Factorisation par fractions continues

Margot Funk, Antoine Hugounet

Vendredi 19 février 2021

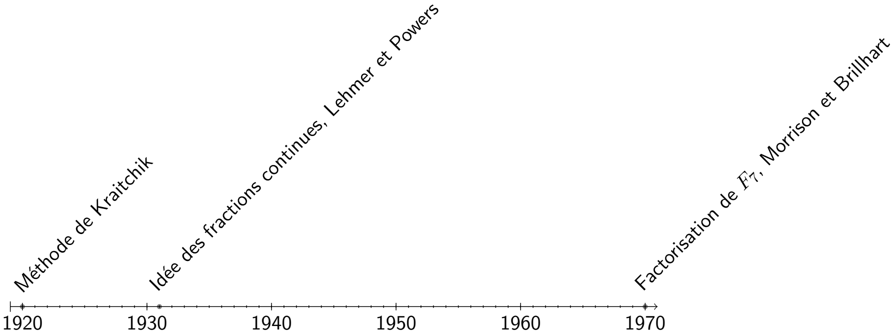
Méthode de Kraitchik
Idée des fractions continues, Lehmer et Powers
Factorisation de F_7, Morrison et Brillhart
1920
1930
1940
1950
1960
1970

Table des matières

Projet basé sur *A Method of Factoring and the Factorization of* F_7, de M. A. Morrison et J. Brillhart, dans Mathematics of Computation 29.129 (1975).

Intuition, définition

Intuitivement, expression de la forme

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}, \quad a_0 \in \mathbb{Z}, \forall i \in \mathbb{N}^* a_i \in \mathbb{N}^*.$$

Définition (Fraction continue)

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

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

Génération (1/2)

On génère un développement en fraction continue ainsi. Soit $x \in \mathbb{R} \setminus \mathbb{Z}$.

- On écrit $x = x + \lfloor x \rfloor - \lfloor x \rfloor$ et

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

  On pose $x_0 = x$ et $x_1 = \frac{1}{x_0 - \lfloor x_0 \rfloor}$.

- On recommence sur x_1 :

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

Génération (2/2)

- Si l'on peut continuer, on construit la suite d'éléments *irrationnels* de terme général

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

La suite est finie si x est rationnel, infinie sinon.

On note $\hat{x}_n = \lfloor x_n \rfloor$ pour tout n, de sorte que si x est irrationnel, on a

$$x = \hat{x_0} + \cfrac{1}{\hat{x}_1 + \cfrac{1}{\hat{x}_2 + \cfrac{1}{\hat{x}_3 + \dots}}}.$$

Réduites (1/2)

Définition (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

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

Définition

Soient $x \in \mathbb{R}$ et f une fraction continue. On dit que f *est un développement en fraction continue de* x si la suite des réduites de f converge vers x.

Réduites (2/2)

Si $x = (\hat{x}_i)_{i \in \mathbb{N}}$, on a

$$[\hat{x}_0, \ldots, \hat{x}_n] = \hat{x_0} + \cfrac{1}{\hat{x}_1 + \cfrac{1}{\ldots + \cfrac{1}{\hat{x}_n}}}$$

et

$$x = [\hat{x_0}, \ldots, \hat{x_n}, x_{n+1}].$$

Irrationels quadratiques

Définition (Irrationel quadratique)

On appelle *irrationel quadratique* tout nombre réel, algébrique sur $\mathbb{Q}$, de degré 2.

Si $M \in \mathbb{Z}$ est sans facteurs carrés, $\sqrt{M}$ est un irrationel quadratique.

Théorie des fractions continues très poussée pour les irrationels quadratiques (Lagrange, Galois, Legendre). Il y a une bijection entre les irrationels et les fractions continues infinies ; on peut donc parler *du* développement en fraction continue d'un irrationel.

Identités

Soit $x \in \mathbb{R}$ un irrationel.

- x_n est irrationel quadratique et s'écrit $x_n = \frac{P_n + x}{Q_n}$,
- la n-ième réduite du développement de x est rationnelle et s'écrit $\frac{A_n}{B_n}, A_n, B_n \in \mathbb{Z}$.

On a

$$\begin{cases} A_{n-1}^2 \equiv (-1)^n Q_n \pmod{N}, \\ P_n < \sqrt{kN}, \\ Q_n < 2\sqrt{kN}. \end{cases}$$