University of Science and Technology

Faculty of Computer Science & Information Technology
Collage of Postgraduate Studies

MSc in Computer Science

Factorization Algorithms for Integers of the Form Z MOD 6 = +1

Thesis submitted in Partial Fulfillment of the Requirements for the Degree of Master of Computer Science

By:

Ebtisam Abaker Adam

Supervisor:

Dr. Noureldien Abdlerhman

Noureldien

2014

Abstract

Prime numbers are known to be in one of two series; $Z \bmod 6 = \pm 1$. In this thesis, we use the concept of Integer Absolute Position in prime series, to develop structures for composite integer numbers in the prime series $Z \bmod 6 = +1$.

The developed structures ware used to state theorems and to develop deterministic algorithms that can test simultaneously for primality and prime factors of integers of the form $Z \bmod 6 = +1$.

The developed algorithms are compared with the one of the best known factoring algorithm Pollard-Roh. The results show that the new developed algorithms performs well when the two factors are same or one of the factors near to the square root or near to the value 1.

Although the current version of the algorithms is of complexity $O((N/6^2)\ ½\ /4)$, but the facts that, the algorithms has a parallel characteristics and its performance is dependent on a matrix search algorithms, makes the algorithms competent for achieving better performance

المستخلص

من المعروف أن الأعداد الأولية هى واحدة من مجموعتين إما (Z MOD 6 = -1) أو (Z MOD 6 = +1) ، فى هذا البحث سيتم إستخدام مفهوم الموقع المطلق (Absolute Position) للأعداد الأولية وإستخدام المفهوم لتطوير هياكل للأرقام الصحيحة المركبة .

سيتم إستخدام الهياكل المطورة لإنشاء نظريات لتطوير خوارزميتين تستطيعان بصورة متزامنة (فى نفس الوقت) إختبار الأولية وإيجاد العوامل الأولية للأعداد الصحيحة فى المجموعة (Z MOD 6 = -1) والمجموعة (Z MOD 6 = +1)، نحن نطمح لتقديم خوارزميات تعملان بصورة سريعة فى حساب الأولية وإيجاد العوامل للأعداد الصحيحة المركبة.

تمت مقارنة الخوارزميات المصممة مع واحدة من أسرع خوارزميات حساب الأولية وإيجاد العوامل للأعداد الصحيحة وهى (Pollard-Roh). تبين من النتائج أن الخوارزميات تكون عند أفضل أداء عندما يكون المعاملان قريبان من بعضهما البعض أو عندما يكون أحد المعاملان قريب من قيمة الجزر التربيعى أو قريب من القيمة واحد.

على الرغم من أن الإصدار الحالي من الخوارزميات هو من فعالية (4 / ½ (N/62))O، إلا أن الحقائق تشير إلى أن الخوارزميات لديها خصائص التوازى فى تنفيذ العمليات وأدائها يعتمد على خوارزمية البحث فى المصفوفة، مما يجعل الخوارزميات المعنية قابلة لتحقيق أداء أفضل.

1.1 Introduction

Natural Numbers (greater than one) which can only be divided by 1 and itself are called prime numbers. Non prime numbers are called composite numbers [2], the property of being prime (or not) is called primality[16].

A composite number is a number that can be written as the product of two positive integers other than 1 and the number itself. For example: 14 is a composite number because it can be written as 7 times 2. In this case, 7 and 2 are called factors of 14 [9].

Factoring a positive integer n means finding positive integers u and v such that the product of u and v equals n, and such that both u and v are greater than 1. Such u and v are called factors (or divisors) of n, and $n = u * v$ is called a factorization of n [3].

Factoring is an important process in algebra which is used to simplify expressions, simplify fractions, and solve equations .

1.2 Problem definition

The problem is how to factorize big numbers very fast. Our exact problem is how to factor or test primality of the form Z mod 6 = + 1, when both factors of Z are of the form Z mod 6 = + 1.

1.3 Research Objectives

The objective of the research is to develop a fast primality testing and factorization algorithm for integer of the form Z mod 6 = +1 Based on work in "A deterministic Factorization and Primality Testing Algorithm for Integers of the form Z mod 6 = -1", presented by Noureldien

Abdelrhman Noureldien, Mahmud Awadelkariem, and DeiaEldien M.Ahmed,, which was doveolp the structural design for prime series Z mod 6 = -1.

1.4 Research Methodology

In this research we adopt an analytical approach to rationale the development of the proposed algorithms, and an empirical approach through experiments to test and compare the developed algorithms.

Based on the work in "A deterministic Factorization and Primality Testing Algorithm for Integers of the form Z mod 6 = -1", this thesis deals with integers of the form Z mod 6 = + 1. Our proposed approach handles primality testing and prime factorization as one problem, and is based on looking for a prime factor for a given integer within a determined search space. If a factor is found within

this space then the given integer is composite otherwise it is prime.

To define the search space, we use the concept of absolute position for composite numbers of the form Z mod 6 = + 1, to define an infinite matrix space of absolute positions for composite numbers.

In this structure or matrix space a composite number is represented by its absolute position, and its location in the matrix space is defined by its factors. To determine the matrix space searching boundaries for a given integer we state and proof some theorems based on absolute position concept.

Based on the stated theory we present a deterministic primality testing and factorization algorithms by constructing simple equations that associate the absolute position of the integer under testing to its prime factors.

1.5 Results

The developed algorithms are compared with the best known factoring algorithm Pollard- Roh. The results show that the developed algorithms for R1 perform well when the two factors are close compared with Pollard-Rho which performs normal.

The worst case of the two algorithms for R1 is when Z is prime number in this case Pollard- Rho will performs well, and the average case is when Z is composite and f1 and f2 are not twins.

This thesis contributes to number theory efforts in introducing new concepts and approaches to develop algorithms that reduce the complexity (speed) of primality testing and factorization algorithms.

1.6 Thesis Organization

This thesis is organized as follows; in chapter two some primality testing algorithms and some factorization algorithms are discussed.

In chapter three the prime series R1 is defined, and the structure of Absolute Position of composite numbers of the form **Z mod 6 =+1** are stated. Based on the structure a primality testing and factorization algorithm for R1 is developed.

In chapter four the developed algorithms are tested against Pollard-Roh algorithm. Conclusions and recommendations for future work are given in chapter five.