entier n est impair et de la forme $8k - 1$. Le plus petit de ces entiers est 7. Maple donne $f_7 = \frac{1520}{273}$. le couple d'entier $(1520, 273)$ est solution de l'équation $x^2 - 31y^2 = 1$.

Comme -1 n'est pas un carré modulo 31, l'équation $x^2 - 31y^2 = -1$ ne possède pas de solution entière.

3. On considère l'équation $x^2 - 53y^2 = -1$. Maple donne le développement de $\sqrt{53}$ en fraction continue : $\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$. Donc la plus petite période est $m = 5$ donc impaire. Le théorème 0.0.23 montre que que l'équation possède des solutions entières et que les solutions dans $\mathbb{N}^2$ sont données par les numérateurs et dénominateurs des réduites f_n où l'entier n est pair et de la forme $5k - 1$. Le plus petit de ces entiers est 4. Maple donne $f_4 = \frac{182}{25}$. Donc le couple d'entier $(182, 25)$ est solution de l'équation $x^2 - 53y^2 = -1$.

En ce qui concerne l'équation de Pell-Fermat $x^2 - 53y^2 = 1$, les solutions dans $\mathbb{N}^2$, autres que $(1, 0)$, sont données par les numérateurs et dénominateurs des réduites f_n où l'entier n est impair et de la forme $5k - 1$. Le plus petit de ces entiers est $n = 9$. Toujours grâce à Maple on obtient : $f_9 = \frac{66249}{9100}$ et donc $(66249, 9100)$ est solution de $x^2 - 53y^2 = 1$.

Les inversibles de l'anneau $\mathbb{Z}[\sqrt{d}\,]$.

L'ensemble des nombres réels de la forme $x + \sqrt{d}y$ forment un sous-anneau du corps des réels noté $\mathbb{Z}[\sqrt{d}\,]$. L'entier d n'étant pas le carré d'un entier, tout élément z de $\mathbb{Z}[\sqrt{d}\,]$ s'écrit de manière *unique* sous la forme $z = x + y\sqrt{d}$ où x et y sont deux entiers relatifs. On peut donc définir une application, appelée conjugaison, de $\mathbb{Z}[\sqrt{d}\,]$ dans lui-même qui à $z = x + y\sqrt{d}$ associe $\overline{z} = x - y\sqrt{d}$. Il est immédiat de vérifier la conjugaison est un homomorphisme d'anneaux. Ensuite on définit la norme (au sens de l'arithmétique) d'un élément z de $\mathbb{Z}[\sqrt{d}\,]$ par $\mathrm{N}(z) = z\overline{z}$. Donc si z s'écrit $z = x + y\sqrt{d}$ où x et y sont deux entiers relatifs, on a la relation $\mathrm{N}(z) = x^2 - dy^2$. L'application

$\mathrm{N} : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{Z}$ est donc multiplicative. Il est facile de vérifier qu'un élément de $\mathbb{Z}[\sqrt{d}\,]$ est inversible si et seulement si sa norme l'est. Comme l'ensemble des éléments inversibles de $\mathbb{Z}$ est $\{-1,+1\}$ il en résulte qu'un élément $z = x+y\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}\,]$ est inversible si et seulement si (x,y) est solution de l'équation $x^2-dy^2 = \pm 1$. Ainsi l'équation de Pell-Fermat revient à déterminer les inversibles de l'anneau $\mathbb{Z}[\sqrt{d}\,]$ qui sont de norme $+1$ et résoudre, en nombres entiers, l'équation $x^2-dy^2 = -1$ revient à déterminer les inversibles de l'anneau $\mathbb{Z}[\sqrt{d}\,]$ qui sont de norme -1. Le théorème classique est le suivant.

Théorème 0.0.24 *Soit d un entier qui n'est pas le carré d'un entier. Il existe un inversible u de l'anneau $\mathbb{Z}[\sqrt{d}\,]$, strictement plus grand que 1, tel que l'ensemble des inversibles de norme $+1$ soit l'ensemble* $\{\pm u^n \mid n \in \mathbb{Z}\}$.

Soient x et y sont des entiers et $z = x+y\sqrt{d}$. Il est clair que si z est un inversible de norme 1 alors, $-z$, $\frac{1}{z}$ et $-\frac{1}{z}$ sont de norme 1. Ceci revient à dire que si (x,y) est solution de l'équation de Pell-Fermat alors $(-x,-y)$, $(x,-y)$ ainsi que $(-x,y)$ sont également des solutions.

L'élément u du théorème, s'il existe, est le plus petit élément de norme 1 qui est strictement plus grand que 1. Le théorème 0.0.22, prouve l'existence d'un couple (x,y) d'entiers naturels non nuls tel que $z = x+y\sqrt{d}$ soit de norme 1. Rappelons comment, à partir de ce résultat, on retrouve le théorème 0.0.26.

Lemme 0.0.25 *Soient $z = x+y\sqrt{d}$ et $z' = x'+y'\sqrt{d}$ où x,x',y,y' des entiers naturels. On suppose que $\mathrm{N}(z) = \mathrm{N}(z') = 1$.*

L'inégalité $z < z'$ équivaut aux deux inégalités : $x < x'$ et $y < y'$.

Démonstration: □ L'hypothèse $\mathrm{N}(z) = \mathrm{N}(z')$ s'écrit $x'^2 - x^2 = (y'^2 - y^2)\sqrt{d}$. On remarque tout d'abord que x et x' sont distincts ainsi que y et y'. En effet l'égalité $x = x'$ équivaut à $x'^2 - x^2 = 0$ (car x et x' sont positifs) et de même l'égalité $y = y'$ équivaut à $y'^2 - y^2 = 0$.

Supposons $z < z'$. L'égalité $(x-x')(x+x') = (y-y')(y'+y)\sqrt{d}$ implique que $(x'-x)$ et $(y'-y)$ sont de même signe, et donc nécessairement strictement positifs.

La réciproque est évidente. □

Il en résulte en particulier que si x et y sont des entiers naturels l'inégalité $1 < x+y\sqrt{d}$ implique $y > 0$. Si a est un réel positif, l'ensemble des éléments de norme 1 qui sont plus petit que a est fini. Donc l'ensemble des éléments de norme 1 qui sont strictement plus grands que 1 possède un plus petit élément. Notons u ce plus petit élément. Si z est positif de norme 1 il existe un entier relatif n tel que $u^n \leqslant z < u^{n+1}$. Soit $v = \frac{z}{u^n}$ qui est positif de norme 1 et vérifie $1 \leqslant v < 1$. La définition de u montre que $v = 1$ et donc $z = u^n$.

Le théorème précédent (0.0.26) est une conséquence immédiate de ceci. On démontre de la même manière le théorème suivant.

Théorème 0.0.26 *Soit d un entier qui n'est pas le carré d'un entier.*

Si l'ensemble des éléments de l'anneau $\mathbb{Z}[\sqrt{d}\,]$ de norme -1 est non vide :

1. *Il existe un inversible v de cet l'anneau, strictement plus grand que 1, tel que l'ensemble des inversibles de norme -1 soit l'ensemble* $\{\pm u^{2n+1} \mid n \in \mathbb{Z}\}$.

2. *De plus $u = v^2$ est de norme 1 et c'est le plus petit de ces éléments, de norme -1, strictement plus grand que 1.*

Note Historique. Quelques remarques concernant la dénomination « équation de Pell-Fermat ». De l'avis unanime des historiens, Pell n'a apporté aucune contribution concernant le problème. Certains disent que Fermat (1601-1665) a montré que l'équation possède une infinité de solutions, mais d'autres affirment que Fermat n'a guère contribué plus que Pell à la résolution de l'équation.

La première résolution complète est due à Lagrange (1736-1813). Cependant, cinq siècles avant Fermat, le mathématicien indien Bhāskara (1114-1185) savait à peu près tout de cette équation. Plus précisément, il connaissait un algorithme, qui pour un entier d donné permet de trouver une solution non triviale de l'équation. Ce que ne savait sans doute pas Bhāskara, c'est que l'algorithme donne, quelque soit l'entier d une solution non triviale. Le lecteur pourra trouver plus de détails, dans le livre de V.S.Varadarajan.

Bibliographie

Samuel Pierre – *Théorie algébrique des nombres.* Hermann ($\star\star$).
Alan Baker – *A concise introduction to the theory of numbers.* Cambrige University Press (1984).
Descombes Roger – *éléments de théorie des nombres.* PUF (1986).
Varadarajan – *Algebra in Ancient and Modern Times.* Hindustan Book Agency (1997).

M.Couchouron