جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى/كلية العلوم / قسم الرياضيات

بعض تطبيقات الكسور المستمرة على عدد كاوسيان صحيح

رسالة مقدمة

الى/جامعة ديالى/كلية العلوم/ قسم الرياضيات كجزء من
متطلبات نيل شهادة الماجستير في علوم الرياضيات

من قبل

وائل محمود عباس

بأشراف

أ.م. د. روكان خاجي محمد

أ.م. د. رفعت زيدان خلف

1444/ ذو الحجة

حزيران /2023

Chapter One

General Introduction

Chapter One

General Introduction

1.1 Overview

A continued fraction is a way of representing real numbers (Finite and infinite) as the sum of successive divisions of the number. Continuous fraction is used in many area . They have given us a way to construct an approximation from rational to irrational numbers. Some computer algorithms use continued fractions to solve for these approximations**.**Pell’s equation has a long history. Pell's equations have drawn the interest of numerous mathematicians, who have worked extensively on them. India saw the first significant advancement in Pell's equations' solution. Brahmagupta explained how to leverage existing solutions to Pell's equation to produce new ones in AD 628. Following that, Bhaskaracharya provided a method for locating a minimally positive solution to Pell's equation in AD 1150.

In addition to providing an algorithm, Brahmagupta discusses how to create fresh solutions from existing ones. Through numerous reductions throughout the years, Bhaskaracharya expanded on Brahmagupta's work on Pell's equation. Because that A and B are positive and D is a positive non-square integer, the quadratic Diophantine equation of form A^2-DB^2 = 1 can be solved. Where D is a positive not perfect square integer and A and B are unknowns, Pell's equation is known as such due to an incorrect attribution of Euler. A solution approach similar to the solution by continuing fractions was described by Brouncker and Wallis.Also, in this thesis, another application of continuous fractions was studied, which is a method of Attacking the RSA Algorithm on Gaussian integers by using Continued Fraction and Number theory is concerned of studying the properties of the positive integers and that cryptography is an application of number theory. Most of the known encryption algorithms are based on using the integers. **[18]**

1.2 Related Works

In mathematics, new results are always constructed from previous results. This way you can improve existing achievements instead of starting from scratch. Therefore, it is necessary to understand the field of continuous fractions and, if necessary, contribute to learning more about its past.

We can to come back to the history of continuous fractions using the Euclid algorithm for the largest common denominator . This algorithm generates continuous fractions as a by-product**. [4]**

For more than 1000 years.using continued fractions was limited to specific examples. And the Indian mathematician Aryabhata used continued fractions to solve linear indeterminate equations .where we can find specific examples and traces of continued fractions throughout Greek and Arab writing.**[4]**

The Dutch mathematician Huygens in 1687 used continuous fractions for the first time. He used the convergents of a continuous fraction to determine the optimum rational approximations for gear ratios, allowing him to build a functional mechanical planetarium.[**33**].

A generic solution to Pell's Equation was found by Lagrange using continuous fractions. By proving that the expansion of an irrational number by regular continuous fractions is periodic, he proved the converse of Euler's Theorem, which states that if an irrational number x is a solution to a quadratic equation, then x is a solution to the equation. Lagrange used continued fractions to develop a general method for obtaining the continuing fraction expansion of the solution to a differential equation in a single variable during his work on integral calculus in 1776.[**9**]

In 1625, Daniel Schwenter was the first mathematicians to make an actual contribution to determining convergence Continuous fractions. His main concern was to reduce fraction, which involve large numbers. He defined the basic rule that we now use for arithmetic. The successive convergences that we rely on today in continuous fractions **[34]**

Viscount The first independent study of continuous fractions was conducted by William Brouncker in 1655; where his work was published in 1656 by his friend John Wallis's Arithmeticas infinitorum. Wallis defined several characteristics of convergents and documented how to compute the nth convergent in his book Opera Mathematica; for example,$\frac{4}{\pi} = 1 + \frac{1}{2+\frac{9}{2+\frac{25}{2+\frac{49}{2+\cdots.}}}}$.(1695) However, Brouncker found a solution to the Pell's Equation A^2 - DB^2 =1. **[4,25]**

In addition, he proved the theory that every continuous fraction is a solution to quadratic equations and calculated a continued fraction expansion, which give us a simple method for calculating the exact value of any periodic continued fractions. **[4,25]**

Using a continuous portion of tan (x), Lambert proved the irrationality of π in 1761. His work one was an extension of Euler's, and he showed that if x is a nonzero rational, then e^x and tan x are irrational. **[4]**

A generic solution to Pell's Equation was found by Lagrange using continuous fractions. By proving that the expansion of an irrational number by regular continuous fractions is periodic, where she proved the opposite of Euler's theorem, which states that if not relative number X is a solution to a quadratic equation, then X is a solution to the equations. Lagrange used continued fractions to develop a general method for obtaining the continuous fractions expansion of the solution to a differential equation in a single variable during his work on integral calculus in 1776. **[4]**

In the year 1997 the scientist Bosma, W., Cannon, J.,and Playoust, wrote research titled The Magma algebra system i: The user language. J. Symb. Comput. **[11]**

And in the year 2018 scientist Bremner, A., Tho, N.X., wrote a research titled The equation (w + x + y + z)(1/w + 1/x + 1/y + 1/z) = n. Int. J. Number Theory. **[8]**

And in the year 2022 the scientist Oleg N. Karpenkov research titled Geometric Continued Fractions. **[20]**

And In the year 2008 the scientist Luchko, Y.F.; Martinez, M.; Trujillo a research titled Fractional Fourier transform and some of its applications. **[19]**

And In the year 2019 the scientist Upadhyay, S.K.; Khatterwani, K a research titled Upadhyay, S.K.; Khatterwani, K. **[31]**

Ibran, Z. , Aljatlawi, E. and Awin, A. (2022) On Continued Fractions and Their Applications. Journal of Applied Mathematics and Physics. **[21]**

1.3. Motivation

The researcher finds himself in important situations, including making decisions about how to handle what he wants you to do. One such application is Pell's equation, for example. An interesting example of Pell's equation on the cattle problem from both an arithmetic and a historical perspective is given by Archimedes' cattle problem (287-212 BC). It is now generally attributed to Archimedes. In twenty-two Greek elegiac pieces, the problem requires the number of white, black, spotted, and brown bulls and cows belonging to the sun god which are subject to several arithmetic constraints in modern mathematical notation. The problem is no less elegant. Writing A, B, C, and D for the numbers of white, black, spotted, and brown bulls, respectively, for that made studying the equation interesting and often challenging. **[2]**

There are also other applications applied in our daily lives, namely Wiener’s attack on RSA This has applications to electronic money transfer as well. Financial information must be secure. Checks can be signed electronically with RSA. Further measures should be taken, such as the implementation of unique check numbers allowing verification of that particular transferable disbursal number. **[6]**

1.3 Problem Statement

The Pell's equation is a quadratic equation with two variables, so its solution depends on the value of D and N,So researchers have asked a set of questions to solve the Pell's equation in the field of Gaussian integer by continuous fractions.

1- Does the equation have a solution in the domain of a Gaussian integer?

2- Are all cases N, D In Pell's equation it has a solution?

3- Can the researcher find solutions theoretically?

4- If we have a basic solution, can the rest of the solutions be obtained .

In addition to that , Is that a public key algorithm RSA It is not safe towards attack by the continuous fracture algorithm, especially when it is d Small . **[6]**

1.4 Aim of Thesis

The purpose of this thesis is :

1. Pell's equation is solvable in the field of Gaussian integers based on value D,N.

2. If it was D Negative, Pell's equation has a finished solution .

3. If it was D the perfect square, We say that D = P^2 Pell's equation becomes $A^2 - P^2B^2 = N$**,** It can be solved directly .

4. If it was D she non-perfect square So solve Pell's equation $A^2 - DB^2 = \pm 1$ depends on the length periodic (even,odd) .

5. Show that Pell's equation has no solution and this has been proven.

6. An algorithm was attacked by RSA where a value was found d Which is used to decode using continuous fraction approximations in the Gaussian integer field.**[6]**

1.6 Thesis Outline

This thesis contains the following chapters:

Chapter One:(General Introduction)

This chapter contains an introduction, previous works, the problem, its solution, and the objective of the thesis

Chapter Two:(Definitions and Basic Concepts)

This chapter explains some basic definitions and basic concepts that will help us in this letter

Chapter Three: (Finite and Infinite Simple Continued Fractions)

This chapter explains the equation of continuous fractions with integers and how to deal with them, as well as the linear Diophantine equation and some examples and applications on it

Chapter Four: (Solving Pell's equation on Gaussian integer and Wiener's attack on RSA with Gaussian Integer)

This chapter explains continuous fractions with Gaussian integers as well as the linear Pell's equation with Gaussian integers

Chapter Five:(Conclusions and Suggestions for Future Works)

In this chapter we give some concluding remarks which are derived from the outputs of the conducted tests are given; also we give some suggestions for future works we are presented.

المستخلص

بدأ حقل الكسر المستمر في النمو سريعا وكان له تطبيقات مهمة ، بما في ذلك استخدامه في حل معادلات ديفونتين ، وكذلك في خوارزميات الحاسبات لحساب تقريب للعدد النسبي للأرقام الحقيقية .

يعود أصل الكسر المستمر إلى وقت اكتشاف خوارزمية إقليدس ، حيث تم استخدام خوارزمية إقليدس للعثور على القاسم المشترك بين عددين صحيحين.

قدمنا في هذه الاطروحة عن وجود علاقة ارتباط بين معادلة بيل $A^2 - DB^2 = 1$ والكسر المستمر اللانهائي. حيث أوضحنا ما إذا كانت معادلة بيل $A^2 - DB^2 = 1$ لديها حل ، فأن حلول الموجبة يمكن أيجادها عن طريق من $B = q_k$, $A = p_k$ وهي تمثل التقارب $\sqrt{D}$ في حقل GI.

وكذلك وضحنا في هذه الأطروحة إذا كان الحل الأساسي هو $(A_1$ ،$B_1)$ للمعادلة $A^2 - DB^2 = 1$ فأن A_n , B_nهو أيضا حل عن طريق

$$(A_1 + \sqrt{D}B_1)^n = A_n + \sqrt{D}B_n$$

هذا يعني أننا نستطيع أن نأخذ الحل الاساسي ، وتستخدمه في هذه العلاقة $(A_1 + \sqrt{D}B_1)^n$ ونقوم بتوليد زوجً آخر من الحلول A_n , B_n .

قدمنا في هذه الأطروحة تطبيقًا آخر لخوارزمية الكسور المستمر, أذ تم استخدام خوارزمية الكسور المستمرة في مهاجمة خوارزمية المفتاح العام (RSA) مع بعض التعديلات على خوارزمية وينر , حيث تم ايجاد قيمة d الذ يستخدم في فك الشفرة على حقل GI.