Lucas Numbers and Cryptography

A Project Report

submitted by

Thokchom Chhatrajit Singh

in partial fulfilment of the requirements
for the award of the degree
of

MASTER OF SCIENCE
IN MATHEMATICS

2012

DEPARTMENT OF MATHEMATICS
NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA
ROURKELA, ORISSA-769008

CERTIFICATE

This is to certify that the project report entitled *Lucas Numbers and Cryptography* is the bonafide review work carried out by *Thokchom Chhatrajit Singh*, student of Master of Science in Mathematics at National Institute Of Technology, Rourkela, during the year 2012, in partial fulfilment of the requirements for the award of the Degree of Master of Science in Mathematics under the guidance of *Dr. Gopal Krishna Panda*, Professor, National Institute of Technology, Rourkela and that the project has not formed the basis for the award previously of any degree, diploma, associateship, fellowship or any other similar title.

(G.K. Panda)

Professor

Department of Mathematics

NIT Rourkela

DECLARATION

I hereby declare that the project report entitled *Lucas Numbers and Cryptography* submitted for the M.Sc. Degree is a review work carried out by me and the project has not formed the basis for the award of any degree, associate ship, fellowship or any other similar titles.

Place: Thokchom Chhatrajit Singh

Date: Roll No. 410MA2113

ACKNOWLEDGEMENT

It is my great pleasure to express my heart-felt gratitude to all those who helped and encouraged me at various stages.

I am indebted to my supervisor Professor Gopal Krishna Panda for his invaluable guidance and constant support and explaining my mistakes with great patience.

His concern and encouragement have always comforted me throughout. I would like to thank brother Sudhansu Sekhar Rout, Ph.D. scholar, for his valuable help during the preparation of this project.

I would like to thank my friends of NIT Rourkela and outside with whom I am in contact and whom I can always rely upon.

Finally, to my family members and relatives who are always there for me and whom I cannot thank enough!

Rourkela,769008

May, 2012 **Thokchom Chhatrajit Singh**

CONTENTS

INTRODUCTION

We know that the Fibonacci numbers are the numbers from Fibonacci sequence. It was discovered by Leonardo de Fibonacci de Pisa. The Fibonacci series was derived from the solution to a problem about rabbits. The problem is: *If a newborn pair of rabbits requires one month to mature and at the end of the second month and every month thereafter reproduce itself, how many pairs will one have at the end of n months?*

Lucas numbers are the numbers from the Lucas sequence. Lucas sequence is defined by the same recurrence relations as Fibonacci sequence with different initial values. We are considering general Lucas sequence defined by second-order relation i.e, $\{T_n\} = PT_{n-1} - QT_{n-2}$. where $gcd(P, Q) = 1$ and $P, Q \in \mathbb{Z}$. The general solution of the sequence is given by $\{c_1\alpha^n + c_2\beta^n\}$, where α and β are the roots of the corresponding polynomial equation of $\{T_n\}$. If we put the particular values of c_1 and c_2 in the general solution, then we get two particular solutions $U_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ where where $(c_1 = \frac{1}{\alpha-\beta} = -c_2)$ and $V_n(P, Q) = \alpha^n + \beta^n$ where $(c_1 = 1 = c_2)$. This $U_n(P, Q)$ gives the Fibonacci sequence and $V_n(P, Q)$ gives the Lucas sequence. The later will use in the LUC cryptosystem.

We also know that Cryptography is very important in security problems. Nowadays, Everybody want secure information.

In the first chapter we give some definations, theorems, lemmas, on elementary number theory. This chapter is useful for next discussion on the main topic. In the second chapter, we shall discuss the properties of Fibonacci numbers and related numbers call Lucas numbers. And also, we shall give few applications of Fibonacci numbers. In the third chapter, we shall discuss basic things of cryptosystem including RSA Public-key system. Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA sys-

tem in 1977. RSA stands for the first letter in each of its inventors' last names. Finally, we shall also discuss about new LUC cryptosystem which is based on Lucas functions.

"*Experience enables you to recognize a mistake when you make it again*"
***B*y :FRANKLIN P. JONES**.

CHAPTER 1

Prelimnaries of Number Theory

In this chapter we recall some definitions and known results on elementary number theory. This chapter serves as base and background for the study of subsequent chapters. We shall keep on referring back to it as and when required.

Division Algorithm: Let a and b be two integers, where $b > 0$. Then there exist unique integers q and r such that $a = bq + r, 0 \leq r < b$.

Definition 1.0.1. (Divisibility) An integer a is said to be divisible by an integer $d \neq 0$ if there exist some integer c such that $a = dc$.

Definition 1.0.2. If a and b are integers, not both zero, then the greatest common divisor of a and b, denoted by $gcd(a, b)$ is the positive integer d satisfying

1. $d \mid a$ and $d \mid b$.
2. if $c \mid a$ and $c \mid b$ then $c \mid d$.

Definition 1.0.3. (Relatively Prime) Two integers a and b, not both of which are zero, are said to be relatively prime whenever $\gcd(a, b) = 1$.

1.1 Euclidean Algorithm

Euclidean algorithm is a method of a finding the greatest common divisor of two given integers. This is a repeated application of the division algorithm

Let a and b two integers whose greatest common divisor is required. Since $gcd(a, b) = gcd(|a|, |b|)$, it is enough to assume that a and b are positive

integers. Without loss of generality, we assume $a > b > 0$. Now by division algorithm, $a = bq_1 + r_1$, where $0 \leq r_1 < b$. If it happens that $r_1 = 0$, then $b \mid a$ and $gcd(a, b) = b$. If $r_1 \neq 0$, by division algorithm $b = r_1q_2 + r_2$, where $0 \leq r_2 < r_1$. If $r_2 = 0$, the process stops. If the $r_2 \neq 0$ by division algorithm $r_1 = r_2q_3 + r_3$, where $0 \leq r_3 < r_2$. The process continues until some zero remainder appears. This must happen because the remainders $r_1, r_2, r_3, ...$ form a decreasing sequence of integers and since $r_1 < b$, the sequence contains at most b non-negative integers. Let us assume that $r_{n+1} = 0$ and r_n is the last non-zero remainder. We have the following relation:

$$
\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b \\
b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\
&\cdots \quad \cdots \quad \cdots \quad \cdots \\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}
$$

Then $gcd(a, b) = r_n$.

Fundamental theorem of Arithmetic: Any positive integer is either 1, or prime, or it can be expressed as a product of primes, the representation being unique except for the order of the prime factors.

Congruence: Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m if $a - b$ is divisible be m and symbolically this is denoted by $a \equiv b(\text{mod } m)$. We also used to say a is congruent to b modulo m.

Some properties of Congruence:

1. $a \equiv a(\text{mod } m)$.
2. If $a \equiv b(\text{mod } m)$, then $b \equiv a(\text{mod } m)$.
3. If $a \equiv b(\text{mod } m)$, $b \equiv c \ (\text{mod } m)$, then $a \equiv c(\text{mod } m)$.

4. If $a \equiv b(\text{mod } m)$, then for any integer c

   $(a + c) \equiv (b + c)(\text{mod } m); \quad ac \equiv bc(\text{mod } m).$

   Observe that properties 1 to 4, we say that $\equiv$ is an equivalence relation.

Definition 1.1.1. (Fibonacci Numbers) Fibonacci numbers are the numbers in the integer sequence defined by the recurrence relation $u_n = u_{n-1} + u_{n-2}$ for all $n \geq 2$ with $u_0 = 0$ and $u_1 = 1$.

Definition 1.1.2. (Lucas Numbers) Lucas numbers are the numbers in the integer sequence defined by the recurrence relation $v_n = v_{n-1} + v_{n-2}$, for $n > 1$ and $v_0 = 2$, $v_1 = 1$.

1.2 Golden Ratio and Golden Rectangle

The golden ratio, denoted by Φ, is an irrational mathematical constant, approximately 1.61803398874989. In mathematics two quantities are in the golden ratio if the ratio of the sum of the quantities to the larger quantity is equal to the ratio of the larger quantity to the smaller one. Two quantities a and b are said to be in the golden ratio if

$$\frac{a+b}{a} = \frac{a}{b} = \Phi$$

Then

$$\begin{aligned}
\frac{a+b}{a} &= 1 + \frac{b}{a} = 1 + \frac{1}{\Phi} \\
&\Rightarrow 1 + \frac{1}{\Phi} = \Phi \\
&\Rightarrow \Phi^2 = \Phi + 1 \\
&\Rightarrow \Phi^2 - \Phi - 1 = 0 \\
&\Rightarrow \Phi = \frac{1+\sqrt{5}}{2} \\
&\Rightarrow \Phi = 1.61803398874989 \\
&\Rightarrow \Phi \cong 1.618.
\end{aligned}$$

Definition 1.2.1. (Golden Rectangle) A golden rectangle is one whose side lengths are in the golden ratio, that is, approximately $1 : \frac{1+\sqrt{5}}{2}$.

1.3 Construction of Golden Rectangle

A golden rectangle can be constructed with only straightedge and compass by this technique

1. Construct a simple square.
2. Draw a line from the midpoint of one side of the square to an opposite corner.
3. Use that line as the radius to draw an arc that defines the height of the rectangle.
4. Complete the golden rectangle.

1.4 Divisibility

Theorem 1.4.1. *For any integers a,b,c*

1. *If $a \mid b$ and $c \mid d$, then $ac \mid bd$.*
2. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*
3. *If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and y.*

Proof. 1. Since $a \mid b$ and $c \mid d$ then there exist $r, s \in \mathbb{Z}$ such that $b = ra$ and $d = cs$. Now $bd = ra \cdot sc = rs \cdot ac \Rightarrow ac \mid bd$.

2. Since $a \mid b$ and $b \mid c$ then there exist $r, s \in \mathbb{Z}$ such that $b = ra$ and $c = sb$. Now $c = sb = sra \Rightarrow a \mid c$.

3. Since $a \mid b$ and $a \mid c$ then there exist $r, s \in \mathbb{Z}$ such that $b = ar$ and $c = as$. But then $bx + cy = arx + asy = a(rx + sy)$ whatever the choice of x and y. Since $rx + sy$ is an integer then $a \mid (bx + cy)$.

□

1.5 Properties of Greatest Common Divisor

Theorem 1.5.1. *Given integers a and b, not both of which are zero, there exist integers x and y such that $gcd(a, b) = ax + by$.*

Proof. We consider the set S of all positive linear combination of a and b: $S = \{au + bv \mid au + bv > 0; u, v, integers\}$. Then S is non-empty. If $a \neq 0$ then the integer $\mid a \mid = au + b.0$ will lie in S, where we choose $u = 1$ or $u = -1$ according as a is positive or negative. By Well-Ordering Principle, S must contain a smallest element d. Thus, there exist integers x and y for which $d = ax + by$. We claim that $d = gcd(a, b)$.

By Division Algorithm, we have integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be written in the form $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$. Here $r > 0$, implies that r is a member of S. This is a contradiction. Therefore $r = 0$ and $a = qd \Rightarrow d \mid a$. Similarly we will get $d \mid b$. Then d is a common divisor of a and b.

Let c be an arbitrary positive common divisor of a and b. Then $c \mid (ax + by) \Rightarrow c \mid d$. Therefore $c = \mid c \mid \leq \mid d \mid = d$ so that d is greater than every positive common divisor of a and b. Hence $d = gcd(a, b)$. □

Theorem 1.5.2. *Let a and b be integers ,not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.*

Proof. If a and b are relatively prime so that $gcd(a, b) = 1$, then there exist integers x and y satisfying $1 = ax + by$. Conversely, suppose that $1 = ax + by$ and $d = gcd(a, b)$. Since $d \mid a$ and $d \mid b$, then $d \mid (ax + by) \Rightarrow d \mid 1$. This implies that $d = 1$. □

Theorem 1.5.3. *If $a \mid bc$, with $gcd(a, b) = 1$, then $a \mid c$.*

Proof. Since $gcd(a, b) = 1$, then there exist integers x and y such that $1 = ax + by$. Now $c = c.1 = c.(ax + by) = acx + bcy$. Again since $a \mid ac$ and $a \mid bc$, then $a \mid (acx + bcy) \Rightarrow a \mid c$. □

Theorem 1.5.4. *If $b \mid c$, then $gcd(a + c, b) = gcd(a, b)$.*

Proof. Let $d = gcd(a, b)$ and $d' = gcd(a + c, b)$.
To prove: $d \mid d'$ and $d' \mid d$.
Now we have $d \mid a$ and $d \mid b$ and also $b \mid c$. Then $d \mid c \Rightarrow d \mid (a+c)$. Therefore $d \mid d'$. Again $d = ax + by$ for some integers x and y. Then $d = ax + cry$ since $b \mid c$.We get $d' \mid d$. Hence $d = d'$. □

CHAPTER 2

Properties of Fibonacci Numbers and Lucas numbers

2.1 The simplest Properties of Fibonacci Numbers

Theorem 2.1.1. *The sum of first n Fibonacci numbers is equal to* $u_{n+2} - 1$.

Proof. We have

$$u_1 = u_3 - u_2,$$
$$u_2 = u_4 - u_3, ...,$$
$$u_{n-1} = u_{n+1} - u_n,$$
$$u_n = u_{n+2} - u_{n+1}.$$

Adding up these equations term by term, we get

$$u_1 + u_2 +, ..., +u_n = u_{n+2} - u_2 = u_{n+2} - 1.$$

□

Theorem 2.1.2. *The sum of first n Fibonacci numbers with odd suffixes is equal to* u_{2n}.

Proof. We know

$$u_1 = u_2,$$
$$u_3 = u_4 - u_2,$$
$$u_5 = u_6 - u_4, ...,$$
$$u_{2n-1} = u_{2n} - u_{2n-2}.$$

Adding these equations term by term , we obtain

$$u_1 + u_3 + u_5 +, ..., +u_{2n-1} = u_{2n}.$$

□

Theorem 2.1.3. $u_1^2 + u_2^2 +, ..., + u_n^2 = u_n u_{n+1}$.

Proof. We know that

$$\begin{aligned} u_k u_{k+1} - u_{k-1} u_k = u_k(u_{k+1} - u_{k-1}) = u_k^2 \\ u_1^2 = u_1 u_2 \\ u_2^2 = u_2 u_3 - u_1 u_2, \cdots, \\ u_n^2 = u_n u_{n+1} - u_{n-1} u_n. \end{aligned}$$

Adding up the equations,we shall get

$$u_1^2 + u_2^2 +, \cdots, + u_n^2 = u_n u_{n+1}.$$

□

Theorem 2.1.4. $u_{n+m} = u_{n-1} u_m + u_n u_{m+1}$.

Proof. We shall prove the theorem by induction on m. For $m = 1$, we get $u_{n+1} = u_{n-1} u_1 + u_n u_{1+1} = u_{n-1} + u_n$ which is true. Suppose that it is true for $m = k$ and $m = k + 1$, we shall prove it is also true that $m = k + 2$. Let

$$u_{n+k} = u_{n-1} u_k + u_n u_{k+1},$$

and

$$u_{n+(k+1)} = u_{n-1} u_{k+1} + u_n u_{k+2}.$$

Adding these two equations, we get

$$u_{n+(k+2)} = u_{n-1} u_{k+2} + u_n u_{k+3}.$$

Hence,

$$u_{n+m} = u_{n-1} u_m + u_n u_{m+1}.$$

□

Theorem 2.1.5. $u_{n+1}^2 = u_n u_{n+2} + (-1)^n$.

Proof. We shall prove the theorem by induction on n. We have since, $u_2^2 = u_1u_3 - 1 = 1$, the assertion is true for $n = 1$. Let us assume that the theorem is true for $n = 1, 2, \cdots, k$. Then adding $u_{n+1}u_{n+2}$ to both sides, we get

$$u_{n+1}^2 + u_{n+1}u_{n+2} = u_{n+1}u_{n+2} + u_nu_{n+2} + (-1)^n,$$

which implies that $u_{n+1}(u_{n+1} + u_{n+2}) = u_{n+2}(u_n + u_{n+1}) + (-1)^n$. This simplifies to $u_{n+1}u_{n+3} = u_{n+2}^2 + (-1)^n$. Finally we have, $u_{n+2}^2 = u_{n+1}u_{n+3} + (-1)^{n+1}$. □

2.2 Number-Theoretic Properties of Fibonacci Numbers

Theorem 2.2.1. *For the Fibonacci Sequence, $gcd(u_n, u_{n+1}) = 1$ for every $n \geq 1$.*

Proof. Let $gcd(u_n, u_{n+1}) = d > 1$. Then $d \mid u_n$ and $d \mid u_{n+1}$. Then $u_{n+1} - u_n = u_{n-1}$ will also be divisible by d. Again, we know that $u_n - u_{n-1} = u_{n-2}$. This implies that $d \mid u_{n-2}$. Working backwards, the same argument shows that $d \mid u_{n-3}$, $d \mid u_{n-4}, \cdots$, and finally that $d \mid u_1 = 1$. This is impossible. Hence $gcd(u_n, u_{n+1}) = 1$ for every $n \geq 1$. □

Theorem 2.2.2. *For $m \geq 1, n \geq 1$, u_{nm} is divisible by u_m.*

Proof. We shall prove the theorem by induction on n. For $n = 1$ the theorem is true. Let us assume that $u_m \mid u_{nm}$, for $n = 1, 2, 3, ...k$. Now $u_{m(k+1)} = u_{mk} + u_m = u_{mk-1}u_m + u_{mk}u_{m+1} + u_m$. The right hand site of the equation is divisible by u_m. Hence $d \mid u_{m(k+1)}$. □

Lemma 2.2.3. If $m = nq + r$, then $gcd(u_m, u_n) = gcd(u_r, u_n)$.

Proof. We have $gcd(u_m, u_n) = gcd(u_{nq+r}, u_n) = gcd(u_{nq-1}u_r + u_{qn}u_{r+1}, u_n) = gcd(u_{nq-1}u_r, u_n)$. Now we claim that $gcd(u_{nq-1}, u_n) = 1$. Let $d = gcd(u_{nq-1}, u_n)$. Then $d \mid u_{nq-1}$ and $d \mid u_n$. Also that $u_n \mid u_{nq}$. Therefore $d \mid u_{nq}$. This d is the positive common divisor of u_{nq} and u_{nq-1}. But $gcd(u_{nq-1}, u_{nq}) = 1$. This is an absurd. Hence $d = 1$. □

Theorem 2.2.4. *The greatest common divisor of two Fibonacci numbers is again a Fibonacci number.*

Proof. Let u_m and u_n be two Fibonacci numbers. Claim $gcd(u_m, u_n) = u_d$, where $d = gcd(m, n)$. Let us assume that $m \geq n$. Then by applying Euclidian Algorithm to m and n, we get the following system of equations

$$\begin{aligned} m &= q_1 n + r_1, 0 \leq r_1 < n \\ n &= q_2 r_1 + r_2, 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, 0 \leq r_3 < r_2, \cdots, \\ r_{n-2} &= q_n r_{n-1} + r_n, 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Then from the previous lemma,

$$gcd(u_m, u_n) = gcd(u_{r_1}, u_n) = gcd(u_{r_1}, u_{r_2}) \quad = \cdots = gcd(u_{r_{n-2}}, u_{r_n}).$$

Since $r_n \mid r_{n-1}$, then $u_{r_n} \mid u_{r_{n-1}}$. Therefore $\gcd(u_{r_{n-1}}, u_{r_n}) = u_{r_n}$. But r_n, being the last non-zero remainder in Euclidian Algorithm for m and n, is equal to $\gcd(m, n)$. Thus $\gcd(u_m, u_n) = u_d$, where $d = gcd(m, n)$. □

Theorem 2.2.5. *In the Fibonacci sequence, $u_m \mid u_n$ if and only if $m \mid n$.*

Proof. If $u_m \mid u_n$, then $gcd(u_m, u_n) = u_m$. But we know that $gcd(u_m, u_n) = u_{gcd(m,n)}$. This implies that $gcd(m, n) = m$. Hence $m \mid n$. □

Theorem 2.2.6. *The sequence of ratio of successive Fibonacci numbers $u_{n+1} \mid u_n$ converges to golden ratio i.e.,*$\lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \Phi$.

Proof. We consider the sequence $r_n = \frac{u_{n+1}}{u_n}$, for $n = 1, 2, \cdots$. Then by definition of Fibonacci numbers, we have $r_n = \frac{u_{n+1}}{u_n} = \frac{u_n + u_{n-1}}{u_n} = 1 + \frac{1}{r_{n-1}}$.

When $n \to \infty$, then we can write the above equation in limits:

$$\begin{aligned} x &= 1 + \frac{1}{x}, \\ \Rightarrow x^2 &= 1 + x = x^2 - x - 1 = 0, \\ \Rightarrow x &= \frac{1+\sqrt{5}}{2} = \Phi. \end{aligned}$$

Hence

$$\lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \Phi.$$

□

2.3 Binet's Formulae for Fibonacci Numbers and Lucas Numbers

Problem 2.3.1. Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, so that α and β are both roots of the equation $x^2 = x + 1$. Then $u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$, for all $n \geq 1$.

Proof. When $n = 1$, $u_1 = 1$ which is true. Let us assume that it is true for $n = 1, 2, ..., n$. Then $u_{k-1} = \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}}$ and $u_k = \frac{\alpha^k - \beta^k}{\sqrt{5}}$. Adding these two equations, we get $u_k + u_{k-1} = \frac{\alpha^k}{\sqrt{5}}(1 + \alpha^{-1}) + \frac{\beta^k}{\sqrt{5}}(1 + \beta^{-1})$. Then $u_{k+1} = \frac{\alpha^{k+1} + \beta^{k+1}}{\sqrt{5}}$. □

Problem 2.3.2. Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, so that α and β are both roots of the equation $x^2 = x + 1$. Then $v_n = \alpha^n + \beta^n$, for all $n \geq 1$.

Proof. For $n = 1$, $v_1 = 1$. Then the theorem is true for $n = 1$. Let us assume that it is for $n = 1, 2, \cdots, k$. We have to prove that it is true for $n = k + 1$. Now

$$\begin{aligned} v_k + v_{k-1} &= \alpha^k + \alpha^{k-1} + \beta^k + \beta^{k-1} \\ \Rightarrow v_{k+1} &= \alpha^k(1 + \alpha^{-1}) + \beta^k(1 + \beta^{-1}) \\ \Rightarrow v_{k+1} &= \alpha^k(1 + \alpha - 1) + \beta^k(1 + \beta - 1) \\ \Rightarrow v_{k+1} &= \alpha^{k+1} + \beta^{k+1}. \end{aligned}$$

□

2.4 Relation Between Fibonacci and Lucas Numbers

Theorem 2.4.1. $v_n = u_{n-1} + u_{n+1}$, *for* $n > 1$.

Proof. We know that

$$\begin{aligned} v_{k+1} &= v_k + v_{k-1} \\ &= (u_{k-1} + u_{k+1}) + (u_{k-2} + u_k) \\ &= (u_{k-1} + u_{k-2} + (u_k + u_{k+1}) \\ &= u_k + u_{k+1}. \end{aligned}$$

□

Theorem 2.4.2. *For all* $n \geq 1$, $u_{2n} = v_n u_n$.

Proof. Now

$$\begin{aligned} v_n u_n &= (\frac{\alpha^n - \beta^n}{\sqrt{5}})(\alpha^n + \beta^n) \\ v_n u_n &= \frac{1}{\sqrt{5}}(\alpha^{2n} - \beta^{2n}) \\ v_n u_n &= u_{2n}. \end{aligned}$$

□

2.5 Applications of Fibonacci Numbers

Proposition 2.5.1. *There is a connection between the Fibonacci numbers and the binomial coefficients.*

Proof. It is enough to prove that the sum of all numbers making up the $(n-2)th$ and the $(n-1)th$ diagonal of Pascal's triangle is equal to the sum of the numbers making up the nth diagonal. On the $(n-2)th$ diagonal, we have the numbers

$$c^0_{n-3}, c^1_{n-4}, c^2_{n-5}, \cdots$$

and on the $(n-1)th$ diagonal the numbers

$$c_{n-2}^0, c_{n-3}^1, c_{n-4}^2, \cdots .$$

The sum of all these numbers can be written as

$$c_{n-2}^0 + (c_{n-3}^0 + c_{n-3}^1) + (c_{n-4}^1 + c_{n-4}^2) + \cdots$$

But for the binomial coefficients

$$c_{n-2}^0 = c_{n-1}^0 = 1$$

and

$$\begin{aligned} c_k^i + c_k^{i+1} &= \frac{k(k-1)\cdots(k-i+1)}{1.2\cdots i} + \frac{k(k-1)\cdots(k-i+1)(k-i)}{1.2\cdots i\cdots(i+1)} \\ &= \frac{k(k-1)\cdots(k-i+1)}{1.2\cdots i}(1+\frac{k-i}{i+1}) \\ &= \frac{k(k-1)\cdots(k-i+1)}{1.2\cdots i}(\frac{i+1+k-i}{i+1}) \\ &= \frac{(k+1)k(k-1)\cdots(k-i+1)}{1.2\cdots i\cdots(i+1)} \\ &= c_{k+1}^{i+1} \end{aligned}$$

. Hence,

$$c_{n-2}^0 + (c_{n-3}^0 + c_{n-3}^1) + (c_{n-4}^1 + c_{n-4}^2) + \cdots = c_{n-1}^0 + c_{n-2}^1 + c_{n-3}^2 + \cdots$$

□

2.6 Fibonacci numbers can be used to approximately convert from miles to kilometers and back.

Fibonacci numbers have a property that the ratio of two consecutive numbers tends to the Golden ratio as numbers get bigger and bigger. If we take two consecutive Fibonacci numbers,u_{n+1} and u_n, we know that their ratio, $\frac{u_{n+1}}{u_n}$ is approximately 1.618. Since the ratio is also almost the same as kilometers per mile, we can write $\frac{u_{n+1}}{u_n} = \frac{[mile]}{[km]}$. Then $u_n[mile] = u_{n+1}[km]$.

2.7 Fibonacci numbers in nature

The Fibonacci numbers really appear in nature, in some plants branch in such a way that they always have a Fibonacci number of growing points. Flowers often have a Fibonacci number of petals, daisies can have $34, 55$ or even as many as 89 petals.

CHAPTER 3

Cryptography

3.1 Cryptography

Cryptography is the science of writing in secret codes. A cryptographic system is any computer system that involves cryptography.

Definition 3.1.1. (Plaintext) In cryptography, plaintext is ordinary readable text before being encrypted into ciphertext.

Definition 3.1.2. (Ciphertext) In cryptography, ciphertext is the result of the process of transforming plaintext using a cipher algorithm in order to make it unreadable to everyone except those how have the knowledge to decode it.

Definition 3.1.3. (Encryption) Encryption is the process of obscuring information to make it unreadable without special knowledge.

Definition 3.1.4. (Decryption) The process of reverting cipher text to its original plaintext is called decryption.

Definition 3.1.5. (Shift Cipher) Shift cipher is a simple substitution cipher, in which we get the encrypted text by replacing a letter with another.

We need the following properties for encyption process

1. Encryption and decryption should be fast.
2. Anyone may be able to see ciphertext but should not be to decrypt easily.
3. Integrability and Repudiability

   The receiver should be able to know that message is not tempered with and sender should not be able to deny the original message.

Private Key Cryptography: In private-key cryptography, the sender and the recipient of the message must agree on a common key.

It is secure but needs a lot of keys for communication with many people. For n people, we need $\begin{pmatrix} n \\ 2 \end{pmatrix}$. It is a big problem to mange if n is large.

Public Key Cryptosystem: A cryptographic system that uses two keys - a public key known to everyone and a private or secret key known only to the recipient of the message. Public-key algorithms are asymmetric algorithms and are based on the use of two different keys, instead of just one. In public-key cryptography, the two keys are called the private key and the public key Private key: This key must be know only by its owner.

Definition 3.1.6. (Public key) It is the key known to everyone.

3.2 The RSA Public Key System

Definition 3.2.1. (A trapdoor function) A trapdoor function is a computable function whose inverse can be computed in a reasonable amount of time only if a amount of additional information is known.

3.3 The mathematics of the RSA System

The public key process used by the RSA(Rivest-Shamir-Adleman) method is defined by two numbers, e and N, which are used in the function:
$C \equiv M^e(modN)$.

If M is a message, then C is the encrypted message, say $M^{'}$. To make C a trapdoor function, N, is chosen to be the product of two large primes, p and q . For the private key process, a number d is needed such that $ed \equiv 1\Phi(N)$.

The Euler totient function of N, denoted $\Phi(N)$ is the number of numbers less than N which are relatively prime to N. If $N = pq$ where p and q are different primes, then $\Phi(N) = (p-1)(q-1)$.

If e is any number relatively prime to $\Phi(N)$ then by the extended Euclidean algorithm, a number d can be found such that $ed = k\Phi(N) + 1$, for some integer k. This implies $ed \equiv 1(mod\Phi(N)$.

When the public key process is applied to a number M, we obtain $(M^e modN)^d = M^{ed}(modN)$.

If the private key process is applied to M followed by the public key process, we obtain the same expression, $M^{ed}(modN)$. Then $M^{ed} = M^{k\Phi(N)+1} = (M^{\Phi(N)})^k \times M$.

The RSA method works because, if M is relatively prime to N, then $M^{\Phi(N)}(modN)$ is 1, by a well-known theorem of Euler. Hence, if M is less than N, $M^{ed} = M^{k\Phi(N)+1} = (M^{\Phi(N)})^k \times M = M(modN)$.

3.4 The LUC Public Key System

It is based on a different trapdoor function from the RSA which is defined by Lucas sequence.

Lucas Sequence:

Let $\{T_n\}$ be Lucas sequence satisfying the second-order recurrence relation

$$T_n = PT_{n-1} - QT_{n-2} \tag{3.1}$$

where $gcd(P, Q) = 1$ and $P, Q \in \mathbb{Z}$. Let α and β be the roots of the characteristic polynomial equation $x^2 - Px + Q = 0$. If c_1 and c_2 are any numbers, then the sequence $\{c_1\alpha^n + c_2\beta^n\}$ has the property that
$P(c_1\alpha^{n-1} + c_2\beta^{n-1}) - Q(c_1\alpha^{n-2} + c_2\beta^{n-2}) = c_1\alpha^{n-2}(P\alpha - Q) + c_2\beta^{n-2}(P\beta - Q) = c_1\alpha^{n-2}(\alpha^2) + c_2\beta^{n-2}(\beta^2) = c_1\alpha^n + c_2\beta^n$.

So this sequence satisfies the second-order linear (3.1) and any sequence $\{T_n\}$ satisfying (3.1) must be of the form $\{c_1\alpha^n + c_2\beta^n\}$, $T_0 = c_1 + c_2$, $T_1 = c_1\alpha + c_2\beta$.

If T_0 and T_1 are integers, then by (3.1) all the terms in the sequence will

be integers, even though α, β, c_1 and c_2 are not integers, and may not even be real.

There are two particular solutions of the general $second - order$ linear recurrence relation. They are denoted by $\{U_n\}$ and $\{V_n\}$, and are defined by $U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ where $(c_1 = \frac{1}{\alpha-\beta} = -c_2)$, and $V_n(P,Q) = \alpha^n + \beta^n$ where $(c_1 = 1 = c_2)$.

These will both be sequences of integers, since we have $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = P$.

3.5 Lucas Sequence Relationships

Since α and β are roots of $x^2 - Px + Q = 0$, then $\alpha + \beta = P$ and $\alpha\beta = Q$ and $D = P^2 - 4Q = (\alpha - \beta)^2$.
Now we have the following relations

1. $V_n^2 - 2Q^n = V_{2n}$

Proof. $V_n^2 - 2Q^n = (\alpha^n + \beta^n)^2 - 2(\alpha\beta)^n = \alpha^{2n} + \beta^{2n} = V_{2n}$. □

2. $PV_n^2 - QV_nV_{n-1} - PQ^n = V_{2n+1}$

Proof. $PV_n^2 - QV_nV_{n-1} - PQ_n = (\alpha+\beta)(\alpha^n+\beta^n)^2 - \alpha\beta(\alpha^n\beta^n)(\alpha^{n-1}+\beta^{n-1}) - (\alpha+\beta)(\alpha\beta)^n = \alpha^{2n+1} + \beta^{2n+1}$ □

3. $V_n^2 = DU_n^2 + 4Q^n$

Proof. $DU_n^2 + 4Q^n = (\alpha - \beta)^2(\frac{\alpha^n - \beta^n}{\alpha - \beta})^2 + 4(\alpha\beta)^n = (\alpha^n - \beta^n)^2 + 4(\alpha\beta)^n = (\alpha^n - \beta^n)^2$ □

4. $2V_{n+m} = V_nV_m + DU_nU_m$

Proof. $V_nV_m + DU_nU_m = (\alpha^n + \beta^n)(\alpha^m + \beta^m) + (\alpha - \beta)^2(\frac{\alpha^n - \beta^n}{\alpha - \beta})(\frac{\alpha^m - \beta^m}{\alpha - \beta}) = 2(\alpha^{n+m} + \beta^{n+m}) = 2V_{n+m}$ □

5. $2Q^mV_{n-m} = V_nV_m - DU_nU_m$.

Proof.

$$L.H.S = V_nV_m - DU_nU_m = (\alpha^n+\beta^n)(\alpha^m+\beta^m - (\alpha-\beta)^2(\frac{\alpha^n-\beta^n}{\alpha-\beta})(\frac{\alpha^m-\beta^m}{\alpha-\beta}) = 2(\alpha^n\beta^m+\beta^n\alpha^m)$$

and

$$R.H.S = 2Q^mV_{n-m} = 2(\alpha\beta)^m(\alpha^{n-m}+\beta^{n-m}) = 2(\alpha^n\beta^m+\beta^n\alpha^m).$$

Thus L.H.S=R.H.S. □

We consider the linear recurrence relation created by using $V_k(P,Q)$ for P and Q^k for Q. Then $T_n = V_k(P,Q)T_{n-1} - Q^kT_{n-2}$.

The roots of the corresponding quadratic equation be α_1 and β_1. Then $\alpha_1+\beta_1 = V_k(P,Q) = \alpha^k+\beta^k$ and $\alpha_1\beta_1 = Q^k = \alpha^k\beta^k$, so $\alpha_1 = \alpha^k$ and $\beta_1 = \beta^k$. This implies that $V_n(V_k(P,Q),Q^k) = (\alpha^k)^n + (\beta^k)^n = \alpha^{nk}+\beta^{nk} = V_{nk}(P,Q)$.

If $Q = 1$,then $V_{nk}(P,1) = V_n(V_k(P,1),1)$

Definition 3.5.1. (Legendre symbol)

$(\frac{D}{p}) = 0$ if $p \mid D$, otherwise
$(\frac{D}{p}) = 1$, if there is a number x such that $D \equiv x^2(modp)$,
$(\frac{D}{p}) = -1$ if no such number exists.

If p is an odd prime number which does not divide Q or D, and ε is $(\frac{D}{p})$ then $U_{k(p-\varepsilon)}(P,Q) \equiv 0(modp)$ for any integer k, and also $V_{k(p-\varepsilon)}(P,Q) \equiv 2Q^{\frac{k(1-\varepsilon)}{2}}(modp)$.

Now the Lehmer totient function of $N = pq$,where p and q are different odd primes, is $T(N) = ((p-(\frac{D}{p})(q-\frac{D}{q}))$. We define $S(N) = lcm((p-(\frac{D}{p}))(q-(\frac{D}{q}))$.

Since $S(N)$ is a product of both $(p-(\frac{D}{p})$ and $(q-(\frac{D}{q})$ then $U_{kS(N)}(M,1) \equiv 0(modN)$ for any integer k and $V_{kS(N)}(M,1) \equiv 2(modN)$ for any integer k.

We have $V_e^2(P,1) - 4 = DU_e^2(P,1)$. Then $(\frac{D}{p}) = (\frac{DU_e^2(P,1}{p}) = (\frac{P^2-4}{p}) = (\frac{V_e^2(P,1)}{p})$.

3.6 The New Public Key System, LUC

Suppose N and e are two chosen numbers, with N the product of two different odd primes, p and q . The number e must be chosen so it is relatively prime to $(p-1)(q-1)(p+1)(q+1)$. Let M be a message which is less than N and relatively prime to N. We define $L \equiv V_e(M,1))(modN)$ where V_e is a Lucas function. This gives an encrypted message say M_1. To define the matching private key process, we need a number d such that $de \equiv 1(mod(S(N))$, where $S(N) = lcm((p-(\frac{D}{p}))(q-(\frac{D}{q}))$, where $D = M_1^2-4$ and $(\frac{D}{p})$ and $(\frac{D}{q})$ are Legendre symbols of p and q. We can assume that D is relatively prime to N.

The number d can be found by the extended Euclidean algorithm such that $ed = kS(N)+1$, for some integer k. Then we get
$V_d(V_e(M,1)) = V_{de}(M,1) = V_{kS(N)+1}(M,1) = MV_{kS(N)}(M,1)-V_{kS(N)-1}(M,1) = MV_{kS(N)}(M,1)-(\frac{1}{2})(V_{kS(N)}(M,1)V_1(M,1)-DU_{kS(N)}(M,1)U_1(M,1)) \equiv (2M-(\frac{1}{2})(2M-0))(modN) = M$. Since $U_{kS(N)}(M,1) \equiv 0(modN)$ for any integer k and $V_{kS(N)}(M,1) \equiv 2(modN)$ for any integer k.

BIBLIOGRAPHY

1. Apostol T.M., "*Introduction to Analytic Number Theory*" , Spinger International Student Edition,Narosa Publishing House (1989).

2. Burton D.M."*Elementary Number Theory*" , Tata McGraw-Hill Edition, Sixth Edition (2006).

3. Hardy G.H.,Wright E.M."*An Introduction to the Theory of Numbers*" Oxford Science Publications, Fifth Edition (1979).

4. Kumundury R,Romero C., "*Number Theory with Computer Application*" Prentice hall (1998).

5. Mapa S.K."*Higher Algebra*" , Milinda De for Levant Books, Sixth Revised Edition (2004).

6. Thomas Koshy, "*Elementary Number Theory with Applications*", Elsevier, second edition (2007).

7. N.N. Vorobev, "*Fibonacci Numbers*", Moscow (1984) (In Russian).