Algorithme de Shor

Problème: factoriser un nombre N arbitraire et grand
(qui ne doit pas être une puissance de 2 ni un carré)

Un tout petit peu d'arithmétique

Soit x quelconque, x<N

Si x n'est pas premier avec N: on a un diviseur de N

Si x est premier avec N, on définit l'ordre de x comme le plus petit entier r tel que:

$$x^r = 1 \quad [N]$$

f(a)=x^a [N] est donc une fonction périodique de période r

Si on connaît r, alors on a une chance sur 2 environ que
r soit pair
et $x^{r/2} \neq -1 \quad [N]$

Alors, le $\gcd(N, x^{r/2} \pm 1)$ *est un facteur non trivial de N*

(il existe des algorithmes classiques efficaces pour trouver le gcd de deux nombres)

Factoriser ou trouver l'ordre d'un entier arbitraire (i.e. le logarithme discret de 1 en base x) sont des problèmes équivalents.
Tous deux sont difficiles avec un ordinateur classique
(pas de preuve mathématique)
L'algorithme de Shor fournit l'ordre en un temps polynomial

Exemple trivial

N=15

(le premier non premier, non pair, non carré)

Au hasard x=7

On calcule 7^a *[15]*

a	7^a [15]
1	7
2	4
3	13
4	1

$7^4=1$ *[15]: l'ordre r de 7 est donc 4*

le gcd de 4+1 et 15 est donc un facteur de 15: 5
le gcd de 4-1 et 15 est donc un facteur de 15: 3

Donc

15=5x3

qui l'eut cru??

Algorithme quantique

idée: *calculer beaucoup de valeurs de x^a [N]*
(en utilisant le parallélisme quantique)
Extraire la période r

On travaille sur 2 registres de m qubits

$$q = 2^m \qquad 2N^2 \le q < 4N^2$$

Etat initial

$$|0,0\rangle$$

Choix de x

Générateur aléatoire classique ou mesure quantique

Préparation d'une superposition de tous les nombres
dans le premier registre

$$|0,0\rangle \xrightarrow{U_H} |j\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a,0\rangle$$

U_H: transformation de Hadamard

sur chaque qubit $|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Exponentiation modulaire

$$|j\rangle \longrightarrow \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \ [N]\rangle$$

Faisable en temps polynomial

Calcul simultané de toutes les valeurs de x^a
Intervention du parallélisme quantique

Mesure des m derniers qubits

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}\left|a, x^a\ [N]\right\rangle$$

On obtient une valeur aléatoire y.

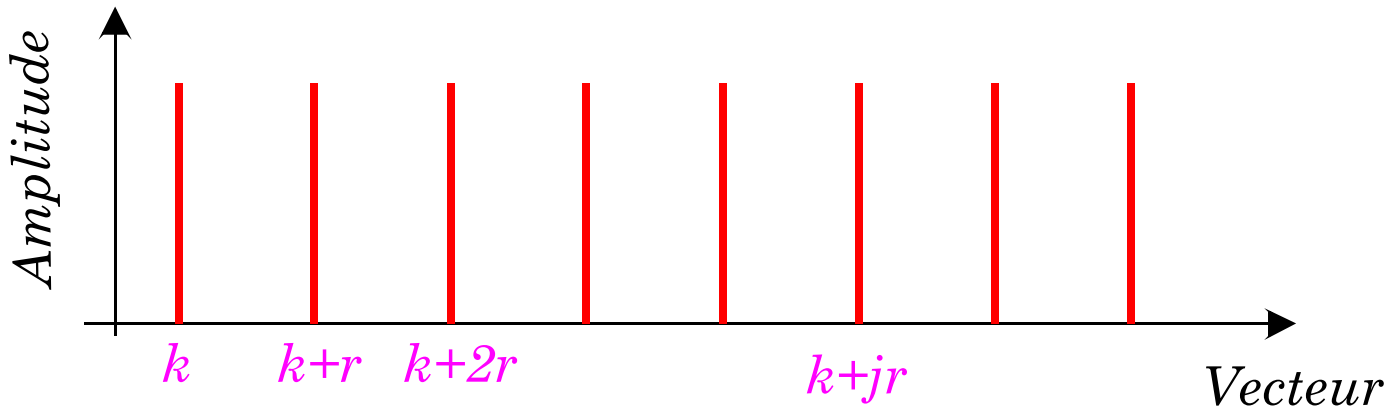
Mais cette valeur a pour antécédent toutes les valeurs de la forme $k+jr$ *où* k *est le plus petit entier tel que* $x^k=y$ *et* j *un entier quelconque*

Les m premiers qubits sont corrélés quantiquement (intriqués) avec ceux que l'on mesure. La mesure les projette sur les états correspondant au résultat obtenu.

L'état, après la mesure du premier registre, est donc:

$$\frac{1}{A}\sum_{j}\left|k+jr\right\rangle$$

Les amplitudes de probabilité sur les différents vecteurs de base forment un peigne de période r



Comme q est de l'ordre de N^2 *et que* $r<N$, *on a au moins N périodes*

On doit extraire cette période et éliminer le décalage aléatoire k.

Pour cela, on effectue sur les premiers qubits une...

Transformée de Fourier discrète

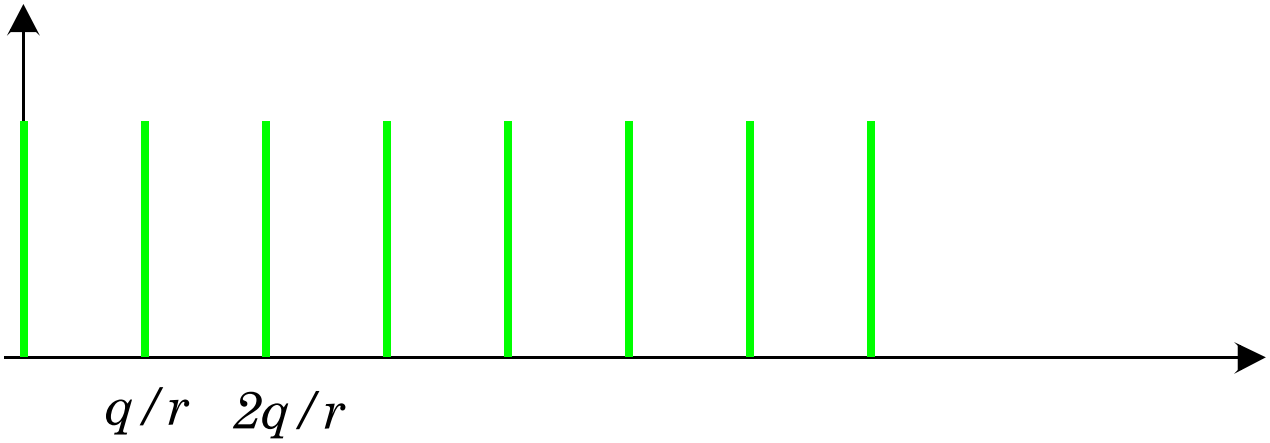
$$\sum_0 a_a |a\rangle \longrightarrow \sum_b b_b |b\rangle$$

avec

$$b_b \propto \sum_a e^{2ip\frac{ab}{q}}$$

Faisable en m^2 opérations au plus (i.e. en un temps polynomial)

Les a_a étant périodique de période r,
les b_b sont périodiques de période q/r (grand entier)



Si on mesure les m premiers bits, on obtient une valeur de la forme

$$l\frac{q}{r}$$

où l est un entier aléatoire

A partir de là, on peut extraire (avec un calculateur classique) avec une probabilité finie la période r
(les détails de cette extraction sont fastidieux)

Quelques caractéristiques importantes de l'algorithme de Shor

Probabiliste

On a une probabilité finie d'obtenir le bon résultat

Mais il est trivial de tester la solution obtenue

et cette probabilité ne décroit pas exponentiellement avec le nombre de bits

Utilise le parallélisme quantique

Pour effectuer en une seule opération toutes les exponentiations modulaires possibles

Revient à "essayer tous les diviseurs à la fois"

Utilise les corrélations quantiques et le postulat de la mesure:

Les deux registres dans l'état

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}\left|a, x^a \left[N\right]\right\rangle$$

sont corrélés quantiquement au même titre que la "paire EPR" dans l'état

$$\frac{1}{\sqrt{2}}\left(\left|\uparrow\downarrow\right\rangle - \left|\downarrow\uparrow\right\rangle\right)$$

La non-localité de la mécanique quantique est essentielle

L'algorithme utilise donc des propriétés authentiquement quantiques

Très différent de ce qu'on pourrait faire avec un calculateur analogique

(même s'il manipulait des superpositions d'états)