

Factorisation par fractions continues

Margot Funk, Antoine Hugounet

Février 2021

Table des matières

1	Théorie	1
1.1	Fractions continues	1
1.1.1	Intuition	1
1.1.2	Formalisation	3
1.1.3	Irrationnels quadratiques	6
1.2	Méthodes de factorisation de Fermat-Kraitchik et utilisation des fractions continues	8
1.2.1	Méthodes de Fermat et Kraitchik	8
1.2.2	Recherche de congruences de carrés	10
1.2.3	Utilisation des fractions continues	11
	Bibliographie	13

1 Théorie

1.1 Fractions continues

1.1.1 Intuition

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

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

telle que $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N}^*$ pour tout $i \in \mathbb{N}^*$. Si la fraction continue est finie, elle est un rationnel ; si la fraction continue est infinie, on lui associe une valeur en calculant

a_0 , puis $a_0 + \frac{1}{a_1}$, puis $a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$, et continuant 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 permettent d'approcher des réels irrationnels par une suite de fractions d'entiers. Par exemple, la fraction $\frac{103993}{33102}$ approche π avec une précision meilleure que le milliardième. Pour générer une telle fraction continue, on part de l'identité $x = x + [x] - [x]$ et l'on écrit

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

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

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

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

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

On associe alors à l'irrationnel x la fraction continue *infinie*¹

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

où l'on a posé

$$\hat{x}_i = [x_i]$$

pour tout $i \in \mathbb{N}$.

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

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

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

puis

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

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 ([Wik19]) et s'exécute plus simplement en utilisant l'algorithme d'Euclide.

1.1.2 Formalisation

Formellement, on peut définir² 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

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

Cette suite est alors notée

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

Notation 1.4. Soit $x \in \mathbb{R}$ un élément irrationnel. 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} indéterminées.

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

$$[X_0] = X_0$$

puis par récurrence

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

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

2. La définition mathématique est descriptive et non prescriptive.

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, \dots, a_n) , pour tout $k \in \llbracket 0, n \rrbracket$ on appelle k -ième réduite de f l'élément $[a_0, \dots, a_k]$.
- 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 $[a_0, \dots, a_k]$.

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

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

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 irrationnel 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 **pourquoi ça fait ça ? avec le 1.1.3 ?**

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

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

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

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

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

Cet élément n'est autre que sa dernière réduite $[a_0, \dots, a_n]$ et on dit que f est égale à l'élément rationnel $[a_0, \dots, a_n]$. 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 $\varphi = 1 + \frac{1}{\varphi} = 1 + \frac{1}{1 + \frac{1}{\varphi}}$. En réalité, φ est égal à une

fraction continue :

$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

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*

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

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 $(\hat{x}_i)_{i \in \mathbb{N}}$. 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 Irrationnels quadratiques

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

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

Les fractions continues d'irrationnels quadratiques 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

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

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'irrationnel $\sqrt{14}$ 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 irrationnel est un irrationnel 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'irrationnel quadratique considéré est une racine carrée.

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

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

Ces phénomènes 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 besoin d'une autre suite importante.

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

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

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

D'après le lemme précédent, x_n est lui aussi un irrationnel 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

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

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'irrationnel x se rencontrent dans un grand nombre d'égalités numériques. Nous choisissons de n'exposer que les plus utiles à notre propos³. Pour tout $n \geq 1$, on a

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

et donc

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

On a également

$$\begin{cases} P_n < \sqrt{kN} \\ Q_n < 2\sqrt{kN}. \end{cases} \quad (4)$$

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

1.2 Méthodes de factorisation de Fermat-Kraitchik et utilisation des fractions continues

Dans toute cette section, N désigne un entier naturel composé impair.

1.2.1 Méthodes de Fermat et Kraitchik

La méthode de factorisation de Fermat part du constat suivant.

Lemme 1.18. *Factoriser N est équivalent à l'exprimer comme différence de deux carrés d'entiers.*

Démonstration. En effet, si $N = u^2 - v^2$, $u, v \in \mathbb{Z}$ alors $N = (u-v)(u+v)$. Réciproquement si l'on a une factorisation $N = ab$, alors

$$N = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

□

La méthode de Fermat cherche donc à exploiter cette propriété en exprimant N comme la différence de deux carrés pour en déduire une factorisation. Celle-ci se montre particulièrement efficace lorsque N est le produit de deux entiers proches l'un de l'autre. Notons $N = ab$ une factorisation de N , $r = \frac{a+b}{2}$ et $s = \frac{a-b}{2}$. On a

$$N = r^2 - s^2$$

et que l'entier r est donc plus grand que \sqrt{N} tout en lui étant proche. Il existe donc un entier positif *u pas trop grand* tel que

$$\lfloor \sqrt{N} \rfloor + u = r$$

et donc tel que $(\lfloor \sqrt{N} \rfloor + u)^2 - N$ soit un carré. Trouver un tel entier u donne alors la factorisation de N . Comme les facteurs de N sont proches l'un de l'autre, on le trouve par essais successifs.

La méthode de Fermat n'est cependant pas du tout efficace lorsque les facteurs de N ne sont pas proches. D'après **MB**, la méthode est alors encore plus coûteuse que la méthode des divisions successives.

Dans les années 1920, Maurice Kraitchik a raffiné la méthode de Fermat pour améliorer son efficacité. Ses idées sont au cœur des algorithmes de factorisations les plus performants en 2020. Son idée essentielle est que pour factoriser N , il n'est pas *nécessaire* de l'exprimer comme différence de deux carrés ; trouver une différence de deux carrés qui soit un multiple de N *suffit*.

Lemme 1.19. Connaître deux entiers $u, v \in \mathbb{Z}$ tels que $u^2 \equiv v^2 \pmod{N}$ et $u \not\equiv \pm v \pmod{N}$ fournit une factorisation de N .

Démonstration. Posons $g = \text{pgcd}(u - v, N)$ et $g' = \text{pgcd}(u + v, N)$. Comme $u \not\equiv \pm v \pmod{N}$, on a $g < N$ et $g' < N$. Enfin ni g et g' ne sont réduits à 1 : si l'un des deux l'est, l'autre vaut N , contradiction. Donc g et g' sont tous deux des facteurs non triviaux de N . \square

Remarque 1.20. Dans l'algorithme, nous nous contenterons de chercher des u, v tels que N divise la différence de leurs carrés, sans vérifier s'ils vérifient $u \not\equiv \pm v \pmod{N}$. Comme le polynôme $X^2 - v^2 \in \mathbb{Z}/N\mathbb{Z}$ a exactement quatre racines, il y a « une chance sur deux » pour que u et v nous fournissent un facteur non trivial de N .

Comment trouver de tels couples (u, v) ? Kraitchik a eu l'idée de ne chercher dans un premier temps que des congruences de la forme :

$$u_i^2 \equiv v_i \pmod{N}$$

Il a remarqué qu'il suffisait d'exhiber une famille v_1, \dots, v_r telle que $\prod_{i=1}^r v_i$ soit un carré pour savoir comment obtenir une congruence de carrés par multiplication de congruences.

Il originellement utilisé le polynôme $K := X^2 - N \in \mathbb{Z}[X]$ qui fournit la congruence $u_i^2 \equiv K(u_i) \pmod{N}$. Si on sait que $K(u_1) \cdots K(u_r)$ est un carré, en posant $u = u_1 \cdots u_r$ et $v = \sqrt{K(u_1) \cdots K(u_r)}$ on a bien :

$$v^2 \equiv K(u_1) \cdots K(u_r) \equiv u_1^2 \cdots u_r^2 \equiv u^2 \pmod{N}$$

Cette méthode souffre toutefois d'un problème d'efficacité, puisqu'il est nécessaire de calculer un grand nombre de $K(x_i)$. La croissance de la fonction associée au polynôme K étant quadratique, le coût des calculs devient prohibitif.

Je suis pas vraiment d'accord que le problème vient de là, pour moi le problème vient de la nécessité de trouver des $K(u_i)$ -friables, comme on a pas de borne c'est moins bien que les fractions continues, mais pas du fait de calculer un carré meme si c'est grand on sait le faire. Crible quadratique utilise le même polynome mais ajoute un crible bien pensé à la place des divisions successives. J'enleverais la remarque et garderais seulement celle qui vient après.

Il reste à savoir comment trouver cette famille $v_1 \cdots v_r$.

1.2.2 Recherche de congruences de carrés

Une méthode qui répond à cette question sans passer par un algorithme de recherche exhaustive a été proposée par Kraitchik lui-même.

Morrison et Brillart, dans leur article exposant la méthode de factorisation avec les fractions continues, ont répondu à cette question. (garder la bonne version, Pomerancedit M et B)

Celle-ci nécessite de travailler avec des congruences de la forme

$$u_i^2 \equiv Q_i \pmod{N}$$

avec $|Q_i|$ suffisamment petit pour en connaître une factorisation. (La notation Q_i fera échos à celle utilisée pour décrire la méthode de factorisation avec les fractions continues).

On commence par se fixer B une base de factorisation, c'est à dire un ensemble non vide fini de nombres premiers.

Définition 1.21. Un entier $Q \in \mathbb{N} \setminus \{0, 1\}$ est dit *B-friable* si tous les facteurs premiers de Q sont dans B .

L'idée principale de Kraitchik **ou M et B** est que connaître suffisamment d'entiers $Q_i \in \mathbb{Z}$ avec $|Q_i|$ *B-friables entièrement factorisés* permet de trouver la famille recherchée.

Proposition 1.22. Soit F une famille d'entiers tels que leur valeur absolue est *B-friables*. Si

$$\#F \geq \#B + 2$$

alors on peut extraire une sous-famille de F dont le produit des éléments est un carré.

Démonstration. Posons $F = \{Q_1, \dots, Q_k\}$ (de sorte que $k = \#F$) et $B = (p_1, \dots, p_m)$ (de sorte que $\#B = m$). Les éléments $Q_j, 1 \leq j \leq k$ s'écrivent alors, comme $|Q_j|$ est *B-friable*,

$$Q_j = (-1)^{v_0} \prod_{i=1}^m p_i^{v_{p_i}(Q_j)}.$$

Fixons $j, j' \in \llbracket 1, k \rrbracket$. Puisque les éléments de B sont fixés et en nombre fini l'élément Q_j peut être vu comme le vecteur

$$v(Q_j) := (v_{p_m}(Q_j), \dots, v_{p_1}(Q_j), v_0)$$

L'entier Q_j est un carré si, et seulement si, les composantes de son vecteur $v(Q_j)$ sont paires, i.e. la réduction du vecteur $v(Q_j)$ modulo 2 est nulle. Par propriété des

valuations, le vecteur associé au produit $Q_j \cdot Q_{j'}$ est le vecteur somme $v(Q_j) + v(Q_{j'})$. Autrement dit, le produit d'une sous-famille $\{Q_{j_1}, \dots, Q_{j_s}\}$ de F est un carré si, et seulement si, les vecteurs $v(Q_{j_1}), \dots, v(Q_{j_s})$ somment à 0 modulo 2. Soit V le \mathbb{F}_2 -espace vectoriel \mathbb{F}_2^{m+1} , qui est de dimension $m+1$. Comme $k \geq m+2$, la famille $\{v(Q_1), \dots, v(Q_k)\}$ est liée dans V et il existe de fait des éléments $l_1, \dots, l_k \in \mathbb{F}_2$ tels que

$$\sum_{j=1}^k l_j v(Q_j) = 0.$$

L'élément $\prod_{j=1}^k Q_j^{l_j}$ est alors un carré. □

Définition 1.23. Soient $B = \{p_1, \dots, p_m\}$ une base de factorisation et Q un entier avec $|Q|$ B -friable. Si $Q = (-1)^{v_0} \prod_{i=1}^m p_i^{v_{p_i}(Q)}$, on appellera vecteur exposant associé à l'entier Q le vecteur

$$v(Q) := (v_{p_m}(Q), \dots, v_{p_1}(Q), v_0) \in \mathbb{F}_2^{m+1}$$

Remarque 1.24. Cette définition sera réutilisée lors de la description de l'algorithme de factorisation avec la méthode des fractions continues. L'ordre des composantes du vecteur présentée ici vient du fait que le v_0 correspondra au bit de poids faible et le $v_{p_m}(Q)$ au bit de poids fort du vecteur.

Notons $B = \{p_1, \dots, p_m\}$ une base de factorisation. Etant données des congruences $u_i^2 \equiv Q_i \pmod{N}$, la preuve de la proposition fournit un procédé d'algèbre linéaire pour extraire une familles Q_1, \dots, Q_r telle que $\prod_{i=1}^r Q_i$ soit un carré. Tout d'abord, il faut trouver des Q_i tels que $|Q_i|$ est B -friable (ce que nous ferons par divisions successives) et retenir leur vecteur exposant associé. **est-ce que la description de la matrice ça va ?**. Disons qu'on a pu en trouver k , notés Q_1, \dots, Q_k . Soit ensuite M la matrice $k \times (m+1)$ dont les lignes correspondent aux vecteurs exposants de Q_1, \dots, Q_k . Soient l_1, \dots, l_k les éléments de \mathbb{F}_2 donnés par la proposition et tels que $\prod_{j=1}^k Q_j^{l_j}$ soit un carré. Le vecteur (l_1, \dots, l_k) est un élément du noyau de la matrice transposée de M . Un tel élément est facilement produit avec des algorithmes usuels d'algèbres linéaires. Nous verrons plus tard une version adaptée du pivot de Gauß qui nous permet d'en produire.

1.2.3 Utilisation des fractions continues

Pour appliquer la méthode ci-dessus, il faut arriver à générer des Q_i avec $|Q_i|$ B -friable pour une base de factorisation donnée, supposée « pas très grande ». Il faut donc chercher à avoir des $|Q_i|$ « petits ». L'introduction des fractions continues est motivée par le constat suivant : si $u_i^2 = Q_i + kNb^2$ avec $|Q_i|$ petit, alors $\left(\frac{u_i}{b}\right)^2 - kN = \frac{Q_i}{b^2}$ est petit en valeur absolue et $\frac{u_i}{b}$ est une bonne approximation de \sqrt{kN} .

mettre référence

Redonnons quelques notations de la sous-section **réf** sur les fractions continues. Nous notons $x := \sqrt{N}$, puis conformément à **réf** $x_0 := x$ et $x_n = \frac{1}{x_{n-1} - [x_{n-1}]}$ pour tout $n \in \mathbb{N}^*$. Le développement en fraction continue de l'irrationnel x est donc

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

Sa n -ième réduite est pour tout n un rationnel et s'exprime de fait comme une fraction réduite $\frac{A_n}{B_n}$ où $A_n, B_n \in \mathbb{Z}$. En posant $\hat{x}_n := [x_n]$ pour tout $n \in \mathbb{N}$, on a l'égalité **réf**

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

Cet élément x_n est un irrationnel quadratique et s'écrit de fait **réf**

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

.

L'algorithme de factorisation repose sur l'égalité suivante :

$$A_{n-1}^2 = (-1)^n Q_n + kN B_{n-1}^2$$

On a donc :

$$A_{n-1}^2 \equiv (-1)^n Q_n \pmod{N}$$

Donnons à présent quelques définitions dont nous nous servirons pour décrire l'algorithme des fractions continues.

Définition 1.25. Pour tout $n \in \mathbb{N}^*$, on appelle n -ième paire (A, Q) le couple (A_{n-1}, Q_n) .

Définition 1.26. Un ensemble de paires (A, Q) indexé par n_1, \dots, n_k est dit *valide* si le produit $\prod_{i=1}^k (-1)^{n_i} Q_{n_i}$ est un carré (dans \mathbb{Z} et non uniquement dans $\mathbb{Z}/N\mathbb{Z}$).

Remarque 1.27. Par abus de langage, nous parlerons à présent du vecteur exposant associé à Q_n pour désigner le vecteur exposant associé à $(-1)^n Q_n = (-1)^{v_0} \prod_{i=1}^m p_i^{v_{p_i}(Q)}$, c'est-à-dire $(v_{p_m}(Q_n), \dots, v_{p_1}(Q_n), v_0) \in \mathbb{F}_2^{m+1}$

D'après la section précédente, étant donnée une base de factorisation B , la méthode consiste à :

- Calculer des couples (A, Q) par développement en fractions continues de \sqrt{kN} où k est un petit coefficient multiplicateur (voir plus loin)
- Sélectionner les Q_n B -friables et leur associer un vecteur exposant
- Trouver un ensemble valide de paires (A, Q) par pivot de Gauss sur la matrice dont les lignes sont formées de ces vecteurs exposants

Nous aurons donc déterminé une famille n_1, \dots, n_k d'indices tels que le produit $Q := \prod_{i=1}^k (-1)^{n_i} Q_{n_i}$ soit un carré (dans \mathbb{Z} et non uniquement dans $\mathbb{Z}/N\mathbb{Z}$). Posons $A := \prod_{i=1}^k A_{n_i}$. Si $A \not\equiv \pm\sqrt{Q} \pmod{N}$, nous aurons factorisé N en vertu du lemme **réf**.

Le principal avantage de l'utilisation des fractions continues plutôt que le polynôme de Kraitchik réside dans leur croissance. L'inégalité **réf** assure que les éléments $Q_n, n \in \mathbb{N}$ seront plus petits (en valeur absolu) que les $K(x'), x' \in \mathbb{Z}$ (dont la croissance lorsque x' s'éloigne de \sqrt{N} est approximativement linéaire de pente $2\sqrt{N}$). Les paires (A, Q) seront donc plus faciles à manier et les Q_n auront plus de chance d'être B -friables. Enfin, il est facile de générer le développement en fraction continue de x et les paires (A, Q) grâce à un algorithme itératif dû à Gaußet exposé dans **réf**.

Pour moi c'est plus ça l'avantage :

Le principal avantage qu'offre l'utilisation des fractions continues par rapport au polynôme de Kraitchik réside dans la croissance des termes $Q_n, n \in \mathbb{N}$. On sait par **réf** que les Q_n seront inférieurs à $2\sqrt{kN}$. Les $K(x)$ donnés par le polynôme de Kraitchik ont eux une croissance lorsque x s'éloigne de \sqrt{N} approximativement linéaire de pente $2\sqrt{N}$. Les Q_n auront donc plus de chance d'être B -friables que les $K(x)$ de Kraitchik. Or, l'étape la plus coûteuse de l'algorithme est celle de la recherche des termes B -friables par divisions successives. Enfin, notons qu'il est facile de générer le développement en fraction continue de x et les paires (A, Q) grâce à un algorithme itératif dû à Gaußet exposé dans **réf**.

A rajouter je pense dans cette partie : critère pour sélectionner la base de factorisation, le problème de la périodicité d'où introduction de k , l'idée à la base de la large prime variation + dans une autre sous-section des trucs sur la complexité

Références

[Wik19] Contributeurs WIKIVERSITÉ. "Introduction à la théorie des nombres/Approximation diophantienne et fractions continues". In : (avr. 2019). URL : <https://fr>.

wikiversity.org/wiki/Introduction_%C3%A0_la_th%C3%A9orie_des_nombres/Approximation_diophantienne_et_fractions_continues.