Algorithme de Shor

Romain Cazali, Justine Sauvage et Jérôme Boillot

15 janvier 2021

1 Introduction

Le problème que l'algorithme de Shor permet de traiter est le suivant : on veut factoriser un nombre N, qui sera en général très grand. N n'est ni un multiple de deux, ni un carré, problèmes qui sont facilement solubles. On va en fait se ramener à un autre problème qui consiste à trouver la période d'une certaine fonction.

Dans l'optique de l'exposé à venir, nous avons eu pour objectif de donner un aspect plutôt visuel et intuitif des différentes opérations effectuées par l'algorithme, notamment pour la partie quantique. Cependant, pour éviter de tomber dans des erreurs dues à une considération trop intuitive, nous avons supporté ce point de vue par les calculs détaillés dans ce rapport.

2 L'algorithme : se ramener à une recherche d'ordre

Présentons tout d'abord l'algorithme dans son ensemble :

1. Choisir un nombre $x < N$.
2. Si $\text{pgcd}(x,\ N) \neq 1$ on a factorisé N.
3. Si $\text{pgcd}(x,\ N) = 1$, on cherche le plus petit entier r tel que $x^r \equiv 1 \pmod{N}$.
4. Si r est impair : retour à l'étape 1.
5. Si r est pair : on peut écrire $x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1)$.
   Or, par définition de r, on a $N \mid x^r - 1$.
   Il y a alors 3 cas possibles :

   - Si N partage des facteurs avec $x^{r/2} + 1$ et $x^{r/2} - 1$,
     ie $N = pq$ (p et q pas forcément premiers) avec $p \mid x^r + 1$ et $q \mid x^r - 1$,
     on obtient ces facteurs de la façon suivante :
     $p = \text{pgcd}(x^r + 1,\ N)$ et $q = \text{pgcd}(x^r - 1,\ N)$.
   - Si $N \mid x^{r/2} + 1$, alors $x^r \equiv -1 \pmod{N}$,
     alors on trouve un facteur trivial : $\text{pgcd}(N,\ x^{r/2} + 1) = N$.

- Sinon $N \mid x^{r/2} - 1$, alors on a $x^{r/2} \equiv 1 \pmod{N}$.
  Ceci est impossible par définition de r, donc r est le plus petit entier tel que $x^r \equiv 1 \pmod{N}$.

6. Vérifier que p ou q divise N. Sinon, reprendre à l'étape 1.

De toutes les étapes de cet algorithme, l'unique étape quantique est l'étape pour trouver r. En effet, en classique, ce problème est plus dur à résoudre que la factorisation. En revanche, en quantique, il existe un algorithme linéaire en le nombre de bits de l'entrée qui a une probabilité assez bonne de ne pas se tromper.

3 L'algorithme quantique : recherche de la période d'une fonction

3.1 Définitions

On a vu dans la partie précédente que trouver la période de la fonction définie par

$$f : a \to x^a \,[N] \tag{1}$$

permet de factoriser N.
On considère qu'on a déjà effectué la première étape de l'algorithme. On a donc choisi x premier avec N de façon aléatoire.

Soit $q = 2^l$ tel que $N^2 \leq q \leq 2N^2$ et $n = \lfloor \log(N) \rfloor$.
On définit alors les opérateurs transformée de Fourier quantique, notés QFT et U_f, respectivement par (2) et (3).

$$\forall |y\rangle \in Vect(|0\rangle, |1\rangle)^l, \quad QFT(|y\rangle) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{\frac{2i\pi xa}{q}} |a\rangle \tag{2}$$

$$\forall |a\rangle \in Vect(|0\rangle, |1\rangle)^l, \quad U_f(|a\rangle \otimes |0^n\rangle) = |a\rangle \otimes |f(a)\rangle \tag{3}$$

3.2 Le détail de l'algorithme.

Nous partons avec comme état de départ, l'état ci-dessous (4)

$$\left|0^l\right\rangle \otimes |0^n\rangle \tag{4}$$

Nous considérerons dans la suite que l'état quantique est composé de deux registres : les deux composantes du produit tensoriel dans ce premier état. Nous allons également suivre rigoureusement l'ordre d'apparition des opérations dans l'algorithme en le lisant de gauche à droite.

Appliquons donc la première transformée de Fourier au premier registre, on obtient alors :

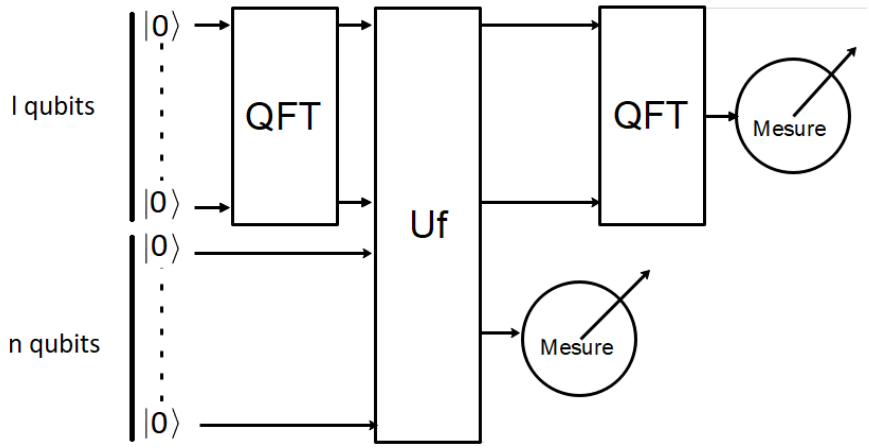

FIGURE 1 – L'algorithme quantique de recherche de période est l'algorithme

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \otimes |0^n\rangle \tag{5}$$

Plus intuitivement, la première transformée de Fourier permet de faire en sorte que le premier registre balaie tout les entiers de 0 à $q-1$.

Maintenant, appliquons U_f à l'ensemble des deux registres. On obtient immédiatement :

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} (|a\rangle \otimes |f(a)\rangle) \tag{6}$$

Nous allons maintenant réaliser la première mesure sur le deuxième registre.
On obtient alors une certaine valeur $f(s) = y$, en posant s le minimum sur $[\![0, q-1]\!]$ vérifiant $f(s) = y$.

Soit $m = card\{j, rj + s \in [\![0; q-1]\!]]\}$ ie le nombre d'entier congru à s *modulo* r dans $[\![0; q-1]\!]$.

Comme f est périodique, on a $\forall j, f(rj+s) = f(s)$.
Donc immédiatement après la mesure on obtient l'état :

$$\frac{1}{\sqrt{q}} \sum_{j=0}^{m-1} |jr+s\rangle \otimes |f(s)\rangle \tag{7}$$

Ce qui donne après renormalisation :

$$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |jr+s\rangle \otimes |f(s)\rangle \tag{8}$$

Il ne reste plus qu'à appliquer la deuxième transformée de Fourier, ce qui donne *in fine* l'état suivant :

$$\frac{1}{\sqrt{mq}} \sum_{b=0}^{q-1} e^{\frac{2i\pi sb}{q}} \sum_{j=0}^{m-1} \left(e^{\frac{2i\pi rb}{q}} \right)^j |b\rangle \otimes |f(s)\rangle \tag{9}$$

"Avec les mains" : On filtre les états congrus à un certain entier s modulo r en mesurant $|f(s)\rangle$. On se retrouve avec des états espacés de la période r. Une transformée de Fourier permettra ensuite d'extraire cette période.

Ceci est illustré en figure 2 :

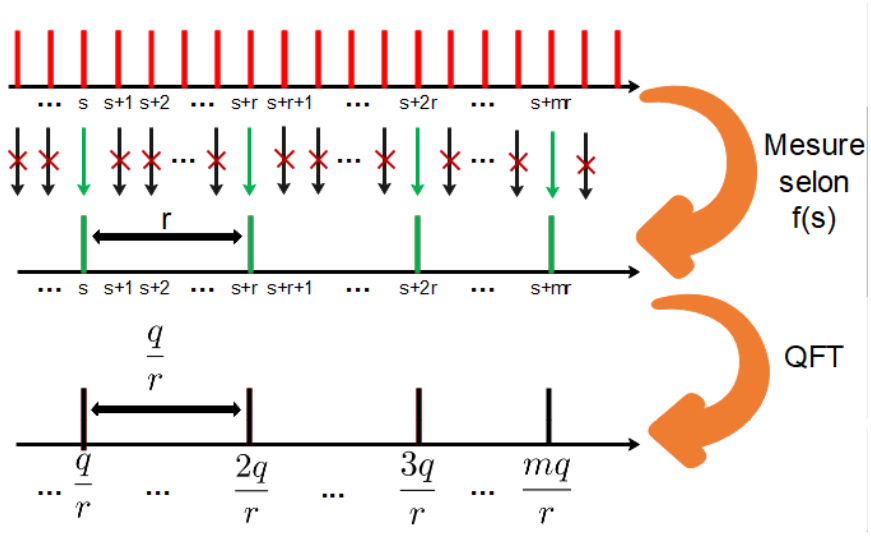

FIGURE 2 – Résumé de la procédure quantique

1. La première ligne représente l'état après l'application de U_f.
2. La seconde montre l'état après la mesure d'un élément particulier de $|f(a)\rangle = |f(s)\rangle$. Seuls les états associés à $|f(s)\rangle$ survivent à la mesure. Ce sont les états tels que $|a = s + jr\rangle$.
3. La troisième ligne montre la répartition des états après la transformée de Fourier.
4. On aura une probabilité très élevée de mesurer un des états situé en un multiple de q/r.

La dernière mesure donnera un $|b\rangle$ particulier qui permettra, parfois, de remonter à r.

3.3 Exploitation du résultat de la mesure

La deuxième QFT donne dans le premier registre, comme cela a été vu précédemment,

$$\frac{1}{\sqrt{mq}} \sum_{b=0}^{q-1} e^{2\pi i \frac{sb}{q}} \left(\sum_{j=0}^{m-1} e^{2\pi i \frac{jrb}{q}} \right) |b\rangle \tag{10}$$

À partir de cela on va déduire la probabilité pour chaque b d'être le résultat de la mesure. La probabilité étant le carré de l'amplitude, on va calculer pour chaque b l'amplitude (complexe) :

$$\frac{1}{\sqrt{mq}} e^{2\pi i \frac{sb}{q}} \left(\sum_{j=0}^{m-1} \omega_0^j \right) \quad \text{avec} \quad \omega_0 = e^{2\pi i \frac{br}{q}} \tag{11}$$

$$\text{On a} \quad \sum_{j=0}^{m-1} \omega_0^j = \begin{cases} m \quad \text{si} & \omega_0 = 1 \\ \dfrac{1 - e^{2\pi i \frac{mrb}{q}}}{1 - e^{2\pi i \frac{rb}{q}}} & \text{sinon} \end{cases} \tag{12}$$

Il y a 2 cas :

3.3.1 Cas simple : r divise q

Dans ce cas, on a $m = {}^{q}\!/_{r}$.
L'équation 12 nous donne que la somme des puissances de ω_0 est égale à m ssi ${}^{rb}\!/_{q}$ est un entier, ie $\exists c \in \mathbb{N}, b = c\dfrac{q}{r}$. Dans ce cas l'équation 12 devient :

$$\frac{1}{\sqrt{mq}} e^{2\pi i \frac{sb}{q}} m = \sqrt{\frac{m}{q}} e^{i \times \ldots} \tag{13}$$

Ainsi, la probabilité d'apparition d'un tel b est de ${}^{m}\!/_{q} = {}^{1}\!/_{r}$. Or, il existe r tels b (car $b = cm$, ${}^{q}\!/_{m} = r$ et $b \leq q$), donc à eux seuls ils accaparent toutes les possibilités et donc la mesure fournira un b tel que $b = {}^{cq}\!/_{r}$ avec c tiré uniformément sur $[\![0; r-1]\!]$.
On a donc ${}^{b}\!/_{q} = {}^{c}\!/_{r}$ et on connaît b et q. Dans ce cas, si $\text{pgcd}(c,\ r) = 1$, alors en divisant b et q par $\text{pgcd}(b,\ q)$ on obtiendra c et r et ainsi on aura le r voulu. Si ce n'est pas le cas, on pourra le remarquer en testant si ${}^{q}\!/_{\text{pgcd}(b,\ q)}$ est un période de f ou non.
La probabilité de succès est la probabilité d'avoir $\text{pgcd}(c,\ r) = 1$ quand c est tiré uniformément dans $[\![0; r-1]\!]$ et cette probabilité est égale à ${}^{\varphi(r)}\!/_{r}$ car φ désigne l'indicatrice d'Euler et donc $\varphi(r)$ désigne le nombre de nombres inférieurs ou égaux à r et premiers avec r. Il y a donc $\varphi(r)$ c tels que $\text{pgcd}(c,\ r) = 1$ parmi les r possibilités pour c. D'où $\mathbb{P}(c \in \{c < r \mid \text{pgcd}(c,\ r) = 1\}) = {}^{\varphi(r)}\!/_{r}$.

D'après [1, p. 234],

$$\forall r \geq 3, \quad \frac{\varphi(r)}{r} > \frac{1}{e^{\gamma} \log\log r + \dfrac{3}{\log\log r}} \tag{14}$$

On peut en déduire par simple majoration ou minoration des différents éléments que :

$$\forall r \geq 3, \quad \frac{\varphi(r)}{r} > \frac{1}{4\log\log r} \tag{15}$$

Ainsi, on a une probabilité d'avoir $\text{pgcd}(c,\ r) = 1$ supérieure ou égale à $1/4\log\log r$.
On peut également remplacer r par q étant donné que $r \leq q$.

Bien que cette probabilité ne soit pas très élevée (déjà inférieure à $1/2$ à partir de $q = 6$), on peut l'amplifier en faisant tourner le circuit plusieurs fois.

Au bout de T fois, on a par indépendance des tirages :

$$\mathbb{P}(\text{Au moins un succès au bout de T itérations}) \geq 1 - \left(1 - \frac{1}{4\log\log q}\right)^T \tag{16}$$

On peut avec cette inégalité rendre la probabilité de succès égale à $1-\varepsilon$ avec $\varepsilon > 0$ en posant $T = \mathcal{O}(|\log\varepsilon|\log\log q)$.

En effet,

$$\begin{aligned}
& 1-\varepsilon \leq 1 - \left(1 - \frac{1}{4\log\log q}\right)^T \\
\Leftrightarrow \quad & \varepsilon \geq \left(1 - \frac{1}{4\log q}\right)^T \\
\Leftrightarrow \quad & \log\varepsilon \geq T\log\left(1 - \frac{1}{4\log q}\right) \\
\Leftrightarrow \quad & \log\varepsilon \geq \frac{-T}{4\log q} \quad \text{pour } q \text{ assez grand} \\
\Leftrightarrow \quad & T \geq 4|\log\varepsilon|\log\log q
\end{aligned}$$

Ainsi, en itérant assez de fois le processus, on aura une bonne probabilité de trouver un tel r.

3.3.2 Cas complexe : r ne divise pas q

Remarquons tout d'abord qu'il est peu probable d'avoir $rb/q \in \mathbb{N}$. On peut avoir une idée de pourquoi avec la figure 3.
Ainsi, il est peu probable que $\omega_0 = 1$. Avec la technique de l'angle moitié on a l'équation 12 qui devient :

$$\frac{1 - e^{2\pi i\frac{mrb}{q}}}{1 - e^{2\pi i\frac{rb}{q}}} = e^{\pi i\frac{rb}{q}(m-1)}\frac{\sin\left(\pi\frac{mrb}{q}\right)}{\sin\left(\pi\frac{rb}{q}\right)} \tag{17}$$

On obtient alors en prenant le module au carré la probabilité $\mathbb{P}(b)$ d'obtenir l'état associé à la valeur propre b :

$$\mathbb{P}(b) = \frac{1}{mq}\left|\frac{\sin\left(\pi\frac{mrb}{q}\right)}{\sin\left(\pi\frac{rb}{q}\right)}\right|^2 \tag{18}$$

Le dénominateur s'annule lorsque $b \equiv {}^{q}/_{r} \pmod{n}$ avec n entier, ce qui donne les pics de probabilités. On obtient donc b un nombre proche de ${}^{q}/_{r}$ avec une probabilité élevée.

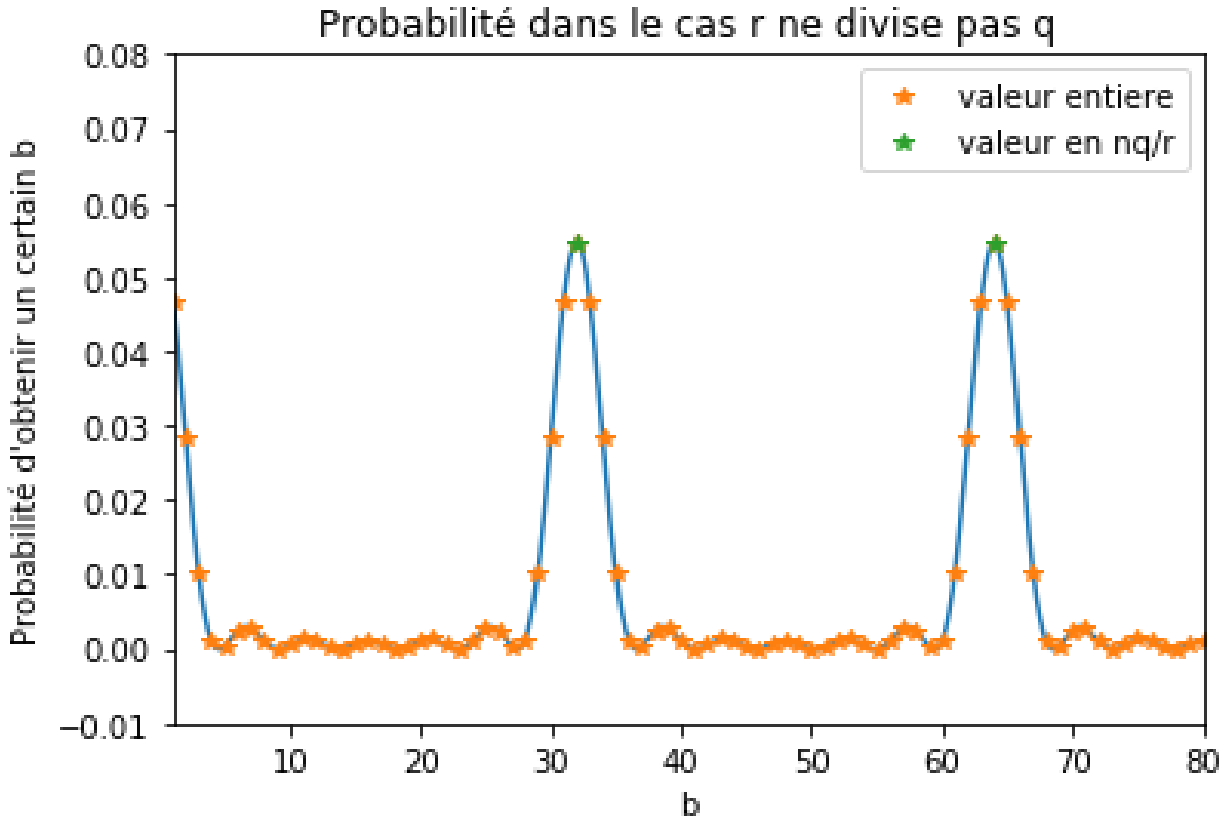

FIGURE 3 – Illustration de la forte probabilité d'obtenir un nombre proche d'un multiple de ${}^{q}/_{r}$. On a tracé en bleu la probabilité de l'équation 18. Les points oranges correspondent aux valeurs potentielles de b (les entiers) et les points en verts correspondent aux valeurs multiples de ${}^{q}/_{r}$.

On admet qu'on peut écrire l'inégalité suivante avec une grande probabilité (la figure 3 donne une idée de pourquoi c'est souvent vrai) :

$$\left|\frac{b}{q} - \frac{c}{r}\right| \leq \frac{1}{2q} \tag{19}$$

En supposant $q > r^2$ on a :

$$\left|\frac{b}{q} - \frac{c}{r}\right| \leq \frac{1}{2r^2} \quad \text{pour} \quad c \in [\![0; r-1]\!] \tag{20}$$

Or, d'après 23, si $\text{pgcd}(c,\ r) = 1$ alors c/r est un convergent de b/q et on peut ainsi déterminer la valeur de r en essayant tous les convergents de b/q. Le nombre d'étapes de l'algorithme d'Euler est en $\mathcal{O}(\log(q))$ donc le nombre de convergents à tester est b/q. Or, on peut tester si le convergent est la période de f en $\mathcal{O}(1)$ donc on va s'en sortir en temps polynômial en le nombre de chiffres de N.
Pour les mêmes raisons que dans le cas simple ci-dessus, on a une probabilité d'avoir $\text{pgcd}(c,\ r) = 1$ de $1/4(\log\log r)$ et on peut faire le même processus pour améliorer les chances de réussite.

4 Conclusion

L'algorithme de Shor ramène la factorisation à une recherche de période, facile à résoudre avec une méthode quantique. Toutes les autres opérations sont effectuées de façon classique. En conclusion, il a de bonnes probabilités de renvoyer un bon résultat tout en s'exécutant en temps polynômial en le nombre de bits de N.
Nous avons découvert en faisant ce rapport que l'algorithme est probabiliste contrairement à ce qui est transmis la plupart du temps dans les différentes vulgarisations de l'algorithme de Shor.
De plus, nous nous sommes rendu compte qu'à causes des fortes limitations sur le nombre de qubits des ordinateurs quantiques, cet algorithme est aujourd'hui encore peu efficace . En effet, le plus grand nombre qui a pu être factorisé à ce jour avec cet algorithme est le nombre 143 en avril 2012 [5]. Cela est loin du petit programme Python que nous avons réalisé qui imite le comportement de l'algorithme de Shor tout en simulant la partie quantique par un équivalent classique : cet algorithme permet de factoriser des nombres bien plus grands peu temps. Cependant, sous réserve de progrès technologiques important, on peut envisager un futur dans lequel le RSA serait compromis.

5 [Annexe] Fractions continues et convergents

5.1 Fractions continues

Tout nombre réel peut être développé en fraction continue. Cependant, on va ici étudier le cas des rationnels. En effet, la propriété ici énoncée est simple à démontrer dans ce cas et c'est lui seul qui nous intéresse.
On va, pour exhiber la fraction continue de $^a/_b$, exécuter l'algorithme d'Euclide ce qui va nous fournir les facteurs de la suite représentant la fraction continue.
Prenons un exemple : $^{634}/_{535}$ et appliquons l'algorithme d'Euclide sur ces deux relatifs.

$$\begin{aligned} 634 &= \mathbf{1} \times 534 &+ 99 \\ 535 &= \mathbf{5} \times 99 &+ 40 \\ 99 &= \mathbf{2} \times 40 &+ 19 \\ 40 &= \mathbf{2} \times 19 &+ 2 \\ 19 &= \mathbf{9} \times \mathbf{2} &+ 1 \end{aligned}$$

On a ainsi l'égalité suivante :

$$\frac{634}{535} = \mathbf{1} + \cfrac{1}{\mathbf{5} + \cfrac{1}{\mathbf{2} + \cfrac{1}{\mathbf{2} + \cfrac{1}{\mathbf{9} + \cfrac{1}{\mathbf{2}}}}}} \tag{21}$$

On peut alors décrire la fraction précédente par $^{634}/_{535} = [\mathbf{1}; \mathbf{5}; \mathbf{2}; \mathbf{2}; \mathbf{9}; \mathbf{2}]$.

5.2 Convergents

On appelle convergent de $[a_0; a_1; \ldots; a_n]$, tout rationnel décrit par $[a_0; a_1; \ldots; a_m]$ avec $m \leq n$.
Deux propriétés viennent enrichir les convergents :
Soit x une fraction continue et $^{p_n}/_{q_n}$ une suite des convergents de x. On a alors :

$$\text{pgcd}(p_n,\ q_n) = 1 \text{ et } \left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2} \tag{22}$$

Et réciproquement

$$\forall\, \frac{p}{q} \in \mathbb{Q} \text{ où } \text{pgcd}(p,\ q) = 1, \left| x - \frac{p}{q} \right| < \frac{1}{2q^2} \ \Rightarrow\ \frac{p}{q} \text{ est un convergent de } x \tag{23}$$

On admettra ici ce théorème qui est montré dans les notes de [4, Theorem 1.3.4 on p. 22].

Références

[1] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory.* MIT Press, Cambridge, MA, USA, 1996.

[2] Ronald de Wolf. Quantum computing, 2011.

[3] EPFL. Factorisation et algorithme de shor, 2014.

[4] Cor Kraaikamp Wieb Bosma. Continued fractions, August 2013.

[5] Nanyang Xu, Jing Zhu, Dawei Lu, Xianyi Zhou, Xinhua Peng, and Jiangfeng Du. Quantum factorization of 143 on a dipolar-coupling nmr system, 2011.

Et merci beaucoup à Elena Kirshanova pour son aide précieuse !