ELEN 162
A. I. Zecevic

Lecture Notes for Week 7

The Order Finding Problem

Finding the prime factors of a large number is closely related to the so-called *order finding problem*. This problem is of particular interest to us because conventional computers cannot solve it in a reasonable amount of time, but quantum computers can. In view of that, we will now explain what is meant by "order finding", and describe a quantum algorithm that can accomplish this task efficiently (we will establish a connection between order finding and prime factorization in our next lecture).

We begin our discussion with the following definition.

Definition 1. Suppose that x and N are positive integers with no common factors. We will say that r is the *order of x modulo N* if it represents the smallest integer that satisfies

$$x^r = 1 \pmod{N} \tag{1}$$

In order to explain how one can compute r for a given choice of x and N, we will need the following two preliminary results.

Lemma 6.1. If r is the order of x modulo N, then $r < N$.

Lemma 6.2. Let r be the order of x modulo N, and let k and j be two distinct positive integers that are smaller than r. Then,

$$x^k \bmod N \neq x^j \bmod N \tag{2}$$

The proofs of both lemmas are quite straightforward, and are provided in the texbook.

Order Finding and Eigenvalue Estimation

The quantum algorithm for order finding relies to a large extent on the eigenvalue estimation method that we previously examined. To get a sense for how this algorithm works, let us assume that we have n qubits at our disposal, and that the standard basis for the resulting n-particle system has the usual form $\{\Psi_0, \Psi_1, \ldots, \Psi_{2^n-1}\}$. Given a pair of co-prime integers x and N, we will now define a new set of functions $\{\Phi_0, \Phi_1, \ldots, \Phi_{r-1}\}$, which can be described as

$$\Phi_s = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} \Psi_{x^k \bmod N} \tag{3}$$

In this expression, r denotes the order of x modulo N, and s is an integer that can take values $\{0, 1, \ldots, r-1\}$.

Remark 1. It is important to keep in mind that there is no direct relationship between n and N. In this context, n represents the number of qubits in the system while N defines the order of x.

Our next step will be to define an operator $\hat{U}_x$ which transforms a basis function Ψ_y as

$$\hat{U}_x \Psi_y = \Psi_{xy \bmod N} \tag{4}$$

This is equivalent to saying that

$$\hat{U}_x \Psi_y = \Psi_z \tag{5}$$

where z is the remainder that is obtained when xy is divided by N. As we saw previously, this remainder must satisfy $0 \leq z < N$ by definition.

Operator $\hat{U}_x$ is of interest to us because $\{\Phi_0, \Phi_1, \ldots, \Phi_{r-1}\}$ happen to be *its eigenfunctions* (this is not difficult to show - a proof is provided in the textbook). It can also be shown that the eigenvalue which correspond to function Φ_s has the form $\lambda_s = e^{\frac{2\pi i s}{r}} = e^{2\pi i \omega_s}$. This means (among other things) that we can directly apply the quantum eigenvalue estimation algorithm to compute the first τ bits of $\omega_s = s/r$ for any s such that $0 \leq s \leq r-1$. As before, we will denote this approximation by $\bar{\omega}_s$.

Some Practical Considerations

Since r appears in the denominator of ω_s, our objective in the following will be to find a way to extract this information from $\bar{\omega}_s$. Prior to doing that, however, we need to adress two practical problems that arise in this context.

The first one has to do with the fact that eigenfunctions

$$\Phi_s = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} \Psi_{x^k \bmod N} \tag{6}$$

are *unknown*, since they depend on r (and r is the number that we want to compute). As a result, we cannot use them as the input to the quantum circuit shown in Fig. 1. It turns out, however, that this is not an insurmountable problem, since basis function Ψ_1 (which is readily available) satisfies

$$\Psi_1 = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \Phi_s \tag{7}$$

This is not difficult to show, and a proof is provided in the textbook.

Given that this is the case, what will the output of our quantum circuit look like if we use Ψ_1 as the input instead of Φ_s? When we previously discussed this scenario (in the context of the eigenvalue estimation algorithm), we established that the output will have the general form

$$\Psi_{\text{out}} = \sum_{s=0}^{r-1} \alpha_s [(\psi_{m_1^{(s)}} \otimes \psi_{m_2^{(s)}} \otimes \ldots \otimes \psi_{m_n^{(s)}}) \otimes \Phi_s] \tag{8}$$

where indices $\{m_1^{(s)}, m_2^{(s)}, \ldots, m_n^{(s)}\}$ correspond to

$$\bar{\omega}_s = 0.m_1^{(s)} m_2^{(s)} \ldots m_n^{(s)} \tag{9}$$

(which matches the first τ bits ω_s).

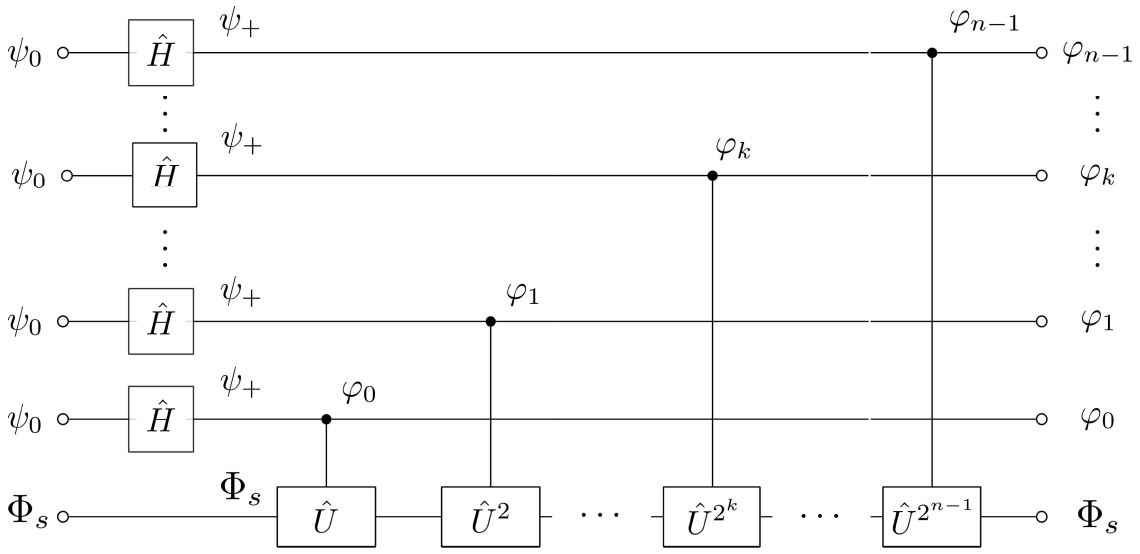

Figure 1: The first step of eigenvalue estimation.

In this particular case, coefficients α_s have the form

$$\alpha_s = \frac{1}{\sqrt{r}} \tag{10}$$

which means that all possible outcomes have the *same* probability

$$|\alpha_s|^2 = \frac{1}{r} \tag{11}$$

As a result, the most that we can say about the measured state is that it will correspond to one of the eigenvalues $\lambda_s = e^{2\pi i \omega_s}$ of operator $\hat{U}_x$. Recalling that s can take values $s = 0, 1, \ldots, r-1$ and that $\omega_s = s/r$, this is equivalent to saying that the computed value $\bar{\omega}_s = 0.m_1^{(s)} m_2^{(s)} \ldots m_n^{(s)}$ will approximate a *randomly chosen* number from the set

$$\Gamma(r) = \left\{ \frac{1}{r}, \frac{2}{r}, \ldots, \frac{r-1}{r} \right\} \tag{12}$$

Although this introduces a certain amount of ambiguity into the process, we should point out that it does not pose a significant challenge, since all elements of set (12) have the *same* denominator (and r happens to be the number that we are interested in). We will see shortly how this number can be computed once $\bar{\omega}_s$ is known.

The second issue that we must resolve has to do with the procedure for estimating eigenvalues, which requires that we replace Φ_s with Ψ_1 in Fig. 1, and then evaluate functions of the form $\hat{U}_x^{2^j}(\Psi_1)$ for $j = 0, 1, \ldots, n-1$. On first glance, this appears to be a major obstacle, since we must apply operator $\hat{U}_x$ as many as 2^{n-1} times to function Ψ_1. Fortunately, there is an elegant way around this potential bottleneck, which relies on the following simple lemma.

Lemma 6.3. Let $\hat{U}_x$ be the operator defined in expression (4), and let Ψ_y be a function that belongs to the standard basis $\{\Psi_0, \Psi_1, \ldots, \Psi_{2^n-1}\}$. Then,

$$\hat{U}_x^k(\Psi_y) = \hat{U}_{x^k \bmod N}(\Psi_y) \tag{13}$$

This lemma is useful because it demonstrates that forming function $\hat{U}_x^{2^j}(\Psi_y)$ does *not* require 2^j successive applications of operator $\hat{U}_x$, and that we can achieve the same objective by applying operator $\hat{U}_{x^{2^j} \bmod N}$ to Ψ_y *once*. This simplifies matters greatly, since operators $\hat{U}_{x^{2^j} \bmod N}$ $(j = 0, 1, \ldots, n-1)$ are not difficult to implement. To see why this is so, it suffices to observe that $x^{2^j} \bmod N$ are numbers that take values from set $\{0, 1, \ldots, N-1\}$. Consequently, applying $\hat{U}_x^{2^j}$ to function Ψ_y entails evaluating $w = x^{2^j} \bmod N$, and subsequently computing $\hat{U}_w(\Psi_y)$.

The following example illustrates how this computation is performed.

Example 1. Suppose that $x = 5$ and $N = 21$. If we assume that our quantum computer has $n = 30$ qubits, the eigenvalue estimation procedure will require applying operators $\{\hat{U}_5, \hat{U}_5^2, \ldots, \hat{U}_5^{2^{29}}\}$ to function Ψ_1. The highest of these powers is 2^{29}, which is obviously a very large number. Fortunately, Lemma 6.3 ensures that

$$\hat{U}_5^{2^{29}}(\Psi_1) = \hat{U}_{5^{2^{29}} \bmod 21}(\Psi_1) \tag{14}$$

so all we need to do is compute

$$w = 5^{2^{29}} \bmod 21 \tag{15}$$

In order to evaluate expression (16), we will make use of the fact that

$$x^{m \cdot k} \bmod N = [x^m \bmod N]^k \bmod N \tag{16}$$

(which is a result that we already encountered in the context of RSA encryption). Since 2^{29} is too large to input directly into a calculator, we will break the procedure down into 3 steps.

STEP 1

$$\begin{aligned} &5^{2^{29}} \bmod 21 = 5^{2^8 \cdot 2^{21}} \bmod 21 = 5^{256 \cdot 2^{21}} \bmod 21 = \left[5^{256} \bmod 21\right]^{2^{21}} \bmod 21 = \\ &= 16^{2^{21}} \bmod 21 = 16^{2^7 \cdot 2^{14}} \bmod 21 \end{aligned} \tag{17}$$

STEP 2

$$\begin{aligned} &16^{2^7 \cdot 2^{14}} \bmod 21 = 16^{128 \cdot 2^{14}} \bmod 21 = \left[16^{128} \bmod 21\right]^{2^{14}} \bmod 21 = \\ &= 4^{2^{14}} \bmod 21 = 4^{2^7 \cdot 2^7} \bmod 21 = 4^{128 \cdot 128} \bmod 21 \end{aligned} \tag{18}$$

STEP 3

$$\begin{aligned} &4^{128 \cdot 128} \bmod 21 = \left[4^{128} \bmod 21\right]^{128} \bmod 21 = \\ &= 16^{128} \bmod 21 = 4 \end{aligned} \tag{19}$$

Having established that

$$5^{2^{29}} \bmod 21 = 4 \tag{20}$$

we now obtain

$$\hat{U}_5^{2^{29}}(\Psi_1) = \hat{U}_{5^{2^{29}} \bmod 21}(\Psi_1) = \hat{U}_4(\Psi_1) \tag{21}$$

which is easily implemented.

Remark 2. In evaluating expressions (17), (18) and (19), we relied on the fact that numbers such as $5^{256} \bmod 21$, $16^{128} \bmod 21$ and $4^{128} \bmod 21$ can be computed using standard modular exponentiation calculators.

Extracting r Using Continued Fractions

Since the algorithm that we just described approximates a random element of set $\Gamma(r)$ defined in (12), we need to consider how this information can be used to compute r. The most effective way to do that is based on the so-called *continued fraction method*, which we will now explain.

To see how this approach works, suppose that x is a rational number, and that we would like to represent it using a sequence of successive approximations p_n/q_n $(n = 0, 1, \ldots, m)$. The fractions p_n/q_n that appear in this iterative process are know as *convergents*, and we will assume that they can be expressed as *continued fractions* whose coefficients are integers $[a_0\ a_1\ ...\ a_n]$. The following example illustrates what this means.

Example 2. Let $x = 500/97$ be a rational number that we would like to approximate by a sequence of continued fractions. As a first step, we can rewrite x as

$$x = 5 + \frac{15}{97} \tag{22}$$

If we retain only the integer part, our initial approximation of x becomes

$$x^{(0)} = 5 = a_0 \tag{23}$$

If we now express (22) as

$$x = 5 + \frac{1}{\frac{97}{15}} = 5 + \frac{1}{6 + \frac{7}{15}} \tag{24}$$

and once again retain only the integer part, we obtain a more accurate approximation of x which has the form

$$x^{(1)} = 5 + \frac{1}{6} \equiv a_0 + \frac{1}{a_1} \tag{25}$$

Since such an expression is uniquely defined by a_0 and a_1, it is usually described by the pair $[\,a_0\ \ a_1\,]$ (which is $[\,5\ \ 6\,]$ in this case).

In the next step, we have

$$x = 5 + \frac{1}{6 + \frac{7}{15}} = 5 + \frac{1}{6 + \frac{1}{\frac{15}{7}}} = 5 + \frac{1}{6 + \frac{1}{2 + \frac{1}{7}}} \tag{26}$$

which allows us to approximate x as

$$x^{(2)} = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = 5 + \frac{1}{6 + \frac{1}{2}} \tag{27}$$

Observing that expression (27) involves three integers, we can equivalently represent it as $x^{(2)} = [\,a_0\ \ a_1\ \ a_2\,] = [\,5\ \ 6\ \ 2\,]$.

Note that the final step in this process requires no further computation, since (26) already has the desired form

$$x = x^{(3)} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}} \tag{28}$$

All that we have to do at this point is recognize that $a_3 = 7$, and that x can be precisely described as $x = x^{(3)} = [\, a_0 \;\; a_1 \;\; a_2 \;\; a_3 \,] = [\, 5 \;\; 6 \;\; 2 \;\; 7 \,]$.

In order to specify the sequence of convergents that are obtained using this method, we need to represent $x^{(0)}$, $x^{(1)}$, $x^{(2)}$ and $x^{(3)}$ as fractions. We can do this by evaluating expressions (23), (25), (27) and (28), which produce

$$\begin{aligned} x^{(0)} &= \frac{p_0}{q_0} = \frac{5}{1} \\ x^{(1)} &= \frac{p_1}{q_1} = \frac{31}{6} \\ x^{(2)} &= \frac{p_2}{q_2} = \frac{67}{13} \\ x^{(3)} &= \frac{p_3}{q_3} = \frac{500}{97} \end{aligned} \tag{29}$$

It is not difficult to see that each successive convergent represents a better approximation of x, and that the last one matches it *precisely*.

Remark 3. It is important to recognize that the continued fraction method actually produces *two* valid results

$$\frac{p_k}{q_k} = a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}} \tag{30}$$

and

$$\frac{p_k}{q_k} = a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{(a_k - 1) + \cfrac{1}{1}}}} \tag{31}$$

This "ambiguity" is advantageous, since it allows us to choose whether x should be represented by an even or odd number of terms in the expansion.

Computing a sequence of rational approximations like the one in (29) can become quite cumbersome in practice, particularly if the number of iterations is large. To see why this is so, we should observe that x is always initially approximated as

$$\frac{p_0}{q_0} = a_0 \tag{32}$$

(which implies that $p_0 = a_0$ and $q_0 = 1$). In the next step, we have an approximation of the form $[\, a_0 \;\; a_1 \,]$, which represents a continued fraction that is made up of *two* coefficients. In

this case, the convergent has the form

$$\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \tag{33}$$

so p_1 and q_1 are related to a_0 and a_1 as

$$\begin{aligned} p_1 &= a_0 a_1 + 1 \\ q_1 &= a_1 \end{aligned} \tag{34}$$

In the third step, we have a continued fraction that is defined by *three* coefficients $[\, a_0 \;\; a_1 \;\; a_2 \,]$. This allows us to approximate x as

$$\frac{p_2}{q_2} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0(a_1 a_2 + 1) + a_2}{a_1 a_2 + 1} \tag{35}$$

and express p_2 and q_2 as

$$p_2 = a_0 a_1 a_2 + a_0 + a_2 \tag{36}$$

and

$$q_2 = a_1 a_2 + 1 \tag{37}$$

We could obviously continue this procedure beyond the third step, but deriving analytic expressions for p_k and q_k becomes increasingly harder as set $\{a_i\}$ grows in size. The following theorem shows, however, that there is a way around this problem, and that convergents can be computed *recursively* for $k > 2$.

Theorem 6.1. Let $\{a_0, a_1, \ldots, a_n\}$ be a given set of positive integers, and let us define p_0, p_1, q_0 and q_1 as

$$\begin{aligned} p_0 &= a_0 \\ q_0 &= 1 \\ p_1 &= a_0 a_1 + 1 \\ q_1 &= a_1 \end{aligned} \tag{38}$$

Suppose further that continued fraction expansions defined by coefficients $[\, a_0 \;\; a_1 \;\; \ldots \;\; a_{n-2} \,]$ and $[\, a_0 \;\; a_1 \;\; \ldots \;\; a_{n-1} \,]$ correspond to p_{n-2}/q_{n-2} and p_{n-1}/q_{n-1}, respectively. The continued fraction expansion $[\, a_0 \;\; a_1 \;\; \ldots \;\; a_n \,]$ can then be expressed as p_n/q_n, where

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \\ q_n &= a_n q_{n-1} + q_{n-2} \end{aligned} \tag{39}$$

The following example illustrates how Theorem 6.1 can help us compute p_k and q_k efficiently in cases when x is given in decimal form, and more than three iterations are needed.

Example 3. Suppose that we would like to represent $x = 0.150537634$ as a sequence of fractions. Since $x < 1$ in this case, our initial approximation will obviously be

$$x^{(0)} = 0 = a_0 \tag{40}$$

Our next step will be to take the reciprocal of 0.150537634, and represent x as

$$x = 0 + \frac{1}{6.6428} = 0 + \frac{1}{6 + 0.6428} \tag{41}$$

From this expression, we can easily deduce that $a_1 = 6$.

Before we proceed to identify p_1 and q_1, we should say a few words about the precision that this process requires. In principle, it is always desirable to retain *as many decimals as possible* when computing continued fractions. We will do so in each iteration, but will display only the first 4 decimals of the result (for the sake of simplicity).

Because rounding is unavoidable, in each step we will also monitor the approximation error, which is defined as

$$\varepsilon^{(k)} = \left| x^{(k)} - x \right| = \left| \frac{p_k}{q_k} - x \right| \tag{42}$$

This will allow us to precisely distinguish between very small errors, and $\varepsilon^{(k)} = 0$ (which is the point when the algorithm terminates).

With that in mind, let us now return to expression (41), which allows us to approximate x as

$$x^{(1)} = a_0 + \frac{1}{a_1} = 0 + \frac{1}{6} \tag{43}$$

This tells us that $p_1 = 1$ and $q_1 = 6$, and the error after the first step becomes

$$\varepsilon^{(1)} = \left| x^{(1)} - x \right| = \left| \frac{p_1}{q_1} - x \right| = \left| \frac{1}{6} - x \right| = 0.01613 \tag{44}$$

To find the next convergent, we should observe that

$$x = 0 + \frac{1}{6 + 0.6428} = 0 + \frac{1}{6 + \dfrac{1}{1.5555}} = 0 + \frac{1}{6 + \dfrac{1}{1 + 0.5555}} \tag{45}$$

If we retain only the integers, we obtain

$$x^{(2)} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = 0 + \frac{1}{6 + \dfrac{1}{1}} \;=\; \frac{1}{7} \tag{46}$$

from which we can conclude that $a_2 = 1$, $p_2 = 1$ and $q_2 = 7$. The corresponding error is easily computed as

$$\varepsilon^{(2)} = \left| x^{(2)} - x \right| = \left| \frac{p_2}{q_2} - x \right| = \left| \frac{1}{7} - x \right| = 0.00768 \tag{47}$$

From this point on, we can use expression (39) to calculate p_k and q_k recursively. In order to do that, it will suffice to focus only on the *last* number that was computed in the continued fraction expansion. The coefficients a_k, p_k and q_k that are obtained in this manner are shown below.

Iteration 3

Since the denominator of the last term in (45) is

$$1 + 0.5555 = 1 + \frac{1}{1.8000} = \frac{1}{1 + 0.8000} \tag{48}$$

it follows that $a_3 = 1$, and that

$$\begin{aligned} p_3 &= a_3 p_2 + p_1 = 2 \\ q_3 &= a_3 q_2 + q_1 = 13 \end{aligned} \tag{49}$$

The error after this step will therefore be

$$\varepsilon^{(3)} = \left| x^{(3)} - x \right| = \left| \frac{p_3}{q_3} - x \right| = \left| \frac{2}{13} - x \right| = 0.00330852 \tag{50}$$

Iteration 4

If we rewrite the denomonator of (48) as

$$1 + 0.8000 = 1 + \frac{1}{1.25} = 1 + \frac{1}{1 + 0.25} \tag{51}$$

we obtain $a_4 = 1$ and

$$\begin{aligned} p_4 &= a_4 p_3 + p_2 = 3 \\ q_4 &= a_4 q_3 + q_2 = 20 \end{aligned} \tag{52}$$

The error after this step is

$$\varepsilon^{(4)} = \left| x^{(4)} - x \right| = \left| \frac{p_4}{q_4} - x \right| = \left| \frac{3}{20} - x \right| = 5.37634 \cdot 10^{-4} \tag{53}$$

Iteration 5

Since expression

$$1 + 0.25 = 1 + \frac{1}{4} \tag{54}$$

produces an integer in the denominator, we know that this will be the final step in the process. Given that $a_5 = 4$ in this case, we obtain

$$\begin{aligned} p_5 &= a_5 p_4 + p_3 = 14 \\ q_5 &= a_5 q_4 + q_3 = 93 \end{aligned} \tag{55}$$

and the approximation error is

$$\varepsilon^{(5)} = \left| x^{(5)} - x \right| = \left| \frac{p_5}{q_5} - x \right| = \left| \frac{14}{93} - x \right| = 0 \tag{56}$$

Since the error is zero, the continued fraction expansion is now complete, and has the form

$$x^{(5)} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5}}}}} = 0 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}}} \tag{57}$$

Having found all the coefficients p_k and q_k, we can easily compute the sequence of convergents that approximate x as

$$\begin{aligned} x^{(0)} &= \frac{p_0}{q_0} = 0 \\ x^{(1)} &= \frac{p_1}{q_1} = \frac{1}{6} \\ x^{(2)} &= \frac{p_2}{q_2} = \frac{1}{7} \\ x^{(3)} &= \frac{p_3}{q_3} = \frac{2}{13} \\ x^{(4)} &= \frac{p_4}{q_4} = \frac{3}{20} \\ x^{(5)} &= \frac{p_5}{q_5} = \frac{14}{93} \end{aligned} \tag{58}$$

As in Example 2, this sequence produces a successively better approximation of x in each step, and the final convergent matches it *exactly*.

The Final Step

We are now ready to apply continued fractions to the order finding problem. In order to do that, we will need the following theorem.

Theorem 6.2. Suppose that x is a rational number, and that fraction p/q approximates it in such a way that inequality

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{2q^2} \tag{59}$$

holds. Then, p/q represents a convergent in the continued fraction expansion of x.

To see how this result can help us solve the order finding problem, we first need to decide how many bits of ω_s we want to compute. For reasons that will become apparent shortly, we will set $\tau = 2L + 1$, where L represents the first integer that is *greater than or equal to* $\log_2 N$ (this number is usually denoted as $L = [\log_2 N]$). Given our choice of τ, we now need to determine the number of qubits that are needed to obtain such an approximation.

As we saw in our earlier discussions, n would have to satisfy

$$n \geq \tau + \log_2(2 + \frac{1}{2\varepsilon}) \tag{60}$$

in order to ensure this level of precision with probability $1 - \varepsilon$. If this condition is met, the error of our approximation can be bounded as

$$|\bar{\omega}_s - \omega_s| = \left| \bar{\omega}_s - \frac{s}{r} \right| \leq 2^{-\tau} = 2^{-2L-1} \tag{61}$$

(since we chose to match the first τ bits of ω_s).

Observing that

$$2^{-2L-1} = \frac{1}{2(2^L)^2} \tag{62}$$

and recalling that Lemma 6.1 implies

$$r < N = 2^{\log_2 N} \leq 2^L \tag{63}$$

it follows that

$$\frac{1}{2(2^L)^2} < \frac{1}{2r^2} \tag{64}$$

As a result, we have that

$$\left|\bar{\omega}_s - \frac{s}{r}\right| \leq 2^{-2L-1} < \frac{1}{2r^2} \tag{65}$$

which means that condition (59) in Theorem 6.2 is satisfied. From this, we can conclude that choosing $\tau = 2L + 1$ guarantees that s/r *will be a convergent* in the continued fraction expansion of $\bar{\omega}_s$.

This result allows us to compute r *precisely* by following the procedure described in Example 3 (note that $\bar{\omega}_s$ is certain to be a rational number, because the algorithm for eigenvalue estimation always produces an approximation with a finite number of bits). Since s/r is a convergent in the expansion of $\bar{\omega}_s$, we know that expression

$$\frac{p_k}{q_k} = \frac{s}{r} \tag{66}$$

will hold for some k. For this particular k, the integer q_k in the denominator will equal r, which represents the order of x modulo N. In view of that, we can say that solving the order finding problem amounts to checking whether $x^{q_k} - 1$ is divisible by N for $k = 0, 1, 2, \ldots$, and identifying the first number q_k that satisfies this condition.

Prime Factorization and Order Finding

In order to explain how the order finding problem relates to prime factorization, we first need to introduce two important concepts - *Euler's φ function*, and the notion of a *cyclic group*. We begin with the following definition.

Definition 2. Euler's function $\varphi(n)$ represents the number of positive integers that are *smaller* than n and are *co-prime* with it.

To get a sense for what this function looks like, it is helpful to observe that

$$\varphi(p) = p - 1 \tag{67}$$

for any prime number $p > 1$. It is not difficult to see why this is so, since p (being a prime number) is not divisible by any number other than itself. Consequently, *every* number that is smaller than p must be co-prime with it. Note that this includes 1 as well, since 1 is co-prime with every number by definition (in other words, $\gcd(p, 1) = 1$ for any choice of p).

The situation is somewhat more complicated when it comes to numbers like p^α, where p is prime and $\alpha > 1$. In such cases, the Euler function cannot be evaluated by inspection, since p^α is divisible by p, p^2, ... , $p^{\alpha-1}$. It is not difficult to show, however, that

$$\varphi(p^\alpha) = p^{\alpha-1}(p - 1) \tag{68}$$

which is something that we will use extensively in our discussion of cyclic groups.

We now provide two theorems which will help us describe another important property of function $\varphi(n)$. The first of them (which is know as Fermat's Little Theorem) is a fundamental result in number theory which dates back to the 17th century.

Theorem 5.7. (Fermat's Little Theorem). Let $p > 1$ be a prime number, and assume that a is an arbitrary integer. Then,

$$a^p = a \pmod{p} \tag{69}$$

If a is co-prime with p, we also have that

$$a^{p-1} = 1 \pmod{p} \tag{70}$$

Although this result is restricted to exponents that are prime numbers, it turns out that expression (70) can be generalized to a broader class of integers. The following theorem show how that can be done using function $\varphi(n)$.

Theorem 5.8. Suppose that a and n are co-prime. Then,

$$a^{\varphi(n)} = 1 \pmod{n} \tag{71}$$

A Brief Overview of Group Theory

The notion of a cyclic group is a bit more complicated to explain, and requires a brief review of group theory. In general, a group can be thought of as a mathematical object that consists of a set $G = \{g_1, \ldots, g_n\}$ and an operation denoted "$\circ$" which is defined on its elements. This operation must have the following four properties.

Property 1 (Closure). Any two elements of G satisfy

$$g_i \circ g_j \in G \tag{72}$$

Property 2 (Associativity). Any three elements of G satisfy

$$(g_i \circ g_j) \circ g_k = g_i \circ (g_j \circ g_k) \tag{73}$$

Property 3 (Identity Element). There exists an element $e \in G$ such that

$$g_i \circ e = g_i \tag{74}$$

for any $g_i \in G$.

Property 4 (Inverse Element). For any $g_i \in G$ there exists an element $g_i^{-1} \in G$ such that

$$g_i \circ g_i^{-1} = e \tag{75}$$

The following example illustrates how these properties can be interpreted.

Example 4. Let G denote the set of all integers, and let "$\circ$" represent standard addition. We will now show that this set constitutes a group by verifying that each of the four properties described in equations (72) - (75) holds.

Property 1. If $a \in G$ and $b \in G$, it is obvious that

$$a + b \in G \tag{76}$$

since the sum of two integers is an integer.

Property 2. For any three integers a, b and c

$$(a + b) + c = a + (b + c) \tag{77}$$

holds true, since integers can be added in any order.

Property 3. The identity element in G is 0, since

$$a + 0 = a \tag{78}$$

for any integer a (note that 0 is considered to be an integer as well).

Property 4. The inverse of $a \in G$ is $-a$, because

$$a + (-a) = 0 \tag{79}$$

Since a is an integer, so is $-a$.

The group that we will be most interested in is denoted by Z_n^*, and consists of all positive integers that are *smaller than* n and are *co-prime with it*. For any pair of elements $a, b \in Z_n^*$, operation "$\circ$" is defined as

$$a \circ b = ab \bmod n \tag{80}$$

(which amounts to modular multiplication).

It is not difficult to show that Z_n^* has all the properties of a group, with 1 as its identity element. The following example demonstrates this for $n = 5$.

Example 5. The elements of group Z_5^* are obviously $\{1, 2, 3, 4\}$, since all of these numbers are smaller than 5 and are co-prime with it. We will now show that Properties 1-4 hold (this will not be a formal proof, but it will nicely illustrate some of the main points that were previously made).

Property 1. Let us consider $a = 2$ and $b = 3$, both of which belong to Z_5^*. In that case, we have

$$a \circ b = 2 \circ 3 = 2 \cdot 3 \bmod 5 = 1 \tag{81}$$

since

$$6 = 1 \cdot 5 + 1 \tag{82}$$

Observing that 1 is an element of Z_5^*, the closure requirement is obviously satisfied in this case.

Property 2. Suppose that $a = 2$, $b = 3$ and $c = 4$. Given that

$$3 \circ 4 = 3 \cdot 4 \bmod 5 = 2 \tag{83}$$

we can conclude that

$$2 \circ (3 \circ 4) = 2 \circ 2 = 2 \cdot 2 \bmod 5 = 4 \tag{84}$$

On the other hand, we also know that

$$(2 \circ 3) \circ 4 = 1 \circ 4 = 1 \cdot 4 \bmod 5 = 4 \tag{85}$$

by virtue of (81). As a result, we can claim that the associative property holds for this choice of a, b and c.

Property 3. It is not difficult to see that the identity element in Z_5^* is 1. This follows directly from the fact that

$$a \circ 1 = a \cdot 1 \bmod 5 = a \tag{86}$$

for any integer $a < 5$ (since $a = 0 \cdot 5 + a$ in all such cases). This obviously applies to the elements of Z_5^*, since they must be smaller than 5 by definition.

Property 4. To illustrate that every element of Z_5^* has an inverse, let us pick $a = 3$ as a test case. Because 3 is co-prime with 5, we know that 3_5^{-1} exists, and can be computed using Euclid's method. If we do so, we obtain

$$3_5^{-1} = 2 \tag{87}$$

as one of the possible values. It is easily verified that 2 is the inverse element of 3 in this group, since $2 \in Z_5^*$ and

$$2 \circ 3 = 2 \cdot 3 \bmod 5 = 1 \tag{88}$$

We can therefore conclude that Property 4 is satisfied for $a = 3$.

Having explained what operation "$\circ$" means in group Z_n^*, we now need to extend this idea to exponentiation. That is not difficult to do, because we can define the k-th power of element $g \in Z_n^*$ as

$$f_k(g) = g \circ g \circ \ldots \circ g \tag{89}$$

(which amounts to applying operation "$\circ$" k times). The following simple lemma shows that in group Z_n^* function $f_k(g)$ corresponds to the remainder that is obtained when g^k is divided by n.

Lemma 7.1. Let $f_k(g)$ be the k-th power of element $g \in Z_n^*$ (in the sense defined by equation (89)). Then, $f_k(g)$ can be expressed as

$$f_k(g) = g^k \bmod n \tag{90}$$

Cyclic Groups and Prime Factorization

A subset of elements $\{g_1, \ldots, g_m\} \subset G$ is said to *generate* group G if every member of this group can be expressed as

$$x = f_{k_1}(g_1) \circ f_{k_2}(g_2) \circ \ldots \circ f_{k_m}(g_m) \tag{91}$$

where "$\circ$" denotes the operation that characterizes the group, and $f_{k_i}(g_i)$ represent powers of g_i. In the special case when a *single* element g generates the entire group, we say that the group is *cyclic*. Any member of such a group can be expressed as

$$x = f_k(g) \tag{92}$$

where k is a positive integer.

The notion of a cyclic group is of central importance for the prime factorization problem, since group Z_n^* falls into this category when n is chosen in a particular way. The following theorem specifies how this choice should be made.

Theorem 7.1. Suppose that p is an odd prime number, and that α is a positive integer. Then, $Z_{p^\alpha}^*$ constitutes a cyclic group, and each of its elements can be represented as

$$x = f_k(g) = g^k \bmod p^\alpha \tag{93}$$

where $g \in Z_{p^\alpha}^*$ is a *group generator*, and k is a positive integer.

Theorem 7.1 has several useful corollaries, two of which we describe below.

Corollary 7.2. Values of k that exceed $\varphi(p^\alpha)$ will not produce any new elements of $Z_{p^\alpha}^*$. This is why we use the term 'cyclic' to describe such groups.

Corollary 7.3. For each k in the set $\{1, 2, \ldots, \varphi(p^\alpha)\}$, expression (93) produces a *different* element of $Z_{p^\alpha}^*$, and $k = \varphi(p^\alpha)$ corresponds to the identity element in this group.

The following result (which represents a generalization of Fermat's Little Theorem) describes another important property of generators in group $Z_{p^\alpha}^*$.

Lemma 7.2. Let g be a generator in group $Z^*_{p^\alpha}$. Then, $k = \varphi(p^\alpha)$ is the *smallest* power of g that satisfies

$$g^k = 1 \pmod{p^\alpha} \tag{94}$$

The only other values of k with this property are multiples of $\varphi(p^\alpha)$.

To get a sense for what group $Z^*_{p^\alpha}$ looks like, we now provide two examples that illustrate how generators can be found for different choices of p and α.

Example 6. Suppose that $p = 5$ and $\alpha = 1$. We know that $\varphi(p^\alpha) = p - 1 = 4$ (since p is a prime number), and it is easily verified that the elements of group Z^*_5 are $\{1, 2, 3, 4\}$. Theorem 7.1 additionally tells us that at least one of them must generate the entire group. If we check each element (except for 1, which cannot be a generator) for this property, we obtain the following:

For $g_1 = 2$:

$$\begin{aligned}
2^1 = 2 = 0 \cdot 5 + 2 \quad &\Longrightarrow \quad g_1^1 \bmod 5 = 2 \quad \Longrightarrow \quad f_1(g_1) = 2 \\
2^2 = 4 = 0 \cdot 5 + 4 \quad &\Longrightarrow \quad g_1^2 \bmod 5 = 4 \quad \Longrightarrow \quad f_2(g_1) = 4 \\
2^3 = 8 = 1 \cdot 5 + 3 \quad &\Longrightarrow \quad g_1^3 \bmod 5 = 3 \quad \Longrightarrow \quad f_3(g_1) = 3 \\
2^4 = 16 = 3 \cdot 5 + 1 \quad &\Longrightarrow \quad g_1^4 \bmod 5 = 1 \quad \Longrightarrow \quad f_4(g_1) = 1
\end{aligned} \tag{95}$$

For $g_2 = 3$:

$$\begin{aligned}
3^1 = 3 = 0 \cdot 5 + 3 \quad &\Longrightarrow \quad g_2^1 \bmod 5 = 3 \quad \Longrightarrow \quad f_1(g_2) = 3 \\
3^2 = 9 = 1 \cdot 5 + 4 \quad &\Longrightarrow \quad g_2^2 \bmod 5 = 4 \quad \Longrightarrow \quad f_2(g_2) = 4 \\
3^3 = 27 = 5 \cdot 5 + 2 \quad &\Longrightarrow \quad g_2^3 \bmod 5 = 2 \quad \Longrightarrow \quad f_3(g_2) = 2 \\
3^4 = 81 = 16 \cdot 5 + 1 \quad &\Longrightarrow \quad g_2^4 \bmod 5 = 1 \quad \Longrightarrow \quad f_4(g_2) = 1
\end{aligned} \tag{96}$$

For $g_3 = 4$:

$$\begin{aligned}
4^1 = 4 = 0 \cdot 5 + 4 \quad &\Longrightarrow \quad g_3^1 \bmod 5 = 4 \quad f_1(g_3) = 4 \\
4^2 = 16 = 3 \cdot 5 + 1 \quad &\Longrightarrow \quad g_3^2 \bmod 5 = 1 \quad f_2(g_3) = 1 \\
4^3 = 64 = 12 \cdot 5 + 4 \quad &\Longrightarrow \quad g_3^3 \bmod 5 = 4 \quad f_3(g_3) = 4 \\
4^4 = 256 = 51 \cdot 5 + 1 \quad &\Longrightarrow \quad g_3^4 \bmod 5 = 1 \quad f_4(g_3) = 1
\end{aligned} \tag{97}$$

From this, we can conclude that group Z^*_5 actually has *two* different generators, $g_1 = 2$ and $g_2 = 3$.

Since $\varphi(p^\alpha) = 4$ in this case, Corollary 7.2 implies that powers higher than 4 cannot produce any new elements of Z^*_5. This is easily verified by considering one of the generators in this group (say, $g_2 = 3$), and computing $f_5(g_2)$, $f_6(g_2)$, etc. If we do so, we obtain the following values

$$\begin{aligned}
3^5 = 243 = 48 \cdot 5 + 3 \quad &\Longrightarrow \quad g_2^5 \bmod 5 = 3 \quad \Longrightarrow \quad f_5(g_2) = 3 \\
3^6 = 729 = 145 \cdot 5 + 4 \quad &\Longrightarrow \quad g_2^6 \bmod 5 = 4 \quad \Longrightarrow \quad f_6(g_2) = 4 \\
3^7 = 2,187 = 437 \cdot 5 + 2 \quad &\Longrightarrow \quad g_2^7 \bmod 5 = 2 \quad \Longrightarrow \quad f_7(g_2) = 2 \\
\vdots \qquad &\qquad \vdots \qquad\qquad \vdots
\end{aligned} \tag{98}$$

all of which already appear in (96). It is also readily observed that the two generators of this group satisfy

$$g_i^{\varphi(p^\alpha)} \bmod p^\alpha = g_i^4 \bmod 5 = 1 \tag{99}$$

and that $\varphi(p^\alpha)$ is the smallest exponent with this property. This is obviously consistent with Lemma 7.2.

Example 7. Suppose that $p = 3$ and $\alpha = 2$. In this case we have

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) = 6 \tag{100}$$

so we know that group Z_9^* consists of 6 different elements. These elements are $\{1, 2, 4, 5, 7, 8\}$ (3 and 6 have been excluded, since they have common divisors with 9). Testing each element of the group, we obtain:

For $g_1 = 2$:

$$\begin{aligned}
2^1 = 2 = 0 \cdot 9 + 2 &\implies g_1^1 \bmod 9 = 2 \implies f_1(g_1) = 2 \\
2^2 = 4 = 0 \cdot 9 + 4 &\implies g_1^2 \bmod 9 = 4 \implies f_2(g_1) = 4 \\
2^3 = 8 = 0 \cdot 9 + 8 &\implies g_1^3 \bmod 9 = 8 \implies f_3(g_1) = 8 \\
2^4 = 16 = 1 \cdot 9 + 7 &\implies g_1^4 \bmod 9 = 7 \implies f_4(g_1) = 7 \\
2^5 = 32 = 3 \cdot 9 + 5 &\implies g_1^5 \bmod 9 = 5 \implies f_5(g_1) = 5 \\
2^6 = 64 = 7 \cdot 9 + 1 &\implies g_1^6 \bmod 9 = 1 \implies f_6(g_1) = 1
\end{aligned} \tag{101}$$

For $g_2 = 4$:

$$\begin{aligned}
4^1 = 4 = 0 \cdot 9 + 4 &\implies g_2^1 \bmod 9 = 4 \implies f_1(g_2) = 4 \\
4^2 = 16 = 1 \cdot 9 + 7 &\implies g_2^2 \bmod 9 = 7 \implies f_2(g_2) = 7 \\
4^3 = 64 = 7 \cdot 9 + 1 &\implies g_2^3 \bmod 9 = 1 \implies f_3(g_2) = 1 \\
4^4 = 256 = 28 \cdot 9 + 4 &\implies g_2^4 \bmod 9 = 4 \implies f_4(g_2) = 4 \\
4^5 = 1,024 = 113 \cdot 9 + 7 &\implies g_2^5 \bmod 9 = 7 \implies f_5(g_2) = 7 \\
4^6 = 4,096 = 455 \cdot 9 + 1 &\implies g_2^6 \bmod 9 = 1 \implies f_6(g_2) = 1
\end{aligned} \tag{102}$$

For $g_3 = 5$:

$$\begin{aligned}
5^1 = 5 = 0 \cdot 9 + 5 &\implies g_3^1 \bmod 9 = 5 \implies f_1(g_3) = 5 \\
5^2 = 25 = 2 \cdot 9 + 7 &\implies g_3^2 \bmod 9 = 7 \implies f_2(g_3) = 7 \\
5^3 = 125 = 13 \cdot 9 + 8 &\implies g_3^3 \bmod 9 = 8 \implies f_3(g_3) = 8 \\
5^4 = 625 = 69 \cdot 9 + 4 &\implies g_3^4 \bmod 9 = 4 \implies f_4(g_3) = 4 \\
5^5 = 3,125 = 347 \cdot 9 + 2 &\implies g_3^5 \bmod 9 = 2 \implies f_5(g_3) = 2 \\
5^6 = 15,625 = 1,736 \cdot 9 + 1 &\implies g_3^6 \bmod 9 = 1 \implies f_6(g_3) = 1
\end{aligned} \tag{103}$$

For $g_4 = 7$:

$$\begin{aligned}
7^1 = 7 = 0 \cdot 9 + 7 \quad &\Longrightarrow \quad g_4^1 \bmod 9 = 7 \quad \Longrightarrow \quad f_1(g_4) = 7 \\
7^2 = 49 = 5 \cdot 9 + 4 \quad &\Longrightarrow \quad g_4^2 \bmod 9 = 4 \quad \Longrightarrow \quad f_2(g_4) = 4 \\
7^3 = 343 = 38 \cdot 9 + 1 \quad &\Longrightarrow \quad g_4^3 \bmod 9 = 1 \quad \Longrightarrow \quad f_3(g_4) = 1 \\
7^4 = 2,401 = 266 \cdot 9 + 7 \quad &\Longrightarrow \quad g_4^4 \bmod 9 = 7 \quad \Longrightarrow \quad f_4(g_4) = 7 \\
7^5 = 16,807 = 1,867 \cdot 9 + 7 \quad &\Longrightarrow \quad g_4^5 \bmod 9 = 7 \quad \Longrightarrow \quad f_5(g_4) = 7 \\
7^6 = 117,649 = 13,072 \cdot 9 + 1 \quad &\Longrightarrow \quad g_4^6 \bmod 9 = 1 \quad \Longrightarrow \quad f_6(g_4) = 1
\end{aligned} \tag{104}$$

For $g_5 = 8$:

$$\begin{aligned}
8^1 = 8 = 0 \cdot 9 + 8 \quad &\Longrightarrow \quad g_5^1 \bmod 9 = 8 \quad f_1(g_5) = 8 \\
8^2 = 64 = 7 \cdot 9 + 1 \quad &\Longrightarrow \quad g_5^2 \bmod 9 = 1 \quad f_2(g_5) = 1 \\
8^3 = 512 = 56 \cdot 9 + 8 \quad &\Longrightarrow \quad g_5^3 \bmod 9 = 8 \quad f_3(g_5) = 8 \\
8^4 = 4,096 = 455 \cdot 9 + 1 \quad &\Longrightarrow \quad g_5^4 \bmod 9 = 1 \quad f_4(g_5) = 1 \\
8^5 = 32,768 = 3,640 \cdot 9 + 8 \quad &\Longrightarrow \quad g_5^5 \bmod 9 = 8 \quad f_5(g_5) = 8 \\
8^6 = 262,144 = 29,127 \cdot 9 + 1 \quad &\Longrightarrow \quad g_5^6 \bmod 9 = 1 \quad f_6(g_5) = 1
\end{aligned} \tag{105}$$

These results indicate that group Z_9^* has *two* different generators, $g_1 = 2$ and $g_3 = 5$. As in the previous example, it is easily verified that powers of g higher than 6 do not produce any new elements, and that the two group generators satisfy

$$g_i^{\varphi(p^\alpha)} \bmod p^\alpha = g_i^6 \bmod 9 = 1 \tag{106}$$

Note that the other elements in this group ($g_2 = 4$, $g_4 = 7$ and $g_5 = 8$) satisfy

$$g_i^k \bmod p^\alpha = 1 \tag{107}$$

for values of k that are *smaller* than $\varphi(p^\alpha)$.

Finding Non-Trivial Divisors of Composite Numbers

Since the prime factorization of N entails finding its non-trivial divisors (i.e. divisors that are neither 1 nor N), we now need to show how that can be done. As a first step, we will establish that all numbers of the form

$$x = 1 + \alpha N \tag{108}$$

and

$$x = -1 + \beta N \tag{109}$$

are solutions of equation

$$x^2 = 1 \ (\text{mod } N) \tag{110}$$

Note that the first group of numbers satisfies

$$x - 1 = \alpha N \;\Leftrightarrow\; x = 1 \pmod{N} \tag{111}$$

and that the second one satisfies

$$x + 1 = \beta N \;\Leftrightarrow\; x = -1 \pmod{N} \tag{112}$$

Because of that, such solutions are commonly referred to as "trivial".

We can verify this property directly, by examining each scenario separately.

CASE 1. If

$$x = 1 + \alpha N \tag{113}$$

we have that

$$\begin{aligned} &x^2 - 1 = (\alpha N + 1)^2 - 1 = \alpha^2 N^2 + 2\alpha N + 1 - 1 = \\ &= (\alpha^2 N + 2\alpha)N = \sigma_1 N \end{aligned} \tag{114}$$

We can therefore conclude that all such numbers are solutions of equation (110).

CASE 2. If

$$x = -1 + \beta N \tag{115}$$

then

$$\begin{aligned} &x^2 - 1 = (\beta N - 1)^2 - 1 = \beta^2 N^2 - 2\beta N + 1 - 1 = \\ &= (\beta^2 N - 2\beta)N = \sigma_2 N \end{aligned} \tag{116}$$

which means that equation (110) is once again satisfied.

Having shown this, we can now group the trivial solutions of equation (110) into two sets:

$$S_1 = \{\dots 1 - 2N, 1 - N, 1, N + 1, 2N + 1, \cdots\} \tag{117}$$

and

$$S_2 = \{\dots - 1 - 2N, -1 - N, -1, N - 1, 2N - 1, \cdots\} \tag{118}$$

Note that both of these sets have infinitely many elements.

The following theorem shows how we can combine this result with Euler's method to compute a *non-trivial* factor of a composite number N. As we mentioned earlier, this is important because it represents a key step in the process of prime factorization.

Theorem 7.2. Let N be a composite number, and suppose that x is a non-trivial solution of equation (110) that satisfies $1 < x < N$. Then, at least one of $a = \gcd(x - 1, N)$ and $b = \gcd(x + 1, N)$ is a non-trivial factor of N.

Theorem 7.2. indicates that the problem of finding a non-trivial divisor of N can be reduced to identifying a non-trivial solution of equation (110). The following theorem will help us develop a systematic procedure for computing such a solution.

Theorem 7.3. Let N be an odd composite number whose prime factorization has the form

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} \tag{119}$$

Suppose further that x is randomly chosen from set $\{1, 2, \ldots, N-1\}$, and that $x \in Z_N^*$. This implies that x is co-prime with N, so r (which represents the order of x modulo N) is properly defined. Under such circumstances, the probability that r will be an even number which satisfies

$$x^{r/2} \neq -1 \pmod{N} \tag{120}$$

is no lower than $1 - (1/2)^m$.

Remark 4. Note that this result explicitly refers to group Z_N^*, which explains why it was necessary to study its properties. The fact that this group is cyclic when $N = \varphi(p^\alpha)$ is a key step in proving Theorem 7.3.

A Quantum Algorithm for Prime Factorization

The quantum algorithm for prime factorization involves a sequence of steps, the first three of which are designed to check whether a non-trivial factor of N can be determined in a way that does *not* involve a significant computational effort (and can therefore be executed efficiently on a classical computer).

STEP 1. Check if N is an even number. If so, keep dividing by 2 until you obtain $N = 2^b M$, where M is an *odd* number.

STEP 2. Check if N has the form $N = a^b$, where $a > 1$ and $b > 1$. If so, a is guaranteed to be a non-trivial factor of N. If N is L bits long, it can be shown that computing a and b requires no more than $L - 1$ steps (see Lemma 7.4 in the textbook).

STEP 3. Randomly pick a positive integer x such that $1 < x < N$, and check whether $w = \gcd(x, N) > 1$. If this happens to be the case, w will be a non-trivial factor of N by definition. Such a procedure involves Euclid's algorithm, and can be executed on a classical computer.

STEP 4. If Steps 1-3 fail to produce a non-trivial factor of N, it is necessary to implement a special procedure which involves finding the order of x modulo N. We should reiterate that this is something that classical computers *cannot* do in a reasonable amount of time when N is large, but quantum computers can.

Before we describe how this procedure works, we should recall that Step 4 is executed *only* if we have determined that N is odd (in Step 1), that it has multiple prime factors (in Step 2), and that the randomly chosen integer x in Step 3 is co-prime with N (and therefore belongs to group Z_N^*). As a result, we can invoke Theorem 7.3 directly.

This theorem tells us that computing the order of x modulo N is likely to yield an *even* r *that satisfies*

$$x^{r/2} \neq -1 \pmod{N} \tag{121}$$

The probability that this will happen is at least 0.75, because we already established that $m \geq 2$ in Step 2. Since we are dealing with probabilities, it is possible that we will not be successful in the first attempt, and that we will obtain an r that is either odd, or fails to satisfy condition (121). However, repeating the procedure several times is bound to produce

the desired outcome. Note that this will not require an excessive amount of time, since we have an efficient quantum algorithm for determining the order of a number.

Suppose now that we have picked an integer x that satisfies the conditions of Theorem 7.3. To see how this theorem can help us compute a non-trivial factor of N, we should first observe that $x^{r/2}$ is certain to be an integer when r is even, which allows us to represent it as

$$x^{r/2} = \alpha N + y \tag{122}$$

where $0 \leq y < N$. It is not difficult to show that the remainder y satisfies equation

$$y^2 = 1 \pmod{N} \tag{123}$$

In order to do that, we will make use of the fact that

$$x^r = (\alpha N + y)^2 = \alpha^2 N^2 + 2\alpha N y + y^2 = y^2 + \mu N \tag{124}$$

Recalling that r is the order of x modulo N, we know that x^r satisfies

$$x^r = 1 + \beta N \tag{125}$$

Equating (124) and (125), we now obtain

$$y^2 + \mu N = 1 + \beta N \quad \Longrightarrow \quad y^2 = 1 + (\beta - \mu)N = 1 + \sigma N \tag{126}$$

which is obviously equivalent to (123).

Since y is the remainder of dividing $x^{r/2}$ by N, we know that it must satisfy $0 \leq y < N$. Equation (126) additionally tells us that y cannot equal 0. To see why this is so, it suffices to observe that substituting $y = 0$ into this equation would produce $\sigma = -1/N$. That, however, would lead to a contradiction, because σ must be an integer and N is assumed to be greater than 1. Taking this into account, we can conclude that

$$1 \leq y < N \tag{127}$$

We will now show that *y cannot be a trivial solution of equation* (123) if r is even and satisfies condition (121). In order to do that, we should first recall that this equation has two sets of trivial solutions:

$$S_1 = \{\ldots, -2N + 1, -N + 1, 1, N + 1, 2N + 1, \ldots\} \tag{128}$$

and

$$S_2 = \{\ldots, -2N - 1, -N - 1, -1, N - 1, 2N - 1, \ldots\} \tag{129}$$

If y happened to belong to set S_2, it would have the form

$$y = -1 + kN \tag{130}$$

and equation (122) would produce

$$x^{r/2} = \alpha N + y = \alpha N - 1 + kN = -1 + (\alpha + k)N \tag{131}$$

Since this implies that

$$x^{r/2} = -1 \pmod{N} \tag{132}$$

condition (121) would be violated, and we would have a contradiction. From this, we can conclude that $y \notin S_2$.

If we assume that $y \in S_1$, it would satisfy

$$y = 1 + kN \tag{133}$$

for some integer k. In that case, $x^{r/2}$ could be expressed as

$$x^{r/2} = \alpha N + y = \alpha N + 1 + kN = 1 + (\alpha + k)N \tag{134}$$

which is equivalent to

$$x^{r/2} = 1 \pmod{N} \tag{135}$$

Since r is even, we know that $r/2$ must be an integer. That, however, leads to a contradiction, since the *smallest* integer that satisfies this condition is r (by definition). Consequently, y cannot belong to set S_1 either.

The fact that $y \notin S_1$ also rules out the possibility that $y = 1$ (since 1 is a member of this set). As a result, inequality (127) becomes

$$1 < y < N \tag{136}$$

Given that y satisfies $1 < y < N$ and is a non-trivial solution of equation (123), we can now apply Theorem 7.2, and claim that at least one of $a = \gcd(y + 1, N)$ and $b = \gcd(y - 1, N)$ must be a non-trivial divisor of N.

If we repeat this algorithm recursively, we will eventually obtain the prime factors of N. As noted earlier, such a procedure is feasible because all four steps (including the quantum order-finding algorithm) can be performed efficiently. The following example illustrates how Step 4 works in practice.

Example 8. Suppose that we are interested in determining the prime factors of $N = 273$, and that we randomly picked $x = 10$. It is not difficult to show that x belongs to group Z^*_{273}, since $x < 273$ and

$$\gcd(10, 273) = 1 \tag{137}$$

We can therefore proceed directly to Step 4, and execute the order finding algorithm. If we do so, we will find that the order of x modulo 273 is $r = 6$.

Observing that

$$x^{r/2} = 10^3 = 3 \times 273 + 181 \tag{138}$$

it follows that

$$x^{r/2} + 1 = 3 \times 273 + 182 \tag{139}$$

so condition (121) is clearly satisfied. Setting $y = 181$, we can now use Euclid's method to obtain

$$\gcd(y + 1, N) = \gcd(182, 273) = 13 \tag{140}$$

and

$$\gcd(y - 1, N) = \gcd(180, 273) = 3 \tag{141}$$

Since both of these numbers are prime, we can conclude that 13 and 3 are prime factors of 273. Dividing 273 by 39, we easily obtain the third prime factor (which happens to be 7).

It is interesting to note in this context that choosing $x = 2$ instead of $x = 10$ would provide a different pair of non-trivial factors. In this case, the order of x would be $r = 12$, and $x^{r/2}$ could be expressed as

$$x^{r/2} = 2^6 = 0 \times 273 + 64 \tag{142}$$

Setting $y = 64$ would then produce

$$\gcd(y + 1, N) = \gcd(65, 273) = 13 \tag{143}$$

and

$$\gcd(y - 1, N) = \gcd(63, 273) = 7 \tag{144}$$

both of which are prime factors of $N = 273$.