Fractions continues

Margaret Bilu

21 novembre 2015

Dans ce petit cours, nous allons parler de fractions continues : ce sont des nombres de la forme

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

où $a_0, a_1, \ldots$ sont des entiers, tous strictement positifs sauf peut-être a_0. Les trois petits points signifient que le nombre de traits de fraction peut être fini, ou bien infini. Nous allons tout d'abord étudier ces objets quand le nombre de traits de fraction est fini, et montrer que tout nombre rationnel (c'est-à-dire toute fraction) s'écrit sous cette forme. Ensuite, nous allons voir ce que cet objet signifie dans le cas où le nombre de traits de fraction est infini, et nous allons expliquer pourquoi tous les nombres peuvent s'écrire sous cette forme. Ensuite, nous allons passer à l'application principale des fractions continues, en regardant comment elles peuvent servir pour trouver des approximations rationnelles d'un nombre. De cela découle en particulier la résolution des équations de Pell-Fermat, que nous allons voir dans la dernière partie.

Avant de nous lancer, un petit historique : les fractions continues apparaissent déjà dans les travaux de quelques mathématiciens du 16e siècle, mais c'est Christian Huygens (1629-1895), mathématicien, physicien et astronome néerlandais, qui le premier les a utilisées de manière importante pour approximer des nombres. Huygens est cependant surtout connu pour ses nombreux autres travaux, au sujet des ondes mais aussi du pendule oscillant, qui l'ont d'ailleurs amené à inventer l'horloge à balancier. En 1666, il a été nommé par Louis XIV membre de l'Académie Royale des Sciences à Paris, et en 1680 il entreprit le projet de construire un planétarium pour celle-ci : ce planétarium était une maquette mobile du système solaire tel qu'on le connaissait à l'époque. On pouvait y voir les orbites des planètes Mercure, Venus, Terre, Mars, Jupiter et Saturne, ainsi que de quelques lunes déjà connues (une des lunes de Saturne, Titan, avait d'ailleurs été découverte par Huygens lui-même quelques années auparavant). Des petites boules représentant les planètes et mises en mouvement par un système d'engrenages bougeaient le long des orbites. C'est pour calculer le nombre de dents optimal pour chaque engrenage (pas trop grand, pour que ce soit possible de le fabriquer, mais suffisamment précis pour que les planètes puissent se mouvoir de manière fluide et cohérente avec la réalité observée) qu'Huygens a utilisé les fractions continues. Il avait mesuré de manière assez précise le temps que mettait chaque planète à faire le tour autour du Soleil. Afin de construire l'engrenage combinant deux roues dentées correspondant à deux des planètes, il calculait le rapport de leurs durées de révolution, ensuite à l'aide d'une fraction continue, il approximait ce dernier par une fraction $\frac{p}{q}$ avec p et q des entiers pas trop grands. L'engrenage était alors constitué d'une roue dentée avec p dents, et d'une autre avec q dents, et le rapport entre les durées de révolution des deux roues était $\frac{p}{q}$. Par exemple, le rapport entre les durées de révolution de Saturne et de la Terre était approximativement $\frac{77708431}{2640858} \approx 29,425$. Il aurait été très difficile de construire des roues avec 77708431 et 2640858 dents. En revanche, grâce aux fractions continues, on trouve que la fraction $\frac{206}{7} \approx 29,428$ en donne une approximation à 0,003 près. Finalement, les roues correspondantes avaient donc respectivement 206 et 7 dents.

Ensuite, la théorie des fractions continues a été grandement développée par Euler et par Lagrange.

1 Fractions continues et leurs réduites

1.1 Fractions continues finies

Définition 1.1. On appelle *fraction continue finie* un nombre écrit sous la forme

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}}}$$

où $a_0, \ldots, a_k$ sont des entiers et si $k \geq 1$, $a_1, \ldots, a_k$ sont supérieurs ou égaux à 1.

Pour gagner de la place, nous allons noter la fraction ci-dessus en écrivant simplement entre crochets les entiers qui interviennent : $[a_0, \ldots, a_k]$.

Exemple 1.2.
1. Tout entier $n \in \mathbf{Z}$ s'écrit comme une fraction continue : il suffit de prendre $k = 0$ et $n = a_0$. Réciproquement, une fraction continue avec $k = 0$ est simplement un entier a_0.
2. Le nombre $\frac{1}{2}$ est une fraction continue, avec $k = 1$, $a_0 = 0$ et $a_1 = 2$.
3. Le nombre $\frac{4}{3}$ s'écrit comme fraction continue : $\frac{4}{3} = 1 + \frac{1}{3}$, donc $k = 1$, $a_0 = 1$ et $a_1 = 3$ conviennent.
4. Le nombre $\frac{3}{4}$ s'écrit comme une fraction continue :

$$\frac{3}{4} = \frac{1}{\frac{4}{3}} = \frac{1}{1 + \frac{1}{3}},$$

et donc $k = 2$, $a_0 = 0$, $a_1 = 1$ et $a_2 = 3$. Cette astuce d'inverser la fraction est la méthode générale que nous emploierons plus bas dès que nous aurons à faire à une fraction dont le numérateur est plus petit que le dénominateur.

Rappelons qu'un nombre *rationnel* α est un nombre qui s'écrit comme une fraction, c'est-à-dire qu'il existe a et b des entiers tels que $\alpha = \frac{a}{b}$. Observons qu'en effectuant des mises au même dénominateur, on peut toujours réécrire une fraction continue sous cette forme. Donnons quelques exemples :

- Nous avons déjà vu qu'une fraction continue avec $k = 0$ est un entier, donc en particulier un rationnel.
- Pour $k = 1$, nous avons $a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$, qui est bien une fraction.
- Pour $k = 2$, nous avons

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0(a_1 a_2 + 1) + a_2}{a_1 a_2 + 1}.$$

qui est bien une fraction

Il est alors naturel de se demander si réciproquement, tout nombre rationnel peut s'écrire sous forme de fraction continue. La proposition suivante répond affirmativement à cette question.

Proposition 1.3. *Tout nombre rationnel s'écrit comme une fraction continue finie.*

La clé pour comprendre cette propriété est l'*algorithme d'Euclide* : dans l'écriture $[a_0, \ldots, a_k]$ d'un rationnel comme fraction continue, $a_0, \ldots, a_k$ sont les quotients successifs dans les différentes étapes de l'algorithme d'Euclide du numérateur par le dénominateur (lorsque la fraction est sous forme irréductible).

Faisons-le sur un exemple : soit $\alpha = \frac{24}{17}$, qui est bien une fraction irréductible. Ecrivons l'algorithme d'Euclide pour 24 et 17 :

$$\begin{array}{rcl} 24 & = & 1 \times 17 + 7 \\ 17 & = & 2 \times 7 + 3 \\ 7 & = & 2 \times 3 + 1 \end{array}$$

Maintenant, nous allons utiliser chacune de ces lignes dans l'ordre pour mettre α sous la forme d'une fraction continue. Tout d'abord :

$$\alpha = \frac{24}{17} = \frac{1 \times 17 + 7}{17} = 1 + \frac{7}{17}$$

On réécrit

$$\frac{7}{17} = \frac{1}{\frac{17}{7}} = \frac{1}{\frac{2\times 7+3}{7}} = \frac{1}{2 + \frac{3}{7}},$$

si bien que nous avons déjà

$$\alpha = 1 + \frac{1}{2 + \frac{3}{7}}.$$

De même

$$\frac{3}{7} = \frac{1}{\frac{7}{3}} = \frac{1}{\frac{2\times 3+1}{3}} = \frac{1}{2 + \frac{1}{3}},$$

et donc

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \frac{1}{3}}}.$$

Ici le processus s'arrête car nous avons atteint une fraction du type $\frac{1}{a}$, qui apparait au moment où l'algorithme d'Euclide termine, en donnant un reste de 1 (ce qui arrive forcément car nous sommes partis de deux nombres premiers entre eux).

Ceci est vrai plus généralement : soit $\frac{p}{q}$ une fraction irreductible, soient $a_0, \ldots, a_{k-1}$ les quotients qui apparaissent dans les étapes successives de l'algorithme d'Euclide pour p et q, et $b_0, \ldots, b_k$ les restes successifs :

$$\begin{array}{rcl} p & = & a_0 q + b_0 \\ q & = & a_1 b_0 + b_1 \\ b_0 & = & a_2 b_1 + b_2 \\ & \vdots & \\ b_{k-2} & = & a_{k-1} b_{k-1} + b_k \end{array}$$

Puisque p et q sont premiers entre eux, nous savons que le dernier reste, qui est égal à leur pgcd, vaut 1, c'est-à-dire que $b_k = 1$. Alors de même que ci-dessus :

$$\begin{aligned}\frac{p}{q} &= a_0 + \frac{b_0}{q} \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{b_1}{b_0}} \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{b_2}{b_1}}}\end{aligned}$$

Nous observons donc qu'à chaque étape, le nouveau dénominateur est mis sous la forme $a_i + \frac{b_i}{b_{i-1}}$: tant que $b_i \neq 1$, c'est-à-dire tant que l'algorithme d'Euclide n'a pas terminé, nous pouvons continuer le processus en réécrivant

$$\frac{b_i}{b_{i-1}} = \frac{1}{\frac{b_{i-1}}{b_i}}$$

et en utilisant la ligne suivante de l'algorithme d'Euclide, qui pose la division euclidienne de b_{i-1} par b_i. En revanche, quand nous atteignons l'étape k, nous avons un dénominateur $a_{k-1} + \frac{1}{b_{k-1}}$, puisque $b_k = 1$, et nous avons terminé. En posant $a_k = b_{k-1}$, nous avons donc

$$\frac{p}{q} = [a_0, a_1, \ldots, a_k].$$

1.2 Fractions continues infinies

Définition 1.4. On appelle fraction continue infinie une expression de la forme

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \tag{1}$$

où a_0 est entier et où $a_1, a_2, \ldots$ sont des entiers supérieurs ou égaux à 1.

On notera cet objet $[a_0, a_1, a_1, \ldots]$ pour gagner de la place. Telle quelle, cette définition ne semble pas avoir beaucoup de sens. Cet objet est-il un vrai nombre ? Comment le calculer ? Nous allons en fait l'approcher par des fractions continues finies, appelées ses *réduites*.

Définition 1.5. Soit n un entier positif ou nul. On appelle *réduite d'ordre* n de la fraction continue infinie (1) la fraction continue finie

$$r_n = [a_0, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}}$$

Nous avons vu que tout rationnel pouvait s'écrire comme une fraction continue finie. Dans la suite, nous allons expliquer pourquoi à tout nombre réel α nous pouvons associer une fraction continue, qui sera infinie si et seulement si α est irrationnel, c'est-à-dire qu'il ne s'écrit pas sous forme de fraction. Les nombres $\sqrt{2}$, π, $\sqrt[5]{7} + 2$ par exemple sont irrationnels. Commençons par une petite définition :

Définition 1.6. Soit x un réel. La partie *entière* de x est le plus grand entier inférieur ou égal à x. Il est noté $[x]$. La partie *fractionnaire* de x est la différence $x - [x]$, notée $\{x\}$.

Remarquons que par définition, on a l'encadrement $0 \leq \{x\} < 1$.

Exemple 1.7. Si n est un entier, alors $[n] = n$ et $\{n\} = 0$. Nous avons aussi $[2,3] = 2$ et $\{2,3\} = 0,3$, $[-1,9] = -2$ et $\{-1,9\} = -1,9 - (-2) = 0,1$, $\left[\frac{3}{2}\right] = [1,5] = 1$, et $\left\{\frac{3}{2}\right\} = \{1,5\} = 0,5$. De plus, puisque $\pi \approx 3,14$, nous avons $[\pi] = 3$.

Algorithme de construction de la fraction continue associée à α Soit α un nombre réel, qui n'est pas un entier. Alors $[\alpha] < \alpha$, c'est-à-dire que $\{\alpha\} \neq 0$ Alors en posant $a_0 = [\alpha]$ et $\alpha_1 = \frac{1}{\{\alpha\}} > 1$, α s'écrit sous la forme

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Si α_1 n'est pas entier, il peut à son tour être représenté sous la forme $\alpha_1 = a_1 + \frac{1}{\alpha_2}$ avec a_1 entier et $\alpha_2 > 1$. On continue de même avec α_2. A chaque étape, nous construisons un nouveau réel $\alpha_i > 1$. Si α_i est entier, on obtient que α est égal à une fraction continue finie, et donc que α est rationnel. Si α_i n'est pas entier, alors nous pouvons poser $a_i = [\alpha_i]$ et $\alpha_{i+1} = \frac{1}{\{\alpha_i\}} > 1$.

Si ce processus s'arrête à un moment, c'est que nous sommes tombés sur un α_i entier, et que donc α est rationnel. Sinon, nous construisons ainsi étape par étape une fraction continue infinie dont les coefficients successifs sont les entiers $a_0, a_1, a_2, \ldots$ avec par construction $a_i \geq 1$ dès que $i \geq 1$.

Exercice 1.8. Se convaincre que dans le cas où α est rationnel, cette méthode coïncide avec celle du paragraphe précédent qui utilisait l'algorithme d'Euclide.

Exemple 1.9. Prenons notre calculatrice, et calculons les quelques premiers termes de la fraction continue associée au nombre π.

- Nous savons que $\pi \approx 3,141592$, donc $a_0 = 3$ et $\alpha_1 \approx \frac{1}{0,141592} \approx 7,062513$.
- On pose $a_1 = 7$, et $\alpha_2 \approx \frac{1}{0,062513} \approx 14,996594$.
- On pose $a_2 = 14$ et $\alpha_3 \approx \frac{1}{0,996594} \approx 1,003417$.
- On pose $a_3 = 1$ et $\alpha_4 \approx \frac{1}{0,003417} \approx 292,634591$.
- On pose $a_4 = 292$ et $\alpha_5 \approx \frac{1}{0,634591} \approx 1,575818$.
- On pose $a_5 = 1$.

Avec cela, on voit que la réduite d'ordre 5 de la fraction continue de π est

$$[3, 7, 14, 1, 292, 1].$$

Notons que la réduite d'ordre 1 est égale à $3 + \frac{1}{7} = \frac{22}{7}$, valeur approchée de π connue depuis l'Antiquité.

1.3 Quelques propriétés des réduites

Soit $\alpha = [a_0, a_1, a_2, \ldots]$ un nombre réel.

Proposition 1.10. *On définit les suites (p_n) et (q_n) par récurrence en posant*

$$p_0 = a_0, \qquad q_0 = 1 \qquad p_1 = a_0 a_1 + 1 \qquad q_1 = a_1,$$

et pour tout $n \geq 1$,

$$\begin{cases} p_{n+1} = p_n a_{n+1} + p_{n-1} \\ q_{n+1} = q_n a_{n+1} + q_{n-1} \end{cases}$$

Alors pour tout $n \geq 0$, la réduite r_n d'ordre n de α est égale à la fraction $\frac{p_n}{q_n}$.

Remarque 1.11. Attention, pour le moment nous n'affirmons pas que p_n et q_n sont respectivement le numérateur et le dénominateur de la forme irréductible de r_n. Pour cela il faut vérifier qu'ils sont premiers entre eux, ce qui se fera dans la proposition suivante.

Démonstration. Les premiers termes se vérifient sans peine : $\frac{p_0}{q_0} = a_0 = r_0$ et $\frac{p_1}{q_1} = \frac{a_0a_1+1}{a_0} = a_0 + \frac{1}{a_1} = r_1$. Vérifions également la propriété pour $n = 2$: nous avons

$$r_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_2(a_0a_1 + 1) + a_0}{a_1a_2 + 1} = \frac{a_2p_1 + p_0}{a_2q_1 + q_0}.$$

Pour la suite, nous allons raisonner par récurrence, en supposant la propriété vraie jusqu'au rang $n \geq 2$. On pose pour tout $x \neq 0$ la fonction

$$f_n(x) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \frac{1}{x}}}}}.$$

Alors par hypothèse de récurrence, $f_n(a_n) = r_n = \frac{p_n}{q_n} = \frac{p_{n-1}a_n+p_{n-2}}{q_{n-1}a_n+q_{n-2}}$. L'astuce maintenant, c'est de remarquer que dans cette expression de $f_n(a_n)$ en fonction de a_n, les coefficients $p_{n-1}, p_{n-2}, q_{n-1}, q_{n-2}$ ne dépendent pas de a_n (mais seulement de $a_0, \ldots, a_{n-1}$). Ainsi, si on remplace a_n par un autre nombre, cela ne change pas ces coefficients. Nous pouvons donc utiliser cette même expression en évaluant f_n en $a_n + \frac{1}{a_{n+1}}$. Ainsi, nous avons

$$r_{n+1} = f_n\left(a_n + \frac{1}{a_{n+1}}\right) = \frac{p_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + p_{n-2}}{q_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + q_{n-2}}.$$

Finalement, en simplifiant cela nous avons

$$r_{n+1} = \frac{p_na_{n+1} + p_{n-1}}{q_na_{n+1} + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}},$$

ce qui conclut. □

Proposition 1.12. *Soient (p_n) et (q_n) les suites définies par les relations de récurrence ci-dessus. Alors pour tout $n \geq 1$, nous avons*

$$p_{n-1}q_n - p_nq_{n-1} = (-1)^n.$$

En particulier, pour tout $n \geq 0$, p_n et q_n sont premiers entre eux.

Démonstration. Nous allons de nouveau raisonner par récurrence. Pour $n = 1$, nous avons

$$p_0q_1 - p_1q_0 = a_0a_1 - (a_0a_1 + 1) = -1 = (-1)^1,$$

donc la propriété est vraie au rang 1. Supposons-la vraie pour un certain $n \geq 1$. Alors en utilisant les relations de récurrence :

$$\begin{aligned} p_nq_{n+1} - p_{n+1}q_n &= p_n(q_na_{n+1} + q_{n-1}) - (p_na_{n+1} + p_{n-1})q_n \\ &= p_nq_{n-1} - p_{n-1}q_n \\ &= -(p_{n-1}q_n - p_nq_{n-1}) = -(-1)^n = (-1)^{n+1}, \end{aligned}$$

ce qui conclut la récurrence. Soit $n \geq 1$ et soit $d \geq 1$ un diviseur commun de p_{n-1} et q_{n-1} . Alors d divise $(-1)^n$, donc $d = 1$. Donc p_{n-1} et q_{n-1} sont premiers entre eux. □

Exemple 1.13. Regardons les premières réduites de la fraction continue infinie avec $a_i = 1$ pour tout i :

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}} = [1, 1, 1, \ldots]$$

Nous avons dans ce cas par définition $p_0 = q_0 = q_1 = 1$, et $p_1 = 2$, et ensuite pour tout $n \geq 1$, $p_{n+1} = p_n + p_{n-1}$ et $q_{n+1} = q_n + q_{n-1}$. Ces deux suites sont donc très proches d'une suite très connue, qui s'appelle la suite de Fibonacci, et qui est définie de la manière suivante : $F_0 = 1$, $F_1 = 1$, et pour tout $n \geq 1$,

$$F_{n+1} = F_n + F_{n-1}.$$

Les premiers termes de cette suite sont

F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
1	1	2	3	5	8	13	21	34	55

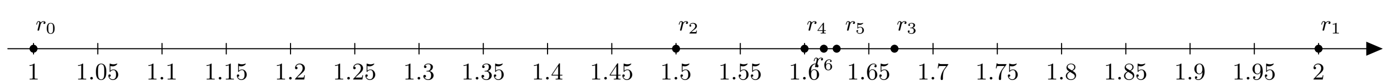
On remarque qu'au vu des premiers termes de (p_n) et de (q_n), nous avons pour tout $n \geq 1$,

$$p_n = F_{n+1} \quad \text{et} \quad q_n = F_n.$$

Autrement dit, la suite (q_n) est exactement la suite de Fibonacci, et la suite (p_n) est la suite de Fibonacci décalée d'un rang. Nous pouvons donc calculer les réduites de la fraction continue ci-dessus grâce au tableau de valeurs de la suite de Fibonacci :

r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8
$\frac{1}{1} = 1$	$\frac{2}{1} = 2$	$\frac{3}{2} = 1,5$	$\frac{5}{3} \approx 1,667$	$\frac{8}{5} = 1,6$	$\frac{13}{8} = 1,625$	$\frac{21}{13} \approx 1,615$	$\frac{34}{21} \approx 1,619$	$\frac{55}{34} \approx 1,618$

Représentons les valeurs obtenues sur un axe.



Nous pouvons observer plusieurs choses : dans l'ensemble, les r_i semblent se rapprocher quand i augmente. De plus, on remarque que $r_0 < r_2 < r_4 < r_6 < r_8$, c'est-à-dire que la suite des r_i avec i pair est croissante, et que celle des r_i avec i impair est décroissante. Ces deux suites semblent converger vers une valeur proche de 1,618, l'une en croissant, l'autre en décroissant. Ce phénomène que nous venons d'observer dans ce cas particulier sera démontré dans le cas général dans les prochaines propositions.

Proposition 1.14. *Pour tout $n \geq 2$, nous avons*

$$p_n q_{n-2} - q_n p_{n-2} = (-1)^n a_n$$

Démonstration. On utilise la relation de récurrence de la proposition 1.10 :

$$p_n q_{n-2} - q_n p_{n-2} = (a_n p_{n-1} + p_{n-2}) q_{n-2} - (a_n q_{n-1} + q_{n-2}) p_{n-2} = a_n (-1)^n$$

d'après la proposition 1.12. $\square$

Proposition 1.15. *Nous avons*

$$1 = q_0 \leq q_1 < q_2 < q_3 < \dots,$$

c'est-à-dire que la suite des dénominateurs est croissante, et strictement croissante à partir du rang 2, et tend vers l'infini. En particulier, la différence entre deux réduites consécutives tend vers zéro, c'est-à-dire que

$$\lim_{n \longrightarrow +\infty} |r_n - r_{n-1}| = 0.$$

Démonstration. Nous avons bien $q_0 = 1$, et $q_1 = a_1 \geq 1 = q_0$. Ensuite, la relation de récurrence $q_{n+1} = q_n a_{n+1} + q_{n-1}$ permet de voir que tous les termes suivants sont strictement positifs, vu que les entiers a_n, $n \geq 1$ le sont. Alors pour tout $n \geq 1$,

$$q_{n+1} = q_n a_{n+1} + q_{n-1} > q_n \times 1 + 0 = q_n$$

en utilisant le fait que $a_{n+1} \geq 1$, et que $q_{n-1} > 0$.

Une suite d'entiers strictement croissante tend vers l'infini. En effet, $q_{n+1} > q_n$ implique que $q_{n+1} \geq q_n + 1$. Ainsi, nous avons

$$q_{n+1} \geq q_n + 1 \geq q_{n-1} + 2 \geq \dots \geq q_1 + n$$

Or la suite de terme général $q_1 + n$ tend vers l'infini, donc la suite (q_n) aussi.

On utilise maintenant la relation de la proposition 1.12, en la divisant par $q_{n-1}q_n$, ce qui donne

$$r_{n-1} - r_n = \frac{(-1)^n}{q_n q_{n-1}}.$$

En valeur absolue, nous avons donc

$$|r_n - r_{n-1}| = \frac{1}{q_{n-1} q_n}.$$

Puisque q_n tend vers l'infini, q_{n-1} également, et donc nous avons le résultat. □

Ainsi, nous venons de montrer que deux réduites consécutives sont de plus en plus proches. Pour cela, nous avons utilisé le fait que leurs dénominateurs sont de plus en plus grands.

Proposition 1.16. *Les réduites d'indice pair forment une suite strictement croissante, c'est-à-dire que nous avons*

$$r_0 < r_2 < r_4 < \dots.$$

Les réduites d'indice impair forment une suite strictement décroissante, c'est-à-dire

$$r_1 > r_3 > r_5 > \dots.$$

Démonstration. D'après la proposition 1.14, nous avons pour tout $n \geq 2$

$$r_n - r_{n-2} = \frac{(-1)^n a_n}{q_{n-2} q_n}.$$

Lorsque n est pair, ceci montre que $r_n - r_{n-2} > 0$, et lorsque n est impair, ceci montre que $r_n - r_{n-2} < 0$, ce qui conclut.

□

Proposition 1.17. *Toute réduite d'indice pair est inférieure à toute réduite d'indice impair, donc nous avons*

$$r_0 < r_2 < r_4 < \dots < r_5 < r_3 < r_1.$$

Démonstration. Observons tout d'abord que d'après la proposition 1.12, pour tout k,

$$r_{2k} - r_{2k+1} = \frac{(-1)^{2k+1}}{q_{2k}q_{2k+1}} = -\frac{1}{q_{2k}q_{2k+1}} < 0,$$

donc tout terme d'indice pair est strictement inférieur ou terme d'indice impair qui le suit. En particulier, par décroissance de la suite des réduites d'indice impair, tous les termes d'indice impair précédents sont aussi strictement plus grands que r_{2k}, c'est-à-dire :

$$r_{2k} < r_{2k+1} < r_{2k-1} < \ldots < r_3 < r_1.$$

Supposons maintenant qu'il existe un entier impair $2m+1$ (avec $m > k$, du coup) tel que $r_{2k} \geq r_{2m+1}$. Par croissance de la suite des réduites d'indice pair, toutes les réduites d'indice pair $2n$ avec $n > k$ sont alors strictement plus grandes que r_{2m+1}, autrement dit, nous avons :

$$r_{2m+1} \leq r_{2k} < r_{2(k+1)} < \ldots < r_{2m} < \ldots$$

En particulier, nous avons

$$r_{2m+1} < r_{2m},$$

ce qui contredit la remarque du début. □

Nous venons de montrer que la suite des réduites d'ordre pair est croissante, que la suite des réduites d'ordre impair est décroissante, et que la différence entre deux réduites consécutives tend vers zéro. Ces deux suites sont donc ce qu'on appelle des suites adjacentes, et elles convergent vers une valeur commune. Il nous reste à identifier cette valeur commune. Si nous sommes partis d'une fraction continue associée à un réel α, ce dernier est un candidat naturel.

Proposition 1.18. *La suites des réduites de la fraction continue associée à α converge vers α.*

Démonstration. Notons $[a_0, a_1, \ldots]$ la fraction continue associée à α, de sorte que pour tout n, $r_n = [a_0, \ldots, a_n]$. On reprend la fonction

$$f_n(x) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \frac{1}{x}}}}}.$$

La variable x se situe sous n traits de fraction, donc la fonction f_n est croissante quand n est pair, et décroissante quand n est impair. On pose

$$\alpha_n = [a_n, a_{n+1}, a_{n+2}, \ldots] = a_n + \cfrac{1}{a_{n+1} + \cfrac{1}{a_{n+2} + \ddots}}.$$

Alors il est clair que pour tout n, nous avons $f_n(\alpha_n) = \alpha$. D'autre part, on a $\alpha_n \geq a_n$, donc pour tout $n = 2k$ pair,

$$\alpha = f_{2k}(\alpha_{2k}) \geq f_{2k}(a_{2k}) = r_{2k},$$

et pour tout $n = 2k-1$ impair,

$$\alpha = f_{2k-1}(\alpha_{2k-1}) \leq f_{2k-1}(a_{2k-1}) = r_{2k-1}.$$

Ainsi, pour tout couple de réduites consécutives, α est compris entre celles-ci. En particulier, pour tout n, nous avons $|\alpha - r_n| \leq |r_{n-1} - r_n|$, et donc $|\alpha - r_n|$ tend vers 0. Cela veut dire que r_n converge vers α. □

2 Approximation à l'aide de fractions continues

2.1 Exemples

Le but de ce paragraphe est de calculer à la main des approximations de certains nombres grâce aux fractions continues.

Décomposition de $\sqrt{2}$ en fraction continue Nous savons que $\sqrt{2}$ est compris strictement entre 1 et 2. En effet, nous avons l'encadrement $1 < 2 < 4$, et par stricte croissance de la fonction racine carrée, cela donne $1 < \sqrt{2} < 2$.

On peut donc écrire $\sqrt{2} = 1 + \frac{1}{x}$ pour un certain $x > 1$. Exprimons x :

$$x = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} = 1 + \sqrt{2}$$

en multipliant le numérateur et le dénominateur par la quantité conjuguée. Or nous avons $\sqrt{2} = 1 + \frac{1}{x}$, d'où $x = 2 + \frac{1}{x}$, ce qui donne :

$$\begin{aligned} \sqrt{2} &= 1 + \frac{1}{x} \\ &= 1 + \cfrac{1}{2 + \cfrac{1}{x}} \\ &= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \frac{1}{x}}} \end{aligned}$$

et on voit que l'on peut continuer ainsi indéfiniment. Le développement en fraction continue de $\sqrt{2}$ est donc $[1, 2, 2, 2, \ldots]$ (un 1 suivi d'une infinité de chiffres 2). Nous allons noter cela $[1, \overline{2}]$, pour indiquer que le chiffre 2 est répété indéfiniment.

Regardons ce que donnent les premières réduites :

$$r_0 = 1 \qquad r_1 = 1 + \frac{1}{2} = 1,5 \qquad r_2 = 1 + \frac{1}{2 + \frac{1}{2}} = 1 + \frac{2}{5} = 1,4.$$

On voit qu'on s'approche déjà un peu de $\sqrt{2} \approx 1,414$.

Regardons les suivantes :

$$r_3 = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = 1 + \frac{1}{2 + \frac{2}{5}} = 1 + \frac{5}{12} \approx 1,417$$

$$r_4 = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = 1 + \frac{1}{2 + \frac{5}{12}} = 1 + \frac{12}{29} \approx 1,414$$

Ainsi, à partir de r_4 nous avons déjà atteint une exactitude au troisième chiffre après la virgule près !

Décomposition de $\sqrt{3}$ en fraction continue De même, nous savons que $\sqrt{3}$ est compris strictement entre 1 et 2. Écrivons donc $\sqrt{3} = 1 + \frac{1}{x}$ avec $x > 1$, et exprimons x en utilisant encore la quantité conjuguée :

$$x = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$$

Ce nombre est encore compris entre 1 et 2 strictement : en effet, nous avons $2 < 1 + \sqrt{3} < 3$, d'où $1 < \frac{1+\sqrt{3}}{2} < \frac{3}{2} < 2$. Ainsi, nous pouvons écrire $x = 1 + \frac{1}{y}$ pour un certain $y > 1$. Exprimons maintenant y :

$$y = \frac{1}{x-1} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{2} = 1 + \sqrt{3} = 2 + \frac{1}{x}.$$

Ainsi, nous pouvons écrire :

$$\begin{aligned}
\sqrt{3} &= 1 + \frac{1}{x} \\
&= 1 + \cfrac{1}{1 + \cfrac{1}{y}} \\
&= 1 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{x}}} \\
&= 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{y}}}}
\end{aligned}$$

Nous voyons que de même, nous pouvons continuer indéfiniment, en remplaçant x par son expression en fonction de y dans une égalité sur deux, et y par son expression en fonction de x dans les autres. Ainsi, la décomposition de $\sqrt{3}$ en fraction continue est $[1, \overline{1, 2}]$, où le trait horizontal indique que la séquence $1, 2$ est répétée une infinité de fois.

Le nombre d'or Une question naturelle se pose : qui est donc le nombre dont la décomposition en fraction continue est

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}} = [1, 1, 1, \ldots]$$

c'est-à-dire où seulement le chiffre 1 apparaît ? Appelons x ce nombre. Remarquons que par définition, le terme au dénominateur de la grande fraction est encore égal à x, et que donc x vérifie l'équation

$$x = 1 + \frac{1}{x}.$$

En multipliant le tout par x (vu qu'il est manifestement non-nul), nous avons l'équation quadratique

$$x^2 - x - 1 = 0.$$

Son discriminant est 5, et ses deux racines sont donc $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$. Laquelle est la bonne ? C'est la première, vu que la deuxième est négative.

Définition 2.1. Le nombre $\varphi = \frac{1+\sqrt{5}}{2}$ est appelé le *nombre d'or.*

Notons que grâce aux calculs de la section précédente, nous savons qu'il est environ égal à 1,618 (ce que nous pouvons d'ailleurs vérifier à la calculatrice). D'autre part, puisqu'il est limite de ses réduites, nous avons montré que la suite des rapports de deux termes consécutifs de la suite de Fibonacci tend vers le nombre d'or, c'est-à-dire

$$\lim_{n\to+\infty} \frac{F_{n+1}}{F_n} = \varphi.$$

Regardons un peu plus en détail le tableau des réduites que nous avions obtenu. On voit que même après 7 étapes, on n'a toujours pas atteint une approximation au troisième chiffre après la virgule près, alors que pour $\sqrt{2}$ il a suffi de 4 étapes. A quoi est-ce dû ? En fait, la qualité de l'approximation d'une fraction $[a_0, a_1, a_2, \ldots]$ par sa réduite $[a_0, \ldots, a_k]$ dépend directement de l'entier k, mais aussi de la taille de l'entier a_k : plus on coupe loin, mieux c'est, mais si on veut économiser des étapes de calcul, il vaut mieux couper au niveau d'un a_k assez grand, car le terme fractionnaire que l'on oublie est d'autant plus négligeable que a_k est grand. Or pour le nombre d'or, tous les a_i valent 1, c'est-à-dire sont minimaux, c'est donc en quelque sorte l'entier que l'on met le plus de temps à bien approximer avec des fractions continues ! Les coefficients de la fraction continue de $\sqrt{2}$ ne sont pas bien grands non plus, vu qu'ils sont tous égaux à 2 sauf le premier, mais cela suffit pour que la convergence soit nettement plus rapide.

Terminons ce paragraphe par une observation : les développements en fraction continue des nombres que nous avons vus dans ce paragraphe sont périodiques, c'est-à-dire qu'à partir d'un certain moment, c'est toujours la même séquence finie de nombres qui se répète : 2 pour $\sqrt{2}$, $1, 2$ pour $\sqrt{3}$, et 1 pour le nombre d'or. On peut alors se poser la question de savoir à quelle condition une fraction continue a des coefficients périodiques. Le théorème suivant nous dit que c'est le cas si et seulement s'il est racine d'une équation de degré 2 à coefficients entiers (on dit que c'est un *irrationnel quadratique*) :

Théorème 2.2. *Soit α un nombre irrationnel. Alors la fraction continue associée à α a des coefficients périodiques si et seulement si α est racine d'une équation de la forme*

$$ax^2 + bx + c = 0$$

avec $a, b, c \in \mathbf{Z}$, et $a \neq 0$.

En particulier, $\sqrt{2}$, $\sqrt{3}$ et φ, racines respectives de $x^2 - 2 = 0$, $x^2 - 3 = 0$ et $x^2 - x - 1 = 0$, entrent dans ce cas de figure. En revanche, des nombres comme $\sqrt[3]{2}$ ou π ont des développements en fraction continue non périodiques. Finalement, de même que nous savons que les nombres avec développement décimal fini sont les nombres décimaux, ceux avec développement décimal périodique sont les nombres rationnels, et les autres sont irrationnels, nous avons également une sorte de classement des nombres par ordre croissant de complexité de leur fraction continue : les fractions continues finies correspondent aux rationnels, celles qui sont périodiques correspondent aux irrationnels quadratiques, et les autres correspondent aux irrationnels restants. Un tel irrationnel peut soit être racine d'une équation de degré strictement plus grand que 2 (par exemple $\sqrt[3]{2}$ est racine de $x^3 - 2 = 0$), soit n'être racine d'aucune équation polynomiale à coefficients entiers (on dit alors qu'il est *transcendant* ; le nombre π en est un exemple).

2.2 Quelques théorèmes d'approximation

Pour chaque nombre réel α, il existe une suite de rationnels qui converge vers α. La plus évidente est la suite de ses approximations décimales : par exemple, on peut approcher $\sqrt[3]{2} \approx 1,259921$ successivement par

$$1, \quad \frac{12}{10}, \ \frac{125}{100}, \ \frac{1259}{1000}, \ \frac{12599}{10000}, \ldots$$

Dans ce qui précède, nous avons vu une autre suite qui fonctionne, à savoir la suite des réduites de la fraction continue de α. Comment comparer la qualité de ces approximations ? Il n'est pas difficile de se convaincre que plus une fraction irréductible est proche de α, plus son dénominateur doit être grand. Une bonne approximation est alors une approximation qui est très proche de α, mais dont le dénominateur n'est pas trop grand, pour qu'on puisse calculer facilement avec. Il est alors raisonnable, pour mesurer la qualité d'une approximation $\frac{p}{q}$ de α, de vouloir borner sa distance à α, à savoir $\left|\alpha - \frac{p}{q}\right|$, en termes de q.

Regardons tout d'abord ce qui se passe dans le cas des approximations décimales. On écrit

$$\alpha = c_0 + \frac{c_1}{10} + \frac{c_2}{100} + \ldots + \frac{c_k}{10^k} + \ldots$$

où c_0 est un entier, et pour tout $i \geq 1$, nous avons $0 \leq c_i \leq 9$. On note

$$c_0 + \frac{c_1}{10} + \frac{c_2}{100} + \ldots + \frac{c_n}{10^n} = \frac{A_n}{10^n}$$

son approximation à 10^n près. Alors

$$\left|\alpha - \frac{A_n}{10^n}\right| = \frac{c_{n+1}}{10^{n+1}} + \frac{c_{n+2}}{10^{n+2}} + \ldots \leq \frac{9}{10^{n+1}} + \frac{9}{10^{n+2}} + \ldots.$$

Le membre de droite s'écrit comme $\frac{9}{10^{n+1}}$ fois la somme infinie

$$1 + \frac{1}{10} + \frac{1}{100} + \ldots$$

Pour tout m, les m premiers termes de cette somme sont les m premiers termes d'une suite géométrique de premier terme 1 et de raison $\frac{1}{10}$, donc leur somme est

$$\frac{1 - \frac{1}{10^m}}{1 - \frac{1}{10}}.$$

Pour obtenir la valeur de la somme infinie, on fait tendre m vers l'infini dans cette expression, et on obtient $\frac{1}{1-\frac{1}{10}} = \frac{10}{9}$. Ainsi, finalement, nous avons

$$\left|\alpha - \frac{A_n}{10^n}\right| \leq \frac{1}{10^n}.$$

Autrement dit, nous venons de montrer

Proposition 2.3. *Soit α un réel. Alors il existe une infinité de rationnels $\frac{p}{q}$ tels que*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q}.$$

Regardons maintenant la qualité de l'approximation par les fractions continues :

Proposition 2.4. *Soit α un nombre réel. Pour toute réduite $\frac{p_n}{q_n}$ de la fraction continue qui lui est associée, nous avons*

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2}.$$

Démonstration. On écrit l'égalité de la proposition 1.12 au rang $n+1$, et on divise par $q_n q_{n+1}$, pour obtenir

$$\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{(-1)^{n+1}}{q_n q_{n+1}}.$$

En prenant des valeurs absolues, et en utilisant le fait que la suite (q_n) est croissante, nous avons :

$$\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \leq \frac{1}{q_n^2}.$$

Enfin, nous avons vu que α est compris entre les réduites consécutives $\frac{p_n}{q_n}$ et $\frac{p_{n+1}}{q_{n+1}}$, donc en particulier :

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \leq \frac{1}{q_n^2}.$$

□

La théorie des fractions continues montre donc le fait suivant :

Proposition 2.5. *Soit α un réel. Alors il existe une infinité de rationnels $\frac{p}{q}$ tels que*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Ce résultat est meilleur que celui obtenu grâce aux approximations par les fractions décimales, puisque $\frac{1}{q^2}$ est très petit par rapport à $\frac{1}{q}$ dès que q est très grand.

Pouvons-nous obtenir une borne encore meilleure que $\frac{1}{q^2}$? Il se trouve que la puissance de q que nous avons trouvée est déjà optimale, c'est-à-dire qu'on peut montrer que si s est un nombre réel strictement plus grand que 2, il existe beaucoup de [1] nombres α tels qu'il n'existe qu'un nombre fini de rationnels $\frac{p}{q}$ tels que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^s}.$$

En particulier, nous n'avons pas de suite de rationnels convergeant aussi vite vers un tel α. En revanche, comme le montre le théorème suivant, nous pouvons améliorer la constante multiplicative :

Théorème 2.6. *(Hurwitz) Soit α un réel. Alors il existe une infinité de rationnels $\frac{p}{q}$ tels que*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

La démonstration de ce théorème utilise encore les fractions continues. Plus précisément, elle consiste à montrer que parmi trois réduites consécutives, au moins l'une vérifie l'inégalité de l'énoncé, ce qui fournit une infinité de rationnels convenables.

La constante $\frac{1}{\sqrt{5}}$ dans le théorème de Hurwitz est optimale, c'est-à-dire que le théorème devient faux si on la remplace par un nombre plus petit, en prenant pour α le nombre d'or :

Proposition 2.7. *Pour tout $c < \frac{1}{\sqrt{5}}$ il n'existe qu'un nombre fini de rationnels $\frac{p}{q}$ tels que*

$$\left|\frac{1+\sqrt{5}}{2} - \frac{p}{q}\right| < \frac{c}{q^2}.$$

Cela rejoint la remarque que nous avions faite plus haut selon laquelle le nombre d'or est le nombre le « moins bien approximable » par des rationnels, à cause du fait que son développement en fraction continue ne contient que des 1.

Le caractère optimal du théorème de Hurwitz, et le fait qu'on utilise les fractions continues pour le prouver, montre qu'en un certain sens, les fractions continues donnent les meilleures approximations possibles d'un réel.

1. Plus précisément, un résultat appelé le théorème de Roth dit que tous les α non transcendants conviennent.

3 Application à la résolution des équations de Pell-Fermat

3.1 Définition

Une équation de Pell[2]-Fermat[3] est une équation de la forme

$$x^2 - my^2 = 1 \tag{2}$$

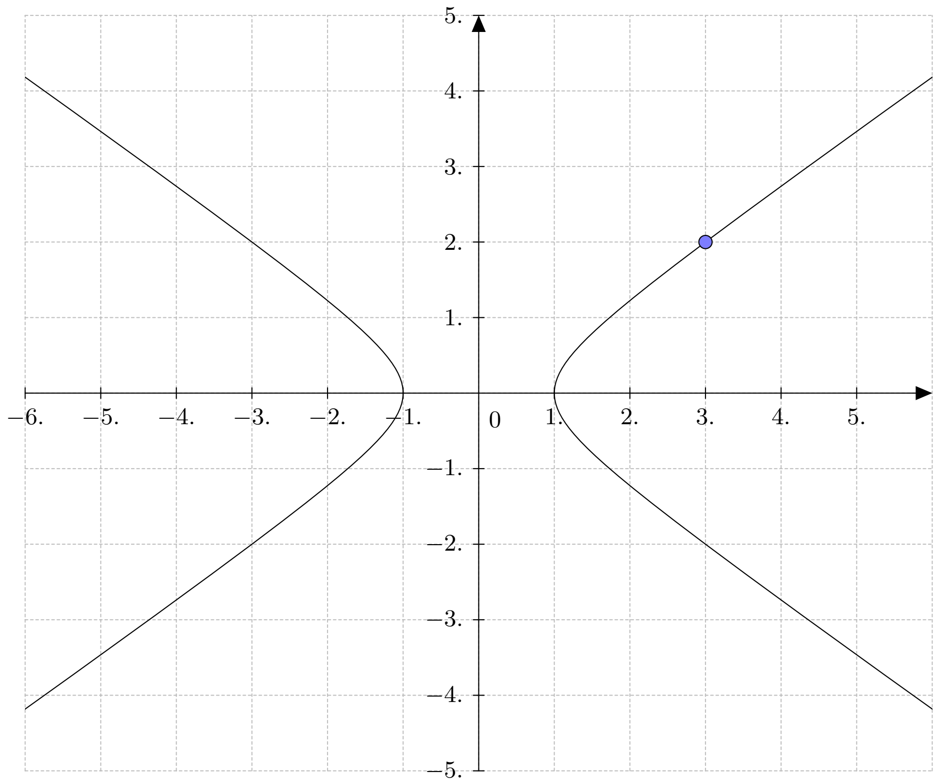
où m est un entier strictement positif qui n'est pas le carré d'un entier.

Notons qu'en dehors de la France, ces équations ont tendance à être appelées équations de Pell (tout court). Mais en France on aime bien ajouter le nom d'un Français aux objets mathématiques qu'on étudie.[4]

Notre but dans la suite sera de trouver tous les couples d'entiers (x, y) qui vérifient cette équation. Commençons par quelques remarques immédiates :

(a) Comme x et y sont mis au carré, leur signe n'importe pas. Si (x, y) est solution, alors $(-x, y)$, $(x, -y)$ et $(-x, -y)$ sont solutions également. Ceci nous permet de nous restreindre à la recherche de solutions (x, y) avec x et y positifs. Notons de plus que dans ce cas x est nécessairement strictement positif, et $x > y$.

(b) Si $y = 0$, nous tombons sur le couple solution $(1, 0)$ (et $(-1, 0)$ aussi du coup). Cette solution existe toujours et ne dépend pas de m, nous l'appelons *solution triviale*. Mettant cette solution de côté, nous allons nous mettre à la recherche des solutions non-triviales. Dans la suite, nous supposerons donc que x et y sont *strictement positifs*.



L'HYPERBOLE $x^2 - 2y^2 = 1$, AVEC UN POINT ENTIER $(3, 2)$

2. John Pell (1611-1685) – mathématicien anglais

3. Pierre de Fermat (1601-1665) – magistrat français, mathématicien et physicien amateur

4. En vrai, dans ce cas nous avons raison de le faire, car, paraît-il, contrairement à Pell, Fermat a véritablement travaillé sur ces équations

(c) Interprétation géométrique : L'équation $x^2 - my^2 = 1$ dessine une figure dans le plan, appelée *hyperbole*. Résoudre l'équation, c'est trouver les points à coordonnées entières de cette hyperbole. Les remarques sur le signe des solutions que nous venons de donner renvoient au fait que l'hyperbole admet une symétrie par rapport à l'axe des ordonnées (qui envoie le point de coordonnées (x, y) sur celui de coordonnées $(-x, y)$, une symétrie par rapport à l'axe des abscisses (qui envoie (x, y) sur $(x, -y)$), ainsi que la composée de ces deux symétries, qui est la symétrie centrale par rapport à l'origine (qui envoie (x, y) sur $(-x, -y)$). Les solutions triviales $(1, 0)$ et $(-1, 0)$ sont les intersections de l'hyperbole avec l'axe des abscisses. Le fait que nous nous restreignions à des solutions positives revient à chercher les points à coordonnées entières du morceau d'hyperbole situé dans le quart de plan supérieur droit.

Remarque 3.1. Pourquoi demande-t-on que m ne soit pas un carré ? Supposons un instant qu'il le soit, et écrivons $m = a^2$ pour un certain $a \in \mathbf{N}^*$. Alors l'équation peut se factoriser :

$$x^2 - a^2y^2 = (x - ay)(x + ay) = 1.$$

Ainsi, les entiers $x - ay$ et $x + ay$ sont deux nombres dont le produit est 1. Or les seules manières d'écrire le nombre 1 comme le produit de deux entiers sont $1 = (-1) \times (-1) = 1 \times 1$. Comme l'entier $x + ay$ est clairement positif, nous avons

$$x - ay = 1 \quad \text{et} \quad x + ay = 1$$

et donc $x = 1$ et $y = 0$. Ainsi, dans le cas où m est un carré, l'équation n'admet que la solution triviale.

3.2 Une solution en appelle une autre

Remarquons quelques opérations que nous pouvons effectuer sur les solutions de l'équation (2). Soient (x, y) et (x', y') deux solutions de l'équation de Pell-Fermat. On considère les réels $x + \sqrt{m}y$ et $x' + \sqrt{m}y'$. Si on les multiplie, alors on obtient

$$(x + \sqrt{m}y)(x' + \sqrt{m}y') = (xx' + myy') + \sqrt{m}(xy' + yx'). \tag{3}$$

Le membre de droite nous définit un nouveau couple d'entiers $(xx' + myy', xy' + yx')$. Notons que si nous multiplions les conjugués des réels ci-dessus, nous obtenons le conjugué du membre de droite :

$$(x - \sqrt{m}y)(x' - \sqrt{m}y') = (xx' + myy') - \sqrt{m}(xy' + yx'). \tag{4}$$

En multipliant (3) et (4), nous obtenons

$$(x^2 - my^2)(x'^2 - my'^2) = (xx' + myy')^2 - m(xy' + yx')^2.$$

Puisque (x, y) et (x', y') sont solutions de l'équation de Pell-Fermat, le membre de gauche vaut 1, ce qui implique que le couple $(xx' + myy', xy' + yx')$ est une nouvelle solution de l'équation ! Observons de plus que si nous sommes partis de solutions strictement positives, alors cette nouvelle solution est encore strictement positive.

Définition 3.2. On appelle cette nouvelle solution le *produit* des solutions (x, y) et (x', y'), et on la note $(x, y) \cdot (x', y')$. On note $(x, y)^n$ le produit de (x, y) par elle-même n fois.

Remarque 3.3. Nous avons

$$(x, y) \cdot (x', y') = (x', y') \cdot (x, y),$$

et

$$(x, y) \cdot (1, 0) = (x, y).$$

L'opération inverse de la multiplication des solutions est la *division* des solutions. Partons de nouveau de deux solutions (x, y) et (x', y'), et écrivons

$$\frac{x+\sqrt{m}y}{x'+\sqrt{m}y'} = \frac{(x+\sqrt{m}y)(x'-\sqrt{m}y')}{(x'+\sqrt{m}y')(x'-\sqrt{m}y')} = \frac{(xx'-myy')+\sqrt{m}(yx'-xy')}{x'^2-my'^2} = (xx'-myy')+\sqrt{m}(yx'-xy').$$

De même que ci-dessus, cela nous fournit une nouvelle solution$(xx'-myy', yx'-xy')$ de l'équation.

Nous allons maintenant montrer comment à l'aide de ces opérations, toutes les solutions positives s'obtiennent à l'aide d'une seule solution « minimale » en un certain sens.

Définition 3.4. On appelle *solution fondamentale* de l'équation (2) un couple (x_0, y_0) d'entiers strictement positifs tels que le réel $x_0 + \sqrt{m}y_0$ est minimal.

Remarque 3.5. La solution fondamentale est unique. En effet, soit (x_1, y_1) une autre solution fondamentale. Alors nous avons

$$x_0 + \sqrt{m}y_0 = x_1 + \sqrt{m}y_1,$$

et si $y_0 \neq y_1$, nous obtenons $\sqrt{m} = \frac{x_1-x_0}{y_0-y_1}$, ce qui est impossible puisque $\sqrt{m}$ est irrationnel. Donc $y_0 = y_1$, et par conséquent $x_0 = x_1$, c'est-à-dire que les deux solutions sont égales.

Remarque 3.6. Géométriquement parlant, parmi les points à coordonnées entières dans le quart supérieur gauche de l'hyperbole, la solution fondamentale correspond au point le plus proche de l'origine, donc le plus « en bas à gauche ». Sur le graphique de l'hyperbole $x^2 - 2y^2 = 1$ ci-dessus, on voit bien que c'est le point $(3, 2)$.

Proposition 3.7. *Soit (x_0, y_0) une solution fondamentale. Alors toute solution positive de l'équation s'écrit sous la forme $(x_0, y_0)^n$ pour un certain n.*

Démonstration. Soit (x, y) une solution positive, avec $x+\sqrt{m}y > x_0+\sqrt{m}y_0$ (autrement dit, (x, y) n'est pas fondamentale). On la divise par (x_0, y_0), ce qui nous fournit une solution $(xx_0 - myy_0, yx_0 - xy_0)$. Par définition, nous avons

$$\frac{x+\sqrt{m}y}{x_0+\sqrt{m}y_0} = xx_0 - myy_0 + \sqrt{m}(yx_0 - xy_0),$$

donc puisque $x_0 + y_0\sqrt{m} > 1$, nous avons

$$xx_0 - myy_0 + \sqrt{m}(yx_0 - xy_0) < x + \sqrt{m}y.$$

Nous avons donc obtenu une solution strictement plus petite. Reste à vérifier qu'elle est toujours positive. Pour cela, notons que puisque (x, y) et (x_0, y_0) sont solutions, nous avons $x > \sqrt{m}y$ et $x_0 > \sqrt{m}y_0$. En multipliant les deux inégalités, on aura $xx_0 - myy_0 > 0$. D'autre part, puisque par hypothèse $y > y_0$, nous avons

$$\left(\frac{x_0}{y_0}\right)^2 + d = \frac{1}{y_0^2} > \frac{1}{y^2} = \left(\frac{x}{y}\right)^2 + d,$$

d'où $yx_0 - xy_0 > 0$. Nous savons donc, à partir d'une solution strictement plus grande que la solution fondamentale, trouver une solution positive plus petite en divisant par la solution fondamentale. Le nombre de solutions positives inférieures à une solution donnée est fini, donc au bout d'un certain nombre de divisions par la solution fondamentale, nous devons tomber sur une solution positive (x', y') telle que $x' + \sqrt{m}y' \leq x_0 + \sqrt{m}y_0$. Par minimalité de $x_0 + \sqrt{m}y_0$, nous avons alors nécessairement égalité, et donc par la remarque 3.5, nous avons $(x', y') = (x_0, y_0)$, ce qui conclut. $\square$

Nous avons donc vu comment, une fois une solution trouvée, nous pouvons construire toutes les autres solutions à partir de celle-ci. Reste à donner un procédé pour trouver cette première solution : c'est ce que nous faisons dans le paragraphe suivant.

3.3 Retour aux fractions continues

Soit (x, y) une solution de l'équation de Pell-Fermat. Alors nous avons $(x - \sqrt{m}y)(x + \sqrt{m}y) = 1$. Si nous supposons x et y grands, alors le réel $x + \sqrt{m}y$ est d'autant plus grand. Mais alors, pour que le produit fasse 1, il faut que $x - \sqrt{m}y$ soit très petit. En divisant par y^2, il faut que $\frac{x}{y} - \sqrt{m}$ soit encore plus petit, c'est-à-dire que le rationnel $\frac{x}{y}$ doit bien approximer $\sqrt{m}$. Nous voyons que la résolution de l'équation de Pell-Fermat a un lien avec l'approximation de $\sqrt{m}$ par des rationnels.

Nous avions déjà évoqué le fait que l'approximation par les réduites d'une fraction continue est en quelque sorte optimale. La proposition suivante (que nous ne démontrerons pas) précise ce point de vue, en affirmant que si un rationnel approxime « bien » un réel, alors il figure parmi les réduites du développement de ce réel en fraction continue.

Proposition 3.8. *Soit α un réel et $\frac{p}{q}$ une fraction irréductible. Si on a*

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{2q^2}$$

alors il existe $i \geq 0$ tel que $\frac{p}{q}$ soit la réduite r_i d'ordre i de la fraction continue associée à α.

Corollaire 3.9. *Soit (x, y) une solution positive de l'équation de Pell-Fermat (2). Alors $\frac{x}{y}$ est une réduite du nombre $\sqrt{m}$.*

Démonstration. Pour utiliser la proposition précédente, il suffit de montrer que

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

ou, en multipliant par y (qui est positif),

$$|x - \sqrt{m}y| < \frac{1}{2y}. \tag{5}$$

Par définition, nous avons

$$1 = x^2 - my^2 = (x - \sqrt{m}y)(x + \sqrt{m}y)$$

(en particulier, $x - \sqrt{m}y$ est positif, donc il suffit de montrer (5) sans la valeur absolue). Or nous savons que $x > y$ et $\sqrt{m} > 1$, donc $x + \sqrt{m}y > 2y$, d'où le résultat. □

Ainsi, les solutions de l'équation de Pell-Fermat sont toutes de la forme (p_i, q_i) où $\frac{p_i}{q_i}$ est une réduite de $\sqrt{m}$ sous forme irréductible. Attention, la réciproque n'est pas vraie, c'est-à-dire que toutes les réduites ne donnent pas une solution de l'équation de Pell-Fermat. En effet, parmi ces réduites, figurent par exemple (si elles existent) également les solutions de l'équation de Fermat inversée :

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

En effet, la démonstration du résultat ci-dessus s'adapte sans problèmes à celles-ci.

Exemple 3.10. On considère l'équation $x^2 - \sqrt{2}y^2 = 1$. Nous avons calculé ci-dessus les premières réduites de $\sqrt{2}$. On remarque que $r_0 = \frac{1}{1}$ nous donne une solution de l'équation inversée : on a $1 - 2 \times 1 = -1$. En revanche, $r_1 = \frac{3}{2}$, et $(3, 2)$ est bien une solution de l'équation, et c'est même la solution fondamentale comme nous l'avons déjà observé. Ensuite, $r_2 = \frac{7}{5}$ donne $7^2 - 2 \times 5^2 = -1$, donc on obtient encore une solution de l'équation inversée. Pour $r_3 = \frac{17}{12}$, nous avons $17^2 - 2 \times 12^2 = 1$, donc cela nous fournit encore une solution de l'équation de Pell-Fermat.

Cet exemple pourrait nous laisser croire qu'une fois sur deux nous tombons sur une solution de l'équation de Pell-Fermat, et une fois sur deux sur une solution de l'équation de Pell-Fermat inversée. Cela n'est pas vrai : en fait, la première réduite pour laquelle nous obtiendrons une solution de l'une des deux équations, c'est celle d'ordre $\ell-1$ où ℓ est la période du développement en fraction continue de l'irrationnel quadratique $\sqrt{m}$. Plus précisément, nous avons le résultat suivant :

Proposition 3.11. *Soit ℓ la longueur de la période de la suite (a_n) des coefficients de la fraction continue associée à $\sqrt{m}$. Alors le couple (p_n, q_n) est une solution de l'équation de Pell-Fermat si et seulement si n est impair de la forme $k\ell - 1$. S'il est pair et de cette forme, on obtient une solution de l'équation de Pell-Fermat inversée.*

En particulier, dans le cas $m = 2$, nous avons $\ell = 1$, donc toutes les réduites d'indice impair donneront des solutions de l'équation de Pell-Fermat, et toutes les réduites d'ordre pair des solutions de l'équation de Pell-Fermat inversée. Remarquons de plus que si ℓ est pair (ce qui arrive par exemple quand $m = 3$), alors tous les entiers de la forme $k\ell - 1$ seront impairs : ainsi, dans ce cas, l'équation de Pell-Fermat inversée n'a pas de solution.