Factorisation par fractions continues

Margot Funk, Antoine Hugounet

Février 2021

Table des matières

1 Théorie

1.1 Fractions continues

1.1.1 Intuition

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

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

telle que $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N}^*$ pour tout $i \in \mathbb{N}^*$. 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 irrationels 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 $x = x + \lfloor x \rfloor - \lfloor x \rfloor$ et l'on écrit

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

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

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

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

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

où l'on a posé

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

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

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 irrationel. Notons $x_0 = x$,

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

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 et s'exécute plus simplement en utilisant l'algorithme d'Euclide ([**wikiu**] ¶ *Les deux fractions continues (finies) d'un rationnel*).

1.1.2 Définition, réduites

Formellement, on peut définir [2] une fraction continue ainsi :

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

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

Cette suite est alors notée

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

Notation 1.4. Soit $x \in \mathbb{R}$ un irrationel. On note $\hat{x}$ la fraction continue infinie canoniquement associée à x par la méthode exposée dans le premier paragraphe.

À toute fraction continue est associée une suite (finie ou infinie) de fractions « intermédiaires » appelées *réduites* [3].

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

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

Définition 1.6 (Réduites d'une fraction continue)**.** Soit f une fraction continue.

2. La définition mathématique est descriptive et non prescriptive.
3. L'utilisation d'indéterminées formelles permet dans la définition d'éviter les divisions par zéro.

— 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

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

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

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

Les réduites de toute fraction continue sont des éléments rationnels, y compris celles de la forme $\hat{x}$ pour un certain irrationel x. De fait, x n'est égal à aucune des réduites de $\hat{x}$. On a toutefois (voir notations 1.1) :

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

Cette égalité est cruciale dans notre algorithme de factorisation.

Si formellement les fractions continues sont des suites (déf. 1.3), leur représentation graphique permet de les voir trivialement comme des éléments du corps $\mathbb{Q}$. Si f est une fraction continue finie de suite $(a_0, \ldots, a_n)$, le rationnel

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

est égal à la dernière réduite $[a_0, \ldots, a_n]$. On dit que f est égale au 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 *converge vers l* ou 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 admet un développement en fraction continue donné par

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

Des raisonnements d'analyse élémentaire ([**wikiu**] ¶ *Bijection entre irrationnels et fractions continues infinies*) permettent de montrer que toute fraction continue infinie converge, et qu'elle converge vers un irrationnel.

Théorème 1.10. *L'application canonique*

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

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

En particulier, un réel une fraction continue converge vers un réel x si, et seulement si, $f = \hat{x}$. Attention, les réels tout entier ne sont pas en bijection avec les fractions continues (finies ou infinies). En effet, un rationnel est égal à exactement deux fractions continues car $[a_0, \dots, a_n] = [a_0, \dots, a_n - 1, 1]$ ([**wikiu**] ¶ *Les deux fractions continues (finies) d'un rationnel*).

1.1.3 Irrationels quadratiques

L'adaptation de l'algorithme de Fermat-Kraitchik avec les fractions continues que nous verrons plus tard 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 des éléments de cette forme.

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 $f = (a_i)_{i\in\mathbb{N}}$ une fraction continue. On dit que f est *périodique* si la suite l'est à partir d'un certain rang. Il existe alors 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 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

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

Les résultats suivants sont fondamentaux (voir [**wikiu**] ¶ *Fraction continue d'un irrationnel quadratique* pour les preuves).

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.*

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*

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

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

Voir [**Lauritzen**] prop. 2.5.2. Fixons N l'entier à factoriser, $k \in \mathbb{N}*$ tel que $\sqrt{kN}$ est un irrationel quadratique et $x := \sqrt{kN}$. D'après l'identité 1 et en reprenant les notations 1.1, 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 irrationel quadratique, i.e. il est solution d'une équation quadratique. On peut ([**Lauritzen**] dém. de 2.5.8) de fait l'écrire de manière unique

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

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. Pour tout $n \geqslant 1$, on a ([**Lauritzen**] § 2.7)

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

et donc

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

On a également ([**Lauritzen**] dém. de 2.5.8)

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

Ces notations et identitées seront cruciales dans la suite.

1.2 Factorisation par fractions continues

Dans tout le reste de 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. 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 exploite cette propriété et 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, $r = \frac{a+b}{2}$, $s = \frac{a-b}{2}$ de sorte que

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

Par hypothèse, 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 est cependant inefficace lorsque les facteurs de N ne sont pas proches. D'après [**Tale**] ¶ *Fermat and Kraitchik*, la méthode est alors encore plus coûteuse que la méthode des divisions successives. Dans les années 1920, Maurice Kraitchik a amélioré l'efficacité de la méthode de Fermat. Son idée essentielle est que pour factoriser N, il *suffit* de trouver une différence de deux carrés qui soit un multiple de N.

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. Plus spécifiquement, les entiers $\operatorname{pgcd}(u-v, N)$ et $\operatorname{pgcd}(u+v, N)$ sont des facteurs non triviaux de N.*

Démonstration. Posons $g = \operatorname{pgcd}(u - v, N)$ et $g' = \operatorname{pgcd}(u + v, N)$. 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 deux l'est, l'autre vaut N, contradiction. Donc g et g' sont tous deux des facteurs non triviaux de N. □

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 fournissentun facteur non trivial de N.

Pour factoriser N, il s'agit donc de trouver de tels couples (u, v). Kraitchik cherche pour cela des couples $(u_i, v_i)_{1\leqslant i\leqslant r}$ vérifiant

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

et tels que l'entier $\prod_{i=1}^r v_i$ soit un carré (dans $\mathbb{Z}$). Posant $u = \prod_{i=1}^r u_i$ et $v = \sqrt{\prod_{i=1}^r v_i}$, il vient

$$v^2 \equiv u^2 \pmod N.$$

En posant $K := X^2 - N \in \mathbb{Z}[X]$, alors $u_i^2 \equiv K(u_i) \pmod N$ pour tout $u_i \in \mathbb{Z}$. Il a donc cherché des éléments v_i de la forme $K(u_i)$ dont le produit est un carré. 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.

régler la question de l'efficacité et du coût

1.2.2 Recherche de congruences de carrés

Nous exposons ici une méthode (**attribution**) de recherche de couples (u, v) tels que $u^2 \equiv v^2 \pmod N$ et $u \not\equiv \pm v \pmod N$. Elle est basée sur la connaissance de congruences de la forme

$$u_i^2 \equiv Q_i \pmod N,$$

où $|Q_i|$ est suffisamment petit pour être factorisé. On fixe pour cela B une base de factorisation, c'est à dire un ensemble non vide fini de nombres premiers, et l'on dit qu'un entier $Q \in \mathbb{N} \setminus \{0, 1\}$ est *B-friable* si tous ces facteurs premiers sont dans B. La connaissance de suffisamment d'entiers Q_i qui sont B-friables permet de factoriser N.

Proposition 1.21. *Soit F une famille d'entiers dont les valeurs absolues sont B-friables. Si*

$$\#F \geqslant \#B + 2$$

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

Démonstration. Posons $F = \{Q_1, \ldots, Q_k\}$ (de sorte que $k = \#F$) et $B = (p_1, \ldots, p_m)$ (de sorte que $\#B = m$). Par hypothèse de friabilité, les éléments $Q_j, 1 \leqslant j \leqslant k$, s'écrivent alors

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

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

$$v_B(Q_j) := (v_{p_m}(Q_j), \ldots, v_{p_1}(Q_j), v_0)$$

L'entier Q_j est un carré si, et seulement si, les composantes de son vecteur $v_B(Q_j)$ sont paires, i.e. la réduction du vecteur $v_B(Q_j)$ modulo 2 est nulle. Par propriété des valuations, le vecteur associé au produit $Q_j \cdot Q_{j'}$ est le vecteur somme $v_B(Q_j) + v_B(Q_{j'})$. Autrement dit, le produit d'une sous-famille $\{Q_{j_1}, \ldots, Q_{j_s}\}$ de F est un carré si, et seulement si, les vecteurs $v_B(Q_{j_1}), \ldots, v_B(Q_{j_s})$ 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 $k \geqslant m + 2$, la famille $\{v_B(Q_1), \ldots, v_B(Q_k)\}$ est liée dans V et il existe de fait des éléments $l_1, \ldots, l_k \in \mathbb{F}_2$ tels que

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

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

Définition 1.22. Soient $B = \{p_1, \ldots, p_m\}$ une base de factorisation et $Q \in \mathbb{Z}$ un entier dont la valeur absolue est B-friable. On appelle *B-vecteur exposant de Q* et l'on note

$v_B(Q)$ le vecteur [4] des valuations

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

Étant données des congruences de la forme $u_i^2 \equiv Q_i \pmod N$, la preuve de la proposition fournit un procédé d'algèbre linéaire pour extraire une sous-famille des Q_i dont le produit des éléments est un carré. On trouve tout d'abord des $Q_{i_1}, \dots, Q_{i_k}$ dont la valeur absolue est B-friable [5]. Soit M la matrice

$$M := \begin{pmatrix} v_B(Q_{i_1}) \\ \vdots \\ v_B(Q_{i_k}) \end{pmatrix} \in \mathcal{M}_{k,\#B+1}(\mathbb{F}_2).$$

Soient $l_1, \dots, l_k$ les éléments de $\mathbb{F}_2$ donnés dans la preuve de la proposition tels que

$$\prod_{j=1}^{k} Q_{i_j}^{l_{i_j}}$$

soit un carré. Le vecteur $(l_1, \dots, l_k)$ est un élément du noyau de la matrice transposée de M. Nous verrons plus tard une adaptation de la méthode du pivot de Gauß permettant d'exhiber un tel élément.

1.2.3 Utilisation des fractions continues

L'introduction des fractions continues est motivée par le constat suivant. Si

$$u_i^2 = Q_i + kNb^2, \quad u_i, Q_i, b \in \mathbb{Z}, k \in \mathbb{N}^*$$

de telle sorte que $|Q_i|$ soit 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 $\sqrt{kN}$ **réf**. Fixons k un entier naturel non nul, posons $x = \sqrt{kN}$ et reprenons les notations 1.1 et celles développées à la fin de la sous-section 1.1.3. En vertu de l'identité

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

nous appelons *méthode de factorisation des fractions continues* la méthode de Kraitchik dans laquelle les entiers u_i sont donnés par les A_{i-1} et les v_i par les $(-1)^i Q_i$. On sait

4. L'élément v_0 est placé à droite et non au début car il correspondra au bit de poids faible du B-vecteur exposant le code.

5. Nous le ferons en factorisant les Q_i à disposition par divisions successives.

que les Q_n sont majorés (4) par $2\sqrt{kN}$; l'inverse, les $x^2 - N \in \mathbb{Z}[X], x \in \mathbb{N}$ ont une croissance linéaire de pente $2\sqrt{N}$ lorsque x s'éloigne de $\sqrt{N}$. À base de factorisation B fixée, 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) grace à un algorithme itératif dû à Gauß et exposé dans **réf**.

Définition 1.23. Pour tout $n \in \mathbb{N}^*$, on appelle *n-ième paire* (A, Q) le couple (A_{n-1}, Q_n).

Définition 1.24. Un ensemble de paires (A, Q) indexé par $n_1, \ldots, n_k$ 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 1.25. Par abus de langage, nous confonderons les B-vecteurs exposants $v_B(Q_n)$ et $v_B((-1)^n Q_n)$.

Je trouve que ça sert à rien de donner à moitié l'algo à cet endroit alors que le lecteur a très bien compris la méthode de Kraitchik et qu'on a donné nos arguments pour les fractions continues. M'est avis que le mieux est de faire ça en plus détaillé en tout début de la prochaine section. Si tu n'es pas d'accord on pourra remettre ce qu'il y avait avant.

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