

Factorisation par fractions continues

Margot Funk, Antoine Hugounet

Vendredi 19 février 2021

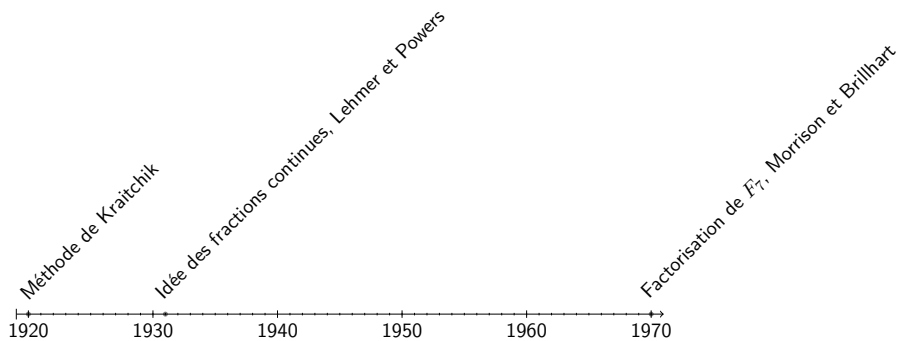


Table des matières

Introduction • Fractions continues

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, une fraction continue est une expression de la forme

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

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

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

Génération (1/2)

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

- On écrit $x = x + [x] - [x]$ et

$$x = [x] + \frac{1}{\frac{1}{x - [x]}}.$$

On pose $x_0 = x$ et $x_1 = \frac{1}{x_0 - [x_0]}$.

- On recommence sur x_1 :

$$x = [x_0] + \frac{1}{x_1} = [x_0] + \frac{1}{[x_1] + \frac{1}{\frac{1}{x_1 - [x_1]}}}.$$

Génération (2/2)

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

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

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

$$x = \hat{x}_0 + \frac{1}{\hat{x}_1 + \frac{1}{\hat{x}_2 + \frac{1}{\hat{x}_3 + \dots}}}.$$

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

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

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

$$[\hat{x}_0, \dots, \hat{x}_n] = \hat{x}_0 + \frac{1}{\hat{x}_1 + \frac{1}{\dots + \frac{1}{\hat{x}_n}}}$$

et

$$x = [\hat{x}_0, \dots, \hat{x}_n, x_{n+1}].$$

Périodicité, identités

Soit $k \in \mathbb{N}^*$ un entier. Posons $x := \sqrt{kN}$.

Proposition

Si kN est sans facteur carré, le développement en fraction continue de x est périodique à partir d'un certain rang.

- x_n est irrationnel 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

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