Factorisation Quantique

journées scientifiques,
université de Toulon,
Avril 2015.

Philippe Langevin

IMATH, université de Toulon

last revision 21 avril 2015.

Une introduction à l'algorithme de factorisation de Peter Shor (1997)

Sommaire

Factorisation classique

fait

L'algorithme du crible algébrique factorise un entier de t bits en

$$\mathrm{O}(\exp\left(ct^{\alpha}\log^{1-\alpha}t\right)) \quad \textit{étapes,}$$

avec $c \leq 1.93$, $\alpha \leq \frac{1}{3}$, complexité sous-exponentielle.

dernier record :

Factorisation classique

fait

L'algorithme du crible algébrique factorise un entier de t bits en

$$\mathrm{O}(\exp\left(ct^{\alpha}\log^{1-\alpha}t\right)) \quad \textit{étapes,}$$

avec $c \leq 1.93$, $\alpha \leq \frac{1}{3}$, complexité sous-exponentielle.

dernier record :

- RSA-768 $= pq$, p et q premiers.
- $\log(p) = \log(q) = 334$, soit 116 chiffres décimaux.

Décembre 2009

L'équipe CACAO (CARAMEL) de l'Inria et ses partenaires suisses, japonais, hollandais et allemands ont réussi à factoriser une clé RSA de 768 bits !

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3.

- 425 PC quadri-coeurs pendant un an.
- 5 Tera-octets.

Thorsten Kleinjung (1), Kazumaro Aoki (2), Jens Franke (3), Arjen K. Lenstra (1), Emmanuel Thomé (4), Joppe W. Bos (1), Pierrick Gaudry (4),Alexander Kruppa (4),Dag Arne Osvik (1), Peter. L. Montgomery (5,6), Herman te Riele (6), Andrey Timofeev (6), and Paul Zimmermann (4)

1 :EPFL ; 2 :NTT ; 3 :Bonn univ ; 4 :INRIA ; 5 :MS Research ; 6 :CWI

Factorisation quantique

fait

L'algorithme quantique de Shor factorise un entier de t bits en

$$\tilde{\mathrm{O}}(t^2) \quad \textit{étapes},$$

complexité polynomiale en temps (et porte quantique).

1996 *Polynomial-Time Algorithm for Prime Factorisation and Discrete Logarithm on a Quantum Computer*

dernier record ?

Factorisation quantique

fait

L'algorithme quantique de Shor factorise un entier de t bits en

$$\tilde{\mathrm{O}}(t^2) \quad \textit{étapes},$$

complexité polynomiale en temps (et porte quantique).

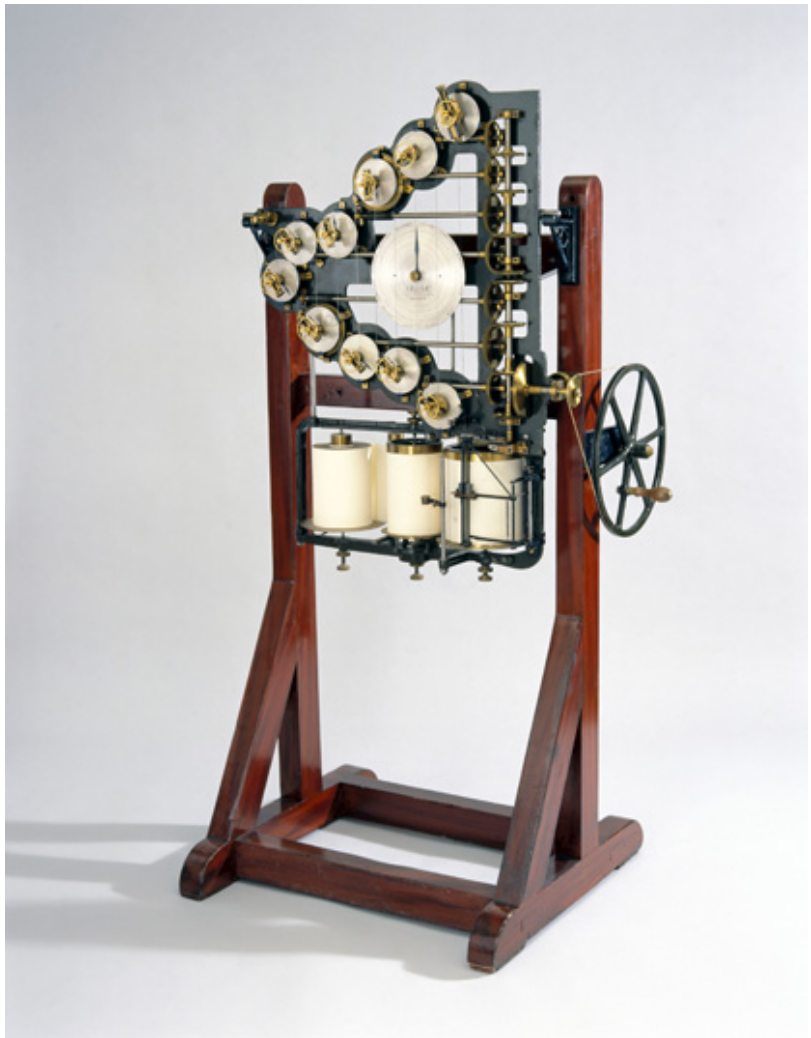
1996 *Polynomial-Time Algorithm for Prime Factorisation and Discrete Logarithm on a Quantum Computer*

dernier record ?

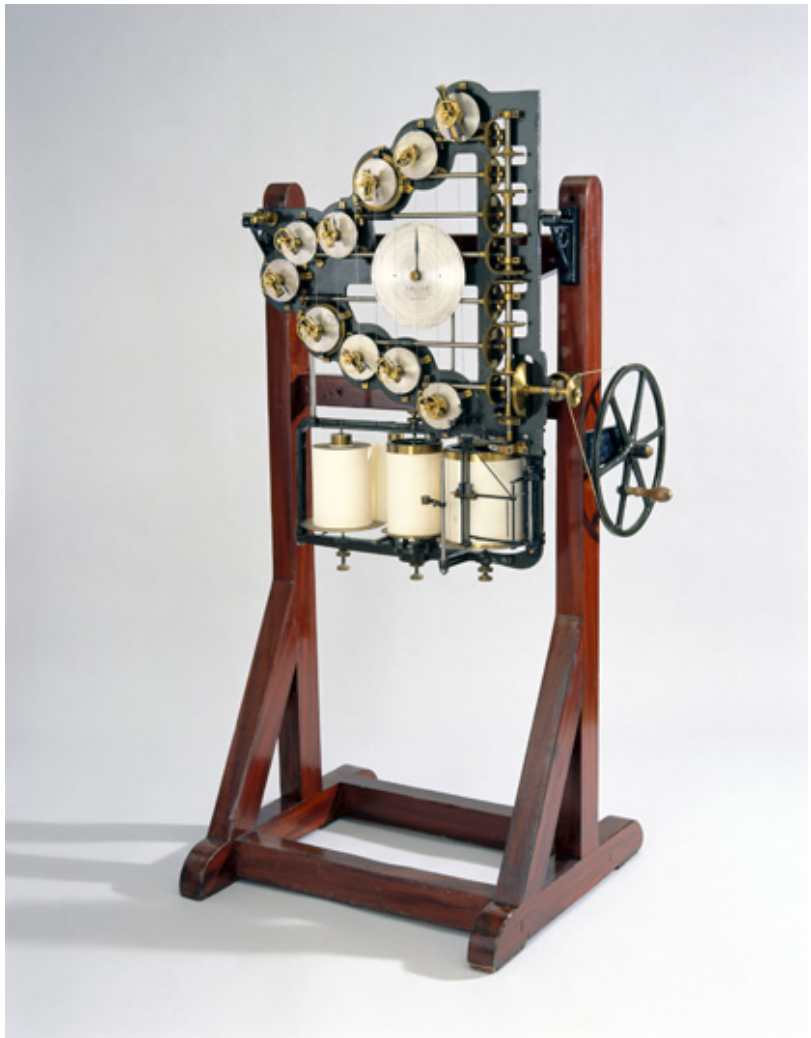
$$21 = 3 \times 7$$

Sommaire

Machine



Machine



La machine de Lord Kelvin.

Alan Turing Project

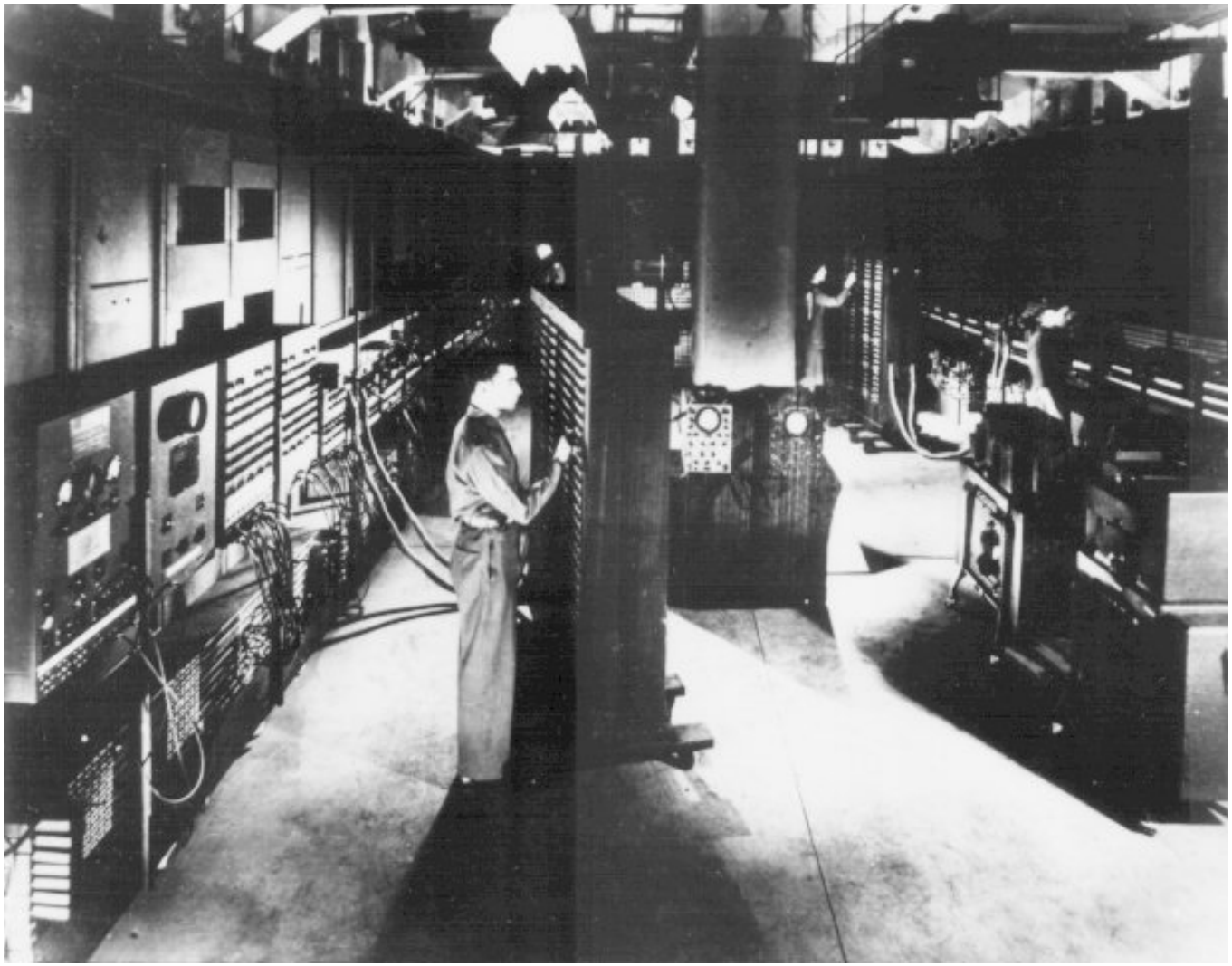
3. A. M. Turing.....£40.

King's College,
Cambridge.
24 *March* 1939.

"1. It is proposed to make calculations of the Riemann zeta-function on the critical line for $1{,}450 < t < 6{,}000$ with a view to discovering whether all the zeros of the function in this range of t lie on the critical line. An investigation for $0 < t < 1{,}464$ has already been made by Titchmarsh. The most laborious part of such calculations consists in the evaluation of certain trigonometrical sums

$$\sum_{r=1}^{m} \frac{1}{\sqrt{r}} \cos(t \log r - \vartheta) \qquad m = \left[\sqrt{\frac{t}{2\pi}}\right]$$

ENIAC



giant brain (1946) : 160 m2, 30 tonnes . . .

factorisation quantique

1980 une idée de Youri Manin

1982 Paul Benioff, Richard Feynman

1985 machine de Turing quantique, David Deutsch.

...

1994 algorithmes de Peter Shor.

...

2001 factorisation du nombre 15

2012 factorisation du nombre 21

Le calcul quantique adiabatique : 143, 56153

Sommaire

réduction algorithmique

factorisation de 21

- Détermination de période.

réduction algorithmique

factorisation de 21

- Détermination de période.

$$5^0 \quad 5^1 \quad 5^2 \quad 5^3 \quad 5^4 \quad 5^5 \quad 5^6 \quad 5^7$$

réduction algorithmique

factorisation de 21

- Détermination de période.

5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
1	5	25	125	625	3125	15625	78125

réduction algorithmique

factorisation de 21

- Détermination de période.

	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
	1	5	25	125	625	3125	15625	78125
mod 21	1	5	4	20	16	17	1	5

réduction algorithmique

factorisation de 21

- Détermination de période.

	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
	1	5	25	125	625	3125	15625	78125
mod 21	1	5	4	20	16	17	1	5

Théorème (Euler)

si $(x, n) = 1$ *alors l'ordre de* x *est un diviseur de* $\phi(n)$.

réduction algorithmique

factorisation de 21

- Détermination de période.

	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
	1	5	25	125	625	3125	15625	78125
mod 21	1	5	4	20	16	17	1	5

Théorème (Euler)

si $(x, n) = 1$ *alors l'ordre de* x *est un diviseur de* $\phi(n)$.

1. choisir x au hasard, x premier avec n.
2. calculer la période de $x^k \pmod n$
3. k est un diviseur de $\phi(n)$

racine de l'unité

fait

Si $N = pq$ alors l'équation

$$X^2 = 1 \mod N$$

possède 4 solutions : ± 1, plus deux non triviales.

racine de l'unité

fait

Si $N = pq$ alors l'équation

$$X^2 = 1 \mod N$$

possède 4 solutions : ± 1, plus deux non triviales.

$$y \neq \pm 1 \implies 0, N \neq \mathrm{pgcd}(y-1, N) \mid N$$

racine de l'unité

fait

Si $N = pq$ alors l'équation

$$X^2 = 1 \mod N$$

possède 4 solutions : ± 1, plus deux non triviales.

$$y \neq \pm 1 \implies 0, N \neq \mathrm{pgcd}(y-1, N) \mid N$$

fait

Si la période r de x est paire alors

$$y := x^{\frac{r}{2}} \implies y^2 = 1.$$

racine de l'unité

fait

Si $N = pq$ alors l'équation

$$X^2 = 1 \mod N$$

possède 4 solutions : ± 1, plus deux non triviales.

$$y \neq \pm 1 \implies 0, N \neq \mathrm{pgcd}(y-1, N) \mid N$$

fait

Si la période r de x est paire alors

$$y := x^{\frac{r}{2}} \implies y^2 = 1.$$

probabilité de succès > 0.25

facteurs de 21

	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
mod 21	1	5	4	20	16	17	1	5

facteurs de 21

	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
mod 21	1	5	4	20	16	17	1	5

$$5^6 = 1, \quad 5^3 - 1 = 19, \quad \mathrm{pgcd}(19, 21) = 1.$$

facteurs de 21

	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
mod 21	1	5	4	20	16	17	1	5

$$5^6 = 1, \quad 5^3 - 1 = 19, \quad \mathrm{pgcd}(19, 21) = 1.$$

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
mod 21	1	2	4	8	16	11	1	2

facteurs de 21

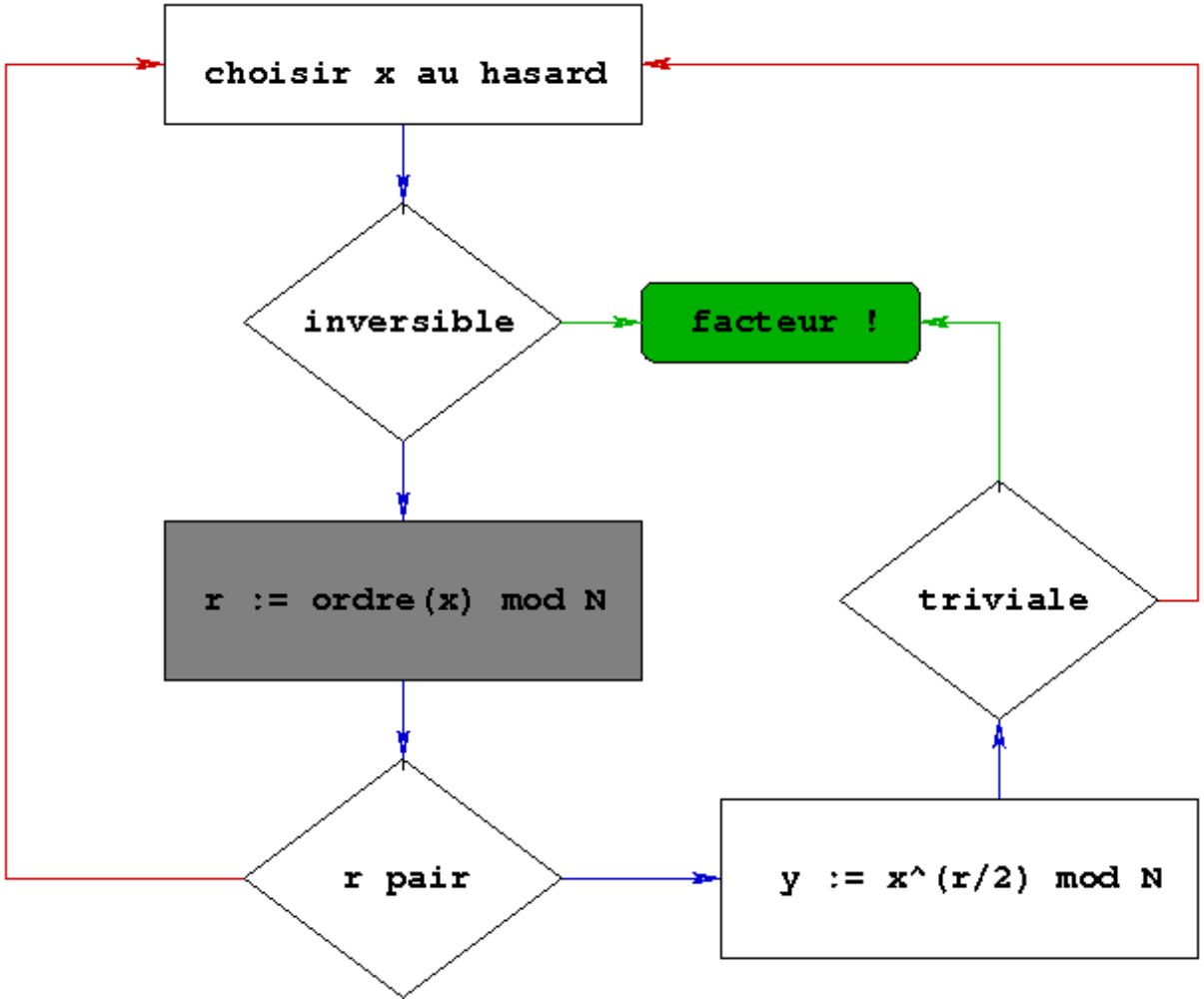
	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7
mod 21	1	5	4	20	16	17	1	5

$$5^6 = 1, \quad 5^3 - 1 = 19, \quad \text{pgcd}(19, 21) = 1.$$

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
mod 21	1	2	4	8	16	11	1	2

$$2^6 = 1, \quad 2^3 - 1 = 7, \quad \text{pgcd}(7, 21) = 7.$$

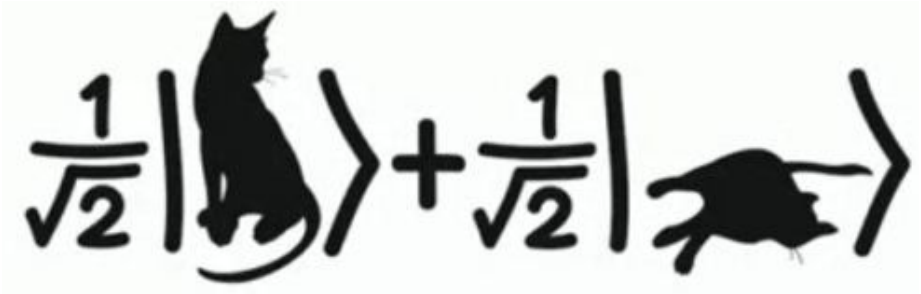
réduction



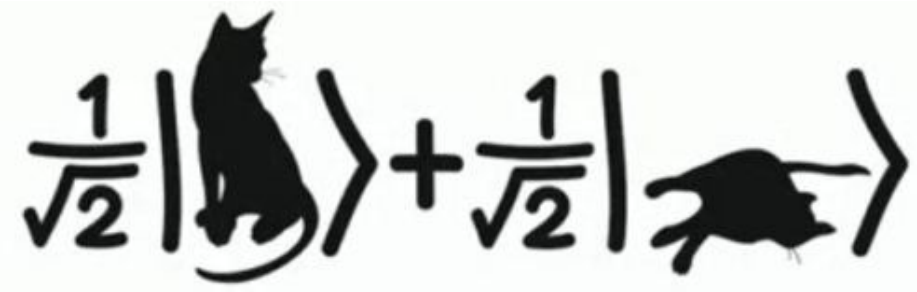
$$y^2 - 1 \equiv 0 \equiv (y-1)(y+1) \Longrightarrow \mathrm{pgcd}(y-1, n) \mid N$$

Sommaire

périphérique de calcul quantique



périphérique de calcul quantique



- superposition
- mesure
- évolution

superposition des états

On note $|1\rangle$, $|2\rangle$, ..., $|N\rangle$ une base orthonormale de $\mathbb{C}^N$.
Les $|i\rangle$ sont les états observables et tout vecteur de norme 1 représente un état quantique.

$$|\psi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle, \quad \sum_{i=1}^{N} |\alpha_i|^2 = 1.$$

- $|\psi\rangle$ est une superposition des $|i\rangle$.

mesure

On ne peut pas voir un état quantique mais on peut l'observer par une mesure

$$|\psi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle, \quad \sum_{i=1}^{N} |\alpha_i|^2 = 1.$$

"projette" $|\psi\rangle$ sur un des états $|j\rangle$.

$$\forall j, \quad |\alpha_j|^2 = \mathrm{Prob}(\mathrm{mes}(|\psi\rangle) \rightsquigarrow j)$$

- observation $\Longrightarrow$ modification
- projection orthogonale

Evolution

Les évolutions d'un système quantique sont décrites par des transformations unitaires i.e.

$$UU^\star = I, \quad U^{-1} = U^\star, \quad \text{matrice unitaire.}$$

- conservation des normes

Sommaire

qubit

Un bit quantique est un vecteur de norme 1 dans $\mathfrak{H} := \mathbb{C} \times \mathbb{C}$,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$

qubit

Un bit quantique est un vecteur de norme 1 dans $\mathfrak{H} := \mathbb{C} \times \mathbb{C}$,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Un registre de n-qubits est un vecteur de norme 1 dans $\mathfrak{H} \otimes \mathfrak{H} \otimes \cdots \otimes \mathfrak{H}$,

$$\begin{aligned} |\psi\rangle &= \sum_{x \in \{0,1\}^n} \alpha_x\,|x\rangle \\ &= \sum_{x=0}^{2^n-1} \alpha_x\,|x\rangle \end{aligned}$$

- Un registre de n-qubits superpose 2^n observables.
- Deux groupes d'ordre Q : $\mathbb{F}_2^m$, $\mathbb{Z}/Q\mathbb{Z}$.

Evolution du registre

$$(u, v) \mapsto (u + v) \mod Q, \quad (u, v) \mapsto u \oplus v, \qquad Q := 2^n.$$

Evolution du registre

$$(u, v) \mapsto (u + v) \mod Q, \quad (u, v) \mapsto u \oplus v, \qquad Q := 2^n.$$

La transformée de Fourier discrète

$$F : |y\rangle \mapsto \sum_{x=0}^{Q-1} \zeta_Q^{xy} |x\rangle, \quad \zeta_Q := \exp(2i\pi/Q)$$

Evolution du registre

$$(u, v) \mapsto (u + v) \mod Q, \quad (u, v) \mapsto u \oplus v, \qquad Q := 2^n.$$

La transformée de Fourier discrète

$$F\colon |y\rangle \mapsto \sum_{x=0}^{Q-1} \zeta_Q^{xy} |x\rangle, \quad \zeta_Q := \exp(2i\pi/Q)$$

La transformée de Fourier-Hadamard-Walsh

$$H\colon |y\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} (-1)^{x.y} |x\rangle$$

Evolution du registre

$$(u, v) \mapsto (u + v) \mod Q, \quad (u, v) \mapsto u \oplus v, \qquad Q := 2^n.$$

La transformée de Fourier discrète

$$F\colon |y\rangle \mapsto \sum_{x=0}^{Q-1} \zeta_Q^{xy} |x\rangle, \quad \zeta_Q := \exp(2i\pi/Q)$$

La transformée de Fourier-Hadamard-Walsh

$$H\colon |y\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} (-1)^{x.y} |x\rangle$$

en particulier

$$H|00\ldots0\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle$$

Sommaire

porte logique

NON

$$|0\rangle \mapsto |1\rangle, \quad |1\rangle \mapsto |0\rangle, \quad |x\rangle \mapsto |\bar{x}\rangle \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

XOR

$$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |x \oplus y\rangle$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

porte logique

NON

$$|0\rangle \mapsto |1\rangle, \quad |1\rangle \mapsto |0\rangle, \quad |x\rangle \mapsto |\bar{x}\rangle \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

XOR

$$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |x \oplus y\rangle$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad Px = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

porte logique

NON

$$|0\rangle \mapsto |1\rangle, \quad |1\rangle \mapsto |0\rangle, \qquad |x\rangle \mapsto |\bar{x}\rangle \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

XOR

$$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |x \oplus y\rangle$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad Px = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

- Hadamard, Pauli, changement de phase ...
- QFT : $O(n^2)$ portes quantiques.

Exponentiation modulaire

```
Exponentiation( x, t, n : nombre )
variable
        y : nombre
debut
      y ← 1
      tant que ( t > 0 )
          si impair( n ) alors
              y ← y * x mod n
          fsi
          t ← t div 2
          x ← x * x  mod n
      ftq
      retourner y
fin
```

exponentielle en parallèle ! ?

$$f(x) = y^x \mod N$$

Shor décrit une transformation unitaire E polynomiale qui envoie

$$E : |x\rangle |0\rangle \mapsto |x\rangle |f(x)\rangle$$

en particulier

$$\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |0\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle$$

Une observation révèle une des images de f

exponentielle en parallèle ! ?

$$f(x) = y^x \mod N$$

Shor décrit une transformation unitaire E polynomiale qui envoie

$$E : |x\rangle |0\rangle \mapsto |x\rangle |f(x)\rangle$$

en particulier

$$\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |0\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle$$

Une observation révèle une des images de f

mais détruit toutes les autres !

Sommaire

Algorithme de Shor

$$
\begin{array}{ccc}
|00\ldots0\rangle\,|00\ldots0\rangle & \xrightarrow{H} & \frac{1}{\sqrt{Q}}\sum_{n=0}^{Q-1}|n\rangle\,|00\ldots0\rangle \\
 & & \downarrow E \\
\frac{1}{Q}\sum_{n=0}^{Q-1}\sum_{s=0}^{Q-1}\zeta_Q^{ns}|s\rangle\,|x^n\rangle & \xleftarrow{F} & \frac{1}{\sqrt{Q}}\sum_{n=0}^{Q-1}|n\rangle\,|x^n \mod N\rangle \\
\downarrow \text{mes} & & \\
|s\rangle\,|y\rangle & \xrightarrow[\text{probabilité}]{} & |\frac{1}{Q}\sum_{x^n=y}\zeta_Q^{ns}|^2
\end{array}
$$

- $N^2 \leq Q < 2N^2$
- x d'ordre multiplicatif p.

La propabilité d'observer $|s\rangle\,|y\rangle$ est égale au carré du module de la somme :

$$\frac{1}{Q}\sum_{x^n=y}\zeta_Q^{ns}$$

Shor montre que si le reste minimal $\{ps\}_Q$ de la division de ps par Q vérifie

$$|\{ps\}_Q| \leq \frac{p}{2}$$

alors la probabilité de l'observable $|s\rangle\,|y\rangle$ est supérieure à $\frac{1}{3p^2}$.

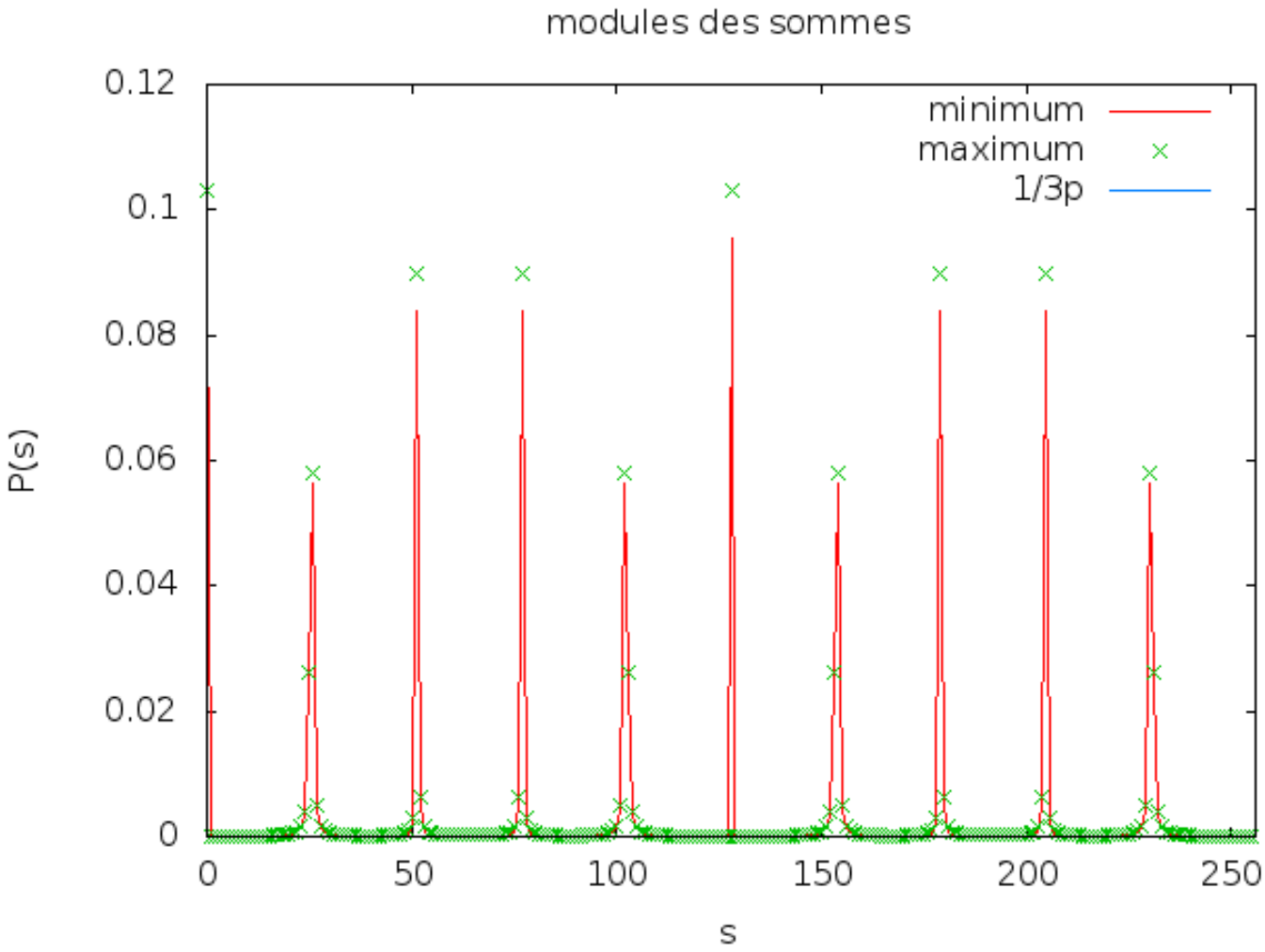


FIGURE : Modules des sommes partielles dans le cas $p = 10$ et $Q = 256$. Les pics se produisent quand $\{sp\}_Q$ est faible. Lorsque le reste minimal $\{ps\}_Q$ est inférieur à $p/2$ le module carré des sommes est minoré par $\frac{1}{3p^2}$

L'hypothèse $N^2 \leq Q < 2N^2$ montre qu'une seule fraction d/p vérifie :

$$0 < |\frac{s}{Q} - \frac{d}{p}| \leq \frac{1}{2Q}$$

Elle peut être déterminée en temps **polynomial** par une décomposition en fraction continue. Pour chaque entier d premier avec p, il existe au moins un s vérifiant

$$|\{ps\}_Q| \leq \frac{p}{2}$$

de sorte que la probabilité de déterminer la période de x est

$$P_{\text{succes}} \geq \frac{\varphi(p)p}{3p^2}$$

car pour chaque s, il y a p observables $|s\rangle |y\rangle$.

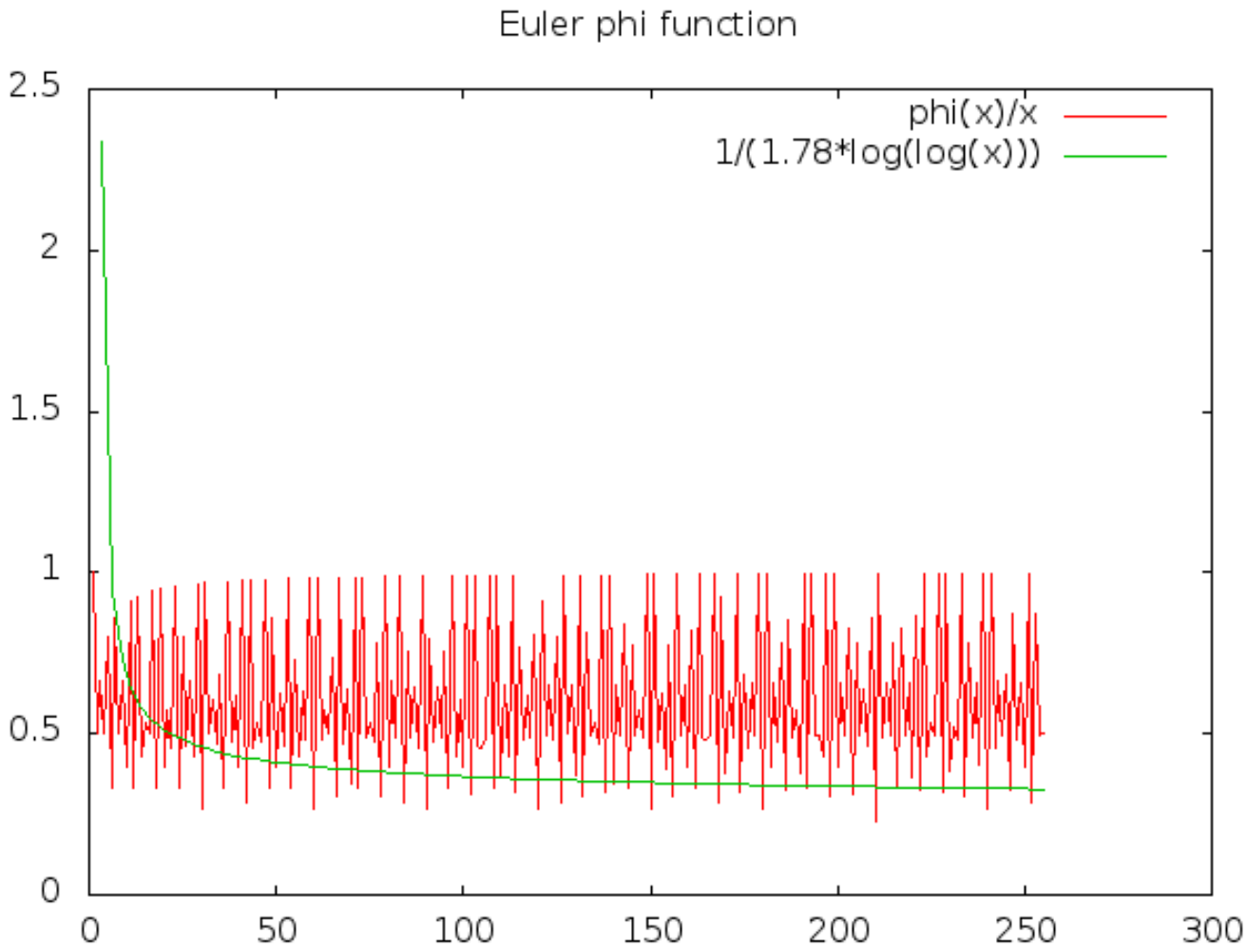


FIGURE : Dans Hardy et Wright, $\liminf \frac{\varphi(n)}{n} \log\log n = e^{-\gamma}$. où $\gamma = 0.577215665\ldots$ est la constante d'Euler. $e^{\gamma} = 1.7810724\ldots$.

On peut montrer que pour $n > 2$,

$$\frac{n}{e^{\gamma}\ \log\log n + \frac{3}{\log\log n}} \leq \varphi(n)$$

et pour une infinité de n :

$$\varphi(n) < \frac{n}{e^{\gamma} \log\log n}$$

$$P_{\text{succes}} \geq \frac{C}{\log\log p}$$

conclusion

On obtient p aprés $\log\log p$ tentatives.