Shor's Factoring Algorithm (Probabilistic algorithm)

No.
Date: / /

Input: $M = p \times q$. p, q 質數　　$a \perp b$: a, b 互質

Output: p, q

演算法:

1) 隨機選取 a, $a \perp M$,

2) 求 a 之 period: 最小 r, $a^r \equiv 1 \bmod M$.

且 (i) r 是偶數　　$(a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1) \equiv 0 \bmod M$

(ii) $a^{\frac{r}{2}}+1 \not\equiv 0 \bmod M$　　$M = p \cdot q \mid (a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1)$

3) $\begin{cases} p = (a^{\frac{r}{2}}+1, M) \\ q = (a^{\frac{r}{2}}-1, M) \end{cases}$　　$\Rightarrow \begin{cases} p \mid a^{\frac{r}{2}}+1 \\ q \mid a^{\frac{r}{2}}-1 \end{cases}$

Example $M = 35$

x	0	1	2	3	4	5	6	7	8
$13^x \bmod 35$	1	13	29	27	1	13	29	27	1

1) $a = 13$,

2) $r = 4$

(i) 偶數

(ii) $170 \not\equiv 0 \bmod 35$

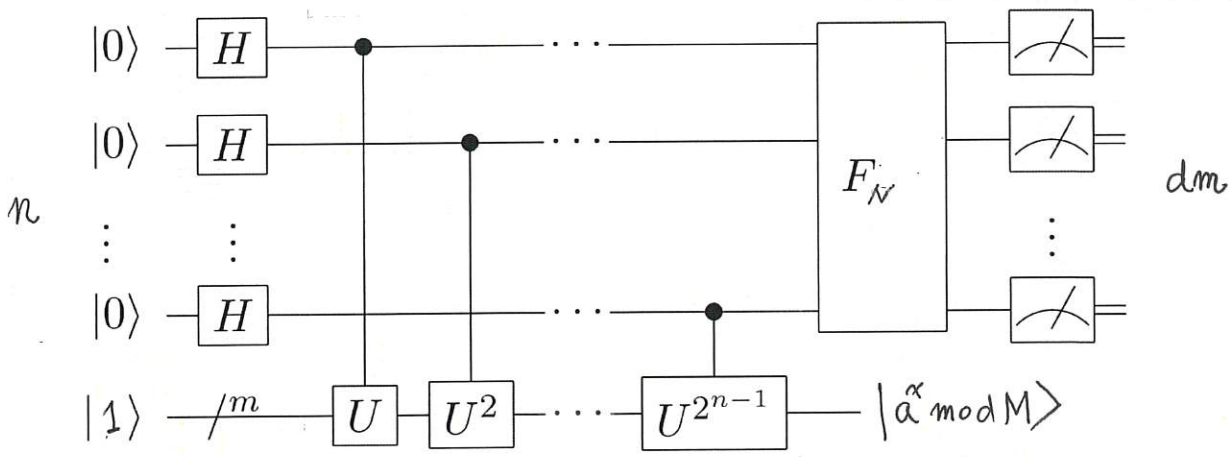
$(13^2+1)(13^2-1) \equiv 0 \bmod 35$

$170 \cdot 168 \equiv 0$ 〃

3) $\begin{cases} p = (170, 35) = 5 \\ q = (168, 35) = 7 \end{cases}$

Period Finding Algorithm

Given a, Find r. mod M,



$H^{\otimes n}$, $U_a: |x,1\rangle \rightarrow |x, a^x \bmod M\rangle$, QFT_N

$|x, f(x)\rangle$

說明:

$$|0^n, 1\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, 1\rangle \qquad N = 2^n$$

$$\xrightarrow{U_a} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle$$

$$\xrightarrow[\text{2nd reg.}]{\text{measure}} \frac{1}{\sqrt{m}} \sum_{x:\, f(x)=f(b)} |x, f(b)\rangle \,, \qquad a \le b < r, \quad m = \left\lfloor \frac{N}{r} \right\rfloor, \left\lceil \frac{N}{r} \right\rceil$$

$$= \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |rj+b\rangle \otimes |f(b)\rangle$$

$$\xrightarrow{QFT_N} \frac{1}{\sqrt{m}} \frac{1}{\sqrt{N}} \sum_{j=0}^{m-1} \sum_{k=0}^{N-1} \omega^{(rj+b)k} |k\rangle$$

$$= \frac{1}{\sqrt{m}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{bk} \sum_{j=0}^{m-1} \omega^{rjk} |k\rangle$$

$\sum_{j=0}^{m-1} \omega^{rjk}$: p_k : QFT 等比列

- $p_k = \frac{1}{\sqrt{m}} \frac{1}{\sqrt{N}} \omega^{bk} \sum_{j=0}^{m-1} \omega^{rjk} = \frac{1}{\sqrt{m}} \frac{1}{\sqrt{N}} \omega^{bk} \left(1 + \omega^{rk} + \omega^{2rk} + \cdots + \omega^{(m-1)rk}\right)$

$$= \begin{cases} \frac{1}{\sqrt{r}} \omega^{bk}, & r|N, \quad k = 0, m, 2m, \cdots, (r-1)m \qquad N = rm \\ \frac{1}{\sqrt{m}} \frac{1}{\sqrt{N}} \omega^{bk} \frac{1 - \omega^{mrk}}{1 - \omega^{rk}}, & r \nmid N \end{cases}$$

- $P_r(|k\rangle) = |p_k|^2 = \begin{cases} \frac{1}{r} & k = dm, \ d = 0, 1, \cdots, r-1, \quad r|N \\ \frac{1}{m \cdot n} \left| \frac{\sin \frac{mrk\pi}{N}}{\sin \frac{rk\pi}{N}} \right|^2 \ge \frac{4}{\pi^2}, & |k - dm| < \frac{1}{2}, \ (k \approx dm) \quad r \nmid N \end{cases}$

- $\frac{k}{N} = \frac{dm}{rm} = \frac{d}{r}$

$M=35,\ N=32,\ a=13$

(1) $H^{\otimes 5}$

x	0 1 2 3	4 5 6 7	8 9 ... 27	28 29 30 31
$13^x \bmod 35$	1 13 29 27	1 13 29 27	1 13 ... 27	1 13 29 27

$\begin{cases} r=4 \\ m=8 \end{cases} = \frac{N}{r}$ $(r \mid N)$

$$QFT_{32}=\left[\begin{array}{cccccc} & \overset{2}{\downarrow} & & \overset{6}{\downarrow} & \overset{10}{\downarrow} \cdots & \overset{30}{\downarrow} \\ \cdots & \omega^{2\cdot k} & \cdots & \omega^{6\cdot k} & \omega^{10k} \cdots & \omega^{30k} \cdots \end{array}\right] |k\rangle$$

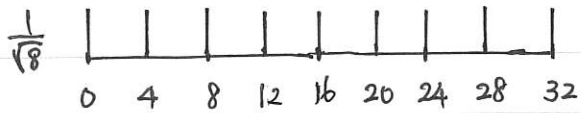
(2) U_a

$$\frac{1}{\sqrt{32}}\left(|0\rangle+|4\rangle+|8\rangle+\cdots+|28\rangle\right)\otimes|1\rangle$$
$$\left(|1\rangle+|5\rangle+|9\rangle+\cdots+|29\rangle\right)\otimes|13\rangle$$
$$\searrow \frac{1}{\sqrt{8}}\left(|2\rangle+|6\rangle+|10\rangle+\cdots+|30\rangle\right)\otimes|29\rangle$$
$$\left(|3\rangle+|7\rangle+|11\rangle+\cdots+|31\rangle\right)\otimes|27\rangle$$

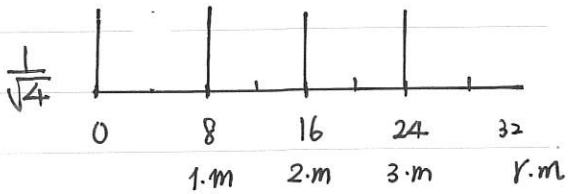
$\xrightarrow{QFT_{32}}$

(3)

$$\frac{1}{\sqrt{4}}\left(|0\rangle+|8\rangle+|16\rangle+|24\rangle\right)$$
$$\left(|0\rangle+\omega^{8}|8\rangle+\omega^{16}|16\rangle+\omega^{24}|24\rangle\right)$$
$$\left(|0\rangle+\omega^{2\cdot 8}|8\rangle+\omega^{2\cdot 16}|16\rangle+\omega^{2\cdot 24}|24\rangle\right)$$
$$\left(|0\rangle+\omega^{3\cdot 8}|8\rangle+\omega^{3\cdot 16}|16\rangle+\omega^{3\cdot 24}|24\rangle\right)$$



$r=4$
$m=8$



$$\frac{1}{\sqrt{8}}\sum_{j=0}^{7}|4j+b\rangle \xrightarrow{QFT_{32}} \frac{1}{\sqrt{8}}\frac{1}{\sqrt{32}}\sum_{j=0}^{7}\sum_{k=0}^{31}\omega^{(4j+b)k}|k\rangle \overset{?}{=} \frac{1}{\sqrt{4}}\left(|0\rangle+\omega^{b\cdot 8}|k\rangle+\omega^{b\cdot 16}|16\rangle+\omega^{b\cdot 24}|24\rangle\right)$$

$b=0,1,2,3$

$$=\frac{1}{\sqrt{8}}\frac{1}{\sqrt{32}}\sum_{k=0}^{31}\omega^{bk}\underbrace{\sum_{j=0}^{7}\omega^{4jk}}|k\rangle$$
$$=p_k$$

證明

$$p_k=\frac{1}{\sqrt{8}}\frac{1}{\sqrt{32}}\omega^{bk}\left(1+\omega^{4k}+\omega^{8k}+\cdots+\omega^{28k}\right)=\frac{1}{\sqrt{4}}\omega^{bk},\ (k=0,8,16,24)$$

$$Pr\left(|k\rangle\right)=|p_k|^2=\frac{1}{4},\ (k=0,8,16,24) \qquad (\Rightarrow |p_k|^2=0,\ 8\nmid k)$$

(i) $\searrow$ $k=24$, $\frac{k}{N}=\frac{dm}{rm}=\frac{d}{r}$ $\xrightarrow{d\perp r}$ $r=4$ (檢驗週期性)

$\frac{24}{32}=\frac{3}{4}$

$Pr=\Omega\left(\frac{1}{\log\log r}\right)$ 成功!

(ii) $\searrow$ $k=16$, $\frac{16}{32}=\frac{1}{2}$ 失敗!

重作 $O(\log\log r)$ 次

$O(\log\log M)$ "

定理[328, Hardy] $\varphi(r)=\Theta\left(\frac{r}{\log\log r}\right)$

$(0\le x<r$ $x\perp r$ 個數)

Continued Fraction (連分數)

{ 一種數的表示法
{ 最約分數去逼近一個數

連分數: $a_0 + \cfrac{1}{a_1 + \cfrac{1}{\vdots \; + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}} = [a_0, a_1, a_2, \cdots, a_n] = \frac{p_n}{q_n}$

定理 1 $\begin{cases} p_0 = a_0, & p_1 = a_1 a_0 + 1, & \cdots & p_n = a_n p_{n-1} + p_{n-2} \\ q_0 = 1, & q_1 = a_1, & & q_n = a_n q_{n-1} + q_{n-2} \end{cases}$

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

定理 2 (i) $\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = (-1)^{n-1} \Rightarrow (p_n, q_n) = 1$

(ii) $q_n \geq 2 q_{n-2}$ (exponentially)

定理 3 $\forall x \in \mathbb{R}$, $\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n^2} \Rightarrow \frac{p_n}{q_n}$ exists & provides good approximation.

Example $x = \frac{27}{32}$, $= [0, 1, 5, 2, 2]$

$x = 0 + \frac{27}{32} = 0 + \cfrac{1}{\frac{32}{27}}$ $\quad \frac{p_n}{q_n} = 0, 1, 5, 1, 1, 6,$

$= 0 + \cfrac{1}{1 + \frac{5}{27}}$ $\quad \left| \frac{27}{32} - \frac{5}{6} \right| < \frac{1}{6^2}$

$= 0 + \cfrac{1}{1 + \cfrac{1}{5 + \frac{2}{5}}}$ $\quad \left| \frac{81}{96} - \frac{80}{96} \right| < \frac{1}{36}$

$= 0 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2 + \frac{1}{2}}}}$

$\rightarrow \frac{d}{r} = \frac{5}{6}$

$M=35,\quad N=2^5=32,\quad a=9$

x	0 1 2 3 4 5	6 7 8	24 25 26 27 28 29	30 31
$9^x \bmod 35$	1 9 11 29 16 4	1 9 11	1 9 11 29 16 4	1 9

$\begin{cases} r=6 \\ m=\lfloor \frac{N}{r} \rfloor = 5,\ 6 \end{cases}$ $(r \nmid N)$

$$\frac{1}{\sqrt{32}}\Big[(|0\rangle+|6\rangle+|12\rangle+|18\rangle+|24\rangle+|30\rangle)\otimes|1\rangle + (|1\rangle+|7\rangle+|13\rangle+|19\rangle+|25\rangle+|31\rangle)\otimes|9\rangle + (|2\rangle+|8\rangle+|14\rangle+|20\rangle+|26\rangle)\otimes|11\rangle + (|3\rangle+|9\rangle+|15\rangle+|21\rangle+|27\rangle)\otimes|29\rangle + (|4\rangle+|10\rangle+|16\rangle+|22\rangle+|28\rangle)\otimes|16\rangle + (|5\rangle+|11\rangle+|17\rangle+|23\rangle+|29\rangle)\otimes|4\rangle\Big]$$

$$\to \frac{1}{\sqrt{6}}(|1\rangle+|7\rangle+|13\rangle+|19\rangle+|25\rangle+|31\rangle) \quad \frac{1}{\sqrt{m}}\sum_{j=0}^{m-1}|jr+b\rangle \quad \begin{matrix}1\\4\end{matrix}$$

$$\to \frac{1}{\sqrt{5}}(|4\rangle+|10\rangle+|16\rangle+|22\rangle+|28\rangle)$$

$$\xrightarrow{QFT_{32}} \frac{1}{\sqrt{5}}\frac{1}{\sqrt{32}}\sum_{j=0}^{4}\sum_{k=0}^{31}\omega^{(6j+4)k}|k\rangle$$

$$p_k = \frac{1}{\sqrt{5}}\frac{\omega^{4k}}{\sqrt{32}}\sum_{j=0}^{4}\omega^{6jk} = \frac{1}{\sqrt{5}}\frac{1}{\sqrt{32}}\omega^{4k}\left(1+\omega^{6k}+\omega^{12k}+\omega^{18k}+\omega^{24k}\right)$$

$$= \frac{1}{\sqrt{5}}\frac{1}{\sqrt{32}}\omega^{4k}\,\frac{1-\omega^{30k}}{1-\omega^{6k}}$$

$$\left|1-e^{2i\alpha}\right| = \left|1-\cos 2\alpha - i\sin 2\alpha\right| = |2\sin\alpha|$$

$$Pr(|k\rangle) = |p_k|^2 = \frac{1}{5}\frac{1}{32}\left|\frac{1-e^{\frac{2\pi i}{N}30k}}{1-e^{\frac{2\pi i}{N}6k}}\right|^2 = \frac{1}{5}\frac{1}{32}\left|\frac{\sin\frac{30k\pi}{N}}{\sin\frac{6k\pi}{N}}\right|^2$$

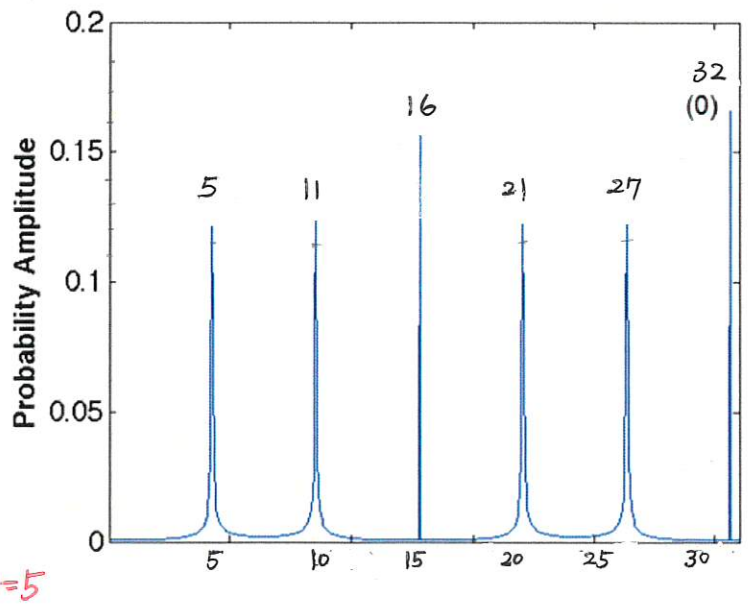
(i) $\to k=27$,

$$\frac{k}{N}=\frac{27}{32} \xrightarrow{\text{連分數}} \frac{d}{r}=\frac{5}{6}$$

(成功)

(ii) $\to k=16$

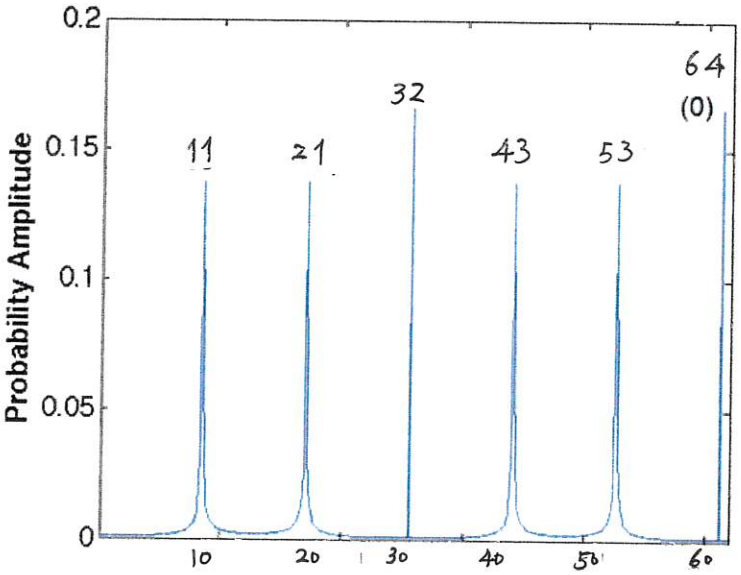
$$\frac{k}{N}=\frac{16}{32}=\frac{1}{2}$$



$m=5$

$$\frac{53}{64} = 0 + \frac{53}{64} = 0 + \frac{1}{1 + \frac{11}{53}} = 0 + \frac{1}{1 + \frac{1}{4 + \frac{9}{11}}} = 0 + \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{2}{9}}}} = 0 + \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}}}}$$

$N = 64 = 2^6$ $\begin{cases} r = 6 \\ m = 10 \end{cases}$



$[0, 1, 4, 1, 4, 2]$

$\frac{r}{d} = \begin{matrix} 0, & 1, & 4, & 5, \\ 1, & 1, & 5, & 6, \end{matrix}$

$\left|\frac{53}{64} - \frac{5}{6}\right| < \frac{1}{6^2}$

$\left|\frac{159}{192} - \frac{160}{192}\right| < \frac{1}{36}$

$\frac{53}{64} \rightarrow \frac{5}{6}$

$N = 512 = 2^9$, $\begin{cases} r = 6 \\ m = 85 \end{cases}$

$\frac{427}{512} = [0, 1, 5, 42, 2]$

$\frac{d}{r} = \begin{matrix} 0, & 1, & 5, \\ 0, & 1, & 6 \end{matrix}$

$\rightarrow \frac{5}{6}$