COMPUTATIONAL METHODS IN NUMBER THEORY

A Thesis

Presented to

the Faculty of the Department of Computer Science

University of Houston

In Partial Fulfillment

of the Requirements for the Degree of

Master of Science

by

Cheng Shyan Shih

August, 1971

ACKNOWLEDGEMENT

The author would like to express her appreciation to her adviser, Dr. M. Meicler, and Dr. A. Newhouse for their guidance, encouragement, and corrections of this paper. Also, I wish to express my deepest thanks to my husband, David, for his constant supporting during its preparation.

COMPUTATIONAL METHODS IN NUMBER THEORY

An Abstract of a Thesis

Presented to

the Faculty of the Department of Computer Science

University of Houston

In Partial Fulfillment

of the Requirements for the Degree of

Master of Science

by

Cheng Shyan Shih

August, 1971

ABSTRACT

This paper presents a number of methods for testing the primality of any given number N. A brief history of number theory is introduced in Chapter I. The main task of this paper is to test the primality of any given number. However, if the test shows a negative result, or that the given number is not a prime but a composite, then the task is extended to the next step - factoring the given number. Several methods for factorization of a given number N are discussed in Chapter III. In addition, a representive example for both tasks as carried out by a computer program written in the Fortran IV language is presented.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

As far back as any records can be found, mankind possessed adequate methods for keeping a tally of things, while our knowledge of ancient civilizations reveals an already highly developed art of denoting and operating on numbers as far back as 3500 B. C. and earlier. A natural number is the original mathematical concept and the most fundamental, the first rudiments of scientific approach to the study of numbers can be traced back to Pythagoras (600 B. C.). It is believed that the distinction between prime and composite numbers was made in the Pythagorean school. By definition, a prime is a number that is divisible only by the number one and itself, while a composite is a number that has divisors other than the number one and itself. The first systematic presentation of results in number theory with proof is to be found in Euclid's Elementa (300 B. C.). Among the later Greek mathematicians, Diophantos (A. D. 350) was responsible for adding further significant advancement to the development of the theory of numbers.

A great impulse to the further development of number theory was not received until the seventeenth century, with the memorable discoveries of many deep and abstruse properties of numbers by Fermat (1601 - 1665). The French mathematician Fermat may rightly be regarded as the father of the more recent number theory.

Fermat stated in 1640 that he had a proof of the fact, now known as Fermat's theorem, that if p is any prime and x is any integer not divisible by p, then $x^{p-1} - 1$ is divisible by p. This is one of the fundamental theorems of the theory of numbers. The case x = 2 was known to the Chinese as early as 500 B. C. The first published proof was given by Euler in 1736. Of first importance is the generalization from the case of a prime p to any integer N, published by Euler in 1760 : If $\phi(N)$ denotes the number of positive integers not exceeding N and relatively prime to N, then $x^{\phi(N)} - 1$ is divisible by N for every integer x relatively prime to N. Another elegant theorem states that, if p is a prime, $1 + \{1 \cdot 2 \cdot 3 \cdots (p - 1)\}$ is divisible by p; it was first published by Waring in 1770, who ascribed it to Sir John Wilson. In 1773, Lagrange was the first one to publish a proof of Wilson's theorem and to observe that its converse is true. In 1801, Gauss stated and suggested methods to prove the generalization of Wilson's theorem : if N denotes the product of the positive integers less than A and prime to A, then N + 1 is divisible by A if A = 4, p^m or $2p^m$, where p is an odd prime, while N - 1 is divisible by A if A is not of one of these three forms.

Many cases have been found in which $a^{(N-1)} - 1$ is divisible by N for a composite number N. But, in 1876, Lucas proved the following converse of Fermat's theorem : if $a^x - 1$ is divisible by N when x = N - 1, but not for $x < (N - 1)$, then N is a prime.

The last hundred years have been charaterized by an intensive development of number theory in many different directions.

In general, the prime numbers may be divided into two classes according to the remainder they give on division by any number taken as " modulus ". Thus, every prime other than 2, which is the only even prime, is a multiple of 4 plus or minus 1. This is expressed by saying they are of the form $4n + 1$ or $4n - 1$. The primes 5, 13, ... belong to the form $4n + 1$, and 3, 7, 11, 19, ... belong to the form $4n - 1$. It is not difficult to show by a slight extension of Euclid's method for all primes, that each of the above sequences contains an infinite number of primes.

CHAPTER II

METHODS FOR TESTING PRIMALITY

It is not a simple matter to determine whether or not N is prime. Therefore, several computational methods for testing primality will be discussed in this chapter.

Eratosthenes [10] devised a systematic method, called the sieve or crib of Eratosthenes, for obtaining all primes up to any given number N. Consider all integers from 2 up to N listed in their natural order. We start with $2 \cdot 2$, striking out all the multiples of 2, i.e. $2 \cdot 2$, $2 \cdot 3$, $2 \cdot 4$, ..., $2 \cdot n$ for all $n \leq (1/2)N$. The next prime integer will be 3, cancelling again all multiples of 3, starting with $3 \cdot 3$, proceed as with the integer 2, i.e. $3 \cdot 3$, $3 \cdot 4$, $3 \cdot 5$, ..., $3 \cdot n$ for all $n \leq N/3$. The next prime integer remaining in our list after 3 is 5; again we follow the same pattern as with 2 and 3, i.e. $5 \cdot 5$, $5 \cdot 6$, ..., and so on. Continue in the same way with all primes not exceeding $N^{1/2}$, their multiples being crossed out of all the series, 2, 3, ..., N. Then the remaining numbers will all be primes not exceeding N. Therefore, if N is in the remaining number list, then N is a prime; otherwise N is a composite. As an example : Suppose N = 39, which is not a prime number. The list is

2, 3, $\cancel{4}$, 5, $\cancel{6}$, 7, $\cancel{8}$, $\cancel{9}$, $\cancel{10}$, 11, $\cancel{12}$, 13, $\cancel{14}$, $\cancel{15}$,
$\cancel{16}$, 17, $\cancel{18}$, 19, $\cancel{20}$, $\cancel{21}$, $\cancel{22}$, 23, $\cancel{24}$, $\cancel{25}$, $\cancel{26}$, $\cancel{27}$,
$\cancel{28}$, 29, $\cancel{30}$, 31, $\cancel{32}$, $\cancel{33}$, $\cancel{34}$, $\cancel{35}$, $\cancel{36}$, 37, $\cancel{38}$, $\cancel{39}$

crossing out all the multiples of primes up to $N^{1/2}$. From the list we know that N was crossed out, so N is not a prime.

From the above example, we realize that some of the integers have been crossed out more than once; for instance, 12 and 18 had to be cancelled both as a multiple of 2, and 3 in the example. This sieve method is a tedious and time-consuming method, even though it is quite effective for obtaining a list of primes up to a reasonably small limit.

Similar to the sieve method, a simple and elementary method [11] for testing the primality of a given number N is to divide N by primes not exceeding its square root; and if one division yields no remainder, then the proposed number is composite, otherwise, it is a prime. Let us test, for example, 1009. Primes not exceeding $1009^{1/2}$ are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 31$$

and on trial we find that none of them divides 1009. Hence 1009 is a prime number.

This simple test of primality is quite workable and convenient when the numbers to be tested are not large; but with increasing size of the numbers, the trials become too numerous and burdensome. Also a table of primes must be created. To obviate this inconvenience other, more expeditious, methods have been devised to ascertain whether or not a number is prime.

Testing Primality by Final Digit [8]

This method for testing the primality of a number N, is to divide it by primes $\leq N^{1/2}$. By considering the choice of final digits the number of primes to be so tested can be restricted. Suppose N has the form of 10C + D where C is an integer, and D = 1, 3, 7, or 9, thus extending the obvious range of the standard procedure by a factor 10. The process depends upon the representation of N in the decimal system, and is based on the following lemma.

<u>Lemma</u> : The number 10c + d divides 10C + D (D, d, = 1, 3, 7, 9) if it divides C - T(c), where T(c) is linear in c depending only on d and D. The 16 values of T(c) are arrayed in the Table below.

		Value of D			
		1	3	7	9
Value of d	1	c	3c	7c	9c
	3	7c+2	c	9c+2	3c
	7	3c+2	9c+6	c	7c+4
	9	9c+8	7c+6	3c+2	c

It will be seen that if

$$N = 10C + D = N_1 \cdot N_2$$

$$= (10c_1 + d_1)(10c_2 + d_2)$$

then

$$C - T(c_1) = c_2 \cdot N_1$$

or

$$C - T(c_2) = c_1 \cdot N_2$$

For example, let $N = 9401 = 10 \cdot 940 + 1$. Thus $C = 940$, and $D = 1$. We need to test for primes $10c + 1$, $10c + 9$, and either $10c + 7$ or $10c + 3$; because the primary condition, in this case, to accomplish the test is to make $d_1 \cdot d_2 = D = 1$. With $d = 9$, $D = 1$, we have $T(c) = 9c + 8$ so that $940 - T(c)$ is divisible by $10c + 9$ for $c = 1, 2, \ldots.$ This is satisfied for $c = 7$, therefore $T(c_1) = 71$, we have

$$940 - 71 = 869 = 79 \cdot 11$$

and so $c_2 = 11$ and $10c_2 + 9 = 119$ and thus

$$9401 = 79 \cdot 119$$

It is equally obvious that if $C - T(c)$ is not a product of the form cN_1 or cN_2 for all c, then N is prime.

This method, possibly with some refinements, is sometime used on the electronic computing machines for testing large numbers. But even so, this procedure is laborious and costly.

Testing Primality by Wilson's Theorem

[2], [11]

E. Waring first published the theorem that $1 + (N - 1)!$ is always divisible by a prime N or in congruence notation,

$$1 \cdot 2 \cdot 3 \cdot \cdot \cdot (N - 1) + 1 \equiv 0 \pmod{N}.$$

The abbreviation " mod " for modulus is used repeatedly:

Two integers a and b whose difference $a - b$ is divisible by a given number m, which is not zero, are said to be congruent for the modulus m or simply congruent mod m. We will use the following form to express the number-theoretical concept of congruence

$$a \equiv b \quad (\bmod m) \qquad (1)$$

means that $a \ (\bmod m) = b \ (\bmod m)$, that is, the difference $a - b$ is an integral multiple of m. Expression (1) is read, " a is congruent to b modulo m ", and b is said to be a " residue " of a (mod m). Any subset S of the set of integers is called a " complete residue system " modulo m if each integer is congruent to one and only one of the members of the subset S. The set

$$\{ 0, 1, 2, 3, \ldots, m - 1 \}$$

is always a complete residue system modulo m.

We shall now state the basic elementary properties of congruence. All variables in the following formulas are assumed to be integers. Two integers are said to be " relatively prime " if they have no common factor,i.e. if their greatest common divisor is 1.

A. The congruence relation modulo m is an " equivalence relation" on the set of integers; that is, the congruence relation modulo m is

(i) reflexive: $a \equiv a \ (\bmod m)$ for every integer a;

(ii) symmetric: if $a \equiv b \ (\bmod m)$, then $b \equiv a \ (\bmod m)$;

(iii) transitive: if $a \equiv b \ (\bmod m)$ and $b \equiv c \ (\bmod m)$, then $a \equiv c \ (\bmod m)$.

B. Two congruences with the same modulo can be added or subtracted or multiplied, member by member, like equalities. In other words, if $a \equiv b \pmod{m}$ and $x \equiv y \pmod{m}$, then $a + x \equiv b + y \pmod{m}$ and $a \cdot x \equiv b \cdot y \pmod{m}$.

C. If $a \cdot x \equiv b \cdot y \pmod{m}$ and $a \equiv b \pmod{m}$, and if a is relatively prime to m, then $x \equiv y \pmod{m}$.

D. $a \equiv b \pmod{m}$ if and only if $a \cdot n \equiv b \cdot n \pmod{mn}$, for $n \neq 0$.

E. If r is relatively prime to s, then $a \equiv b \pmod{rs}$ if and only if $a \equiv b \pmod{r}$ and $a \equiv b \pmod{s}$.

Theorem (Wilson's) : $(N - 1)! + 1 \equiv 0 \pmod{N}$ if and only if N is a prime.

Proof :

(a) Suppose $(N - 1)! + 1 \equiv 0 \pmod{N}$, we have to prove N is a prime.

Assume that N is not a prime, so N is a product of two numbers i.e. $N = a \cdot b$ where $1 < a < N$ and $1 < b < N$, so that $(N - 1)!$ can be divided by a or b. But $(N - 1)! + 1$ can not be divided by a or b. This implies that N does not divide $(N - 1)! + 1$. So that

$$(N - 1)! + 1 \not\equiv 0 \pmod{N}.$$

This is a contradition to the hypothesis

$$(N - 1)! + 1 \equiv 0 \pmod{N},$$

therefore N is a prime.

(b) (Due to Gauss [11]). Suppose N is prime, then we have to prove $(N - 1)! + 1 \equiv 0 \pmod{N}$.

Suppose x is any number of the sequence

$$1, 2, 3, 4, \ldots, N - 1$$

then

$$x, 2x, 3x, 4x, \ldots, (N - 1)x$$

forms a complete system of residues (mod N) with the exclusion of 0, and one and only one of these numbers is congruent to 1 (mod N). In other words, to any $x = 1, 2, \ldots, N - 1$ corresponds one and only one number x' in the same sequence, such that

$$xx' \equiv 1 \pmod N$$

x and x' are called " associate numbers ". Numbers which are identical with their associates are 1 and $N - 1$. Indeen the congruence

$$x^2 \equiv 1 \pmod N$$

is equivalent to

$$(x - 1)(x + 1) \equiv 0 \pmod N.$$

Whence either $x \equiv 1 \pmod N$ or $x \equiv -1 \pmod N$; that is $x = 1$ or $x = N - 1$. If we exclude 1 and $N - 1$, all the remaining numbers

$$2, 3, 4, \ldots, N - 2$$

can be combined in pairs of associate numbers, and we have as many congruences of the type

$$xx' \equiv 1 \pmod N$$

as there are such pairs. Multiplying all these congruences, member by member, the left-hand side of the congruence will be the product $2 \cdot 3 \cdot 4 \cdots (N - 2)$, while the right-hand side will be 1. Thus,

$$2 \cdot 3 \cdot 4 \cdots (N - 2) \equiv 1 \pmod N \qquad (2)$$

Now multiplying

$$1 \cdot (N - 1) \equiv -1 \pmod{N}$$

with (2) we get

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots (N - 1) \equiv -1 \pmod{N}$$

which is Wilson's theorem.

Let's take an example to illustrate Wilson's Theorem. Suppose N = 13, then the associate pairs are : 2, 7; 3, 9; 4, 10; 5, 8; 6, 11 and

$$2 \cdot 7 \equiv 1 \pmod{13}; \qquad 3 \cdot 9 \equiv 1 \pmod{13}$$

$$4 \cdot 10 \equiv 1 \pmod{13}; \qquad 5 \cdot 8 \equiv 1 \pmod{13}$$

$$6 \cdot 11 \equiv 1 \pmod{13}.$$

Multiplying the left-hand sides together, we have

$$2 \cdot 7 \cdot 3 \cdot 9 \cdot 4 \cdot 10 \cdot 5 \cdot 8 \cdot 6 \cdot 11$$

and the right-hand side 1. So the result will be

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \equiv 1 \pmod{13}$$

multiplying this by

$$1 \cdot 12 \equiv -1 \pmod{13}$$

we get

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv -1 \pmod{13}$$

so

$$(N - 1)! + 1 \equiv 0 \pmod{13}$$

thus, N = 13 is a prime.

When we want to know whether any given number N is prime we may apply Wilson's theorem. For according to this theorem N is prime if and only if N is a factor of the expression (N-1)! + 1.

A generalization of Wilson's theorem which can be used to investigate primality of a given number N is as follows.

Suppose N is prime, then the following congruence is true

$$(N - 1)! + 1 \equiv 0 \pmod{N}. \tag{3}$$

We may rewrite (3) as

$$(N - 1)(N - 2)! + 1 \equiv 0 \pmod{N} \tag{4}$$

the left-hand side can be rearranged as

$$N(N - 2)! - (N - 2)! + 1 = N(N - 2)! - ((N - 2)! - 1).$$

Since (4) is true, we have

$$N(N - 2)! - ((N - 2)! - 1) \equiv 0 \pmod{N}. \tag{5}$$

We know that two congruences with the same moduli can be added or subtracted, member by member, like equalities, so (5) can be split into

$$N(N - 2)! \equiv 0 \pmod{N} \tag{6}$$

and

$$(N - 2)! - 1 \equiv 0 \pmod{N}. \tag{7}$$

Again, we rewrite (7) as

$$(N - 2)(N - 3)! - 1 \equiv 0 \pmod{N}.$$

Thus

$$N(N - 3)! - 2(N - 3)! - 1$$
$$= N(N - 3)! - (2(N - 3)! + 1) \equiv 0 \pmod{N}$$

we have

$$2(\ N-3\ )!+1\equiv 0 \qquad (\ \mathrm{mod}\ N\ ). \qquad (\ 8\ )$$

Again, (8) can be expressed as

$$2(\ N-3\ )(\ N-4\ )!+1\equiv 0 \quad (\ \mathrm{mod}\ N\ )$$

$$2N(\ N-4\ )!-2\cdot 3\cdot(\ N-4\ )!+1$$

$$=2N(\ N-4\ )!-(\ 6(\ N-4\ )!-1\ )\equiv 0 \quad (\ \mathrm{mod}\ N\ )$$

therefore,

$$6(\ N-4\ )!-1\equiv 0 \quad (\ \mathrm{mod}\ N\ ). \qquad (\ 9\ )$$

Now let us write the four congruences (3), (7), (8), and (9) this way :

$$\left.\begin{aligned} 0!\ (\ N-1\ )!+1&\equiv 0\\ 1!\ (\ N-2\ )!-1&\equiv 0\\ 2!\ (\ N-3\ )!+1&\equiv 0\\ 3!\ (\ N-4\ )!-1&\equiv 0\ . \end{aligned}\right\} \quad (\ \mathrm{mod}\ N\ )$$

Continuing with this process we obtain

$$q!(\ N-(\ q+1\ ))!+(\ -1\ )^q\equiv 0 \qquad (\ \mathrm{mod}\ N\ ). \qquad (\ 10\ )$$

As an illustration, let us assume N = 7, and q from 0 to 3, then

$$0!(\ 7-1\ )!+1=721=7\cdot 103$$

$$1!(\ 7-2\ )!-1=119=7\cdot 17$$

$$2!(\ 7-3\ )!+1=49=7\cdot 7$$

$$3!(\ 7-4\ )!-1=35=7\cdot 5.$$

By each of these four calculations we have shown that 7 is a prime.

But we could cut these calculations short. In (10), choose $q=\lfloor N/2\rfloor$, where $\lfloor N/2\rfloor$ has the value of greatest integer less than or equal to N/2, and we have

$$(\ \lfloor N/2\rfloor\,!\ )^2-1=(\ q!\ )^2-1\equiv 0 \quad (\ \mathrm{mod}\ N\ ) \qquad (\ 11\ )$$

for any odd N.

Therefore, to determine whether or not 7 is prime, it is not necessary to compute (6!) + 1, but only $(3!)^2 - 1$. It would be a significant saving when the number to be computed is large. For (11), we still have a further simplification

$$(q!)^2 - 1 = (q! - 1)(q! + 1)$$

so either

$$(q! - 1) = \lfloor N/2 \rfloor ! - 1$$

or

$$(q! + 1) = \lfloor N/2 \rfloor ! + 1$$

contains N as factor, then N is a prime. Even so, for large N the factors of N/2 ! become very numerous .

In conclusion, while this tests the primality of a given number N, it is not practical.

Testing Primality by the Lucas-Lehmer Method

[3], [4]

There are two distinct efficient methods for determining the primality of a large integer without trying possible divisors. One of the two methods is the Lucas-Lehmer test which is particularly well adapted to investigate the Mersenne numbers which have the form $M_p = 2^p - 1$, where p is prime.

Perhaps the most remarkable results of the Lucas-Lehmer method are included in a set of theorems concerning the prime or composite character of Mersenne numbers.

Let P and Q be relatively prime integers and a, b are the roots of the quadratic

$$x^2 - Px + Q.$$

Then the Lucas functions are defined by

$$U_n = (a^n - b^n)/(a - b) \tag{12}$$

$$V_n = a^n + b^n \tag{13}$$

where n is a positive integer. It follows from (12) and (13) that U_n and V_n are integers for every n, and

$$U_o = 0 , \qquad U_1 = 1$$

$$U_{n+1} = PU_n - QU_{n-1} \tag{14}$$

$$V_o = 2 , \qquad V_1 = P$$

$$V_{n+1} = PV_n - QV_{n-1} \tag{15}$$

$$U_{2n} = U_n \cdot V_n \tag{16}$$

$$V_{2n} = V_n^2 - 2Q^n . \tag{17}$$

We will state the Lucas-Lehmer test for Mersenne numbers and prove its validity using only very simply principles of number theory. For P = 4, Q = 1, the equations (14) and (15) become

$$U_o = 0, \quad U_1 = 1, \quad U_{n+1} = 4U_n - U_{n-1} \tag{18}$$

$$V_o = 2, \quad V_1 = 4, \quad V_{n+1} = 4V_n - V_{n-1} \tag{19}$$

According to (18) and (19), we have then

$n =$	0	1	2	3	4	5	6	7	8 ...
$U_n =$	0	1	4	15	56	209	780	2911	10864...
$V_n =$	2	4	14	52	194	724	2702	10084	37634...

The following properties can be established :

(i) $$U_n = U_{n-2} + V_{n-1} \qquad (20)$$

Proof : Since a, b are the roots of the quadratic

$$x^2 - 4x + 1$$

thus

$$a + b = 4 \quad \text{and} \quad a \cdot b = 1$$

$$U_{n-2} + V_{n-1} = \frac{a^{n-2} - b^{n-2}}{a - b} + a^{n-1} + b^{n-1}$$

$$= \frac{a^{n-2} - b^{n-2} + a^n + ab^{n-1} - a^{n-1}b - b^n}{a - b}$$

$$= \frac{\cancel{a}^{n-2} - \cancel{b}^{n-2} + a^n - b^n + \cancel{abb}^{n-2} - \cancel{aba}^{n-2}}{a - b}$$

$$= \frac{a^n - b^n}{a - b} = U_n \,.$$

(ii) $$V_n = U_{n+1} - U_{n-1} \qquad (21)$$

Actually this equation is a rearranged form from (20).

(iii) $$U_{m+n} = U_m \cdot U_{n+1} - U_{m-1} \cdot U_n \qquad (22)$$

Proof :

$$U_m U_{n+1} - U_{m-1} U_n = \frac{a^m - b^m}{a - b} \times \frac{a^{n+1} - b^{n+1}}{a - b} - \frac{a^{m-1} - b^{m-1}}{a - b} \times \frac{a^n - b^n}{a - b}$$

$$= \frac{a^{m+n+1} - a^{n+1} b^m - a^m b^{n+1} + b^{m+n+1} - a^{m+n-1}}{(a - b)}$$

$$\frac{+ a^n b^{m-1} + a^{m-1} b^n - b^{m+n-1}}{(a - b)}$$

$$= \frac{1}{(a - b)^2} \left(\frac{a^{m+n}}{b} + \frac{b^{m+n}}{a} - \frac{a^{m+n}}{a} - \frac{b^{m+n}}{b} \right)$$

$$= \frac{a^{m+n} - b^{m+n}}{a - b} \left(\frac{1}{b(a - b)} - \frac{1}{a(a - b)} \right)$$

$$= \frac{a^{m+n} - b^{m+n}}{a - b} \left(\frac{a - b}{ab(a - b)} \right)$$

$$= \frac{a^{m+n} - b^{m+n}}{a - b}$$

$$= U_{m+n} .$$

For our choice of Q, the equation (17) becomes

$$V_{2n} = V_n^2 - 2 \tag{23}$$

To develop tests for primality of Mersenne numbers, we prove the following lemmas,

Lemma 1 :

$$U_q \equiv 3^{(q-1)/2} \quad (\bmod q) \tag{24}$$

$$V_q \equiv 4 \quad (\bmod q) \tag{25}$$

where q is an odd prime.

Proof : Since a and b are the roots of $x^2 - 4x + 1$, we have

$$a = 2 + \sqrt{3} \quad \text{and} \quad b = 2 - \sqrt{3}.$$

We can obtain an expression for U_q by substituting $(2 \pm \sqrt{3})^q$ in (12) the binomial expansion of a^q and b^q, we obtain

$$U_q = \sum_{k=0}^{(q-1)/2} \binom{q}{2k+1} 2^{q-2k-1} 3^k .$$

If we use the fact that $\binom{q}{2k+1}$ is a multiple of q except when $k = (q - 1)/2$, we find that

$$U_q \equiv 3^{(q-1)/2} \quad (\bmod q).$$

To prove (25), we expand (13) in the same way, thus

$$V_q = \sum_{k=0}^{(q-1)/2} \binom{q}{2k} 2^{q-2k+1} 3^k$$

In this case all the binomial coefficients except $k = 0$ are divisible by q. Hence,

$$V_q \equiv 2^{(q+1)} \quad (\bmod q).$$

Since

$$2^{q+1} = 2^{q-1+2} = 2^{q-1}2^2 = 4\cdot 2^{q-1},$$

we get $V_q \equiv 4 \pmod q$ using Fermat's Theorem.

Lemma 2 : For all primes $q>3$, either $U_{q+1} \equiv 0 \pmod q$ or $U_{q-1} \equiv 0 \pmod q$.

Proof : If $q \neq 3$, then Fermat's Theorem tells us that $3^{(q-1)} \equiv 1 \pmod q$, so that

$$(3^{(q-1)/2} + 1)(3^{(q-1)/2} - 1) \equiv 0 \quad (\bmod q)$$

therefore,

$$(3^{(q-1)/2}) \equiv \pm 1 \quad (\bmod q).$$

Since we have proved that

$$U_q \equiv 3^{(q-1)/2} \quad (\bmod q)$$

it follows that

$$U_q \equiv \pm 1 \quad (\bmod q).$$

The first case, when $U_q \equiv +1 \pmod q$ we have

$$U_{q-1} = 4U_q - U_{q+1} = 4U_q - V_q - U_{q-1}.$$

Since

$$U_q \equiv 1 \quad (\bmod q) \quad \text{and} \quad V_q \equiv 4 \quad (\bmod q)$$

it follows that

$$U_{q-1} \equiv -U_{q-1} \qquad (\bmod q)$$

hence

$$U_{q-1} \equiv 0 \qquad (\bmod q).$$

The second case, when $U_q \ (\bmod q) = -1$ we have

$$U_{q+1} = 4U_q - U_{q-1} = 4U_q + V_q - U_{q+1}$$

so

$$U_{q+1} \equiv 0 \qquad (\bmod q).$$

Now if N is any positive integer, and if $w = m(N)$ is the smallest positive integer such that $U_w \ (\bmod N) = 0$, we have $U_n \equiv 0 \ (\bmod N)$ if and only if n is a multiple of $m(N)$

where the number $m(N)$ is called the " rank of apparition " of N in the sequence (U_n).

Lemma 3 : If w is the rank of apparition of N, then $w \leq N+1$.

Proof : It is obviously sufficient to prove that N divides $U_{N+1} \cdot U_{N-1}$. From lemma 2, we have proved that

$$U_{N+1} \equiv 0 \qquad (\bmod N)$$

or

$$U_{N-1} \equiv 0 \qquad (\bmod N)$$

therefore N divides $U_{N+1} \cdot U_{N-1}$. Hence lemma 3 is proved.

We are now in a position to show three theorems.

Theorem 1 : If $N \pm 1$ is the rank of apparition of N, then N is a prime.

Proof : See [4].

Theorem 2 (Lucas-Lehmer) : The number $N = 2^p - 1$ is prime, where p is an odd prime, if and only if N divides the (p - 2)nd term of the sequence (L_n), i.e. $L_{p-2} \equiv 0 \pmod{N}$; where

$$L_o = 4, \qquad L_{n+1} \equiv (L_n^2 - 2) \pmod{N}.$$

Proof : Equation (23) and induction, we have

$$L_n \equiv V_{2^n} \pmod{N}.$$

(I) Proof of sufficiency :

Suppose that $L_{p-2} \pmod{N} = 0$, we have to show that N is a prime.

From (18) and (21) we have

$$U_{n+1} = 4U_n - U_{n+1} + V_n$$

or

$$2U_{n+1} = 4U_n + V_n.$$

Since V_n is always even and U_n has no factor in common with U_{n+1}, it follows that U_n and V_n can only have 2 as common factor, Therefore, if $L_{p-2} \equiv 0 \pmod{N}$, we have using (16)

$$U_{2^{p-1}} = U_{2^{p-2}} V_{2^{p-2}} = U_{2^{p-2}} L_{p-2} \equiv 0 \pmod{N}$$

but

$$U_{2^{p-2}} \equiv 0 \qquad (\bmod N)$$

and

$$U_{2^p} = U_{2^{p-1}} V_{2^{p-1}} \equiv 0 \qquad (\bmod N).$$

Now let m be any prime factor of N and let w be the rank of apparition of m, w must divide 2^p or 2^{p-1}, but it does not divide 2^{p-2}, hence $w = 2^p$ or $w = 2^{p-1}$.

When $w = 2^p$ we have by lemma 3

$$m \geqq w - 1 = 2^p - 1 = N.$$

Since m is a prime factor of N, thus m = N, and w is a rank of apparition of N. By Theorem 1, it follows that N is a prime.

When $w = 2^{p-1}$, we have

$$m \geqq w - 1 = 2^{p-1} - 1.$$

Since $2^{p-1} - 1$ does not divide $N = 2^p - 1$, this implies that $m \neq 2^{p-1} - 1$. Since m is a factor of N, and can't be greater than $2^p - 1$, m = N. This implies that N is a prime.

(II) Proof of necessity :

Suppose $N = 2^p - 1$ is a prime, we must show that $V_{2^{p-2}} \equiv 0 \ (\bmod N)$.

Since $V_{2^{p-1}} = (V_{2^{p-2}})^2 - 2$, if suffices to prove that $V_{2^{p-1}} \equiv -2 \ (\bmod N)$. Now

$$2 \pm .3 = ((\sqrt{2} \pm \sqrt{6})/2)^2$$

then since

$$V_n = a^n + b^n$$

so

$$V_{2^{p-1}} = (((\sqrt{2} + \sqrt{6})/2)^2)^{2^{p-1}} + (((\sqrt{2} - \sqrt{6})/2)^2)^{2^{p-1}}$$

$$= ((\sqrt{2} + \sqrt{6})/2)^{N+1} + ((\sqrt{2} - \sqrt{6})/2)^{N+1}$$

$$V_{2^{p-1}} = 2^{-n} \sum_{k=0}^{(N+1)/2} \binom{N+1}{2k} \sqrt{2}^{\,N+1-2k} \sqrt{6}^{\,2k}$$

$$= 2^{(1-N)/2} \sum_{k=0}^{(N+1)/2} \binom{N+1}{2k} 3^k .$$

Since N is prime,

$$\binom{N+1}{2k} = \binom{N}{2k} + \binom{N}{2k-1}$$

is divisible by N except when $k = 0$ and $k = (N + 1)/2$; hence

$$V_{2^{p-1}} \equiv 2^{(1-N)/2} (1 + 3^{(N+1)/2}) \quad (\bmod N)$$

$$2^{(N-1)/2} V_{2^{p-1}} \equiv 1 + 3^{(N+1)/2} \quad (\bmod N).$$

Since

$$2N + 2 = (N + 1) \cdot 2 = 2^p \cdot 2$$

$$= 2^{p+1} = (2^{(p+1)/2})^2$$

$$\equiv 2 \quad (\bmod N)$$

so

$$(2^{(N-1)/2}) = (2^{(p+1)/2})^{(N-1)}$$

by Fermat's Theorem,

$$2^{(N-1)/2} \equiv (2^{(p+1)/2})^{(N-1)} \equiv 1 \quad (\text{mod } N).$$

Since N (mod 3) = 1, and N (mod 4) = 3, so by a simple case of the law of quadratic reciprocity [6], [11], we get

$$3^{(N-1)/2} \equiv -1 \quad (\text{mod } N).$$

But

$$3^{(N+1)/2} = 3^{(N-1)/2} \cdot 3$$

thus,

$$1 \cdot V_{2^{p-1}} \equiv 1 + (-1) \cdot 3$$

$$\equiv -2 \quad (\text{mod } N).$$

This means

$$V_{2^{p-1}} \equiv -2 \quad (\text{mod } N)$$

so

$$V_{2^{p-2}} \equiv 0 \quad (\text{mod } N).$$

Thus, we have completed the proof of this theorem.

Theorem 3 (Lucas-Lehmer) : Let N be a positive integer relatively prime to $2P^2 - 8Q$, where P and Q are relatively prime integers. If U_{N+1} (mod N) = 0, and U_{m_i} (mod N) $\neq$ 0, where m_i = (N + 1)/p_i for each prime p_i dividing N + 1, then N is a prime.

The proof of this theorem is similar to that of Theorem 2. And this theorem provides a test for any given number.

The advantage of this method, of course, is that it employs the factorization of $N + 1$, rather than $N - 1$, so that in case the complete factorization of $N - 1$ is not obtainable, we may still be able to factor $N + 1$.

Testing Primality by the Converse of Fermat's Theorem [3], [5], [7]

In this section we will discuss the converse of Fermat's Theorem and its use as a method of testing for primality. This is one of the efficient and practical methods for investigating primality of a given number N. Therefore, it is the method which is chosen in this paper to be demonstrated by a computer program, in Chapter IV.

For a long time it has been known that the simple converse of Fermat's Theorem, which stated : If $a^{(N-1)} \equiv 1 \pmod{N}$, then N is a prime, is not true. We can show this by a simple example,

$$4^{14} \equiv 1 \pmod{15},$$

but obviously 15 is not a prime.

In 1876, Lucas first stated a true converse of Fermat's Theorem.

If $a^{(N-1)} \equiv 1 \pmod{N}$, but $a^q \not\equiv 1 \pmod{N}$ for all proper divisors of $(N - 1)$, then N is a prime.

Before stating the improved forms, we make the following definitions :

Definition 1 : If h is the smallest positive integer such that $a^h \equiv 1 \pmod N$, then a is said to belong to the exponent h modulo N, or h is the order of a $\pmod N$.

Definition 2 : The number of positive integers r, not exceeding N and coprime with N is denoted by $\phi(N)$ which is called " Euler ϕ function ", or totient of N.

<u>Theorem 1</u> : If for each prime divisor p_i of $(N - 1)$, there exists an a_i for which $a_i^{(N-1)} \pmod N = 1$ but $a_i^{(N-1)/p_i} \pmod N \neq 1$, then N is prime.

<u>Proof</u> : Let d_i be the order of $a_i \pmod N$, that is $a_i^{d_i} \equiv 1 \pmod N$, and let D be the least common multiple of all d_i's. Then $D \mid (N - 1)$ that is D divides $(N - 1)$. D does not divide $(N - 1)/p_i$, if it did, then $a_i^{(N-1)/p_i} \equiv 1 \pmod N$; and this is contradition to the hypothesis. Thus $D = N - 1$. Since

$$a_i^{\phi(N)} \equiv 1 \pmod N \qquad \text{(by Euler [6])},$$

$\phi(N)$ is a multiple of d_i for all p_i, and $\phi(N) \geq D$. But $\phi(N)<N-1$ when N is not prime. This implies that $\phi(N) = N - 1$, so N is prime.

The most laborious but an important part of the test is the determining of

$$a^{(N-1)} \equiv 1 \pmod N .$$

If $a^{(N-1)} = 1$ (mod N) is not true, then N is composite, and we can use any one of the methods described in the next chapter to obtain its prime factors. Otherwise, we need to go on to test

$$a^{(N-1)/p_i} \not\equiv 1 \quad (\bmod N).$$

There is a rapid " binary method ", for evaluating powers of a number, so the conditions $a^{(N-1)} \equiv 1$ (mod N) and $a^{(N-1)/p_i} \not\equiv 1$ (mod N) can be tested efficiently. Usually when we want to compute x^{16}, we simply start with x and then multiply fifteen times by x. But it is possible to obtain the same answer with only four multiplications by using the " binary method ".

In a binary machine, the binary representation of n which is the exponent of x will guide us through the following algorithm : Scanning from left to right,

Step 1 : Ignore the leading " 1 ".

Step 2 : Scan the next digit. If it is a " 1 ", first square x then multiply by x. Otherwise, equare x only.

Step 3 : Repeat step 2 until the end of the binary representation is reached.

Step 4 : Terminate the process.

For example $x^n = x^{23}$, thus n = 23 and its binary representation of n is 10111. We should successively compute x^2, x^4, x^5, x^{10}, x^{11}, x^{22}, x^{23}.

If we use a decimal number system, we can divide n by 2 to obtain a remainder of 1 or 0, i.e. the binary representation from right to left. The following procedure is the process of the right to left scan binary method based on a decimal number system :

Step 1 : We first set the initial values to start the process; $Y = 1$ and $Z = x$.

Step 2 : We divide n by 2, i.e. $Q = \lfloor n/2 \rfloor$, $R = n - n \cdot Q$. Then set $n = Q$; and at the same time determine whether or not the remainder R is zero. If R is zero, then go to step 5.

Step 3 : We multiply Z by Y; i.e. $Y = Z \cdot Y$.

Step 4 : Checking n. If $n = 0$, then this process terminates with Y as the answer.

Step 5 : At this point we set $Z = Z \cdot Z$, then go back to step 2.

As an example, x^{23} , of this process, the successive computation is shown below :

n	R	Y	Z
23		1	x
11	1	x	x
11	1	x	x^2
5	1	x^3	x^2
5	1	x^3	x^4
2	1	x^7	x^4
2	1	x^7	x^8
1	0	x^7	x^{16}
0	1	x^{23}	x^{16}

No matter if we use the left to right or the right to left binary method, we will have the same result. This method is usually not of importance for small values of n, say $n \leq 10$, unless the time for a multiplication is comparatively large. The left to right binary method is preferable, and a little bit faster than the right to left scan binary method. This method would make an efficient test for the conditions of $a^{(N-1)} \pmod N = 1$ and $a^{(N-1)/p} \pmod N \neq 1$.

Theorem 1 has some disadvantages when applied to a particular N. In the first place, the complete factorization of $N - 1$ must be known. Secondly, the number of factors which must be tried in order to show that $a^{(N-1)/p_i} \pmod N \neq 1$ may be large. These two disadvantages have been circumvented by Raphael M. Robinson [7]. He reduces the problem of complete factorization in the following manner.

<u>Lemma</u> : Suppose that $a^{(N-1)} \equiv 1 \pmod N$ and let $N = kq^n + 1$, where $q > k > 0$, $n > 0$, and q is prime. Then every prime factor p of N which does not divide $a^{(N-1)/q} - 1$ satisfies the congruence

$$p \equiv 1 \pmod{q^n}.$$

In particular, if $(a^{(N-1)/q} - 1, N) = 1$, then every prime factor p of N satisfies this congruence.

<u>Proof</u> : Suppose that a belongs to the exponent d (mod p), i.e. $a^d \equiv 1 \pmod p$; therefore, d divides ($p - 1$). Since p is a factor of N, it follows that d divides ($N - 1$) also. By the assumption that $N = kq^n + 1$, so $kq^n = N - 1$, this implies that d divides kq^n.

Since q is a prime, d does not divide ($N - 1$)/q, thus d does not divide kq^{n-1}, i.e. $d \nmid kq^{n-1}$. It follows that q^n divides d, i.e. $q^n \mid d$, therefore $q^n \mid (p - 1)$. Thus we have proved the congruence $p \equiv 1 \pmod{q^n}$ is true.

Theorem 2 : Suppose that $a^{(N-1)} \pmod N = 1$ where $N = kQ + 1$ and $0 < k < Q$, but $(a^{(N-1)/q} - 1, N) = 1$ for every prime factor q of Q. Then N is prime.

Proof : Suppose p and q are primes, and p is a factor of N, and q is factor of Q, therefore, p divides N and q^n divides Q. By the lemma, we have

$$p \equiv 1 \pmod{q^n}.$$

It follows that

$$p \equiv 1 \pmod{Q}.$$

Thus,

$$p^2 > Q^2 \geq (k + 1)Q > N.$$

That is, for every prime p which divides N we have $p^2 > N$. It follows that N is a prime.

The most striking advantage of Theorem 2 over Theorem 1 is that it does not require the complete factorization of N - 1.

Although the converse of Fermat's Theorem for testing primality of a given number N has disadvantages, it is still an efficient and practical method for testing primality. If N is in a special form such as the Mersenne numbers, or if the factors of N - 1 are too difficult to obtain, then another efficient method, which has been introduced in the section of "Testing Primality by the Lucas-Lehmer Method", should be used.

CHAPTER III

METHODS OF FACTORING

So far we have discussed in the previous two chapters tests for the primality of a given number. There has been no discussion of cases where the number has been tested and has been shown not to be a prime. In this chapter, we will concentrate on factoring a given composite number.

A composite number N can be expressed in the form

$$N = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_t^{r_t}$$

where the r's are positive integers and the p's are prime numbers. Several computational methods that will simplify the factoring problem will be discussed individually.

The Method of Factoring by Division [3]

This method makes use of an auxiliary sequence of "trial divisors"

$$d = 2, 3, 5, \ldots$$

which includes all prime numbers less than or equal to $N^{1/2}$.

For any composite number N the following algorithm will produce a complete factorization in the above form.

Step 1 : Set the initial index $i = 0$, $k = 1$, $p_i = 0$.

Step 2 : If $N = 0$, then terminate the algorithm.

Step 3 : Let $N_1 = \lfloor N/d_k \rfloor$, $Nr = N - N_1 \cdot d_k$.

Step 4 : If $Nr \neq 0$, go to step 7.

Step 5 : If $p_i = d_k$, increase r_i by 1. Set $N = N_1$ and go to step 2.

Step 6 : Increase i by 1, $p_i = d_k$, set $r_i = 1$ and $N = N_1$. Go to step 2.

Step 7 : If N_1 is greater than d_k, increase k by 1, go to step 3.

Step 8 : Increase i by 1, $p_i = N$ and $r_i = 1$, then terminate the process.

Example :

Suppose $N = 135723$, we immediately find that $N = 3 \cdot 45241$; hence $p_1 = 3$. Furthermore, $N = 45241 = 7 \cdot 6463$, so $p_2 = 7$. Next, $N = 6463 = 23 \cdot 281$; hence $p_3 = 23$. Since 281 is a prime, so $p_4 = 281$, such that the original N is a product of $3 \cdot 7 \cdot 23 \cdot 281$, i.e. $N = 3 \cdot 7 \cdot 23 \cdot 281$.

This method requires to have a table of all the necessary primes as part of the program. So if N is small, this method is workable and rather quick. But if N is large, we run into the problem : how big a table of primes would we requre ? Furthermore, this method requres a lot of iterations to generate all prime factors of N.

The Method of Factoring by a Difference of Squares [1], [3]

Evidently, the "factoring by division" is too slow to find large prime factors of N. The problem of finding large prime factors of a number N is solved if we can express N as $x^2 - y^2$, i.e. $N = x^2 - y^2$, which was used by Pierre de Fermat [3] . This factoring method is based on the familiar exclusion method of Gauss [11] in which the Diophantine equation

$$N = x^2 - y^2$$

is effectively replaced by the combinatorial problem of solving the set of simultaneous congruences $y^2 \equiv x^2 - N \pmod{E}$ with various "exclusion" moduli E which are primes. In this exclusion method, all quadratic nonresidues of E are excluded for solving the congruence $x^2 \equiv N \pmod{E}$. Quadratic residues and quadratic nonresidues are defined by :

If the congruence

$$x^2 \equiv N \qquad (\bmod\ E)$$

can be satisfied by some integer x, the number N is said to be a quadratic residue of the number E. Otherwise, N is said to be a quadratic nonresidue of E. A table of examples is given below to show the quadratic residues and nonresidues of primes not exceeding 19.

E = 3	r : 0 , 1	where r denotes residue
	n : 2	and n denotes nonresidue
E = 5	r : 0, 1, 4	
	n : 2, 3	
E = 7	r : 0, 1, 2, 4	
	n : 3, 5, 6	

E = 11	r : 0, 1, 3, 4, 5, 9
	n : 2, 6, 7, 8, 10
E = 13	r : 0, 1, 3, 4, 9, 10, 12
	n : 2, 5, 6, 7, 8, 11
E = 17	r : 0, 1, 2, 4, 8, 9, 13, 15, 16
	n : 3, 5, 6, 7, 10, 11, 12, 14
E = 19	r : 0, 1, 4, 5, 6, 7, 9, 11, 16, 17
	n : 2. 3, 8, 10, 12, 13, 14, 15, 18.

From the above table it is noticed that there are (p-1)/2 quadratic residues and (p-1)/2 nonresidues if p is an odd prime. When s moduli are used, only one x value in 2^s will generally survive the exclusion.

To illustrate this method let N = 11111. We may consider the following table :

E	if x mod E is
3	0, 1, 2
5	0, 1, 2, 3, 4
7	0, 1, 2, 3, 4, 5, 6
11	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

E	then x^2 mod E is
3	0, 1, 1
5	0, 1, 4, 4, 1
7	0, 1, 4, 2, 2, 4, 1
11	0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1

E	and $(x^2 - N)$ mod E is
3	1, 2, 2
5	4, 0, 3, 3, 0
7	5, 6, 2, 0, 0, 2, 6
11	10, 0, 3, 8, 4, 2, 2, 4, 8, 3, 0

If $x^2 - N$ is to be a perfect square y^2, it must have a quadratic residue mod E for all E. For example, if $x \bmod 3 \neq 0$, then for $N = 11111$, $(x^2 - N) \bmod 3 = 2$, so $x^2 - N$ cannot be a perfect square; therefore x must be a multiple of 3 whenever $N = 11111 = x^2 - y^2$. Thus, we have narrowed down the search for x to the table below :

$$\left.\begin{array}{l} x \bmod 3 = 0 \\ x \bmod 5 = 0,\ 1,\ \text{or } 4 \\ x \bmod 7 = 2,\ 3,\ 4,\ \text{or } 5 \\ x \bmod 11 = 1,\ 2,\ 4,\ 7,\ 9,\ \text{or } 10 \end{array}\right\} \qquad (26)$$

In this case, we must have $x \geq \lceil\sqrt{N}\rceil = \lceil\sqrt{11111}\rceil = 106$. This notation of $\lceil N \rceil$, called the " ceiling " of N, had the value of the least integer greater than or qual to N. It is easy to verify that the first values of $x \geq 106$ which satisfies all of the conditions in (26) is $x = 144$. But $144^2 - 11111 = 9625$ is not a square. The first value of $x > 144$ which satisfies both (26) and $x^2 - 11111 = y^2$ is $x = 156$. So we have the desired solution $x = 156$ and $y = \sqrt{x^2 - N} = 115$. Since $N = x^2 - y^2 = (x - y)(x + y) = (156 - 115)(156 + 115) = 41 \cdot 271$, thus the two factors of N are 41 and 271.

The modular method just described is called a " sieve procedure ". Since we can imagine passing all integers x through a " sieve " for which only those values with $x \bmod 3 = 0$ come out, then sifting these numbers through another sieve which allows only numbers with $x \bmod 5 = 0, 1$, or 4 to pass, etc. Each sieve by itself will remove about half of the remaining values; and when we sieve with respect to moduli which are relatively prime in pairs, each sieve is independent of the other.

When the " sieve method " is employed to factor a given odd composite number N, we need to prepare a " sieve table "

$$S\ i,j = \begin{cases} 1 & \text{if } j^2 - N = y^2 \ (\bmod E_i) \text{ has a solution } y \\ 0 & \text{otherwise} \end{cases}$$

where the moduli E_i are prime and $0 \leq j \leq E_i$. Only for the values of x which lead to a "1" in the sieve table need to be examine whether or not $x^2 - N$ is a square. This method is most successful when N has two factors that are close together. Therefore, this is one of the efficient methods to find prime factors of N.

The Method of Factoring by Addition and Subtraction [3]

Another method to find large factors is also base on Fermat's method, however,

$$N = x^2 - y^2$$

is obtained without using any division.

Assume that N is an odd composite number, i.e. $N = U \cdot V$. If we let

$$x = (U + V)/2, \qquad y = (V - U)/2$$

then

$$N = x^2 - y^2 = (U + V)^2/4 - (V - U)^2/4$$
$$= U V$$

where $0 \leq y < x \leq N$.

Let a, b, r correspond respectively to $2x + 1$, $2y + 1$, $x^2 - y^2 - N$. Then

$$x = \frac{a - 1}{2} , \qquad y = \frac{b - 1}{2}$$

it follows that

$$U = x - y = \frac{a - 1 - b + 1}{2} = \frac{a - b}{2}$$

and

$$V = x + y = \frac{a - 1 + b - 1}{2} = \frac{a + b - 2}{2} .$$

In summary, the procedure for this method is shown in the following steps.

Step 1 : We extract the square root of N, and let $a = 2\lfloor\sqrt{N}\rfloor + 1$, and $b = 1$, $r = \lfloor\sqrt{N}\rfloor^2 - N$.

Step 2 : If r is zero or negative, then go to step 4.

Step 3 : Decrease r by b and increase b by 2, then go back to step 2.

Step 4 : Checking r. If r is zero, this means that we have the desired solution a, b which satisfy

$$U = \frac{a - b}{2} \quad , \qquad V = \frac{a + b - 2}{2} \ .$$

Otherwise, we go to the next step.

Step 5 : We increase r by a and a by 2, then go to step 3.

According to the above procedure for N = 9401, the computation proceeds as follows :

a	b	r	a	b	r	a	b	r
193	1	-185	197	13	167	197	29	7
195	1	8	197	15	154	197	31	-22
195	3	7	197	17	139	199	31	175
195	5	4	197	19	122	199	33	144
195	7	-1	197	21	103	199	35	111
197	7	194	197	23	82	199	37	76
197	9	187	197	25	59	199	39	39
197	11	178	197	27	34	199	41	0

Thus $9401 = \frac{199 - 41}{2} \cdot \frac{199 + 41 - 2}{2} = 79 \ 119.$

While for large N this calculation can only be executed efficientely with a computer.

The Method of Factoring by Final Digit [8]

This method has been discussed in detail for testing primality of a given number N, (see Chapter II). As we recall, if no prime factors could be found, the given number N is a prime number. If its prime factors are found by this method, the given number is a composite number. Obviously enough, this prime factor finding method is also a feasible method for factoring a given number.

CHAPTER IV

EXAMPLE

An example of a program written in the Fortran IV language is shown in this chapter in order to demonstrate the feasibility of automating the testing for primality and, if necessary, to find the prime factors of a given number N. For practical reasons, the converse of Fermat's theorem is employed here as the method for testing the primality. When the given number, however, is recognized as composite; the program continues to find the factors by the addition and substraction method.

The procedure of this program is as follows :

Step 1 : Generate a suitable table of primes.

Step 2 : Check by the method of division, if N has any prime factors within the range of the table in step 1. If it does, then we divide out those factors to reduce N to a number whose prime factors all exceed the largest prime in the table.

Step 3 : From step 2 we know N must be relatively prime to the small primes, for instance, 3. So we test if N is prime by computing $3^{(N-1)}$ (mod N). If $3^{(N-1)}$(mod N) $\neq 1$, N is not prime, then go to step 5.

Step 4 : Find the factors of $N - 1$; in other words, start recursively at step 2, with N replaced by $N - 1$, and come back to this point of the procedure when $N - 1$ has been completely factored. Then for each prime factor p_i of $N - 1$ find a value of $a = 2, 3, 5, 7, 11, \ldots$ such that

$a^{(N-1)}$ (mod N) = 1, but $a^{(N-1)/p_i}$ (mod N) $\neq$ 1. Continue this process until either finding $a^{(N-1)}$ (mod N) $\neq$ 1, or finding some p_i dividing N - 1 such that $a^{(N-1)/p_i}$ (mod N) = 1 for all primes a within the range of the table in step 1, then go to step 5. Otherwise, N is a prime.

Step 5 : Use the method of factoring by addition and substraction to find the prime factors.

```
          COMMON /S/IFACT(500),NPRIME(500),LS
          DIMENSION NO(20),LT(20)
C         THIS ROUTINE IS TESTING THE PRIMALITY OF A GIVEN
C         NUMBER N BY THE CONVERS  OF FERMAT'S THEOREM.
          ITEM=100
          K=1
          I=2
          NPRIME(1)=2
          CALL GPRIME(I,K,ITEM)
   15     READ(5,7,END=100) N
    7     FORMAT(I10)
          WRITE(6,10) N
   10     FORMAT(//5X,'*****  THE INPUT OF N IS .',I10,2X,'*****')
          IT=1
          LIMIT=100
          II=1
          NO=N
          CALL CAST(LIMIT,II,NO)
          ISW=II-1
          IF(LIMIT .EQ. 0) GO TO 101
          N=NO
          N2=NO
          NC(IT)=N
   20     LT(IT)=II
          NO=NO-1
          NY=2
          LZ=3
          NA=N2
          CALL DIGIT(NA,MA)
          LS=MA
          CALL TEST(NO,N2,LZ,NY)
          IF(LZ .NE. 1) GO TO 110
          WRITE(6,25) N2
   25     FORMAT(/5X,'NOW WE TEST WHETHER OR NOT ',I10,' IS A PRIME')
          WRITE(6,30)
   30     FORMAT(//10X,'A',10X,'P',10X,'A**(N-1)/P MOD N',
         15X,'A**(N-1) MOD N')
          LIMIT=100
          CALL CAST(LIMIT,II,NO)
          IF(LIMIT .EQ. 0) GO TO 51
          IT=IT+1
          NC(IT)=NO
          N2=NO
          GO TO 20
   51     M=LT(IT)
   52     KK=1
   53     NY=NPRIME(KK)
          LZ=NY
          NO=(N2-1)/IFACT(M)
          CALL TEST(NO,N2,LZ,NY)
          NO=N2-1
```

```
      L1=L2
      L2=NY
      CALL TEST(NC,N2,L2,NY)
      WRITE(6,40) NY,IFACT(M),L1,L2
   40 FORMAT(8X,I10,1X,I10,12X,I10,15X,I10)
      IF(L1 .EQ. 1) GO TO 70
      M=M+1
      IF(M .GE. II) GO TO 70
      GO TO 52
   70 KK=KK+1
      IF(KK .LE. 100) GO TO 53
      LIMIT=100
      NC=N2
      M1=II
      CALL CAST(LIMIT,II,NC)
      IF(LIMIT .EQ. 0) GO TO 75
      WRITE(6,105) N2
  105 FORMAT(5X,I12,'COULD BE A PRIME')
      GO TO 15
   75 IF(IT .LE. 1) GO TO 30
      WRITE(6,60) N2
   60 FORMAT(/5X,'THE NUMBER OF ',I10,' IS A PRIME')
      II=LT(IT)
      IFACT(II)=N2
      II=II+1
      IT=IT-1
      N2=NC(IT)
      N4=N2
      CALL DIGIT(N4,M4)
      L5=M4
      GO TO 51
   80 IF(ISW .EQ. 0) GO TO 85
      ISW=ISW+1
      IFACT(ISW)=N2
  101 WRITE(6,90)
   90 FORMAT(5X,'THE GIVEN NUMBER IS NOT A PRIME,THE FACTORS ARE')
      WRITE(6,91) (IFACT(L),L=1,ISW)
   91 FORMAT(10X,10(I10,1X)/)
      GO TO 15
   85 WRITE(6,92)
   92 FORMAT(5X,'THE GIVEN NUMBER IS A PRIME')
      GO TO 15
  110 NO=NO+1
      CALL FBAS(NC,II)
      IF(II .GT. 1) GO TO 51
      ISW=II-1
      GO TO 101
  100 STOP
      END
```

```
      SUBROUTINE GPRIME(I,K,ITEM)
      COMMON /S/IFACT(500),NPRIME(500),LS
C     THIS ROUTINE IS GOING TO GENERATE A TABLE OF PRIMES UP
C     TO A SUITABLE RANGE BY USING THE FORMS OF 4N+1 AND 4N-1
      DIMENSION NT(2)
    3 NTO=4*K
      J=1
      NT(J)=NTO-1
    5 KK=1
    7 NQ=NT(J)/NPRIME(KK)
      NR=NT(J)-NQ*NPRIME(KK)
      IF(NR .EQ. 0) GO TO 12
      NSQURE=NPRIME(KK)**2
      IF(NT(J) .LE. NSQURE) GO TO 10
      KK=KK+1
      GO TO 7
   10 NPRIME(I)=NT(J)
      I=I+1
   12 IF(J .NE. 1) GO TO 15
      J=2
      NT(J)=NTO+1
      GO TO 5
   15 IF(I .GT. ITEM) GO TO 20
      K=K+1
      GO TO 3
   20 WRITE(6,90) (NPRIME(J),J=1,ITEM)
   90 FORMAT(1H,5X,5I10/)
      RETURN
      END
```

```
      SUBROUTINE CAST(LIMIT,II,NO)
      COMMON /S/IFACT(500),NPRIME(500),LS
C     THIS ROUTINE IS TO CAST OUT THOSE FACTORS WITHIN
C     THE RANGE OF THE GENERATED TABLE OF PRIMES.
      IS=II
      KK=1
   10 NQ=NO/NPRIME(KK)
      NR=NO-NQ*NPRIME(KK)
      IF(NR .EQ. 0) GO TO 20
      NSQURE=NPRIME(KK)**2
      IF(NO .LE. NSQURE) GO TO 30
      KK=KK+1
      IF(KK .LE. LIMIT) GO TO 10
      GO TO 70
   20 IFACT(II)=NPRIME(KK)
      II=II+1
      NO=NQ
      GO TO 10
   30 LIMIT=0
      IFACT(II)=NO
```

```
      II=II+1
      GO TO 75
   70 LIMIT=1
   75 RETURN
      END


      SUBROUTINE MULT(IZ,NZ,MULTF,LZ,N2)
      COMMON /S/IFACT(500),NPRIME(500),LS
      DIMENSION NZ(15),MULTF(15),NW(30)
C     THIS ROUTINE IS DOING THE ' MULTIPLICATION' FOR LZ*LZ, IF LZ IS
C     BIGER THAN THE 10**5, AND THE ' MODULUS' JOB.
      J=1
      MB=IZ
      M1=0
      LK=0
    5 LK=LK+1
      NT=0
      M=IZ
   10 NPRO=NZ(M)*MULTF(MB)
      IF(NT .NE. 0) NPRO=NPRO+NT
      IF(LK .EQ. 1) GO TO 15
      IF(J .GT. M1) GO TO 15
      NPRO=NPRO+NW(J)
   15 NT=NPRO/10
      NW(J)=NPRO-NT*10
      J=J+1
      M=M-1
      IF(M .GT. 0) GO TO 10
      IF(NT .EQ. 0) GO TO 25
      NW(J)=NT
      M1=J
      GO TO 27
   25 M1=J-1
   26 IF(J .EQ. 1) NW(J)=0
   27 J=LK+1
      MB=MB-1
      IF(MB .GT. 0) GO TO 5
      MA=M1
      M=MA
      IF(MA .GT. LS) M=LS
      NP=0
      DO 95 L=1,M
      NP=NP*10+NW(MA)
   95 MA=MA-1
   35 IF(NP .GE. N2) GO TO 90
      IF(MA .EQ. 0) GO TO 100
      NP=NP*10+NW(MA)
      MA=MA-1
      GO TO 35
   90 NK=NP/N2
      NP=NP-NK*N2
```

```
      GO TO 95
  100 LZ=NP
      RETURN
      END
```

```
      SUBROUTINE TEST(NC,N2,LZ,NY)
C     THIS ROUTINE IS USING BINARY METHOD TO EVALUATE POWERS, AND
C     TESTING A**(N-1) MOD N AND A**(N-1/F MOD N
      COMMON /S/IFACT(500),NPRIME(500),LS
      K1=1
      DO 100 M=1,35
      N1=FLD(M,1,NC)
      IF(N1 .EQ. 0) GO TO 15
      IF(K1 .GE. 2) GO TO 10
    5 K1=K1+1
      GO TO 100
   10 NSW=1
      GO TO 20
   15 IF(K1 .LE. 1) GO TO 100
      NSW=0
   20 IF(LZ .GT. 10**5) GO TO 80
      LZ=LZ**2
   25 IF(LZ .GE. N2) GO TO 30
      GO TO 40
   30 N3=LZ/N2
      LZ=LZ-N3*N2
   40 IF(NSW .EQ. 0) GO TO 5
      LZ=LZ*NY
      NSW=0
      GO TO 25
   80 CALL TRY(LZ,N2)
      GO TO 40
  100 CONTINUE
      RETURN
      END
```

```
      SUBROUTINE TRY(LZ,N2)
      COMMON /S/IFACT(500),NPRIME(500),LS
      DIMENSION NZ(15),MULTP(15)
      N4=LZ
      CALL DIGIT(N4,M4)
      I2=M4
      DO 20 L=1,I2
      M4=M4-1
      NZ(L)=LZ/(10**M4)
      MULTP(L)=NZ(L)
```

```
   20 LZ=LZ-NZ(L)*(10**MA)
      CALL MULT(IZ,NZ,MULTIP,LZ,N2)
      RETURN
      END
```

```
      SUBROUTINE DIGIT(NA,MA)
      MA=0
   10 NQD=NA/10
      IF(NQD .EQ. 0) GO TO 15
      MA=MA+1
      NA=NQD
      GO TO 10
   15 NRD=NA-NQD*10
      IF(NRD .NE. 0) MA=MA+1
      RETURN
      END
```

```
      SUBROUTINE FEAS(NO,II)
      COMMON /S/ IFACT(500),NPRIME(500),LS
C     THIS ROUTINE IS TO FIND THE PRIME FACTORS OF N BY
C     THE METHOD OF ADDITION AND SUBSTRACTION.
      LX=SQRT(NO)
      LY=1
      LR=LX**2-NO
      LX=2*LX+1
   20 IF(LR .LE. 0) GO TO 40
   30 LR=LR-LY
      LY=LY+2
      GO TO 20
   75 IFACT(II)=NO
      II=II+1
      GO TO 72
   40 IF(LR .EQ. 0) GO TO 60
      LR=LR+LX
      LX=LX+2
      GO TO 30
   60 N3=(LX-LY)/2
      N4=(LX+LY-2)/2
      NO=N3
      LSW=0
   70 LIMIT=100
      CALL CASI(LIMIT,II,NO)
      IF(LIMIT .EQ. 1) GO TO 75
   72 IF(LSW .NE. 0) GO TO 80
      NO=N4
      LSW=LSW+1
      GO TO 70
   80 RETURN
      END
```

EXAMPLE OUTPUT

TABLE OF PRIMES

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97
101	103	107	109	113
127	131	137	139	149
151	157	163	167	173
179	181	191	193	197
199	211	223	227	229
233	239	241	251	257
263	269	271	277	281
283	293	307	311	313
317	331	337	347	349
353	359	367	373	379
383	389	397	401	409
419	421	431	433	439
443	449	457	461	463
467	479	487	491	499
503	509	521	523	541

*****   THE INPUT OF N IS 1653701519   *****

NOW WE TEST WHETHER OR NOT 1653701519 IS A PRIME

A	P	A**(N-1)/P MOD N	A**(N-1) MOD N
2	2	1	1
3	2	1	1
5	2	1	1
7	2	1653701518	1
2	7	765403525	1
2	19	332950669	1
2	23	1154237310	1
2	137	373782156	1
2	1973	490790919	1

THE GIVEN NUMBER IS A PRIME

*****   THE INPUT OF N IS   7432339871   *****

NOW WE TEST WHETHER OR NOT   2337949 IS A PRIME

A	P	A**(N-1)/P MOD N	A**(N-1) MOD N
2	2	2337948	1
2	2	2337948	1
2	3	1	1
3	3	194956	1
2	3	1	1
3	3	194956	1
2	101	1688071	1
2	643	1314576	1

THE GIVEN NUMBER IS NOT A PRIME,THE FACTORS ARE
11   17   17   2337949

*****   THE INPUT OF N IS   29087881   *****
THE GIVEN NUMBER IS NOT A PRIME,THE FACTORS ARE
2731   10651

```
*****  THE INPUT OF N IS  2147483647  *****

NOW WE TEST WHETHER OR NOT 2147483647 IS A PRIME
```

A	P	A**(N-1)/P MOD N	A**(N-1) MOD N
2	2	1	1
3	2	2147483646	1
2	3	1	1
3	3	1	1
5	3	1513477735	1
2	3	1	1
3	3	1	1
5	3	1513477735	1
2	7	1	1
3	7	1752599774	1
2	11	1	1
3	11	298192073	1
2	31	4096	1
2	151	1	1
3	151	556513938	1
2	331	1	1
3	331	272122069	1

THE GIVEN NUMBER IS A PRIME

BIBLIOGRAPHY

1. Dickson, L. E., History of Theory of Numbers, V. 1, New York G. E. Stechert & Co., 1934.
2. Elston, F. G., A Generalization of Wilson's Theorem, Math. Mag. 30(1957), pp. 159 - 162.
3. Knuth, D. E., Seminumerical Algorithms - the Art of Computer Programming, V. 2, Addison-Wesley publishing Company, 1969.
4. Lehmer, D. H., An Extended Theory of Lucas' Function, Ann. of Math., V. 31, 1930, pp. 419 - 448.
5. Lehmer, D. H., Tests for Primality by the Converse of Fermat's Theorem, Bull. Amer. Math. Soc., V. 33, 1927, pp. 327 - 340.
6. Niven, I. and Zuckerman, H. S., An Introduction to the Theory of Numbers, New York and London, John Wiley & Sons, Inc., 1960.
7. Robinson, R. M., The Converse of Fermat's Theorem, Amer. Math. Monthly, V. 64, 1957, pp. 703 - 710, MR 20 #4520.
8. Rumney, M., A Simple Device for Testing Primality, Math. Gaz., 41(1957), p. 121.
9. Shanks, D., Solved and Unsolved Problems in Number Theory, V. 1, Washington, Spartan Books, 1962.
10. Stewart, B. M., Theory of Numbers, 2nd ed., New York, Macmillan, 1964.
11 Uspensky, J. V. and Heaslet, M. A., The Elementary Number Theory, McGraw - Hill Book Company, Inc., 1939.