FERMAT'S PRIME FACTORIZATION

M. K. NESA BALAN A/L KRISHNASAMY

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF BACHELOR
OF SCIENCE WITH HONOURS

MATHEMATICS WITH ECONOMICS PROGRAM
SCHOOL OF SCIENCE AND TECHNOLOGY
UNIVERSITI MALAYSIA SABAH

April 2007

UNIVERSITI MALAYSIA SABAH

BORANG PENGESAHAN STATUS TESIS@

JUDUL: FERMAT'S PRIME FACTORIZATION

Ijazah: SARJANA MUDA SAINS, DGNGAN KEPUJIAN

SESI PENGAJIAN: 2004 – 2007

Saya M.K. NESA BALAN A/L KRISHNASAMY

(HURUF BESAR)

mengaku membenarkan tesis (LPS/Sarjana/Doktor Falsafah)* ini disimpan di Perpustakaan Universiti Malaysia Sabah dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Malaysia Sabah.
2. Perpustakaan Universiti Malaysia Sabah dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (/)

□ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

□ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

☑ TIDAK TERHAD

Disahkan oleh

(TANDATANGAN PENULIS)

Alamat Tetap: 36, JALAN MUDA
OFF JALAN MERU
41050 KLANG SELANGOR

Tarikh: 23/4/07

(TANDATANGAN PUSTAKAWAN)

Mr. Rajasegeren
Nama Penyelia

Tarikh: ________

CATATAN: * Potong yang tidak berkenaan.

** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT dan TERHAD.

@ Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan, atau disertasi bagi pengajian secara kerja kursus dan penyelidikan, atau Laporan Projek Sarjana Muda (LPSM).

DECLARATION

I affirm that this dissertation is of my own effort, except for the materials referred to as cited in the reference section.

10 March 2007

M. K. NESA BALAN A/L KRISHNASAMY
HS2004-2579

CERTIFIED BY

Signature

1. **SUPERVISOR**

   (Mr. Rajasegeran Ramasamy)

2. **EXAMINER 1**

   (Mr. Tiong Kung Ming)

3. **DEAN**

   (Supt./Ks. Prof. Madya Dr. Shariff AK Omang)

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor, Mr. Rajasegeran Ramasamy for giving me the motivation, supervision and all the help needed to finalize and complete this thesis, for the hours spent reading and correcting the many drafts and for his efforts in guiding me throughout these months while ensuring that I get his utmost from his knowledge and experience.

I would also like to thank all my friends, housemates, fellow course mates and also my family for giving me the motivation and ideas needed to see myself through this dissertation.

Last but not least, I thank God for blessing me with everything that I needed in order to fulfill this thesis.

ABSTRACT

Prime numbers are numbers that have only two factors, itself and the number one. The factorization of a number into its constituent primes is known as prime factorization. This thesis focuses on a prime factorization method known as Fermat Factorization Method which was the work of French mathematician Peirre de Fermat. In this disertation, Fermat's method is compared with another method to see how efficient the method is. Microsoft Excel 2003 Program is also used in order to enhance Fermat Factorization Method to obtain the factors of any given number faster with lesser amount of work and time used. This is due to the fact that the amount of time and iterations required to factorize an integer into it's prime factors increases rapidly with the increment of the size of the integer. The usage of Microsoft Excel 2003 program was successful in enhancing the speed of calculating the prime factors thus saving a lot of time and energy while avoiding from computing large sums of iterations. As a result, integers up to ten digits were factorized in Microsoft Excel using Fermat's method.

PEMFAKTORAN PERDANA

ABSTRAK

Nombor Perdana merupakan nombor yang hanya mmpunyai dua factor iaitu nombor itu sendiri dan nombor satu. Pemfaktoran sesuatu nombor kepada nombor-nombor perdananya dikenali sebagai pemfaktoran perdana. Desertasi ini menumpu kepada satu kaedah pemfaktoran perdana yang dikenali sebagai Kaedah Pemfaktoran Perdana Fermat. Kaedah ini merupakan hasil kerja ahli matematik Pierre de Fermat. Dalam disertasi ini, kaedah Fermat dibandingkan kepada satu kaedah yang lain untuk memerhatikan kaedah mana yang memperlihatkan keputusan dan analisis yang lebih efisien. Program Microsoft Excel 2003 turut digunakan untuk memudahkan pengiraan serta mengurangkan langkah-langkah dalam kaedah Fermat disebalik mendapatkan keputusan dengan lebih cepat lagi. Program ini digunakan disebabkan amaun masa serta langkah-langkah yang diperlukan untuk memfaktorkan sesuatu nombor akan bertambah apbila saiz nombor tersebut meningkat. Penggunaan Microsoft excel berjaya mempercepatkan proses pengiraan faktor perdana dan dengan itu menjimatkan masa serta mngelak daripada melakukan iterasi yang banyak. Hasil itu, integer sebesar sepuluh digit dapat difaktorkan dalam Microsoft Excel dengan mnggunakan kaedah Fermat.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

Z	Integers
∈	Element of
=	Equal sign
≡	Equivalence
→	Arrow
Δ	Delta
⌈ ⌉	Ceiling brackets
⌊ ⌋	Floor brackets
[ ]	Square brackets
( )	Parentheses
≤	Inequality sign; lesser than or equal to
≥	Inequality sign; greater than or equal to
〉	Inequality sign; greater than
〈	Inequality sign; lesser than
•	Multiplication sign
+	Addition sign
-	Subtraction sign
/	Division sign
$\lvert\ \rvert$	Modulus
{	Left brace
∏	Product with no limits
√	Square root sign
O	Omicron
Θ	Theta

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

1.1.1 An Introduction To Integer Factorization

Mathematicians have long been fascinated with the problem of factoring integers. Factorization is the determination of factors or divisors of a given integer. In other words, factorization or factoring is the decomposition of an integer into a product of other integers, or factors, which when multiplied together give the original integer (Rosen, 2005). For example, 2 and 8 are factors of 16, because $2 \times 8 = 8 \times 2 = 16$. Some numbers have more than one factorization depending on the way it is being factored. For instance, 10 can be factored as 1×10, 2×5 or $1 \times 2 \times 5$.

Factoring integers is an extremely active and equally important area of mathematical research, especially because it is essential in the art of cryptography, which is the study of codes. The aim of factoring is usually to reduce something to "basic building blocks", such as reducing numbers into prime numbers, or polynomials to irreducible polynomials (Rosen, 2005). We will specifically further look into the integer factorization of prime numbers below.

1.1.2 Prime Numbers

The ancient Greek mathematicians first studied prime numbers and their properties extensively. The mathematicians of Pythagoras's school (500 BC to 300 BC) were interested in numbers for their mystical and numerological properties. They understood the idea of primality and were then further interested in the study of prime numbers itself (Katz, 1993).

A prime number p is a counting number that only has two factors, itself and one. In other words, a prime number cannot be expressed as the product of smaller numbers (Burton, 2002). For an example, we use the number 13. 13 cannot be expressed as the product of any smaller numbers. Its' only factors are the numbers 1 and 13 itself. Counting numbers which have more than two factors, such as the number eight, whose factors are 1, 2, 4 and 8, are said to be composite numbers. The number one only has one factor and is considered to be neither prime nor composite. The first few numbers in prime number series goes as follows: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 57, 59, 61, 67,...

1.1.3 Prime Factorization

In many cases of interest particularly in prime factorization, factorization is unique, and so gives the simplest representation of a given quantity in terms of smaller parts. The fundamental theorem of arithmetic is a very important theory that concludes that the primes are the multiplicative building blocks of the integer. This theorem is also called the unique factorization theorem. According to the theory, every positive integer greater than 1 can be written uniquely as a product of primes (Rosen, 2005). In other words, any whole number bigger than 1 can be represented in exactly one way as a product of primes. The recognition of the fact that whole numbers bigger than 1 can be represented in just one way as the product of primes is attributed to Euclid, who lived from 325 BC until he died in Alexandria, Egypt in 265 BC (Katz, 1993).

It is already understood that prime factorization is the factorization of a number into its constituent primes. Given a positive integer $n \geq 2$, the prime factorization is written

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \bullet\bullet\bullet\, p_k^{\alpha_k} \tag{1.1}$$

where the p_is are the k prime factors, each of order α_i. Each factor $p_i^{\alpha_i}$ is called a primary (www.mathworld.wolfram.com). As an example, we can write the integer 2844 as the product of $2 \times 2 \times 3 \times 3 \times 79$. Therefore, the prime factorization for 2844 is $2^2 \bullet 3^2 \bullet 79$. The first few prime factorizations are given in the following table below. Note that the integer 1 does not have a prime factorization.

Table 1.1 Simple prime factorization

n	prime factorization
2	2
3	3
4	2^2
5	5
6	$2 \bullet 3$
7	7
8	2^3
9	3^2
10	$2 \bullet 5$
11	11
12	$2^2 \bullet 3$
13	13
14	$2 \bullet 7$
15	$3 \bullet 5$
16	$2^3 \bullet 2$
17	17
18	$2 \bullet 3^2$
19	19
20	$2^2 \bullet 5$

Note that the prime factors in the product or divisors are always usually written in a nondecreasing order. The prime-power factorization of a positive integer *n* encodes valuable information about *n*. Once given the product of the factorization, we can immediately deduce whether a prime *p* divides *n* since *p* divides *n* if and only if it appears in this factorization. Also, by expressing numbers as products of prime factors, it is easy to find their Greatest Common Divisor, or their Least Common Multiple. The greatest common divisor or GCD of two or more numbers is the largest number that evenly divides all the numbers. The Least Common Multiple of two nonzero integers is the smallest positive integer that is divisible by both of the mentioned two nonzero integers (Rosen, 2005).

In general, prime factorization is a difficult problem as it becomes harder and harder to factorize an integer as the integer becomes larger, and many sophisticated prime factorization algorithms have been devised for special types of numbers. Given an algorithm for integer factorization, one can factor any integer down to its constituent primes by repeated application of this algorithm. For very large numbers, besides computer based algorithm, no efficient algorithm is known for prime number factorization. For smaller numbers, however, there are varieties of different algorithms that can be applied in the factorization of primes.

As has been said earlier, many algorithms have been devised for determining the prime factors of a given number. The simplest method of finding prime factorizations is called the direct-search factorization or better known as the trial division. In this method, all possible factors are systematically tested using trial division to see if they actually divide the given number. It is practical only for very small numbers. The fastest known fully-proven deterministic algorithm is the Pollard-Strassen method. Other popular algorithms are such as the Fermat factorization method, continued fraction factorization method, Euler's factorization method and many more.

In this dissertation, we will touch briefly into some of the known prime factorization algorithm. We will also look closely at the work of Pierre de Fermat and his Fermat factorization method.

1.1.4 A brief History On Pierre de Fermat

Pierre de Fermat was a lawyer by profession. He was a noted jurist at the provincial parliament in the French city of Toulouse. Probably the most famous amateur mathematician in history, he was the son of a wealthy leather merchant and second consul of Beaumont- de- Lomagne. He attended at the University of Toulouse before moving to Bordeaux somewhere in the middle of the 1620s. From Bordeaux, Fermat went to Orléans where he studied law at the University. Soon after, he received a degree in civil law. He then purchased the offices of councilor at the parliament in Toulouse. So by the year 1631 Fermat was a lawyer and government official in Toulouse and because of the office he now held he became entitled to change his name from Pierre Fermat to Pierre de Fermat (Wikipedia, 2005).

For the remainder of his life he lived in Toulouse but he also worked in his home town of Beaumont-de-Lomagne and a nearby town of Castres throughout the years. Fermat worked in the lower chamber of the parliament from his appointment on 14 May 1631 but on 16 January 1638 he was appointed to a higher chamber and then in 1652 he was promoted to the highest level at the criminal court in Toulouse. Still further promotions seem to indicate a fairly meteoric rise through the profession but promotion was done mostly on seniority and the plague that struck the region in the early 1650s meaning that many of the older men died. Fermat himself was struck down by the plague but he soon recovered from it.

The French lawyer pursued mathematics in his spare time. Although he pursued it as an amateur, his work in number theory was of such exceptional quality and erudition. Fermat was one of the inventors of analytic geometry. Furthermore, he also helped lay the foundations of calculus. Together with Pascal, he gave a mathematical basis to the concept of probability. His work on prime numbers was equally essential. He invented his own method for prime factorization named Fermat factorization method and also derived the Fermat number. Some of his renowned theorems are the Fermat's Last Theorem and the Fermat's Little Theorem. He solved many fundamental calculus problems, and made important contributions to number theory and optics. Fermat was also fluent in French, Greek, Latin, Italian, and Spanish (Wolfram, 1999).

Figure 1.1 Pierre de Fermat (1601-1665)

1.2 RESEARCH OBJECTIVES

The objectives of this research are as follows:

i) To fully understand the integer factorization of prime numbers and the many sophisticated prime factorization algorithms that has been devised to factor such numbers.

ii) To introduce one of the methods used in prime factorization which is the Fermat factorization method.

iii) To understand and use Fermat factorization in order to factorize any given numbers.

iv) To compare Fermat's method with another method to see how efficient this method is.

v) To use Microsoft Excel 2003 Program in order to enhance Fermat Factorization Method to obtain the factors of any given number faster with lesser amount of work and time used.

1.3 RESEARCH SCOPE

This dissertation will mainly revolve around the five main objectives mentioned above. It will be fully concentrated in showing the various algorithms used in prime factorization mainly the Fermat factorization method. As Fermat's method is a rather primitive method, we shall focus on factoring numbers only up to 10 digits as it becomes difficult to factor number beyond that size with our method.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Throughout the ages, many algorithms have been devised for determining the prime factors of a given number. They vary quite a bit in sophistication and complexity. It is very difficult to build a general-purpose algorithm for this computationally hard problem because factoring large numbers can be very difficult and time consuming. Even so, a remarkable number of essential mathematics and a significant number of the most important mathematicians in history have contributed to the findings of these many prime powered factorization methods.

2.2 PRIME FACTORIZATION ALGORITHMS

2.2.1 Trial Division

One of the earliest and most direct methods to factorize integers is known as the trial division. This method is a trial and error method which requires one to continuously divide integer n successively by the primes 2, 3, 5,…., not exceeding $\sqrt{n}$ until we get the prime factorization of n or we conclude that n is prime (Rosen, 2005). However, this method for finding the prime factorization of an integer is quite inefficient and rather time consuming. As it is a trial and error method, finding the factors for a very large integer will require a fairly large number of divisions and equally huge amount of time. Only divisors up to $\lfloor\sqrt{n}\rfloor$ need to be tested when using this method on a number n since if all integers less than this had been tried, then

$$\frac{n}{\sqrt{n}+1}\langle\sqrt{n} \tag{2.1}$$

This would mean that all possible factors have had their cofactors already tested. This would then confirm that when the smallest prime factor p of n is $\rangle\sqrt[3]{n}$, then its cofactor m must be prime. In order to prove this, suppose that the smallest p is $\rangle\sqrt[3]{n}$. If $m = ab$, then the smallest value a and b that we could assume is p. But then

$$n = mp = pab \geq p^3\rangle n \tag{2.2}$$

which cannot be true. Therefore, m must be prime, so

$$n = p_1 p_2 \tag{2.3}$$

2.2.2 Euler's Factorization Method

The Euler's factorization method is a factorization algorithm which works by expressing N as a quadratic form in two different ways (Wikipedia, 2005). Then

$$N = a^2 + b^2 = c^2 + d^2 \tag{2.4}$$

so that

$$a^2 - c^2 = d^2 - b^2$$
$$(a-c)(a+c) = (d-b)(d+b)$$

then k will then be set as the greatest common divisor of $a-c$ and $d-b$ so that we may write

$$a-c=kl \tag{2.5}$$

$$d-b=km \tag{2.6}$$

whereby l and m equals 1. Therefore we can continue writing

$$l(a+c)=m(d+b)$$

but since l and m equals 1, $m \mid a+c$ and

$$a+c=mn$$

which gives

$$d+b=lm$$

so we have

$$\begin{aligned}\left[\left(\frac{1}{2}k\right)^2+\left(\frac{1}{2}n\right)^2\right](l^2+m^2) &= \frac{1}{4}(k^2+n^2)(l^2+m^2)\\ &= \frac{1}{4}\left[(km)^2+(kl)^2+(nm)^2+(nl)^2\right]\\ &= \frac{1}{4}\left[(d-b)^2+(a-c)^2+(a+c)^2+(d+b)^2\right]\\ &= \frac{1}{4}(2a^2+2b^2+2c^2+2d^2)\\ &= \frac{1}{4}(2N+2N)=N \qquad (2.7)\end{aligned}$$

2.2.3 Continued Fraction Factorization Method

The continued fraction factorization method (CFRAC), stemming from ideas of Legendre, Kraitchik, Lehmer and Powers, and developed for computer use by

Brillhart and Morrison, is a prime factorization algorithm which uses residues produced in the continued fraction of $\sqrt{mN}$ for some suitably chosen m to obtain a square number (Cohen, 1993). The main idea of CFRAC is to find integers x and y such that

$$x^2 \equiv y^2 (\bmod n)$$

by finding an m for which m^2 $(\bmod n)$ has the smallest upper bound. Since $x^2 - y^2 = (x-y)(x+y)$, it is clear that the greatest common divisor$(N, x+y)$ will be a non-trivial factor of N . Therefore, we can obtain a congruence $x^2 \equiv y^2 (\bmod n)$ and hence a non-trivial splitting of N . This method requires by conjecture, about $\exp\left(\sqrt{2 \ln n \ln \ln n}\right)$ steps, and was the fastest prime factorization algorithm in use before the quadratic sieve.

2.2.4 Dixon's Factorization Method

The Dixon's factorization method is a modified form of the Fermat factorization method whereby in order to find integers x and y such that

$$x^2 \equiv y^2 (\bmod n)$$

in which case there is a 50% chance that the greatest common divisor$(N, x+y)$ is a factor of n, choose a random integer r_i, compute

$$g(r_i) \equiv r_i^{\,2} (\bmod n),$$

and try to factor $g(r_i)$. If $g(r_i)$ cannot be easily factorized to some small trial divisor d, then try another r_i. The trial r_s are usually taken to be $\lfloor \sqrt{n} \rfloor + k$, with k = 1, 2,...

REFERENCES

Bourbaki, N., 1991. *Elements of the History of Mathematics.* Springer-Verlag, New York.

Bressoud, D. M., 1989. *Factorization and Primality Testing*. Springer-Verlag, New York.

Buhler, J. P., 1998. *Algorithmic Number Theory*. Springer-Verlag, Germany.

Burton, D. M., 2002. *Elementary Number Theory*. The McGraw-Hill Companies, Inc., New York.

Cohen, H., 1993. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Germany.

Conway, J. H. and Guy, R. K., 1996. *The Book of Numbers*. Springer-Verlag, New York, Inc., USA.

Ebbinghaus, H. & Remmert, R., 1990. *Numbers*. Springer-Verlag, New York.

Katz, V. J., 1993. *A History of Mathematics*. HarperCollins College Publishers, New York.

Mollin, R. A., 1998. *Fundamental Number Theory with Applications*. CRC Press LLC, Florida.

Rosen, K. H., 2005. *Elementary Number Theory*. McGraw-Hill, New York.

Scharlau, W. and Opolka, H., 1985. *From Fermat to Minkowski*. Springer-Verlag, New York.

The University of Utah, 1996, *The 10000 Smallest Prime Numbers*, Retrieved 12 March 2007

http://www.math.utah.edu/~pa/math/p10000.html

Wikipedia, 2005. *Fermat Factorization*. Retrieved 23 August 2006.

http://en.wikipedia.org/wiki/Fermat_Factorization.

Wolfram, 1999. *Prime Factorization*. Retrieved 24 August 2006.

http://www.mathworld.wolfram.com/PrimeFactorization.html

Wolfram, 1999. *Fermat Factorization*. Retrieved 24 August 2006.

http://www.mathworld.wolfram.com/ Fermat Factorization.html