Peter Shor's Factoring Algorithm

by

Samuel J. Lomonaco, Jr.

Dept. of Comp. Sci. & Electr. Engr.
University of Maryland Baltimore County
1000 Hilltop Circle
Baltimore, MD 21250
Email: Lomonaco@UMBC.EDU
WebPage: http://www/csee.umbc.edu/~lomonaco

0

A Cryptanalyst's Dream

Crack RSA by finding a superfast factoring algorithm.

Problem. Given an integer N which is the product of two unknown primes p & q, i.e., $N = pq$, find p and q, i.e., factor N.

Shor's Algorithm (Cont.)

$\mathbb{N} = \{0, 1, 2, \ldots\}$ Natural Numbers

<u>Problem</u>. Given a periodic function

$$f: \mathbb{N} \longrightarrow \mathbb{N}$$

find period P of f

> <u>Choose</u> a suff. large positive integer Q. Restrict f to
>
> $$S_Q = \{0, 1, 2, \ldots, Q-1\}$$
>
> Hence, $f: S_Q \longrightarrow \mathbb{N}$

<u>Simplification</u>. To avoid minor technicalities, we assume that Q is a multiple of P, i.e.,

$$P \mid Q$$

Shor's Algorithm (Cont.)

- Choose integer n s.t. $\begin{cases} Q < 2^n \\ Max(f) < 2^n \end{cases}$

- Construct two n-qubit registers, i.e., reg1 and reg2.

$$|reg1\rangle |reg2\rangle = |a_{n-1} a_{n-2} \ldots a_0\rangle |b_{n-1} b_{n-2} \ldots b_0\rangle$$

arguments of f

Values of f

<u>Convention</u>:

Represents this integer

$$|a_{n-1} a_{n-2} \ldots a_0\rangle = \left|\sum_{j=0}^{2^n - 1} a_j 2^j\right\rangle$$

For example,

$$|10111\rangle = |23\rangle$$

Shor's Algorithm (Cont.)

$$
\begin{aligned}
|\text{Reg1}\rangle\,|\text{Reg2}\rangle &= \sum_{x=0}^{Q-1} |x\rangle\,|f(x)\rangle \\
&= \sum_{x_0=0}^{P-1} \sum_{x_1=0}^{\frac{Q}{P}-1} |Px_1 + x_0\rangle\,|f\,(Px_1 + x_0)\rangle \\
&= \sum_{x_0=0}^{P-1} \sum_{x_1=0}^{\frac{Q}{P}-1} |Px_1 + x_0\rangle\,|f\,(x_0)\rangle \\
&= \sum_{x_0=0}^{P-1} \left(\sum_{x_1=0}^{\frac{Q}{P}-1} |Px_1 + x_0\rangle \right) |f\,(x_0)\rangle
\end{aligned}
$$

Shor's Algorithm (Cont.)

$$
|\text{Reg1}\rangle\,|\text{Reg2}\rangle = \sum_{x_0=0}^{P-1} \left(\sum_{x_1=0}^{\frac{Q}{P}-1} |Px_1 + x_0\rangle \right) |f\,(x_0
$$

Step 3. Measure Reg2.

$j_0 \in \{0, 1, 2, \ldots, P-1\}$

$\text{Prob}(x_0 = j_0) = \frac{1}{P}$

Whoosh

$$
|\text{Reg1}\rangle\,|\text{Reg2}\rangle = \sum_{x_1=0}^{\frac{Q}{P}-1} |Px_1 + j_0\rangle\,|f\,(j_0)\rangle
$$

$$|\mathrm{Reg1}\rangle\,|\mathrm{Reg2}\rangle = \sum_{\lambda=0}^{P-1} \omega^{j_0 \lambda \frac{Q}{P}} \left|\lambda \tfrac{Q}{P}\right\rangle |f(j_0)\rangle$$

Step 5. Measure Reg1.

$\lambda_0 \in \{0, 1, 2, \ldots, P-1\}$

$\text{Prob}(\lambda = \lambda_0) = \frac{1}{P}$

Whoosh ∇_0

$$|\mathrm{Reg1}\rangle\,|\mathrm{Reg2}\rangle = \left|\lambda_0 \tfrac{Q}{P}\right\rangle |f(j_0)\rangle$$

Hence, we have obtained $\lambda_0 \left(\frac{Q}{P}\right)$ for some

$$\lambda_o \in \{0, 1, \ldots, P-1\}$$

Repeat steps 1 thru 5 until we have obtained a large enough subset

$$\mathcal{S} \subset \left\{ \lambda \frac{Q}{P} \;\middle|\; \lambda = 0, 1, \ldots, P-1 \right\}$$

to determine $\frac{Q}{P}$, and hence P.

Note. $\frac{Q}{P}$ is obtained from $\mathcal{S}$ by using a continued fraction expansion.

Where $\phi(P)$ denotes

Euler's totient function,

i.e., where

$$\boxed{\phi(P) = \{n \in \mathbb{Z} \mid 0 < n < P \text{ and } \gcd(n, P) = 1\}}$$

Reminder. The integer Q was chosen s.t.

$$\boxed{N^2 \le Q = 2^L < 2N^2}$$

Observation

$Prob(y)$ is really a prob. distribution on the additive cyclic group

$$\boxed{\mathbb{Z}_Q = \left(\tfrac{1}{Q}\mathbb{Z}\right)/\mathbb{Z} = \left\{\tfrac{0}{Q}, \tfrac{1}{Q}, \tfrac{2}{Q}, \ldots, \tfrac{Q-1}{Q}\right\} \bmod 1},$$

which we call the **probing quotient group**.

If a $\frac{y}{Q}$ is selected from $\mathbb{Z}_Q$ according to Shor's prob. distribution, then the prob. is high $\left(\ge \frac{4}{\pi^2}\frac{\phi(P)}{P}\right)$ that it is "close" to an element of the additive cyclic group

$$\boxed{\mathbb{Z}_P = \left(\tfrac{1}{P}\mathbb{Z}\right)/\mathbb{Z} = \left\{\tfrac{0}{P}, \tfrac{1}{P}, \tfrac{2}{P}, \ldots, \tfrac{P-1}{P}\right\} \bmod 1},$$

which we call the **hidden quotient group**.

Two Norms on the Unit Circle

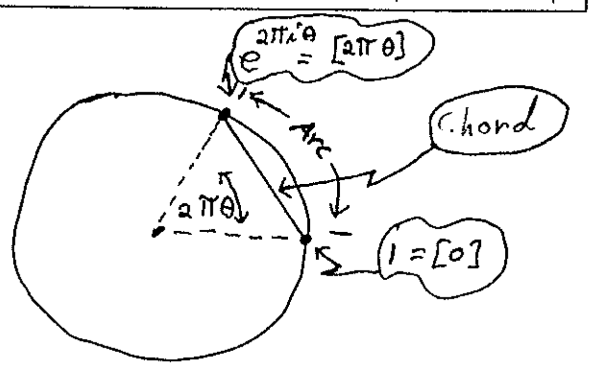
Arclength Norm

$$\boxed{\text{Arc}(2\pi\theta) = 2\pi\,(\theta \bmod 1) = (2\pi\theta) \bmod 2\pi}$$

where $\boxed{\theta \bmod 1}$ is the unique residue of magnitude $\le \frac{1}{2}$, and where $\boxed{(2\pi\theta) \bmod 2\pi}$ is the unique residue of magnitude $\le \pi$.

Chordal Norm

$$\boxed{\text{Chord}(2\pi\theta) = 2\,|\sin(\pi\theta)| = \left|e^{2\pi i\theta} - 1\right|}$$



What Properties do these Norms Have?

Def. A **norm** on a group G is a map

$$\|-\| : G \times G \longrightarrow \mathbf{R}$$

such that

1) $\|g\| = 0$ iff $g = \begin{cases} 1 & \text{Mult. Notation} \\ 0 & \text{Additive Notation} \end{cases}$

2) $\|g\| \geq 0$ for all $g \in G$

3) $\begin{cases} \|g_1 \cdot g_2\| \leq \|g_1\| + \|g_2\| & \text{Mult. Notation} \\ \text{or} & \\ \|g_1 + g_2\| \leq \|g_1\| + \|g_2\| & \text{Additive Notation} \end{cases}$

Choose an integer

$$\boxed{Q = 2^L}$$

such that

$$\boxed{N^2 \le Q < 2N^2}$$

Moreover, let ω be a primitive Q-th root of unity, e.g.,

$$\boxed{\omega = e^{2\pi i \frac{1}{Q}}}$$

Creating Shor's Prob. Distr.

Shor finds y as follows:

$\boxed{\text{STEP 2.0}}$ Initialize registers 1 and 2, i.e.,

$$|\psi_0\rangle = |\text{Reg1}\rangle\,|\text{Reg2}\rangle = |0\rangle\,|1\rangle = |00\cdots 00\rangle\,|00\cdots 01\rangle$$

$\boxed{\text{STEP 2.1}}$ Apply Fourier transf. F to Reg1.

$$|\psi_0\rangle = |0\rangle\,|1\rangle \xrightarrow{\mathcal{F}\otimes I} |\psi_1\rangle\,. = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|1\rangle$$

$\boxed{\text{STEP 2.2}}$ Apply $U_f : |x\rangle\,|0\rangle \longmapsto |x\rangle\,|0\rangle$

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|1\rangle \overset{U_f}{\longmapsto} |\psi_2\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|f(x)\rangle$$

The **sole** purpose of executing STEPS 2.1 to 2.4 was to create the classical probability distribution on the set

$$\{0, 1, 2, \ldots, Q-1\}$$

given by

$$Prob(y) = \frac{\langle \Upsilon(y) \mid \Upsilon(y) \rangle}{Q^2} ,$$

where

$$|\Upsilon(y)\rangle = \sum_{x=0}^{Q-1} \omega^{xy} \, |f(x)\rangle = \sum_{x=0}^{Q-1} e^{\frac{2\pi i}{Q} xy} \, |f(x)\rangle$$

$$\boxed{\text{But what is } Prob(y) \text{ ?}}$$

$$\boxed{\text{But what is } Prob(y) \text{ ?}}$$

Recall

$$|\Upsilon(y)\rangle = \sum_{x=0}^{Q-1} \omega^{xy} \, |f(x)\rangle$$

Let

$$\begin{cases} Q = Pq + r \ , & 0 \leq r < P \\ x = Px_1 + x_0 \ , & 0 \leq x_0 < P \end{cases}$$

Hence,

$$|\Upsilon(y)\rangle = \sum_{x_0=0}^{P-1} \omega^{x_0 y} \left(\sum_{x_1=0}^{q-1+\delta(x_0)} \omega^{Px_1 y} \right) |f(x_0)\rangle \ ,$$

where

$$\delta(x_0) = \begin{cases} 1 & \text{if } x_0 < r \\ 0 & \text{otherwise} \end{cases}$$

$$\boxed{Prob\,(y) = \frac{1}{Q^2}\sum_{x_0=0}^{P-1}\frac{\text{Chord}^2\left(2\pi\frac{Py}{Q}[q+\delta(x_0)]\right)}{\text{Chord}^2\left(2\pi\frac{Py}{Q}\right)}}$$

But ...

$$\boxed{\text{Arc}(2\pi\theta) \geq \text{Chord}(2\pi\theta) \geq \frac{2}{\pi}\text{Arc}(2\pi\theta)}$$

Hence,

$$\boxed{Prob\,(y) \geq \frac{4}{\pi^2}\frac{1}{Q^2}\sum_{x_0=0}^{P-1}\frac{\text{Arc}^2\left(2\pi\frac{Py}{Q}[q+\delta(x_0)]\right)}{\text{Arc}^2\left(2\pi\frac{Py}{Q}\right)}}$$

$$\boxed{Prob\,(y) \geq \frac{4}{\pi^2}\frac{1}{Q^2}\sum_{x_0=0}^{P-1}\frac{\text{Arc}^2\left(2\pi\frac{Py}{Q}[q+\delta(x_0)]\right)}{\text{Arc}^2\left(2\pi\frac{Py}{Q}\right)}}$$

Lemma.

If $\frac{y}{Q}$ is suff. "close" to a rational of the form $\frac{d}{P}$, i.e., if

$$\boxed{\text{Arc}\left(2\pi\frac{y}{Q} - 2\pi\frac{d}{P}\right) \leq \frac{\pi}{Q}\left(1 - \frac{P}{Q}\right)}$$

then

$$\boxed{\text{Arc}\left(2\pi\frac{Py}{Q}\right) \leq \frac{\pi}{q+\delta(x_0)}}$$

Also, we know that

$$\boxed{\text{Arc}(2\pi\theta) \leq \frac{\pi}{|n|} \Longrightarrow \text{Arc}(2\pi n\theta) = |n|\text{Arc}(2\pi\theta)}$$

Recall

$$\boxed{Q = Pq + r, \qquad 0 \leq r < P}$$

Problem

Even if $\frac{y}{Q}$ is sufficiently close to $\frac{d}{P}$, the period P can **only** be recovered from y if

$$\boxed{\gcd(d, P) = 1}$$

The probability that this happens is

$$\boxed{\frac{\phi(P)}{P}},$$

where $\phi(P)$ is Euler's totient function, defined by

$$\boxed{\phi(P) = \#\{0 < u < P \mid \gcd(d, P) = 1\}}$$

Theorem. The probability that the $\frac{y}{Q}$ produced is "sufficiently close" to a rational of the form $\frac{d}{P}$ s.t. $\gcd(d, P) = 1$ is bounded below by

$$\boxed{\frac{4}{\pi^2}\frac{\phi(P)}{P}\left(1 - \frac{P}{Q}\right)^2 \gtrsim \frac{4}{\pi^2}\frac{1}{e^\gamma \ln 2}\frac{1}{\lg\lg N} = \Omega\left(\frac{1}{\lg\lg N}\right)},$$

where γ denotes Euler's constant

Second Part of Shor's Algorithm

Given a

$$0 < \frac{y}{Q} < 1$$

that is **"close"** to a rational of the form

$$0 < \frac{d}{P} < 1 \text{ (with } \gcd(d, P) = 1) ,$$

i.e., such that

$$\left|\frac{y}{Q} - \frac{d}{P}\right| \le \frac{1}{2Q}\left(1 - \frac{P}{Q}\right) ,$$

how do we find the period P ?

Theorem. If

$$\left|\frac{y}{Q} - \frac{d}{P}\right| \le \frac{1}{2P^2} ,$$

then $\frac{d}{P}$ is a **convergent** $\frac{p_k}{q_k}$ of the **continued fraction expansion** of $\frac{y}{Q}$.

Continued Fractions: Example

$$\xi = \frac{212}{97} = 2+\frac{18}{97} = 2+\frac{1}{\left(\frac{97}{18}\right)}$$

$$= 2+\frac{1}{5+\frac{7}{18}} = 2+\frac{1}{5+\frac{1}{\left(\frac{18}{7}\right)}}$$

$$= 2+\frac{1}{5+\frac{1}{2+\frac{4}{7}}} = 2+\frac{1}{5+\frac{1}{2+\frac{1}{\left(\frac{7}{4}\right)}}}$$

$$= 2+\frac{1}{5+\frac{1}{2+\frac{1}{1+\frac{3}{4}}}} = 2+\frac{1}{5+\frac{1}{2+\frac{1}{1+\frac{1}{\left(\frac{4}{3}\right)}}}}$$

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

But What is a Convergent of a Continued Fraction ?

Definition. The k-th **convergent** of a continued fraction

$$[a_0, a_1, \ldots, a_N]$$

is defined as

$$\frac{p_k}{q_k} = [a_0, a_1, \ldots, a_k] \ ,$$

where p_k and q_k are **relatively prime,** and are given by the recursion

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2}, \\ q_n = a_n q_{n-1} + q_{n-2} \ . \end{cases}$$

and

$$\begin{cases} p_0 = a_0, \quad p_1 = a_1 a_0 + 1, \\ q_0 = 1, \quad q_1 = a_1, \end{cases}$$

Why Continued Fractions?

Answer. They tell us how closely a real number can be approximated by rational numbers.

Theorem. Let ξ be a positive real number, and let d and P be integers with $P > 0$. If

$$\left|\xi - \frac{d}{P}\right| \leq \frac{1}{2P^2},$$

then

$$\frac{d}{P}$$

is a *convergent* of the continued fraction expansion of ξ. In other words, there exists an integer k such that

$$\frac{d}{P} = \frac{p_k}{q_k}$$