Compléments pour l'algorithme de Shor

Mathis Beaudoin, C2T3, Trois-Rivières

Été 2024

Table des matières

Avant-propros

Le présent document a été conçu lors de mon stage au C2T3 durant l'été 2024. Il s'agit d'un complément au document principal sur l'algorithme de Shor. Ainsi, on y trouve de la documentation sur les différents outils mathématiques qui permettent à l'algorithme de fonctionner, mais qui ne sont pas absolument nécessaires pour le réaliser. Encore une fois, je ne prétends pas être un expert des champs mathématiques que j'expose, car il s'agit là aussi de ma seule expérience jusqu'à maintenant.

Ce complément contient une section sur la transformée de Fourier, la théorie des groupes, la théorie des nombres, les fractions continues, l'explication du pseudocode et sur une manière de tricher pour rendre l'algorithme de Shor surpuissant. Finalement, les références se trouvent à la fin complètement.

J'espère que ce document pourra être utile. Bonne lecture !

- Mathis Beaudoin, étudiant au baccalauréat en sciences de l'information quantique à l'UdS

A Transformée de Fourier

Une fonction périodique est une fonction qui se répète après un certain temps T qu'on nomme la période. En termes mathématiques, on écrit que $f(x+T) = f(x)$. De plus, il va de soi que pour tout entier m, $f(x+mT) = f(x)$. Par exemple, les fonctions sinus, cosinus et constantes sont des fonctions périodiques. Aussi, si on combine deux fonctions différentes de même période, alors la fonction résultante est périodique et a la même période. On peut montrer que l'ensemble de fonctions $\{\sin(nx), \cos(nx)\}_{\forall n \in \mathbb{N}} = \{1,\ \cos(x),\ \sin(x),\ ...,\ \cos(nx),\ \sin(nx),\ ...\}$ forme une base pour les fonctions périodiques, c'est-à-dire que toute fonction $f(x)$ période s'écrit comme une combinaison linéaire des éléments de cet ensemble [1].

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cos(nx) + b_n \sin(nx)\right) \tag{A.1}$$

Les a_n et b_n sont tous des coefficients réels. Évidemment, (A.1) est vraie si la série infinie converge, ce qui se produit la plupart du temps et qu'on peut montrer à l'aide de théorèmes qui ne nous intéressent pas ici [1]. Le facteur $\frac{1}{2}$ pour a_0 est présent afin de plus facilement généraliser des résultats qui arriveront plus tard. En fait, l'équation (A.1) correspond à la série de Fourier de la fonction périodique $f(x)$ sous la forme sinus-cosinus. Il existe d'autres formes qu'on montrera plus tard. On aimerait savoir comment calculer la valeur des coefficients afin de connaître véritablement l'expansion de $f(x)$ en série de Fourier, car pour l'instant les a_n et b_n sont des variables bidon.

Détermination des coefficients (forme sinus-cosinus)

Soit une fonction périodique $f(x)$ de période $T = 2\pi$ qu'on peut exprimer selon (A.1). On intègre (A.1) de $-\pi$ à π pour obtenir la valeur de a_0.

$$\int_{-\pi}^{\pi} f(x)dx = \int_{-\pi}^{\pi} \left[\frac{1}{2}a_0 + \sum_{n=1}^{\infty}(a_n \cos(nx) + b_n \sin(nx))\right] dx$$

$$= \int_{-\pi}^{\pi} \frac{1}{2}a_0 dx + \sum_{n=1}^{\infty}\left(\int_{-\pi}^{\pi} a_n \cos(nx)dx + \int_{-\pi}^{\pi} b_n \sin(nx)dx\right) = \frac{1}{2}2\pi a_0 + \sum_{n=1}^{\infty}(a_n \cdot 0 + b_n \cdot 0) = \pi a_0$$

$$\implies a_0 = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)dx \tag{A.2}$$

Puis, on intègre (A.1) de $-\pi$ à π mais en multipliant d'abord par $\cos(mx)$ où m est un entier positif quelconque. On utilisera le fait que $\cos(nx)\cos(mx) = \frac{1}{2}\cos((n-m)x) + \frac{1}{2}\cos((n+m)x)$ et on ferra attention aux différents cas possibles ($n \neq m, n = m$).

$$\int_{-\pi}^{\pi} f(x)\cos(mx)dx = \int_{-\pi}^{\pi}\left(\frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos(nx) + b_n \sin(nx))\right)\cos(mx)dx$$

$$= \int_{-\pi}^{\pi}\frac{a_0}{2}\cos(mx)dx + \sum_{n=1}^{\infty}\left(\int_{-\pi}^{\pi} a_n \cos(nx)\cos(mx)dx + \int_{-\pi}^{\pi} b_n \sin(nx)\cos(mx)dx\right)$$

$$= \sum_{n=1}^{\infty}\left(\int_{-\pi}^{\pi}\frac{a_n}{2}\cos((n-m)x)dx + \int_{-\pi}^{\pi}\frac{a_n}{2}\cos((n+m)x)dx\right) = a_m\pi$$

$$\implies a_m = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(mx)dx \implies a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(nx)dx \tag{A.3}$$

Finalement, on intègre (A.1) de $-\pi$ à π mais en multipliant par $\sin(mx)$ où m est un entier positif quelconque. On utilisera le fait que $\sin(nx)\sin(mx) = \frac{1}{2}\cos((n-m)x) - \frac{1}{2}\cos((n+m)x)$ et on ferra attention aux différents cas possibles ($n \neq m, n = m$). Des calculs similaires à ce qui permet de trouver (A.3) indique que

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(nx)dx \tag{A.4}$$

Pour résumer, les coefficients de (A.1) sont :

1. $a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(nx)dx,\ \forall n = 0, 1, 2, ...$
2. $b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(nx)dx,\ \forall n = 1, 2, ...$

Il n'y a aucune justification particulière quant au choix des bornes d'intégration. Autrement dit, on aurait pu prendre n'importe quel intervalle d'intégration de taille 2π (0 à 2π par exemple) pour faire les calculs précédents du fait que $f(x)$ est périodique. De plus, on ne vérifie pas ici les critères permettant d'inverser la somme et l'intégrale, mais on peut montrer que la permutation est autorisée dans ce cas [1]. En général, beaucoup de fonctions périodiques ont une série de Fourier bien que pour cela, certaines conditions doivent être respectées [1]. Finalement, si on additionne deux fonctions périodiques f_1 et f_2 ayant une série de Fourier, alors la fonction résultante $f_1 + f_2$ possède aussi une série de Fourier et ses coefficients correspondent à la somme des coefficients de f_1 et f_2 [1].

Détermination des coefficients (forme exponentielle)

On sait que $\cos(nx) = \frac{e^{inx}+e^{-inx}}{2}$ et que $\sin(nx) = \frac{e^{inx}-e^{-inx}}{2i}$. On remplace cela dans (A.1) afin d'avoir

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty}\left(a_n\left(\frac{e^{inx}+e^{-inx}}{2}\right) + b_n\left(\frac{e^{inx}-e^{-inx}}{2i}\right)\right) = \frac{a_0}{2} + \sum_{n=1}^{\infty} e^{inx}\left(\frac{a_n - ib_n}{2}\right) + \sum_{n=1}^{\infty} e^{-inx}\left(\frac{a_n + ib_n}{2}\right)$$

On remarque que les termes entre parenthèses dans la dernière égalité sont conjugués l'un de l'autre. Alors, on fait des tours de passe-passe avec l'indice des sommes pour les combiner.

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} c_n e^{inx} + \sum_{n=1}^{\infty} \bar{c}_n e^{-inx} = \frac{a_0}{2} + \sum_{n=1}^{\infty} c_n e^{inx} + \sum_{n=-1}^{-\infty} \bar{c}_{-n} e^{inx}$$

$$= \sum_{n=-\infty}^{\infty} c_n e^{inx} \quad \text{où} \quad c_n = \begin{cases} \frac{1}{2}(a_{-n} + ib_{-n}) & \text{si } n \leq -1 \\ \frac{1}{2}(a_n - ib_n) & \text{si } n \geq 1 \\ \frac{a_0}{2} & \text{si } n = 0 \end{cases} \tag{A.5}$$

Afin de trouver la valeur des c_n, on peut remplacer (A.3) et (A.4) dans chacun des cas de (A.5).

$n \geq 1$:

$$\frac{1}{2}(a_n - ib_n) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\left(\cos(nx) - i\sin(nx)\right)dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-inx}dx$$

$n = 0$:

$$\frac{a_0}{2} = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)dx$$

$n \leq -1$:

$$\frac{1}{2}(a_{-n} + ib_{-n}) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\left(\cos(-nx) + i\sin(-nx)\right)dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-inx}dx$$

Donc, $\forall n$:

$$c_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-inx}dx \tag{A.6}$$

Période quelconque pour la forme sinus-cosinus

Jusqu'à présent, on a fait les calculs seulement pour des fonctions ayant une période de 2π. On veut étendre les équations à une fonction $f(t)$ de période T quelconque. Pour ce faire, on peut employer un changement de variable afin de redimensionner la fonction pour qu'elle est une période de 2π. On pose $t = \frac{x}{2\pi}T$, ce qui donne bien à $f(x)$ une période de 2π et lui permet d'être écrite comme (A.1). Cependant, on voudrait que les équations soient écrites selon la variable d'origine t. Puisque $x = \frac{2\pi}{T}t$, alors $dx = \frac{2\pi}{T}dt$ et l'intervalle d'intégration passe de $[-\pi, \pi]$ à $[-\frac{T}{2}, \frac{T}{2}]$. On obtient alors la série de Fourier pour une fonction ayant une période arbitraire

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty}\left(a_n\cos\left(\frac{2\pi n}{T}t\right) + b_n\sin\left(\frac{2\pi n}{T}t\right)\right) \tag{A.7}$$

avec des coefficients

$$a_n = \frac{2}{T}\int_{-T/2}^{T/2} f(t)\cos\left(\frac{2\pi n}{T}t\right)dt,\ b_n = \frac{2}{T}\int_{-T/2}^{T/2} f(t)\sin\left(\frac{2\pi n}{T}t\right)dt \tag{A.8}$$

Période quelconque pour la forme exponentielle

On peut appliquer le même raisonnement à (A.5) et (A.6) pour obtenir

$$f(t) = \sum_{-\infty}^{\infty} c_n e^{\frac{2\pi in}{T}t} \tag{A.9}$$

avec des coefficients

$$c_n = \frac{1}{T}\int_{-T/2}^{T/2} f(t)e^{\frac{-2\pi in}{T}t}dt \tag{A.10}$$

Obtention de la transformée de Fourier

On pose $k_n = \frac{2\pi n}{T}$, $\Delta k = \frac{2\pi}{T}$ et $C(k_n) = \frac{T}{\sqrt{2\pi}} c_n = \frac{1}{\sqrt{2\pi}} \int_{-T/2}^{T/2} f(t) e^{-ik_n t} dt$ qu'on remplace dans (A.9) et (A.10) [2].

$$f(t) = \sum_{n=-\infty}^{\infty} c_n e^{ik_n t} = \sum_{n=-\infty}^{\infty} \left(\frac{1}{T} \int_{-T/2}^{T/2} f(t) e^{-ik_n t} dt \right) e^{ik_n t} = \frac{1}{2\pi} \sum_{n=-\infty}^{\infty} \left(\int_{-T/2}^{T/2} f(t) e^{-ik_n t} dt \right) e^{ik_n t} \Delta k$$

$$= \frac{1}{\sqrt{2\pi}} \sum_{n=-\infty}^{\infty} C(k_n) e^{ik_n t} \Delta k \tag{A.11}$$

Si on laisse $T \to \infty$, les k_n deviennent de plus en plus proches les uns des autres et finissent par être continus. De plus, Δk devient de plus en plus petit dans ce cas.

$$\lim_{T\to\infty} C(k_n) = \lim_{T\to\infty} \frac{1}{\sqrt{2\pi}} \int_{-T/2}^{T/2} f(t) e^{-ik_n t} dt = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(t) e^{-ikt} dt = \hat{f}(k)$$

$$\implies \lim_{T\to\infty} f(t) = \lim_{T\to\infty} \frac{1}{\sqrt{2\pi}} \sum_{n=-\infty}^{\infty} C(k_n) e^{ik_n t} \Delta k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \hat{f}(k) e^{ikt} dk = \check{f}(t)$$

On définit la transformée de Fourier d'une fonction f comme étant

$$\hat{f}(k) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \check{f}(t) e^{-ikt} dt \tag{A.12}$$

et la transformée de Fourier inverse comme étant

$$\check{f}(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \hat{f}(k) e^{ikt} dk \tag{A.13}$$

Il n'est pas évident de voir cela directement, mais la transformée de Fourier permet de faire un changement de base [1]. Par exemple, on peut retrouver les différentes fréquences pures contenues dans un signal sonore dans le temps grâce à ces équations. En ce sens, la transformée de Fourier permet de passer de la base temporelle à la base des fréquences. La transformée de Fourier inverse permet évidemment de faire le changement de base dans l'autre direction. Une vidéo intuitive de 3Blue1Brown explique la transformée de Fourier de manière conceptuelle, bien que davantage de notions en analyse de Fourier soient nécessaires pour comprendre pleinement les équations.

B Théorie des groupes

Un groupe est l'union d'un ensemble non-vide G avec une certaine opération $\ll \cdot \gg$ [3] [4]. Un groupe doit respecter les propriétés suivantes :

1. Fermeture : $g_1 \cdot g_2 \in G, \ \forall g_1, g_2 \in G$
2. Associativité : $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3), \ \forall g_1, g_2, g_3 \in G$
3. Élément neutre : $\exists \ e \in G \ \ \text{t.q} \ \ g \cdot e = e \cdot g = g, \ \forall g \in G$
4. Élément inverse : $\exists \ g^{-1} \in G \ \ \text{t.q} \ \ g \cdot g^{-1} = g^{-1} \cdot g = e, \ \forall g \in G$

De plus, on dit qu'un groupe est fini si le nombre d'éléments dans G est fini. Justement, on appelle « l'ordre » de G le nombre d'éléments dans G qu'on symbolise par $|G|$. Aussi, un groupe est « abélien » si, en plus des propriétés de base d'un groupe, ses éléments commutent sous l'opération, c'est-à-dire que $g_1 \cdot g_2 = g_2 \cdot g_1,\ \forall g_1, g_2 \in G$. On définit « l'ordre » d'un élément $g \in G$ comme étant le plus petit entier positif r où $g^r = e$. De surcroît, un sous-groupe H de G est un sous-ensemble de G qui forme aussi un groupe sous la même opération. Finalement, pour alléger la notation, on écrira $g_1 g_2$ pour désigner $g_1 \cdot g_2$.

- *B.1* : $\forall g \in G$ où G est un groupe fini, $\exists$ un entier positif r tel que $g^r = e$.

> Si $g = e$, alors $r = 1$. Sinon, par la propriété de fermeture, à chaque puissance de g, on atteint un nouvel élément du groupe. Éventuellement, puisque G est fini, on atteint l'élément neutre à partir d'une certaine puissance de g. L'exposant de cette puissance correspond à r. □

- *B.2* : $1 \leq r \leq |G|$.

> L'ordre vaut 1 quand il s'agit de l'élément neutre. Sinon, pour tout autre élément $g \in G$, en poussant le raisonnement de la précédente démonstration à l'extrême, on peut atteindre tous les autres éléments avant d'arriver finalement à l'élément neutre. Dans ce cas, l'ordre correspond à $|G|$. □

Théorème de Lagrange : Si H est un sous-groupe d'un groupe fini G, alors $|H|$ divise $|G|$.

> On prend un élément $x \notin H$, mais qui est malgré tout dans G. On construit $Hx = \{hx \mid h \in H\}$. On voit que $Hx \cap H = \emptyset$ puisque pour que cela ne soit pas le cas, il faudrait par la propriété de fermeture que h et x soient dans H, ce qui n'est pas le cas pour x. De plus, on construit les éléments de Hx directement depuis H, donc forcément $|Hx| = |H|$. Si $Hx \cup H = G$, on a terminé. Sinon, on recommence avec $Hy = \{hy \mid h \in H\}$ où y n'est à la fois pas dans Hx et H. Ainsi de suite, puisque G est fini, on finit par couvrir tout G avec des sous-ensembles disjoints de même taille que H. Donc, $|H|$ divise $|G|$. □

- *B.3* : L'ordre d'un élément $g \in G$ divise $|G|$.

> Soient $g \in G$ un élément d'ordre r et $A = \{e, g, g^2, ..., g^{r-1}\}$. Il est assez facile de montrer que A forme un sous-groupe de G ayant une taille r. Par le théorème de Lagrange, on sait que $|A| = r$ divise $|G|$. □

On utilise des générateurs pour construire depuis ceux-ci les différents éléments de leur groupe. En d'autres mots, il s'agit d'une liste d'éléments $[g_1, ..., g_l]$ tous dans G qui, lorsqu'on leur applique parfois de manière répétée l'opération du groupe, permet de générer tout le groupe. On écrit $G = < g_1, ..., g_l >$ pour spécifier que la liste $[g_1, ..., g_l]$ génère le groupe G. Par exemple, à la démonstration B.3, $A = < g >$.

Un groupe G est cyclique s'il existe un élément $a \in G$ tel que $\forall g \in G,\ g = a^n$ pour un certain entier positif n. Dans ce cas, a est l'unique générateur pour G et il va de soi que l'ordre de a vaille $|G|$. Par exemple, le sous-groupe de la démonstration B.3 est cyclique.

- *B.4* : Tout groupe d'ordre premier est cyclique.

> Si l'ordre d'un groupe est un nombre premier p, sachant que l'ordre des éléments divise l'ordre du groupe, alors l'ordre des éléments vaut 1 ou p. S'il vaut 1, alors il s'agit de l'ordre pour l'élément neutre. Donc, pour tous les autres éléments, l'ordre est p. Comme p correspond aussi à la taille du groupe, cela veut dire que, depuis les puissances d'un certain élément $g \neq e$, on peut atteindre tout le monde dans le groupe. Il s'agit de la définition d'un groupe cyclique. □

- *B.5* : Tout sous-groupe d'un groupe cyclique est aussi cyclique.

Soient $G = < a >$ un groupe cyclique généré par a et H un sous-groupe de G. Si $H = \{e\}$, alors c'est vrai forcément. Sinon, H contient au moins un élément $a^n \neq e$ pour un certain entier positif n. Soit m le plus petit entier positif tel que $a^m \in H$. Puisque $m \leq n$, on peut dire qu'il existe q et r tels que $n = qm + r$ où $0 \leq r < m$. Donc, $a^n = a^{qm+r} = (a^m)^q a^r \implies a^r = (a^m)^{-q} a^n$. Du fait que $a^m \in H$, toutes ses puissances et leurs inverses sont aussi dans H. Par fermeture, puisque $(a^m)^{-q}$ et a^n sont dans H, a^r l'est aussi. Pourtant, on sait que $0 \leq r < m$ où m est le plus petit entier positif tel que $a^m \in H$. Forcément, il faut que $r = 0$. Donc, $n = qm \implies a^n = (a^m)^q$. Ainsi, n'importe quel élément de H est généré depuis a^m, ce qui fait de H un sous-groupe cyclique de G. □

- *B.6* : Si $g \in G$ a un ordre fini r, alors $g^m = g^n$ ssi $m \equiv n \bmod r$.

($\implies$) : Avec un ordre fini, on peut générer un sous-groupe cyclique $\{e, g, g^2, ..., g^{r-1}\}$. Si $m = n$, alors c'est vrai. Sinon, on peut dire sans perte de généralité que $m > n$. Pour que $g^m = g^n$, il faut donc forcément que $m = kr + q$ pour un certain entier k où $0 \leq q < r$. Ainsi, $g^m = g^{kr+q} = g^{kr} g^q = g^q$. De ce fait, $g^m = g^n = g^q$ où q est le résultat modulo r de m. Alors, $m \equiv n \bmod r$. □

($\impliedby$) : Puisque $m \equiv n \bmod r$, $g^m = g^{kr+n} = g^{kr} g^n = g^n$. □

- *B.7* : Si G est un groupe fini et que $a \in G$ possède un ordre r, alors $< a^k > = < a^l >$ ssi $\text{pgcd}(k, r) = \text{pgcd}(l, r)$. Il suit que les seuls sous-groupes distincts de $< a >$ soient les sous-groupes $< a^d >$ où d est un diviseur positif de r.

($\impliedby$) : Si $\text{pgcd}(k, r) = \text{pgcd}(l, r) = d$, alors $\text{pgcd}(k, r) = \text{pgcd}(l, r) = \text{pgcd}(d, r) = d$. Donc, d divisent k, l et r. On crée $< a^d > = \{e, a^d, a^{2d}, ..., a^{r-d}\}$ qui est un sous-groupe de $< a >$ ayant une taille $\frac{r}{d}$. Puisque $d|k$, $a^k \in < a^d > \implies < a^k > \subseteq < a^d >$. De plus, par Bézout, $ks + rt = d \implies a^d = a^{ks+rt} = (a^k)^s (a^r)^t = (a^k)^s \implies a^d \in < a^k > \implies < a^d > \subseteq < a^k >$. Ainsi, $< a^k > = < a^d >$. En suivant la même démarche, on peut aussi dire que $< a^l > = < a^d >$. Au final, $< a^k > = < a^d > = < a^l >$. □

($\implies$) : Si $< a^k > = < a^l >$, alors $\text{pgcd}(k, r) = x = \text{pgcd}(x, r)$ et $\text{pgcd}(l, r) = y = \text{pgcd}(y, r)$. Par la démonstration de l'autre direction de cette preuve, $< a^x > = < a^k > = < a^l > = < a^y >$ où $| < a^x > | = \frac{r}{x}$ et $| < a^y > | = \frac{r}{y}$. Comme forcément $| < a^x > | = | < a^y > |$, on voit que $\frac{r}{x} = \frac{r}{y} \implies x = y$. Au final, $\text{pgcd}(k, r) = \text{pgcd}(l, r)$. □

On peut tirer plusieurs choses de la précédente preuve. Premièrement, on comprend que tous les sous-groupes distincts de $< a >$ sont de la forme $< a^d >$ où d est un diviseur positif de r. De plus, par construction, l'ordre de a^d correspond à $| < a^d > | = \frac{r}{d} = d'$. Par conséquent, les éléments $a^k \in < a >$ où $< a^k > = < a^d >$ ont aussi le même ordre $d' = \frac{r}{d} = \frac{r}{\text{pgcd}(k,r)}$, c'est-à-dire le même pgcd avec r.

- *B.8* : Si G est un groupe fini et que $a \in G$ possède un ordre r, alors le nombre d'éléments dans $< a >$ ayant un ordre $\frac{r}{d} = d'$ où d, d' sont des diviseurs positifs de r correspond à $\phi(d')$.

On veut connaître le nombre de sous-groupes $< a^k >$ où $1 \leq k \leq r$ qui sont équivalents au sous-groupe $< a^d >$ pour un certain diviseur positif d de r. On sait par B.7 que $< a^k > = < a^d >$ si $\text{pgcd}(k, r) = d \implies d|k, r \implies < a^k > = < a^{ld} > = < a^d >$ pour $1 \leq l \leq \frac{r}{d}$. Donc, on doit chercher parmi les sous-groupes $< a^{ld} >$.

Ainsi, a^{ld} possède le même ordre que a^d, soit $\frac{r}{d}$. Cependant, puisque $a^{ld} \in < a^d >$, on sait aussi que l'ordre de a^{ld} correspond à $\frac{\frac{r}{d}}{\text{pgcd}(ld, \frac{r}{d})}$. Alors, $\frac{r}{d} = \frac{\frac{r}{d}}{\text{pgcd}(ld, \frac{r}{d})} \implies \text{pgcd}(ld, \frac{r}{d}) = 1 \implies \text{pgcd}(l, \frac{r}{d}) = 1$. On compte donc le nombre de valeurs l dans l'intervalle $1 \leq l \leq \frac{r}{d}$ qui respecte cela, ce qui équivaut à $\phi(\frac{r}{d}) = \phi(d')$. □

Une autre notion fondamentale en théorie des groupes est le concept d'isomorphisme. Si G forme un groupe avec l'opération * et H forme un groupe avec l'opération &, un isomorphisme est une bijection $\psi : G \to H$ respectant $\psi(a * b) = \psi(a)\ \&\ \psi(b)\ \forall a, b \in G$. De plus, il y a une relation inverse $\psi^{-1} : H \to G$ respectant $\psi^{-1}(c\ \&\ d) =$

$\psi^{-1}(c) * \psi^{-1}(d)$ $\forall c, d \in H$. Dans un sens, deux groupes isomorphes sont équivalents, ce qu'on écrit $G \cong H$. Un isomorphisme possède plusieurs propriétés comme, par exemple, le fait que $\psi(a^k) = \psi(a)^k$ $\forall a \in G$ et $k \in \mathbb{Z}$.

- *B.9* : Si $G \cong H$, alors G est cyclique ssi H l'est aussi.

($\Longrightarrow$) : On suppose que G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = < g >$. Soit $\psi : G \to H$ et un élément quelconque $h \in H$. Alors, on sait qu'il existe $x \in G$ tel que $h = \psi(x)$. Puisque G est cyclique, $x = g^n$ pour un certain entier $n \implies \psi(x) = \psi(g^n) = (\psi(g))^n \in < \psi(g) > \implies H = < \psi(g) >$ $\implies$ H est cyclique. □

($\Longleftarrow$) : On suppose que H est cyclique, c'est-à-dire que $H = < h >$. On sait que $h = \psi(g)$ pour un certain $g \in G$. De plus, pour $x \in G$ quelconque, $\psi(x) \in H \implies \psi(x) = h^m$ pour un certain entier m. Donc, $\psi(x) = h^m = (\psi(g))^m = \psi(g^m) \implies g^m = x \implies x \in < g > \implies G = < g >$. Ainsi, G est cyclique. □

Par ailleurs, un autre aspect important en théorie des groupes est le produit cartésien de plusieurs groupes qu'on écrit $\prod_{i=1}^{n} G_i = G_1 \times ... \times G_n = \{(g_1, ..., g_n) \mid g_i \in G_i\}$. Le produit cartésien de groupes est aussi un groupe sous l'opération $(g_1, ..., g_n)(g_1^{'}, ..., g_n^{'}) = (g_1 g_1^{'}, ..., g_n g_n^{'})$. Il va de soi que $|G_1 \times ... \times G_n| = |G_1| \cdot ... \cdot |G_n|$.

- *B.10* : $\forall (g_1, ..., g_n) \in G_1 \times ... \times G_n$, l'ordre de $(g_1, ..., g_n)$ est le ppcm de l'ordre de chaque g_i.

On souhaiterait que $(g_1, ..., g_n)^m = (g_1^m, ..., g_n^m) = (e_{G_1}, ..., e_{G_n})$ où e_{G_i} est l'élément neutre du groupe G_i. Ainsi, il faut avoir assez de puissances de chaque élément du tuple pour retrouver l'élément neutre de chaque G_i. De plus, l'ordre requiert de trouver le plus petit m où cela se produit.

On rappelle que si r est l'ordre d'un élément g_i, alors $g_i^{kr} = (g_i^r)^k = (e)^k = e$ pour tout multiple kr de r. En prenant le ppcm de l'ordre des g_i du tuple, on sait qu'il s'agit du plus petit multiple de l'ordre de chaque g_i qui permet d'avoir $(e_{G_1}, ..., e_{G_n})$. Ainsi, ce ppcm correspond à l'ordre de $(g_1, ..., g_n)$ dans $G_1 \times ... \times G_n$. □

- *B.11* : Si les G_i sont cycliques et que leur ordre pair à pair est copremier, alors $\prod_{i=1}^{n} G_i$ est aussi cyclique.

Puisque les G_i sont cycliques, $G_1 = < g_1 >$ pour un certain $g_1 \in G_1$, ..., $G_n = < g_n >$ pour un certain $g_n \in G_n$. Par B.10, on sait que l'ordre de $(g_1, ..., g_n)$ correspond au ppcm de l'ordre de chaque g_i, soit ppcm$(|G_1|, ..., |G_n|)$ du fait que les groupes sont cycliques. Pour que $\prod_{i=1}^{n} G_i$ soit aussi cyclique, il faut un élément dont l'ordre est $|G_1| \cdot ... \cdot |G_n| = \prod_{i=1}^{n} |G_i|$. Si les $|G_i|$ sont tous copremiers entre eux, alors ppcm$(|G_1|, ..., |G_n|) = \prod_{i=1}^{n} |G_i| \implies \prod_{i=1}^{n} G_i = < (g_1, ..., g_n) >$. □

C Théorie des nombres

Divisibilité

Un entier d divise un autre entier n (qu'on note $d|n$) si et seulement si $n = dk$ pour un certain entier k [5]. Dans ce cas, d est un diviseur/facteur de n. Le plus grand commun diviseur entre a et b qu'on écrit pgcd(a, b) correspond au plus grand entier divisant à la fois a et b. Le pgcd est toujours ≥ 1, car 1 est le plus grand entier qui divise tous les entiers (l'autre étant -1, mais $-1 < 1$). Deux entiers a et b sont copremiers s'ils ne partagent que ± 1 comme facteur commun, c'est-à-dire si leur pgcd vaut 1. Un nombre p est premier s'il est uniquement divisible par 1 et lui-même.

- *C.1* : Si $a|b$ et $b|c$, alors $a|c$.

$a|b$ ssi $b = ak$, $b|c$ ssi $c = bk^{'} = akk^{'} = aq$. Donc, a est un facteur de c, ce qui veut dire que $a|c$. □

- *C.2* : Si $d|a$ et $d|b$, alors $d|ax+by$ où $x, y \in \mathbb{Z}$.

$d|a$ ssi $a = dk$, $d|b$ ssi $b = dk^{'}$. $ax + by = dkx + dk^{'}y = d(kx + k^{'}y)$. Donc, d est un facteur de $ax + by$, ce qui veut dire que $d|ax + by$. □

- *C.3* : Si $a, b \geq 1$ et $a|b$, alors $a \leq b$.

$a|b$ ssi $b = ak$. Puisque $a, b \geq 1$, il faut que $k \geq 1$. Forcément, $a \leq b$. □

- *C.4* : Si $a, b \geq 1$, $a|b$ et $b|a$, alors $a = b$.

Par C.3, on aurait que $a \leq b$ et $b \leq a \implies a = b$. □

- *Lemme de Gauss* : Pour $a, b, c \in \mathbb{Z}$, si $a|bc$ et que $\text{pgcd}(a, b) = 1$ (a et b sont copremiers), alors $a|c$.

Puisque $a|bc$, alors a divise soit b, soit c ou les deux. Dans les deux derniers cas, le lemme fonctionne. Dans le cas où $a|b$ uniquement, du fait qu'ils sont copremiers, il faut nécessairement que $a, b = \pm 1$. Ainsi, peu importe la valeur de c, $a = \pm 1$ le divise forcément. □

- *Théorème fondamental de l'arithmétique* : Pour un entier $a \geq 2$, il existe une factorisation unique de a en nombres premiers, c'est-à-dire une unique représentation $a = p_1^{\alpha_1}...p_n^{\alpha_n}$ où $\{p_j\}$ sont des nombres premiers distincts et $\{\alpha_j\}$ sont des entiers positifs (≥ 1).

Existence :

Pour $a = 2$, on dit que $p_1 = 2$ (2 est un nombre premier) et $\alpha_1 = 1$. Ensuite, on suppose qu'il existe une telle factorisation pour $2 \leq a \leq n$ et on regarde si c'est le cas pour $a = n + 1$. Si $n + 1$ est un nombre premier, alors c'est bon. Sinon, c'est que $n + 1$ est un nombre composé ($n+1 = kl$). Forcément, $2 \leq k, l \leq n$. Par l'hypothèse, k et l ont une factorisation en nombres premiers. Donc, $n+1$ est le produit de nombres premiers ce qui lui donne aussi une factorisation en nombres premiers. Au final, par récurrence, tous les nombres $a \geq 2$ ont une factorisation en nombres premiers. □

Unicité :

On suppose qu'il existe deux factorisations en nombres premiers différentes pour un même nombre a, c'est-à-dire que $a = p_1^{\alpha_1}...p_n^{\alpha_n} = q_1^{\beta_1}...q_n^{\beta_n}$. Alors, il y a au moins un des $p_i \notin \{q_i\}$ (ou inversement). Disons qu'il s'agisse de p_1. Puisque $p_1|a$, alors $p_1|q_1^{\beta_1}...q_n^{\beta_n}$, ce qui est équivalent à $p_1|q_1(q_1^{\beta_1-1}...q_n^{\beta_n})$. p_1 et q_1 sont des nombres premiers distincts, donc copremiers. Par le lemme de Gauss, $p_1|q_1^{\beta_1-1}...q_n^{\beta_n}$, ce qui indique que p_1 divise un des q_i. Cela n'est possible puisque les q_i sont premiers et différents de p_1. En répétant la même idée pour tous les p_i, on en déduit que $\{p_i\} = \{q_i\}$, ce qui veut dire en fait que $a = p_1^{\alpha_1}...p_n^{\alpha_n} = p_1^{\beta_1}...p_n^{\beta_n}$. Maintenant, on suppose qu'il y a un $\alpha_i \neq \beta_i$. Dans le cas où $\alpha_i < \beta_i$, $p_2^{\alpha_2}...p_n^{\alpha_n} = p_1^{\beta_1-\alpha_1}...p_n^{\beta_n}$. Alors, $p_1|p_2^{\alpha_2}...p_n^{\alpha_n}$, ce qui est impossible puisque les p_i sont distincts. Dans le cas où $\alpha_i > \beta_i$, $p_1^{\alpha_1-\beta_1}...p_n^{\alpha_n} = p_2^{\beta_2}...p_n^{\beta_n}$. Alors, $p_1|p_2^{\beta_2}...p_n^{\beta_n}$, ce qui est impossible puisque les p_i sont distincts. Ainsi, $\{\alpha_i\} = \{\beta_i\}$. □

- *Théorème de Bézout* : Pour $a, b \in \mathbb{Z}^*$ et $x, y \in \mathbb{Z}$, $\text{pgcd}(a, b) = ax + by$.

Soit G l'ensemble contenant les entiers positifs (≥ 1) qui s'écrivent sous la forme $ax + by$ où $a, b \in \mathbb{Z}^*$ sont des entiers posés à l'avance et $x, y \in \mathbb{Z}$ des entiers quelconques. Tout d'abord, G n'est pas vide.

Effectivement, si a est positif, alors $a \cdot 1 + b \cdot 0 \in G$. Alors, G est un sous-ensemble de $\mathbb{N}^*$ et, naturellement, G possède un plus petit élément d tel que $d \leq g \ \forall g \in G$. Puisque $d \in G$, on sait que $d = ax + by$.

Soient q, r le quotient et le reste de la division $\frac{a}{d}$. Alors, $a = dq + r$ où $0 \leq r < d$. En isolant r, on trouve que $r = a - dq = a - (ax + by)q = a(1 - xq) + b(yq)$. En supposant r non nul ($0 < r < d$), cela implique que $r \in G$. Cependant, il y a une contradiction du fait que $r < d$ et que d est sensé être le plus petit élément de G. Donc, $r = 0$ et $d|a$. On suit le même principe depuis $\frac{b}{d}$ pour dire que $d|b$. Alors, on peut dire que $d \leq \text{pgcd}(a, b)$. De plus, on sait que $\text{pgcd}(a, b)|ax + by = d \implies \text{pgcd}(a, b) \leq d$. Au final, on en conclue forcément que $\text{pgcd}(a, b) = d = ax + by$. □

- *C.5* : Si $a|c$, $b|c$ et $\text{pgcd}(a, b) = 1$, alors $ab|c$.

On sait que $c = ak$ et que $c = bk'$. De plus, par le théorème de Bézout, $ax + by = 1$. Donc, $cax + cby = c \implies abk'x + abky = c \implies ab(k'x + ky) = c$. On voit que ab est un facteur de c, ce qui veut dire que $ab|c$. □

- *C.6* : Si $c|a$ et $c|b$, alors $c|\text{pgcd}(a, b)$.

Puisque $c|a$ et $c|b$, alors $c|ax + by$. Donc, du fait que $\text{pgcd}(a, b) = ax + by$ par Bézout, $c|\text{pgcd}(a, b)$. □

Arithmétique modulaire

La section 1 du document principal sur Shor explique certains concepts de l'arithmétique modulaire qu'on ne répètera pas ici. Dorénavant, on n'écrira pas « mod n » avec les relations d'équivalence afin d'alléger la notation. Donc, $a \equiv b \bmod n \iff a \equiv b$ pour un certain entier n positif fixe mais qui n'est pas spécifié.

- *C.7* : $a \equiv b$ ssi $n|(a - b)$.

$(\implies) : a \equiv b \implies a = kn + b \implies kn = a - b \implies n|(a - b)$. □

$(\impliedby) : n|(a - b) \implies a - b = kn \implies a = kn + b \implies a \equiv b$. □

- *C.8* : $a \equiv b \implies b \equiv a$.

$a \equiv b \implies a = kn + b \implies b = -kn + a = k'n + a \implies b \equiv a$. □

- *C.9* : $a \equiv b$ et $b \equiv c \implies a \equiv c$.

$a \equiv b \implies a = kn + b$, $b \equiv c \implies b = k'n + c$. Donc, $a = kn + k'n + c = (k + k')n + c \implies a \equiv c$. □

- *C.10* : $a \equiv b$ et $c \equiv d \implies a + c \equiv b + d$.

$a \equiv b \implies a = kn + b$, $c \equiv d \implies c = k'n + d$. Alors, $a + c = (kn + b) + (k'n + d) = (k + k')n + (b + d) \implies a + c \equiv b + d$. □

- *C.11* : $a \equiv b$ et $c \equiv d \implies ac \equiv bd$.

$ac = (kn + b)(k'n + d) = (kk'n + kd + k'b)n + bd \implies ac \equiv bd$. □

On se demande maintenant comment trouver l'inverse multiplicatif modulo n d'un entier a. Il s'agit d'une notion plus subtile en arithmétique modulaire, car on cherche une valeur a^{-1} qui respecte $aa^{-1} \equiv 1$. De plus, on ne peut pas dire que $a^{-1} = \frac{1}{a}$, car on travaille avec des entiers.

- *C.12* : Pour $n > 1$, un entier a possède un inverse multiplicatif modulo n ssi $\text{pgcd}(a, n) = 1$ (a et n sont copremiers).

($\Longrightarrow$) : Si a possède un inverse multiplicatif modulo n, alors $aa^{-1} \equiv 1$, c'est-à-dire que $aa^{-1} = kn + 1$. Donc, $aa^{-1} - kn = 1$, ce qui veut dire par le théorème de Bézout que $\text{pgcd}(a, n) = 1$. □

($\Longleftarrow$) : Si $\text{pgcd}(a, n) = 1$, alors $ax+ny = 1$ par le théorème de Bézout. Donc, $(ax+ny) \bmod n = 1 \bmod n$, ce qui implique que $ax \equiv 1$. On prend alors x comme inverse multiplicatif modulo n pour a. □

On voit par la précédente démonstration que ce ne sont pas tous les entiers a qui ont un inverse multiplicatif modulo n, mais seulement les entiers qui sont copremiers avec n. Par conséquent, si n est un nombre premier, il va de soi que tous les entiers dans $\{1, ..., n-1\}$ ont un inverse multiplicatif modulo n du fait qu'ils sont forcément tous copremiers avec n.

- *C.13* : Si b et b' sont des inverses multiplicatifs modulo n d'un même entier a, alors $b \equiv b'$.

$b \equiv 1 \cdot b \implies b \equiv ab'b \implies b \equiv (ab)b' \implies b \equiv 1 \cdot b' \implies b \equiv b'$. □

- *C.14* : Soit $a, b \in \mathbb{Z}$ et r le reste de la division entière $\frac{a}{b}$. Si $r \neq 0$, alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

On peut dire que $r = a - kb$ pour un certain k. Donc, puisque $\text{pgcd}(a, b)$ divise forcément a et b, il divise aussi r qui est une combinaison linéaire de a et b. Puis, comme $\text{pgcd}(a, b)|b$ et $\text{pgcd}(a, b)|r$, on sait par C.6 que $\text{pgcd}(a, b)|\text{pgcd}(b, r)$. De plus, $\text{pgcd}(b, r)$ divise forcément b et r. Comme $a = kb + r$, $\text{pgcd}(b, r)$ divise a. Donc, $\text{pgcd}(b, r)$ divise b et a, ce qui veut dire qu'il divise aussi $\text{pgcd}(a, b)$. Au final, $\text{pgcd}(a, b)|\text{pgcd}(b, r)$ et $\text{pgcd}(b, r)|\text{pgcd}(a, b)$, ce qui signifie que $\text{pgdc}(a, b) = \text{pgcd}(b, r)$. □

Depuis cette dernière preuve, on peut concevoir un algorithme (l'algorithme d'Euclide) qui permet de calculer le pgcd entre deux entiers positifs a et b. On commence par ordonner a et b de telle sorte que $a > b$. Puis, on divise a par b, ce qui donne $a = k_1 b + r_1$. Par la précédente preuve, on sait que $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$. Puis, on divise b par r_1, donnant $b = k_2 r_1 + r_2$. Alors, $\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$. On continue le processus jusqu'à un reste de 0, c'est-à-dire quand $r_{m-1} = k_{m+1} r_m$ avec $r_{m+1} = 0$. Alors, $\text{pgcd}(a, b) = ... = \text{pgcd}(r_{m-1}, r_m) = r_m$. Par exemple, l'algorithme d'Euclide permet d'affirmer que $\text{pgcd}(6825, 1430) = 65$.

$$6825 = 4 \cdot 1430 + 1105$$
$$1430 = 1 \cdot 1105 + 325$$
$$1105 = 3 \cdot 325 + 130$$
$$325 = 2 \cdot 130 + 65$$
$$130 = 2 \cdot 65 + 0$$

On peut adapter l'algorithme d'Euclide pour trouver les coefficients x, y du théorème de Bézout. Pour y arriver, on exécute l'algorithme d'Euclide normalement. Puis, depuis l'avant-dernière ligne, on fait des substitutions avec les lignes précédentes. En employant le même exemple que tantôt, on trouve que $x = -9$ et $y = 43$.

$$65 = 325 - 2 \cdot 130 = 325 - 2 \cdot (1105 - 3 \cdot 325) = ... = -9 \cdot 6825 + 43 \cdot 1430$$

De surcroît, en calculant $\text{pgcd}(a, n)$ où a et n sont copremiers grâce l'algorithme d'Euclide puis en trouvant les coefficients du théorème de Bézout comme on vient de le voir, on peut trouver l'inverse multiplicatif modulo n de

a (le coefficient pour a sera son inverse). On peut montrer que l'algorithme d'Euclide, la recherche des coefficients x, y et la recherche de l'inverse multiplicatif modulo n ont une complexité polynomiale [4].

- *Théorème des restes chinois* : Soient $m_1, ..., m_n$ des entiers positifs tous copremiers entre eux, c'est-à-dire que $\text{pgcd}(m_i, m_j) = 1 \ \ \forall i \neq j$. Alors, le système d'équations $x \equiv a_1 \bmod m_1, ..., x \equiv a_n \bmod m_n$ a une solution. De plus, deux solutions pour le système d'équations sont équivalentes modulo $M = m_1...m_n$.

Existence d'une solution :

Soit $M_i = \frac{M}{m_i}$. Alors, $\text{pgcd}(M_i, m_i) = 1$ du fait que $\text{pgcd}(m_i, m_j) = 1 \ \ \forall i \neq j$. Ainsi, M_i a un inverse modulo m_i qu'on note N_i. Soit $x = \sum_i a_i M_i N_i$. On sait que $M_i N_i \equiv 1 \bmod m_i$, car on multiplie un nombre et son inverse modulo m_i. De plus, $M_i N_i \equiv 0 \bmod m_j \ \forall i \neq j$, car m_j est un facteur de M_i et, par conséquent, de $M_i N_i$ aussi. Au final, on en conclue que $x \equiv a_i \bmod m_i \ \forall i$, ce qui correspond à une solution pour le système d'équations qu'on cherchait à résoudre. □

Solutions équivalentes :

Si x et $x^{'}$ sont deux solutions, alors $x - x^{'} \equiv 0 \bmod m_i \ \forall i$. Donc, $m_i | x - x^{'} \ \forall i$ et par C.5 $M | x - x^{'} \implies kM = x - x^{'} \implies x = kM + x^{'} \implies x \equiv x^{'} \bmod M$. □

Par exemple, on essaie de résoudre le système suivant :

$$\begin{cases} x \equiv 4 \bmod 13 \\ x \equiv 2 \bmod 10 \end{cases}$$

On sait qu'une solution est $x = 4 \cdot 10 \cdot p + 2 \cdot 13 \cdot q = 40p + 26q$. De plus, on sait que $x \bmod 13 = (40p + 26q) \bmod 13 = 4$ et que $x \bmod 10 = (40p + 26q) \bmod 10 = 2$. En développant les égalités, on trouve que $p = 4$ et $q = 2$ conviennent. Donc, $x = 40 \cdot 4 + 26 \cdot 2 = 212$. On peut vérifier que 212 satisfait bien le système d'équations et que, par équivalence, $x^{'} = 212 \bmod 13 \cdot 10 = 82$ convient aussi.

- *C.15* : Si p est un nombre premier et que k est un entier dans $\{1, ..., p-1\}$, alors p divise $\binom{p}{k}$.

$\binom{p}{k} = \frac{p!}{k!(p-k)!} \implies \binom{p}{k} k! = \frac{p!}{(p-k)!} = p(p-1)...(p-k+1) \implies p | p(p-1)...(p-k+1) \implies p | \binom{p}{k} k!$.
Comme $k \leq p - 1$, p ne peut pas diviser $k!$ donc il divise $\binom{p}{k}$. □

Petit théorème de Fermat : Si p est un nombre premier et a un entier, alors $a^p \equiv a \bmod p$. De plus, si a ne divise pas p, alors $a^{p-1} \equiv 1 \bmod p$.

Pour les $a \geq 0$:

Si $a = 0$, alors $0^p = 0 \equiv 0 \bmod p$. Quand $a = 1$, $a^p = 1^p \equiv 1 \bmod p$. On suppose que c'est vrai jusqu'à une certaine valeur arbitraire de a et on regarde si c'est aussi vrai pour $a + 1$. Par la formule du binôme, $(1 + a)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$. En utilisant la précédente preuve, tous les termes de la somme sauf le premier et le dernier sont divisibles par p. Donc, $(1 + a)^p \equiv (\binom{p}{0} a^0 + \binom{p}{p} a^p) \bmod p \equiv (1 + a^p) \bmod p$. Par hypothèse, $a^p \equiv a \bmod p$. Alors, $(1 + a^p) \bmod p \equiv (1 + a) \bmod p$. □

Si a ne divise pas p, alors $\text{pgcd}(a, p) = 1 \implies \exists a^{-1}$. Alors, $a^{p-1} = a^p a^{-1} \equiv a a^{-1} \bmod p \equiv 1 \bmod p$. Cela fonctionne peu importe la valeur de a et n'est pas spécifique aux a positifs. □

Pour les $a < 0$:

On sait que $(-a)^p = (-1)^p \cdot a^p$. Dans le cas où p est un nombre premier pair ($p = 2$), alors $(-a)^p = a^p \equiv a \bmod p$ par la démonstration sur les a positifs. Sinon, dans le cas où p est un nombre premier impair, $(-a)^p = -1 \cdot a^p$. Donc, $-1 \cdot a^p \bmod p = (-1 \bmod p)(a^p \bmod p) \bmod p = (p-1)a \bmod p \equiv -a \bmod p$. □

Les ensembles $\mathbb{Z}_n$ et $\mathbb{U}_n$

On définit $\mathbb{Z}_n$ comme l'ensemble des valeurs possibles/des équivalences modulo n, c'est-à-dire l'ensemble des valeurs entre 0 et $n-1$ [3]. Pour tout entier $x \in \mathbb{Z}$, on lui applique la transformation $x \bmod n$ pour connaître son équivalence dans $\mathbb{Z}_n$. Aussi, on définit $\mathbb{U}_n \subseteq \mathbb{Z}_n$ comme l'ensemble des éléments de $\mathbb{Z}_n$ qui ont un inverse multiplicatif modulo n, c'est-à-dire qui sont copremiers avec n. Il va de soi que $|\mathbb{Z}_n| = n$.

- *C.16* : Pour $n = ab$ où a et b sont copremiers, $\mathbb{U}_n \cong \mathbb{U}_a \times \mathbb{U}_b$. Cela s'étend facilement à un plus grand nombre de produits.

On ne le montrera pas ici, mais il est assez évident que $\mathbb{U}_n$ forme un groupe pour tout n sous la multiplication modulo n.

Soit $x \in \mathbb{U}_n$. On sait que $\text{pgcd}(x, n) = \text{pgcd}(x, ab) = 1 \implies \text{pgcd}(x, a) = \text{pgcd}(x, b) = 1$. On cherche maintenant à construire $\psi : \mathbb{U}_n \to \mathbb{U}_a \times \mathbb{U}_b$. Soit $y = x \bmod a \implies x = ka + y$ pour un certain entier k. Par Bézout, $\text{pgcd}(x, a) = 1 \implies xq + ar = 1 \implies (ka + y)q + ar = yq + a(kq + r) = 1 \implies \text{pgcd}(y, a) = \text{pgcd}(x \bmod a, a) = 1$. Par le même raisonnement, $\text{pgcd}(x \bmod b, b) = 1$. Donc, $x \bmod a \in \mathbb{U}_a$ et $x \bmod b \in \mathbb{U}_b \implies (x \bmod a, x \bmod b) \in \mathbb{U}_a \times \mathbb{U}_b$.

Ensuite, on suppose que $x_1, x_2 \in \mathbb{U}_n$ soient associés à la même paire dans $\mathbb{U}_a \times \mathbb{U}_b$. Alors, $x_1 \bmod a = x_2 \bmod a \implies x_1 \equiv x_2 \bmod a$. De plus, $x_1 \bmod b = x_2 \bmod b \implies x_1 \equiv x_2 \bmod b$. On en conclue que a et b divisent $x_1 - x_2$ et on se rappelle que $\text{pgcd}(a, b) = 1$. Par C.5, $ab | x_1 - x_2 \implies n | x_1 - x_2 \implies ln = x_1 - x_2 \implies x_1 = ln + x_2 \implies x_1 \equiv x_2 \bmod n$. Cependant, comme $x_1, x_2 \in \mathbb{U}_n \implies 0 \leq x_1, x_2 < n$, alors $x_1 \equiv x_2 \bmod n \implies x_1 = x_2$. Au final, $\psi : \mathbb{U}_n \to \mathbb{U}_a \times \mathbb{U}_b$ correspond à $x \to (x \bmod a, x \bmod b)$.

Aussi, on veut $\psi^{-1} : \mathbb{U}_a \times \mathbb{U}_b \to \mathbb{U}_n$. Soient $g \in \mathbb{U}_a$ et $h \in \mathbb{U}_b$. On cherche $(g, h) \to x$ pour $x \in \mathbb{U}_n$ quelconque. Donc, il suit que $x \equiv g \bmod a$ et $x \equiv h \bmod b$ dont on sait par le théorème des restes chinois que x existe. De plus, en appliquant le modulo n sur la solution x qu'on aura trouvée, on s'assure que $0 \leq x < n$ et donc la solution trouvée sera dans $\mathbb{U}_n$.

Puis, si (g_1, h_1) et (g_2, h_2) pointent vers la même valeur $x \in \mathbb{U}_n$, cela veut dire que $x \equiv g_1 \bmod a$, $x \equiv g_2 \bmod a$, $x \equiv h_1 \bmod b$ et $x \equiv h_2 \bmod b$. Ainsi, $g_1 \equiv g_2 \bmod a$ et $h_1 \equiv h_2 \bmod b$. Par contre, $0 \leq g_1, g_2 < a$ et $0 \leq h_1, h_2 < b \implies g_1 = g_2$ et $h_1 = h_2$.

Pour conclure, on voit qu'il y a une une bijection entre $\mathbb{U}_n$ et $\mathbb{U}_a \times \mathbb{U}_b \implies \mathbb{U}_n \cong \mathbb{U}_a \times \mathbb{U}_b$. Par ailleurs, cela nous indique que $|\mathbb{U}_n| = |\mathbb{U}_a| \cdot |\mathbb{U}_b|$. □

Fonction ϕ d'Euler

La fonction $\phi(n)$ d'Euler permet de connaître le nombre d'entiers positifs plus petits ou égaux à n qui sont copremiers avec n [5]. En d'autres mots, $\phi(n) = |\mathbb{U}_n| \ \forall n$. Par exemple, pour un nombre premier p, $\phi(p) = p - 1$, car tous les entiers positifs plus petits que p sont copremiers avec lui. De plus, les seuls entiers positifs plus petits ou égaux à p^α qui ne sont pas copremiers avec lui sont les multiples $\{p, 2p, 3p, ..., (p^{\alpha-1} - 1)p, p^{\alpha-1}p\}$. Alors,

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

où p^α est le nombre d'entiers positifs plus petits ou égaux à p^α et $p^{\alpha-1}$ est le nombre d'entiers positifs plus petits ou égaux à p^α qui ne sont pas copremiers avec lui.

- *C.17* : Si a et b sont copremiers, alors $\phi(ab) = \phi(a)\phi(b)$.

On utilise C.16 pour en arriver à $\phi(ab) = |\mathbb{U}_{ab}| = |\mathbb{U}_a| \cdot |\mathbb{U}_b| = \phi(a)\phi(b)$. □

- *C.18* : $\phi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1)\ \forall n \geq 2$.

On démarre depuis la factorisation en nombres premiers de n (qui existe si $n \geq 2$), soit $n = p_1^{\alpha_1}...p_k^{\alpha_k}$. Alors, $\phi(n) = \phi(p_1^{\alpha_1}...p_k^{\alpha_k})$. On remarque que $p_1^{\alpha_1}$ n'a pas de facteurs en commun avec $p_2^{\alpha_2}...p_k^{\alpha_k}$, ce qui amène à conclure que $\text{pgcd}(p_1^{\alpha_1}, p_2^{\alpha_2}...p_k^{\alpha_k}) = 1$. Donc, il est possible d'affirmer que $\phi(p_1^{\alpha_1}...p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}...p_k^{\alpha_k})$. On peut répéter le processus pour les autres $p_j^{\alpha_j}$ afin d'en arriver à

$$\phi(n) = \prod_{j=1}^{k} \phi(p_j^{\alpha_j}) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1)\ \square$$

- *C.19* : $n = \sum_{d|n} \phi(d)$ où la somme se fait sur tous les diviseurs d de n (1 et n inclus).

Pour $n = 1$, $\sum_{d|1} \phi(d) = \phi(1) = 1 = n$. Autrement, pour $n \geq 2$, on commence par montrer que $p^\alpha = \sum_{d|p^\alpha} \phi(d)$.

$$\sum_{d|p^\alpha} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + ... + \phi(p^\alpha) = 1 + \sum_{j=1}^{\alpha} \phi(p^j) = 1 + \sum_{j=1}^{\alpha} p^j - p^{j-1} = 1 + p^\alpha - p^0 = p^\alpha$$

Ensuite, on utilise la factorisation en nombres premiers de n pour dire que

$$n = p_1^{\alpha_1}...p_k^{\alpha_k} = \left(\sum_{d_1|p_1^{\alpha_1}} \phi(d_1)\right) ... \left(\sum_{d_k|p_k^{\alpha_k}} \phi(d_k)\right) = \sum_{d|n} \phi(d).\ \square$$

On peut généraliser le petit théorème de Fermat grâce à la fonction ϕ d'Euler.

- *Théorème d'Euler* : Si un entier a est copremier avec un entier $n > 0$, alors $a^{\phi(n)} \equiv 1 \bmod n$.

On montre d'abord que $a^{\phi(p^\alpha)} \equiv 1 \bmod p^\alpha$. Si $\alpha = 1$, alors il s'agit du théorème de Fermat et la relation tient. On suppose que c'est vrai jusqu'à un certain $\alpha \geq 1$ et on regarde si c'est aussi vrai pour $\alpha + 1$.

$$a^{\phi(p^{\alpha+1})} = a^{p^\alpha(p-1)} = a^{p\phi(p^\alpha)} = \left(a^{\phi(p^\alpha)}\right)^p = (kp^\alpha + 1)^p = \sum_{j=0}^{p} \binom{p}{j} k^j p^{\alpha j} = 1 + \sum_{j=1}^{p} \frac{(p-1)!}{j!(p-j)!} k^j p^{\alpha j + 1}$$

$$= 1 + \sum_{j=1}^{p} \frac{(p-1)!}{j!(p-j)!} k^j p^{\alpha(j-1)} p^{\alpha+1}$$

Alors, on voit que $p^{\alpha+1}$ divise tous les termes de la somme. Forcément, $a^{\phi(p^{\alpha+1})} \equiv 1 \bmod p^{\alpha+1}$. De plus, avoir un multiple de $\phi(p^\alpha)$ en exposant revient à la même conclusion. Donc, $a^{\phi(n)} = a^{\phi(p_1^{\alpha_1}...p_k^{\alpha_k})} = a^{\phi(p_1^{\alpha_1})...\phi(p_k^{\alpha_k})}$ et cela indique que $\phi(n)$ est un multiple de tous les $\phi(p_j^{\alpha_j})$. De ce fait, $a^{\phi(n)} \equiv 1 \bmod p_j^{\alpha_j}$ $\forall j$. Par la partie sur les solutions équivalentes du théorème des restes chinois, on sait que $a^{\phi(n)} \equiv 1 \bmod p_1^{\alpha_1}...p_k^{\alpha_k} \implies a^{\phi(n)} \equiv 1 \bmod n$. □

La fonction ϕ d'Euler est aussi très pertinente pour montrer que $\mathbb{U}_{p^\alpha}$ est un groupe cyclique [3].

- *C.20* : Pour $n = p$ un nombre premier impair, $\mathbb{U}_p$ forme un groupe cyclique sous la multiplication modulo n.

On sait que $|\mathbb{U}_p| = \phi(p) = p-1$. Pour montrer que le groupe est cyclique, on cherche au moins un élément dans $\mathbb{U}_p$ d'ordre $p-1$. On sait que les seuls ordres possibles sont les diviseurs positifs d de $p-1$. Pour chaque d, on construit $A_d = \{a \in \mathbb{U}_p \mid \text{l'orde de } a \text{ vaut } d\}$. Donc, l'union des A_d correspond à $\mathbb{U}_p$, ce qui indique que $|\mathbb{U}_p| = \sum_{d|p-1} |A_d|$. Aussi, par C.19, $|\mathbb{U}_p| = \sum_{d|p-1} \phi(d) \implies \sum_{d|p-1} (\phi(d) - |A_d|) = 0$.

On compare maintenant $\phi(d)$ et $|A_d|$ pour tous les diviseurs d. Rien n'empêche que $|A_d| = 0 \implies |A_d| \leq \phi(d)$. Sinon, $|A_d| > 0$ et on choisit un de ses éléments g pour construire $< g >= \{1, g, g^2, ..., g^{d-1}\}$. Par B.8, on sait qu'il y a $\phi(d)$ éléments dans $< g >$ d'ordre d. Comme $\sum_{d|p-1} \phi(d) = p-1$, il faut forcément que $|A_d| = \phi(d)\ \forall d \implies |A_d| \leq \phi(d)\ \forall d$. Donc dans tous les cas, $|A_d| \leq \phi(d)\ \forall d$.

On combine $\sum_{d|p-1} (\phi(d) - |A_d|) = 0$ et $|A_d| \leq \phi(d)\ \forall d$ pour dire que $|A_d| = \phi(d)\ \forall d$. $p-1$ étant un des diviseurs, $|A_{p-1}| = \phi(p-1) \neq 0 \implies \exists$ au moins un élément de $\mathbb{U}_p$ ayant un ordre $p-1 \implies \mathbb{U}_p$ est cyclique. □

- *C.21* : Pour $n = p$ un nombre premier impair, $\mathbb{U}_{p^2}$ est cyclique.

Soit $a \in \mathbb{U}_p$ où $\mathbb{U}_p = < a >$. Cet élément fait aussi partie de $\mathbb{U}_{p^2}$ et possède dans ce groupe un certain ordre k. Donc, $|\mathbb{U}_{p^2}| = \phi(p^2) = p(p-1) \implies k|p(p-1)$. Aussi, on sait que $a^k \equiv 1 \bmod p^2$ puisque k correspond à l'ordre de a. Alors, $a^k = lp^2 + 1 = (lp)p + 1 = l^{'}p + 1 \implies a^k \equiv 1 \bmod p \implies a^k = 1 \in \mathbb{U}_p \implies p-1|k$.

Ainsi, $k|p(p-1) \implies p(p-1) = xk$ et $p-1|k \implies k = y(p-1)$. En combinant ces équations, on a $p(p-1) = xy(p-1) \implies p = xy$. Puisque p est un nombre premier impair, soit $x = 1$ et $y = p$ ou $x = p$ et $y = 1$. De ce fait, k vaut soit $p-1$ ou $p(p-1)$. Dans le premier cas, a ne peut pas être un générateur pour $\mathbb{U}_{p^2}$, car l'ordre ne correspond pas à $|\mathbb{U}_{p^2}| = p(p-1)$. Dans le second cas, $\mathbb{U}_{p^2} = < a >$.

On doit trouver un autre générateur dans le cas où $\mathbb{U}_{p^2} \neq < a >$, c'est-à-dire lorsque l'ordre de a est $p-1$ autant dans $\mathbb{U}_p$ que dans $\mathbb{U}_{p^2}$. Soit $a + p \in \mathbb{U}_{p^2}$ d'ordre m. Comme $a + p \equiv a \bmod p$, $\mathbb{U}_p = < a >$ $= < a + p >$ et par les précédentes démarches, on sait que $m = p-1$ ou $m = p(p-1)$. En d'autres mots, $(a+p)^{p-1} \equiv 1 \bmod p^2$ ou $(a+p)^{p(p-1)} \equiv 1 \bmod p^2$.

$$(a+p)^{p-1} = \sum_{j=0}^{p-1} \frac{(p-1)!}{j!(p-1-j)!} a^j p^{p-1-j} = \sum_{j=0}^{p-1} \frac{(p-1)!}{j!(p-1-j)!} a^j p^2 p^{p-3-j}$$

$$= a^{p-1} + (p-1)pa^{p-2} + \sum_{j=0}^{p-3} \frac{(p-1)!}{j!(p-1-j)!} a^j p^2 p^{p-3-j} \implies (a+p)^{p-1} \equiv a^{p-1} - a^{p-2}p \bmod p^2$$

$$\equiv 1 - a^{p-2}p \bmod p^2 \not\equiv 1 \bmod p^2$$

du fait que p ne divise pas a. Alors, $p(p-1)$ doit être la valeur de l'ordre $\implies \mathbb{U}_{p^2} = < a+p >$. Au final, on choisit $< a >$ ou $< a+p >$ comme générateur selon la valeur de l'ordre de a dans $\mathbb{U}_{p^2}$. Dans tous les cas, $\mathbb{U}_{p^2}$ est cyclique. □

- *C.22* : Pour $n = p$ un nombre premier impair et $\alpha \geq 1$, $\mathbb{U}_{p^\alpha}$ est cyclique.

Soit $\mathbb{U}_{p^2} = < b >$ où forcément p ne divise pas b. On suppose que $\mathbb{U}_{p^\alpha} = < b >$ pour un certain entier $\alpha \geq 2$ et on montre que $\mathbb{U}_{p^{\alpha+1}} = < b >$.

On sait que $|\mathbb{U}_{p^{\alpha+1}}| = \phi(p^{\alpha+1}) = p^\alpha(p-1)$ et $|\mathbb{U}_{p^\alpha}| = \phi(p^\alpha) = p^{\alpha-1}(p-1)$. De plus, $b \in \mathbb{U}_{p^{\alpha+1}}$ avec un certain ordre m dans ce groupe. Alors, $m|p^\alpha(p-1) \implies b^m \equiv 1 \bmod p^{\alpha+1} \implies b^m \equiv 1 \bmod p^\alpha \implies b^m = 1 \in \mathbb{U}_{p^\alpha} \implies p^{\alpha-1}(p-1)|m$. De manière équivalente à la démonstration C.21, on trouve $m = p^{\alpha-1}(p-1)$ ou $m = p^\alpha(p-1)$.

Par hypothèse, $\mathbb{U}_{p^{\alpha-1}} = < b > \implies b^{\phi(p^{\alpha-1})} = b^{p^{\alpha-2}(p-1)} = 1 \in \mathbb{U}_{p^{\alpha-1}} \implies b^{p^{\alpha-2}(p-1)} \equiv 1 \bmod p^{\alpha-1} \implies b^{p^{\alpha-2}(p-1)} = tp^{\alpha-1}+1$ où $t \geq 1$. Par ailleurs, $\mathbb{U}_{p^\alpha} = < b > \implies b^{p^{\alpha-2}(p-1)} \not\equiv 1 \bmod p^\alpha \implies b^{p^{\alpha-2}(p-1)} = tp^{\alpha-1}+1$ où $t \geq 1$ et p ne divise pas t. On teste maintenant les valeurs possibles pour l'ordre m.

$$b^{p^{\alpha-1}(p-1)} = \left(b^{p^{\alpha-2}(p-1)}\right)^p = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} t^k p^{k(\alpha-1)} = 1 + tp^\alpha + \sum_{k=2}^{p} \frac{p!}{k!(p-k)!} t^k p^{\alpha+1} p^{\alpha(k-1)-k-1}$$

$$\implies b^{p^{\alpha-1}(p-1)} = \left(b^{p^{\alpha-2}(p-1)}\right)^p = \left(1+tp^{\alpha-1}\right)^p \equiv 1 + tp^\alpha \bmod p^{\alpha+1} \not\equiv 1 \bmod p^{\alpha+1}$$

parce que p ne divise pas t. Ainsi, $m = p^\alpha(p-1) \implies \mathbb{U}_{p^{\alpha+1}} = < b >$. Donc, $\mathbb{U}_{p^\alpha}$ est cyclique pour $\alpha \geq 2$. Par C.20, $\mathbb{U}_p = \mathbb{U}_{p^1}$ est aussi cyclique. Au final, $\mathbb{U}_{p^\alpha}$ est cyclique pour tout $\alpha \geq 1$. □

D Fractions continues

Soit a un nombre rationnel, c'est-à-dire un nombre qui s'écrit sous la forme d'une fraction $\frac{p}{q}$ où p et q sont des entiers. Les fractions continues permettent, depuis la valeur décimale de a, de retrouver p et q pour connaître la forme fractionnaire de a [5].

On illustre les fractions continues avec un exemple. Prenons $a = 0.352$. Tout d'abord, on sépare la partie entière de la partie fractionnaire : $0.352 = 0 + 0.352$. On assigne la partie entière à une variable a_0. Donc, $a_0 = 0$. Puis, on manipule la partie fractionnaire et on garde encore sa partie entière qu'on assigne à a_1. Alors, $0.352 = 0 + \frac{1}{\frac{1}{0.352}} = 0 + \frac{1}{2.8409...} = 0 + \frac{1}{2+0.8409...} \implies a_1 = 2$. On continue ainsi de suite et, éventuellement, il y aura au dénominateur un entier qui n'a pas de partie fractionnaire, ce qui finira le processus. Au final, on se retrouve avec une liste $[a_0, ..., a_n]$ qu'on nomme la représentation en fractions continues de a. Pour en revenir à $a = 0.352$, on aurait [0,2,1,5,3,2].

$$a = [a_0, ..., a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + ...}}$$

Cependant, qu'est-ce qui nous garantit qu'il y a une telle représentation finie pour tout nombre rationnel ? On montre ci-dessous pourquoi c'est le cas lorsque a est positif (bien que cela soit aussi vrai si a est négatif).

- *D.1* : Si a est un nombre rationnel positif, alors a possède une représentation finie en fractions continues, c'est-à-dire que $a = [a_0, ..., a_n]$ est une liste finie.

En fait, les fractions continues peuvent être reliées à l'algorithme d'Euclide. Pour comprendre, on utilise un exemple où $a = \frac{43}{19} = 2.263...$. Sa représentation en fractions continues est $[2, 3, 1, 4]$ et le calcul du pgcd entre 43 et 19 donne

$$43 = 2 \cdot 19 + 5,\ 19 = 3 \cdot 5 + 4,\ 5 = 1 \cdot 4 + 1,\ 4 = 4 \cdot 1 + 0$$

De là, on remarque que les nombres en rouge (la partie entière de $\frac{43}{19}$, $\frac{19}{5}$, ...) correspondent aux a_i de la représentation en fractions continues. Cela a du sens, car on garde la partie entière de chaque division dans les fractions continues et que justement les nombres en rouge dans l'algorithme d'Euclide y correspondent.

$$\frac{43}{19} = 2 + \frac{1}{\frac{19}{5}} = 2 + \frac{1}{3 + \frac{1}{\frac{5}{4}}} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}$$

L'algorithme d'Euclide contient un nombre fini de divisions et, comme on tire les a_i de ces divisions, la liste $[a_0, ..., a_n]$ doit aussi être finie. Par le fait même, cela montre qu'une telle représentation existe forcément pour tout nombre rationnel positif. En fait, dans le cas où $0 < a < 1$, on peut obtenir sa représentation en fractions continues en effectuant l'algorithme d'Euclide sur $\frac{1}{a}$, puis de là en extraire la liste $[a_0, ..., a_n]$ pour finalement rajouter 0 au début de la liste. □

Les termes $\{a_0,\ a_0 + \frac{1}{a_1},\ a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, ...\}$ correspondant respectivement à $\{[a_0], [a_0, a_1], [a_0, a_1, a_2], ...\}$ sont des « convergents » de la représentation en fractions continues de a du fait qu'ils convergent progressivement vers sa réelle valeur. Effectivement, chaque convergent, lorsqu'on le calcule, nous donne une certaine fraction $\frac{p_i}{q_i}$ qui se rapproche de la véritable fraction $a = \frac{p_n}{q_n}$. Particulièrement, le dernier convergent $[a_0, ..., a_n]$ correspond à $\frac{p_n}{q_n}$. Par exemple, on écrit ci-dessous les convergents pour $a = 0.352 = \frac{44}{125}$.

- $[0] = 0 = \frac{0}{1}$
- $[0, 2] = 0 + \frac{1}{2} = \frac{1}{2}$
- $[0, 2, 1] = 0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3}$
- $[0, 2, 1, 5] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{5}}} = \frac{6}{17}$
- $[0, 2, 1, 5, 3] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3}}}} = \frac{19}{54}$
- $[0, 2, 1, 5, 3, 2] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3 + \frac{1}{2}}}}} = \frac{44}{125}$

Un autre fait intéressant est qu'on peut choisir dans la représentation en fractions continues si on veut une liste de taille paire ou impaire. En effet, on peut faire un changement trivial pour le dernier dénominateur afin que la taille de la liste des a_i augmente de 1. Ainsi, on peut passer d'un nombre pair à impair de a_i et inversement. Par exemple,

$$0.352 = [0, 2, 1, 5, 3, 2] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3 + \frac{1}{2}}}}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3 + \frac{1}{1 + \frac{1}{1}}}}}} = [0, 2, 1, 5, 3, 1, 1]$$

- *D.2* : Si $[a_0, ..., a_n]$ est la représentation en fractions continues de a, alors $a = \frac{p_n}{q_n}$. Plus généralement, on a que $p_0 = a_0$, $q_0 = 1$, $p_1 = 1 + a_0 a_1$, $q_1 = a_1$ et, pour $2 \leq i \leq n$, que $p_n = a_n p_{n-1} + p_{n-2}$ avec $q_n = a_n q_{n-1} + q_{n-2}$.

D'abord,

$$[a_0] = a_0 = \frac{a_0}{1} \implies p_0 = a_0 \text{ et } q_0 = 1$$

Puis,

$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{1 + a_0 a_1}{a_1} \implies p_1 = 1 + a_0 a_1 \text{ et } q_1 = a_1$$

On regarde ensuite le cas de base pour la récursion.

$$[a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_0(a_1 a_2 + 1) + a_2}{a_1 a_2 + 1} = \frac{a_2(a_0 a_1 + 1) + a_0}{a_2 a_1 + 1}$$

Cela respecte la formule de récursion. On suppose maintenant que la relation de récursion fonctionne pour $2 \leq i \leq n-1$ et on regarde si elle est aussi respectée quand $i = n$. En premier lieu, on remarque que $[a_0, ..., a_n] = [a_0, ..., a_{n-2}, a_{n-1} + \frac{1}{a_n}]$ par définition. Ensuite, comme il y a $n-1$ éléments dans la liste, on sait par hypothèse que $[a_0, ..., a_{n-2}, a_{n-1} + \frac{1}{a_n}] = \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}$. Donc,

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{(a_{n-1} + \frac{1}{a_n})p_{n-2} + p_{n-3}}{(a_{n-1} + \frac{1}{a_n})q_{n-2} + q_{n-3}} = \frac{a_{n-1}p_{n-2} + p_{n-3} + \frac{p_{n-2}}{a_n}}{a_{n-1}q_{n-2} + q_{n-3} + \frac{q_{n-2}}{a_n}} = \frac{p_{n-1} + \frac{p_{n-2}}{a_n}}{q_{n-1} + \frac{q_{n-2}}{a_n}} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}$$

$$\implies [a_0, ..., a_n] = [a_0, ..., a_{n-2}, a_{n-1} + \frac{1}{a_n}] = \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{p_n}{q_n} \ \square$$

- *D.3* : $q_n p_{n-1} - p_n q_{n-1} = (-1)^n \ \forall n \geq 1$.

Si $n = 1$, on a $q_1 p_0 - p_1 q_0 = a_1 a_0 - (1 + a_0 a_1) = -1 = (-1)^1$. On suppose que c'est vrai jusqu'à n et on regarde si la relation fonctionne pour $n+1$. Par D.2, $p_{n+1} = a_{n+1}p_n + p_{n-1}$ et $q_{n+1} = a_{n+1}q_n + q_{n-1}$. Donc,

$$q_{n+1}p_n - p_{n+1}q_n = (a_{n+1}q_n p_n + q_{n-1}p_n) - (a_{n+1}p_n q_n + p_{n-1}q_n) = -1 \cdot (q_n p_{n-1} - p_n q_{n-1})$$

$$= -1 \cdot (-1)^n = (-1)^{n+1} \ \square$$

Pour l'algorithme de Shor, les fractions continues servent à trouver l'ordre r depuis $\frac{s}{r}$. Cependant, selon le degré de précision de la QPE, on peut se retrouver avec une estimation de $\frac{s}{r}$. Comme il ne s'agit pas de la valeur exact, est-ce que les fractions continues permettent tout de même de trouver r ? Oui, mais seulement si l'approximation est suffisamment proche de la valeur exacte.

- *D.4* : Soient x et $\frac{p}{q}$ deux nombres rationnels tels que $|\frac{p}{q} - x| \leq \frac{1}{2q^2}$. Alors, $\frac{p}{q}$ est un convergent des fractions continues pour x.

Soit $\frac{p}{q} = [a_0, ..., a_n]$ où $\frac{p_n}{q_n} = \frac{p}{q}$. On définit

$$x = \frac{p}{q} + \frac{\delta}{2q^2} = \frac{p_n}{q_n} + \frac{\delta}{2q^2}$$

où $|\delta| < 1$ ainsi que le nombre rationnel

$$\lambda = 2\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta}\right) - \frac{q_{n-1}}{q_n} = \frac{2(-1)^n}{\delta} - \frac{q_{n-1}}{q_n}$$

On remarque alors que

$$\frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}} = \frac{\frac{2p_n(-1)^n}{\delta} - \frac{p_n q_{n-1}}{q_n} + p_{n-1}}{\frac{2q_n(-1)^n}{\delta}} = \frac{2p_n(-1)^n + \delta\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{q_n}\right)}{2q_n(-1)^n} = \frac{2p_n(-1)^n + \frac{\delta(-1)^n}{q_n}}{2q_n(-1)^n}$$

$$= \frac{p_n}{q_n} + \frac{\delta}{2q_n^2} = x$$

Donc, $x = [a_0, ..., a_n, \lambda]$ et il s'en suit que $\frac{p_n}{q_n} = \frac{p}{q} = [a_0, ..., a_n]$ est un convergent de la représentation en fractions continues de x. □

Ainsi, pour en revenir à Shor, on peut trouver l'ordre en calculant les convergents de l'estimation de $\frac{s}{r}$ puis vérifier si le dénominateur respecte les critères de l'ordre ($a^r \bmod N = 1$). Le tout se calcule en temps polynomial [4].

E Explication du pseudocode

On montre ci-dessous le pseudocode pour l'algorithme de Shor afin, par la suite, d'expliquer chacune des étapes et les moments où l'algorithme peut échouer [4].

Algorithme de Shor

Entrée : Un nombre N composé et positif
Sortie : Un facteur non-trivial de N

1: **Si** N est pair **alors :**
2: **retourner** 2
3:
4: **Si** N est une puissance pure, c'est-à-dire si $N = x^y$ pour des entiers $x \geq 1$ et $y \geq 2$, **alors :**
5: **retourner** (x, y)
6:
7: Choisir aléatoirement a où $1 < a < N - 1$.
8: **Si** $\text{pgcd}(a, N) > 1$, **alors :**
9: **retourner** $\text{pgcd}(a, N)$
10:
11: Utiliser la recherche d'ordre pour trouver l'ordre r de $a^r \equiv 1$ modulo N.
12: **Si** r est pair et que $a^{\frac{r}{2}} \not\equiv -1 \bmod N$, **alors :**
13: Calculer $\text{pgcd}(a^{\frac{r}{2}} \pm 1, N)$.
14: **Si** $\text{pgcd}(a^{\frac{r}{2}} + 1, N)$ et/ou $\text{pgcd}(a^{\frac{r}{2}} - 1, N)$ sont des facteurs de N, **alors :**
15: **retourner** $\text{pgcd}(a^{\frac{r}{2}} + 1, N)$ et/ou $\text{pgcd}(a^{\frac{r}{2}} - 1, N)$
16:
17: Revenir à la ligne 7.

Lignes 1-2

Pour commencer, il n'est pas bête de se demander si N est pair. On peut facilement vérifier si c'est le cas classiquement (regarder la valeur du bit de poids faible) et de là en tirer 2 comme facteur. Si N continue d'être pair, on

va à force factoriser une certaine puissance de 2. Ainsi, peu importe si on trouve un facteur ou non grâce à cette étape, on s'assure en temps polynomial que N est impair pour le reste du pseudocode.

Lignes 4-5

Par la suite, il se peut que N soit une puissance pure, c'est-à-dire que $N = x^y$ avec des entiers $x \geq 1$ et $y \geq 2$. Il existe des algorithmes classiques capables de vérifier cela en temps polynomial. Ainsi, on s'assure que N est un nombre composé de différents nombres premiers impairs.

Lignes 7-9

La prochaine étape consiste à choisir un nombre a aléatoirement où $1 < a < N - 1$. Puis, on calcule le pgcd entre a et N en temps polynomial grâce à l'algorithme d'Euclide. On voit que le choix des bornes pour a est important, car sinon le calcul du pgcd peut donner un facteur trivial (1 ou N) qui n'amène aucune progression quant à la factorisation de N. Effectivement,

$$\text{pgcd}(1, N) = 1 \ \forall N, \ \text{pgcd}(N, N) = N \ \forall N \text{ et } \text{pgcd}(N - 1, N) = 1 \ \forall N$$

En prenant a entre 1 et $N - 1$, on se donne au moins une chance de trouver un facteur en calculant le pgcd. Ainsi, si $\text{pgcd}(a, N)$ est plus grand que 1, alors il est un facteur de N puisque $\text{pgcd}(a, N)$ divise N. Dans le cas où le pgcd vaut 1, on s'assure que a et N soient copremiers.

Lignes 11-17

Finalement, si les précédentes étapes n'ont permis de factoriser N, on utilise la recherche d'ordre quantique et les fractions continues pour résoudre $a^r \equiv 1 \bmod N$. Ainsi, dans le cas où on trouve la bonne valeur pour l'ordre, $a^r - 1 = kN$ pour un certain k. En supposant que r est pair, on peut aussi dire que $(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) = kN$ et que N divise l'un ou l'autre des termes entre paranthèses/les deux termes entre parenthèses. Donc, du fait que N est composé, il a un facteur en commun avec $(a^{\frac{r}{2}} + 1)$ et/ou $(a^{\frac{r}{2}} - 1)$ qu'on peut trouver en calculant leur pgcd.

Cependant, on veut éviter qu'il s'agisse d'un facteur trivial. On observe que

$$\text{pgcd}(a^{\frac{r}{2}} + 1, N) = \text{pgcd}\left((a^{\frac{r}{2}} + 1) \bmod N, N\right) = \text{pgcd}\left(((a^{\frac{r}{2}} \bmod N) + 1) \bmod N, N\right)$$

$$\text{pgcd}(a^{\frac{r}{2}} - 1, N) = \text{pgcd}\left((a^{\frac{r}{2}} - 1) \bmod N, N\right) = \text{pgcd}\left(((a^{\frac{r}{2}} \bmod N) + N - 1) \bmod N, N\right)$$

donnent un facteur trivial dans le cas où $a^{\frac{r}{2}} \equiv \pm 1 \bmod N$. Par contre, $a^{\frac{r}{2}} \equiv 1 \bmod N$ n'est pas possible, car on suppose que r est la bonne valeur de l'ordre pour a. Dans le cas restant,

$$\text{pgcd}((N - 1 + 1) \bmod N, N) = \text{pgcd}(0, N) = N$$

$$\text{pgcd}((N - 1 + N - 1) \bmod N, N) = \text{pgcd}((2N - 2) \bmod N, N) = \text{pgcd}(N - 2, N) = 1 \ (N \text{ est impair})$$

Ces équations expliquent les conditions à la ligne 12 du pseudocode et nous donnent une chance de trouver un facteur non-trivial grâce au calcul du pgcd à la ligne 13.

Cas où l'algorithme échoue

Il existe quelques façons pour qu'une itération de l'algorithme échoue. Cela se produit lors de la partie quantique de l'algorithme. D'abord, il se peut que le circuit de la recherche d'ordre n'est pas permis par D.4 d'avoir la vraie valeur de l'ordre de a. De ce fait, le reste du pseudocode ne peut pas marcher parce qu'on se base justement sur la supposition qu'on a obtenu le bon ordre. De plus, si les deux conditions de la ligne 12 ne sont pas respectées, le reste du pseudocode ne fonctionnera pas comme on vient de le voir mathématiquement. Peu importe le cas où l'algorithme échoue, le fait de prendre une autre valeur a lui donne la possibilité de ne pas tomber dans ces cas d'échecs lors de la prochaine itération. On ne le montre pas ici par manque de temps, mais la probabilité de succès à chaque itération est plus grande que $\frac{1}{2}$ [4] [6].

- *E.1* : Soient p un nombre premier impair et 2^d la plus grande puissance de 2 qui divise $\phi(p^\alpha)$. Alors, 2^d divise l'ordre d'un élément aléatoire dans $\mathbb{U}_{p^\alpha}$ avec une probabilité $\frac{1}{2}$.

p étant impair, on sait que $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ est pair. Ainsi, $d \geq 1$ forcément. Par le fait que $\mathbb{U}_{p^\alpha} = < g >$ est cyclique, tous ses éléments sont de la forme $g^k \bmod p^\alpha$ pour $k \in \{1, ..., \phi(p^\alpha)\}$. Soit $x = g^k \bmod p^\alpha$ d'ordre r pour un certain k.

Si k est impair, $g^{kr} \equiv 1 \bmod p^\alpha \implies \phi(p^\alpha)|kr$. Sachant que $2^d|\phi(p^\alpha)$, on conclue que $2^d|kr \implies 2^d|r$ puisque k est impair.

Si k est pair, $g^{k\frac{\phi(p^\alpha)}{2}} \equiv 1^{\frac{k}{2}} \bmod p^\alpha \equiv 1 \bmod p^\alpha$. Donc, $r|\frac{\phi(p^\alpha)}{2}$ et $2^d \nmid \frac{\phi(p^\alpha)}{2}$ indiquent que $2^d \nmid r$.

Au final, on peut séparer $\mathbb{U}_{p_\alpha}$ en deux parties égales, une contenant les éléments dont 2^d divise leur ordre et l'autre contenant les éléments pour lesquels 2^d ne divise pas leur ordre. Ainsi, on a une probabilité $\frac{1}{2}$ de choisir un élément de $\mathbb{U}_{p^\alpha}$ où $2^d|r$. □

- *E.2* : Soient $N = p_1^{\alpha_1}...p_k^{\alpha_k}$ un nombre composé impair et x un élément d'ordre r choisi aléatoirement depuis $\mathbb{U}_N$. Alors, $p(r$ est pair et $x^{\frac{r}{2}} \not\equiv -1 \bmod N) \geq 1 - \frac{1}{2^{k-1}}$.

Par l'isomorphisme entre $\mathbb{U}_N$ et $\prod_j \mathbb{U}_{p_j^{\alpha_j}}$, choisir un élément x d'ordre r aléatoirement dans $\mathbb{U}_N$ revient à choisir $x_j \in \mathbb{U}_{p_j^{\alpha_j}}$ d'ordre r_j aléatoirement où on impose que $x \equiv x_j \bmod p_j^{\alpha_j}\ \forall j$. Ainsi, par B.10, r correspond au ppcm des r_j et donc $r_j|r\ \forall j$. On remarque que $p(r$ est pair et $x^{\frac{r}{2}} \not\equiv -1 \bmod N) = 1 - p(r$ est impair ou $x^{\frac{r}{2}} \equiv -1 \bmod N)$ et on calcule cette dernière probabilité afin de prouver l'affirmation.

Dans le cas où r est impair, puisque $r_j|r$, les r_j sont tous impairs aussi $\implies d_j = 0\ \forall j$. Ainsi, pour que r soit impair, il faut que la même puissance de 2 divise tous les $r_j \implies$ par E.1 que $p(\text{impair}) = \left(\frac{1}{2}\right)^k = \frac{1}{2^k}$.

Dans le cas où $x^{\frac{r}{2}} \equiv -1 \bmod N$ (r est pair forcément), par le théorème des restes chinois, il faut que $x^{\frac{r}{2}} \equiv -1 \bmod p_j^{\alpha_j}\ \forall j \implies r_j \nmid r$ car $\frac{r}{2}$ n'est pas un multiple de r_j. Tout de même, $r_j|r \implies d_j = d\ \forall j$. Par E.1, $p(x^{\frac{r}{2}} \equiv -1 \bmod N) = \frac{1}{2^k}$.

Au final, $1 - p(r$ est impair ou $x^{\frac{r}{2}} \equiv -1 \bmod N) = 1 - \left(\frac{1}{2^k} + \frac{1}{2^k}\right) = 1 - \frac{1}{2^{k-1}} \geq 1 - \frac{1}{2^{k-1}}$. □

***Je ne suis vraiment pas sûr de cette preuve.

F Version compilée de l'algorithme de Shor

La version compilée de l'algorithme de Shor permet essentiellement de tricher dans le but de factoriser rapidement de très grands nombres. En effet, en se basant sur l'observation que différentes bases a amènent à la mesure de

différents ordres r [7], on peut tricher afin de choisir une base particulière qui donne une petite valeur pour l'ordre ($r = 2$ par exemple). Si on sait que l'ordre est petit, on peut grandement réduire la taille et les ressources qu'on utiliserait normalement pour l'algorithme de Shor, et ce à tel point que le circuit quantique ne serve pratiquement à rien. Ainsi, la recherche d'ordre devient extrêment facile et l'algorithme en lui-même est grandement accéléré. Au final, il devient très facile de trouver un facteur même pour de très grands nombres, et ce de manière quasi instantanée.

Smolin montre qu'il est toujours possible de trouver une base où l'ordre vaut 2 lorsqu'on connaît les facteurs [7]. En fait, connaître les facteurs accélère grandement l'obtention d'une telle base, mais on peut aussi l'avoir par force brute (pour des petits nombres évidemment) si on ne connaît pas a priori les facteurs. Aussi, Smolin indique que la plupart des articles scientifiques qui ont réussi à factoriser des nombres sur un ordinateur quantique utilisaient un truc du genre afin de faciliter la tâche à l'ordinateur quantique [7]. Par exemple, on peut factoriser RSA-768 instantanément grâce à la version compilée de Shor avec la base $a_{\text{RSA-768}}$, ce qui semble totalement fou. Il faut alors faire attention pour ne pas trop vite sauter aux conclusions quand on lit des articles prétendant exécuter le véritable algorithme de Shor sur une machine quantique.

RSA-768 = 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

$a_{\text{RSA-768}}$ = 1029031793302493258003488818376905875264575120178567995715921117383374063780955476265714655965556097487715509708453134212472071241551710737667646125017671995537319749739035045345865275994668289350825576184000476274812558092995299399 39

Remerciements

Je tiens d'abord à remercier Derek Courchesne qui m'a donné l'opportunité de travailler avec lui ce projet et qui a grandement aidé à ma compréhension des concepts clés de l'algorithme. Ton soutien a été essentiel dans mon apprentissage et dans mon développement de nouvelles compétences. De plus, je souhaite addresser mes remerciements à Stepan Gorgutsa et à toute l'équipe du C2T3 pour cette opportunité de stage incroyable. Merci également à Elisabeth, à Moras et à toute la chatastrophe pour leur compagnie tout au long de cet été enrichissant.

Références

[1] E. Kreyszig, H. Kreyszig, and E. J. Norminton, *Advanced Engineering Mathematics*. Hoboken, NJ : Wiley, tenth ed., 2011.

[2] B. Schumacher and M. Westmoreland, *Quantum Processes Systems, and Information*. Cambridge University Press, 2010.

[3] U. of Waterloo, "Chapter 3. the group of units modulo n."

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford, fourth ed., 1975.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, p. 1484–1509, Oct. 1997.

[7] J. A. Smolin, G. Smith, and A. Vargo, "Oversimplifying quantum factoring," *Nature*, vol. 499, p. 163–165, July 2013.