Continued fraction

r: the order of x' modulo N'.
We are given

$$x = 0.b_1 b_2 \dots b_t$$

that is close to s/r with high probability. The remaining task is to compute r from $b_1 b_2 \dots b_t$. r can be determined by the continued fraction algorithm.

A continued fraction is

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_N}}}}, \tag{1}$$

where $a_1, \dots, a_N$ are positive integers and $a_0 \geq 0$.
Denote the value of Eq. (1) by $[a_0, a_1, \dots, a_N]$.
The representation of a continued fraction of rational x can be found, for example, as follows:

$$\begin{aligned} & \frac{31}{13} \\ = \; & 2 + \frac{5}{13} \\ = \; & 2 + \frac{1}{\frac{13}{5}} \end{aligned}$$

2009-11-1

$$
\begin{aligned}
&= 2 + \frac{1}{2 + \frac{3}{5}} \\
&= 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}} \\
&= 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} \\
&= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}} \\
&= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}
\end{aligned}
$$

Recall that we have to find r from

$$x = 0.b_1 b_2 \ldots b_t$$

such that x is close to s/r. We have the following theorem.

Theorem 1: Let $[a_0, \ldots, a_N]$ be the continued fraction of x. If $|x - s/r| < \frac{1}{2r^2}$ and $\gcd(s, r) = 1$, then s/r is equal to $[a_0, \ldots, a_n]$ for some $0 \leq n \leq N$.

We can make $|x - s/r| < \frac{1}{2r^2}$ by increasing t (the number of qubits used for phase estimation). If we execute the order finding several times, we will eventually have $\gcd(s, r) = 1$. If we assume Theorem 1, the factorization can be found as follows: Compute the continued fraction of x as $[a_0, \ldots, a_N]$. For each $0 \leq n \leq N$, write $[a_0, \ldots, a_n]$ as p_n/q_n and check whether q_n satisfies that $(x')^{q_n} \bmod N' = 1$ and $(x')^{q_n/2} \pm 1$ is a factor of N'. If it is the case, we found a factor of N'. Otherwise, try again.

Thus, if we assume Theorem 1, then what we have to do is to check the speed (required computational time) of continued fraction computation.

Cost of continued fraction

Theorem 2: Let $[a_0, \ldots, a_N]$ be the continued fraction of rational $x > 1$. Define $p_0 = a_0$, $q_0 = 1$, $p_1 = 1 + a_0 a_1$, $q_1 = a_1$,

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

Then we have

$$\frac{p_n}{q_n} = [a_0, \ldots, a_n]$$

for $n = 0, \ldots, N$.

From the above theorem we can evaluate the required number of computational steps. Observe that $p_n > p_{n-1}$ and $q_n > q_{n-1}$. So we have $p_n \geq 2p_{n-2}$ and $q_n \geq 2q_{n-2}$. If $x = p/q > 1$ then $N \leq \log_2 p$.

Proof of Theorem 1

Theorem 1: Let $[a_0, \ldots, a_N]$ be the continued fraction of x. If $|x - s/r| < \frac{1}{2r^2}$ and $\gcd(s, r) = 1$, then s/r is equal to $[a_1, \ldots, a_i]$ for some $0 \leq i \leq N$.
Proof (almost the same as the textbook): Let $[a_0, \ldots, a_n]$ be the continured fraction of s/r, also define (as in Theorem 2)

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

Notice that $s = p_n$ and $r = q_n$. Define δ by

$$x = \frac{p_n}{q_n} + \frac{\delta}{2q_n^2}.$$

The assumption in the theorem implies $|\delta| < 1$. Also define λ by

$$\lambda = 2\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta}\right) - \frac{q_{n-1}}{q_n}.$$

This definitiion of λ implies

$$x = \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}}.$$

2009-11-5

To see this equality, substituting the definition of λ gives

$$\begin{aligned} & \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}} \\ = & \frac{\left[2\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta}\right) - \frac{q_{n-1}}{q_n}\right] p_n + p_{n-1}}{\left[2\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta}\right) - \frac{q_{n-1}}{q_n}\right] q_n + q_{n-1}} \\ = & \frac{p_n}{q_n} + \frac{\delta}{2q_n^2}. \end{aligned}$$

The last equality can be verified by a tedious computation.

We can assume that n is even, because if n is odd then $[a_0, \ldots, a_n] = [a_0, \ldots, a_n - 1, 1]$.

Theorem 3: For $n \geq 1$ we have $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$.

Proof can be done by induction on n.

By using Theorem 3 on the definition of λ

$$\lambda = 2\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta}\right) - \frac{q_{n-1}}{q_n}.$$

we get

$$\begin{aligned} \lambda &= \frac{2(-1)^n}{\delta} - \frac{q_{n-1}}{q_n} \\ &= \frac{2}{\delta} - \frac{q_{n-1}}{q_n} \\ &> 2 - 1 = 1. \end{aligned}$$

By Theorem 2 and the definition of λ, we see that

$$x = [a_0, \ldots, a_n, \lambda].$$

Since λ is a rational number > 1, it has the continued fraction $[b_0, \ldots, b_m]$. Therefore, $x = [a_0, \ldots, a_n, b_0, \ldots, b_m]$. Theorem 1 has been proved.

Exercise

Submit your answer to the box in front of Room 311, S3 building, by 17:00 Thursday, if you don't finish by 12:10.

Let $N' = 15$, $x' = 7$, and $x = 0.110001$.

1. Compute the continued fraction of x.

2. Let $[a_0, \ldots, a_N]$ be the continued fraction of x. Detemine the index n such that q_n is the order of x' modulo N', where $p_n/q_n = [a_0, \ldots, a_n]$.

3. If your answers to the previous exercises were evaluated as incorrect, please indicate whether or not you agree to that evaluation. Write which part in today's lecture was difficult for your understanding.