Chapitre 7

Factorisation et Algorithme de Shor

Un des développements les plus spectaculaires du calcul quantique est l'algorithme de Shor. Il s'agit d'un algorithme de factorisation pour les entiers de complexité polynomiale dans la taille de l'entier.

Le théorème fondamental de l'arithmétique nous assure que tout entier N peut être décomposé de facon unique en un produit de nombres premiers. étant donné les facteurs de N, il est facile de vérifier que le produit de ces facteurs redonne N. Plus précisément supposons que $N = p \cdot q$ avec p et q deux nombres premiers à $\mathrm{O}(b)$ bits. Si p et q sont connus, la vérification $N = p \cdot q$ peut se faire facilement avec $\mathrm{O}(b^2)$ opérations. Par contre étant donné un entier général N avec $\mathrm{O}(b)$ bits on ne connaaît pas d'algorithme polynomial permettant de calculer p et q (on ne sait même pas s'il en existe un ou non). On connaît plusieurs algorithmes plus rapides que $\mathrm{O}\left((1+\epsilon)^b\right)$ pour tout $\epsilon > 0$. Le meilleur algorithme connu possède un temps de calcul $\mathrm{O}\left(\exp(\frac{64}{9}b)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right)$. Concrètement un des records [1] relativement récents de factorisation atteint le 12 décembre 2009 pour un nombre à 232 décimales (b=768 bits) a utilisé des centaines de processeurs sur deux années de calcul.

Comme nous le verrons plus tard, l'algorithme de Shor permet une factorisation en temps polynomial avec un circuit quantique de taille polynomiale. L'algorithme de Shor résoud en fait un autre problème de théorie des nombres appelé *la recherche de l'ordre*. Il est connu depuis 1976 (environ) que la factorisation peut se réduire à la recherche de l'ordre.

Pour analyser la compexité de l'algorithme de Shor nous aurons aussi besoin de quelques notions supplémentaires sur les fractions continuées et la fonction d'Euler. Celles-ci ainsi que la réduction de la factorisation à la

1. Voir http ://en.wikipedia.org/wiki/RSA_numbers#RSA-768

recherche de l'ordre sont exposées dans la section suivante.

7.1 Une parenthèse de théorie de nombres

7.1.1 Factorisation basée sur la recherche de l'ordre

Soit $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ avec $p_i \neq 2$ et $k \geq 2$. En d'autres termes N ne contient pas de puissance de 2 et N n'est pas la puissance d'un nombre premier unique ($N \neq p^e$). Notez que les puissances de 2 sont aisément extraites car il est facile de voir si un entier et pair et de diviser par 2. De plus si $N = p^e$ il existe une méthode efficace pour trouver p et e.

Algorithme de factorisation basé sur la recherche de l'ordre.

a. Choisir aléatoirement uniformément $a \in \{2, \cdots, N-1\}$ et calculer

$$d = \mathrm{PGCD}\,(a, N)$$

grâce à l'algorithme d'Euclide (de complexité $O((\log_2 N)^3)$).

b. Si $d > 1$ nous avons un facteur non-trivial de N car $d|N$, (d divise N). On garde ce facteur et on retourne à a.

c. Si $d = 1$ (c'est-à-dire que a et N sont premiers entre eux) on calcule *le plus petit* entier r tel que

$$a^r = 1 \mod N.$$

Cet entier s'appelle *l'ordre de* $a \mod N$ aussi noté $r = \mathrm{Ord}_N(a)$. *Pour cette étape on ne connaaît pas d'algorithme classique polynomial. C'est l'étape qui sera traitée par l'algorithme de Shor.*

d. Supposons que r soit impair. Output `Fail` et retourner à a.

e. Si r est pair alors on sait que

$$a^r - 1 = \left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)$$

Notez que N divise $a^r - 1$. Donc il y a a priori 3 possibilités :

e1. N divise $a^{\frac{r}{2}} - 1$. Ceci est en fait impossible car alors on aurait $a^{\frac{r}{2}} = 1 \mod N$ et $\frac{r}{2}$ serait l'ordre.

e2. N divise $a^{\frac{r}{2}} + 1$. C'est-à-dire $a^{\frac{r}{2}} = -1 \mod N$. Output `Fail` et retourner à a.

e3. N partage des facteurs non-triviaux avec $a^{\frac{r}{2}} - 1$ et $a^{\frac{r}{2}} + 1$. Par exemple si $N = pq$ il faut que $p|(a^{\frac{r}{2}} - 1)$ et $q(|a^{\frac{r}{2}} + 1)$ ou vice versa. En d'autres termes

$$d_{\pm} = \mathrm{PGCD}\left(a^{\frac{r}{2}} \pm 1, N\right)$$

sont non-triviaux $d_+ > 1$ et $d_- > 1$ et nous avons 2 facteurs non-triviaux de N. Ceux-ci sont calculés grâce à l'algorithme d'Euclide (Complexité $\mathrm{O}\left((\log_2 N)^3\right)$).

f. Vérifier si le produit des facteurs trouvés dans les étapes précédentes vaut N. Si ce n'est pas encore le cas retourner à a.

Nous voyons qu'en présence d'un oracle qui permettrait résoudre l'étape c. la complexité d'une expérience (un round) provient uniquement de l'algorithme d'Euclide qui est $\mathrm{O}(b^3)$. Néanmoins cette expérience est probabiliste (étape a) et nous devons nous assurer que la probabilité de succès est non-négligeable. En fait on peut prouver $\mathrm{Prob}\,(\text{succès}) \geq \frac{3}{4}$. Cela implique qu'avec $T = \frac{|\ln \epsilon|}{|\ln 2|}$ expériences (rounds) on peut amplifier cette probabilité de succès à $\mathrm{Prob}\,(\text{succès en T rounds}) \geq 1 - \epsilon$.

Lors d'un round les seuls output `Fail` interviennent en d. et e2. Cela correspond à l'évènement

$$(r \text{ est impair}) \text{ ou } (a^{\frac{r}{2}} = -1 \mod N)$$

Ainsi

$$\mathrm{Prob}\,(\text{échec}) = \mathrm{Prob}\left((r \text{ est impair}) \text{ ou } (a^{\frac{r}{2}} = -1 \mod N)\right).$$

Théorème. Soit a pris uniformément aléatoirement dans $2, \cdots, N-1$. Soit r les plus petit entier satisfaisant à $a^r = 1 \mod N$. Alors $\mathrm{Prob}\,(\text{échec}) \leq \frac{1}{4}$.

Nous ne donnons pas de preuve ici. Ce théorème assure que la probabilité de succès de l'algorithme de factorisation basé sur la recherche de l'ordre est d'au moins $\frac{3}{4}$ lors d'un seul round. En faisant des ronds successifs il est possible d'amplifier cette probabilité à $1 - \epsilon$ ($\epsilon \ll 1$). Comme d'habitude le nombre de rounds requis est de l'ordre de $\mathrm{O}\left(|\ln \epsilon|\right)$.

7.1.2 Fractions continuées

Dans ce paragraphe nous donnons, sans démonstration, quelques résultats de théorie des nombres, utiles pour le développement ultérieur de l'algorithme de Shor.

Tout nombre réel peut être développé en *fraction continuée*. Ici nous discutons ce processus uniquement pour les *fractions rationnelles*. Prenons un exemple. Soit la fraction $x = \frac{263}{189}$. Les étapes succesives de l'algorithme d'Euclide du calcul du PGCD $(263, 189)$ sont :

$$\begin{aligned} 263 &= 1 \cdot 189 + 74 \\ 189 &= 2 \cdot 74 + 41 \\ 74 &= 1 \cdot 41 + 33 \\ 41 &= 1 \cdot 33 + 8 \\ 33 &= 4 \cdot 8 + 1 \end{aligned}$$

On voit que PGCD $(263, 189) = 1$. Etant donné qu'à chaque fois on divise par un nombre ≥ 2 le nombre d'étapes (de lignes ci-dessus) est de l'ordre de $\log_2(263)$, c'est-à-dire $\log_2(N)$ en général. De plus, chaque division requiert $\mathrm{O}\left((\log_2 N)^2\right)$ opérations. Donc le nombre total d'opérations pour l'algorithme d'Euclide est $\mathrm{O}\left((\log_2 N)^3\right)$. Maintenant, pour obtenir le *développement en fraction continuée*, on procède de la sorte :

$$\begin{aligned} \frac{263}{189} = 1 + \frac{74}{189} = 1 + \frac{1}{\frac{189}{74}} = 1 + \cfrac{1}{2 + \cfrac{41}{74}} \\ = 1 + \cfrac{1}{2 + \cfrac{1}{\cfrac{74}{41}}} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{33}{41}}} \\ = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\cfrac{41}{33}}}} \\ = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{8}{33}}}} \\ = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{33}{8}}}}} \end{aligned}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{8}}}}}$$

On dit que le développement en fraction continue est

$$\frac{263}{189} = [1; 2; 1; 1; 4; 8]$$

La forme générale du développement est :

$$x = [a_0; a_1; \cdots; a_n]$$

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Si $x > 1$ on a $a_0 \geq 1$ et si $x < 1$ on a $a_0 = 0$. De plus, ce développement n'est pas unique car on peut toujours écrire le dernier terme $\frac{1}{a_n}$ comme $\frac{1}{(a_n-1)+\frac{1}{1}}$. Ainsi

$$x = [a_0; a_1; \cdots a_{n-1}; a_n] = [a_0; a_1; \cdots; a_{n-1}; a_n - 1; 1]$$

Mais à cette ambigÃ¼ité près le développement est unique. De plus on peut le rendre unique en déclarant que l'on choisit toujours le développement le plus court possible. Le nombre d'opérations requises est le même que pour l'algorithme d'Euclide, $\mathrm{O}\left((\log_2 N)^3\right)$ ou $N = \max(\text{numérateur, dénominateur})$. La longueur du développement est $\mathrm{O}\left((\log_2 N)\right)$.

Définition : Notion de Convergent. Soit $x = [a_0; a_1; a_2; \cdots; a_n]$ un développement en fraction continuée de x. On appelle *convergents* les séries tronquées $[a_0; a_1; a_2; \cdots; a_m]$, $1 \leq m \leq n$. Ces convergents sont des nombres rationnels

$$[a_0; a_1; a_2; \cdots; a_m] = \frac{p_m}{q_m}.$$

Théorème : Propriétés des Convergents. Soit p_m/q_m l'ensemble des convergents d'une fraction x. Alors

a) PGCD $(p_m, q_m) = 1$ (p_m et q_m sont premiers entre eux) et $\left|x - \frac{p_m}{q_m}\right| \leq \frac{1}{q_m^2}$ (les convergents forment de bonnes approximations).

b) Réciproquement, toutes les approximations de la forme p/q avec p et q premiers entre eux, telles que $\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$ sont données par l'ensemble des convergents de x. On peut donc calculer ces approximations de facon systématique.

Pour nous, c'est la propriété b) qui sera utile dans l'analyse de l'algorithme de Shor.

Exercice : Donnez la liste de tous les convergents de $x = \frac{263}{189}$ et vérifiez l'affirmations (a) du théorème..

7.1.3 Fonction d'Euler

Pour un entier $r > 2$ on dit que $a \in \{1, 2, 3, \ldots, r-1\}$ est premier avec r (a is coprime with r) si PGCD $(a, r) = 1$. Le nombre de tels entiers a est donné par $\varphi(r)$, la *fonction d'Euler*. Si N est premier, $N = p$ on a bien sur : $a = 1, 2, 3, \ldots, p-1$ et $\varphi(p) = p - 1$. En général on montre que si

$$N = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

est la décomposition (unique) en facteurs premiers de N,

$$\begin{aligned}\varphi(N) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \ldots \varphi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \ldots p_k^{e_k-1}(p_k - 1)\end{aligned}$$

Exemple. Si $N = 9$ les a premiers avec N sont $a = 1, 2, 4, 5, 7, 8$ et donc $\varphi(9) = 6$. On vérifie $\varphi(9) = 3^{2-1}(3 - 1) = 6$

L' inégalité suivante (valable pour r assez grand) sera utile pour nous :

$$\varphi(r) \geq \frac{r}{4 \ln \ln r}$$

Le dénominateur $\ln \ln r$ croît extrèmement lentement. Par exemple pour $r = 10^{1000}$ (ce qui représente un nombre à 1000 dècimales) on a $\ln \ln r = \ln(1000 \ln 10) = 3 \ln 10 + \ln \ln 10 \leq 8$. En d'autre termes, étant donné r, une fraction appréciable des $r - 1$ nombres inférieurs sont premiers avec r (dans l'exemple cette fraction est supérieure à 1/32). Cette propriété peut être ré-exprimée comme suit. Fixons r et tirons $k \in \{1, 2, \ldots, r\}$ au hasard, uniformément, (c.a.d avec probabilité $\frac{1}{r}$. Alors :

$$\text{Prob}\,(\text{PGCD}\,(k, r) = 1) = \frac{\varphi(r)}{r} \geq \frac{1}{4(\ln \ln r)}$$

Le membre de droite de l'inégalité décroît trés lentement : on pourra y penser comme étant $O(1)$ (même si cela n'est pas vrai bien sur !).

7.2 Recherche de la période d'une fonction arithmétique

Comme nous l'avons expliqué, on peut ramener la factorisation d'un entier N à la recherche de l'ordre d'un nombre a pris au hasard dans $\{2, 3, ..., N-1\}$. L'ordre $Ord_n(a)$ est le plus petit entier r tel que

$$a^r = 1 \mod N.$$

En d'autres termes, nous cherchons la période de la fonction arithmétique

$$\begin{aligned} f_{a,N} : \mathbb{Z} &\to \mathbb{Z} \\ x &\to f_{a,N}(x) = a^x \mod N. \end{aligned}$$

Cette période (ou l'ordre) est le plus petit entier r t.q.

$$f_{a,N}(x) = f_{a,N}(x + r), \qquad \forall x \in \mathbb{Z}.$$

Nous commençons donc par étudier un algorithme général de "recherche de la période d'une fonction arithmétique".

Soit $f : \mathbb{Z} \to \mathbb{Z}$ de période inconnue

$$f(x) = f(x + r), \qquad \forall x \in \mathbb{Z}.$$

Comme nous serons obligés de travailler avec un nombre fini de bits, nous allons tronquer $\mathbb{Z}$ à $\frac{\mathbb{Z}}{M\mathbb{Z}} = \{0, 1, 2, ...M-1\}$ où M est choisi bien plus grand que r : $M >> r$. Ici, $\frac{\mathbb{Z}}{M\mathbb{Z}}$ est le groupe additif des entiers pris $\mod M$. En fait r est inconnu, mais nous supposons que l'on connait une borne supérieure, et qu'il est donc possible de choisir $M >> r$. Par exemple, pour la recherche de l'ordre, nous savons que $r < N$. Nous verrons dans ce cas que $M = O(N^2)$ est suffisant.

Tout d'abord il nous faut représenter les entiers $x \in \{0, ..., M-1\}$ par des états quantiques. Nous prenons (sans perte de généralité) $M = 2^m$ et notons que x peut être représenté grâce à son expansion binaire

$$x = 2^{m-1}x_{m-1} + 2^{m-2}x_{m-2} + ... + 2^2x_2 + 2x_1 + x_0,$$

avec m bits

$$x = \underbrace{(x_{m-1}.....x_0)}_{\text{dev binaire de x}}.$$

En particulier $(0, ..., 0) = 0$ et $(1, ..., 1) = 2^m - 1$. Il est donc naturel de prendre comme espace de Hilbert

$$\mathcal{H} = \underbrace{C^2 \otimes C^2 \otimes ... \otimes C^2}_{\text{m fois}},$$

et de stocker l'entier x dans un état quantique $|x\rangle \in \mathcal{H}$ construit à partir de m qubits (m systèmes à 2 niveaux : spins nucléaire, polarization des photons...)

$$|x\rangle = |x_{m-1}\rangle \otimes ... \otimes |x_0\rangle = |x_{m-1}, ..., x_0\rangle.$$

La fonction f est comme d'habitude représentée par l'opération unitaire

$$U_f : |x\rangle \otimes |0\rangle \to U_f|x\rangle \otimes |0\rangle = |x\rangle \otimes |f(x)\rangle$$

où $|0\rangle$ et $|f(x)\rangle$ dont des états à m qubits (dans l'algorithme de shor on calcule $f(x)$ mod N et donc m bits suffisent certainement). Nous aurons aussi besoin de la "Transformée de Fourrier Quantique" définie par :

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} |y\rangle \quad = \frac{1}{2^{m/2}} \sum_{y_0....y_{m-1} \in \{0,1\}^m} e^{2\pi i \frac{xy}{M}} |y_0....y_{m-1}\rangle$$

Cette opération est linéaire c.a.d que si $|\Psi\rangle = \sum_{x=0}^{M-1} c_x|x\rangle$, alors

$$QFT|\Psi\rangle = \sum_{x=0}^{M-1} c_x QFT|x\rangle.$$

On peut aussi montrer que l'opération est unitaire : ceci est un prérequis important pour pouvoir la réaliser grâce à un circuit quantique.

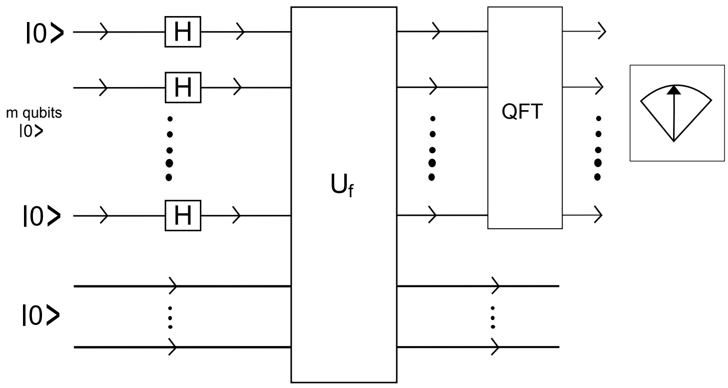

FIGURE 7.1 – Circuit quantique pour la recherche de la période d'une fonction arithmétique

7.3 Circuit pour la recherche de la période

Le circuit de l'algorithme de recherche de la période est représenté sur la figure 7.1.

Le circuit pour U_f dépend de la fonction spécifique. Pour la recherche de l'ordre nous prendrons la fonction $f(x) = a^x \mod N$ et verrons comment réaliser son circuit au paragraphe 7.7. Le circuit pour QFT sera réalisé au paragraphe 7.6.

Calculons maintenant l'évolution de l'état initial :

$$|0\rangle \otimes |0\rangle = \underbrace{|0...0\rangle}_{\text{m fois}} \otimes \underbrace{|0...0\rangle}_{\text{m fois}}.$$

Juste après les portes de Hadamard :

$$H^{\otimes m} \underbrace{|0...0\rangle}_{\text{m fois}} \otimes |0\rangle ... = \left(\frac{1}{2^{\frac{m}{2}}} \sum_{x_0...x_{m-1} \in \{0,1\}^m} |x_{m-1}....x_0\rangle \right) \otimes |0\rangle.$$

C'est un état de superposition cohérente sur toutes les entrées classiques. Il peut aussi s'écrire de façon plus compacte :

$$\left(\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \right) \otimes |0\rangle.$$

Après U_f nous obtenons l'état

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle.$$

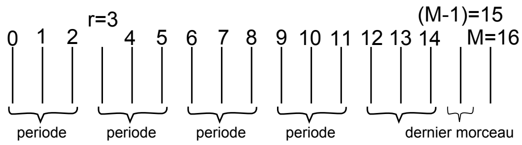

FIGURE 7.2 – Exemple de décomposition de $\{0, 1, ..., M-1\}$ pour $r = 3$ et $M = 16$

Exploitons le fait que f est périodique pour réorganiser cette somme. L'intervalle $[0, M-1]$ est décomposé en morceaux de longueur r, sauf pour le dernier qui sera plus court. Les entiers dans la premiere periode sont $x_0 \in \{0, 1, ..., r-1\}$. Si M était un multiple de r, on pourrait représenter chaque x comme

$$x = x_0 + jr \text{ avec } 0 \leq j \leq \frac{M}{r} - 1.$$

Dans le cas gén'eral (voir figure 7.2) on aura

$$x = x_0 + jr \text{ avec } 0 \leq j \leq A(x_0) - 1,$$

et $A(x_0)$ un entier dépendant de x_0 qui doit satisfaire

$$M - r \leq x_0 + (A(x_0) - 1)r \leq M - 1.$$

Nous avons :

$$\begin{aligned}
\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0 + jr)\rangle \\
=& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0)\rangle.
\end{aligned}$$

Finalement nous agissons sur cet état avec QFT. L'état obtenu est :

$$\begin{aligned}
|\Psi_{\text{fin}}\rangle =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} QFT|x_0 + jr\rangle \otimes |f(x_0)\rangle \\
=& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{(x_0+jr)y}{M}} |y\rangle \otimes |f(x_0)\rangle \\
=& \frac{1}{M} \sum_{x_0=0}^{r-1} \left(\sum_{y=0}^{M-1} \left(e^{2\pi i \frac{x_0 y}{M}} \sum_{j=0}^{A(x_0)-1} e^{2\pi i \frac{jy}{M/r}} \right) |y\rangle \right) \otimes |f(x_0)\rangle.
\end{aligned}$$

Cette dernière expression est l'état final $|\Psi_{\text{fin}}\rangle$ juste avant la mesure.

7.4 Le Processus de Mesure

Il reste maintenant à analyser l'opération de mesure. Tout d'abord il nous faut choisir une "base représentant l'appareil de mesure“. Celle-ci est formée par l'ensemble des projecteurs.

$$P_y = |y\rangle\langle y| \otimes \mathbb{I}_{m\times m}, \qquad y \in \{0, 1, 2, \cdots M-1\}.$$

L'état quantique résultant juste après la mesure est

$$\frac{P_y|\Psi\rangle_{\text{fin}}}{\langle\Psi_{\text{fin}}|P_y|\Psi_{\text{fin}}\rangle},$$

avec la probabilité

$$\text{Prob}(y) = \langle\Psi_{\text{fin}}|P_y|\Psi_{\text{fin}}\rangle.$$

D'abord, on calcule $P_y|\Psi_{\text{fin}}\rangle$,

$$P_y|\Psi_{\text{fin}}\rangle == \frac{1}{M}\sum_{x_0=0}^{r-1}\left(e^{2\pi i\frac{x_0 y}{M}}\sum_{j=0}^{A(x_0)-1} e^{2\pi i\frac{jy}{M/r}}\right)|y\rangle \otimes |f(x_0)\rangle.$$

Puis $\langle\Psi_{\text{fin}}|P_y|\Psi_{\text{fin}}\rangle = \langle\Psi_{\text{fin}}|P_y P_y|\Psi_{\text{fin}}\rangle$. Cela donne

$$\text{Prob}(y) = \frac{1}{M^2}\sum_{x_0=0}^{r-1}\left|\sum_{j=0}^{A(x_0)=1} e^{2\pi i\frac{jy}{M/r}}\right|^2.$$

Remarquons que les différents termes de la somme sur x_0 n'interfèrent pas car les kets $|f(x_0)\rangle$ sont orthogonaux entre eux.

7.5 Analyse de la probabilité $\text{Prob}(y)$

7.5.1 Traitons d'abord le cas (irréaliste) simple ou M serait multiple de r

Dans ce cas, $A(x_0) = \frac{M}{r}$ et donc

$$\text{Prob}(y) = \frac{r}{M^2}\left|\sum_{j=0}^{\frac{M}{r}-1} e^{2\pi i\frac{jy}{M/r}}\right|^2.$$

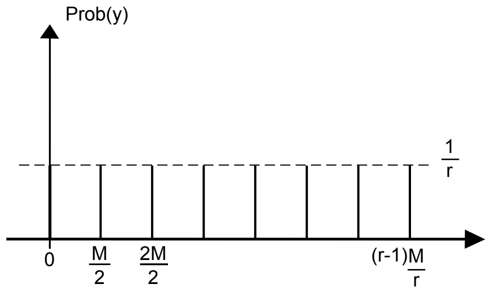

FIGURE 7.3 – Distribution de probabilité des résultats de mesures pour M multiple de r.

Si $y = k\frac{M}{r}$ avec $k = \{0, 1, ..., r-1\}$ on a

$$e^{2\pi i \frac{jy}{M/r}} = e^{2\pi ijk} = 1.$$

Si bien que $\text{Prob}(y) = \frac{r}{M^2}\left|\frac{M}{r}\right|^2 = \frac{1}{r}$. Puisque cette probabilité doit se sommer à 1, nous en déduisons qu'elle est nulle pour toutes les autres valeurs de $y \neq k\frac{M}{r}$. Cette distribution est représentée sur la figure 7.3.

La mesure donne avec probabilité 1 une valeur de y de la forme

$$y = k\frac{M}{r} \ \ avec \ \ k \in \{0, 1, ..., r-1\}.$$

Puisque M est connu, grâce à la valeur de y donnée par la mesure, nous calculons $\frac{y}{M}$. Deux cas de figure se presentent à nous :

- $\frac{y}{M} = \frac{k}{r}$ et PGCD $(k, r) = 1$. Alors nous pouvons trouver k et r en simplifiant la fraction $\frac{y}{M}$ "au maximum" jusqu'à ce que les numérateurs et dénominateurs n'aient plus de facteurs communs. Nous trouvons ainsi r.
- $\frac{y}{M} = \frac{k}{r}$ et PGCD $(k, r) \neq 1$. Alors nous ne savons pas jusqu'où simplifier la fraction (et n'avons pas de facon systématique de trouver k et r).

En "pratique" nous ne savons pas à priori si k et r sont premiers entre eux ou non. Ainsi nous adoptons la procédure suivante : dans tous les cas simplifier la fraction $\frac{y}{M}$ au maximum, et tester si le r trouvé est une période de $f(x)$ ou non.

La probabilité de succès est la probabilité d'avoir PGCD $(k, r) = 1$ quand k est tiré uniformément dans $\{0, 1, ..., r-1\}$. D'après ce que nous avons appris dans le chapitre précédent :

$$\text{Prob}(\text{PGCD}\,(k, r) = 1, k \in \{0, 1, ..., r-1\}) = \frac{\varphi(r)}{r} \geq \frac{1}{4(\ln \ln r)}.$$

Puisque $r < M$, nous avons *une probabilité de succès pour une expérience* :

$$\text{Prob(succes)} \geq \frac{1}{4 \ln \ln M} \qquad \left(= \frac{1}{4 \ln 2 \ln m}\right).$$

Bien que cette probabilité soit faible, nous pouvons l'amplifier en faisant tourner le circuit plusieurs fois. Au bout de T expériences (ou "rounds") :

$$\text{Prob(au moins 1 succes au bout de T rounds)} \geq 1 - \left(1 - \frac{1}{4 \ln \ln M}\right)^T,$$

ce qui peut être rendu proche de $1 - \epsilon$ si on prend

$$T = O(|\ln \epsilon| \ln \ln M) = O(|\ln m||\ln \epsilon|).$$

En effet :

$$\begin{aligned}
&1 - \left(1 - \frac{1}{4 \ln M}\right)^T \geq 1 - \epsilon \\
&\leftrightarrow \epsilon \geq \left(1 - \frac{1}{4 \ln M}\right)^T \leftrightarrow \ln \epsilon \geq T \ln \left(1 - \frac{1}{4 \ln M}\right) \\
&\leftrightarrow \ln \epsilon \geq -T \frac{1}{4 \ln M} \ (M \text{ grand}) \\
&\leftrightarrow T \geq 4(\ln \ln M)|\ln \epsilon|
\end{aligned}$$

7.5.2 Passons maintenant au cas général ou M n'est pas un multiple de r.

Nous allons utiliser un Lemme technique (la démonstration n'est pas donnée ici). Une illustration graphique de son contenu est fournie par la figure 7.4. En gros, le Lemme affirme que la distibution de probabilité Prob(y) est concentrée sur les entiers proches des fractions kM/r.

Lemme. Soit $I = \cup_{k=0}^{r-1} \left[k\frac{M}{r} - \frac{1}{2}, k\frac{M}{r} + \frac{1}{2}\right] = \cup_{k=0}^{r-1} I_k$ une union d'intervalles disjoints I_k. Alors,

$$\text{Prob}(y \in I) \geq \frac{2}{5}.$$

Ainsi, avec probabilité au moins $\frac{2}{5}$ les mesures fournissent des entiers y proches de $k\frac{M}{r}$ avec $k \in \{0, 1, ..., r-1\}$. Lorsqu'une mesure donne $y \in I$ cela signifie qu'il existe k entier tel que

$$k\frac{M}{r} - \frac{1}{2} \leq y \leq k\frac{M}{r} + \frac{1}{2},$$

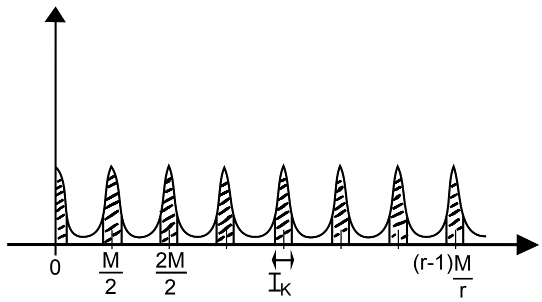

FIGURE 7.4 – Distribution de probabilité fournie par les mesures. L'aire hachurée est superieure a $\frac{2}{5}$. Notez que les intervalles I_k ont une longueur 1 et sont distant d'environ $M/r >> 1$.

ce qui est équivalent à

$$\left|\frac{y}{M}-\frac{k}{r}\right| \leq \frac{1}{2M}. \tag{7.1}$$

Maintenant supposons que nous prenions $M > r^2$. Alors cette inégalité entraine,

$$\left|\frac{y}{M}-\frac{k}{r}\right| \leq \frac{1}{2r^2} \text{ pour } k \in \{0, 1, ..., r-1\}.$$

Comment pouvons nous determiner k et r à partir de y et M ? D'après ce que nous avons vu dans la théorie des fractions continuées, si le PGCD $(k, r) = 1$, alors $\frac{k}{r}$ est nécessairement un "convergent" du développement en fractions continuées de $\frac{y}{M}$. Il y a un nombre fini de "convergents" car $\frac{y}{M}$ est rationnel, et ceux-ci peuvent être systématiquement calculés grâce à l'algorithme d'Euclide (en temps $O((\ln M)^3)$. Par contre si PGCD $(k, r) \neq 1$ on ne peut pas affirmer que $\frac{k}{r}$ est un convergent de $\frac{y}{M}$ et n'avons, dans ce cas, pas de moyen systématique de calculer k et r.

Nous adoptons donc la procédure suivante. Nous calculons tous les convergents de $\frac{y}{M}$ (grâce à l'algorithme d'Euclide) et examinons leurs dénominateurs r. Pour chacun de ces dénominateurs nous testons si c'est une période de $f(x)$. Le succès est assuré si PGCD $(k, r) = 1$, ce qui a lieu avec probabilté $O(\frac{1}{4 \ln \ln r})$.

Récapitulons. Quel est la probabilité de succès lors d'une expérience avec le circuit quantique ? Le circuit quantique est initialisé dans l'état $|0\rangle \otimes |0\rangle$. L'evolution unitaire conduit à l'état $|\Psi_{final}\rangle$, après quoi on effectue une mesure. Cette mesure donne l'entier y. Pour en déduire r avec succès, il faut remplir deux conditions :

– $y \in I$ pour un certain $k \in \{0, 1, ..., r-1\}$.
– Etant donné $y \in I_k$ il faut PGCD $(k, r) = 1$.
Donc :

$$\text{Prob(succes)} \geq \frac{2}{5} \times \frac{1}{4 \ln \ln r}.$$

En itérant l'experience $T \approx O(|\ln \epsilon| \ln \ln r)$ fois on peut amplifier la probabilité de succès à $1 - \epsilon$.

7.6 Le circuit de la QFT

Dans ce paragraphe nous montrons comment réaliser le circuit de la QFT. En exercice nous avons vu que pour $M = 2$, on a $QFT = H$ (la porte de Hadamard) :

$$(QFT)_{M=2}|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle).$$

Pour $M = 4$,

$$\begin{aligned}
(QFT)_{M=4}|x\rangle &= \frac{1}{\sqrt{4}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle + e^{i\pi x}|2\rangle + e^{3i\frac{\pi}{2}x}|3\rangle\right) \\
&= \frac{1}{\sqrt{4}}\left(|00\rangle + e^{i\frac{\pi}{2}x}|01\rangle + e^{i\pi x}|10\rangle + e^{3i\frac{\pi}{2}x}|11\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi x}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle\right).
\end{aligned}$$

En notation binaire $x \in \{0, 1, 2, 3\}$ est représenté par

$$x = 2x_1 + x_0\,;\ x_0, x_1 \in \{0, 1\}$$

si bien que $e^{i\pi x} = e^{2\pi i x_1}e^{i\pi x_0} = (-1)^{x_0}$ et $e^{i\frac{\pi}{2}x} = e^{i\pi x_1}e^{i\frac{\pi}{2}x_0} = (-1)^{x_1}e^{i\frac{\pi}{2}x_0}$. On trouve alors

$$(QFT)_{M=4}|x\rangle = \left(\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + (-1)^{x_1}e^{i\frac{\pi}{2}x_0}|1\rangle}{\sqrt{2}}\right).$$

Cette factorisation est à la base de la réalisation du circuit de la QFT. La factorisation suggère le circuit suivant de la figure 7.5. La première opération $SWAP$ échange les deux qubits. Elle peut être réalisée par trois portes $CNOT$ (figure 7.6). La seconde operation de la figure 7.5 est une porte de

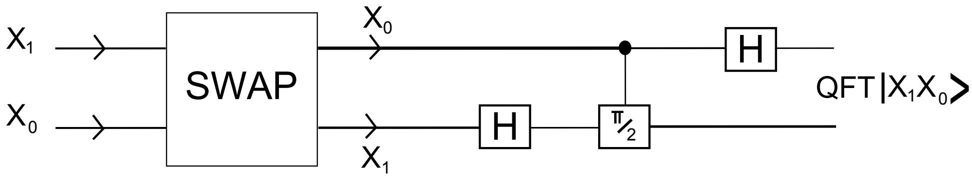

FIGURE 7.5 – Circuit de la $(QFT)_{M=4}$.

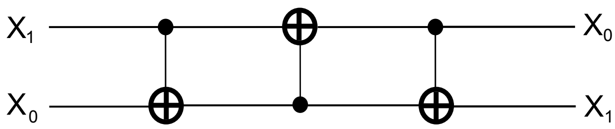

FIGURE 7.6 – Circuit pour un $SWAP$.

Hadamard agissant sur $|x_1\rangle$ pour produire $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$. La troisième opération est un "phase shift" controlé par le premier bit x_0 : si $x_0 = 0$ il n'y a pas de phase shift et le second bit reste dans l'etat $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$; par contre si $x_0 = 1$, il y a un phase shift et le second bit est transformé en $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}e^{i\frac{\pi}{2}}|1\rangle)$. Enfin, la dernière porte de Hadamard agit sur $|x_0\rangle$ pour produire $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0}|1\rangle)$.

Le circuit général de la QFT est obtenu par une généralisation des remarques ci-dessus.

Lemme. Pour $x \in \{0, 1, ...M - 1\}$ et $M = 2^m$

$$QFT|x\rangle = \prod_{l-1}^{m} \frac{(|0\rangle + e^{i\frac{\pi}{2^{l-1}}x}|1\rangle)}{\sqrt{2}}.$$

Démonstration. Rappelons que

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}}|y\rangle = \frac{1}{2^{\frac{m}{2}}} \sum_{y=0}^{2^m-1} e^{2\pi i \frac{xy}{2^m}}|y\rangle.$$

Chaque $y \in \{0, 1, ..., 2^m - 1\}$ possède un developpement binaire

$$\begin{aligned} y &= 2^{m-1}y_{m-1} + 2^{m-2}y_{m-2} + ... + 2y_1 + y_0 \\ &= 2y' + y_0 \end{aligned}$$

où $y' = 2^{m-2}y_{m-1} + ... + y_1$. On décompose la somme sur y en une somme avec $y_0 = 0$ et une somme avec $y_0 = 1$ (cela revient a séparer les y pairs et impairs.)

$$QFT|x\rangle = \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x2y'}{2^m}} |y'\rangle \otimes |0\rangle + \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x(2y'+1)}{2^m}} |y'\rangle \otimes |1\rangle$$

$$= \left(\frac{1}{2^{\frac{m-1}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{xy'}{2^{m-1}}} |y'\rangle \right) \otimes \left(|0\rangle + e^{\frac{\pi i x}{2^{m-1}}} |1\rangle \right).$$

Cette factorisation peut maintenant être répétée sur la premiere parenthèse. La seule difference est que $m \to m-1$. On obtient

$$QFT|x\rangle = \left(\frac{1}{2^{\frac{m-2}{2}}} \sum_{y''=0}^{2^{m-2}-1} e^{2\pi i \frac{xy''}{2^{m-2}-1}} |y''\rangle \right) \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-2}}} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-1}}} |1\rangle}{\sqrt{2}}.$$

En itérant ce procédé, on obtient le résultat du lemme.

La dernière étape consiste à remplacer x par son développement binaire (comme nous l'avons fait pour $M = 4$)

$$x = 2^{m-1} x_{m-1} + ... + 2^2 x_2 + 2x_1 + x_0,$$

ce qui implique pour tout $1 \leq l \leq m$

$$e^{i\frac{\pi}{2^{l-1}} x} = e^{i\pi x_{l-1}} e^{i\frac{\pi}{2} x_{l-2}} ... e^{i\frac{\pi}{2^{l-1}} x_0}.$$

Ici le point est que les bits x_i avec $i \geq l$ ne contribuent pas. Remplacant cette expression dans la formule du lemme, on trouve la décomposition finale qui permet de construire un circuit :

$$QFT|x\rangle = \prod_{l=1}^{m} \left(\frac{|0\rangle + e^{i\pi x_{l-1}} e^{i\frac{\pi}{2} x_{l-2}} ... e^{i\frac{\pi}{2^{l-1}} x_0} |1\rangle}{\sqrt{2}} \right).$$

La figure 7.7 représente le circuit correspondant à cette dernière formule pour $m = 4$, c.a.d $M = 16$. On peut se convaincre que l'opération de $SWAP$ requiert $O(3m)$ portes $CNOT$. D'autre part, le nombre de portes H et déphasages controlés est

$$m + (m-1) + ... + 1 = \frac{m(m+1)}{2}.$$

La profondeur du circuit est donc de l'ordre de $O(m^2)$. Cette profondeur indique comment le temps de calcul pour la QFT augmente avec la taille des entrées. D'autre part la largeur du circuit est m. Ainsi la taille totale est profondeur $\times$ largeur $= O(m^3)$.

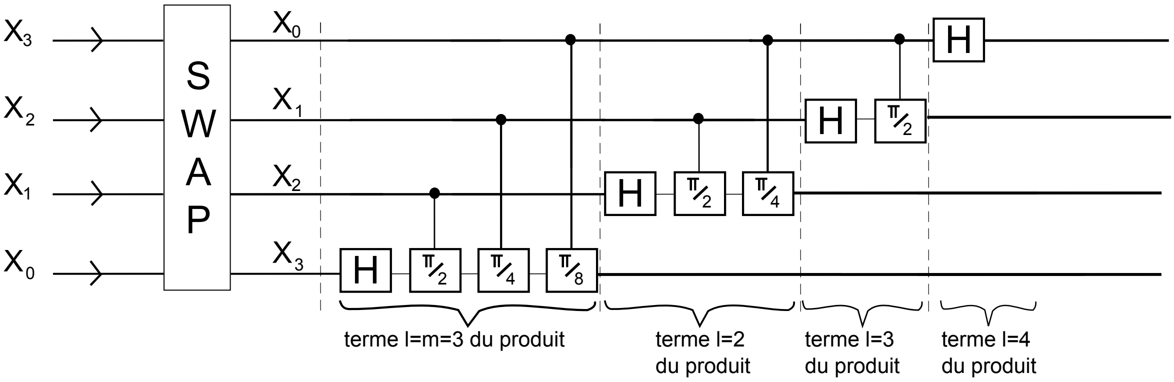

FIGURE 7.7 – Circuit de la QFT pour 4 qubits.

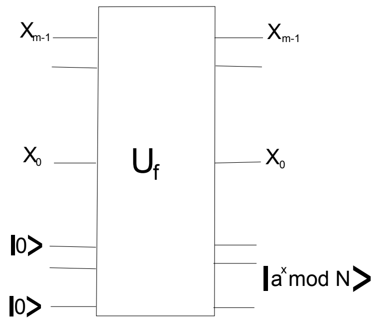

FIGURE 7.8 – Représentation unitaire de l'exponentielle modulaire

7.7 Circuit pour $U_{f_{a,N}}$

Dans le chapitre précédent nous avons donné un algorithme aléatoire de factorisation d'entiers N basé sur la recherche de la période de l'exponentielle modulaire. Plus précisement, pour a t.q. PGCD $(a, N) = 1$, on cherche la période de la fonction $f_{a,N}(x) = a^x \mod N$. Ceci est équivalent à la recherche de $Ord_N(a) = r$ c.à.d le plus petit entier r t.q $a^r = 1 \mod N$.

Nous devons trouver un circuit qui réalise l'opérateur unitaire correspondant $U_{f_{a,N}}$. Notons d'abord que

$$\begin{aligned} a^x &= a^{2^{m-1}x_{m-1}} a^{2^{m-2}x_{m-2}} \dots a^{2x_1} a^{x_0} \\ &= \left(a^{2^{m-1}}\right)^{x_{m-1}} \left(a^{2^{m-2}}\right)^{x_{m-2}} \dots \left(a^2\right)^{x_1} a^{x_0}. \end{aligned}$$

Il est possible de pré-calculer les puissances $\{a, a^2, a^4, a^8, ..., a^{2^{m-1}}\}$ en un nombre polynomial d'opérations. En effet on part de a qui posséde m bits (au plus). Son carré a^2 se calcule en m^2 opérations. Puisque a^2 est pris

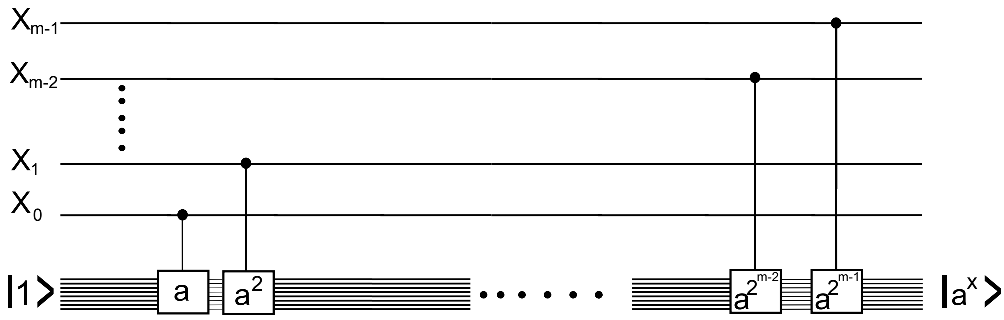

FIGURE 7.9 – Circuit pour l'exponentielle modulaire.

mod M, a^2 possède aussi m bits au plus. Le carré de ce dernier $a^4 = (a^2)^2$ se calcule en m^2 opérations, et ainsi de suite. En itérant ce procédé m fois, on va jusqu'au calcul de $a^{2^{m-1}}$. Ainsi on peut pré-calculer toutes ces puissances en $O(m^3)$ opérations. Il existe des circuits classiques réversibles pour faire ce calcul, et puisqu'ils sont réversibles, ils peuvent aussi être rendus quantiques (c.à.d unitaires). Finalement pour calculer a^x, en vertu de l'identité ci-dessus il suffit de prendre le circuit (figure 7.9) : La profondeur de ce circuit est $O(m^3)$, sa largeur $O(m)$ et sa taille $O(m^4)$.

7.8 Résumé de l'algorithme de Shor

Nous sommes maintenant en mesure de résumer la totalité de l'algorithme quantique de Shor pour la factorisation d'un entier N.

<u>input</u> : N impair et avec au moins deux facteurs premiers distincts.

<u>output</u> : facteur non trivial de N.

<u>temps de calcul</u> : $O((\ln N)^3 \ln\ln N |\ln \epsilon|)$ pour une probabilité de succès supérieure à $1 - \epsilon$.

<u>taille du circuit</u> : $O((\ln N)^3)$.

<u>Algorithme</u> :

1. Choisir uniformément aléatoirement $a \in \{2....N-1\}$.

2. Calculer PGCD $(a, N) = d$ par l'algorithme d'Euclide :

– si $d > 1 \rightarrow$ SUCCES ; on a un facteur,

– sinon $d = 1 \rightarrow$ aller en 3.

3. Calculer $Ord_N(a)$ (i.e $a^r = 1 \mod N$, trouver le plus petit r). Pour cela utiliser le circuit quantique avec m qubits et $2^m = M \approx N^2$. Faire une mesure quantique et considérer le résultat y. Calculer les convergents de $\frac{y}{M}$ (grâce à l'algorithme d'Euclide). Trouver si r se trouve parmi les dénominateurs de ces convergents en testant $a^r = 1 \mod N$.
– si oui (la théorie assure que c'est le plus petit possible) $\rightarrow$ aller en 4,
– sinon $\rightarrow$ ECHEC.

4. Verifier si r est pair et $a^r \neq -1 \mod N$
– si oui $\rightarrow$ aller en 5,
– sinon $\rightarrow$ ECHEC.

5. Calculer PGCD $\left(a^{\frac{r}{2}} + 1, N\right)$ et PGCD $\left(a^{\frac{r}{2}} - 1, N\right)$. Cela donne deux facteurs non triviaux de N (grâce à l'algorithme d'Euclide).

La probabilité de succès d'un tel "round" est $O\left(\frac{1}{\ln \ln N}\right)$ et sa complexité (temps de calcul) $O((\ln N)^3)$. On peut amplifier (comme d'habitude) la probabilité de succès à $1 - \epsilon$ en faisant $O(\ln \ln N)$ rounds. Le temps de calcul total sera alors $O(|\ln \epsilon|(\ln \ln N)(\ln N)^3)$.