AN ABSTRACT OF THE THESIS OF

Omar Mahmoud Hamad for the **Master of Science**

in **Mathematics** presented on **May 1994**

Title: **Integer Factorization**

Abstract approved: Essam Abotteen

The aim of this study is to discuss some of the old integer factoring methods, as well as some of the more recent methods that utilize the Kraitchik scheme. In the first chapter, the statement of the factoring problem is presented. A review of some concepts of elementary number theory and some details about continued fractions that are needed in later chapters are given. In chapter two, some of the old factoring methods, Trial Division, Legendre's, Gauss' and Fermat's factoring methods, are discussed. In chapter three, the Continued Fraction method is presented. In chapter four, the Quadratic Sieve method with some of its improvements are presented. In chapter five, the Number Field Sieve method is presented.

INTEGER FACTORIZATION

A Thesis

Presented to

The Division of

Mathematics and Computer Science

EMPORIA STATE UNIVERSITY

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

---

by

Omar Mahmoud Hamad

May 1994

L. Scott

Approved for the Major Division

Faye N. Vowell

Approved for the Graduate Council

ACKNOWLEDGEMENTS

In the Name of Allah, Most Gracious, Most Merciful, without Whose help and guidance this work would not been accomplished.

I would like to express my sincere thanks and my deep appreciation to my advisor Dr. Essam Abotteen for his expert guidance, assistance, and encouragement in conducting this research.

I express my gratitude to my committee, Dr. B. Dawson, Dr. C. Cornell, and Dr. L. Fosnaugh.

My thanks goes also to my father, mother, brothers, and sisters for their prayers and support.

Finally, a very special thanks and love goes to my dearest wife Abla, and my wonderful children Mahmoud, Mohammed, Nour, and Alaa, for their limitless patience and love.

Contents

List of Tables

Chapter 1

Introduction

Until the last decade, the centuries-old problem of factoring large integers was of interest mainly to specialists. Worldwide interest in factoring integers increased dramatically in 1978, when Rivest, Shamir and Adleman [21] published their public key cryptosystem. The security of this system relies on the fact that some large integers are hard to factor. With the advent of powerful computing tools and numerous advances in mathematics computer science and cryptography, computational number theory in general and factoring large integers in particular has become an important subject in its own right. The aim of this paper is to give an overview of some of the factoring methods known today, with an emphasis on those factoring methods that utilize the Kraitchik factoring scheme.

1.1 Statement of the Factoring Problem:

The factoring problem can be simply stated as follows: Given an integer $N > 1$ which is not a prime, find integers a and b both greater than 1, such that $N = a * b$. This process may be further applied to a and b, their factors, and so on, obtaining in the end the complete prime factorization of N.

There are really two problems here. The first problem is the determination that N is not a prime, and the second is the calculation of a and b. In this paper, we are concerned with the second problem. For readers interested in the first problem and the determination of the primeness of an integer (i.e. the problem of primality testing), we recommend few references to the enormous literature [1], [3], and [20].

Given that we know that N is composite, how can we proceed to find the factors of N? This seems a much harder problem than that of showing that N is composite. Everyone knows an algorithm on input of an integer $N > 1$ either proves N is prime or produces the complete prime factorization of N when N is composite. This is the trial division algorithm. The trial division algorithm consists of making trial divisions of the number N by all primes less than or equal to $\sqrt{N}$. In the worst case, this is an $O(\sqrt{N})$ algorithm and, when N is large, means that it could take a very long time to execute. For example, we might use the trial division algorithm on a computer that can do one million trial divisions per second to determine if a given integer N is prime or composite. If N is a prime near 10^{40}, the running time would be about one million years. If N is a prime near 10^{50}, the age of the universe would not suffice. Thus in factoring large integers, the main concern is in reducing the running time of the factoring method and developing new factoring methods with lower running times. Several ingenious ways to speed up the factoring process have been discovered.

REMARKS CONCERNING THE EXAMPLES GIVEN IN THE PAPER:

The factoring methods presented in this paper are employed to factor large integers - in some cases over a 100 decimal digit integers using high speed computers. However, in this paper the examples presented to illustrate the different factoring methods are of small integers so that calculations can be carried out by hand or with a calculator.

1.2 Review of Elementary Number Theory

The object of this introductory section is to provide the readers with a short account of the concepts from elementary number theory that we need in later chapters. Most of the results in this section are given without proof. The proofs can be found in most elementary number theory books, such as [22], [23].

<u>DEFINITIONS</u>

1. An integer $P > 1$ is called a <u>prime</u> number, or simply a prime, if its only positive divisors are 1 and P.
2. An integer which is not a prime is called a <u>composite number</u>.
3. If a and b are integers, we say that a <u>divides</u> b if

there is an integer c such that b = ac. If a divides b we denote this by $a|b$. We write $a\nmid b$ to indicate that b is not divisible by a.

4. Let a and b be given integers, where at least one of them is different from zero. The <u>greatest common divisor</u> of a and b, denoted by gcd (a, b), is the positive integer d satisfying:

   (a) $d|a$ and $d|b$

   (b) if $c|a$ and $c|b$, then $c \le d$.

5. The <u>least common multiple</u> of two nonzero integers a and b, denoted by lcm [a, b], is the positive integer m satisfying

   (a) $a|m$ and $b|m$

   (b) if $a|c$ and $b|c$ with $c > 0$, then $m \le c$.

6. Let n be a fixed positive integer. Two integers a and b are said to be <u>congruent</u> modulo n, symbolized by $a \equiv b$ (mod n), if n divides the difference a - b. That is if a - b = kn for some integer k.

7. Let P be an odd prime and a an integer such that gcd (a, P) = 1. If the congruence $x^2 \equiv$ a (mod P) has a solution, then a is said to be a <u>quadratic residue</u> of P. Otherwise a is called a quadratic nonresidue of P.

8. Let p be an odd prime and gcd (a, p) = 1, then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{if a is quadratic residue of p} \\ -1 & \textit{if a is quadratic nonresidue of p} \end{cases}$$

THEOREMS (WITHOUT PROOFS)

Theorem 1: If a, b, c, d, k and m are integers where m > 0, k > 0, such that $a \equiv b$ (mod m), and $c \equiv d$ (mod m), then

(1) $a + c \equiv b + d \pmod m$

(2) $a - c \equiv b - d \pmod m$

(3) $ac \equiv bd \pmod m$

(4) $a^k \equiv b^k \pmod m$

(5) $f(a) \equiv f(b) \pmod m$ where f(x) is a polynomial with integer coefficients.

Theorem 2: If a, b, c, and m are integers such that m > 0. d = *gcd* (c, m) and $ac \equiv bc \pmod m$, then $a \equiv b \pmod{\frac{m}{d}}$.

Theorem 3: If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., and $a \equiv b \pmod{m_k}$, where a, b, m_1, m_2, m_k are integers with m_1, m_2,..., m_k are positive then $a \equiv b$ (mod lcm $[m_1, m_2, \ldots, m_k]$).

Theorem 4 (Euler's Criterion): Let p be an odd prime and let a be a positive integer not divisible by p. Then $\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \pmod p$.

Theorem 5: Let p be an odd prime and let a and b be integers relatively prime to p, then

(1) if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$

(4) $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$

Theorem 6 (Law of Quadratic Reciprocity): If p and q are distinct odd primes and either p or q is $\equiv 1 \pmod{4}$, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

If both p and q are $\equiv 3 \pmod{4}$, then

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Theorem 7 (The Chines Remainder Theorem): Let m_1, m_2, ..., m_r be pairwise relatively prime positive integers. Then the system of congruences

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2}.$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}.$$

has a unique solution modulo $M = m_1.m_2...m_r$.

Theorem 8 (The Euclidean algorithm): Let $r_0 = a$ and $r_1 = b$ be integers such that $a \geq b > 0$. If the division algorithm is successively applied to obtain $r_j = r_{j+1} q_{j+1} + r_{j+2}$ with

$0 < r_{j+2} < r_{j+1}$ for $j = 0, 1, 2, \ldots, n-2$ and $r_{n+1} = 0$ then gcd $(a, b) = r_n$, the last nonzero remainder.

Example: To find gcd (252,198), we apply the Euclidean algorithm as follows:

$$252 = 198 \bullet 1 + 54$$

$$198 = 54 \bullet 3 + 36$$

$$54 = 36 \bullet 1 + 18$$

$$36 = 18 \bullet 2$$

18 is the last nonzero remainder, hence gcd (252,196) = 18.

Fast Exponentiation (or modular exponentiation): We apply this algorithm to congruences involving large powers of integers. An example would be finding the least positive residue of b^N mod m when both m and N are very large. To illustrate this algorithm, we proceed as follows: Let m, b, N be positive integers. To compute b^N mod m, where N and m are large integers; we first express the exponent N in binary notation as $N = (a_k\, a_{k-1} \ldots a_1\, a_0)_2$. Then we find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, by successively squaring and reducing modulo m. Finally, we multiply the least positive residues modulo m of b^{2^j} for those a_j with $a_j = 1$, reducing modulo m after each multiplication.

<u>Example</u>: Find the least positive residue of 2^{644} mod 645.

Solution: First we express 644 in binary notation

$$644 = 2 \cdot 322 + 0$$
$$322 = 2 \cdot 161 + 0$$
$$161 = 2 \cdot 80 + 1$$
$$80 = 2 \cdot 40 + 0$$
$$40 = 2 \cdot 20 + 0$$
$$20 = 2 \cdot 10 + 0$$
$$10 = 2 \cdot 5 + 0$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$
$$1 = 2 \cdot 0 + 1$$

Therefore, $(644)_{10} = (1010000100)_2 =$ $1 \cdot 2^9 + 0 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$. We have here b = 2, N = 644, m = 645. We find the least positive residue of b, b^2, ..., b^{2^k} modulo N by squaring and reducing mod m as follows

$$2 \equiv 2 \pmod{645}$$
$$2^2 \equiv 4 \pmod{645}$$
$$2^4 \equiv 16 \pmod{645}$$

$$2^8 \equiv 256 \pmod{645}$$

$$2^{16} \equiv (2^8)^2 \equiv 391 \pmod{645}$$

$$2^{32} \equiv (2^{16})^2 \equiv 16 \pmod{645}$$

$$2^{64} \equiv 256 \pmod{645}$$

$$2^{128} \equiv 391 \pmod{645}$$

$$2^{256} \equiv 16 \pmod{645}$$

$$2^{512} \equiv 256 \pmod{645}.$$

We multiply the least positive residues modulo 645 of 2^{2^j} for these j with $a_j = 1$. This gives $2^{644} =$ $2^{2^9} \bullet 2^{2^7} \bullet 2^{2^4} = 2^{512+128+4} = 2^{512} \bullet 2^{128} \bullet 2^4 \equiv 256.391.16 \equiv 1 \pmod{645}$.

1.3 Continued Fractions:

This section gives a brief introduction to continued fractions. We will restrict the discussion of this fascinating subject to only those features which will be needed in the paper.

A continued fraction is an expression of the form

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cfrac{a_4}{b_4 + \dots}}}}$$

where a_1, a_2, ... and b_1, b_2, ... are real (or complex) numbers, and the number of terms may be finite or infinite.

The numbers a_j are called partial numerators and the numbers b_i (apart from b_0) are called partial denominators (or partial quotients).

A much more convenient way of writing a continued fraction is $b_0 + \frac{a_1}{b_1 +}\ \frac{a_2}{b_2 +}\ \frac{a_3}{b_3 +}\cdots$.

If all partial numerators a_i are equal to 1, and if b_0 is an integer and all partial denominators b_i are positive integers, the continued fraction is said to be simple or regular. A simple continued fraction would have the form

$$b_0 + \frac{1}{b_1 +}\ \frac{1}{b_2 +}\ \frac{1}{b_3 +}\cdots.$$

Another convenient way to write the simple continued fraction above is

$$[b_0, b_1, b_2, \ldots].$$

Let us consider the finite simple continued fraction

$$x = 2 + \frac{1}{3+}\ \frac{1}{4+}\ \frac{1}{2}.$$

$$= 2 + \frac{1}{3} + \frac{1}{4 + \frac{1}{2}}$$

$$= 2 + \frac{1}{3 + \frac{1}{\frac{9}{2}}}$$

$$= 2 + \cfrac{1}{3 + \cfrac{2}{9}} = 2 + \cfrac{1}{\cfrac{29}{9}} = 2 + \frac{9}{29}$$

$$= \frac{67}{29}.$$

Thus, the continued fraction represents the rational number $\frac{67}{29}$. Conversely, let $x = \frac{24}{19}$.

Then, $\frac{24}{19} = 1 + \frac{5}{19} = 1 + \cfrac{1}{\cfrac{19}{5}}$

$$\frac{19}{5} = 3 + \frac{4}{5} = 3 + \cfrac{1}{\cfrac{5}{4}}$$

$$\frac{5}{4} = 1 + \frac{1}{4}.$$

Thus, $x = \frac{24}{19} = 1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}$

or, $x = 3 + \frac{1}{1+}\,\frac{1}{4}.$

In general, we have the following theorem whose proof can be found in [23].

Theorem 1.1:

Any finite simple continued fraction represents a rational number. Conversely, any rational number $\frac{p}{q}$ can be represented as a finite simple continued fraction in a unique way.

Now, let us construct the continued fraction of irrational numbers. The procedure for expanding an irrational number is fundamentally the same as that used for rational numbers.

Let x be an irrational number. The continued fraction expansion of x is achieved by successively computing the numbers $b_0, b_1, b_2, \ldots, b_n, \ldots$ and the numbers $x_1, x_2, x_3, \ldots, x_n, \ldots$ as follows:

Let $b_0 = [x]$ be the greatest integer less than or equal to x and express x in the form $x = b_0 + \frac{1}{x_1}$, $0 < \frac{1}{x_1} < 1$, where the number x_1 is given by $x_1 = \frac{1}{x - b_0} > 1$.

Note that x_1 is irrational, for, if an integer (in this case b_0) is subtracted from an irrational number (in this case x_1), the result and the reciprocal of the result are irrational.

Let $b_1 = [x_1]$ and express x_1 in the form

$x_1 = b_1 + \frac{1}{x_2}$, $0 < \frac{1}{x_2} < 1$, $b_1 \geq 1$ where, again, the number

$x_2 = \frac{1}{x_1 - b_1} > 1$, is irrational.

This calculation may be repeated indefinitely, producing the following equations:

$$b_0 = [x],$$

$$x = b_0 + \frac{1}{x_1}, \quad x_1 > 1, \quad b_1 = [x_1],$$

$$x_1 = b_1 + \frac{1}{x_2}, \quad x_2 > 1, \quad b_1 \geq 1, \quad b_2 = [x_2]$$

$$\vdots$$

$$b_n = [x_n]$$

$$x_n = b_n + \frac{1}{x_{n+1}}, \quad x_{n+1} > 1, \quad b_n \geq 1,$$

$$\vdots$$

where b_0, b_1, ..., b_n, ... are all integers and the numbers x_0, x_1, x_2, ..., x_n, ... are all irrational. This process cannot terminate, for the only way this could happen would be for some integer b_n to be equal to x_n, which is impossible since each successive x_i is irrational.

If we combine all the above equations, we obtain the continued fraction expansion for x as

$$x=b_0+\frac{1}{b_1+}\ \frac{1}{b_2+}\ \frac{1}{b_3+}\cdots\ \frac{1}{b_n+}\cdots \text{ or}$$

$$x=[b_0, b_1, b_2, b_3, \ldots, b_n, \ldots].$$

<u>Example</u>: Expand $\sqrt{2}$ into an infinite simple continued fraction.

$$b_0=[\sqrt{2}]=1, \quad \sqrt{2}=1+\frac{1}{x_1},$$

$$x_1=\frac{1}{\sqrt{2}-1}=\sqrt{2}+1, \quad b_1=[x_1]=2,$$

$$x_1=2+\frac{1}{x_2}, \quad x_2=\frac{1}{x_1-2}=\frac{1}{(\sqrt{2}+1)-2}=\frac{1}{\sqrt{2}-1}=\sqrt{2}+1.$$

Since x_2 has turned out to be the same as x_1, there is no need for further calculation, because the calculation of x_3, x_4, ... in each case will produce the same result, namely $\sqrt{2}+1$ and b_3, $= b_4 = \ldots = 2$. Thus, the continued fraction expansion of $\sqrt{2}$ is

$$\sqrt{2}=1+\frac{1}{2+}\ \frac{1}{2+}\ \frac{1}{2}+\ldots$$

$$= [1, 2, 2, \ldots]$$

$=[1,\overline{2}]$, where the bar over the 2 on the right hand side indicates that the number 2 is repeated indefinitely.

Similarly we have

$$\sqrt{3} = 1 + \frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{1\ +}\,\frac{1}{2} + \ \ldots$$

$$= [1, \overline{1, 2}]$$

$$\sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

In these examples, the continued fractions are periodic. In fact, this is true for any irrational number of the form $\sqrt{N}$. In general we have the following theorem:

<u>Theorem 1.2</u> (Lagrange):

Any quadratic irrational number $x = \frac{P + \sqrt{D}}{Q}$, where P and Q $\neq 0$ are integers, and D is a positive integer which is not a perfect square, has a continued fraction expansion which is periodic from some point onwards.

The proof of Lagrange's Theorem is given in [23]. Our next objective is to study some general properties of continued fractions, whose validity does not depend on the nature of the terms b_1, b_2, b_3, ... of the continued fraction. For the time being, therefore, we treat the terms of a continued fraction as real numbers.

Let $b_0 + \frac{1}{b_1 +}\,\frac{1}{b_2} + \ldots$ be any continued fraction. The continued fractions $b_0, b_0 + \frac{1}{b_1}, b_0 + \frac{1}{b_1 +}\,\frac{1}{b_2}, \ldots$ obtained by stopping the expansion process after the first, second, third, ... steps, are called the first, second, third, ... convergents respectively. In general, the nth convergent is

$$C_n = b_0 + \frac{1}{b_1 +}\,\frac{1}{b_2 +}\cdots\frac{1}{b_n}.$$

It is important to develop a systematic way of computing these convergents.

We write $c_0 = \frac{b_0}{1} = \frac{A_0}{B_0}$, where $A_0 = b_0,\ B_0 = 1$

$$c_1 = b_0 + \frac{1}{b_1} = \frac{b_0 b_1 + 1}{b_1} = \frac{A_1}{B_1},$$

where $A_1 = b_0 b_1 + 1,\ B_1 = b_1$, $C_2 = b_0 + \frac{1}{b_1 +}\,\frac{1}{b_2} = \frac{b_0 b_1 b_2 + b_0 + b_2}{b_1 b_2 + 1} = \frac{A_2}{B_2}$,

$$C_3 = b_0 + \frac{1}{b_1 +}\,\frac{1}{b_2 +}\,\frac{1}{b_3} = \frac{b_0 b_1 b_2 b_3 + b_0 b_1 + b_0 b_3 + b_2 b_3 + 1}{b_1 b_2 b_3 + b_1 + b_3} = \frac{A_3}{B_3}.$$

Now, let us take a closer look at these convergents. For example $C_2 = \frac{b_0 b_1 b_2 + b_0 + b_2}{b_1 b_2 + 1} = \frac{b_2\,(b_0 b_1 + 1) + b_0}{b_2\,(b_1) + 1} = \frac{b_2 A_1 + A_0}{b_2 B_1 + B_0} = \frac{A_2}{B_2}$.

Thus, $A_2 = b_2 A_1 + A_0$ and $B_2 = b_2 B_1 + B_0$.

Also $C_3 = \frac{b_3\,(b_0 b_1 b_2 + b_0 + b_2) + (b_0 b_1 + 1)}{b_3\,(b_1 b_2 + 1) + (b_1)} = \frac{b_3 A_2 + A_1}{b_3 B_2 + B_1} = \frac{A_3}{B_3}$.

Thus, $A_3 = b_3 A_2 + A_1$ and $B_3 = b_3 B_2 + B_1$.

In general, we have the following theorem.

Theorem 1.3:

Let b_0 , b_1, ..., b_n, ... be real numbers, with b_1, b_2, ... b_n, ... positive. Let the sequences A_0, A_1, ..., A_n,... and B_0, B_1, ..., B_n, ... be defined recursively by $A_0 = b_0$, $B_0 = 1$, $A_1 = b_0 b_1 + 1$, $B_1 = b_1$ and $A_k = b_k A_{k-1} + A_{k-2}$, $B_k = b_k B_{k-1} + B_{k-2}$ for $k = 2, 3, \ldots$. Then, the kth convergent $c_k = [b_0, b_1, \ldots, b_k]$ is given by $C_k = \frac{A_k}{B_k}$.

Proof:

The proof is by mathematical induction on k. For k = 0 we have $C_0 = [b_0] = \frac{b_0}{1} = \frac{A_0}{B_0}$.

For k = 1, $C_1 = [b_0, b_1] = b_0 + \frac{1}{b_1} = \frac{b_0 b_1 + 1}{b_1} = \frac{A_1}{B_1}$. Hence, the

theorem is valid for k = 0, 1. Assume that the theorem is valid for the integers 0, 1, 2, ..., k for some integer $k \geq 1$. Thus $C_k = [b_0, b_1, \ldots, b_k] = \frac{A_k}{B_k} = \frac{b_k A_{k-1} + A_{k-2}}{b_k B_{k-1} + B_{k-2}}$. $C_{k+1} = [b_0, b_1,$

$\ldots, b_k, b_{k+1}] = [b_0 , b_1, \ldots, b_k] + \frac{1}{b_{k+1}} = [b_0, b_1, \ldots b_{k-1},$

$$b_k + \frac{1}{b_{k+1}}] = \frac{\left(b_k + \frac{1}{b_{k+1}}\right)A_{k-1} + A_{k-2}}{\left(b_k + \frac{1}{b_k+1}\right)B_{k-1} + B_{k-2}}$$

$$= \frac{(b_k b_{k+1} + 1)\, A_{k-1} + b_{k+1} A_{k-2}}{(b_k b_{k+1} + 1)\, B_{k-1} + b_{k+1} B_{k-2}}$$

$$= \frac{b_{k+1}\,(b_k A_{k-1} + A_{k-2}) + A_{k-1}}{b_{k+1}\,(b_k B_{k-1} + B_{k-2}) + B_{k-1}}$$

$$= \frac{b_{k+1} A_k + A_{k-1}}{b_{k+1} B_k + B_{k-1}}$$

$$= \frac{A_{k+1}}{B_{k+1}}.$$

Thus, the theorem is valid for k+1 and $C_n = \frac{A_n}{B_n}$ for any non-negative integer n.

Theorem 1.4:

Let $C_k = \frac{A_k}{B_k}$ be the kth convergent of the continued fraction $[b_0, b_1, \ldots,]$ where k = 1, 2, ... If A_k and B_k are as defined in Theorem 1.3 above, then

$A_kB_{k-1}-A_{k-1}B_k=(-1)^{k-1}$ for any integer $k\geq 1$.

<u>Proof</u>:

The proof is by mathematical induction on k.

For k = 1 we have $A_1B_0-A_0B_1=(b_0b_1+1)\bullet 1-b_0\bullet b_1=1=(-1)^{1-1}$.

Assume the theorem is true for some integer $k\geq 1$. Thus, $A_kB_{k-1}-A_{k-1}B_k=(-1)^{k-1}$. Then, we have

$A_{k+1}B_k-A_kB_{k+1}=(b_{k+1}A_k+A_{k-1})B_k-A_k(b_{k+1}B_k+B_{k-1})$

$=b_{k+1}A_kB_k+A_{k-1}B_k-A_kb_{k+1}B_k-A_kB_{k-1} = A_{k-1}B_k-A_kB_{k-1} = -(A_kB_{k-1}-A_{k-1}B_k)$

$=-(-1)^{k-1}=(-1)^k$.

Thus, the theorem is true for k + 1, and

$A_kB_{k-1}-A_{k-1}B_k=(-1)^{k-1}$ for any integer $k\geq 1$.

<u>Corollary 1</u>:

Let $C_k=\dfrac{A_k}{B_k}$ be the kth convergent of the simple

continued fraction $[b_0, b_1, b_2, \ldots]$. Then, the integers A_k and B_k are relatively prime.

<u>Proof</u>:

Let d = $\gcd(A_k,B_k)$, then $d|A_k$ and $d|B_k$. Thus, $d|(xA_k+yB_k)$ for any integers x and y. In particular let $x=B_{k-1}$ and $y=-A_{k-1}$, then $d|(A_kB_{k-1}-A_{k-1}B_k)$. But, $A_kB_{k-1}-A_{k-1}B_k=(-1)^{k-1}$. Hence $d|(-1)^{k-1}$. Therefore d = 1 and A_k and B_k are relatively prime.

Corollary 2:

Let $C_k = \frac{A_k}{B_k}$ be the kth convergent of the continued fraction $[b_0, b_1, \ldots]$. Then, $C_k - C_{k-1} = \frac{(-1)^{k-1}}{B_k B_{k-1}}$ for all $k \geq 1$ and $C_k - C_{k-2} = \frac{b_k(-1)^k}{B_k B_{k-2}}$ for all $k \geq 2$.

Proof:

From Theorem 1.4 we have $A_k B_{k-1} - B_k A_{k-1} = (-1)^{k-1}$.

Dividing both sides by $B_k B_{k-1}$, we obtain $\frac{A_k}{B_k} - \frac{A_{k-1}}{B_{k-1}} = \frac{(-1)^{k-1}}{B_k B_{k-1}}$.

Thus, $C_k - C_{k-1} = \frac{(-1)^{k-1}}{B_k B_{k-1}}$. To establish the second identity, we have $C_k - C_{k-2} = \frac{A_k}{B_k} - \frac{A_{k-2}}{B_{k-2}} = \frac{A_k B_{k-2} - B_k A_{k-2}}{B_k B_{k-2}}$. Since $A_k = b_k A_{k-1} + A_{k-2}$ and $B_k = b_k B_{k-1} + B_{k-2}$,

$$C_k - C_{k-2} = \frac{(b_k A_{k-1} + A_{k-2})B_{k-2} - (b_k B_{k-1} + B_{k-2})A_{k-2}}{B_k B_{k-2}}$$

$$= \frac{b_k A_{k-1} B_{k-2} + A_{k-2} B_{k-2} - b_k B_{k-1} A_{k-2} - B_{k-2} A_{k-2}}{B_k B_{k-2}} = \frac{b_k (A_{k-1} B_{k-2} - B_{k-1} A_{k-2})}{B_k B_{k-2}} =$$

$$= \frac{b_k(-1)^k}{B_k B_{k-2}}.$$

Theorem 1.5:

Let x be a real number whose continued fraction expansion x = [b_1, b_2, b_3, ...] has convergents $\frac{A_i}{B_i}$. Then,

for each i, either $\frac{A_i}{B_i} < x < \frac{A_{i+1}}{B_{i+1}}$, or $\frac{A_{i+1}}{B_{i+1}} < x < \frac{A_i}{b_i}$.

Proof:

Let $x = b_1 + \frac{1}{b_2 +} \frac{1}{b_3 +} \cdots \frac{1}{b_{n-1} +} \frac{1}{x_n}$, where x_n denotes the rest of the fraction, that is, $x_n = b_n + \frac{1}{b_{n+1} +} \frac{1}{b_{n+2}} + \ldots =$ $b_n + \frac{1}{x_{n+1}}$, and $x_{n+1} = b_{n+1} + \frac{1}{b_{n+2}} + \frac{1}{b_{n+3}} + \ldots$. We have $x_n = b_n + \frac{1}{x_{n+1}} > b_n$ since $\frac{1}{x_{n+1}} > 0$. Similarly, $x_{n+1} > b_{n+1}$ or $\frac{1}{x_{n+1}} < \frac{1}{b_{b+1}}$.

Thus $b_n < x_n = b_n \frac{1}{x_{n+1}} < b_n + \frac{1}{b_{n+1}}$ ... (*)

Now, $\frac{A_n}{B_n} = b_1 + \frac{1}{b_2+}\frac{1}{b_3+}\cdots\frac{1}{b_{n-1}+}\frac{1}{b_n}$

$$x = b_1 + \frac{1}{b_2+}\frac{1}{b_3+}\cdots\frac{1}{b_{n-1}+}\frac{1}{x_n}$$

$$\frac{A_{n+1}}{B_{n+1}} = b_1 + \frac{1}{b_2+}\frac{1}{b_3+}\cdots\frac{1}{b_n+}\frac{1}{b_{n+1}}.$$

From (*) we thus have

$\frac{A_n}{B_n} = b_1 + \frac{1}{b_2+}\cdots\frac{1}{b_{n-1}+}\frac{1}{b_n} = x - x_n + b_n < x$, since $b_n - x_n < 0$.

Also $\frac{A_{n+1}}{B_{n+1}} = b_1 + \frac{1}{b_2+}\cdots\frac{1}{b_{n-1}+}\frac{1}{b_n+}\frac{1}{b_{n+1}} = (x - x_n) + b_n + \frac{1}{b_{n+1}}$

$= x + (b_n + \frac{1}{b_{n+1}} - x_n) > x$, since $(b_n + \frac{1}{b_{n+1}} - x_n) > 0$.

Hence $\frac{A_n}{B_n} < x < \frac{A_{n+1}}{B_{n+1}}$.

THE CONTINUED FRACTION EXPANSION OF $\sqrt{N}$:

We shall now demonstrate how the continued fraction expansion of $\sqrt{N}$ can be used to find small quadratic residues mod N. First we present an algorithm for finding the simple continued fraction of $\sqrt{N}$.

Theorem 1.6:

Let N be a positive integer that is not a perfect square. Define $x_k = \frac{P_k + \sqrt{N}}{Q_k}$, where P_k and $Q_k \neq 0$ are integers, determined by $P_0 = 0, Q_0 = 1, P_{k+1} = b_k Q_k - P_k$, and $Q_{k+1} = \frac{N - P_{k+1}^2}{Q_k}$, for $k = 0, 1, 2, \ldots$ where $b_k = [x_k]$. Then the continued fraction expansion of $\sqrt{N}$ is given by $\sqrt{N} = [b_0, b_1, b_2, \ldots]$.

Proof:

First by using mathematical induction on k, we will show that P_k and Q_k are integers with $Q_k \neq 0$ and $Q_k | (N - P_k^2)$ for $k = 0, 1, 2, \ldots$. For $k = 0$, we have $P_0 = 0$ and $Q_0 = 1$ are integers and $Q_0 | N$ holds from the hypothesis of the theorem. Now assume that P_k and Q_k are integers with $Q_k \neq 0$ and $Q_k | (N - P_k^2)$ for some integer $k \geq 0$, then $P_{k+1} = b_k Q_k - P_k$ is also an integer. Further, $Q_{K+1} = \frac{N - P_{k+1}^2}{Q_K} = \frac{N - (b_k Q_k - P_k)^2}{Q_k}$

$$= \frac{N - (b_k^2 Q_k^2 - 2 b_k Q_k P_k + P_k^2)}{Q_k} = \frac{(N - P_k^2)}{Q_k} + (2 b_k P_k - b_k^2 Q_k).$$ Since

$Q_k | (N - P_k^2)$ by the induction hypothesis, we see that Q_{K+1} is an integer, and since N is not a perfect square $N - P_k^2 \neq 0$, thus $Q_{K+1}=\frac{N-P_k^2}{Q_k}\neq 0$. Since $Q_k=\frac{N-P_{k+1}^2}{Q_{k+1}}$, we can conclude that

$Q_{K+1}|(N-P_{K+1}^2)$. Therefore the assertion is true for k + 1.

This completes the inductive argument.

Next we need to show that the integers b_0, b_1, b_2, ... are the partial quotients of the simple continued fraction of $\sqrt{N}$. We accomplish this by showing that $x_{k+1}=\frac{1}{x_k-b_k}$, for k

$= 0, 1, 2, \ldots.$ $x_k-b_k=\frac{P_k+\sqrt{N}}{Q_k}-b_k=\frac{\sqrt{N}-(b_kQ-K-P_k)}{Q_k}=\frac{\sqrt{N}-P_{k+1}}{Q_k}$

$$=\frac{\sqrt{N}-P_{k+1}}{Q_k}\bullet\frac{\sqrt{N}+P_{k+1}}{\sqrt{N}+P_{k+1}}=\frac{N-P_k^2}{Q_k(\sqrt{N}+P_{k+1})}=\frac{Q_kQ_{k+1}}{Q_k(\sqrt{N}+P_{K+1})}=\frac{Q_{k+1}}{\sqrt{N}+P_{K+1}}=\frac{1}{X_{k+1}}.$$

Hence $\sqrt{N}=[b_0, b_1, b_2, \ldots]$.

We illustrate the use of the algorithm given in Theorem 1.6 above with the following example.

Example:

Let N = 14

Table 1.1

k	P_k	Q_k	x_k	b_k
0	0	1	$\sqrt{14}$	3

1	3	5	$\frac{3+\sqrt{14}}{5}$	1
2	2	2	$\frac{2+\sqrt{14}}{2}$	2
3	2	5	$\frac{2+\sqrt{14}}{5}$	1
4	3	1	$\frac{3+\sqrt{14}}{1}$	6
5	3	5	$\frac{3+\sqrt{14}}{5}$	1

Since $x_5 = x_1$, also $x_6 = x_2$, and so on, which means that the block of integers 1, 2, 1, 6, 1, repeats indefinitely. Thus the continued fraction expansion of $\sqrt{14}$ is periodic and is given by $\sqrt{14} = [3, \overline{1, 2, 1, 6, 2}]$. Notice that just before recurrence starts we have $Q_k = 1$, thus $x_k = P_k + \sqrt{N}$, hence

$b_k = [x_k] = P_k + [\sqrt{N}] = P_k + b_0$. Also

$Q_{k+1} = N - P_{k+1}^2 = N - (b_k - P_k)^2 = N - b_0^2 = Q_1$.

$P_{k+1} = b_k Q_k - P_k = b_k - P_k = b_0 = P_1$.

Thus we have proved the following theorem.

Theorem 1.7:

Suppose that $Q_k = 1$. then the pair (P_{k+1}, Q_{k+1}) is a repeat of the pair (P_1, Q_1), and hence the calculation of P_k's, Q_k's, x_k's and b_k's starts to repeat: $b_{k+1}=b_1, b_{k+2}=b_2$, etc.

There is one more result we need to prove here about the continued fraction expansion of $\sqrt{N}$. This result is in fact the key (or one of the keys) to find small quadratic residues mod N.

Theorem 1.8:

Let N be a positive integer that is not a perfect square. Define $x_k=\frac{P_k+\sqrt{N}}{Q_k}$, $b_k=[x_k]$, $P_{k+1}=b_kQ_k-P_k$ and

$Q_{k+1}=\frac{N-P_{k+1}^2}{Q_k}$, for k = 0, 1, 2, ... where $x_o=\sqrt{N}$ $P_0 = 0$ and Q_0

= 1. Furthermore, let $\frac{A_k}{B_k}$ denote the kth convergent of the

continued fraction expansion of $\sqrt{N}$. Then

$A_k^2-NB_k^2=(-1)^{k+1}Q_{k+1}$.

To prove the theorem we need the following lemma.

Lemma 1.9:

Let N be a positive integer that is not a perfect square and a, b, c, and d are rational numbers. Then a + b$\sqrt{N}$ = c + d$\sqrt{N}$ if and only if a = c and b = d.

Proof:

Clearly if a = c and b = d then a + b$\sqrt{N}$ = c + d$\sqrt{N}$. Conversely, assume that a + b$\sqrt{N}$ = c + d$\sqrt{N}$, if b ≠ d then $\sqrt{N}=\frac{a-c}{d-b}$ but $\frac{a-c}{d-b}$ is a rational number and $\sqrt{N}$ is irrational, thus b = d. Hence a + b$\sqrt{N}$ = c + b$\sqrt{N}$ implies a = c.

Proof: (Theorem 1.8)

Since $\sqrt{N}=x_0=[b_0, b_1, \ldots, b_k, x_{k+1}]$ then $\sqrt{N}=\frac{A_{k+1}}{B_{k+1}}$.

By Theorem 1.6 we have $\sqrt{N}=\frac{x_{k+1}A_k+A_{k-1}}{x_{k+1}B_k+B_{k-1}}$. Since

$x_{k+1}=\frac{(P_{k+1}+\sqrt{N})}{Q_{k+1}}$ we have $\sqrt{N}=\frac{(P_{k+1}+\sqrt{N})A_k+Q_{k+1}A_{k-1}}{(P_{k+1}+\sqrt{N})B_k+Q_{k+1}B_{K-1}}$. Thus

$$\sqrt{N}[(P_{k+1}+\sqrt{N})B_k+Q_{k+1}B_{k-1}]=(P_{k+1}+\sqrt{N})A_k+Q_{k+1}A_{k-1}).$$

Or $NB_k+(P_{k+1}B_k+Q_{k+1}B_{k-1})\sqrt{N}=(P_{k+1}A_k+Q_{k+1}A_{k-1})+A_k\sqrt{N}$

By Lemma 1.9 we must have (1) $N B_k = P_{k+1} A_k + Q_{k+1} A_{k-1}$, and (2) $P_{k+1} B_k + Q_{k+1} B_{k-1} = A_k$. Multiply the first equation by B_k

and the second equation by A_k we obtain

(3) $NB_k^2 = P_{k+1}A_kB_k + Q_{k+1}A_{k-1}B_k$

(4) $A_k^2 = P_{k+1}B_kA_k + Q_{k+1}B_{k-1}A_k$.

subtract equation (3) from equation (4) we obtain

$A_k^2 - NB_k^2 = (A_kB_{k-1} - A_{k-1}B_k)\, Q_{k+1} = (-1)^{k+1}Q_{k+1}$.

How large can the quadratic residues mod N we obtain from the continued fraction expansion of $\sqrt{N}$ be?

First we need to prove the following Lemma.

Lemma 1.10:

Let x > 1 be a real number whose continued fraction expansion has convergent $\frac{A_i}{B_i}$. Then for all i the inequality hold: $|A_i^2 - x^2B_i^2| < 2x$.

Proof:

By Theorem 1.5 we have $\frac{A_i}{B_i} < x < \frac{A_{i+1}}{B_{i+1}}$.

Consider $\left|\frac{A_{i+1}}{B_{i+1}} - \frac{A_i}{B_i}\right| = \frac{|A_{i+1}\bullet B_i - A_iB_{i+1}|}{B_iB_{i+1}} = \frac{|(-1)^{i+1}|}{B_iB_{i+1}}$

$= \frac{1}{B_iB_{i+1}}$ (By Theorem 1.4).

Thus $|A_i^2 - x^2B_i^2| = B_i^2\,|\frac{A_i^2}{B_i^2} - x^2| \;\; = B_i^2\,|\frac{A_i}{B_i} - x| \bullet |\frac{A_i}{B_i} + x|$

$$= B_i^2\,|x - \frac{A_i}{B_i}| \bullet |x + \frac{A_i}{B_i}| \;\; = B_i^2\,|x - \frac{A_i}{B_i}| \bullet (x + \frac{A_i}{B_i}) \;\; < B_i^2\,|\frac{A_{i+1}}{B_{i+1}} - \frac{A_i}{B_i}|\left(x + \frac{A_i}{B_i}\right)$$

$= B_i^2 \bullet \frac{1}{B_iB_{i+1}}\left(x + \frac{A_i}{B_i}\right) \;\; < B_i^2 \bullet \frac{1}{B_iB_{i+1}}\left(x + (x + \frac{1}{B_iB_{i+1}})\right)$. Hence

$$|A_i^2 - x^2B_i^2| - 2x < B_i^2 \bullet \frac{1}{B_iB_{i+1}}\left(x + (x + \frac{1}{B_iB_{i+1}})\right) - 2x$$

$$= \frac{B_i}{B_{i+1}}\left(2x + \frac{1}{B_iB_{i+1}}\right) - 2x \;\; = 2x\left(\frac{B_i}{B_{i+1}} + \frac{1}{2xB_{i+1}^2} - 1\right) \;\; < 2x\left(\frac{B_i}{B_{i+1}} + \frac{1}{B_{i+1}} - 1\right)$$

$= 2x\left(\frac{B_i + 1}{B_{i+1}} - 1\right) < 2x\left(\frac{B_{i+1}}{B_{i+1}} - 1\right) = 0$. *Thus* $|A_i^2 - x^2B_i^2| < 2x$.

<u>Theorem 1.11</u>:

Let N be a positive integer which is not a perfect square. Let $\frac{A_i}{B_i}$ be the convergents in the continued fraction expansion of $\sqrt{N}$. Then the residue of A_i^2 (mod N) which is smallest in absolute value (i.e. between $-\frac{N}{2}$ and $\frac{N}{2}$) is less than $2\sqrt{N}$.

Proof:

Apply the previous Lemma with $x=\sqrt{N}$. Then $A_i^2 \equiv b_i^2 - NB_i^2$ (mod N), but $|A_i^2 - NB_i^2| < 2\sqrt{N}$.

This theorem implies the Q_k's satisfy the inequality $0 < Q_k < 2\sqrt{N}$ for each k.

Chapter 2

Classical Factoring Techniques

In this chapter, we present a description of some classical factoring techniques. The factoring techniques presented are either currently in use in factoring large numbers or they are used in conjunction with one of the more recently developed factoring algorithms. In fact, many recent factoring algorithms are themselves based on these techniques.

Along with each factoring technique presented in this chapter is discussed not only the technique but the theory behind the technique. Improvements that speed the algorithms are discussed, and each algorithm is illustrated by examples. For some of the algorithms presented, a running time estimate is given as well.

2.1 Trial Division Method

Trial division is probably the first method that comes into consideration when attempting to factor an integer N (or of proving it prime). If $N = a \bullet b$ with $a > 1$ and $b > 1$, the a and b must be one of integers 2, 3,..., N - 1. Thus, the trial division algorithm in its simplest form consists of dividing N by 2, 3, 4, ..., N - 1 in turn and to "cast out" each factor that is discovered. That is, if the trial division of N by one of the integers, say, a, leaves a zero remainder, a factorization $N = a \bullet (\frac{N}{a})$ has been obtained.

The time required to find a factor of N by trial division is closely related to the number of possible trial divisors. Thus, most improvements to the speed the trial division algorithm attempt to eliminate some of the trial divisors in advance. Other improvements attempt to increase the speed of the algorithm by replacing some of the divisions by cheaper operations. The first step toward eliminating trial divisors is based on the simple observation that the list of divisors need not contain a number u whose factors occur prior to u in the list. This observation actually reduces the trial divisors to all primes below N.

A second step in eliminating more trial divisors is based on the following theorem.

Theorem 2.1:

If N is a composite integer, then N has a prime factor P not exceeding $\sqrt{N}$.

Proof:

If an integer N > 1 is composite, then it may be written as N = a b, where 1 < a < N and 1 < b < N. Assuming that $a \leq b$, we get $a^2 \leq ba = N$ and ultimately $a \leq \sqrt{N}$. Since a > 1, then a has at least one prime factor P, and $P \leq a \leq \sqrt{N}$.

Thus, in the trial division algorithm it is sufficient to try as divisors all the primes less than or equal to

$[\sqrt{N}]$, where $[\sqrt{N}]$ denotes the greatest integer less than or equal to $\sqrt{N}$.

This reduction in the number of trial divisors leads to a speeding up of the algorithm. With these improvements we can outline the algorithm as follows:

First we divide N successively by the primes 2, 3, 5, ..., P, where P is the largest prime $\leq [\sqrt{N}]$, until discovering the first one, say q_1 for which $q_1|N$. Then q_1 is the smallest prime factor of N, and the same process may be applied to $\frac{N}{q_1}$ by successively dividing $\frac{N}{q_1}$ by q_1 and the primes greater than q_1. The process stops when the unfactored part that remains is less than the square of the last prime we tested; for if m is the unfactored part that remains and q_m is the last prime tested and m < q_m^2, then $[\sqrt{m}] \leq q_m$ and m must be prime.

Although the trial division algorithm is quite simple, the question remains: How can we generate all primes less than or equal to $[\sqrt{N}]$? If N is not too large (say N $\leq$ 100,000), then it is convenient to store a table of primes up to some limit and take the sequence of trial divisors from this list. For example, if N is less than a million, we need to store a table of all primes less than 1000, and there are 168 primes less than 1000. However, if the integer N we wish to factor is too large, storing a table of primes less than or equal to $[\sqrt{N}]$ would speed the algorithm at the expense of using a good deal of storage space. An alternative to storing a table of primes would be to generate the primes. This leads to an algorithm running a little slower, but demanding less storage space. One way to improve the running time of the algorithm in the latter case is to use the integers 2 and 3 and then all positive integers of the form $6k \pm 1$ as trial divisors. Clearly, this list of integers includes all primes and also includes some composite numbers, namely 24, 35, 49, ... To generate all integers of the form $6k \pm 1$, we start with 5 and then alternately add 2 and 4 thus getting $5 + 2 = 7$, $7 + 4 = 11$, $11 + 2 = 13$, $13 + 4 = 17$, and so on. Other methods to reduce the number of trial divisors have been developed by Legendre and Gauss who used the theory of quadratic residues. Both methods will be presented in sections 2.2 and 2.3.

Let us illustrate the trial division algorithm by examples:

Example 1:

Let $N = 25852$.

The list of trial divisors are 2, 3, 5, 7, 11, 13, 17, ..., 157. Since $2|N$ then $q_1 = 2$ is a prime divisor of N. Now, we consider the integer $N_1 = \frac{N}{q_1} = 12926$. With $2|12926$, $q_2 = 2$ is a prime factor of N_1. Next we consider the integer $N_2 = \frac{N_1}{q_2} = 6463$. We find N_2 is not divisible by 2, 3, 5, 7, 11, 13, 17, 19, but $23|6463$, hence $q_3 = 23$ is a prime factor of N_2. Now, we consider the integer $N_3 = \frac{N_2}{q_3} = 281$. Since N_3 is less than the square of the last prime tested, we know $N_3 =$ 281 must be a prime, and here we stop. Thus the factorization of N is $N = 25852 = 2 \cdot 2 \cdot 23 \cdot 281$.

Note that the factorization of N = 25852 has involved a total of 11 division operations, namely the division by 2 three times and the division one time by each of the integers 2, 5, 7, 11, 13, 17, 19, and 23.

Example 2:

Let N = 25849.

The list of trial divisors are 2, 3, 5, 7, 11, 13, 17, ..., 163. By dividing N successively by the trial divisors, we find none of them divides N. Thus we conclude that N = 25849 is prime.

Note that the number of division operations involved to attempt to factor N = 25849 is 37. Thus the number of division operations needed to attempt to factor 25849 is more than three times the number of division operations needed to factor 25852. A natural question one may ask is, how many trial divisions are necessary to factor (or prove the primality) of an integer N by using the trial division algorithm? Obviously, the number of trial divisions depends heavily on the size of the prime factors of N. For example, if N is a power of 2, say, $N = 2^k$, the number of trial division is approximately $k = \log_2 N$. On the other hand, if N is a prime, the number of trial divisions is approximately $\sqrt{N}$. To measure the trial division algorithm time complexity, that is, to estimate the expected running time required to factor an integer N (or prove its primality) by the trial division algorithm, we may count the number of trial divisions the algorithm must perform. Thus, the best-case complexity of the algorithm is $O(\log N)$ and the worst-case complexity of the algorithm is $O(\sqrt{N})$. For a random integer, the time complexity of the algorithm has been studied by Knuth and Pardo [8]. In [8] it is shown that the probability that the kth largest prime factor of N is less than N^x, where x is a real number between 0 and $\frac{1}{2}$,

approaches a limit $F_k(x)$ as N approaches infinity. The tabulated values of $F_k(x)$ given in the paper enables one to estimate the probability that the factorization of N will be completed in $O(N^x)$ steps, for varying x. For example, the number of trial divisions will be less than or equal to $N^{0.35}$ about 50% of all cases, and in more than 70% of all cases the running time will be less than or equal to $N^{0.4}$. Although the trial division algorithm is inefficient and hence not well suited for factoring large numbers completely, the algorithm has certain advantages. Some of the advantages of the trial division algorithm are:

1. The method often succeeds in quickly removing one or two small prime factors of the number thereby reducing the size of the number and the running time of other factoring methods that can be used to complete the factorization of the number.
2. The factors produced by the trial division algorithm are guaranteed to be prime. This property is not shared by any other factorization method.
3. Upon dividing N by primes up to some limit, say B without success in finding a factor of N, it guarantees that N has no prime factor below B. This information is not easily obtained by other factoring methods. Moreover, this information leads to a guarantee that if a factor q of N is discovered by another factor method and $q < B^2$ then q is a prime factor of N.

Because of these advantages, if one is given no information about the number N, the trial division algorithm should always be attempted up to some bound B before using a more powerful factoring algorithm.

2.2 Legendre's Factoring Method:

Legendre's factoring method is based on restricting the trial divisors in the trial division method by constructing small quadratic residues of the number N. After a sufficient number of small quadratic residues have been found, a sieve is used in which each quadratic residue restricts the possible factors of N to a particular form, by the Law of quadratic reciprocity.

First let us recall that a number m is a quadratic residue modulo N if gcd(m, N) = 1 and the congruence $x^2 \equiv m \pmod N$ has a solution. If m is a quadratic residue mod N we denote this by m R N.

Now, if $N = a \bullet b$ and m R N, then m R a and m R b. To see the reasons why, assume x = r is a solution to the congruent $x^2 \equiv m \pmod N$, in which case $r^2 \equiv m \pmod{a \bullet b}$, hence $r^2 \equiv m \pmod a$ and $r^2 \equiv m \pmod b$.

Example 1:

m = 1 is a quadratic residue modulo 15 since x = 4 is a solution to the congruence $x^2 \equiv 1 \pmod{15}$. Thus, m = 1 is a quadratic residue mod 3 and a quadratic residue mod 5. In fact, $4^2 \equiv 1 \pmod 3$ and $4^2 \equiv 1 \pmod 5$.

Knowing a quadratic residue m mod N, where N is the number we want to factor, allows us to restrict the possible divisors of N to the set of trial divisors u for which m is a quadratic residue modulo u, i.e. $\{2 \le u \le [\sqrt{N}] \mid mRu\}$.

Example 2:

Let N = 77.

m = -6 is a quadratic residue mod 77. The set of trial divisors u for which m = -6 is a quadratic residue mod u are $\{2 \le u \le 8 \mid -6 R u\} = \{5, 7\}$.

Example 3:

Let N = 1537.

m = -1 is a quadratic residue mod 1537. The set of prime divisors is $\{2 \le P \le 39 \mid -1 R P\} = \{5, 13, 17, 29, 37\}$.

The above discussion raises the following questions:

1. How many trial divisors u with $2 \le u \le [\sqrt{N}]$ will survive the condition m R u?
2. How do we find the necessary quadratic residues mod N?
3. How do we use the quadratic residues mod N to restrict the possible factors of N to particular forms?

The overall plan of this section is to answer these questions gradually until we can finally state a precise version of Legendre's factoring algorithm.

The answer to the first question is based on the following theorem.

Theorem 2.2:

If P is an odd prime, then there are exactly $\frac{P-1}{2}$ quadratic residues mod P and $\frac{P-1}{2}$ quadratic nonresidues mod

P among the integers 1, 2, 3,..., p-1.

Proof:

To find all the quadratic residues of p among the integers 1, 2, ..., p - 1 we compute the least positive residues modulo p of the squares of the integers 1, 2, ..., p - 1. Since there are p - 1 squares to consider and since each congruence $x^2 \equiv a \pmod{p}$ has either zero or two solutions, there must be exactly $\frac{(p-1)}{2}$ quadratic residues of P among the integers 1, 2, ..., p - 1. The remaining $p-1-\frac{(p-1)}{2}=\frac{(p-1)}{2}$ positive integers less than p - 1 are quadratic nonresidues of p.

We need to know how the residues and non-residues are distributed in a subinterval of the interval of integers [1, p - 1]. The answer is given by the following theorem, whose proof is beyond the scope of this paper.

Theorem 2.3:

Suppose that α and β $(\alpha<\beta)$ are two fixed proper fractions. For a large prime p, about one half the integers in the subinterval $[\alpha p, \beta p]$ are quadratic residues x mod p. That is, the quadratic residues mod p are equally distributed in the interval [1, p - 1].

It follows from this theorem that only about one half of all trial divisors between 2 and $\sqrt{N}$ will satisfy the condition m R u for a particular m. In addition, knowing several quadratic residues m_1, m_2, ..., m_k of N with no common divisor, the restrictions imposed by each m_i are independent and only about $(\frac{1}{2})^k$ of all trial divisors in the set of all divisors u that satisfy the conditions m_i R u will be left for actual trial divisions. Thus 20 known quadratic residues will reduce the number of trial divisions necessary by a factor of abut $2^{20} \approx 1{,}000{,}000$.

The answer to the second question is relatively simple. To find some quadratic residues mod N simply take a number x, square it, and reduce the result modulo N. However, it is not easy to determine the arithmetic progression to which the primes in {p : m is a quadratic residue mod p} belong when m is large. Thus, it would be more useful to have a number of small quadratic residues, whereby new quadratic residues may be obtained. The method is based on the following Lemma.

Lemma 2.4:

If $m = n \cdot a^2$ is a quadratic residue mod N, where a and n are integers, then n is a quadratic residue mod N.

Proof:

Since $m = n \cdot a^2$ is a quadratic residue the congruence $x^2 \equiv n \cdot a^2 \pmod{N}$ has a solution, say $x = x_0$. Thus $x_0^2 \equiv n \cdot a^2$

(mod N)...(*) hold. By definition, gcd(a^2 n,N) = 1, thus gcd(a^2, N) = 1. Thus, a has an inverse mod N; that is, there exists an integer b such that $a \bullet b \equiv 1$ (mod N). By multiplying both sides of (*) by b^2, we obtain $b^2 x_0^2 \equiv n(a \bullet b)^2$ (mod N). Thus $(x_0 \bullet b)^2 \equiv n$ (mod N). Hence n is a quadratic residue mod N.

<u>Example</u>:

m = 60 = 15 • 2^2 is a quadratic residue mod 77 because $26^2 \equiv$ 60 (mod 77). By removing the square factor 2^2 from m we obtain n = 15 and thus by the lemma, 15 is a quadratic residue mod 77. In fact, since b = 39 is the inverse of 2 mod 77, $(26 \bullet 39)^2 \equiv 15$ (mod 77).

We now assume that we have an initial set of small quadratic residues which can be completely factorized. These quadratic residues can then be combined easily by multiplication and removing the square factors to yield new quadratic residues.

It remains to specify how the initial set of quadratic residues mod N is formed. Legendre used the continued fraction expansion of $\sqrt{N}$ to find the initial set of quadratic residues. However, before we describe how the initial set of quadratic residues is found, we must answer the third question. The answer is based on the following version of the law of quadratic reciprocity.

<u>Theorem 2.5</u>:

Let q be a fixed positive odd prime, and let p range over the odd positive primes $\neq$ q. Every such p has a unique representation in exactly one of the two forms

(1) $p=4qk\pm a$ with k an integer, $0<a<4q$, $a\equiv 1 \pmod 4$. When (1) holds, (2) $\left(\frac{q}{p}\right)=\left(\frac{a}{q}\right)$. Thus the p for which $\left(\frac{q}{p}\right) = 1$, are exactly those $p \equiv \pm a \pmod{4q}$, for all a such that

(3) $0 < a < 4q$, $a \equiv 1 \pmod 4$, $\left(\frac{a}{q}\right) = 1$. The a's satisfying (3) are given by the smallest positive remainders (mod 4q) of the odd squares $1^2, 3^2, 5^2, \ldots, (q-2)^2$.

Proof:

By the division algorithm, there are unique integers k', a' such that $p = 4qk' + a'$, where $1 \le a' < 4q$. Clearly a' is odd. If $a' \equiv 1 \pmod 4$, (1) holds with the plus sign and with $k = k'$, $a = a'$. If $a' \equiv -1 \pmod 4$, (1) holds with the minus sign and $k = k' + 1$, $a = 4q - a'$. Any other value of k than k' and k' + 1 would yield $|a| \ge 4q$. To verify (2), let us suppose that the plus sign is correct in (1). Then $p \equiv 1 \pmod 4$ and $p \equiv a \pmod q$, making $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=\left(\frac{a}{q}\right)$. If the minus sign is correct, the $p \equiv -1 \pmod 4$ and $p \equiv -a \pmod q$, so either $q \equiv -1 \pmod 4$, and $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)=-\left(\frac{-a}{q}\right)=\left(\frac{a}{q}\right)$, or q

$\equiv 1 \pmod 4$, and $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=\left(\frac{-a}{q}\right)=\left(\frac{a}{q}\right)$. Finally, if $\left(\frac{a}{q}\right)=1$, there is an integer b such that $a \equiv b^2 \pmod q$ and $1 \le b \le q-1$, whereby also $a \equiv (q-b)^2 \pmod q$ and $1 \le q-b \le q-1$. Since either b or q-b is odd-say b'-we have $a \equiv b^2 \pmod q$, $1 \le b' \le q-2$, $b' \equiv 1 \pmod 2$. But, likewise, $a \equiv 1 \equiv b^2 \pmod 4$, so that $a \equiv b^2 \pmod{4q}$. This completes the proof.

Example 1:

We illustrate the theorem by taking q = 3. in which case the only integer satisfying the condition (3) is a = 1, so that 3 is a quadratic residue of the primes $p = 12k \pm 1$. Every other odd number is of one of the forms $12k \pm 3$ or $12k \pm 5$, and no prime except 3 occurs in the progressions $12k \pm 3$. Hence $\left(\frac{3}{p}\right)$ is completely determined by the equations $\left(\frac{3}{p}\right)=\begin{cases} 1 & if\ p \equiv \pm 1 \pmod{12} \\ -1 & if\ p \equiv \pm 5 \pmod{12} \end{cases}$.

Example 2:

Let q = 17. Consider the squares 1^2, 3^2, 5^2, 7^2, 9^2, 11^2, 13^2, 15^2, which reduce (mod $4 \bullet 17$) to 1, 9, 25, 49, 13, 53, 33, 21. Thus, 17 is a quadratic residue of primes of the forms $68k \pm 1$, 9, 13, 21, 25, 33, 49, and 53.

Determining the primes of which a composite number is a quadratic residue is somewhat more complicated. We illustrate this in the next example.

Example 3:

Let us find the primes p such that $\left(\frac{6}{p}\right)=1$.

$\left(\frac{6}{p}\right)=1$ if and only either $\left(\frac{2}{p}\right)=\left(\frac{3}{p}\right)=1$ or $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$.

$\left(\frac{2}{p}\right)=1$ if and only if $p\equiv\pm1 \pmod 8$.

$\left(\frac{3}{p}\right)=1$ if and only if $p\equiv\pm1 \pmod{12}$.

$\left(\frac{2}{p}\right)=-1$ if and only if $p\equiv\pm3 \pmod 8$.

$\left(\frac{3}{p}\right)=-1$ if and only if $p\equiv\pm5 \pmod{12}$.

Thus we have the following pairs of congruences, each pair to be solved simultaneously.

$p\equiv1 \pmod 8$ $\qquad$ $p\equiv-1 \pmod 8$

$p\equiv1 \pmod{12}$ $\qquad$ $p\equiv-1 \pmod{12}$

$p\equiv1 \pmod 8$ $\qquad$ $p\equiv-1 \pmod 8$

$p\equiv-1 \pmod{12}$ $\qquad$ $p\equiv1 \pmod{12}$

$p\equiv3 \pmod 8$ $\qquad$ $p\equiv-3 \pmod 8$

$p\equiv5 \pmod{12}$ $\qquad$ $p\equiv-5 \pmod{12}$

$p\equiv 3 \pmod 8$ $\qquad$ $p\equiv -3 \pmod 8$

$p\equiv -5 \pmod{12}$ $\qquad$ $p\equiv 5 \pmod{12}$.

Four of these pairs are internally inconsistent, while the other that implies $\left(\frac{6}{p}\right)=1$ are given by $p\equiv \pm 1, \pm 5 \pmod{24}$.

The primes in the set of possible divisors $\{p|\ 2\le p\le [\sqrt{N}]$, m R p} where m R N have been extensively tabulated by Legendre [11] for small values of m. The primes in arithmetic progression for some values of m are given in table 2.1.

We now describe how the continued fraction expansion of $\sqrt{N}$ can be used to find small quadratic residues mod N.

From Theorem 1.8 we have for every non-negative integer k, $A_k^2-NB_k^2=(-1)^{k+1}Q_{k+1}$. Thus,for every non-negative integer k, we have $A_k^2\equiv(-1)^{k+1}Q_{k+1} \pmod N$. Thus, $(-1)^{k+1}Q_{k+1}$ is a quadratic residue mod N. We note that the Q_k's are small compared to N. Recall that the Q_k's satisfy the following inequality $0<Q_k<2\sqrt{N}$ for each k.

Table 2.1

m	The form of p	m	The form of p
-1	4k + 1		

-2	8k + 1, 3	2	8k ± 1
-3	6k + 1	3	12k ± 1
-5	20k + 1, 3, 7, 9	5	10k ± 1
-6	24k + 1, 5, 7, 11	6	24k ± 1, 5

Example 1:

Let N = 1537.

The sequence $\{Q_k\}$, together with x_k and the convergentes $\frac{A_k}{B_k}$ generated by the continued fraction expansion of $\sqrt{1537}$, are given in table 2.2:

Since m = -16 (-1)(4^2) is a quadratic residue mod 1537, then m = -1 is also a quadratic residue mod 1537. Thus the prime factors of N = 1537 are the form p = 4k + 1, k ≥ 1. We now apply the trial division algorithm with trial divisors the primes of the form 4k + 1 up to p = 37. The set of trial prime divisors are {5, 13, 17, 29, 37}. Since $29|1537$ then 29 is a prime factor of 1537. Since $\frac{1537}{29}=53$ is prime then the prime factorization of N = 1537 is 1537 = 29•53.

Table 2.2

k	$x_k = \frac{P_\alpha + \sqrt{N}}{Q_k}$	$\frac{A_k}{B_k}$	$A_k^2 - NB_k^2$	Q_{k+1}
0	$x_0 = 39 + \frac{1}{x_1}$	$\frac{39}{1}$	$39^2 - 1537 \cdot 1^2 = -16$	$Q_1 = 16$
1	$x_1 = 4 + \frac{1}{x_2}$	$\frac{157}{4}$	$157^2 - 1537 \cdot 4^2 = 57$	$Q_2 = -57$
2	$x_2 = 1 + \frac{1}{x_3}$	$\frac{196}{5}$	$196^2 - 1537 \cdot 5^2 = -9$	$Q_3 = 9$
3	$x_3 = 7 + \frac{1}{x_4}$	$\frac{1529}{39}$	$1529^2 - 1537 \cdot 39^2 = 64$	$Q_4 = 64$

In summary, Legendre's factoring method of a composite integer N consists of the following steps:

1. Form a set of initial quadratic residues mod N by expanding $\sqrt{N}$ in a continued fraction.
2. Reduce the set of quadratic residues to obtain square free residues. Notice that a complete prime factorization of each initial quadratic residue is necessary to perform the reduction.
3. Use the quadratic residues to determine the arithmetic progression and hence the form of prime divisors of N.

4. Use the trial division algorithm to find the actual prime divisors left over from the elimination process.

<u>Example</u>: factor N = 1711.

The continued fraction expansion of $\sqrt{1711}$ yields the following table of sequences $\{Q_k\}$ and $\{A_k\}$.

Table 2.3

k + 1	A_k	$(-1)^{k+1}Q_{k+1}$	Factorization of $(-1)^{k+1} Q_{k+1}$
1	41	-30	$-1 \bullet 2 \bullet 3 \bullet 5$
2	83	45	$3^2 \bullet 5$
3	124	-23	$-1 \bullet 23$
4	331	57	$3 \bullet 19$
5	455	-6	$-1 \bullet 2 \bullet 3$
6	-598	5	5
7	-558	-38	$-2 \bullet 19$
8	-3	9	$3 \bullet 3$

Since m = 5 is a quadratic residue of N, the prime divisors of N are the form 10k ± 1. This reduces the trial divisors in the set $\{p|2 \le p \le 41\}$ to only {11, 19, 29, 31, 41}. Then, the trial division algorithm gives the factor $p = 29$ of $N = 1711$ and the other factor is $\frac{1711}{29} = 59$. We may use also the fact that $m = -6$ is a quadratic residue of N to restrict the possible prime divisors of N to {5, 7, 11, 29, 31} and then use the trial division algorithm to find the actual prime divisors of N among the primes in the set {5, 7, 11, 29, 31}. However, the two lists of primes restrict the possible prime divisors of N less than $[\sqrt{N}]+1$ to {11, 19, 29, 31, 41} $\cap$ {5, 7, 11, 29, 31} = {11, 29, 31}.

2.3 Gauss's Factoring Method:

Gauss' factoring method is very similar to that of Legendre, discussed in section 2.2. It differs only in the procedure for finding small quadratic residues of N. Like Legendre's method Gauss' method is a sort of exclusion method which, by finding more and more quadratic residues mod N, excludes more and more primes from being possible factors of N. Then one may apply the trial division algorithm by those remaining possible factors to factor N.

Gauss' factoring method consists of two steps. The first step is to find many small quadratic residues mod N. The second is to use these quadratic residues to reduce the number of trial divisors in the trial division algorithm. How can we find many small quadratic residues? To find a quadratic residue mod N, simply take an integer and square it and then reduce the square (mod N). In general this method leads to big quadratic residues mod N when N is large. However, we need to find small quadratic residues mod N in order to exclude a number of primes as possible divisors of N. Gauss used the following method to find small quadratic residues mod N:

If a is a quadratic residue mod N, then the congruence $x^2 \equiv a \pmod{N}$ has a solution, and $x^2 - a = kN$ for some integer k or $a = x^2 - kN$. Thus, we find small quadratic residues mod N, by letting x close to $[\sqrt{kN}]$. As the product of two quadratic residues is again a quadratic residue, we can combine these quadratic residues by multiplication and removing the square factors to yield new quadratic residues.

In general, we want the value of a to be such that $|a| < 50{,}000$ and the prime factors of a less than 100. Let us illustrate the method of finding quadratic residues by an example.

<u>Example</u>:

Let N = 12007001

Consider the equation $a = x^2 - kN$

Our goal is to choose values of x close to $[\sqrt{kN}]$ for different values of k such that $|a| = |x^2 - kN| < 50{,}000$ and the prime factors of a are less than 100.

For k = 1 we have $[\sqrt{N}] = 3465$. Take x = 3459 then $a = (3459)^2 - 12007001$. Thus $a = -42320 = (-1)\cdot 2^4 \cdot 5 \cdot 23^2$. For x = 3460, a = -35401 has no prime factor less than 100. Thus we discard this x. For $x = 3461$, $a = -1 \cdot 2^6 \cdot 5 \cdot 89$. For $x = 3463$, $a = -1 \cdot 2^3 \cdot 31 \cdot 59$, and

$x = 3464, \to a = 5 \cdot 23 \cdot 67$

$x = 3465 \to a = -1 \cdot 2^3 \cdot 97$.

For $k = 2$,

$[\sqrt{kN}] = [\sqrt{24014002}] = 4900$.

Let

$x = 4898 \to a = -1 \cdot 2 \cdot 3^3 \cdot 19 \cdot 23$

$x = 4900 \to a = 2 \cdot 3 \cdot 23 \cdot 29$

For $k = 3$,

$[\sqrt{kN}] = [\sqrt{36021003}] = 6001$

Let

$x = 6003 \to a = 2 \cdot 3 \cdot 41 \cdot 61$

For $k = 5$,

$[\sqrt{kN}] = [\sqrt{6003505}] = 7748$

Let

$x = 7745 \to a = -1 \cdot 2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 17$

For $k = 8$,

$[\sqrt{kN}] = [\sqrt{96056008}] = 9800$

$x = 9788 \to a = -1 \cdot 3 \cdot 11 \cdot 13 \cdot 83$

For $k = 10$,

$[\sqrt{kN}] = [\sqrt{120070010}] = 10957$

$x = 10957 \to a = -1 \cdot 7^2 \cdot 17^2$

For k = 11,

$[kN] = [\sqrt{132077011}] = 11492$

$x = 11491 \to a = -1 \bullet 2 \bullet 3^2 \bullet 5 \bullet 13 \bullet 29$

$x = 11492 \to a = -1 \bullet 3 \bullet 41 \bullet 89$

For k = 14,

$[kN] = [\sqrt{168098014}] = 12965$

$x = 12964 \to a = -1 \bullet 2 \bullet 3 \bullet 7 \bullet 19 \bullet 41$

$x = 12965 \to a = -1 \bullet 3 \bullet 31 \bullet 73$

for k = 17,

$[kN] = [\sqrt{204119017}] = 14287$

$x = 14287 \to a = -1 \bullet 2^3 \bullet 3^4$

for k = 19,

$[kN] = [\sqrt{228133019}] = 15104$, $x = 15105$

$\to a = 2 \bullet 11 \bullet 19 \bullet 67$

for k = 21,

$[kN] = [\sqrt{252147021}] = 15879$, $x = 15879$

$\to a = -1 \bullet 2^2 \bullet 3 \bullet 5 \bullet 73$

At this point we remove the square factors from the quadratic residues we obtained in order to find new ones.

$a = -1 \bullet 2^4 \bullet 5 \bullet 23^2$ *gives* $a = -5$.

$a = -1 \bullet 7^2 \bullet 17^2$ *gives* $a = -1$.

As the product of two quadratic residues is itself a quadratic residue, the above quadratic residues when multiplied gives the quadratic residue a = 5.

$a=-1\cdot 2^6\cdot 5\cdot 89$ and a = -5 gives a = 89.

$a=-1\cdot 2^3\cdot 3^4$ gives a = 2.

a = 2 and $a=2^3\cdot 97$ gives a = 97.

$a=-3\cdot 31\cdot 73$ and $a=-1\cdot 2^2\cdot 3\cdot 5\cdot 73$ gives a = 31.

$a=-2^3\cdot 31\cdot 59$ gives a = 59.

$a=2\cdot 3\cdot 41\cdot 61$ and $a=-3\cdot 41\cdot 89$ gives a = 61.

Thus, we have the following set of small quadratic residues (mod 12007001); $a=-1, \pm 2, \pm 5, \pm 31, \pm 59, \pm 61, \pm 89$ and ± 97.

The second step in Gauss' method is to use the quadratic residues we found to reduce the number of possible prime factors of N. Since a = -1 is a quadratic residue mod N, only primes of the form p = 4k + 1 can divide N. a = 2 gives p = 8k ± 1. However, every prime of the form p = 4k + 1 is also of the form p = 8k + 1 = 4(2k) + 1. Thus, only primes of the form p = 8k + 1 are possible divisors of N. Since a = 5 is a quadratic residue mod N, this restricts the prime divisors of N to primes of the form p = 10k ± 1. Thus, a prime divisor of N must satisfy p = 8k + 1 and p = 10k + 1 for some k. If p = 8k + 1 and p = 10k + 1 then p must be of the form p = 40k + 1. If p = 8k + 1 and p = 10k -1 then p must be of the form p = 40k + 9.

Now we determine which of the primes of the two forms p = 40k + 1 and p = 40k + 9 below $[\sqrt{N}]=[\sqrt{12007001}]$ = 3465 has as a quadratic residue, all of the quadratic residues mod N that we obtained, namely, $a = \pm 2, \pm 31, \pm 59, \pm 61, \pm 89, \pm 97$ by computing the value of Legendre's symbol $\left(\frac{a}{p}\right)$. As soon as we find $\left(\frac{a}{p}\right) = -1$ for a prime p, that prime is eliminated as a possible divisor of N. This procedure eliminates about half of the remaining primes for each new value of a that is used. The only primes below 3465 of the form p = 40k + 1 or p = 40k + 9 such that $\left(\frac{31}{p}\right) = +1$ are: p = 41, 281, 521, 769, 1249, 1289, 1321, 1361, 1409, 1489, 1601, 1609, 1721, 2081, 2281, 2521, 2609, 2726, 3001, 3089, 3169, 3209, 3449.

We now compute the Legendre's symbol $\left(\frac{59}{p}\right)$ for these primes.

$\left(\frac{59}{p}\right) = +1$ for p = 41, 281, 521, 1361, 1609, 2081, 2729, 3001, 3089, 3449.

By computing $\left(\frac{61}{p}\right)$ for the above primes we find $\left(\frac{61}{p}\right) = +1$ for p = 41, 1361, 2729, 3001, 3089. Finally, by computing $\left(\frac{89}{p}\right)$, we find $\left(\frac{89}{p}\right) = +1$ for p = 3001. Thus, p = 3001 is a prime factor of N = 12007001. In fact, 12007001 = 3001•4001.

Gauss' factoring method becomes more complicated and tedious when the number of known quadratic residues mod N is large, say 100 or more quadratic residues are known. Other factoring methods will be presented in later chapters of this study, which like Gauss' factoring method, start by finding many small quadratic residues of N and breaking these up into prime factors. But, unlike Gauss' method, the quadratic residues in these methods are not used to restrict the possible prime factors of N. Instead, they are used to find nontrivial solutions to the congruence $x^2 \equiv y^2 \pmod{N}$. Three factoring methods, namely, the continued fraction method, the quadratic sieve method, and the number field sieve will be presented in this study, and are based upon the fact that any time we are able to obtain a nontrivial solution to the congruence $x^2 \equiv y^2 \pmod{N}$, we immediately find a factor of N.

2.4 Fermat's Factoring Method:

In this section, we present a very important factorization technique, known as Fermat factorization, which was discovered by Fermat in 1643. Although the method is not always efficient, it is of theoretical as well as some practical interest. Fermat's idea is employed in some of today's most powerful factoring algorithms, the quadratic sieve and the number field sieve algorithms. Fermat's method is based on the following Lemma.

<u>Lemma 2.6</u>

Let N be a positive odd integer. There is a one-to-one correspondence between factorization of N in the form $N = ab$, where $a \geq b > 0$, and representations of N in the form $x^2 - y^2$, where x and y are nonnegative integers.

Proof:

Let N be an odd positive integer and $N = a\,b$ be a factorization of N into two positive integers. Thus, N can be written as the difference of two squares

$N = ab = x^2 - y^2$, where $x = \frac{(a+b)}{2}$ and $y = \frac{(a-b)}{2}$ are both integers since a and b are both odd.

Conversely, if N is the difference of two squares, say $N = x^2 - y^2$, then we can factor N by noting that $N = ab$, where $a = x + y$ and $b = x - y$. Moreover, if $N = (x + y)(x - y) = z^2 - w^2$ then $z = x$ and $w = y$.

Suppose $N > 1$ is an odd, non-square integer, so we do not have to worry about the trivial exceptions. Thus, $N = a \bullet b$ for some integers a and b where $1 \leq a < b < N$. From Lemma 2.6, we know there exists nonnegative integers x and y such that $N = x^2 - y^2 = (x - y)(x + y)$, a factorization of N. The problem of factoring N is then reduced to finding nonnegative integers x and y such that $x^2 - y^2 = N$. Obviously, x must be greater than $\sqrt{N}$. Thus we start with x equal to the smallest integer greater than or equal to the square root of N. That is; we start with $x = [\sqrt{N}] + 1$.

Then we consider $z = x^2 - N$ and check whether this number is a square. If it is, we have $y^2 = x^2 - N$, hence $N = x^2 - y^2$ and we are done. Otherwise, we increase x by 1, i.e. we try $x = [\sqrt{N}] + 2$, and compute $([\sqrt{N}]+2)^2-N$, and test whether this is a square, and continue to search for a square among the sequence of integers $([\sqrt{N}]+3)^2-N$, $([\sqrt{N}]+4)^2-N$, ... This procedure is guaranteed to terminate, since the trivial factorization of $N = N \cdot 1$ leads to the equation
$N=\left(\frac{N+1}{2}\right)^2-\left(\frac{N-1}{2}\right)^2$, in which case N is prime.

We illustrate the above procedure by examples.

Example 1:

Let N = 2027651281.

$[\sqrt{N}]=45029$.

Thus, we start with x = 45030 and compute $z = x^2 - N$ = 49619, which is not a square. Then successively we compute $x^2 - N$ for x = 45031, 45032, ... until a square is found. The calculations are given in the table below:

Table 2.4

x	$x^2 - N$	x	$x^2 - N$	x	$x^2 - N$
45030	49619	45035	499944	450340	950319
45031	139680	45036	590015	45041	1040400 (square)

45032	229743	45037	680088		
45033	319808	45038	770163		
45034	409875	45039	860210		

From the table we have 1040400 = $(1020)^2$, then $y^2 = (1020)^2$. Hence $N = (45041)^2 - (1020)^2 = (45041 - 1020)(45041 + 1020) =$ 44021 • 46061.

<u>Example 2</u>: Factor N = 44021?

Solution: $[\sqrt{N}] = 209$. Thus we start with x = 210, and compute $z = x^2 - N$. $z = (210)^2 - 44021 = 79$ which is not a perfect square. Then successively we compute $x^2 - N$ for x = 210, 211, 212, ... until a square is found. The calculation is given in the table below.

Table 2.5

x	$x^2 - N$	x	$x^2 - N$
210	79	215	2204
211	500	216	2635
212	923	217	3068
213	1348	218	3503
214	1775	219	3940

These calculations terminate when $z = \left(\frac{N+1}{2}\right)^2 - N$ and this leads to the equation N = $\left(\frac{N+1}{2}\right)^2-\left(\frac{N-1}{2}\right)^2$.

i.e, 44021 = $\left(\frac{44022}{2}\right)^2-\left(\frac{44020}{2}\right)^2$ $=(22011)^2-(22010)^2$ $=44021$.

Thus N is a prime.

Remark:

In Fermat factorization one can rule out most of the non-square values of x^2 - N by looking at the last two digits of x^2 - N. The possible final two digits of a perfect square contain the following 22 combinations: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, and 96.

In Example 1, above, the only possible perfect squares are 499944 and 1040400. However, 499944 is not a square because it is divisible by 3 but is not divisible by 9.

We are now going to determine how much work is required to factor an integer N. If N = pq, with p < q and p and q are primes, then the factorization of N will be achieved when x = $\frac{p+q}{2}$ and y = $\frac{q-p}{2}$. Since the starting value of x is approximately $\sqrt{N}$ and q = $\frac{N}{p}$, for x to increase from $[\sqrt{N}]+1$ to $\frac{p+q}{2}$ will take approximately $\frac{p+\frac{N}{p}}{2}-\sqrt{N}=\frac{(\sqrt{N}-p)^2}{2p}$

steps. In particular, Fermat Factorization is most effective when x is close to $\sqrt{N}$. That is, when p and q are almost equal factors. In this case, the amount of work needed to find a factorization is small.

If N = ab, where a < b are not close in value, then one can attempt to find some multiplier k such that Nk admits a factorization into two very close factors. If we choose k $\approx \frac{b}{a}$, then Nk will have two factors $a \cdot k \approx b$ and b which are close. However, how can we find k when we do not know the size of $\frac{b}{a}$? We could choose numbers at random, hoping to produce an a and b of about the same size, or possibly successively try k = 1, 2, ..., $[N^{\frac{1}{3}}]$ and apply the Fermat Factorization to $N \cdot k$, for each value of k. Another method is to choose a highly composite integer (i.e. an integer containing many factors of different sizes) hoping that the factors of k will combine with the factors of N to produce a and b of about the same size and then we can apply Fermat Factorization to $N \cdot k$. Suitable choices of a highly composite integer k could be factorial numbers $1 \cdot 2 \cdot 3 \ldots m = m!$. Another systematic method of choosing m is due to Lehman [12]. Lehman's method of choosing m makes the time complexity of Fermat Factorization $O(N^{\frac{1}{3}})$.

Example:

We shall illustrate the idea of multiplying N by an integer k to produce factors a and b of N of about the same size by an example.

Let N = 64803 = 3•21601. Choose k = 7201, then $N \cdot k = 21603 \cdot 21601$. Then apply Fermat Factorization to $N \cdot k$.

The idea behind Fermat's method led to several of today's most powerful factorization algorithms. Maurice Kraitchick, in the 1920's realized that a major saving of time could be accomplished if, instead of looking for x and y satisfying $x^2 - y^2 = N$, we select x and y satisfying a congruence $x^2 \equiv y^2 \pmod{N}$. Finding such a pair of integers x and y satisfying the above congruence no longer guarantees a factorization of N. It does mean that $N | (x^2 - y^2)$ or $N | (x-y)(x+y)$. Thus, there is a chance that $gcd(x-y, N)$ or $gcd(x+y, N)$ will be a nontrivial factor of N. Kraitchick's approach for finding such pairs (x, y) was rather ad hoc.

A few years later, in 1931, D. H. Lehmer and R. Powers [13] showed how to find these pairs systematically by using continued fractions. Their algorithm, however, was not practical until the coming of high speed computers. With the advance in computer technology in early 1970, mathematicians realized that the Lehmer-Powers algorithm was worth re-examination. Daniel Shank [24] was one of the first to come up with a practical algorithm using Lehmer-

Powers and Kraitchick's ideas. Shank's method is called the square forms factorization. In 1975, John Brillhart and Michael Morrison [16] modified the Lehmer-Powers method to one of the fastest methods of factoring large integers that is still in use today. The Brillhart-Morrison method is called the continued fraction method and will be presented in Chapter 3. In 1981, Carl Pomerance [18] developed a different method called quadratic sieve, for finding x and y and it will be presented in Chapter 4. In 1990, John Pollard and others [14] developed the number field sieve, which will be presented in Chapter 5.

Chapter 3

The Continued Fraction Method

In this chapter, the continued fraction method (commonly known as CFRAC method) for factoring large integers is described. The method was discovered by John Brillhart and Michael Morrison in 1975 [16]. The original idea of the continued fraction method is actually due to D. H. Lehmer and R. E. Powers [13] and it draws much of its inspiration from Legendre's factorization method and an idea of Maurice Kraitchik [10].

3.1 The Kraitchik Factoring Scheme:

The continued fraction method is one of several factoring methods that utilize an idea of Kraitchik. If N is the number to be factored, then the idea is to multiply congruences $u \equiv v \pmod{N}$, where $u \neq v$ and complete or partial factorizations (depending on the method) have been obtained for u and v, so as to produce a square congruence $x^2 \equiv y^2 \pmod{N}$. Utilizing this approach, one stands a good chance that the greatest common divisor, $gcd(x-y, N)$ or $gcd(X+y, N)$ are nontrivial factors of N. These factoring methods have several phases:

1. Generation of Congruences $u \equiv v \pmod{N}$.
2. Determination of the complete or partial factorization of u or v for some of the congruences.
3. Determination of a subset of the factored congruences

which can be multiplied to produce a square congruence $x^2 \equiv y^2 \pmod{N}$.

4. The computation of $gcd(x-y,N)$ and $gcd(x+y,N)$ by the Euclidean algorithm.

The difference between these factoring methods lies in how the congruences $u \equiv v \pmod{N}$ are generated and the way the u's or v's are factored. For example in the continued fraction method, the congruences $u \equiv v \pmod{N}$ are obtained as in Legendre's factorization method, from the continued fraction expansion of $\sqrt{kN}$. Historically, the situation in the continued fraction method as well as the other factoring methods that utilized Kraitchik's idea is much the same as for Pollard's (p - 1) method. The underlying ideas have been known for quite a long time and occasionally have been applied to specific cases, in particular by D. H. Lehmer and R. E. Powers [13] and by Kraitchik himself [10]. The current version of the continued fraction method is due to Brillhart and Morrison who have systematically explored the potentials of these ideas and have constructed a good algorithm which has been put to extensive use on computers in the past twenty years. Before giving a full description of the continued fraction method, we need to establish a few preliminary results.

For every integer N, prime or composite, the square congruence $x^2 \equiv y^2 \pmod{N}$ has the trivial solutions $x \equiv \pm y$

(mod N). However, if N is composite and not a power of a prime, the square congruence also has other non-trivial solutions, which can be used to factor N. Assume that N is composite and we have a pair of integers x and y such that $x^2 \equiv y^2 \pmod{N}$ and $x \not\equiv \pm y \pmod{N}$; that is, x and y are nontrivial solution. Thus we have $x^2 \equiv y^2 \pmod{N}$, or $x^2 - y^2 \equiv (x - y)(x + y) \equiv 0 \pmod{N}$. Thus $N|(x-y)(x+y)$. But since $x \not\equiv \pm y \pmod{N}$, then $N\nmid(x+y)$ and $N\nmid(x-y)$. Hence $gcd(x+y,N) \neq 1$ or N and $gcd(x-y,N) \neq 1$ or N. Thus, $gcd(x+y,N)$ and $gcd(x-y,N)$ are proper factors of N.

Example:

Suppose we want to factor N = 4633. Note that x = 118 and y = 5 is a non-trivial solution to the square congruence $x^2 \equiv y^2 \pmod{4633}$. Thus, $gcd(118+5,4633)$ and $gcd(118-5,4633)$ are factors of N. By the Euclidean algorithm one can find $gcd(118+5,4633)=41$, and $gcd(118-5,4633)=113$. Hence $4633 = 41 \bullet 113$.

The reader might wonder where the solution x = 118 and y = 5 came from? As we mentioned earlier, several very important factorization methods make use of square congruences. However, they differ only in the way in which the solutions to the congruences $x^2 \equiv y^2 \pmod{N}$ are found. Next, we want to show that if N is composite and not a power of prime, then the square congruence has non-trivial solutions. To prove this fact, we use the following Lemma.

Lemma 3.1:

Let P be an odd prime and a an integer not divisible by P. Then the congruence $x^2 \equiv a \pmod{P}$ has either no solutions or exactly two incongruent solutions (mod P).

Proof:

If $x^2 \equiv a \pmod{P}$ has a solution, say $x = x_0$, then $x = -x_0$ is a second incongruent solution since $(-x_0)^2 \equiv x_0^2 \equiv a$ (mod P). We note that $x_0 \not\equiv -x_0 \pmod{P}$. For, if $x_0 \equiv -x_0$ (mod P), then $2x_0 \equiv 0 \pmod{P}$ i.e., $P|2x_0$. This is impossible (since P is odd and $P \nmid x_0$ since $x_0^2 \equiv a \pmod{P}$ and $P \nmid a$). To show that there are no more than two incongruent solutions, assume that $x = x_0$ and $x = x_1$ are both solutions of $x^2 \equiv a$ (mod P). Then we have $x_0^2 \equiv x_1^2 \equiv a \pmod{P}$, so that

$x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{P}$. Hence $p|(x_0 + x_1)$ or $p|(x_0 - x_1)$ so that $x_1 \equiv x_0 \pmod{P}$ or $x_1 \equiv x_0 \pmod{P}$.

Therefore, if there is a solution of $x^2 \equiv a \pmod{P}$, there are exactly two incongruent solutions.

Corollary:

The congruence $x^2 \equiv a^2 \pmod{P}$ for any prime has precisely two solutions (mod P), namely $x \equiv \pm a \pmod{P}$.

Now, consider the congruences $u^2 \equiv y^2 \pmod{P}$ and $u^2 \equiv y^2$ (mod q), where y is considered as a fixed integer P and q are two distinct odd primes with $P \nmid y$ and $q \nmid y$. Thus, the congruence $x^2 \equiv y^2$ (mod pq) has four solutions, which we may find by combining in four ways the two solutions (mod P) and the two solutions (mod q):

$$\left\{\begin{matrix} u \equiv y \pmod{P} \\ u \equiv y \pmod{q} \end{matrix}\right\} \text{ giving } x \equiv y \pmod{Pq},$$

$$\left\{\begin{matrix} u \equiv -y \pmod{P} \\ u \equiv -y \pmod{q} \end{matrix}\right\} \text{ giving } x \equiv -y \pmod{Pq},$$

$$\left\{\begin{matrix} u \equiv y \pmod{P} \\ u \equiv -y \pmod{q} \end{matrix}\right\} \text{ giving } x \equiv z \pmod{Pq},$$

$$\left\{\begin{matrix} u \equiv -y \pmod{P} \\ u \equiv y \pmod{q} \end{matrix}\right\} \text{ giving } x \equiv -z \pmod{Pq}.$$

Thus, if N = Pq, the congruence $x^2 \equiv y^2$ (mod N) has four solutions, namely, the trivial solutions $x \equiv \pm y$ (mod N), and one more pair of solutions $x \equiv \pm z$ (mod N).

Example:

Let N = 77 = 7 • 11. Consider the congruence $x^2 \equiv y^2$ (mod 77). $u^2 \equiv (36)^2$ (mod 7) has two solutions (mod 7), namely $u \equiv \pm 36$ (mod 7). $u \equiv (36)^2$ (mod 11) has two solutions (mod 11), namely $u \equiv \pm 36$ (mod 11). By combining these solutions we have

$$\left\{\begin{matrix} u \equiv 36 \pmod{7} \\ u \equiv 36 \pmod{11} \end{matrix}\right\} \rightarrow x \equiv 36 \pmod{77}$$

$$\left\{\begin{matrix} u \equiv -36 \pmod{7} \\ u \equiv -36 \pmod{11} \end{matrix}\right\} \rightarrow x \equiv -36 \pmod{77}$$

$\begin{cases} u \equiv 36 \pmod{7} \\ u \equiv -36 \pmod{11} \end{cases} \rightarrow x \equiv 8 \pmod{77}$

$\begin{cases} u \equiv -36 \pmod{7} \\ u \equiv 36 \pmod{11} \end{cases} \rightarrow x \equiv -8 \pmod{77}$

Thus x = 36 and y = 8, satisfying the congruence $x^2 \equiv y^2$ (mod 77).

If N has more than two prime factors, the method still works in a similar way since the above reasoning can be applied to one of the prime factors p and the corresponding co-factor a = $\frac{N}{p}$, which in this case will be composite.

3.2 The Continued Fraction Algorithm:

We are now ready to present the continued fraction algorithm. First, we give an outline of the algorithm. Let N > 1 be an odd, composite integer that we seek to factor. The algorithm has four major steps:

<u>Step I</u>: The Expansion step.

In this step, the regular continued fraction expansion of $\sqrt{N}$ or $\sqrt{kN}$ for some suitably chosen integer k > 1 is computed. Using the notations of Theorem 1.6, we have: For each value of i, $1 \le i \le N_0$, we have $A_i^2 - kNB_i^2 = (-1)^{i+1}Q_{i+1}$, and hence $A_i^2 \equiv (-1)^{i+1}Q_{i+1}$ (mod kN), where $\frac{A_i}{B_i}$ is the ith convergent of $\sqrt{kN}$. Each pair of positive integers (A_i, Q_{i+1}) on the last congruence is called an "A - Q pair".

Step II: Finding square sets (or s-sets)

In this step we use some of the A-Q pairs generated in Step I to form certain subsets of integers, called square sets or s-sets, each having the property that $\prod_{j=1}^{m} (-1)^{i_j} Q_{i_j}$ is a square. If no s-set can be found, we return to step I to expand $\sqrt{kN}$ further.

Step III: Finding solutions to $x^2 \equiv y^2$ (mod kN).

Each s-set found in step II can be used to find a solution to the square congruence $x^2 \equiv y^2$ (mod kN). Let $\prod_{j=1}^{m} (-1)^{i_j} Q_{i_j} = Q^2$. We set x = $A_{i_1} \bullet A_{i_2} \bullet \ldots A_{i_m}$ (mod kN), where A_{i_j} are the integers corresponding to the Q_{i_j} in the (A - Q) pairs, we found in step I, for j = 1, 2, ..., m. The $x^2 \equiv A_{i_1}^2 \bullet A_{i_2}^2 \bullet \ldots \bullet A_{i_m}^2$ (mod kN), and since $A_{i_j}^2 \equiv (-1)^{i_j} Q_{i_j}$ (mod kN) individually, then $x^2 \equiv A_{i_1}^2 \bullet A_{i_2}^2 \bullet \ldots \bullet A_{i_m}^2 \equiv \prod_{j=1}^{m} Q_{i_j} \equiv Q^2$ (mod kN) is a solution to the square congruence $x^2 \equiv y^2$ (mod kN). This congruence may fail to factor kN if x ≡ y or x ≡ -y (mod kN). In this case we use another s-set and if no s-set gives a non-trivial solution to the congruence $x^2 \equiv y^2$ (mod kN), we can go back to step I and expand $\sqrt{kN}$ further.

Step IV: Computing $gcd(x-y, kN)$ and $gcd(x+y, kN)$.

The final step in the continued fraction method is the calculation of $gcd(x-y, kN)$ and $gcd(x+y, kN)$ by the Euclidean algorithm for non-trivial solutions x and y. Then $gcd(x-y, kN) = u$ and $gcd(x+y, kN) = v$ are non-trivial factors of kN.

We now explain steps I - IV, outlined above, and give examples to illustrate each step.

Step I: The Expansion Step.

Expand $\sqrt{kN}$ for a suitably chosen integer k > 1, into a simple continued fraction by the following algorithm:

The expansion algorithm generates the integers: A_n, Q_n, b_n, r_n and P_n, n = 1, 2, ...

(i) Set $A_{-1} = 0$, $A_0 = 1$, $Q_{-1} = kN$, $r_0 = g = [\sqrt{kN}]$ $P_0 = 0$ and $Q_0 = 1$.

(ii) We use the following formula $r_{n+1} = (g+P_n) \bmod Q_n$ ... (1) to generate r_n for $n \geq 1$.

(iii) Compute b_n, $n \geq 1$ from the formula $b_{n+1} = \left[\frac{(g+P_n)}{Q_n}\right]$.. (2)

(iv) We use the recursion formula $A_{n+1} \equiv b_{n+1}A_n + A_{n-1} (\text{mod} kN)$.. (3) to compute A_n (mod kN) for $n \geq 0$.

(v) We use the formula $g + P_{n+1} = 2g - r_{n+1}$ ... (4) to generate $g + P_{n+1}$ for $n \geq 0$.

(vi) We use the formula $Q_{n+1}=Q_{n-1}+b_{n+1}(r_{n+1}-r_n)$ ... (5) to generate Q_{n+1} for $n \geq 0$.

(vi) Increase n by 1 and return to (ii).

Remarks:

1. Recall that the integers Q_n and P_n satisfy the inequalities $0 \leq P_n < \sqrt{kN}$ and $0 < Q_n < 2\sqrt{kN}$ for $n \geq 0$. Thus, the Q_n's and P_n's are small compared to N.

With little luck we may find a complete factorization of some of the Q_n's by trial division. The pairs (A_n, Q_{n+1}) where Q_{n+1} is too difficult to factor by trial division are simply discarded. In this way, only Q_{n+1}, having small prime factors, are saved for later use to generate the s-sets in step II. In factoring some of the Q_n's an attempt will be made to choose a relatively small fixed set of primes, called the factor base, and use trial division to consider only those Q_n's that have all of their prime factors in the factor base. Using a factor base to factor some of the Q_n's saves trial divisions and discards pairs (A_n, Q_{n+1}) having little chance of entering an s-set.

2. To calculate $g = [\sqrt{kN}]$ one may use the following modification of the Newton-Raphson method:

   a. Choose a number x_0 such that $x_0 > \sqrt{kN}$.

   b. For $n \geq 0$ successively compute $x_{n+1} = \left[\dfrac{x_n^2 + kN}{2x_n}\right]$

c. When $x_{n+1} - x_n \geq 0$, then $g = x_{n+1}$.

3. Since the continued fraction expansion of $\sqrt{N}$ is periodic, in those cases where the period of $\sqrt{N}$ is too short for the method to succeed, it is necessary to choose an integer $k > 1$ and expand $\sqrt{kN}$. Selecting an integer $k > 1$, may result in including more small primes as possible divisors of Q_n than by using $k = 1$. On the other hand, a large value of k will make the Q_n's larger, hence will be less likely to factor completely. We want to balance these tendencies by choosing k wisely. R. Schroeppel suggests that the best choice of k is the value that maximizes

$$\sum_{p\ prime} f(p, kN) \log p = \frac{1}{2} \log k, \text{ where}$$

$f(p, kN)$ = the average number of times p divides $A^2 - (kN)B^2$, when A and B are two relatively prime independent random integers and the sum is over all primes less than or equal to p_m, where p_m is the largest prime in the factor base. The function $f(p, d)$ is given by

$$f(p, d) = \begin{cases} \dfrac{2p}{p^2-1} & if\ d^{\frac{p-1}{2}} \bmod p = 1 \\ 0 & if\ d^{\frac{p-1}{2}} \bmod p = p-1 \end{cases} .$$

For more details about the selection of k, see Knuth [7] and Morrison and Brillhart[16].

<u>Example 1</u>:

Let N = 77 and k = 2. Table 3.1 contains the results of the expansion of $\sqrt{kN}$ up to n_0 = 21 in a simple continued fraction. $g = [\sqrt{2*77}] = 12$

<u>Example 2</u>:

Let N = 13290059 and k = 1. Then $g = [\sqrt{13290059}] =$ 3645. Table 3.2 contains selected results from the expansion of $\sqrt{N}$.

Table 3.1

n	A_n mod N	Q_n	b_n	r_n	P_n	Q_n Factored
-1	0	154	-	-	-	-
0	1	1	-	12	0	1
1	12	10	12	0	12	2 • 5
2	25	9	2	4	8	3 • 3
3	62	6	2	2	10	2 • 3
4	57	15	3	4	8	3 • 5
5	42	7	1	5	7	7
6	64	15	2	5	7	3 • 5
7	29	6	1	4	8	2 • 3

8	74	9	3	2	10	3 • 3
9	23	10	2	4	8	2 • 5
10	43	1	2	0	12	1
11	54	10	24	0	12	2 • 5
12	74	9	2	4	8	3 • 3
13	48	6	2	2	10	2 • 3
14	64	15	3	4	8	3 • 5
15	35	7	1	5	7	7
16	57	15	2	5	7	3 • 5
17	15	6	1	4	8	2 • 3
18	25	9	3	2	10	3 • 3
19	65	10	2	4	8	2 • 5
20	1	1	2	0	12	1
21	12	10	24	0	12	2 • 5
22	25	9	2	4	8	3 • 3

Table 3.2

n	A_n Mod N	Q_n	b_n	r_n	P_n	Q_n Factored
-1	0	13290059	-	-	-	-

0	1	1	-	3645	0	1
1	3645	4034	3645	0	3645	2•2017
2	3646	3257	1	3256	389	3257
3	7291	1555	1	777	2868	5•311
4	32810	1321	4	293	3352	1321
5	1713412	2050	5	392	3253	$2 \cdot 5^2 \cdot 41$
10	6700527	1333	3	748	2673	31•43
22	5235158	4633	4	986	1134	41•113
23	1914221	226	1	146	3499	2•113
26	11455708	3286	31	138	1977	2•31•53
31	1895246	5650	1	2336	2603	$2 \cdot 5^2 \cdot 113$
40	3213960	4558	1	598	2931	2•43•53
52	2467124	25	1	2018	3628	5^2

Step II: Finding S-Sets

In this step, we need to determine if any s-sets exist in the set of (A_n, Q_{n+1}) pairs generated in step I and to devise a procedure to find them when they exist.

A simple procedure can be used to both determine if any s-sets exist and to find them when they do exist. The idea is to factor some of the Q_n's over a relatively small fixed set of primes, called the factor base, so that some subset of the factored Q_n's, when multiplied together will give an integer c whose square is congruent to a perfect square mod N. The details follow.

Definition 3.1:

A factor base is a set $B = \{P_1, P_2, \ldots, P_h\}$ of distinct primes, except that P_1 may be the integer -1.

Definition 3.2:

Let B be a factor base. An integer a is called a B-number (for a given N) if the integer c that is defined by the conditions (i) and (ii) below can be written as a product of numbers from B.

(i) $c = a^2 \bmod N$ (ii) $-\frac{N}{2} \leq c \leq \frac{N}{2}$.

The number c is called the least absolute residue of a mod N.

Examples:

(1) For N = 4633 and B = {-1, 2, 3} the integers $a^1 = 67$, $a_2 = 68$, and $a_3 = 69$ are B-numbers for $a_1^2 \equiv 67^2 \equiv -144 \pmod{4633}$ and $-144 = -1 \cdot 2^4 \cdot 3^2$.

$a_2^2 \equiv 68^2 \equiv -9 \pmod{4633}$ and $-9 = -1 \cdot 3^2$.

$a_3^2 \equiv 69^2 \equiv 128 \pmod{4633}$ and $128 = 2^7$.

(2) For $N = 1729$ and $B = \{-1, 2, 5\}$, show that $a_1 = 186$ and $a_2 = 267$ are B-numbers.

Let Z_2^h denote the vector space whose elements consists of h-tuples of zeros and ones over the field of two elements Z_2. We are given an integer N and $B = \{P_1, P_2, \ldots, P_h\}$ as a factor base. Let a be a B-number then the least absolute residue of a (mod N) can be written as $\Pi_{j=1}^{h} p_j^{\alpha_j}$ where $\alpha_j \geq 0$.

We associate a vector $\varepsilon(a) \in Z_2^h$ with a where $\varepsilon(a) = (\alpha_1 \pmod 2), \alpha_2 \pmod 2) \ldots, \alpha_h \pmod 2))$. Note that $\alpha_i \pmod 2 = \begin{cases} 0 & \text{if } \alpha_i \text{ is even} \\ 1 & \text{if } \alpha_i \text{ is odd} \end{cases}$.

<u>Example</u>:

In example (1) above, the vector associated with a = 67 is $\varepsilon(67) = (1, 0, 0)$, the vector associated by a = 68 is $\varepsilon(68) = (1, 0, 0)$ and the vector associated with a = 69 is $\varepsilon(69) = (0, 1, 0)$.

Suppose we have a set of B-numbers $\{a_1, a_2, \ldots, a_n\}$ such that the corresponding vectors $\varepsilon_i = (\varepsilon_{i1}, \varepsilon_{i2}, \ldots, \varepsilon_{ih})$, $i = 1, 2, \ldots, n$ add up to the zero vector in Z_2^h. Let C_i, $i = 1, 2, \ldots, n$ be the least absolute residues of a_i (mod N). Write each C_i as $c_i = \Pi_{j=1}^{h} P_j^{\alpha_{ij}}, \alpha_{i_j} \geq 0$. Then

$\prod_{i=1}^{h} C_i = \prod_{i=1}^{h} \left(\prod_{j=1}^{h} P_j^{\alpha_{ij}} \right) = \prod_{j=1}^{h} P_j^{\Sigma_{i=1}^{n} \alpha_{ij}}$. The exponent $\sum_{i=1}^{h} \alpha_{i_j}$ of each

P_j on the right hand side is an even number. Thus $\prod_{j=1}^{h} P_j^{\Sigma_{i=1}^{n} \alpha_{ij}}$ is a square. If we set $\gamma_j = \frac{1}{2} \sum_{i=1}^{n} \alpha_{i_j}$ then

$\prod_{j=1}^{h} p_j^{\Sigma_{i=1}^{n} \alpha_{ij}} = \left(\prod_{j=1}^{h} p_j^{\gamma_j} \right)^2$. Set a = $\prod_{i=1}^{n} a_i$ mod N (least positive

residue) and c = $\prod_{j=1}^{h} P_j^{\gamma_j}$ mod N (least positive residue). We

have $c_i \equiv a_i^2$ (mod N) for each i = 1, 2, ..., n, thus $\prod_{i=1}^{n} C_i \equiv \prod_{i=1}^{n} a_i^2$ (mod N) and hence $c^2 = (\prod_{j=1}^{h} p_j^{\gamma_j})^2 \equiv \prod_{i=1}^{n} a_i^2 \equiv a^2$ (mod N).

When can we be sure that we have enough B-numbers a_i so that the sum of the corresponding vectors ε_i is the zero vector? In other words, given a collection of vectors in $\mathbf{Z}_2^h$, when can we be sure of being able to find a subset of them whose sum is zero? This happens if the set of vectors in the collection is linearly dependent over the field $\mathbf{Z}_2$. From linear algebra we know this is guaranteed to occur if the number of vectors in the collection is larger than or equal to h + 1. Thus, at worst we will have to generate h + 1 different B-numbers in order that $(\Pi_i a_i)^2 \equiv (\Pi_j p_j^{\gamma_{ij}})^2 \bmod N$.

Of course, we may obtain a linearly dependent set of vectors sooner.

Example:

Let N = 4633 and B = {-1, 2, 3}. Example (1) above demonstrates that the integers $a_1 = 67$ and $a_2 = 68$ are B-numbers. The vectors corresponding to a_1 and a_2 are $\varepsilon_1 = (1, 0, 0)$ and $\varepsilon_2 = (1, 0, 0)$. $\varepsilon_1 + \varepsilon_2 = (1, 0, 0) + (1, 0, 0) = (0, 0, 0)$. We compute a = 67 • 68 (mod 4633) and obtain a ≡ -77 (mod 4633). The least absolute residues of a_1 and a_2 as (mod 4633) are respectively

$c_1 = -144 = -1 \cdot 2^4 \cdot 3^2$

$c_2 = -9 = -1 \cdot 3^2$.

$c_1 \cdot c_2 = (-1)^2 \cdot 2^4 \cdot 3^4 \Rightarrow \gamma_1 = 1, \gamma_2 = 2$ and $\gamma_3 = 2$. Thus $c = -1 \cdot 2^2 \cdot 3^2 = -36$. Note that $(-77)^2 \equiv (-36)^2$ (mod 4633).

Example:

Let N = 4633 and B = {-1, 2, 3, 5}. The integers $a_1 = 68$, $a_2 = 69$, and $a_3 = 96$ are B-numbers. The vectors corresponding to these numbers are respectively $\varepsilon_1 = (1, 0, 0, 0)$, $\varepsilon_2 = (0, 1, 0, 0)$ and $\varepsilon_3 = (1, 1, 0, 0)$. $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = (0, 0, 0, 0)$. We compute a = 68 • 69 • 96 (mod 4633) and obtain a ≡ 1031 (mod 4633). The least absolute residues of a_1, a_2, and a_3 mod 4633 are respectively:

$c_1 = -9 = -1 \cdot 3^2$

$c_2 = 128 = 2^7$

$c_3 = -50 = -1 \cdot 2 \cdot 5^2$

$\therefore\ c_1 \cdot c_2 \cdot c_3 = (-1)^2 \cdot 2^8 \cdot 3^2 \cdot 5^2 \rightarrow \gamma_1 = 1,\ \gamma_2 = 4,\ \gamma_3 = 1,\ \gamma_4 = 1.$

Thus, $c = -1 \cdot 2^4 \cdot 3^1 \cdot 5^1 = -240$. $a^2 = (1031)^2 \equiv (-240)^2 \pmod{4633}$.

In the examples we presented above, we were able to find a subset of vectors ε_i which sums to zero. However, if the factor base has many elements, that is, if h is large, we might not be able to find a subset of vectors ε_i which sum to zero just by inspection. In that case, we write the vectors ε_i as rows in a matrix and use a process similar to the Gaussian elimination method to find a linearly dependent set of rows. First, we write the vectors ε_i as rows in a matrix (E_{ij}). Then we start reducing this matrix to a form where, for each j, only one row has its left most 1 in column j. This is accomplished by performing the following for $j = 1, 2, \ldots, m$. If more than one row has its left most 1 in column j, we keep the first row with 1 in column j and add this row to the rows below it that have 1 in column j. As the reduction proceeds, we keep a record of the actual contents of each row as a sum of ε_i. When the reduction is completed, the reduced matrix is searched for occurrences of zero rows. Since each row is recorded as a sum of $\varepsilon_{1,}$ these vectors are linearly dependent. We illustrate the procedure above by examples.

<u>Example</u>:

Let B = {-1, 2, 3, 5}.

$a_1 = 15 = 3 \bullet 5 \rightarrow \varepsilon_1 = (0, 0, 1, 1)$

$a_2 = 9 = 3^2 \rightarrow \varepsilon_2 = (0, 0, 0, 0)$

$a_3 = -10 = -1 \bullet 2 \bullet 5 \rightarrow \varepsilon_3 = (1, 1, 0, 1)$

$a_4 = 15 = 3 \bullet 5 \rightarrow \varepsilon_4 = (0, 0, 1, 1)$

$a_5 = -6 = -1 \bullet 2 \bullet 3 \rightarrow \varepsilon_5 = (1, 1, 1, 0)$

n	-1	2	3	5
1	0	0	1	1
2	0	0	0	0
3	1	1	0	1
4	0	0	1	1
5	1	1	1	1

Starting in column 1, we keep row 3 unchanged and replace row 5 by the sum of row 5 and row 3 (note that we record rows are summed to the left). To get:

n	-1	2	3	5
1	0	0	1	1
2	0	0	0	0
3	1	1	0	1

4	0	0	1	1
3+5	0	0	1	1

Since no row has its left-most 1 in column 2, we proceed to column 3. We keep row 1 and replace row 4 by the sum of rows 1 and row 4 and replace the new row 5 by the sum of this row and row 1 and get:

n	-1	2	3	5
1	0	0	1	1
2	0	0	0	0
3	1	1	0	1
1+4	0	0	0	0
1+3+5	0	0	0	0

No row has its left-most 1 in column 4. Therefore the reduction is completed, and the following sets of vectors are identified as linearly dependent: $\{\varepsilon_2\}$, $\{\varepsilon_1, \varepsilon_4\}$ and $\{\varepsilon_1, \varepsilon_3, \varepsilon_5\}$. The question that remains to be answered in this step is, how do we choose a factor base and B-numbers in factoring an integer N? The answer to this question is given by the following theorem.

<u>Theorem 3.2</u>:

If in the continued fraction expansion of $\sqrt{kN}$ an odd prime p divides Q_n, $n \geq 1$, then the value of the Legendre symbol $(\frac{kN}{p}) = +1$ or 0.

<u>Proof</u>: Suppose $n \geq 1$ and $p | Q_n$. In this case the identity $A_{n-1}^2 - kNB_{n-1}^2 \equiv (-1)^n Q_n \equiv 0 \pmod{p}$ implies $A_{n-1}^2 \equiv kNB_{n-1}^2 \pmod{p}$. However, p cannot divide B_{n-1}, since by corollary 1 to Theorem 1.4, $\gcd(A_{n-1}, B_{n-1}) = 1$. Thus, $\left(\frac{A_{n-1}}{B_{n-1}}\right)^2 \equiv kN$ (mod p). That is, kN is a quadratic residue of p, hence $\left(\frac{kN}{p}\right) = 1$ if $p \nmid kN$ and if $p | kN$ then $\left(\frac{kN}{p}\right) = 0$. This completes the proof.

The factor base can now be chosen by selecting the smallest possible odd primes $p_2, p_3, \ldots, p_B$ for which $\left(\frac{kN}{p_i}\right) = 0$ or 1. In addition, the prime $p_1 = 2$ and $p_0 = -1$ (that is needed to hold the sign of Q_n) are always included in the factor base. The parameter $B \approx [\sqrt[4]{kN}]$.

The B-numbers are the Q_n's that factor completely over the factor base. The other Q_n's are discarded.

<u>Example</u>:

Let $N = 77$, $k = 2$.

The following table contains some "A - Q" pairs of the continued fraction expansion of $\sqrt{2 \cdot 77} = \sqrt{154}$, and the vectors associated with each factored Q_n.

Table 3.3

n	A_n mod 154	A_n^2 mod 154	$(-1)^n Q_n$	Factorization of Q_n
1	12	144	-10	$-1 \cdot 2 \cdot 5$
2	25	9	9	$3 \cdot 3$
3	62	148	-6	$-1 \cdot 2 \cdot 3$
4	57	15	15	$3 \cdot 5$
5	42	70	-7	$-1 \cdot 7$
6	64	92	15	$3 \cdot 5$
7	29	71	-6	$-1 \cdot 2 \cdot 3$
8	74	86	9	$3 \cdot 3$
9	23	67	-10	$-1 \cdot 2 \cdot 5$
10	43	1	1	1

Since $\left(\frac{154}{3}\right) = \left(\frac{154}{5}\right) = 1$ and $B = [\sqrt[4]{154}] = 3$, we choose

factor base $B = \{-1, 2, 3, 5\}$. By applying the

Gaussian elimination method to the vectors $\varepsilon_{n,}$ we obtain

Table 3.4

k	ε_k	k	ε_k	k	ε_k
1	1 1 0 1	1	1 1 0 1	1	1 1 0 1
2	0 0 0 0	2	0 0 0 0	2	0 0 0 0
3	1 1 1 0	1+3	0 0 1 1	1+3	0 0 1 1
4	0 0 1 1	4	0 0 1 1	1+3+4	0 0 0 0
5	0 0 1 1	5	0 0 1 1	1+3+5	0 0 0 0
6	1 1 1 0	1+6	0 0 1 1	1+3+1+6	0 0 0 0
7	0 0 0 0	7	0 0 0 0	7	0 0 0 0
8	1 1 0 1	1+8	0 0 0 0	1+8	0 0 0 0

After developing step III below, we will use the results of this example to find a complete factorization of N=77.

Step III: Finding solutions to $x^2 \equiv y^2 \pmod{kN}$

Assume that in step II, above, we obtained a subset of "A- Q" pairs, such that Q_{i1}, Q_{i2}, ..., Q_{im} are completely factored over the factor base and their product is a square. That is, $\Pi_{j=1}^{m}(-1)^{i_j}Q_{i_j}=Q^2$. Let x_j

$= A_{i_j}$, j = 1, 2, ..., m be the corresponding value of Q_{i_j} in the "A - Q" pairs. Set $y_j = (-1)^{i_j} \bullet Q_{i_j}$ for j = 1, 2, ..., m. Thus, the set of pairs (x_j, y_j) satisfy the conditions $\Pi_{j=1}^{m} y_j = Q^2$ and $x_j^2 \equiv y_j$ (mod kN) for j = 1, 2, ..., m. Let $x = \prod_{j=1}^{m} x_j$ (mod kn), then $x^2 = \Pi_{j=1}^{m} x_j^2$.

Thus, $x^2 \equiv Q^2$ (mod kN) is a solution to the square congruence $x^2 \equiv y^2$ (mod kN). This congruence may fail to factor kN (if $x \equiv y$ (mod kN) or $x \equiv -y$ (mod kN)). In this case, we would look for another square set until we either find one or determine that if no square sets exist. In the latter case, we would go back and continue to expand $\sqrt{kN}$ to obtain more "A - Q" pairs.

<u>Example</u> (Continuation of Last Example)

From the previous example, $(-1)^2\ Q_2 = 9$ is a square. Thus, $x_1 = 25$, $y_1^2 = 9$ is a solution of $x^2 \equiv y^2$ (mod 154).

Other solutions of $x^2 \equiv y^2$ (mod 154) are:

$y_2^2 = (-1)^1\ Q_1 \bullet (-1)^3\ Q_3 \bullet (-1)^4\ Q_4 = 900$,

$x_2 = A_1 \bullet A_3 \bullet A_4$ mod 154 = 58

$y_3^2 = (-1)^1\ Q_1 \bullet (-1)^3\ Q_3 \bullet (-1)^6\ Q_6 = 900$

$x_3 = A_1 \bullet A_3 \bullet A_1 \bullet A_6 \bmod 154 = 30$ (trivial solution)

$y_4^2 = (-1)^1\ Q_1 \bullet (-1)^3\ Q_3 \bullet (-1)^1\ Q_1 \bullet (-1)^7\ Q_7 = 3600$

$x_4 = A_1 \bullet A_3 \bullet A_1 \bullet A_7 \bmod 154 = 38$

Compute $\gcd(kN,\ x_1 - y_1) = \gcd(154,\ 22) = 22 = 2 \bullet 11$

$\gcd(kN,\ x_2 - y_2) = \gcd(154,\ 28) = 14 = 2 \bullet 7$

$\gcd(kN,\ x_4 - y_4) = \gcd(154,\ 22) = 22 = 2 \bullet 11$

Thus $154 = 2 \bullet 7 \bullet 11$.

<u>Example</u>: Factor N = 1711, as another illustration of the continued fraction algorithm.

<u>Step 1</u> The Expansion step:

The following table contains the expansion of $\sqrt{N}$ up to k = 12.

Table 3.5

k+1	A_k	Q_{k+1}	Factorization of (Q's)
1	41	-30	$-1 \bullet 2 \bullet 3 \bullet 5$
2	83	45	$3 \bullet 3 \bullet 5$
3	124	-23	$-1 \bullet 23$
4	331	57	$3 \bullet 19$
5	455	-6	$-1 \bullet 2 \bullet 3$

6	-598	5	5
7	-558	-38	-1 • 2 • 19
8	-3	9	3 • 3
9	-582	-54	-1 • 2 • 3 • 3 • 3
10	-585	-25	-1 • 5 • 5
11	-41	-30	-1 • 2 • 3 • 5
12	-667	29	29
13	336	-30	-1 • 2 • 3 • 5

The factor base = {-1, 2, 3, 5, 19}

The Q's which are factored completely over the factor base are: -30, 45, 57, -6, 5 ,-38, 9, -54, 25, -30.

The corresponding vectors to these Q's are the following.

ε_1 (-30) = (1, 1, 1, 1, 0) ε_2(45) = (0, 0, 0, 1, 0)

ε_3 (57) = (0, 0, 1, 0, 1) ε_4(-6) = (1, 1, 1, 0, 0)

ε_5 (5) = (0, 0, 0, 1, 0) ε_6(-38) = (1, 1, 0, 0, 1)

ε_7 (9) = (0, 0, 0, 0, 0) ε_8(54) = (1, 1, 1 ,0,0)

ε_9 (25) = (0,0, 0, 0, 0) ε_{10}(-30) = (1, 1, 1, 1,0)

<u>Step II</u>: Finding Square Sets (S-sets):

In this step, we form the binary matrix whose rows are the above vectors, then apply a Gaussian elimination method on this matrix to obtain zero-rows.

n	-1	2	3	5	19
1	1	1	1	1	0
2	0	0	0	1	0
3	0	0	1	0	1
4	1	1	1	0	0
5	0	0	0	1	0
6	1	1	0	0	1
7	0	0	0	0	0
8	1	1	1	0	0
9	0	0	0	0	0
10	1	1	1	1	0

The reduced matrix will be as follows:

n	-1	2	30	5	19
1	1	1	1	1	0
2	0	0	0	1	0

3	0	0	1	0	1
1+4+2	0	0	0	0	0
2+5	0	0	0	0	0
1+3+6+2	0	0	0	0	0
7	0	0	0	0	0
1+8+2	0	0	0	0	0
9	0	0	0	0	0
1+10	0	0	0	0	0

After the reduction is completed, the following sets of vectors are linearly dependent and lead to a solution to the congruence $x^2 \equiv y^2 \pmod{1711}$.

a) $\{\varepsilon_1, \varepsilon_2, \varepsilon_4\}$

b) $\{\varepsilon_2, \varepsilon_5\}$

c) $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_6\}$

d) $\{\varepsilon_7\}$

e) $\{\varepsilon_1, \varepsilon_2, \varepsilon_8\}$

f) $\{\varepsilon_9\}$

g) $\{\varepsilon_1, \varepsilon_{10}\}$

Step III: Finding solutions to Legendre's Congruence $x^2 \equiv y^2 \pmod{N}$.

Each s-set found in step II can be used to find a solution to the Legendre congruence $x^2 \equiv y^2 \pmod{N}$.

1) set (a). Let $x = A_1 \bullet A_2 \bullet A_3 = 41 \bullet 83 \bullet 455$ $= 1548365$. Let $y^2 = Q_1 \bullet Q_2 \bullet Q_3 = (-1)^2\ (2 \bullet 3^2 \bullet 5)^2 \rightarrow$ $y = 90$. Since $1584365 \equiv -90 \pmod{1711}$, this set does not lead to factorization of N.

2) set (b). Let $x = A_2 \bullet A_6 = 83 \bullet 598 = 49634$
Let $y^2 = Q_2 \bullet Q_6 = (3 \bullet 5)^2 \rightarrow y = 15$. Since $49634 \equiv 15 \pmod{1711}$, this set also does not lead to factorization of N. The same results are obtained for sets c and d

3) set (e). Let $x = A_1 \bullet A_2 \bullet A_8 = 41 \bullet 83 \bullet 582 =$ 1980546. Let $y^2 = Q_1 \bullet Q_2 \bullet Q_9 = -30 \bullet 45 \bullet -54 =$ $(-1)(2 \bullet 3 \bullet 5)(3 \bullet 3 \bullet 5)(-1)\ (3 \bullet 3 \bullet 3)(2) =$ $(-1)^2\ (2 \bullet 3^3 \bullet 5)^2$, then
$y = 2 \bullet 3^3 \bullet 5 = 270$.

Since $x \not\equiv \pm\ y \bmod N$, we have now a great chance of factoring N.

<u>Step IV</u>: Computing gcd$(x - y, N)$ or gcd$(\ x + y, N)$:

We apply the Euclidian algorithm to find gcd$(x - y, N)$

$x - y = 1980276$

$1980276 = 1157 \bullet 1711 + 649$

$1711 = 2 \bullet 649 + 413$

$413 = 1 \bullet 236 + 177$

$236 = 1 \bullet 177 + 59$

$177 = 3 \bullet 59$

Thus, gcd$(1980276, 1711) = 59$, which is a factor of

1711. $\frac{1711}{59} = 29$. Therefore, 59 and 29 are the factors of 1711.

3.3 Concluding Remarks:

No one as yet has offerred a complete explanation as to why the continued fraction algorithm is able to factor large numbers so successfully. A heuristic analysis given by Wunderlich [25], following ideas by Schroeppel, indicates that the continued fraction algorithm will factor an integer N in $O(N^{L(N)})$ operations, where $L(N) \approx \sqrt{\frac{3\ln(\ln N)}{\ln N}}$. Most of the time in the continued fraction algorithm is spent in the trial division of the Q_n and many important improvements to the algorithm have been given to speed up this phase of the algorithm. (See [7] and chapters 4 and 5 of this paper.) Another important improvement to the continued fraction algorithm is the so called "early abort" strategy that has been developed by Pomerance [19]. It is based on the following idea. Most of the time is being spent in the factorization of the residues Q_n. (This is why methods using sieves such as the Quadratic Sieve algorithm and the Number Field Sieve are much faster than the Continued Fraction algorithm.) If a Q_n does not have any small prime factors, it is not likely to factor at all before the largest prime of the factor base has been reached. Thus, it may be advantageous to give up the trial division on Q_n after a number of primes have been tried and the unfactored portion is too large. Rather, we should abort the factoring procedure and generate a new residue Q_n.

Another important improvement to the algorithm is the use of the so called "large prime variation." It is based on the following idea. A large number of the residues Q_n will not factor completely on our factor base but will give congruences of the form $x^2 \equiv Ep \pmod N$ where E does factor completely and p is a large prime number not in the factor base. A single such relation is, of course, useless. But, if we have two Q's with the same large prime p, say $x_1^2 \equiv E_1 p \pmod N$ and $x_2^2 \equiv E_2 p \pmod N$, we will have $(\frac{x_1 x_2}{p})^2 \equiv E_1 E_2 \pmod N$, which is a useful relation. The question at this point, however, is how likely is it that getting the same p twice? It could be expected to get the same p twice is very rare! This, however, is not true, and is another instance of the well known "birthday paradox." What it says in our case is that if k numbers are picked at random among the integers less than some bound B, then, if $k > \sqrt{B}$, there will be a probability larger than $\frac{1}{2}$ that two of the numbers picked will be equal.

Finally, the Gaussian elimination step over $\mathbb{Z}_2$ is a non-trivial task since the matrices involved can be very huge. However, these matrices are very sparse. Recently, some special techniques have been developed for such matrices. An example, the "intelligent Gaussian elimination" method developed by LaMacchia and Odlyzko [15].

Chapter 4

The Quadratic Sieve Method

4.1 Introduction:

In this chapter, we present one of the "big guns" of factoring large integers, namely,the quadratic sieve algorithm. The quadratic sieve algorithm was developed in 1981 by Carl Pomerance [18]. The basic idea of the quadratic sieve method is the same as in the continued fraction method. We find integers x and y such that $x^2 \equiv y^2$ (mod N) where $x \not\equiv \pm y$ (mod N) by utilizing the Kraitchik factoring scheme. The difference between the continued fraction method and the quadratic sieve method is the way in which we find solutions to the square congruence $x^2 \equiv y^2$ (mod N). In the continued fraction method, we find small quadratic residues Q_k ($Q_k < 2\sqrt{N}$) from the convergents $\frac{A_k}{B_k}$ of the continued fraction expansion of $\sqrt{N}$ and multiply some of them to obtain a square integer, while, by means of the congruence relations $(-1)^{k+1} Q_{k+1} \equiv A_k^2 \pmod{N}$, find integers x and y such that x2 ≡ y2 (mod N).

In the continued fraction method, most of the computing time in factoring an integer is spent on trying to factor the quadratic residues Q_k by trail division of the primes in the factor base. What is particularly disadvantageous is that most of the Q_k do not factor completely within the factor base. For example, in factoring Fermat's 7th number $F_7 = 2^{2^7} + 1$, Morrison and Brillhart [16], after having computed 1,330,000 Q_k's from the continued fraction expansion of $\sqrt{257F_7}$, found only 2059 Q's completely factored within the factor base.

In the quadratic sieve method, the factoring of the quadratic residues is accomplished by a much faster sieving procedure that uses a faster operation than division, namely substraction. At the time the quadratic sieve algorithm was first published, it became the method of choice to factor large integers. In fact, it is considered to be faster than any previously published general purpose algorithm for factoring large integers. To support this idea, a running time analysis for the continued fraction algorithm and the quadratic sieve algorithm, under certain reasonable assumptions, has been done by Carl Pomerance [18]. He found that the running time estimate for the continued fraction algorithm is of order $O(\exp\sqrt{2\log N \log\log N})$, where N is the number to be factored and the running time estimate for factoring N by the quadratic sieve algorithm is of order $O(\exp\sqrt{1.125\log N \log\log N})$.

4.2 Outline of the Algorithm

As we mentioned in the introduction to this chapter, the quadratic sieve method employs the Kraitchik factoring scheme. Thus, there are four major steps to the quadratic sieve algorithm.

Step I: Generation of Congruences $u \equiv v \pmod{N}$.

This is accomplished by calculating a sequence of values of the polynomial $Q(x) = (x + [\sqrt{N}])^2 - N$ for small integers x, say $|x| < T$, where $T \approx [\sqrt[4]{N}]$. Note that Q(x) is a quadratic polynomial with integer coefficients. For integer values of x, we have $Q(x) = (x + [\sqrt{N}])^2 - N \equiv (x + [\sqrt{N}])^2 \pmod{N}$, where the congruence is not trivial, i.e., it is not equality. This congruence plays the role of the congruence $A_k^2 \equiv (-1)^{k+1} Q_{k+1} \pmod{N}$ in the continued fraction method.

Step II:

Determinetion of a complete factorization of some values of the Q(x) was computed in Step I over a prescribed - but restricted - set of small primes called the factor base. The primes in the factor base consist of precisely those primes for which N is a quadratic residue, i.e., 2 and the odd primes, p, for which the Legendre symbol $\left(\frac{N}{p}\right) = 1$ and $p \le B$ for some appropriate value of B.

Step III:

In this step, we need to find a subset of the quadratic residues $Q(x)$ that completely factors over the factor base we obtained in step 2 and which, when multiplied, gives a square integer. Suppose that we could find a set of distinct integers $x_1, x_2, \ldots, x_k$ such that $Q(x_1), \ldots, Q(x_k)$ completely factored over the factor base and their product is a square, say $Q(x_1)\, Q(x_2) \ldots Q(x_k) = y^2$.

Since $Q(x_i) \equiv (x_i + [\sqrt{N}])^2 \pmod{N}$ for each $i = 1, 2, \ldots, k$, the integers y and $X = (x_1 + [\sqrt{N}])(x_2 + [\sqrt{N}]) \ldots (x_k + [\sqrt{N}])$ satisfy the square congruence $X^2 \equiv Y^2 \pmod{N}$. If $X \not\equiv \pm Y \pmod{N}$ we proceed to Step IV. Otherwise, we find another subset of $Q(x)$ whose product is a square.

Step IV:

In this step, we compute $\gcd(X - Y, N)$ and $\gcd(X + Y, N)$ by the Euclidean algorithm. Since $X \not\equiv \pm Y \pmod{N}$, we have found proper factors of N, namely $\gcd(X-Y,N)$ and $\gcd(X+Y,N)$.

4.3 The Quadratic Sieve Algorithm:

We are now ready to present the quadratic sieve algorithm in more detail.

Step 1:

In this step, we generate small quadratic residues of N by computing the value of the quadratic polynomial with integer coefficients $Q(x) = (x + [\sqrt{N}])^2 - N$, for small values of x compared to N, say $|x| < T$. How large should we choose the parameter T? We must choose T large enough to generate many quadratic residues to be able to find a subset of which, when multiplied, produces a square. Heuristics suggest we choose $T \approx [\sqrt[4]{N}]$, but this is only a very rough guide. The choice of T depends of course on the size of the integer we need to factor and also on the computing machine we are using.

Note that with the choice of values of x such that $|x| < [\sqrt[4]{N}]$ we have $Q(x) = (x + [\sqrt{N}])^2 - N = x^2 + 2x\,[\sqrt{N}] + [\sqrt{N}]^2 - N \approx x^2 + 2x\,[\sqrt{N}] = 2x\sqrt{N} + O(\sqrt{N})$. That is, Q(x) grows essentially like a linear function of x for values of x in the range $-\sqrt[4]{N} < x < \sqrt[4]{N}$. The values of Q(x) start around $\sqrt{N}$ and go up to around $2N^{\frac{3}{4}}$. It should be noted that, while considerably smaller than N itself, these values can be quite large. For example, if $N \approx 10^{100}$, the values of Q(x) will be around 10^{50} to 10^{75}. Many important improvements to the algorithm have been given to overcome this problem.

<u>Example</u>:

To illustrate Step 1, above, and the other steps of the quadratic sieve algorithm, we take N = 5069. $[\sqrt{N}] = [\sqrt{5069}] = 71$ and $\sqrt[4]{5069} \approx 9$. Thus, $Q(x) = (x + 71)^2 - 5069$ with $|x| \le 9$. The values of Q(x) for values of x in the ranges $-9 \le x \le 9$ are given in table 4.1.

Step 2:

In this step, we need to find some $Q(x)$'s that factor completely over a set of small primes, called the factor base. The potential prime divisors of $Q(x)$ are exactly those primes for which N is a quadratic residue, i.e., p_1 = 2 and the odd primes p_i, for which the Legendre symbol $\left(\frac{N}{p_i}\right)$ = 1. This follows from the following theorem (4.1).

Table 4.1

x	-9	-8	-7	-6
Q(x)	-1225	-1100	-973	-844
x	-5	-4	-3	-2
Q(x)	-713	-580	-445	-308
x	-1	0	1	2
Q(x)	-169	-28	115	260
x	3	4	5	6
Q(x)	407	556	707	860
x	7	8	9	
Q(x)	1015	1172	133	

Theorem 4.1:

If p is an odd prime, then $Q(x) = (x + [\sqrt{N}])^2 - N \equiv 0 \pmod{p^\alpha}$ has a solution, in fact two, if and only if, $\left(\frac{N}{p}\right)=1$. If p = 2 and $\alpha \geq 3$, then $Q(x) \equiv 0 \pmod{2^\alpha}$ has a solution, in fact four, if and only if, $N \equiv 1 \pmod 8$. If p = 2 and $\alpha = 2$, then $Q(x) \equiv 0 \pmod 4$ has two solutions if $N \equiv 1 \pmod 4$ but no solution if $N \not\equiv 1 \pmod 4$. Finally, if p = 2 and $\alpha = 1$ then $Q(x) \equiv 0 \pmod 2$ has one solution, namely $x \equiv 1 \pmod 2$.

Proof:

Let $x + [\sqrt{N}] = z$. To say in this case that $Q(x) \equiv 0 \pmod{p^\alpha}$ has a solution is equivalent to saying that $z^2 \equiv N \pmod{p^\alpha}$ has a solution.

First, assume p is an odd prime. If $z^2 \equiv N \pmod{p^\alpha}$, has a solution, then so does $z^2 \equiv N \pmod p$. In fact, they have the same solution - whence $\left(\frac{N}{p}\right) = 1$.

Conversely, assume that $\left(\frac{N}{p}\right) = 1$. We show that $z^2 \equiv N \pmod{p^\alpha}$ has a solution by induction on α. If $\alpha = 1$, there is really nothing to prove because $\left(\frac{N}{p}\right) = 1$ is just another way of saying that $z^2 \equiv N \pmod p$ has a solution.

Assume that the result holds for $\alpha = k$ for some $k \geq 1$. Thus, $z^2 \equiv N \pmod{p^k}$ has a solution say, z_0. Then $z_0^2 \equiv N \pmod{p^k}$, or $z_0^2 = N + bp^k$ for some integer b. Now, we need to show that $z^2 \equiv N \pmod{p^{k+1}}$ has a solution. Consider the linear congruence equation $2z_0y \equiv -b \pmod{p}$. This linear congruence has a unique solution since $\gcd(2z_0, p) = 1$. Let y_0 be this unique solution.

Claim: $z_1 = z_0 + y_0p^k$ is a solution to the congruence $z^2 \equiv N \pmod{p^{k+1}}$. $(z_0 + y_0 p^k)^2 = z_0^2 + 2z_0y_0p^k + y^2p^{2k} = (N + b p^k) + 2z_0y_0p^k + y_0^2p^{2k} = N + (b + 2z_0y_0)p^k + y_0^2p^{2k}$. However, $p|(b + 2z_0y_0)$, from which it follows that $b + 2z_0y_0 = pd$ for some integer d. Thus, $z_1^2 = N + dp^{k+1} + (y_0^2 p^{k-1})p^{k+1} \equiv N \pmod{p^{k+1}}$, and the congruence $z^2 \equiv N \pmod{p^\alpha}$ for $\alpha = k + 1$, and, by induction, for all positive integers α.

Next, we shall assume that $p = 2$.

If $\alpha = 1$, then $z = 1$ is a solution of $z^2 \equiv N \pmod{2}$, since N is an odd integer.

If $\alpha = 2$ and $N \equiv 1 \pmod{4}$, then $N = 4k + 1$ and the congruence $z^2 \equiv N \pmod{4}$ has two solutions mod 4, namely $z = 1$ and $z = 3$. On the other hand, if $N \not\equiv 1 \pmod{4}$, then $z^2 \equiv N \pmod{4}$ has no solution because the square of any odd integer is congruent to 1 modulo 4.

Next, we consider the case in which $\alpha \geq 3$.

Since the square of any odd integer is congruent to 1 modulo 8, we see that for the congruence $z^2 \equiv N \pmod{2^\alpha}$ to have a solution it is necessary that N should be of the form 8k + 1. To go the other way, let us suppose that $N \equiv 1 \pmod 8$ and proceed by induction on α. When $\alpha = 3$, the congruence $z^2 \equiv N \pmod 8$ certainly has a solution. In fact, the integers 1, 3, 5, and 7 satisfy $z^2 \equiv 8k + 1 \pmod 8$. Assume that $z^2 \equiv N \pmod{2^\alpha}$ has a solution for $\alpha = n$ where $n \geq 3$, and say that z_0 is a solution. Thus, $z_0^2 = N + b\, 2^n$ for some integer b. Since N is odd, so are the integers z_0^2 and z_0. Thus, the linear congruence $z_0 y \equiv -b \pmod 2$, has a unique solution, say y_0.

Claim: $z_1 = z_0 + y_0\, 2^{n-1}$ satisfies the congruence $z^2 \equiv N$ (mod 2^{n+1}). $z_1^2 = (z_0 + y_0\, 2^{n-1})^2 = z_0^2 + z_0 y_0 2^n + y_0^2\, 2^{2n-2} = N + (b + z_0 y_0) 2^n + y_0^2\, 2^{2n-2}$. But, $2 | (b + z_0 y_0)$ implies $b + z_0 y_0 = 2d$ for some integer d. Hence $z_1^2 = N + d \bullet 2^{n+1} + y_0^2 \bullet 2^{n-3} \bullet 2^{n+1} \equiv N \pmod{2^{n+1}}$. Thus, $z^2 \equiv N \pmod{2^{n+1}}$ has a solution, and by induction, $z^2 \equiv N \pmod{2^\alpha}$ has a solution for all $\alpha \geq 3$. This completes the proof.

It follows from Theorem 4.1, that the odd prime p for which $\left(\frac{N}{p}\right) = -1$ has no chance at all to divide any value of $Q(x)$. Thus, we choose the factor base to be the integers $p_0 = -1$ that is needed to hold the sign of $Q(x)$, the even prime $p_1 = 2$ and the $B - 1$ smallest odd primes p_i for which $\left(\frac{N}{p_i}\right)=1$, i.e., $FB=\{-1,2\}\cup\{p_i \mid \left(\frac{N}{p_i}\right)=1, i=2,...,B-1\}$, where B is a parameter to be chosen so that the number of the quadratic residues $Q(x)$, that factor completely into factors in the factor base, is large enough to be able to find some subset of the $Q(x)$ among which the prime factors have all occurred an even number of times. Heuristics suggest thay we choose $B = [\sqrt{\exp\sqrt{(logN)\log logN}}]$. The primes in the factor base are roughly the random half of the first $2B$ primes, since primes p with $\left(\frac{N}{p}\right) = 1$ and those with $\left(\frac{N}{p}\right) = -1$ are roughly equally distributed.

The question now arises as to which values of $Q(x)$ will factor completely over the factor base? One of the advantages the quadratic sieve method has over the continued fraction method is that we do not need to (painfully) factor all the $Q(x)$'s we obtained in Step 1 over the factor base. In fact, most of them do not factor, so this would represent a waste of time. Here, since $Q(x)$ is a polynomial with integer coefficients, it so happens that if p is a prime in the factor base and $p^\alpha | Q(x_0)$ for some x_0, then $p^\alpha | Q(x_0 \pm h p^\alpha)$, $h = 0, 1, 2, ...$ Let us state a more general theorem.

Theorem 4.2:

Let $f(x)$ be a polynomial with integer coefficients and let m be a positive integer such that $f(x_0) \equiv 0 \pmod{m}$ for an integer x_0. Then, $f(x_0 + km) \equiv 0 \pmod{m}$ for any integer k.

Proof:

For any integer k we have $x_0 + km \equiv x_0 \pmod{m}$. Since $f(x)$ is a polynomial with integer coefficients, it follows from the properties of congruences that $f(x_0 + km) \equiv f(x_0) \pmod{m}$. But, $f(x_0) \equiv 0 \pmod{m}$ implies $f(x_0 + km) \equiv 0 \pmod{m}$.

Corollary:

If p is a prime in the factor base, such that $p^\alpha | Q(x_0)$ for some integer x_0, then $p^\alpha | Q(x_0 + hp^\alpha)$ for any integer h.

Proof:

$p^\alpha | Q(x_0)$ is equivalent to $Q(x_0) \equiv 0 \pmod{p^\alpha}$

Hence $Q(x_0 + hp^\alpha) \equiv 0 \pmod{p^\alpha}$ and thus $p^\alpha | Q(x_0 + hp^\alpha)$.

It follows from this corollary that if one single value of x can be located, for which $p^\alpha | Q(x)$ for a prime p in the factor base, then other instances of this event can be found by a sieving procedure on x, similar to the sieve of Eratosthenes for locating multiples of p^α in an interval. This sieving procedure on x will be discussed a little later. However, the justification for referring to this factoring method as the quadratic sieve method is now apparent.

The next question we need to answer is the following: How can one find an integer x (if it exists) such that $p^{\alpha} | Q(x)$ where p is a prime in the factor base? In light of Theorem 4.1, to find an integer x such that $p^{\alpha} | Q(x)$ we need only to solve the congruence $Q(x) \equiv 0 \pmod{p^{\alpha}}$.

There are two cases to consider in solving this congruence:

Case I: p is an odd prime:

If p is an odd prime and $p \nmid N$ and x_0 is a solution to the congruence $Q(x) \equiv 0 \pmod{p^{\alpha-1}}$, then a whole series of solutions can be found by putting $z = x_0 + y\, p^{\alpha-1}$, yielding $Q(z) = Q(x_0 + y\, p^{\alpha-1}) = (x_0 + y\, p^{d-1} + [\sqrt{N}])^2 - N = (X_0 + [\sqrt{N}])^2 + 2y\, p^{\alpha-1}\, (x_0 + [\sqrt{N}]) - N$. Dividing by $p^{\alpha-1}$ we get $\frac{(x_0 + [\sqrt{N}])^2 - N}{p^{\alpha-1}} + 2y(x_0 + [\sqrt{N}] \equiv 0 \pmod{p}$. This is a linear

congruence in y, whose solution is unique, say y_0 and $z = x_0 + y_0\, p^{\alpha-1}$ is a solution to the congruence $Q(x) \equiv 0 \pmod{p^{\alpha}}$. Thus, the problem of solving the congruence $Q(x) \equiv 0 \pmod{p^{\alpha}}$ is reduced to solving the congruence $Q(x) \equiv 0 \pmod{p}$, which in turn can be solved by different methods. The first method of solving the congruence $Q(x) \equiv 0 \pmod{p}$ is trial and error for values of x in the set $\{0, 1, 2, \ldots, p - 1\}$. The trial and error method of solving the congruence is appropriate here because the primes in the factor base are relatively small. Moreover, once we find one solution x_1, the second solution $x_2 \equiv -(x_1 + 2[\sqrt{N}])$ (mod p). A second method for solving the congruence $Q(x) \equiv 0$ (mod p), for primes of the form $p = 4k + 3$ or $p = 8k + 5$ is given in the following theorem.

<u>Theorem 4.3</u>:

For the congruence $Q(x) \equiv 0$ (mod p), where p is an odd prime in the factor base:

(1) If $p = 4k + 3$ then $x \equiv N^{\frac{(p+1)}{4}} \equiv N^{k+1}$ (mod p), is a solution to the congruence.

(2) If $p=8k+5$ and $N^{2k+1} \equiv 1$ (mod p), then $x \equiv N^{k+1}$ (mod p) is a solution.

(3) If $p=8k+5$ and $N^{2k+1} \equiv -1$ (mod p), then $x=(4N)^{k+1} \bullet \left(\frac{p+1}{2}\right)$ (mod p) is a solution.

<u>Proof</u>:

Since $\left(\frac{N}{p}\right) = 1$, by Euler's criterion $N^{\frac{(p-1)}{2}} \equiv 1$ (mod p).

(1) If $p = 4k + 3$, then $(N^{k+1})^2 = N^{2k+2} = N \bullet N^{2k+1} = N \bullet N^{\frac{(p-1)}{2}} \equiv N$ (mod p).

(2) If $p = 8k + 5$, then $N^{4k+2} \equiv 1$ (mod p, which implies that $N^{2k+1} \equiv 1$ or -1 (mod p). Thus if $N^{2k+1} \equiv 1$ (mod p), then

$(N^{k+1})^2 = N^{2k+1} \cdot N = N^{\frac{(p-1)}{2}} \cdot N \equiv N \pmod{p}$.

(3) If $N^{2k+1} \equiv -1 \pmod{p}$, then $\frac{(4N)^{2k+2}}{4} \equiv 2^{4k+2} \cdot N^{2k+2} \equiv -1 \cdot (-N) \equiv N$

(mod p).

This completes the proof.

A third method of solving the congruence $Q(x) \equiv 0$ (mod p) is based on the following algorithm that was suggested by D. H. Lehmer in 1969 [1].

Algorithm to solve the congruence $z^2 \equiv N \pmod{p}$:

Consider the congruence $z^2 \equiv N \pmod{p}$, where p is any odd prime in the factor base.

Choose an integer h so that the Legendre symbol $\left(\frac{h^2-4N}{p}\right) = -1$. Define a sequence of integers v_1, v_2, ... by the recursion

$$v_1 = h_1$$

$$v_2 = h^2 - 2N$$

$$\vdots$$

$$v_i = h \cdot v_{i-1} - N \cdot v_{i-2}.$$

We then have $v_{2i} = v_i^2 - 2N^i$, and $v_{2i+1} = v_i \cdot v_i + 1 - h \cdot N^i$.

Then, $z \equiv v_{\frac{(p+1)}{2}} \cdot (\frac{p+1}{2}) \pmod{p}$ is a solution, and $x \equiv z -$

$[\sqrt{N}]$ (mod p) is a solution to $Q(x) \equiv 0$ (mod p).

Example:

To illustrate the above algorithm, consider the congruence $z^2 \equiv 77$ (mod 13).

Let h = 24. Then, $\left(\frac{h^2-4N}{p}\right) = \left(\frac{268}{13}\right)$. By the law of quadratic reciprocity, we have

$$\left(\frac{268}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = (-1)^{21} = -1.$$

$v_1 = 24$

$v_2 = v_1^2 - 2N = 422$

$v_3 = v_1 \bullet v_2 - h \bullet N = 8280$

$v_4 = v_2^2 - 2N^2 = 166226$

$v_5 = v_2 \bullet v_3 - h \bullet N^2 = 3351864$

$v_6 = v_3^2 - 2N^3 = 67645334$

$v_7 = v_3 \bullet v_4 - h \bullet N^3 = 1365394488$

Then $z \equiv v_7 \bullet (\frac{p+1}{2}) \equiv 8$ (mod 13) is a solution.

Case II:

The second case is solving the congruence $Q(x) \equiv 0$ (mod 2^α), for powers of the prime p = 2.

Solutions of the congruence are given in Theorem 4.1 and its proof. The existence of solutions and the number of solutions depends on α and the residue class of N mod 8. The number N to be factored is odd, and hence it is congruent modulo 8 to 1, 3, 5, or 7. Let us consider these cases.

(1) If $N \equiv 3$ or $7 \pmod 8$, the $Q(x) \equiv 0 \pmod{2^\alpha}$ has a solution if $\alpha = 1$ but it has no solution for any $\alpha \geq 2$.

We have shown that $x \equiv 1 - [\sqrt{N}] \pmod 2$ is a solution. Now we are going to show if $\alpha \geq 2$, then $Q(x) \equiv 0 \pmod{2^\alpha}$ has no solution. We have $N = 8k + 3$ or $N = 8K + 7$ for some integer k. In order for the congruence, $Q(x) = (x + [\sqrt{N}])^2 - N \equiv 0 \pmod{2^\alpha}$ to have a solution, it is necessary that $x + [\sqrt{N}\}$ is odd, say $x + [\sqrt{N}] = 2m + 1$. Thus, $(2m+1)^2-(8k+3)=4m^2 +4m+1-8k-3=4m^2+4m-8k-2=2(2m^2+2m-4k-1)\not\equiv 0 \pmod{2^\alpha}$ if $\alpha \geq 2$. Similarly $(2m + 1)^2 - (8k + 7) = 4m^2 + 4m + 1 - 8k - 7 = 2(2m^2 + 2m - 8k - 3) \not\equiv 0 \pmod{2^\alpha}$ if $\alpha \geq 2$.

(2) If $N \equiv 5 \pmod 8$ then $Q(x) \equiv 0 \pmod{2^\alpha}$ has two solutions if $\alpha=2$ and $N \equiv 1 \pmod 4$, but has no solutions for any $\alpha\geq 3$.

In Theorem 4.1 we have shown that $x \equiv 1 - [\sqrt{N}] \pmod 4$ and $x \equiv 3 - [\sqrt{N}] \pmod 4$ have solutions if $N \equiv 1 \pmod 4$. Now, assume that $\alpha \geq 3$, and $N = 8k + 5$. In order for $(x +[\sqrt{N}])^2 - N \equiv 0 \pmod{2^\alpha}$ to have a solution it is necessary that $x + [\sqrt{N}]$ is odd, say $x + [\sqrt{N}] = 2m + 1$. Then

$(2m + 1)^2 - (8k + 5) = 4m^2 + 4m + 1 - 8k - 5$

$= 4(m^2 + m - 2k - 1) \not\equiv 0 \pmod{2^\alpha}$ if $\alpha \geq 3$.

(3) If $N \equiv 1 \pmod 8$, the congruence $Q(x) \equiv 0 \pmod{2^\alpha}$, has four solutions for any $\alpha \geq 3$.

Thus, if $N \equiv 1 \pmod 8$ then $Q(x) \equiv 0 \pmod{2^\alpha}$ has a solution for every positive integer α. This in turn increases the odds that $Q(x)$'s will factor completely. Therefore, we would clearly like to make the number N we want to factor congruent to 1 mod 8.

If the number N we need to factor is not congruent to 1 modulo 8, then upon multiplying N by a appropriate factor we get a number that is congruent to 1 modulo 8. If $N \equiv 3 \pmod 8$, we multiply both sides by 3 to obtain $3N \equiv 9 \equiv 1 \pmod 8$. If $N \equiv 5 \pmod 8$ we multiply both sides by 5 to obtain $5N \equiv 25 \equiv 1 \bmod 8$. Finally if $N \equiv 7 \pmod 8$ we multiply by 7 to obtain $7N \equiv 49 \equiv 1 \pmod 8$. Thus to factor an integer N that is not congruent 1 modulo 8, we first multiply N by an appropriate integer k so that $kN \equiv 1 \pmod 8$ and then apply the quadratic sieve algorithm to factor kN.

Example:

This example is a continuation of factoring $N = 5069$ by the quadratic sieve algorithm. In Step 1 we generated values of $Q(x)$ for $-9 \leq x \leq 9$. Now, we shall proceed to apply step 2.

We select a factor base $FB = \{-1, 2, p_2, \ldots p_B\}$ where $p_2, \ldots, p_B$ are the first $B - 1$ odd primes such that $\left(\frac{5069}{p_i}\right)$

$= 1$ and $B = [\sqrt{\exp\sqrt{\log 5069 \log\log 5069}}] = 4$. The first 4 odd such primes are 5, 7, 11, and 13.

Hence, the factor base is FB = {-1, 2, 5, 7, 11, 13}. Next we need to solve the congruences $Q(x) \equiv 0 \pmod{p_i}$ for each prime in the factor base.

For $p_1 = 2$:

Since $5069 \equiv 5 \pmod 8$ and $5069 \equiv 1 \pmod 4$, the congruence $Q(x) = (x + [\sqrt{5069}])^2 - 5069 \equiv 0 \pmod{2^\alpha}$ has two solutions if $\alpha = 2$. The solutions are:

$A_1 \equiv 1 - [\sqrt{5069}] \equiv 1 - 71 \equiv 0 \pmod 2$ and

$B_1 \equiv 3 - [\sqrt{5069}] \equiv 3 - 71 \equiv 0 \pmod 2$.

Thus, $2^2 | Q(0 + 2h)$ for any integer h and $2^\alpha \nmid Q(x)$ for any integer x.

For $p_2 = 5$, the congruence $Q(x) = (x + 71)^2 - 5069 \pmod 5$ has two solutions

$A_2 \equiv 1 \pmod 5$ and $B_2 = -(1 + 2[\sqrt{5069}]) \equiv -3 \equiv 2 \pmod 5$.

Thus, $5 | Q(1 + 5h)$ and $5 | Q(2 + 5h)$ for every integer h.

For $p_3 = 7$, the solutions are $A_3 \equiv 5 \pmod 7$ and $B_3 \equiv -(5 + 2 \bullet 71) \equiv 0 \pmod 7$. Thus, $7 | Q(5 + 7h)$ and $7 | Q(0 + 7h)$ for every integer h.

For $p_4 = 11$, the solutions are $A_4 \equiv 3 \pmod{11}$ and $B_3 \equiv -(3 + 2 \bullet 71) \equiv -2 \pmod{11}$. Thus, $11 | Q(3 + 11h)$ and $11 | Q(-2 + 11h)$ for every integer h.

For $p_5 = 13$, the solutions are $A_5 = 2 \pmod{13}$ and $B_5 \equiv -(2 +$

$2 \cdot 71) \equiv -1 \pmod{13}$. Thus, $13|Q(2 + 13h)$ and $13|Q(-1 + 13h)$ for every integer h.

The table below shows the values of Q(x) for $-9 \le x \le 9$, the prime factors we obtained above and the residual values of Q(x) after they are divided by primes.

Table 4.2

x	Q(x)	Prime Factors from FB	Residuals
-9	-1225	5 & 7	335
-8	-110	2^2 & 5 & 11	5
-7	-973	7	139
-6	-844	2^2	211
-5	-713	-	713
-4	-580	2^2 & 5	29
-3	-445	5	89
-2	-308	2^2 & 7 & 11	1
-1	-169	13	13
0	-28	2^2 & 7	1
1	115	5	23
2	260	2^2 & 5 & 13	1
3	407	11	37

4	556	2^2	139
5	707	7	101
6	860	2^2 & 5	43
7	1015	5 & 7	29
8	1172	2^2	293
9	1331	11	121

Note that we solved the congruence $Q(x) \equiv 0 \pmod{p_i^\alpha}$ where p_i is an odd prime in the factor base only for $\alpha = 1$. To find solutions (if they exist) for $\alpha > 1$, we either apply the technique outlined in case I above, or simply check whether p_i divides the new Q(x)'s value. If it does, we divide it out and repeat the process until p_i does not divide the Q(x).

In the table below, we have the complete factorizations of the Q(x)'s over the primes in the factor base.

Table 4.3

x	Q(x)	Prime Factors from FB	Residuals	Factorization of Q(x) over FB
-9	-1225	5 & 7	335	$-1 \cdot 5^2 \cdot 7^2$
-8	-1100	2^2 & 5 & 11	5	$-1 \cdot 2^2 \cdot 5^2 \cdot 11$

-7	-973	7	139	$7 \bullet 139$
-6	-844	2^2	211	$2^2 \bullet 211$
-5	-713	-	713	713
-4	-580	2^2 & 5	29	$23 \bullet 5 \bullet 29$
-3	-445	5	89	$5 \bullet 89$
-2	-308	2^2 & 7 & 11	1	$-1 \bullet 2^2 \bullet 7 \bullet 11$
-1	-169	13	13	$-1 \bullet 13^2$
0	-28	2^2 & 7	1	$-1 \bullet 2^2 \bullet 7$
1	115	5	23	$5 \bullet 23$
2	260	2^2 & 5 & 13	1	$2^2 \bullet 5 \bullet 13$
3	407	11	37	$11 \bullet 37$
4	556	2^2	139	$2^2 \bullet 139$
5	707	7	101	$7 \bullet 101$
6	860	2^2 & 5	43	$2^2 \bullet 5 \bullet 43$
7	1015	5 & 7	29	$5 \bullet 7 \bullet 29$
8	1172	2^2	293	$2^2 \bullet 293$
9	1331	11	121	11^3

Step 3:

We now come to the last and most important step in the quadratic sieve algorithm, namely, finding the $Q(x)$'s that factor completely over the factor base. This can be accomplished with a very simple sieve procedure. First, we describe the sieve procedure for the odd primes in the factor base. For each odd prime p_i in the factor base, let A_i and B_i be the solutions of the congruence $Q(x) \equiv 0 \pmod{p_i}$ that corresponds to this prime. For each x in the sieving interval $[-T, T]$, we compute very crudely $\log_2|Q(x)|$ and store these in an array indexed by x. Then, for each of our primes p_i, we subtract $\log_2 p_i$ from the number in location x in the array if and only if, $x \equiv A_i$ or $B_i \pmod{p_i}$.

Second, we describe the sieve procedure for the prime $p = 2$. You will recall that the solutions of the congruence $Q(x) \equiv 0 \pmod{2^\alpha}$, depend on the α and the residue class of N modulo 8. Thus, the indices for sieving with powers of 2 must be chosen in a somewhat different fashion depending on the residue class of N mod 8. Following a suggestion of Carl Pomerance, those sieving parameters are assigned as follows.

1. If $N \equiv 3$ or $7 \pmod 8$, the congruence has one solution $A_1 \equiv \pmod 2$. Thus, we subtract $\log_2 2 = 1$ from the number in location x in the array if and only if, $x \equiv A_1 \pmod 2$.
2. If $N \equiv 5 \pmod 8$ and $N \equiv 1 \pmod 4$, the congruence has two solutions A_1 and B_1. Thus, we subtract $\log_2 2^2 = 2$ from the number in location x in the array if and only

if, $x \equiv A_1 \pmod 4$ or $x \equiv B_1 \pmod 4$.

3. If $N \equiv 1 \pmod 8$, the congruence has four solutions A_1, A_2, B_1, and B_2. Thus, we subtract $\log_2 2^3 = 3$ from the number in location x in the array if and only if $x \equiv A_1, A_2, B_1$, or $B_2 \pmod 8$.

When all the values $\log_2 p_i$ have been subtracted for all the primes (or for higher prime powers) in the factor base, a Q(x) will factor completely on our factor base at those locations in the array that have a value close to zero. If the logs are exact, it would be exactly zero. To see this, assume that $Q(x_0)$ factors completely over the factor base. Then, $Q(x_0) = \prod_{i=1}^{B} p_i^{\alpha_i}$, $\alpha_i \geq 0$. Taking $\log_2$ of both sides to obtain

$$\log_2|Q(x_0)| = \log_2\left(\prod_{i=1}^{B} p_i^{\alpha_i}\right) = \sum_{i=1}^{B} \log_2 p_i^{\alpha_i} = \alpha_i \sum_{i=1}^{B} \log_2 p_i.$$

Thus

$$\log_2|Q(x_0)| - \alpha_i \sum_{i=1}^{B} \log_2 p_i = 0.$$

Those Q(x)'s which after the sieving is completed have their corresponding entries close to zero will be few enough that we can run trial division on them to see exactly which ones factor completely over the factor base.

<u>Example</u>:

Apply the sieving procedure to factor N = 5069.

The initial array of the values of $\log_2|Q(x)|$ is given in column two in the table below. The other columns in the table give the result of the sieving procedure.

Table 4.4

	R_0	R_1	R_2	R_3	R_4	R_5
x	$\log_2\|Q(x)\|$	p = 2	p = 5	p = 7	p = 11	p = 13
-9	10.2	10.2	5.6	0	0	0
-8	10.0	8.0	3.4	3.4	0	0
-7	9.9	9.9	9.9	7.1	7.1	7.1
-6	9.7	7.7	7.7	7.7	7.7	7.7
-5	9.4	9.4	9.4	9.4	9.4	9.4
-4	9.1	7.1	4.8	4.8	4.8	4.8
-3	8.7	8.7	6.4	6.4	6.4	6.4
-2	8.2	6.2	6.2	3.4	0	0
-1	7.4	7.4	7.4	7.4	7.4	7.4
0	4.8	2.8	2.8	0	0	0
1	6.8	6.8	4.5	4.5	4.5	4.5
2	7.9	5.9	3.6	3.6	3.6	-0.1
3	8.6	8.6	8.6	8.6	5.2	5.2

4	9.1	7.1	7.1	7.1	7.1	7.1
5	9.4	9.4	9.4	6.6	6.6	6.6
6	9.7	7.7	5.4	5.4	5.4	5.4
7	9.9	9.9	7.6	4.8	4.8	4.8
8	10.1	8.1	8.1	8	8	8
9	10.3	10.3	10.3	10.3	10.3	-0.8

From the last column in the table the locations in the array with values close to zero correspond to the following values of x: -9, -8, -2, -1, 0, 2, and 9. Thus the Q(x)'s that factor completely over the factor base are:

$Q_1(-9) = -1 \cdot 5^2 \cdot 7^2$

$Q_2(-8) = -1 \cdot 2^2 \cdot 5^2 \cdot 11$

$Q_3(-2) = -1 \cdot 2^2 \cdot 7 \cdot 11$

$Q_4(-1) = -1 \cdot 13^2$

$Q_5(0) = -1 \cdot 2^2 \cdot 7$

$Q_6(2) = 2^2 \cdot 5 \cdot 13$

$Q_7(9) = 11^3$

We now find a subset of the Q(x)'s which factored completely over the factor base whose product is a perfect square. For each address x_i at which $Q(x_i)$ factored completely over the factor base, we have $Q(x_i) = \prod_{j=0}^{B} p_j^{\alpha_{ij}}$ where $\alpha_{ij} \geq 0$. We associate with each $Q(x_i)$ a vector $\varepsilon_i \in Z_2^{B+1}$, given by

$\varepsilon_i = (\alpha_{ij})$, where $\alpha_{ij} = \begin{cases} 1 \text{ if } \alpha_{ij} \text{ is odd} \\ 0 \text{ if } \alpha_{ij} \text{ is even} \end{cases}$.

We now use the Gaussian elimination method on the matrix whose ith row is ε_i to find a subset E of the ε_i's such that their sum is the zero vector. Once such a subset E is found, the integers $X \equiv \prod_E (x + [\sqrt{N}])$ (mod N) and $y^2 \equiv \prod_E Q(x)$ (mod N), satisfy the square congruence $X^2 \equiv y^2$ (mod N). Let us apply the Gaussian elimination method to the previous example. The result of the Gaussian elimination method is given in the table below.

Table 4.5

n	-1	2	5	7	11	13
1	1	0	0	0	0	0
2	1	0	0	0	1	0
3	1	0	0	1	1	0
4	1	0	0	0	0	0
5	1	0	0	1	0	0
6	0	0	1	0	0	1
7	0	0	0	0	1	0
1	1	0	0	0	0	0
1+2	0	0	0	0	1	0

1+1+2+3	0	0	0	1	0	0
1+4	0	0	0	0	0	0
1+1+1+2+3+5	0	0	0	0	0	0
6	0	0	1	0	0	0
1+2+7	0	0	0	0	0	0

We have three solutions to the square congruence $X^2 \equiv y^2$ (mod 5069), namely $X_1 = (-9 + 71)\ (-1 + 71) \equiv 4340$ (mod 5069)

$y_1^2 = Q_1(-9) \bullet Q_4(-1) = 4265$ (mod 5069)

$X_2 = (-9 + 71)^3\ (-8 + 71)\ (-2 + 71)\ (0 + 71) \equiv 2070$ (mod 5069)

$y_2^2 = (Q_1(-9))^3\ (Q_2(-8))\ Q_3(-2)\ Q_5(0) \equiv 1595$ (mod 5069)

$X = (-9 + 71)\ (-8 + 71)\ (9 + 71) \equiv 3271$ (mod 5069)

$y_3^2 = Q_1(-9) \bullet Q_2(-8) \bullet Q_7(9) \equiv 3851$ (mod 5069)

<u>Step 4</u>:

For the integers X and y with $X^2 \equiv y^2$ (mod N) and $X \neq \pm y$ (mod N) we compute gcd(X - y), N) and gcd(X + y, N) by the Euclidian algorithm

In the example above the solutions to the square congruence $X^2 \equiv y^2$ (mod 5069) are $X_1 = 4340$, $Y_1 = 455$;

$X_2 = 2070$, $y_2 = 2481$

$X_3 = 3271$, $y_3 = 1798$ (trivial solution). Then

$\gcd(X_1 - y_1, N) = \gcd(3885, 5069) = 37,$

$\gcd(X_1 + y_1, N) = \gcd(4795, 5069) = 137,$

$\gcd(X_2 - y_2, N) = \gcd(411, 5069) = 137,$

$\gcd(X_2 + y_2, N) = \gcd(4551, 5069) = 37,$

The above calculations lead to the factorization of N = 5069 = 37 • 137.

Example:

Use the quadratic sieve algorithm to factor N = 247.

Step 1 Finding the Factor Base:

In this step, we start by placing a bound B on the factor base using the heuristic suggestion.

$$B = [\sqrt{\exp\sqrt{\ln 247 \ln\ln 247}}] = 4$$

This means that our factor base consists of {-1, 2, p_2, p_3, p_4}. Next, we evaluate the Legendre symbol to find the primes p_2, p_3, and p_4.

$\left(\frac{247}{3}\right) = +1$ since $247 \equiv 1 \pmod 3$

$\left(\frac{247}{5}\right) = -1$ since $(247)^2 \not\equiv 1 \pmod 5$

$\left(\frac{247}{7}\right) = +1$ since $(247)^3 \equiv 1 \pmod 7$

$\left(\frac{247}{11}\right) = +1$ since $(247)^5 \equiv 1 \pmod{11}$

Thus, the factor base = {-1, 2, 3, 7, 11}.

Step 2 Solving the congruence $Q(x) \equiv 0 \pmod p$ for each p in the factor base.

We start by finding Q(x)'s taking the values of x from the interval [-T, T] where $T = [\sqrt[4]{N}]$. Thus, $T = [\sqrt[4]{247}] = 3$. Therefore, the sieving interval is [-3, 3]. The table below shows the results.

Table 4.6

x	1	2	3	x	0	-1	-2	-3
$x+[\sqrt{N}]$	16	17	18	$x+[\sqrt{N}]$	15	14	13	12
Q(x)	9	42	77	Q(x)	-22	-51	-78	-103

The solutions for the congruence $Q(x) \equiv 0 \pmod p$, where $p \in FB$, are the following:

a) $A_1 = 0$, since $247 \equiv 7 \pmod 8$. Thus, $2|Q(0 \pm 2h)$ and 2 divides Q(0), Q(2) and Q(-2).

b) $A_2 = 1$, $B_2 = -(1 + 2 \cdot 15) = -31 \equiv -1 \pmod 3$. Thus, $3|Q(1 \pm 3h)$ and $3|Q(-1 \pm 3h)$. Therefore, 3 divides Q(1), Q(-2), Q(-1) and Q(2).

c) $A_3 = 2$, $B_3 = -(2 + 2 \cdot 15) = -32 \equiv -4 \pmod 7$. Thus, $7|Q(2 \pm 7h)$ and $7|(Q(-4 \pm 7h)$. Therefore, 7 divides Q(2), and Q(3).

6d) $A_4 = 0$, $B_4 = (0 + 2 \cdot 15) = -30 \equiv -8 \pmod{11} \equiv 3 \pmod{11}$. Thus, $11|Q(0 \pm 11h)$ and $11|Q(3 \pm 11h)$. Therefore, 11 divides Q(0), and Q(3). The table below shows these results.

Table 4.7

x	$x + [\sqrt{N}]$	$Q(x)$	Factors from base	Residual
1	16	9	3•3	
2	17	42	2•3•7	
3	18	77	7•11	
0	15	-22	-1•2•11	
-1	14	-51	-1•3	17
-2	13	-78	-1•2•3	13
-3	12	-103	-1	103

<u>Step 3</u> Sieving process:

We start sieving over the interval $[-3, 3]$. We compute $\log_2 Q(x)$ and store these numbers at locations indexed by x. Then successively, we subtract from these numbers $\log_2 p$ if $p|Q(x)$. At the end of this process, we consider $Q(x)$ if the residual number at its location is close to or equal to zero. The table below shows the results.

Table 4.8

	$\log_2 Q(x)$	$\log_2 2^\alpha$	$\log_2 3^\alpha$	$\log_2 7^\alpha$	$\log_2 11^\alpha$	$\log_2 Q(x) - \log_2 P_i^\alpha$
Q(1)	3.1680		2(1.5840)			0
Q(2)	5.3891	0.9994	1.5840	2.8057		0
Q(3)	6.2631			2.8057	3.4574	0
Q(0)	4.4568	0.9994			3.4574	0
Q(-1)	5.6691		1.5840			4.0851
Q(-2)	6.2817	0.9994	1.5840			3.6983
Q(-3)	6.6826					6.6826

<u>Step 4</u> Solving for dependencies:

We associate the vectors ϵ_1, ϵ_2, ϵ_3 and ϵ_4 for Q(1), Q(2), Q(3) and Q(0) respectively.

$\epsilon_1 = (0, 0, 0, 0, 0)$.

$\epsilon_2 = (0, 1, 1, 1, 0)$.

$\epsilon_3 = (0, 0, 0, 1, 1)$.

$\epsilon_4 = (1, 1, 0, 0, 1)$.

Next, we form the binary matrix corresponding to these vectors,

	-1	2	3	7	11
ϵ_1	0	0	0	0	0
ϵ_2	0	1	1	1	0
ϵ_3	0	0	0	1	1
ϵ_4	1	1	0	0	1

We apply the Gaussian elimination method on the above matrix to find linear dependencies. The reduced matrix will be as follows:

	-1	2	3	7	11
ϵ_1	0	0	0	0	0
ϵ_2	0	1	1	1	0
ϵ_3	0	0	0	1	1
ϵ_4	1	1	0	0	1

Therefore $\{\epsilon_1\}$ is the only set of dependency and hence forms a square set.

Let $Q(1) = y^2 \Rightarrow y^2 = 3^2$

Let $x = 16$.

Then, we form the congruence $x^2 \equiv y^2 \pmod{N}$

$16^2 \equiv 3^2 \pmod{247}$. Since $16 \not\equiv \pm 3 \pmod{47}$, this congruence has nontrivial solutions.

Step 5:

We calculate gcd$(x - y, N)$ or gcd$(x + y, N)$ by Euclidean algorithm. Therefore,

gcd$(16 - 3, 247) = 13$ and

gcd$(16 + 3, 247) = 19$

and these are the factors of 247.

4.4 The Multiple Polynomial Quadratic Sieve:

The quadratic sieve just explained in section 4.3 is called the basic quadratic sieve algorithm. Many modifications have been suggested to improve its performance. Among these are the large prime variations (see section 3.3). But, by far the most important improvement was given by Peter Montgomery. In this section, we give a brief discussion of Montgomery's work.

One drawback of the basic quadratic algorithm just described is that as $|x|$ moves away from 0, the values of the polynomial $Q(x)$ grow and become less likely to factor completely over the factor base. This problem can be overcome by using other polynomials and sieving each one over a shorter interval. This variation of the quadratic sieve is called the multiple polynomial quadratic sieve.

Now, we will describe a family of polynomials that can be used in place of $Q(x)$. Consider the polynomial

$f(x) = a\,x^2 + 2bx + c$, when a, b, and c are integers with $a > 0$, such that $N|(b^2 - ac)$. This gives congruences just as nicely as before, since $af(x) = (ax + b)^2 - (b^2 - ac). \equiv (ax + b)^2 \pmod{N}$, so that af(x) is a quadratic residue modulo N. The requirement that $|f(x)|$ be small for values of x in the sieving interval [-T, T] led Montgomery to choose $a \approx \frac{\sqrt{2N}}{T}$, where a is a prime with $\left(\frac{N}{a}\right) = 1$. After an integer a is chosen, we choose an integer b satisfying $b^2 \equiv N \pmod{a}$, $0 \le b < a$. Finally, c is chosen so that $c = \frac{b^2 - N}{a}$. Since there are many primes a near $\frac{\sqrt{2N}}{T}$ with $\left(\frac{N}{a}\right) = 1$, we can construct many good polynomials.

As in the basic quadratic sieve algorithm, we compute for each prime power p^α in the factor base the solutions of the congruences $f(x) \equiv 0 \pmod{p^\alpha}$, with which we will initialize an array and apply the sieving procedure.

The multiple polynomial quadratic sieve described above has a number of nice features. For example, the upper bound on the value of f(x) is less than the bound on Q(x), so that we have a better chance of factoring our numbers. We can use a much shorter sieving interval. If we do not get enough completely factored f(x)'s then we generate a new polynomial and sieve again over our shortened interval. Keeping the interval short increases the chances that a given f(x) will factor. One of the nicest features is that the sieving parallelizes perfectly. With K processors, one can assign a different polynomial to each processor and the algorithm runs K times as fast.

Chapter 5

The Number Field Sieve

In this chapter, we present the most recent and potentially the most powerful known factoring method, the number field sieve. Section 5.1 gives the necessary background on number fields needed for the development of the number field sieve algorithm. Sections 5.2 and 5.3 describe the algorithm. In section 5.4 a special case of the algorithm employed in factoring numbers of the form $N = r^e - s$, where r and $|s|$ are small positive integers, $r > 1$, and e is large, is presented.

5.1 Algebraic Number Fields:

Let **Q** be the field of rational numbers. The set of polynomials in one indeterminate and rational coefficients with the usual addition and multiplication of polynomials forms a commutative ring with identity denoted by **Q**[x]. If $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Q}[x]$ and $a_n \neq 0$, then n is called the degree of $f(x)$.

Definition:

A polynomial $f(x) \in \mathbf{Q}[x]$ is called irreducible over **Q** if no polynomials $g(x)$ and $h(x)$, both with positive degree, exist in **Q**[x] satisfying $f(x) = g(x)\,h(x)$.

Definition:

A polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Q}[x]$ is called monic if the leading coefficient $a_n = 1$.

Definition:

Let $\alpha \in \mathbf{C}$. Then, α is called an algebraic number if there exists $f(x) \in \mathbf{Q}[x]$, such that $f(\alpha) = 0$. If $f(x) \in \mathbf{Z}[x]$ and $f(\alpha) = 0$, then α is called an algebraic integer.

We state without proof some facts about the set of algebraic numbers. The proofs can be found in [22].

Theorem 5.1:

(i) The set of algebraic numbers with the operations of complex addition and multiplication is a field denoted by $\overline{Q}$.

(ii) The set of algebraic integers with the same operations in (i) is an integral domain.

Theorem 5.2:

If $\alpha \in \mathbf{C}$ is an algebraic number, then there exists a unique monic irreducible polynomial over $\mathbf{Q}$, $f(x) \in \mathbf{Q}[x]$ with the property $f(\alpha) = 0$. We call this polynomial the minimal polynomial for α and its degree is called the degree of the algebraic number α.

Theorem 5.3:

Let α be an algebraic number of degree n. Let $Q(\alpha)$ denote the subset of the set of algebraic integers consisting of the elements of the form

$$Q(\alpha) = \{a_0 + a_1\alpha + \ldots a_{n-1}\alpha^{n-1} | a_i \in \mathbf{Q}\}.$$

Then, $Q(\alpha)$ is a field under the operations of complex addition and multiplication. The field $\mathbf{Q}(\alpha)$ is called an algebraic number field of degree n over $\mathbf{Q}$.

Definition:

Let α be an algebraic number and let $f(x) \in \mathbf{Q}[x]$ be its minimal polynomial. A conjugate of α is any root of the equation $f(x) = 0$.

Let $\alpha_{(1)} = \alpha$, $\alpha_{(2)}$, ..., $\alpha_{(n)}$, be the conjugates of an nth degree algebraic number α. Let $\beta = a_0 + a_1\alpha + a_2\alpha^2 + \ldots a_{n-1}\alpha^{n-1} \in Q(\alpha)$, then the numbers $\beta_i = a_0 + a_1\alpha_{(i)} + \ldots + a_{n-1}\alpha_{(i)}^{n-1}$, $i = 1, \ldots, n$ are called the conjugates of β.

<u>Definition</u>:

Let $\beta \in Q(\alpha)$ and let $\beta_1, \ldots, \beta_n$ be its conjugates. The norm of β is given by $N(\beta) = \beta_1 . \beta_2 \ldots \beta_n$.

<u>Theorem 5.4</u>:

(1) If $\beta, \beta' \in Q(\alpha)$, then $N(\beta\beta') = N(\beta)\, N(\beta')$

(2) $N(\beta) \neq 0$ for every $\beta \neq 0$.

The following example illustrates the forgoing concepts.

<u>Example</u>: Let $\alpha = \sqrt[3]{2}$ denote the real cube root of 2. The minimal polynomial of α is $f(x) = x^3 - 2$.

Then, $\mathbf{Q}(\sqrt[3]{2}) = \{a_0 + a_1(\sqrt[3]{2}) + a_2(\sqrt[3]{2})^2 \mid a_i \in \mathbf{Q}\}$.

The three conjugates of $\alpha = \sqrt[3]{2}$ are $\alpha_{(1)} = \sqrt[3]{2}$, $\alpha_{(2)} = \dfrac{-1-\sqrt{3}\,i}{2^{\frac{2}{3}}}$, $\alpha_{(3)} = \dfrac{-1+\sqrt{3}\,i}{2^{\frac{2}{3}}}$. Let $\beta = 3 + 2\sqrt[3]{2} \in Q(\alpha)$, in which case the conjugates of β are $\beta_1 = 3 + 2\alpha_{(1)} = 3 + 2\sqrt[3]{2}$,

$\beta_2 = 3 + 2\alpha_{(2)} = 3 + 2\left(\dfrac{-1-\sqrt{3}i}{2^{\frac{2}{3}}}\right)$, and $\beta_3 = 3 + 2\alpha_{(3)} = 3 +$

$2\left(\dfrac{-1+\sqrt{3}i}{2^{\frac{2}{3}}}\right)$. Also

$$N(\beta) = \left(3+2\sqrt[3]{2}\right)\left(3+2^{\frac{1}{3}}\left(\frac{-1-\sqrt{3}}{2^{\frac{2}{3}}}i\right)\right)\left(3+2^{\frac{1}{3}}\left(\frac{-1+\sqrt{3}}{2^{\frac{2}{3}}}i\right)\right)$$

$$= (3 + 2\sqrt[3]{2})\ (3 + 2^{\frac{1}{3}}(-1 - \sqrt{3}i))\ (3 + 2^{\frac{1}{3}}(-1 + \sqrt{3}\ i))$$

$$= 9 + 2^{\frac{2}{3}}.$$

If α is an algebraic integer, we define $\mathbf{Z}[\alpha]$ to be the set of all complex numbers of the form $f(\alpha)$, where $f(x) \in \mathbf{Z}[x]$. That is, $\mathbf{Z}[\alpha] = \{f(\alpha) | f(x) \in \mathbf{Z}[x]\}$. $\mathbf{Z}[\alpha]$ is an integral domain under the operations of complex addition and multiplication. If the degree of α is n, then $\mathbf{Z}[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} | a_i \in \mathbf{Z}\}$.

For example, $\alpha = \sqrt{5}i$ has degree 2 because $f(x) = x^2 + 5$ is its minimal polynomial. Thus, $\mathbf{Z}[\sqrt{5}i] = \{a_0 + a_1\sqrt{5}i | a_0, a_1 \in \mathbf{Z}\}$. The conjugate of $\alpha = \sqrt{5}i$ is $\overline{\alpha} = -\sqrt{5}i$. The conjugates of $\beta = b_0 + b_1\sqrt{5}i$ are β and $\overline{\beta} = b_0 - b_1\sqrt{5}i$, and $N(\beta) = \beta\overline{\beta} =$

$= \beta\bar{\beta} = b_0^2 + 5b_1^2$.

In general, for any $\beta \in \mathbf{Z}[\alpha]$, $N(\beta)$ is an integer.

The following theorem is important for the design of the number field sieve algorithm.

Theorem 5.5:

Let α be an algebraic integer, $f(x) \in \mathbf{Z}[x]$ be its minimal polynomial and $n > 0$ and m be integers such that $f(m) \equiv 0 \pmod{n}$. Then, there is a natural ring homomorphism $\Phi:\mathbf{Z}[\alpha] \to \mathbf{Z}_n$ induced by $\Phi(\alpha) = m \bmod n$.

<u>Proof</u>:

A typical element in $\mathbf{Z}[\alpha]$ has the form $g(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$, where $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}$. Define $\Phi:\mathbf{Z}[\alpha] \to \mathbf{Z}_n$ by $\Phi(g(\alpha) = \Phi(\sum_{i=0}^{n-1} a_i\alpha^i) = \sum_{i=0}^{n-1} a_i m^i \bmod n = g(m) \bmod n$.

First, we are going to show Φ is well defined. That is, if $g(\alpha) = h(\alpha)$ in $\mathbf{Z}[\alpha]$, then $\Phi(g(\alpha)) = \Phi(h(\alpha))$, and we need to show $g(m) \equiv h(m) \bmod n$. Since $g(\alpha) = h(\alpha)$, we have $g(\alpha) - h(\alpha) = 0$ thus $f(x) \mid (g(x) - h(x))$. Thus, $g(x) - h(x) = f(x)r(x)$ for some $r(x) \in \mathbf{Z}[x]$. $g(m) - h(m) = f(m)\ r(m) \equiv 0 \pmod{n}$. Hence $g(m) \equiv h(m) \pmod{n}$. Thus, Φ is well-defined.

Let $g(\alpha), h(\alpha) \in \mathbf{Z}[\alpha]$. Then $g(\alpha) = \sum_{i=0}^{n-1} a_i\alpha^i$, and $h(\alpha) = \sum_{i=0}^{n-1} b_i \alpha^i$ where a_i, $b_i \in \mathbb{Z}$, for $i = 0, \ldots, n - 1$.

Then $\Phi(g(\alpha) + h(\alpha)) = \Phi(\sum_{i=0}^{n-1} (a_i + b_i)\ \alpha^i)$

$$= \Sigma\ (a_i + b_i)\ m^i \bmod n$$

$$= (g + h)(m) \bmod n.$$

$$= g(m) + h(m) \bmod n$$

$$= (g(m)) \bmod n + (h(m)) \bmod n$$

$$= \Phi(g(\alpha)) + \Phi(h(\alpha)).$$

$$\Phi(g(\alpha)h(\alpha)) = \Phi((\sum_{i=0}^{n-1} a_i \alpha^i)(\sum_{i=o}^{n-1} b_i \alpha^i))$$

$$= \Phi(\sum_{i=0}^{2(n-1)} \sum_{k=0}^{i} a_k b_{i-k} \alpha^i) = \sum_{i=0}^{2(n-1)} \sum_{k=0}^{i} a_k b_{i-k} m^i \bmod n$$

$$= (g \bullet h)(m) \bmod n = g(m) \bullet h(m) \bmod n$$

$$= \Phi(g(\alpha))\ \Phi(h(\alpha)).$$

Therefore Φ is a ring homomorphism.

5.2 Outline of the Number Field Sieve Algorithm:

The main idea of the number field sieve algorithm is the same as in the continued fraction method and the quadratic sieve method. We find integers x and y such that $x^2 \equiv y^2 \pmod N$ where $x \neq \pm y \pmod N$ by utilizing the Kraitchik factoring scheme. In the number field sieve, we achieve this as follows:

We choose a number field $K = Q(\alpha)$ for some algebraic integer α, and let $f(x) \in \mathbf{Z}[x]$ be the minimal polynomial of α. Assume that we know an integer m, such that $f(m) \equiv 0 \pmod{N}$. By Theorem 5.5, there exists a natural ring homomorphism $\Phi:\mathbf{Z}[\alpha] \to \mathbf{Z}_N$, where $\Phi(\alpha) = m \bmod N$. Let $S = \{g(x) | g(x) \in \mathbf{Z}[x]\}$ be a finite set of polynomials in $\mathbf{Z}[x]$ such that:

(i) $\prod_{g\in S} g(m)$ is a square in $\mathbf{Z}$, say $\prod_{g\in S} g(m) = X^2$.

(ii) $\prod_{g\in S}$ $(g(\alpha)$ is a square in $\mathbf{Z}[\alpha]$, say $\prod_{g\in S} g(\alpha) = \beta^2$ in $\mathbf{Z}[\alpha]$.

Let Y be some integer with $\Phi(\beta) = Y \bmod N$. The $Y^2 \equiv (\Phi(\beta))^2$ $\equiv \Phi(\beta^2) \equiv \Phi(\prod_{g\in S} g(\alpha))$

$$\equiv \prod_{g\in S} \Phi(g(\alpha)) \equiv \prod_{g\in S} g(m) \equiv X^2 \pmod{N}.$$

That is, we have found a pair of squares that are congruent mod N, and so we may attempt to factor N by computing gcd(X - Y, N) or gcd(X + Y, N).

The above scenario raises the questions:

(1) How are the polynomial f(x) and the integer m are constructed?

(2) How can the set S of elements $g(\alpha) \in \mathbf{Z}[\alpha]$ can be found that satisfies conditions (i) and (ii) above?

5.3 The Number Field Sieve Algorithm:

The overall plan of this section is to answer these questions gradually until, finally, we can state a precise version of the number field sieve algorithm.

Step 1: Finding A Polynomial:

Given a positive integer N that is not a prime power, the first step of the number field sieve algorithm is to find a polynomial $f(x) \in \mathbf{Z}[x]$ and an integer m such that $f(m) \equiv 0 \pmod{N}$. Assume that the polynomial f(x) has degree $N > 2^{d^2}$ (in practice $d \approx \sqrt[3]{\left(\frac{3\log N}{\log\log N}\right)}$). We set $m = [N^{\frac{1}{d}}]$. We write N in the base m, and proceed to find integers $c_0, c_1, \ldots, c_d$, where $0 \le c_i \le m - 1$ with $N = c_d m^d + c_{d-1}m^{d-1} + \ldots + c_0$. Let $f(x) = c_d x^d + c_{d-1}x^{d-1} + \ldots + c_0$. Note that $f(m) = N$.

Theorem 5.6:

The leading coefficient c_d of f(x) is equal to 1 and $c_{d-1} \le d$.

Proof:

Since $m = [N^{\frac{1}{d}}]$, $N^{\frac{1}{d}}-1<m\le N^{\frac{1}{d}}$ or $N^{\frac{1}{d}}<m+1\le N^{\frac{1}{d}}+1$. Therefore, $N < (m + 1)^d$. Consider $(m+1)^d=m^d+\binom{d}{1}m^{d-1}+\binom{d}{2}m^{d-2}+\ldots+ 1$.

$2^d = (1 + 1)^d = 1 + \binom{d}{1} + \binom{d}{2} + \ldots + \binom{d}{d-1} + 1$. Thus,

$2^d - 2 = \binom{d}{1} + \binom{d}{2} + \ldots + \binom{d}{d-1} \geq \binom{d}{k}$ for every k = 1, 2, ..., d - 1. However, $N>2^{d^2}$ implies $N^{\frac{1}{d}}>2^d$. Hence, $N^{\frac{1}{d}}-2>2^d-2\geq\binom{d}{k}$ and $\binom{d}{k} \leq N^{\frac{1}{d}} - 2 \leq m - 1$.

Therefore the digits of $(m + 1)^d$ in base m are the binomial coefficients $\binom{d}{k}$. However, $m^d \leq N < (m + 1)^d$ or $m^d \leq c_d m^d + c_{d-1}m^{d-1} + \ldots + c_0 < m^d + \binom{d}{1} m_1^{d-1} \ldots + 1$. $c_d = 1$ and $c_{d-1} \leq \binom{d}{1} = d$. Thus $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0 \in \mathbb{Z}[x]$ is a monic polynomial and f(m) = N.

Is f(x) irreducible? Most likely, it is irreducible over $\mathbb{Z}$. However, if f(x) is not irreducible then we have been lucky. Indeed, if f(x) = g(x) h(x) is a non-trivial factorization of f(x) in $\mathbb{Z}[x]$, then N = f(m) = g(m) h(m) and hence g(m) and h(m) are non-trivial factors of N. On the other hand, if f(x) is irreducible in $\mathbb{Z}[x]$, we proceed to obtain a finite set $s = \{g(x) \in \mathbb{Z}[x]\}$ of polynomials such that $\prod_{g\in S} g(m) = X^2$ in $\mathbb{Z}$ and $\prod_{g\in S} g(\alpha) = \beta^2$ in $\mathbb{Z}[\alpha]$.

Step 2: Finding a set S

From Step 1, we have a polynomial $f(x) \in \mathbb{Z}[x]$ that is irreducible and monic and has degree d. We have also an integer m with the property $f(m) \equiv 0 \pmod{N}$. Let $\alpha \in \mathbf{C}$ be a zero of the polynomial f(x). Taking for our polynomials $g(x) \in \mathbf{Z}[x]$, the linear polynomials $g(x) = a + bx$ where a, b are small coprime integers with $0 < b \leq B$ and $0 \leq |a| \leq B$. In practice, $B \approx \exp\left(\sqrt[3]{\frac{8}{9}\log N(\log\log N)^2}\right)$. Since $m \approx N^{\frac{1}{d}}$, the integers a + bm are small compared to N.

The construction of the set S proceeds in two steps. First, we use a sieve to find a set T of pairs (a, b), such that $g(m) = a + bm$ is z-smooth (i.e. a + bm factors into primes $\leq$ z) and $g(\alpha) = a + b\alpha$ is smooth in $\mathbf{Z}[\alpha]$. Next, we use linear algebra over the field $\mathbf{Z}_2$ to find a set $S \subseteq T$.

Let $U = \{(a, b) | a, b \in \mathbf{Z}, \gcd(a, b) = 1, 0 \leq |a| \leq B, 0 < b \leq B\}$. First, we are going to use a sieving method to find pairs (a, b), such that $g(m) = a + bm$ are z-smooth where z is an integer depending on N.

For each fixed integer b with $0 < b \leq B$, an array is initialized with the integers a + bm for $-B \leq a \leq B$. For each prime $p \leq z$, the numbers in the array corresponding to values of a with $a \equiv -bm \pmod{p}$ are picked up one at a time, then each is divided by the highest power of p that divides them and the quotient is replaced in the same array at the same location from which the number is picked. At the end of this procedure the number in the a^{th} location is, up to sign, the largest divisor of a + bm that is coprime to the primes up to z. Any location that contains the number 1 or -1 at the end of the procedure corresponds to a number a + bm that is z-smooth. We denote the subset of pairs (a, b) $\in$ U such that a + bm is z-smooth by T_1, i.e., $T_1 = \{(a, b) \in U | a + bm \text{ is z-smooth}\}$. The factor base is the set of primes less than or equal to z, i.e., $FB = \{p | p \text{ is a prime and } p \leq z\} \cup \{-1\}$. In practice, $z \approx B \approx \exp\left(\sqrt[3]{\frac{8}{9}\log N(\log\log N)^2}\right)$.

Now, assume that the number of elements in T_1 is more than the number of elements in the factor base FB. Let $\pi(z) = h$ be the number of primes up to z. Then, the number of elements in FB is less than or equal to h + 1. For each z-smooth integer, write $g(m) = a + bm = \prod_{j=0}^{h} P_j^{e_j}$, where p_j denotes the j^{th} prime, for $1 \leq j \leq h$ and $P_0 = -1$. We assign a vector $v(a + bm) = (e_0 \bmod 2, e_1 \bmod 2, \ldots, e_n \bmod 2) \in Z_2^{h+1}$. Since the number of vectors for each $(a, b) \in T_1$ exceeds the dimension of the vector space Z_2^{h+1}, there is a non-empty subset $S \subseteq T_1$ such that $\sum_{(a,b) \in S} v(a + bm) = 0 \in Z_2^{h+1}$. Therefore $\prod_{(a,b) \in S} (a + bm) = X^2$ is a square in $\mathbf{Z}$.

Our next objective is to use a sieving method similar to the one we discussed above to find a set S of pairs (a, b) ϵ U such that $\prod_{(a,b)\in S}$ (a + bα) is a square in $\mathbf{Z}[\alpha]$.

<u>Definition</u>:

An element $\beta \in \mathbf{Z}[\alpha]$ is called z-smooth if its norm $N(\beta) \in \mathbf{Z}$ is z-smooth.

We can calculate the norm of an element of the form a + bα ϵ $\mathbf{Z}[\alpha]$ by substituting a, b for X and Y in the homogenous polynomial $(-Y)^d\ f(-\frac{X}{Y})$, where $f(x)=x^d+c_{d-1}x^{d-1}+\ldots+ c_0$. Thus,

$N(a + b\alpha) = a^d - c_{d-1}a^{d-1}b+ \ldots + (-1)^d c_0 b^d$. For each prime, let $R(p) = \{r|0 \le r \le p - 1,\ f(r) \equiv 0 \pmod P\}$. For any fixed integer b, with $0 < b \le B$ and $b \not\equiv 0 \pmod P$, the integers a with $N(a + b\alpha) \equiv 0 \pmod P$ are those with $a \equiv -br \pmod P$ for some $r \in R(p)$.

Note that if $b\equiv 0 \pmod P$, then there are no integers a with $(a,b) \in U$ and $N(a + bd) \equiv 0 \pmod P$.

Now a modification of the earlier sieving method can be used to find the set $T_2 = \{(a, b) \in U | a + b\alpha \text{ is z-smooth}\}$, as follows:

For each fixed b, initialize an array with the numbers $N(a \pm b\alpha)$ for $-B \le a \le B$. For each prime $p \le z$ that does not divide b, and each choice of $r \in R(p)$, the positions corresponding to a that are congruent to $-br \pmod p$ are identified. The numbers in these positions are picked up and divided by the highest power of p that divides them and then the quotient is replaced in the array as before. At the end of this process, the locations containing ± 1 correspond to z-smooth values of $a + b\alpha$ with $\gcd(a, b) = 1$ and hence to elements of T_2.

The next step is to apply linear algebra over the field $\mathbb{Z}_2$ to obtain a subset S of T_2 such that $\prod_{(a,b) \in S} (a + b\alpha)$ is a square in $\mathbb{Z}[\alpha]$. To achieve this goal, we assign to every $(a, b) \in T_2$ a vector $v(a + b\alpha) = (v_{p,r}(a + b\alpha))$ such that $v_{p,r}(a + b\alpha)$ is defined for every prime $P \leq z$ and every element $r \in R(P)$ by

$$v_{p,q}(a + b\alpha) = \begin{cases} ord_P(N(a+b\alpha)) & \text{if } a+br=0 \pmod{P} \\ 0 & otherwise, \end{cases},$$

where $ord_p(k)$ is the number of prime factors p in k. Clearly, we have $N(a + b\alpha) = \pm \prod_{P,r} P^{v_{p,r}(a+b\alpha)}$. The following theorem justifies the choice of the vectors $v_{p,r}(a + b\alpha)$.

<u>Theorem 5.7</u>:

Let $S = \{(a, b) \in T_2\}$ be a finite subset of T_2 with the property that $\prod_{(a,b) \in S} (a + b\alpha)$ is a square in the algebraic number field $Q(\alpha)$. Then, for each prime number $p \leq z$ and each $r \in R(p)$, we have $v_{p,r}(a + b\alpha) \equiv 0 \pmod{2}$.

The proof of this theorem can be found in [14]. For the number field sieve, we are interested in the converse of the theorem: Namely, if $(a + b\alpha) \equiv 0 \pmod 2$ for every prime p $\leq z$ and $r \in R(p)$, does it follow that $(a + b\alpha)$ is a square in $\mathbb{Z}[\alpha]$? Unfortunately, the answer is "no" as the following example shows. In $\mathbb{Z}[i]$, let $S = \{(2, 1), (-1, 2)\}$. Then the elements $2 + i$ and $-1 + 2i$ have norms $N(2+i)=(2+i)(2-i)=5$ and $N(-1 + 2i) = (-1 + 2i)(-1 - 2i) = 5$.

Thus, $v_{p,r}(2 + i) = \begin{cases} 0 \; if \; p \neq 5 \\ 1 \; if \; p = 5 \end{cases}$

and $v_{p,r}(-1 + 2i) = \begin{cases} 0 \; if \; p \neq 5 \\ 1 \; if \; p = 5 \end{cases}$.

Therefore $v_{p,r}(2 + i) + v_{p,r}(-1 + 2i) \equiv 0 \pmod 2$, but $(2 + i)(-1 + 2i) = i(2 + i)^2$ is not a square in $\mathbb{Z}[i]$.

The condition $\sum_{(a,b) \in S} v_{p,r}(a + b\alpha) \equiv 0 \pmod 2$ does not guarantee that $\prod_{(a,b) \in S} (a + b\alpha)$ is a square in $\mathbb{Z}[\alpha]$. This obstacle can be overcome by the use of quadratic characters. The details of this procedure are beyond the scope of this thesis and can be found in [13]. For now, let us assume that this problem is solved and try to put the above ideas together to write the number field sieve algorithm.

You will recall that our objective is to construct a set S such that $\prod_{(a,b) \in S}(a+bm) = X^2$ in $\mathbb{Z}$ and $\prod_{(a,b) \in S} (a + b\alpha)$

$= \beta^2$ in $\mathbf{Z}[\alpha]$. We accomplish this task as follows: For a coprime pair (a, b) for which a + bm and a + bα are both z-smooth in $\mathbf{Z}$ and $\mathbf{Z}[\alpha]$ respectively, we assign the vector e(a, b), which has the usual exponent vector v(a + bm) in its first $1 + \pi(z)$ coordinates and the exponent vector $v_{p,r}$ (a + bα) in the next $1 + \sum_{p \le z} |R(p)|$ coordinates. If we find a set S of coprime integers (a, b) with $\sum_{(a,b) \in S}$ e(a, b) (mod 2) being the zero vector, then both $\prod_{(a,b) \in S}$ (a + bα) will be a square in $\mathbf{Z}[\alpha]$ and $\prod_{(a,b) \in S}(a+bm)$ will be a square in $\mathbf{Z}$ and our goal is achieved.

5.11 The Special Number Field Sieve Algorithm:

Assume that N is of the form $N = r^e - s$, where r and |s| are small positive integers, r > 1, and e is large. The first factorization obtained by means of the number field sieve was the factorization of numbers of the above form, namely the Fermat numbers $F_7 = 2^{2^7} + 1$ and $F_9 = 2^{2^9} + 1$. In the case of F_7, the polynomial that was employed is $f(x) = x^3 + 2$, $m = 2^{42}$ and the algebraic number field is $Q(-2^{\frac{1}{3}})$. In the case of F_9, the polynomial was $f(x) = x^5 + 8$. $m = 2^{103}$ and the algebraic number field is $Q(-2^{\frac{3}{5}})$. In general, we first choose d (d = 5 for numbers having 70 digits or more) and take $m = r^k$, where $k = \left[\frac{e}{d}\right]$. The number $N = r^e - s$ in base m is $N = m^d - sr^{kd-e}$, and hence the polynomial f(x), is given by $f(x) = x^d - sr^{kd-e}$. Since $0 \le kd - e < d$ and s and r are small, so is $s\, r^{kd-e}$. Moreover, $f(m) = m^d - sr^{kd-e} = r^k - sr^{kd-e} = r^{kd-e}(r^e - s) = r^{kd-e}N \equiv 0 \pmod N$.

REFERENCES

[1] Bressoud, D. M. Factorization and Primality Testing, Springer-Verlag, New York, 1989.

[2] Brillhart, J. Fermat's Factoring Method and its Variants, Congressus Numeratium, Volume 31 (1981), pp. 29-48.

[3] Cohen, H. A Course in Computational Algebraic Number Theory, Springer-Verlag, 1993.

[4] Davis, J. A. and D. B. Holdridge , Factorization Using the Quadratic Sieve Algorithm, Sandia Report Sand 83-1346, Sandia National Laboratories, Albuquerque, NM (1983).

[5] Dixon, J. D. Factorization and Primality Tests. American Mathematical Monthly. Volume 91 (1984), pp. 333-353.

[6] Guy, R. K. How to Factor a Number. Proceedings of the Fifth Manitoba Conference on Numerical mathematics. Utilitas, Winnepeg, Manitoba, (1975), pp. 49-89.

[7] Knuth, D. E. Art of Computer Programming: Semi-Numerical Algorithms, Volume 2, 2nd ed., Addison-Wesley, Reading, Massachusetts, 1981.

[8] Knuth, D. E. and Luis Trabb-Pardo, Analysis of a Simple Factorization Algorithm, Theoretical Computer Sc. 3 (1976) pp. 321-348.

[9] Koblitz, N. A Course in Number Theory and Cryptography, Springer-Verlag, New York, 1987.

[10] Kraitchik, M. Recherches Sur la Theorie des Nombers, Tom 11. Factorisation. Gautheir-Villars, Paris, 1929.

[11] Legendre, A. M. Theorie des Nombers, Vol. 1 (3rd ed.), Paris, 1830.

[12] Lehman, R. S. Factoring Large Integers, Math Comp. 28 (1974) pp. 637-646.

[13] Lehmer, D. H. and R.E. Powers, On Factoring Large Numbers, Bull Am. Math Soc. 37 (1931) pp. 770-776.

[14] Lenstra, A. K. and H. W. Lenstra, Jr. (eds), The Development of the Number Field Sieve, Lecture Notes in Mathematics, 1554, Springer-Verlag, Berlin, 1993.

[15] Menezes, A. and S. Vanstone (eds.) Solving Large Sparse Linear Systems Over Finite Fields, Advances in Cryptology: Crypto 90, Lecture Notes in Computer Science, Springer-Verlag, 1991.

[16] Morrison, M. A. and John Brillhart, A Method of Factoring and the Factorization of F_7. Math. Comp. 29 (1975) pp. 183-205.

[17] Pomerance, C. (ed.) Cryptology and Computational Number Theory. American Mathematical Society, 1990.

[18] Pomerance, C. The Quadratic Sieve Factoring Algorithm, in Advances in Cryptology-Proceedings of EUROCRYPT 84 (T. Beth, et. al. eds.) Lecture notes in Computer Science 209, Springer-Verlag, Berlin, (1985), pp. 169-182.

[19] Pomerance,C. Analysis and Comparison of Some Integer Factoring Algorithms, printed in H. W. Lenstra, Jr. and R. Tijdeman, Computational Methods in Number Theory, Part I, Mathematisck Centrum Tract 154, Amsterdam 1982, pp.

89-139.

[20] Riesel, H. Prime Numbers and Computer Methods for Factorization, Birkhauser, Boston, 1985.

[21] Rivest, R., A. Shamir, and L. M. Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM, Volume 21 (1978), pp. 120-126.

[22] Rose, H. E. A Course in Number Theory, Clarendon Press, Oxford, 1988.

[23] Rosen, K. H. Elementary Number Theory and Its Applications, Addison-Wesley, Reading, MA, 1993.

[24] Shanks, D. Class Number, A Theory of Factorization, and Genera, American Mathematical Society, Proc. Symposia in Pure Math, 20 (1971) pp. 415-440.

[25] Wunderlich, M. C., A Running Time Analysis of Brillhart's Continued Fraction Factoring Method, in M. B. Nathanson, ed., Number Theory Carbondale 1979, Lecture Notes in Math. 751 (1979), pp. 328-342.

I, Omar Mahmoud Hamad, hereby submit this thesis/report to Emporia State University as partial fulfillment of the requirements for an advanced degree. I agree that the Library of the University may make it available for use in accordance with its regulations governing materials of this type. I further agree that quoting, photocopying, or other reproduction of this document is allowed for private study, scholarship (including teaching) and research purposes of a nonprofit nature. No copying which involves potential gain will be allowed without written permission of the author.

Omar Hamad
Signature of Author

5/11/1994
Date

Integer Factorization
Title of Thesis/Research Project

Doug Cooper
Signature of Graduate Office Staff Member

May 11, 1994
Date Received

Distribution: Director, William Allen White Library
Graduate School Office
Author