1 Théorie

1.1 Fraction continues

1.1.1 Intuition

Intuitivement, une fraction continue est une expression — finie ou infinie — de la forme suivante [1] :

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

telle que $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N}^*$ pour tout $i \in \mathbb{N}^*$. Toujours intuitivement, nous voulons affûbler cette fraciton continue d'une valeur. Si la fraction continue est finie, cette une bonne vieille fraciton, c'est à dire un élément du corps $\mathbb{Q}$; si la fraction continue est infinie, on calcule d'abord a_0, puis $a_0 + \frac{1}{a_1}$, puis $a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$, et on continue une infinité de fois. La limite de la suite générée est la « valeur » de la fraction continue. Nous ferons sens plus précis de l'intuition dans la prochaine sous-section.

Les fractions continues émanent de la volonté d'approcher des réels irrationels par des fractions d'entiers. Par exemple, la fraction $\frac{103993}{33102}$ approche π avec une précision meilleure que le milliardième. Comment générer une telle fraction continue pour un réel irrationnel x ? On part de l'identité $x = x + \lfloor x \rfloor - \lfloor x \rfloor$ et l'on écrit

$$x = \lfloor x \rfloor + \cfrac{1}{\cfrac{1}{x - \lfloor x \rfloor}}.$$

On pose $x_0 = x$ et $x_1 = \frac{1}{x_0 - \lfloor x_0 \rfloor}$ (qui est bien défini par irrationalité de x) et l'on répète la première étape sur x_1 :

$$x = \lfloor x_0 \rfloor + \frac{1}{x_1} = \lfloor x_0 \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{\cfrac{1}{x_1 - \lfloor x_1 \rfloor}}}.$$

Comme le réel x est irrationnel, on peut répéter ce procédé indéfiniment. Nous construisons alors la suite d'éléments *irrationnels* de terme général

$$x_n = \frac{1}{x_{n-1} - \lfloor x_{n-1} \rfloor}, \quad \forall n \geqslant 1.$$

1. Notez que nous ne nous autorisons que des 1 aux numérateurs.

On associe alors à *l'irrationnel* x la fraction continue *infinie*[2]

$$\hat{x}_0 + \cfrac{1}{\hat{x}_1 + \cfrac{1}{\hat{x}_2 + \cfrac{1}{\hat{x}_3 + \dots}}},$$

où l'on a posé

$$\hat{x}_i = \lfloor x_i \rfloor$$

pour tout $i \in \mathbb{N}$. Fixons ces notations :

Notation 1.1. Soit $x \in \mathbb{R}$ un élément irrationel. Notons $x_0 = x$ puis

$$x_n := \frac{1}{x_{n-1} - \lfloor x_n \rfloor}, \quad \forall n \geqslant 1.$$

Par ailleurs, notons

$$\hat{x}_n := \lfloor x_n \rfloor, \quad \forall n \in \mathbb{N}.$$

Remarque 1.2. La méthode de construction d'une fraction continue *finie* pour un rationnel est la même : il faut simplement s'arrêter lorsque l'on tombe sur un $\hat{x}_n$ vérifiant $\hat{x}_n = \lfloor \hat{x}_n \rfloor$. Cet algorithme termine (**ref**) et s'exécute plus simplement en utilisant... l'algorithme d'Euclide.

1.1.2 Formalisation

Formellement, on peut définir[3] une fraction continue ainsi :

Définition 1.3 (Fraction continue)**.** On appelle *fraction continue* toute suite non vide (finie ou infinie) $(a_i)_{i \in U} \in \mathbb{N}^{\mathbb{N}}$, $U \subset \mathbb{N}$, d'entiers qui vérifie

$$a_i \geqslant 1, \quad \forall i \in U \setminus \{0\}.$$

Cette suite est alors notée

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}.$$

2. Lorsque nous aurons correctement défini la notion de fraction continue, cette fraction continue canoniquement associée à x sera notée $\hat{x}$.

3. La définition mathématique est descriptive et non prescriptive.

Notation 1.4. Soit $x \in \mathbb{R}$ un élément irrationel. On note $\hat{x}$ la fraction continue infinie canoniquement associée à x par la méthode exposée dans le premier paragraphe. Autrement dit, $\hat{x}$ est la fraction continue donnée par la suite infinie (voir 1.1.3) $(\hat{x}_i)_{i\in\mathbb{N}}$.

Il est naturel d'associer à une fraction continue (finie ou infinie) une suite (finie ou infinie) de fractions « intermédiaires » appelées *réduites*. Pour n'avoir aucun problème de division par zéro, nous nous plaçons temporairement dans un corps de fractions rationnelles en $\mathbb{N}$ indeterminées.

Définition 1.5 (Réduites formelles)**.** Soit $(X_i)_{i\in\mathbb{N}}$ une suite (infinie) d'indeterminées sur le corps $\mathbb{Q}$. On définit

$$[X_0] = X_0]$$

puis par récurrence

$$[X_1, \ldots, X_n] = X_0 + \frac{1}{[X_1, \ldots, X_n]}.$$

Ces éléments sont dans $\mathbb{Q}((X_i)_{i\in\mathbb{N}})$.

Définition 1.6 (Réduites d'une fraction continue)**.** Distinguons les cas finis et infinis. Soit f une fraction continue.

— Si f est donnée par la suite finie $(a_0, \ldots, a_n)$, pour tout $k \in [\![0, n]\!]$ on appelle *k-ième réduite de f* l'élément $[a_0, \ldots, a_k]$.

— Si f est donnée par la suite infinie $(a_i)_{i\in\mathbb{N}}$, pour tout $k \in \mathbb{N}$ on appelle *k-ième réduite de f* l'élément $[a_0, \ldots, a_k]$.

Exemple 1.7. Soit f la fraction continue infinie donnée par la suite $(1)_{i\in\mathbb{N}}$. La première réduite est $[1] = 1$, la deuxième est

$$[1, 1] = 1 + \frac{1}{[1]} = 1 + \frac{1}{1},$$

la troisième est

$$[1, 1, 1] = 1 + \frac{1}{[1, 1]} = 1 + \frac{1}{1 + \frac{1}{1}}.$$

Plus généralement, la k-ième réduite de f est de la forme

$$[1, 1, \ldots, 1] = 1 + \cfrac{1}{1 + \cfrac{1}{\cdots \cfrac{1}{1 + \frac{1}{1}}}}.$$

Remarquons que les réduites de toute fraction continue sont des éléments rationnels, ce même si la fraction continue est égale à $\hat{x}$ pour un certain irrationel x. De fait, x n'est égal à aucune des réduites de $\hat{x}$. Mais en reprenant les notations 1.1.3, on a toutefois

$$1.1.3x = [\hat{x}_1, \ldots, \hat{x}_{n-1}, x_n], \quad \forall x \in \mathbb{N}. \tag{1}$$

Cette égalité sera cruciale dans notre algorithme de factorisation.

Même si les fractions continues finie restent des suites (déf. 1.3), leur représentation graphique permet de les voir trivialement comme des éléments du corps $\mathbb{Q}$. En effet, en représentant

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$$

la fraction continue finie f associée à la suite finie $(a_0, \ldots, a_n)$, on peut la voir comme l'élément rationnel

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}.$$

Cet élément n'est autre que sa dernière réduite $[a_0, \ldots, a_n]$ et on dit que f est égale à l'élément rationnel $[a_0, \ldots, a_n]$. Pour les fractions continues infinies, ce n'est pas aussi simple.

Définition 1.8. Soient l un réel et f une fraction continue donnée par la suite infinie $(a_i)_{i\in\mathbb{N}}$. On dit que f *est égale à* l, que f *converge vers* l, ou encore que f *est le développement en fraction continue de* l et l'on note $f = l$ si la suite des réduites de f converge vers l. Si une fraction continue infinie est égale à un certain réel, on dit qu'elle converge.

Exemple 1.9 (Nombre d'or)**.** On appelle *nombre d'or* et l'on note φ l'unique racine réelle positive du polynôme $X^2 - X - 1 \in \mathbb{Z}[X]$. On a $\varphi = \frac{1+\sqrt{5}}{2} \simeq 1,618$. Comme $\varphi^2 = \varphi + 1$ et que $\varphi \neq 0$, on a $\varphi = 1 + \frac{1}{\varphi} = 1 + \cfrac{1}{1 + \cfrac{1}{\varphi}}$. En réalité, φ est égal à une fraction continue :

$$\varphi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}}.$$

Dans quelle mesure une fraction continue converge-t-elle ? Des raisonnements d'analyse élémentaire (**réf**) permettent de montrer que toute fraction continue infinie converge, et qu'elle converge vers un irrationnel !

Théorème 1.10. *La fonction canonique*

$$x \mapsto \cfrac{1}{\hat{x}_0 + \cfrac{1}{\hat{x}_1 \ + \cfrac{1}{\hat{x}_2 + \dots}}}$$

est une bijection *entre l'ensemble des nombres réels irrationnels et des fractions continues infinies.*

En particulier, un réel x et une fraction continue f sont égaux si, et seulement si, f est la fraction continue donnée par la suite $(\hat{x}_{i\in\mathbb{N}})$. Attention, les réels tout entier ne sont pas en bijection avec les fractions continues (finies ou infinies). En effet, un rationnel est égal (au sens donné dans les paragraphes précédents) à exactement deux fractions continues : si un rationnel est égal à $[a_0, \dots, a_n]$, il est aussi égal à $[a_0, \dots, a_n - 1, 1]$ et n'est égal à aucune autre fraction continue (**ref**).

1.1.3 Irrationels quadratiques

L'adaptation de l'algorithme de Fermat-Kraitchik avec les fractions continues utilise crucialement le développement en fraction continue de $\sqrt{kN}$, où N est le nombre à factoriser et $k \in \mathbb{N}*$ un entier arbitraire. Intéréssons nous aux fractions continues de ces nombres.

Définition 1.11 (Irrationel quadratique)**.** On appelle *irrationel quadratique* tout nombre réel, algébrique sur $\mathbb{Q}$, de degré 2. Un irrationel quadratique est dit *réduit* si son conjugué est dans l'intervalle $]\!]-1, 0[\![$.

Les fractions continues d'irrationnels quaratiques sont sujettes à des phénomènes de périodicité.

Définition 1.12. Soit f la fraction continue donnée par une suite $(a_i)_{i\in\mathbb{N}}$. On dit que f est *périodique* si la suite l'est à partir d'un certain rang. Autrement dit, il existe un rang $n_0 \in \mathbb{N}$ et une période $p \in \mathbb{N}^*$ tels que

$$a_i = a_{i+p}, \quad \forall i \geqslant n_0.$$

On note alors

$$f = [a_0, \dots, a_{n_0-1}, \overline{a_{n_0}, \dots, a_{n_0+p-1}}].$$

On dit enfin que f est *purement périodique* si $n_0 = 0$.

Exemple 1.13. La fraction continue du nombre d'or est purement périodique de période 1. La fraction continue de l'irrationel $\sqrt{14}$ vaut

$$\sqrt{14} = [4, \overline{2, 1, 3, 1, 2, 8}].$$

Nous disposons des deux résultats fondamentaux suivants.

Théorème 1.14 (Lagrange, 1770)**.** *Un réel irrationel est un irrationel quadratique si, et seulement si, son développement en fraction continue est périodique.*

Théorème 1.15 (Galois, 1829)**.** *Un irrationnel quadratique est réduit si, et seulement si, son développement en fraction continue est purement périodique.*

Un troisième résultat donne encore plus d'informations dans le cas où l'irrationel quadratique considéré est une racine carrée.

Théorème 1.16 (Legendre, 1798)**.** *Un réel irrationel est la racine carrée d'un entier* > 1 *si, et seulement si, son développement en fraction continue est de la forme*

$$[a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}].$$

Ces phrénomènes de périodicité devront être pris en compte dans les paramètres d'entrée de l'algorithme de factorisation, voir **réf**. En plus de la suite des réduites, nous aurons besoins d'une autre suite importante.

Lemme 1.17. *Soit* x *un irrationel quadratique. Alors l'élément* $\frac{1}{x-\lfloor x \rfloor}$ *est lui aussi un irrationel quadratique.* ***réf***

Fixons N l'entier à factoriser et $k \in \mathbb{N}*$ tel que $\sqrt{kN}$ est un irrationel quadratique. Posons alors $x := \sqrt{kN}$. D'après l'identité et en reprenant les notations , nous pouvons écrire donner un développement partiel (jusqu'à un rang donné $n \in \mathbb{N}$) de x en fraction continue

$$x = [\hat{x}_1, \ldots, \hat{x}_{n-1}, x_n].$$

D'après le lemme précédent, x_n est lui aussi un irrationel quadratique, i.e. il est solution d'une équation quadratique. On peut (**réf, dém. de 2.5.8**) de fait l'écrire de manière unique

$$x_n = \frac{P_n + x}{Q_n}, \quad P_n, Q_n \in \mathbb{Z}. \tag{2}$$

Ces notations P_n et Q_n seront réutilisées plus tard. La n-ième réduite de x étant un nombre rationnel, on peut l'écrire sous la forme $\frac{A_n}{B_n}$, où A_n, B_n sont entiers et la fraction est irréductible bien définie. Les entiers A_n, B_n, Q_n et l'irrationel x se rencontrent dans

un grand nombre d'égalités numériques. Nous choisissons de n'exposer que les plus utiles à notre propos [4]. Pour tout $n \geqslant 1$, on a

$$A_{n-1}^2 - kNB_{n-1}^2 = (-1)^n Q_n$$

et donc

$$A_{n-1}^2 \equiv (-1)^n Q_n. \tag{3}$$

On a également

$$\begin{cases} P_n < \sqrt{kN} \\ Q_n < 2\sqrt{kN}. \end{cases} \tag{4}$$

4. Pour plus de contenu et de détails, la lectrice pourra se référer à **réf**.