AN ABSTRACT OF THE THESIS OF

M.Mizanur Rahman (name of student) for the Master of Science (Degree)

in Mathematics (Major) Presented on July 1992 (date)

Title : Pseudoprime Numbers

Abstract Approved: Essam Abbeen

Our objective in this paper is to study pseudoprime numbers. In the course of its development, we discuss pseudoprime to the base 2, and subsequently generalize it to any base a. In chapter 1, we provide readers with a short account of the necessary background from elementary number theory that is needed throughout the paper. We answer questions regarding the number of pseudoprimes, recognition of pseudoprimes and the distribution of pseudoprimes for both the base 2 and a. Necessary and sufficient conditions for an integer to be pseudoprime is established and several sequences generating infinitely many pseudoprimes are given. We discuss some special kinds of pseudoprimes including absolute pseudoprimes(or Carmichael numbers), Euler pseudoprimes, and strong pseudoprimes. We conclude the paper with a brief discussion of two probabilistic primality tests, one based on the concept of Euler pseudoprime and the other on strong pseudoprimes.

PSEUDOPRIME NUMBERS

A Thesis

Presented to

The Division of

Mathematics and Computer Science

EMPORIA STATE UNIVERSITY

In Partial Fulfilment

of the Requirements for the Degree

Master of Science

---

by

M.Mizanur Rahman

July 1992

Essam Abattem

Approved for the major Division

Faye M. Vowell

Approved for the Graduate Council

ACKNOWLEDGEMENTS

I wish to express my deep sense of gratitude to Dr. Essam Abotteen, whose continuous support and patience has made this paper possible. I also would like to extend my thanks to the other members of my committee for their encouragement and support.

I would also like to express my thanks to Dr. Linda Fosnaugh for her help in translating some original articles from French into English that I incorporated in this paper, and for her role as a member in my committee.

Table of Contents

Chapter 1

INTRODUCTION

The object of this introductory chapter is to provide readers with a short account of the concepts from elementary number theory that we need in later chapters. All the results in this chapter are given without proof. The proofs can be found in any elementary number theory books, such as [3], [25].

1.1 DEFINITIONS

1. An integer $p > 1$ is called a **prime** number, or simply a prime, if its only positive divisors are 1 and p.

2. An integer n which is not a prime is called a **composite number**.

3. If a and b are integers, we say that a **divides** 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 **greatest common divisor** of a and b, denoted by gcd(a, b), is the positive integer d satisfying

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

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

5. The **least common multiple** of two non zero 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 $m \leq c$.

6. Let n be a fixed positive integer. Two integers a and b are said to be **congruent** modulo n, symbolized by $a \equiv b \pmod{n}$, if n divides the difference a-b. That is if $a-b = kn$ for some integer k.

7. Let $n > 1$ and $\gcd(a, n) = 1$. The **order** of a modulo n (in older terminology: The exponent to which a belongs modulo n) is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. We denote the order of a modulo n by $\text{ord}_n(a)$.

8. **Euler's ϕ Function.** For $n \geq 1$, $\phi(n)$ denotes the number of positive integers not exceeding n that are relatively prime to n.

9. If $\gcd(a,n) = 1$ and a is of order $\phi(n)$ modulo n, then a is called **primitive root** of n.

10. Let p be an odd prime and a an integer such that $\gcd(a, p) = 1$. If the congruence $x^2 \equiv a \pmod{p}$ has a solution, then a is said to be a **quadratic residue** of p. Otherwise a is called a quadratic nonresidue of p

11. Let p be an odd prime and $\gcd(a,p) = 1$, the Legendre symbol

$\left(\frac{a}{p}\right)$ is defined by

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

12. Let a and b > 1 be relatively prime integers, with b odd. If $b = p_1 p_2 \ldots p_r$ is the decomposition of b into odd primes (not necessarily distinct) then the **Jacobi symbol** is defined by

$$\left[\frac{a}{b}\right] = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$$

1.2 THEOREMS (WITHOUT PROOFS)

Theorem 1.1. If a, b, c, d, k and m are integers where m > 0, k > 0, such that $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then

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

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

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

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

Theorem 1.2. 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 1.3. 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

$a \equiv b \pmod{\text{lcm}[m_1, m_2, \ldots, m_k]}$.

Theorem 1.4 (Fermat's Little Theorem). If p is prime and a is a positive integer with $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary. If p is a prime and a is positive integer, then $a^p \equiv a \pmod{p}$.

Theorem 1.5 (Euler's Theorem). If m is a positive integer with $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Theorem 1.6. If a and n are relatively prime integers with $n > 0$, then the positive integer x is a solution of the congruence $a^x \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid x$.

Theorem 1.7 (Euler's Criterion). Let p be an odd prime and let a be a positive integer not divisible by p. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Theorem 1.8. Let n be an odd positive integer and let a and b be integers relative prime to n, then

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

(2) $\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right]\left[\frac{b}{n}\right]$

(3) $\left[-\frac{1}{n}\right] = (-1)^{\frac{(n-1)}{2}}$

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

Theorem 1.9 (The Chinese Remainder Theorem). Let $m_1, m_2, \ldots m_r$ 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 $M = m_1 m_2 \ldots m_r$.

Theorem 1.10. If p is a prime and gcd(a,p) = 1, then the congruence $x^n \equiv a \pmod{p}$ has d solutions if $a^{(p-1)/(d)} \equiv 1 \pmod{p}$, where d = gcd(n,p-1) and no solution if $a^{(p-1)/(d)} \not\equiv 1 \pmod{p}$.

Chapter 2

PSEUDOPRIMES

Our objective in this chapter is to define pseudoprime numbers and investigate their properties. In number theory, it is quite natural when studying a set of numbers--in this case the set of pseudoprime numbers--to ask the following questions:

1. How many pseudoprime numbers are there?
2. How do you recognize whether a number is pseudoprime?
3. Are there functions (which are computable in practice) to produce some or all pseudoprime numbers?
4. How are the pseudoprime numbers distributed?

The discussion of these questions will be the main focus of this chapter.

2.1 BASIC DEFINITIONS AND EXAMPLES

According to **Fermat's** Little Theorem, if p is a prime, then for any positive integer a, $a^p \equiv a \pmod{p}$.

It was believed that nearly 25 centuries ago the ancient Chinese mathematicians discovered this theorem in the case a = 2, and they claimed that if an integer n > 1 satisfies the congruence

$2^n \equiv 2 \pmod{n}$, then n must be a prime [12]. Recently, **Mann-Keung Siu**, a Chinese mathematician who is deeply interested in the history of Chinese mathematics, believes this is a myth originated in **Jean's** paper [12]. He states it would be impossible for the ancient Chinese mathematicians to have made such a claim since they never formulated the concept of prime numbers [24].

An example disproving the claim that if n satisfies the congruence $2^n \equiv 2 \pmod{n}$, then n is a prime was not discovered until 1819, when **Sarrus** [8; page 92] showed that $2^{341} \equiv 2 \pmod{341}$, yet $341 = 11*31$ is a composite number. It is not hard to see why the above congruence holds. By **Fermat's** Little Theorem we see that $2^{10} \equiv 1 \pmod{11}$ and hence
$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$. Also $32 \equiv 1 \pmod{31}$. Thus $(32)^{68} = (2^5)^{68} = 2^{340} \equiv 1 \pmod{31}$. Hence it follows that $2^{340} \equiv 1 \pmod{11.31}$, and by multiplying both sides of this congruence by 2, we obtain $2^{341} \equiv 2 \pmod{341}$. In fact $n = 341$ is the smallest composite positive integer that satisfies $2^n \equiv 2 \pmod{n}$.

Definition 2.1. A positive integer n is called a **pseudoprime** if n is composite and $2^n \equiv 2 \pmod{n}$.

Note that if n is an odd composite positive integer then n is a pseudoprime if and only if $2^{n-1} \equiv 1 \pmod{n}$. The pseudoprime numbers are sometimes called "**almost prime**

numbers" and they are also called **poulet numbers.** **P.Poulet** [22], has tabulated all the odd pseudoprimes below 10^8.

Example. n = 561, n = 161038 are pseudoprimes.

To show that 561 is a pseudoprime, by **Fermat's** Little Theorem, we have

$$2^2 \equiv 1 \pmod 3$$

$$2^{10} \equiv 1 \pmod{11}$$

$$2^{16} \equiv 1 \pmod{17}.$$

Hence, $2^{561-1} = (2^2)^{280} \equiv 1 \pmod 3$ . . . (1)

$2^{561-1} = (2^{10})^{56} \equiv 1 \pmod{11}$ . . . (2)

$2^{561-1} = (2^{16})^{35} \equiv 1 \pmod{17}$ . . . (3)

Now combining (1), (2),and (3), we have $2^{560} \equiv 1 \pmod{561}$. thus 561 is a pseudoprime.

To show that n = 161038 is a pseudoprime, we have n = 2*73*1103

$$n-1 = 3^2*29*617$$

$$2^9-1 = 7*73,\ 2^{29}-1 = 233*1103*2089.$$

Since $9 \mid n-1$ and $29 \mid n-1$, by Lemma 2.1 below, $2^9-1 \mid 2^{n-1}-1$ and $2^{29}-1 \mid 2^{n-1}-1$.

Since $73 \mid 2^9-1$ and $1103 \mid 2^{29}-1$, we conclude $2^{n-1}-1$ is divisible by 73 and 1103. Hence, the number 2^n-2 is divisible by 73 and 1103. But the number 2^n-2 is an even number, and hence $2 \mid 2^n-2$. Therefore $n \mid 2^n-2$ and thus n is a pseudoprime.

Note (1). In fact, for any positive integer a relatively prime to 561, $a^{561} \equiv a \pmod{561}$ holds. Composite numbers n that satisfy $a^n \equiv a \pmod{n}$ for all positive integers a with gcd(a,n) = 1 are called **absolute pseudoprimes** or **Carmichael numbers** and are discussed in Chapter 4.

Note (2). n = 161038 is the smallest even pseudoprime number, discovered by **D.H.Lehmer** in 1950. Later in this chapter we will show that there exist infinitely many even pseudoprimes.

The following lemma will be used throughout the paper.

Lemma 2.1. If d and n are positive integers such that d divides n, then for any integer a, a^d-1 divides a^n-1.

Proof: Since $d|n$, there is a positive integer t with dt = n. Consider the identity $(x^n -1) =(x-1)\ (x^{n-1} + x^{n-2} + \ldots + 1)$. Putting n = dt, and x = a, we obtain $((a^d)^t-1) = (a^d-1)(a^{d(t-1)} + a^{d(t-2)} + \ldots +a^d + 1)$

or $(a^n-1) = (a^d-1)(a^{d(t-1)} + a^{d(t-2)} + \ldots a^d +1)$, consequently $a^d-1|a^n-1$. This completes the proof.

Theorem 2.2. Every composite **Fermat** number $F_m = 2^{2^m}+1$, is a pseudoprime.

Proof: First we prove that $2^{m+1} \mid 2^{2^m}$ by mathematical induction on m. For m = 1, we have $\frac{2^2}{2^2} = 1$, and the statement is true for m = 1. Let us assume that the statement is true for some m = k ≥ 1, i.e., $2^{k+1} \mid 2^{2^k}$. We need to show that the statement is true for k+1. We have $\frac{2^{2^{k+1}}}{2^{(k+1)+1}} = \frac{(2^2)^k(2^{2^1})}{(2^{k+1})2^1}$. Since $2^{k+1} \mid 2^{2^k}$ the statement $2^{k+2} \mid 2^{2^{k+1}}$ is true.

Hence $2^{m+1} \mid 2^{2^m}$ for every m ≥ 1. Since $2^{m+1} \mid 2^{2^m}$, by Lemma 2.1, it follows that $2^{2^{m+1}}-1 \mid 2^{2^{2^m}}-1$ or $2^{2^{m+1}}-1 \mid 2^{F_m-1}-1$. But $F_m \mid 2^{2^{m+1}}-1$, since $2^{2^{m+1}}-1 = (2^{2^m}+1)(2^{2^m}-1) = F_m(2^{2^m}-1)$.

Hence $2^{F_m-1} \equiv 1 \pmod{F_m}$.

Hence $F_m = 2^{2^m}+1$ is a pseudoprime. This completes the proof.

Later on in this chapter we are going to use Theorem 2.2 to establish the existence of infinitely many pseudoprimes.

Theorem 2.3. Let n be a composite number. Then n is a pseudoprime if and only if $\text{ord}_n(2)$ divides n-1.

Proof: Assume $\text{ord}_n(2) \mid n-1$. Then $n-1 = k.\text{ord}_n(2)$ for some positive integer k. Hence $2^{n-1} = 2^{(k\, ord_n(2))^k} = (2^{ord_n(2)})^k \equiv 1^k \equiv 1$

(mod n). Hence n is a pseudoprime.

Assume that n is a pseudoprime. Hence by the Division Algorithm, there exist unique integers q and r such that (n-1) = q $ord_n(2)$ + r, where $0 \leq r < ord_n(2)$. From this equation, we have $2^{n-1} = 2^{q\, ord_n(2)+r} = 2^{q\, ord_n(2)}.2^r \equiv 2^r \pmod{n}$. Then $2^r \equiv 1 \pmod{n}$.
From the inequality $\phi \leq r < ord_n(2)$, we must have $r = \phi$, since by definition $y = ord_n(2)$ is the least positive integer such that $2^y \equiv 1 \pmod{n}$. Thus we have $n-1 = q\, ord_n(2)$. Therefore $ord_n(2) \mid n-1$. This completes the proof.

Lehmer [15] gave the following necessary and sufficient conditions for an integer n that is the product of two distinct odd primes to be a pseudoprime.

Theorem 2.4. An integer n = pq, where p and q are distinct odd primes, is a pseudoprime if and only if $e_q = ord_q(2)$ divides p-1 and $e_p = ord_p(2)$ divides q-1.

Proof: Let us assume that the composite number n = pq, where p and q are odd primes is a pseudoprime. From the definition of pseudoprime we have $2^{pq} \equiv 2 \pmod{pq}$. Since p is a prime divisor of pq, we have $2^{pq} \equiv 2 \pmod{p}$ .. .(1). Again since p is a prime, from **Fermat's** Little Theorem, we have $2^p \equiv 2 \pmod{P}$, hence $(2^p)^q \equiv 2^q \pmod{P}$ or $2^{pq} \equiv 2^q \pmod{p}$...(2). By subtracting (1) from (2), we obtain $\phi \equiv$

$2^q - 2 \pmod p$ or $2^q \equiv 2 \pmod p$ or $2^{q-1} \equiv 1 \pmod p$. Thus $ord_p(2) \mid q-1$. Similarly it can be shown that $ord_q(2) \mid p-1$.

Assume that $ord_p(2) \mid q-1$ and $ord_q(2) \mid p-1$. Then we have $2^{q-1} \equiv 1 \pmod p$ and $2^{p-1} \equiv 1 \pmod q$. Thus We have $2^{q-1}2^{p-1} \equiv 2^{p-1} \equiv 1 \pmod p$ and $2^{p-1} \cdot 2^{q-1} \equiv 2^{q-1} \equiv 1 \pmod q$. Thus $2^{q-1} \cdot 2^{p-1} \equiv 1 \pmod{pq}$.

From **Euler's** Theorem, $2^{\phi(pq)} \equiv 1 \pmod{pq}$, multiplying both sides by 2 implies

$$2^{\phi(pq)+1} \equiv 2 \pmod{pq}$$

$$\text{or } 2^{(p-1)(q-1)+1} \equiv 2 \pmod{pq}$$

$$\text{or } 2^{pq-p-q+2} \equiv 2 \pmod{pq}$$

$$\text{or } 2^{pq-(p-1)-(q-1)} \equiv 2 \pmod{pq}$$

$$\text{or } 2^{pq} \equiv 2 * 2^{p-1} * 2^{q-1} \pmod{pq}$$

$$\text{or } 2^{pq} \equiv 2*1*1 \equiv 2 \pmod{pq}.$$

Hence, n = pq is a pseudoprime. This completes the proof.

Example.

Using Theorem 2.4, let us see which of the following integers are pseudoprime : (a) 13*67, (b) 19*73, (c) 23*89, (d) 29*97.

(a) Let p = 13, q = 67,

$ord_p(2) = 12 \nmid (q-1) = 66$.

Hence, 13*67 is not a pseudoprime.

(b) Let p = 19, q = 73, $ord_p(2) = 18 \mid (q-1) = 72$

and $ord_q(2) = 9 \mid (p-1) = 18$.

Hence, 19*73 is a pseudoprime.

(c) Let p = 23, q = 89,

$ord_p(2) = 11 \mid (q-1) = 88$,

and $ord_q(2) = 11 \mid (p-1) = 22$.

Hence, 23*89 is a pseudoprime.

(d) Let p = 29, q = 97,

$ord_p(2) = 28 \nmid (q-1) = 96$, thus 29*97 is not a pseudoprime.

Theorem 2.5. If n = pqr, where p, q, and r are distinct odd primes, is a pseudoprime then the least common multiple of $e_p = ord_p(2)$ and $e_q = ord_q(2)$ divides r(p+q-1)-1.

Proof: By **Fermat's** Little Theorem, $2^p \equiv 2 \pmod p$. Hence $(2^p)^{qr} \equiv 2^{qr} \pmod p$ or $2^{pqr} \equiv 2^{qr} \pmod p$. But by the assumption, $2^{pqr} \equiv 2 \pmod{pqr}$, hence $pqr \mid 2^{pqr}-2$ or $2^{pqr}-2 = pqrk$... (1) for some k, hence $p \mid 2^{pqr}-2^{rq}$ or $2^{pqr}-2^{rq} = pt$... (2) for some t. From (1), $2^{pqr} = pqrk+2$. From (2), $2^{pqr} = pt+2^{rq}$. Thus $2^{rq} + pt = pqrk+2$ or $2^{rq}-2 = pqrk-pt$, hence $p \mid (2^{rq}-2)$, and this implies $rq-1 \equiv o \pmod{e_p}$ also we have $p-1 \equiv 0 \pmod{e_p}$ and hence $r(p-1) \equiv o \pmod{e_p}$. By adding $rq-1 \equiv o \pmod{e_p}$ to the last congruence, we obtain $pr+rq-r-1 \equiv o \pmod{e_p}$ or $e_p \mid r(p+q-1)-1$. Similarly it can be shown that $e_q \mid r(p+q-1)-1$. Thus $lcm(e_p, e_q) \mid r(p+q-1)-1$. This completes the proof.

Theorem 2.6. If p and q are primes such that $2^p \equiv 2 \pmod{pq}$ and $2^q \equiv 2 \pmod{pq}$, then pq is a pseudoprime.

Proof: We have $2^p \equiv 2 \pmod{pq}$.

$$(2^p)^q \equiv 2^q \pmod{pq}.$$

Thus $2^{pq} \equiv 2 \pmod{pq}$, since by assumption $2^q \equiv 2 \pmod{pq}$. Hence, pq is a pseudoprime. This completes the proof.

Theorem 2.7 (Rotkiewcz [26]). The number n = pq, where p and q are distinct primes is a pseudoprime if and only if the number $M_pM_q = (2^p-1)(2^q-1)$ is a pseudoprime.

Proof: Assume that n = pq is a pseudoprime. First we are going to show that p and q must be odd primes. Without loss of generality assume that p = 2. Since n = 2q is a pseudoprime, then

$2^{2q} \equiv 2 \pmod{2q}$. But $p = 2 < q$, hence $\gcd(2, q) = 1$, and

$$2^{2q-1} \equiv 1 \pmod{q} \quad ...(1)$$

From **Fermat's** Little Theorem, we have

$$2^{q-1} \equiv 1 \pmod{q} \text{ and } 2^{2(q-1)} \equiv 1 \pmod{q} \quad ... \quad (2).$$

Note that $2^{2q-1}-1 = 2^{2(q-1)}*2-1$.

From (1) and (2), $q|(2^{2q-1}-1) = (2^{2(q-1)}*2-1)$ and $q|(2^{2(q-1)}-1)$. Hence, $q|2(2^{2(q-1)})-1) - (2^{2q-1}-1)$ or $q|(2*2^{2(q-1)}-1) - (2*2^{2q-1}-1)-1$, implies $q|(-1)$ a contradiction.

Thus p is an odd prime, and since $q > p$, q is also odd prime.

Now, we have

$2^{pq-1}-1 = 2^{(p-1)q}.2^{q-1}-1 \equiv 2^{q-1}-1 \pmod{p}$ and since

$2^{pq-1}-1 \equiv 0 \pmod{pq}$, then

$2^{pq-1}-1 \equiv 0 \pmod{p}$. Thus we have $2^{q-1} \equiv 0 \pmod{p}$.

From **Fermat's** Little Theorem,

$2^{q-1}-1 \equiv 0 \pmod{q}$. Therefore we have

$2^{q-1}-1 \equiv 0 \pmod{pq}$ and

$2^{q}-2 \equiv 0 \pmod{pq}$.

Similarly it can be shown that $2^{p}-2 \equiv 0 \pmod{pq}$.

Thus $2^{p}-1 \equiv 1 \pmod{pq}$ and $2^{q}-1 \equiv 1 \pmod{pq}$,

from which we get $M_pM_q \equiv 1 \pmod{pq}$. Now since $\gcd(2^{p}-1,2^{q}-1) = 2^{\gcd(p,q)}-1 = 1$, one has

$M_pM_q = (2^{p}-1)(2^{q}-1) \mid (2^{pq}-1) \mid (2^{M_pM_q-1}-1)$.

Hence M_pM_q is a pseudoprime.

Suppose now that M_pM_q is a pseudoprime. One therefore has

$$(2^{p}-1)(2^{q}-1) \mid (2^{M_pM_q-1}-1) \quad \ldots (3)$$

Since $\gcd(2^{p}-1,2^{q}-1) = 1$, it follows from (3) that

$$2^{p}-1 \mid (2^{M_pM_q-1}-1),$$

and $(2^{q}-1) \mid (2^{M_pM_q-1}-1)$. Hence $p \mid (M_pM_q-1)$ and $q \mid (M_pM_q-1)$.

Therefore

$$pq \mid (M_pM_q-1).$$

From **Fermat's** Little Theorem,

$$2^{p}-1 \equiv 1 \pmod{p}.$$

Multiplying both sides of this congruence relation by 2^q-1, we obtain

$$(2^p-1)(2^q-1) \equiv (2^q-1) \pmod{p}$$

and $(2^p-1)(2^q-1)-1 \equiv 2^q-2 \pmod{p}$.

Hence, $p \mid (2^q-2)$ . . . (4).

Similarly $q \mid (2^p-2)$ . . . (5)

Thus by Theorem 2.4, it follows that n = pq is a pseudoprime. This completes the proof.

Theorem 2.8. Let p be a prime greater than 3, then

$$n = \frac{2^{2p}-1}{3} \text{ is a pseudoprime.}$$

Proof: $n-1 = \frac{2^{2p}-1}{3} - 1 = \frac{2^{2p}-4}{3} = \frac{4*2^{2p-2}-4}{3} = \frac{4*(2^{p-1}+1)(2^{p-1}-1)}{3}$

By **Fermat's** Little Theorem, $2^{p-1} \equiv 1 \pmod{p}$. Hence $p \mid 2^{p-1}-1$.

Claim: $3 \mid (2^{p-1}-1)$.

Since p is odd, p-1 is even, hence p-1 = 2k, for some integer k.

Thus $2^{p-1}-1 = 2^{2k}-1 = 4^k-1$.

Now we proceed by induction on k to show that $3 \mid (4^k-1)$ for any integer $k \geq 1$. For k = 1, clearly $3 \mid (4^1-1)$. Assume $3 \mid (4^k-1)$ for some integer $k \geq 1$. Then $4^{k+1}-1 = 4*4^k-1 = 4*4^k-4+3 = 4(4^k-1)+3$. Since $3 \mid (4^k-1)$ by inductive hypothesis, then $3 \mid (4(4^k-1)+3)$. Thus $3 \mid (4^k-1)$. For any integer $k \geq 1$. Thus $3 \mid (2^{p-1}-1)$ for any $p > 3$. Since gcd(3,p) = 1, it

follows that $3p \mid (2^{p-1}-1)$. (This follows from corollary 2, p. 31 of [3]. Thus $2^{p-1}-1 = 3pt$, for some integer t.

Now $n-1 = \frac{4(2^{p-1}+1)(2^{p-1}-1)}{3} = \frac{4(2^{p-1}+1)}{3} * 3pt = (2p)(2t(2^{p-1}+1)) =$

$2pm$, where $m = 2t(2^{p-1}+1)$. Thus $2^{n-1}-1 = 2^{2pm}-1 = (2^{2p})^m-1 =$

$(2^{2p}-1)(2^{2p(m-1)}+2^{2p(m-2)} +\ldots+1)$

$= 3n(2^{2p(m-1)}+ \ldots + 1)$, since $2^{2p}-1 = 3n$, by hypothesis.

Hence $2^{n-1} \equiv 1 \pmod{n}$. Moreover n is composite, since $n = \frac{2^{2p}-1}{3} = \frac{(2^p-1)(2^p+1)}{3}$. Thus n is a pseudoprime. This completes the proof.

Corollary. There are infinitely many pseudoprimes.

Proof: Theorem 2.8 implies for any prime $p > 3$, the integer $n = \frac{2^{2p}-1}{3}$ is a pseudoprime. Since there are infinitely many primes > 3, it suffices to show that two distinct primes $p > 3$ and $q > 3$ generate two different pseudoprimes. Assume $p \neq q$ and $\frac{2^{2p}-1}{3} = \frac{2^{2q}-1}{3}$ this implies $2^{2p} = 2^{2q}$ and hence, $p = q$, a contradiction. This completes the proof.

Clearly the sequence $(\frac{2^{2p}-1}{3}; p > 3$ is a prime) does not generate all the pseudoprime numbers. It does not even generate all odd pseudoprimes. For example, $n = 561$ is not

an element of this sequence, since for p = 5, n = 341, and for p = 7, n = 5461.

The question of whether there is a function f(n), defined for natural numbers n, which is computable in practice and generates the set of all pseudoprimes remains unsolved. Later in this chapter we will consider other sequences that generate infinitely many pseudoprimes.

2.2 HOW MANY PSEUDOPRIME NUMBERS ARE THERE?.

We have shown in Section 2.1 there are infinitely many pseudoprimes. The proof there was based on finding an infinite sequence of odd pseudoprimes. In this section we are going to discuss different ways of generating infinite sequences of pseudoprimes.

The first proof of the existence of infinitely many pseudoprimes was given in 1903 by **Malo** [18].

Lemma 2.9. If n is a pseudoprime then $n' = 2^n-1$ is also a pseudoprime that is larger than n.

Proof: Since n is a pseudoprime then n is composite, let n = rs with $1 < r \leq s < n$. n = rs implies $r|n$, using Lemma 2.1, we have $(2^r-1)|(2^n-1)$ or $(2^r-1)|n'$. Thus n' is composite. According to our hypothesis, $2^n \equiv 2 \pmod{n}$, and hence $2^n-2 = kn$ for some integer k.

Hence, $2^{n'-1} = 2^{2^n-2} = 2^{kn}$.

Thus $2^{n'-1}-1 = 2^{kn}-1 = (2^n)^k-1$

$= (2^n-1)\ (2^{n(k-1)} + 2^{n(k-2)} + \ . \ . \ .+ 2^n + 1)$

$= n'\ (2^{n(k-1)} + 2^{n(k-2)} + \ . \ . \ . + 2^n + 1)$

$\equiv 0 \pmod{n'}$.

Hence, $2^{n'} \equiv 2 \pmod{n'}$. So n' is a pseudoprime. This completes the proof.

Theorem 2.10. There are infinitely many pseudoprimes.

Proof: This theorem follows immediately from Lemma 2.9. Since we have shown that if n is odd pseudoprime, then $n' = 2^n-1$ is also odd pseudoprime larger than n.

Moreover, since there is at least one odd pseudoprime, e.g. $n_0 = 341$, we can construct infinitely many odd pseudoprimes by taking $n_0 = 341$ and $n_{k+1} = 2^{n_k}$ for k = 0, 1, 2, 3, ... Clearly these odd integers are all different and $n_0 < n_1 < n_2 \ . \ . \ . \ n_k < n_{k+1} < \ . \ . \ . \ .$ Thus the proof is complete.

In 1904, **Cipolla** [6] gave another proof of the existence of infinitely many pseudoprimes using the **Fermat**

numbers. First we need to establish some properties of **Fermat** numbers.

Lemma 2.11. For the **Fermat** numbers F_n and F_m where $m > n \geq 0$, $\gcd(F_m, F_n) = 1$.

Proof: Let $d = \gcd(F_m, F_n)$. Since **Fermat** numbers are odd integers, d must be odd. We have

$$F_m - 2 = 2^{2^m}+1-2$$

$$= 2^{2^m}-1$$

$$= 2^{2^{m+n-n}}-1$$

$$= (2^{2^n})^{2^{m-n}}-1 .$$

Setting $2^{2^n} = x$ and $2^{m-n} = k$.

$$\text{Hence, } \frac{F_m-2}{F_n} = \frac{(2^{2^n})^{2^{m-n}}-1}{2^{2^n}+1} = \frac{x^k-1}{x+1}$$

$$= \frac{(x+1)(x^{k-1}+\ldots-1)}{x+1}$$

$$= x^{k-1}-x^{k-2}+ \ldots -1.$$

Since $k > 1$, $x^{k-1}-x^{k-2} + \ldots -1$ is an integer, hence $F_n \mid (Fm-2)$. But $d = \gcd(F_n, F_m)$. Thus $d \mid F_n$ and $F_n \mid (F_m-2)$ implies $d \mid_m-2$. Also $d \mid F_m$. Hence, $d \mid (F_m-(F_m-2))$ or $d \mid 2$ thus $d = 1$, or 2. But d is odd, thus $d = 1$. This completes the proof.

Q is an odd integer. Hence $2^{n_1+1} | 2^{2^{n_k}} Q$ this implies $n_1+1 \leq 2^{n_k}$, thus $n_1 < 2^{n_k}$.

The converse follows by just reversing the above argument. This completes the proof.

Now we employ Theorem 2.13 and Theorem 2.2 to give another proof of the existence of infinitely many pseudoprimes.

Theorem 2.14. There are infinitely many pseudoprimes.

Proof: The number of composite **Fermat** numbers is either infinite or finite. (It is not known yet whether there exist infinitely many composite **Fermat** numbers or there is at least one **Fermat** number > F_4 that is prime). Thus there are two cases to consider.

Case (1). There are infinitely many composite **Fermat** numbers. In this case the proof follows from Theorem 2.2.

Case (2). There is only finitely many composite **Fermat** numbers. In this case it follows that, for a certain positive integers a > 1, all the numbers F_n, n = a, a+1, a+2 . . . are prime. Let $N = F_{i+1} \cdot F_i$, where i > a.

Now, note that $2^i > i+1$ for every i > 1. (This is a simple mathematical induction proof). Thus by Theorem 2.13,

$N = F_{i+1} F_i$ is a pseudoprime for every i> a. This completes the proof.

So far we have shown the existence of infinitely many odd pseuodprimes by finding sequences that generate such numbers. The natural question one may ask is: Are there any even pseudoprime numbers? The answer to this question was given by **Lehmer** in 1950. He found that n = 161038 is a pseudoprime. It was by no means easy to find this number. However, the proof that n = 161038 is a pseudoprime is quite elementary and simple. In fact, the necessary computation to show that n = 161038 is a pseudoprime was given at the beginning of this chapter. One year after **Lehmer** found the first even pseudoprime number, **Beeger** [2] showed that there exist infinitely many even pseudoprime numbers. Our objective now is to prove this result.

Lemma 2.15. If m is a pseuodprime then m is not divisible by 4.

Proof: Assume the contrary, that is $4 \mid m$, then m = 4k for some integer k. Then $m \mid 2^m - 2$ implies $4k \mid 2^{4k}-2$.
Thus $2^{4k}-2 = 4kn$ for some $n \in \mathbf{Z}$, or $2^{4k}-4\,kn = 2$ or $4^{2k}-4kn = 2$, hence $4(4^{2k-1}-kn) = 2$, or $2(4^{2k-1}-kn) = 1$, a contradiction. This completes the proof.

Thus if m is a pseudoprime then either m is an odd positive integer or m = 2n, where n is an odd positive integer. If m = 2n, the congruence relation $2^m \equiv 2 \pmod{m}$ becomes $2^{2n} \equiv 2 \pmod{2n}$, and this is equivalent to $2^{2n-1} \equiv 1 \pmod{n}$. Moreover, if p is a prime factor of n, then p is odd. Now let e_p be the order of 2 (mod p), i.e., $e_p = \text{ord}_p(2)$. By **Fermat's** Little Theorem, we have $2^{p-1} \equiv 1 \pmod{p}$. Thus $e_p | p-1$.

Theorem 2.16. If the congruence $2^{2n-1} \equiv 1 \pmod{n}$ holds for some n, then n has at least two distinct prime factors.

Proof: Assume that the congruence relation holds for some $n = p^k$. Since $2^{2p^{k-1}} \equiv 1 \pmod{p^k}$, then $e_p | 2p^k-1$. Also $e_p | p-1$. But $2p^k - 1 = 2(p^k-1)+1$. Hence $e_p | 1$ implies $e_p = 1$ implies $2^1 = 1 \pmod{p}$, a contradiction. This completes the proof.

Theorem 2.17. If $n = p_1 p_2 \ldots p_k$, then the congruence relation $2^{2n-1} \equiv 1 \pmod{n}$ holds if and only if $e_{p_i} | 2np_i^{-1}-1$ for all $i = 1, 2, \ldots, k$.

Proof: Assume that $e_{p_i} | 2np_i^{-1}-1$ implies $2np_i^{-1}-1 = e_{p_i}k_i$ for some $k_i \in \mathbf{Z}$. Then $2n-1 = 2np_i^{-1}(p_i-1) + (2np_i^{-1}-1)$. Thus

$$2^{2n-1} = 2^{2np_i^{-1}(p_i-1)+(2np_i^{-1}-1)}$$

$$= 2^{(e_{p_i}k_i+1)(p_i-1)+e_{p_i}k_i}$$

$= 2^{p_i e_{p_i} k_i + p_i - 1}$, for i = 1,2,..., k

$= (2^{e_{p_i}})^{p_i k_i} . 2^{p_i - 1} \equiv 1 \pmod{p_i}$, for all i = 1,2,...,k. Thus $2^{2n-1} \equiv 1 \pmod{n}$.

Conversely, assume that $2^{2n-1} \equiv 1 \pmod{n}$.

Then $2^{2n-1} \equiv 1 \pmod{p_i}$.

Since $2n-1 = 2np_i^{-1}(p_i-1)+2np_i^{-1}-1$, we have $2^{2n-1} = 2^{2np_i^{-1}(p_i-1)+(2np_i^{-1}-1)}$

$= 2^{2np_i^{-1}(p_i-1)} . 2^{2np_i^{-1}-1} \equiv 2^{2np_i^{-1}-1} \pmod{p_i}$. Since $2^{2n-1} \equiv 1 \pmod{p_i}$, we have $2^{2np_i^{-1}-1} \equiv 1 \pmod{p_i}$, and hence $e_{p_i} | 2np_i^{-1}-1$. This completes the proof.

Beeger obtained three new solutions of $2^m-2 \equiv 0 \pmod{m}$ by applying Theorem 2.17 to the case n = 23*31*p.

First, we need to find the order of 2 modulo the integer 23 and 31.

$2^{11}-1 = 2048-1 = 2047$

$23 | 2047$, hence $e_{23} = 11$.

Again, $2^{15}-1 = 32768-1 = 32767$, so $31 | 32767$, thus $e_{31} = 15$ also $e_2 = 1$.

In order for 2n to be a pseudoprime by Theorem 2.17, $e_{p_i} | 2np_i^{-1}-1$ must hold. Now, $2* 23.*31* 31^{-1}p = 46p$ and $2* 31* 23. 23^{-1}p = 62p$.

So by Theorem 2.17, p must satisfy

$62p \equiv 1 \pmod{15}$ . . . (1)

$46p \equiv 1 \pmod{15}$ . . . (2)

$146p \equiv 1 \pmod{e_p}$ . . . (3).

The solutions of (1) & (2) are:

$$P \equiv 19 \pmod{11} \quad \ldots \quad (4)$$

$$p \equiv 1 \pmod{15} \quad \ldots \quad (5),$$

and again since p is odd, we have

$$p \equiv -1 \pmod{2}$$

$$-1 \equiv 151 \pmod{2}.$$

Hence, $p \equiv 151 \pmod{2}$ . . . (6).

From (5)& (6), we have

$$62p \equiv 1 \pmod{11}$$

$$46p \equiv 1 \pmod{15}$$

$$7p \equiv 1 \pmod{11}$$

$$p \equiv 1 \pmod{15}$$

$p = 1+15k$ for some k

implies $7(1+15k) \equiv 1 \pmod{11}$

$99k + 6k \equiv -6 \pmod{11}$

or $6k \equiv -6 \pmod{11}$

or $k \equiv -1 \pmod{11}$

or $k = -1+11m$ for some m

$p = 1+15(-1+11m)$

$= -14 + 165m$

or $p \equiv -14 \pmod{165}$

or $p \equiv 151 \pmod{165}$ . . . (7).

From (6) & (7), $p \equiv 151 \pmod{330}$.

From (3), $1426p \equiv 1 \pmod{e_p} \Rightarrow e_p$ is some divisor of 1425; the divisors of 1425 are found to be k = 1,3,5,15,19,25,52,75,95,285,475,1425.

Only three values of p = 151, 1801, 100801 satisfy the congruence $p \equiv 151 \pmod{330}$. Thus the three corresponding values of m that satisfy the congruence

$$2^m - 2 \equiv 0 \pmod{m}$$

are: 215326, 2568226, 143742226.

Before we prove the existence of infinitely many even pseudoprimes, we need the following lemma whose proof can be found in [1].

Lemma 2.18. For every integer $k > 6$, $r = 2^k-1$ has a primitive prime factor. That is, there exists a prime p such that $2^k-1 \equiv 0 \pmod{p}$ and $2^t-1 \not\equiv 0 \pmod{p}$ for $1 \leq t < k$.

Theorem 2.19. Let m = 2n, where n is an odd positive integer. Then the congruence $2^m - 2 \equiv 0 \pmod{m}$ has infinitely many solutions.

Proof: The proof consists of showing that given any solution m of $2^m \equiv 2 \pmod{m}$, there exists a prime p depending on m such that mp is also a solution. Let m = 2n be any solution of $2^m \equiv 2 \pmod{m}$. Thus $2^{2n-1} - 1 \equiv 0 \pmod{n}$ holds. By Lemma 2.18, there exists a primitive prime factor

p of $2^{2n-1} - 1$. Thus $e_p = 2n-1$ and $2^{2n-1} \equiv 1 \pmod{p}$. Since p is a prime, by **Fermat's** Theorem we have $2^{p-1} \equiv 1 \pmod{p}$. Thus $e_p | p-1$. Hence $2n-1 | p-1$, or $(p-1) = (2n-1)k$ for some k, thus $p = (2n-1)k+1 > n$. So p and n are coprime. We have $2^{2pn-1} = 2^{2n-1 + 2n(p-1)} = 2^{2n-1 + 2n[(2n-1)k + 1 - 1]} = 2^{(2n-1)(2nk+1)} \equiv 1 \pmod{m}$... (1) and also $2^{2pn-1} = 2^{(2n-1)(2nk+1)} \equiv 1 \pmod{p}$... (2). Combining (1) & (2), we have $mp | 2^{(2n-1)(2nk+1)}$. This completes the proof.

One may ask, "how far" are the pseudoprimes from being primes? The answer to this question will definitely depend on what we mean by the phrase "how far". In 1949, **Erdös** [9] proved that for every integer $k \geq 2$, there exists infinitely many pseudoprimes which are the product of exactly k distinct primes.

First we are going to prove a special case of this due to **Lehmer** [15].

Lemma 2.20. There are infinitely many pseudoprimes n that are the product of two distinct primes.

Proof: By Lemma 2.18, for every odd integer $m > 6$, both 2^m-1 and $2^m + 1$ have primitive prime factors, say p and q respectively. Thus

$2^m-1 \equiv 0 \pmod{p}$ and $2^k-1 \not\equiv 0 \pmod{p}$ for $1 \leq k < m$,

$2^m+1 \equiv 0 \pmod{q}$ and $2^k+1 \not\equiv 0 \pmod{q}$ for $1 \leq k < m$.

The first congruence implies that $ord_p(2) = m$. Thus $m|\phi(p) = p-1$ or $p - 1 \equiv 0 \pmod{m}$. Also since p is an odd prime, we have $p-1 \equiv 0 \pmod{2}$. Thus $p-1 \equiv 0 \pmod{2m}$. On the other hand since $2^m \equiv -1 \pmod{q}$, then $2^{2m} \equiv 1 \pmod{q}$. Hence $ord_p(2) = 2m$ which implies $2m|\phi(q) = q-1$, or $q-1 \equiv 0 \pmod{2m}$. Moreover, $2^{2m} \equiv 1 \pmod{p}$ and $2^{2m} \equiv 1 \pmod{q}$ implies $2^{2m} \equiv 1 \pmod{pq}$. Now we are going to prove that pq is a pseudoprime.

We have $2^{pq-1} \equiv 2^{(p-1)(q-1)}.2^{p-1}.2^{q-1}$. From **Fermat's** Little Theorem, $2^{p-1} \equiv 1 \pmod{p}$ and $2^{q-1} \equiv 1 \pmod{q}$. Thus $2^{(p-1)(q-1)} \equiv 1 \pmod{p}$ and $2^{(p-1)(q-1)} \equiv 1 \pmod{q}$ implies $2^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. $p-1 \equiv 0 \pmod{2m}$ implies $p-1 = 2mk$ and hence $2^{p-1} = 2^{2mk} \equiv 1 \pmod{pq}$. Similarly $2^{q-1} \equiv 1 \pmod{pq}$. Thus $2^{pq-1} \equiv 1 \pmod{pq}$. Hence pq is a pseudoprime. To complete the proof, we must show that to different values of m correspond to two different values of pq. Assume the contrary. That is, assume that for another odd integer $m' > 6$ correspond the same pseudoprime pq. Without loss of generality, assume that $m' < m$. If p is a primitive prime factor of $2^{m'}-1$, then $2^{m'}-1 \equiv 0 \pmod{p}$. But this contradict the fact that p is a primitive prime factor of $2^m - 1$. On the other hand if q is a primitive prime factor of $2^{m'}-1$, then $2^{m'}-1 \equiv 0 \pmod{q}$. Since $m' < m$ then $m = m'+t$ for some integer $0 < t < n$. Thus $2^m+1 = 2^{m'+t}+1 \equiv 2^t+1 \pmod{q}$ and this implies $2^t \equiv -1 \pmod{}$

q), which contradicts the fact that q is a primitive prime factor of $2^m + 1$. This completes the proof.

Next we present the prove of the general case.

Theorem 2.21 (Erdös). For every integer $k \geq 2$, there exists infinitely many square free pseudoprime with exactly k prime factors.

proof: The general case can be proved by induction on k. Let $n_1 < n_2 < \ldots$ be an infinite sequence of pseudoprimes with k-1 prime factors. Let p_i be one of the primitive prime factors of $2^{n_i-1}-1$. We claim $p_i n_i$ is a pseudoprime. Since n_i is a pseudoprime, we have $2^{n_i-1} \equiv 1 \pmod{n_i}$. Again since p_i is a primitive prime factor of $2^{n_i-1}-1$, then

$$2^{n_i-1} \equiv 1 \pmod{p_i}$$

and hence

$$2^{n_i-1} \equiv 1 \pmod{p_i n_i}.$$

Since p_i is a primitive prime factor of $2^{n_i-1}-1$, then $ord_{p_i}(2) = n_i-1$. But $ord_{p_i}(2) \mid \phi(p_i)$, hence $(n_i-1) \mid (p_i-1)$, thus, $p_i - 1 \equiv 0 \pmod{(n_i-1)}$.

Since $p_i-1 \equiv 0 \pmod{(n_i-1)}$, then $p_i-1 = k_i(n_i-1)$ for some $k_i \in \mathbf{Z}$. Hence $2^{p_i-1} = 2^{k_i(n_i-1)} = (2^{n_i-1})^k \equiv 1 \pmod{n_i}$.

By **Fermat's** Little Theorem, we have $2^{p_i-1} \equiv 1 \pmod{p_i}$. The last two congruences imply $2^{p_i-1} \equiv 1 \pmod{p_i n_i}$.

We also have $2^{n_i-1} \equiv 1 \pmod{n_i p_i}$.

Thus $2^{n_i p_i-1} = 2^{(n_i-1)(p_i-1)} 2^{n_i-1}.2^{p_i-1} \equiv 1 \pmod{p_i n_i}$.

Also $p_i > n_i$ since $p_i-1 \equiv 0 \pmod{n_i-1}$ and n_i is not a prime. Thus $p_i n_i$ has k prime factors. Moreover, the integer $n_i p_i$ are distinct. This completes the proof.

2.3. HOW ARE THE PSEUDOPRIME NUMBERS DISTRIBUTED?

So far we have given various constructive proofs of the existence of infinitely many odd pseudoprimes as well as even pseudoprimes. We proved that certain sequences generate infinitely many pseudoprimes. However, these sequences do not generate all the pseudoprimes. Furthermore, one cannot determine how many pseudoprimes are less than any given integer x. In this section, however, we are going to estimate from above as well as from below the number of pseudoprimes less than a given integer x(when x is larger). As in the case of the distribution of primes, proofs concerning the distribution of pseudoprimes are mathematically involved and are beyond the scope of this paper.

Theorem 2.22. Let $p\pi(x)$ denote the number of pseudoprimes less than or equal to x. Then, for x sufficiently large, we have: $c \log x < p\pi(x) < x \exp\{-1/3 (\log x)^{1/4}\}$, where c is a positive real number.

The proof of this theorem is beyond the scope of this study, the proof is given by **Erdös** [10]. On the other hand we are going to prove a corollary to this theorem that gives some insight concerning the distribution of pseudoprimes.

Corollary(Szymiczek [34]). Let p_n denote the nth pseudoprime in the sequence of all pseudoprimes. Then the series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converges.

Proof: Let $x = p_n$ in Theorem 2.22. Then for sufficiently large n. $p\pi(x) = p\pi(p_n) = n < p_n \exp\{-1/3(\log p_n)^{1/4}\}$

$$\Rightarrow n < \frac{p_n}{\exp((\log p_n)^{1/4})^{1/3}} \Rightarrow \frac{n}{P_n} < \frac{1}{\exp((\log P_n)^{1/4})^{1/3}}.$$

Since $n < p_n$, we have $(\log n)^{1/4} < (\log p_n)^{1/4}$,

and $\frac{1}{(\log p_n)^{1/4}} < \frac{1}{(\log n)^{1/4}}$.

Thus $\frac{n}{p_n} < \frac{1}{\exp((\log p_n)^{1/4})^{1/3}} < \frac{1}{\exp((\log n)^{1/4})^{1/3}}$

$$\Rightarrow \frac{1}{p_n} < \frac{1}{n\,(\exp((\log n)^{1/4})^{1/3})}.$$

On the other hand for larger m, $m^{1/4} > 4 \log m$. Let $m = (\log n)$. Then

$(\log n)^{1/4} > 4 \log(\log n)$

$\Rightarrow (\log n)^{1/4} > \log(\log n)^4$

$\Rightarrow 1/3\ (\log n)^{1/4} > \log\ (\log n)^{4/3}$

$$\Rightarrow \exp\{ 1/3 (\log n)^{1/4} \} > \exp\{ \log (\log n)^{4/3} \}$$

$$= (\log n)^{4/3}.$$

Thus $\frac{1}{p_n} < \frac{1}{n(\log n)^{4/3}}$. But the series $\sum_{n=2} \frac{1}{n(\log n)^{4/3}}$ converges,

(this can be proved by the integral test). Hence $\sum_{n=1}^{\infty} \frac{1}{P_n}$

converges. This completes the proof.

Remarks. It is well known that the series $\sum_{p \text{ prime}} \frac{1}{p}$ is

divergent [25]. Thus it may be said somewhat "vaguely" that the primes are not so sparsely distributed as the pseudoprimes.

An improvement for the upper bound of $p\pi(x)$ was given in 1981 by **Pomerance** [21]. He showed that for large x

$$p\pi(x) \leq \frac{x}{\sqrt{L(x)}}.$$

where L(x) = exp{(log x).log (log (logx)}/log (log x).

Remarks. Let $\pi(x)$ denote the number of primes $\leq$ x where x is any real number. The Prime Number Theorem [25] states

$\lim_{x \to \infty}$.

Thus for large value of x, $\pi(x) < C \frac{x}{\log x}$, where C is a

positive constant whose value is very close to 1. The above estimate of $p\pi(x)$ implies that the number of pseudoprimes

less than or equal to x is very much less than the number of primes less than or equal to x , because for large x,

$$\frac{x}{\sqrt{L(x)}} < \frac{x}{\log x}.$$

For examples, if $x = 10^{20}$, then $p\pi(10^{20}) < \frac{10^{20}}{\sqrt{L(10^{20})}}$,

$$L(10^{20}) = \exp\{\log 10^{20})*\log(\log(\log 10^{20}))\}/ \log(\log(10^{20}))$$

$$\approx \exp(16.146) \approx 1.029*10^{7}.$$

Thus $p\pi(10^{20}) \leq 3.117*10^{16}$.

On the other hand $\frac{x}{\log x} = \frac{10^{20}}{\log 10^{20}} \approx 2.171* 10^{18}$.

Thus $\pi(x) \leq 2.171*10^{18}$.

Hence, $\frac{p\pi(10^{20})}{\pi(10^{20})} \approx 1.435*10^{-2}$.

The tables of pseudoprimes suggest that for every x > 170 there exists a pseudoprime between x and 2x. However, this has not yet been proved. In this direction **Ratkiewicz** [27] proved the following three results concerning gaps between pseudoprimes.

Theorem 2.23. If n > 19 is an integer, there exists a pseudoprime between n and n^2.

Theorem 2.24. For every $\epsilon > 0$ there exists $x_0 = x_0(\epsilon) > o$ such that if $x > x_0$, there is a pseudoprime between x and $x^{1+\epsilon}$.

Another result concerning the distribution of pseudoprimes in an arithmetical progression was settled by **Ratkiewicz** in 1967 [28]. He proved an analogous result to the well known **Dirichlet** Theorem on the distribution of primes in an arithmetic progression.

Theorem 2.25. If a, b ≥ 1 are integers and gcd(a, b) = 1, there exists infinitely many pseudoprimes in on arithmetic progression {a+bk:k ≥ 1}.

The proofs of the last three theorems are beyond the scope of this paper.

Chapter 3

PSEUDOPRIMES TO ANY BASE

In this chapter, we will be studying one of many generalizations of pseudoprimes. Our treatment here will follow the pattern we already laid out for pseudoprimes in chapter 2. The following is the list of questions whose discussion will be the main focus of this chapter are:

1. How do you recognize whether a natural number is a pseudoprime to the base a?
2. How many pseudoprimes to the base a are there?
3. Are there functions that produce some or all pseudoprimes to the base a?
4. How are the pseudoprimes to the base a distributed?

3.1 BASIC DEFINITIONS AND EXAMPLES

Definition 3.1. Let a be an integer. A positive integer n is called a **pseudoprime to the base a** if n is composite and $a^n \equiv a \pmod{n}$.

Examples.

1. Show that n = 91 = (13*7) is a pseudoprime to the base 3.

We have $3^{90} \equiv (729)^{15} \equiv (1)^{15} \equiv 1 \pmod{91}$, hence $3^{91} \equiv 3 \pmod{}$

91) and since 91 is a composite number, then 91 is a pseudoprime to the base 3.

2. Show that n = 25 = (5*5) is a pseudoprime to the base 7. We have $(7)^{24} \equiv (7^2)^{112} \equiv (-1)^{12} \equiv 1 \pmod{25}$, hence $7^{25} \equiv 7 \pmod{25}$ and since 25 is a composite number, then 25 is a pseudoprime to the base 7.

Remarks:

1. If n is a pseudoprime to the base a, then we sometimes say n is a pseudoprime with respect to a or simply n is an a-pseudoprime.

2. The pseudoprimes we studied in chapter 2 are simply the pseudoprimes to the base a = 2.

If n is a pseudoprime to the base a such that gcd(a,n) = 1, then the congruence $a^n \equiv a \pmod{n}$ is equivalent to $a^{n-1} \equiv 1 \pmod{n}$.
Similarly if n is a composite positive integer such that $a^{n-1} \equiv 1 \pmod{n}$, then n is a pseudoprime to the base a.

Theorem 3.1. Let n be a composite positive integer.

(a). n is a pseudoprime to the base a, where gcd(a,n) = 1 if and only if the order of a mod n, $\text{ord}_n(a)$, divides n-1.

(b). If n is a pseudoprime to the bases a and b, where gcd(a,n) = gcd(b,n) = 1, then n is a pseudoprime to the base ab.

(c). If n is a pseudoprime to the base b, then n is a pseudoprime to the base b^{-1}, where b^{-1} is an integer which is inverse to b (mod n) (i.e, $bb^{-1} \equiv 1 \pmod{n}$).

(d). If n is an odd pseudoprime to the base a, where gcd(a,n) = 1, then n is a pseudoprime to the base n-a.

Proof: (a). Let us assume that $ord_n(a) | n-1$. then $n-1 = k\, ord_n(a)$, for some k.

$$a^{n-1} = a^{k\, ord_n(a)} = \left(a^{ord_n(a)}\right)^k \equiv 1 \pmod{n}.$$

Hence, n is a pseudoprime to the base a. Conversely, assume that

$$a^{n-1} \equiv 1 \pmod{n},$$

by the Division Algorithm, we have

$$n-1 = q\, ord_n(a) + r, \quad \text{where } 0 \le r < ord_n(a).$$

Hence

$$a^{n-1} = a^{q\, ord_n(a) + r}$$

$$= a^{q\, ord_n(a)} . a^r = \left(a^{ord_n(a)}\right)^q . a^r \equiv a^r \pmod{n}.$$

Since

$$a^{n-1} \equiv 1 \pmod{n},$$

then

$$a^r \equiv 1 \pmod{n}.$$

From the inequality $0 \le r < ord_n(a)$, we conclude that r = 0,

So that $n-1 = q\ ord_n(a)$. Hence $ord_n(a) | n-1$. This completes the proof of part (a).

(b). Let us assume that n is a pseudoprime to the bases a and b. Then we have

$$a^{n-1} \equiv 1 \pmod{n} \quad \ldots (1)$$

and

$$b^{n-1} \equiv 1 \pmod{n} \ldots (2).$$

Multiplying (1) and (2), we have

$$(ab)^{n-1} \equiv 1 \pmod{n}.$$

Again by our assumption that n is a pseudoprime to the bases a and b, We have

$$gcd(a,n) = 1 \text{ and } gcd(b,n) = 1,$$

so that

$$1 = ax+ny = bu+nv, \quad \text{for some integers } x,y,u,v.$$

Hence,

$$1*1 = (ax+ny)(by+nv)$$

Or

$$1 = abxu+axnv+nbyu+nynv$$
$$= ab(nu)+n(axv+byv).$$

Hence,

$gcd(ab,n) = 1$. So $(ab)^{n-1} = 1 \pmod{n}$, and $gcd(ab,n) = 1$ implies n is a pseudoprime to the base ab. This completes the proof of part (b).

(c). Now, since $b^n \equiv b \pmod{n}$, multiplying both sides by

$(b^{-1})^n$, we obtain

$(bb^{-1})^n \equiv b(b^{-1})(b^{-1})^{n-1} \equiv (b^{-1})^{n-1} \pmod{n}$. Hence $(b^{-1})^{n-1} \equiv 1 \pmod{n}$.

Again since n is a pseudoprime to the base b, gcd(b,n) = 1. Hence,

$1 = bx+ny$, for some integers x, y.

So that

$$1 = b^{-1}(bb)x+ny$$
$$= b^{-1}(b^2x)+n(y).$$

Thus $\gcd(b^{-1},n) = 1$. Hence n is a pseudoprime to the base b^{-1}. This completes the proof of part (c).

(d). By the binomial theorem, we have

$(n-a)^n = (n-a)(n^{n-1}-(n-1)n^{n-2}a+(n-1)(n-2)/2\ n^{n-3}+ \ldots +a^{n-1})$

$\equiv (n-a)\ a^{n-1} \pmod{n}$.

Since n is a pseudoprime to the base a, we have

$a^{n-1} \equiv 1 \pmod{n}$.

Hence,

$(n-a)^n \equiv (n-a) \pmod{n}$. So n is a pseudoprime to the base (n-a). This completes the proof of part (d).

Theorem 3.2. Every odd composite positive integer n is a pseudoprime to the bases a = 1 and a = -1.

Proof: Let us assume that n is an odd composite positive integer.

Then n is a pseudoprime to the base a if and only if $a^n \equiv a \pmod{n}$. We have

$$1 \equiv 1 \pmod{n},$$

hence

$$(1)^n \equiv (1)^n \equiv 1 \pmod{n}.$$

Again since $-1 \equiv -1 \pmod{n}$, and n is an odd integer,

$$(-1)^n = -1.$$

So that

$$(-1)^n \equiv -1 \pmod{n}.$$

Hence, n is a pseudoprime to the bases a = 1,-1. This completes the proof.

Theorem 3.3. Let p be a prime. Then $n = p^r$, where $r \geq 2$ is an integer, is a pseudoprime to the base a if and only if $a^{p-1} \equiv 1 \pmod{p^r}$.

Proof: Let us assume that $n = p^r$ is a pseudoprime to the base a. Then we have

$$a^{p^r} \equiv a \pmod{p^r}.$$

Raising both sides to the (p-1)st power, we obtain

$$a^{p-1} \equiv a^{p^r(p-1)} \pmod{p^r} \quad . \; . \; . \quad (1).$$

By **Euler's** Theorem, we have

$$a^{\phi(p^r)} \equiv 1 \pmod{p^r},$$

thus

$$\left(a^{\phi(p^r)}\right)^p \equiv 1 \pmod{p^r},$$

or

$$a^{p^{r}(p-1)} \equiv 1 \pmod{p^r}.$$

From (1) we obtain,

$$a^{p-1} \equiv 1 \pmod{p^r}.$$

Conversely, let us assume that the congruence relation

$$a^{p-1} \equiv 1 \pmod{p^r} \text{ holds.}$$

Then

$$(a^{p-1})^k \equiv 1 \pmod{p^r} \text{ for any positive integer } k.$$

Let

$$k = \frac{p^r-1}{p-1} = \frac{(p-1)(p^{r-1}-p^{r-2}+\ldots-1)}{p-1}$$

$$= p^{r-1}-p^{r-2}+\ldots-1.$$

Since $r \geq 2$, then k is a positive integer.

Thus

$$(a^{p-1})^k = (a^{p-1})^{\frac{p^r-1}{p-1}} = a^{p^r-1} \equiv 1 \pmod{p^r},$$

and hence $n = p^r$ is a pseudoprime to the base a. This completes the proof.

Theorem 3.4. Let n = pq, where p and q are distinct primes. Then n is a pseudoprime to the base a if and only if $a^d \equiv 1 \pmod{n}$, where d = gcd(p-1,q-1).

Proof: Let us assume that n = pq is a pseudoprime to the base

a.

Thus

$$a^{n-1} = a^{pq-1} \equiv 1 \pmod{pq}.$$

Hence $a^{pq-1} \equiv 1 \pmod{p}$, since p is a divisor of n.

Since

$$q-1 = (pq-1)-q(p-1),$$

then

$$a^{q-1} = a^{pq-1}.(a^{p-1})^{-q} \equiv 1 \pmod{p}.$$

Again since

$$\gcd(p-1,q-1) = d,$$

then,

$$x(p-1)+y(q-1) = d \text{ for some } x,y.$$

Hence,

$$a^d \equiv a^{x(p-1)}.a^{y(q-1)} \equiv 1 \pmod{p}.$$

So that

$$a^d \equiv 1 \pmod{p} \ldots (1).$$

Similarly it can be shown that

$$a^d \equiv 1 \pmod{q} \ldots (2).$$

(1)&(2) implies

$$a^d \equiv 1 \pmod{pq}.$$

In other words,

$$a^d \equiv 1 \pmod{n}.$$

Conversely, let us assume that

$$a^d \equiv 1 \pmod{pq}.$$

Hence,

$$a^d \equiv 1 \pmod{p}, \text{ and } a^d \equiv 1 \pmod{q}.$$

Since gcd(p-1, q-1) = d, then d|p-1 and d|q-1.

Thus p-1 = kd, and q-1 = cd, for some integers k and c, so that

$$a^{q-1} = a^{cd} \equiv (a^d)^c \equiv 1 \pmod{p}.$$

Similarly,

$$a^{p-1} \equiv 1 \pmod{q}.$$

From **Fermat's** Little Theorem, we have

$$a^p \equiv a \pmod{p}.$$

Hence,

$$a^{pq} \equiv a^q \equiv a \pmod{p}.$$

Similarly,

$$a^{pq} \equiv a \pmod{q}.$$

Thus

$$a^{pq} \equiv a \pmod{pq}.$$

Hence, n = pq is a pseudoprime to the base a. This completes the proof.

3.2.HOW MANY PSEUDOPRIMES ARE THERE TO THE BASE a?

In this section we are going to answer the question concerning the number of pseudoprimes to a base a. As it turns out, not surprisingly, there are infinitely many pseudoprimes to the base a and we will see there are many ways to generate infinite sequences of pseudoprimes.

The first proof of the existence of infinitely many pseudoprimes to the base a was given by **Cipolla** [6]. He proved

the following theorem:

Theorem 3.5. Let p be an odd prime such that $p \nmid a(a^2-1)$, where $a \geq 2$. Then $m = \frac{a^{2p}-1}{a^2-1}$ is a pseudoprime to the base a.

Proof: $m = \frac{a^{2p}-1}{a^2-1} = \frac{(a^p-1)(a^p+1)}{(a-1)(a+1)}$

$$= \frac{(a-1)(a^{p-1}+a^{p-2}+\ldots+1)}{(a-1)} \cdot \frac{(a+1)(a^{p-1}-a^{p-2}+\ldots+1)}{(a+1)}$$

$$= (a^{p-1}+a^{p-2}+\ldots+1)(a^{p-1}-a^{p-2}+\ldots+1).$$

So m is a composite number.

$$(m-1) = \frac{a^{2p}-1}{a^2-1} - 1 = \frac{a^{2p}-1-a^2+1}{a^2-1}.$$

or

$$(a^2-1)(m-1) = a^{2p}-a^2 = (a^p-a)(a^p+a) = a(a^{p-1}-1)(a^p+a)$$

Since a and a^p are both even or odd,

$$2 \mid a^p + a.$$

By **Fermat's** Little Theorem,

$$p \mid a^{p-1}-1.$$

We also have

$$(a^2-1) \mid a(a^{p-1}-1)(a^p + a).$$

But since p-1 is even, then p-1 = 2k for some k, then

$$a^{p-1}-1 = a^{2k}-1 = (a^2-1)(a^{2k-2} + a^{2k-3} + \ldots + 1).$$

Hence,

$$(a^2-1) \mid (a^{p-1}-1).$$

We have by assumption

$$p \nmid a(a^2-1),$$

which implies

$$p \nmid (a^2-1).$$

Thus

$$p(a^2-1) \mid a^{p-1}-1.$$

So We have

$$2p(a^2-1) \mid (a^2-1)(m-1),$$

which implies

$$2p \mid m-1,$$

hence,

$$m = 2pk + 1, \text{ for some integer } k.$$

Now,

$$m = \frac{a^{2p}-1}{a^2-1}.$$

Hence,

$$a^{2p} = m(a^2-1)+1 \equiv 1 \pmod{m}.$$

So that

$$a^{m-1} = a^{2pk} \equiv 1 \pmod{m}.$$ This completes the proof.

Corollary. There are infinitely many pseudoprime to the base a.

Proof: The proof follows directly from Theorem 3.5. Let p be

odd prime such that $p \nmid a(a^2-1)$, for example take $p > a(a^2-1)$.

Then $m = \frac{a^{2p}-1}{a^2-1}$ is a pseudoprime to the base a, since there are infinitely many primes $p > a(a^2-1)$, then there are infinitely many pseudoprime to the base a.

Using Theorem 3.5, **Steuerwald** [33], developed a method of generating increasing sequences of pseudoprimes to the base a. First we need the following lemma.

Lemma 3.6. Let n be a pseudoprime to the base a, then the integer $N = \frac{a^n-1}{a-1}$ is a pseudoprime to the base a provided that $\gcd(a-1, n) = 1$, moreover $\gcd(a-1,N) = 1$.

Proof: We have $N-1 = \frac{a^n-1}{a-1} - 1 = \frac{a^n-a}{a-1} = \frac{a(a^{n-1}-1)}{a-1}$.

Since n is a pseudoprime to the base a then $n \mid a^{n-1}-1$, and hence,

$$n \mid a(a^{n-1}-1).$$

Thus

$$a(a^{n-1}-1) = nk \text{ for some integer } k.$$

Therefore,

$N-1 = \frac{nk}{a-1}$, but since $\gcd(a-1,n) = 1$, $\frac{k}{a-1}$ must be

an integer, say

$$\frac{k}{a-1} = k' \text{ and thus } N-1 = nk'.$$

Again, $N(a-1) = a^n-1$,

implies

$$N \mid a^n-1$$

or

$$a^n \equiv 1 \pmod{N}.$$

Since $N-1= nk'$,

we have

$$a^{N-1} = a^{nk'} = (a^n)^{k'} \equiv 1 \pmod{N}.$$

Next we are going to show that N is a composite integer.

Since n is a composite integer ,let $n = rs$, $r,s > 1$.

So

$$N = \frac{a^n-1}{(a-1)} = \frac{a^{rs-1}}{a-1}$$

$$= \frac{(a^r)^s-1}{a-1}$$

$$= \frac{(a^r-1)(a^{r(s-1)}+a^{r(s-2)}+\ldots+a+1)}{a-1}$$

$$= \frac{(a-1)(a^{r-1}+a^{r-2}+\ldots+a+1)(a^{r(s-1)}+\ldots+a+1)}{a-1}$$

$$= (a^{r-1}+a^{r-2}+\ldots+a+1)(a^{r(s-1)}+a^{r(s-2)}+\ldots+a+1).$$

So N is a composite number. Hence N is a pseudoprime to the

base a.

It remains to show that gcd(a-1,N) = 1.

By the binomial theorem,

$$N = \frac{a^n-1}{a-1}$$

$$= \frac{[(a-1)+1]^n}{a-1}$$

$$= \frac{[(a-1)^n+\binom{n}{1}(a-1)^{n-1}+\ldots+\binom{n}{n-1}(a-1)+1]-1}{a-1}$$

$$= \frac{(a-1)^n+n(a-1)^{n-1}+\ldots+n(a-1)}{a-1}$$

$$= (a-1)^{n-1}+n(a-1)^{n-2}+\ldots+n$$

$$\equiv n \pmod{(a-1)}.$$

Hence, gcd(N,a-1) = gcd(n,a-1) = 1. This completes the proof.

Let a be an integer and p be a prime such that a-1 = q is a prime and $p > a^2-1$. Let $n = \frac{a^{2p}-1}{a^2-1}$, by Theorem 3.5, n is a pseudoprime to the base a.

Let

$$n_1 = \frac{a^p-1}{a-1} = a^{p-1}+a^{p-2}+ \ldots +a+1, \text{ and}$$

$$n_2 = \frac{a^p+1}{a+1} = a^{p-1}-a^{p-2}+ \ldots +a^2-a+1.$$

Since a = q+1, then for any positive integer k, $a^k = (q+1)^k \equiv 1 \pmod{q}$. Thus

$$n_1 = a^{p-1}+a^{p-2}+ \ . \ . \ . \ +a+1 \equiv 1+1 \ . \ . \ . \ +1 \equiv p \pmod{q}.$$

Similarly,

$n_2 \equiv 1 \pmod{q}$. Hence $n = n_1 n_2 \equiv p \pmod{q}$, and this implies $\gcd(q,n) = \gcd(q,p) = 1$ and thus $\gcd(a-1,n) = 1$.

Now, we consider the sequence $f(n) = \frac{a^n-1}{a-1} > n$. By Lemma 3.6, f(n) is a pseudoprime to the base a. This process may be iterated and leads to an increasing sequence of pseudoprimes to the base a, namely $n < f(n) < f(f(n)) < f(f(f(n))) < \ . \ . \ .$.

Another elementary proof of the existence of infinetely many pseudoprimes to a base a was given by **Crocker** [7].

Theorem 3.7. Let a be an even positive integer, but not of the form 2^{2^r} with $r \geq 0$. Then, for every integer $n \geq 1$, the number $N = a^{a^n}+1$ is a pseudoprime to the base a.

Proof: We have $a^{2a^n}-1 = (a^{a^n}+1)(a^{a^n}-1)$,

so that

$$a^{a^n}+1 \mid a^{2a^n}-1.$$

Since $a^n > n$ for all $n \geq 1$(this follows from the fact that $a^n > 2^n > n$) and a is even then $2 \mid a^{a^n-n}$.

Hence,

$$2a^n \mid a^{a^n}.$$

By using Lemma 2.1, we have,

$$a^{2a^n}-1 \mid a^{a^{a^n}}-1.$$

Now

$$a^{a^n}+1 \mid a^{2a^n}-1 \text{ and } a^{2a^n}-1 \mid a^{a^{a^n}}-1,$$

implies $a^{a^n}+1 \mid a^{a^{a^n}}-1$,

or

$$a^{N-1} \equiv 1 \pmod{N}.$$

Moreover,

$$a^{a^n}+1 = (a^a+1)(a^{a^{n-1}}-a^{a^{n-2}}+\ldots+1) \quad \text{for any } n \geq 1.$$

So $N = a^{a^n}+1$ is a composite number.

Hence, $N = a^{a^n}+1$ is a pseudoprime to the base a. This completes the proof.

This theorem shows constructively how to generate infinitely many pseudoprime to the base a. This construction, unlike the previous ones is not in terms of primes, which are very difficult to determine, but in terms of the positive integers.

3.3 HOW ARE THE PSEUDOPRIMEES TO THE BASE a DISTRIBUTED ?

Let $p\pi_a(x)$ denote the number of pseudoprimes to the base a that are less than or equal to x. The same result concerning the distribution of pseudoprime to the base 2 also holds for any base a was given by **Pomerence** in 1981 [21].

Theorem 3.8. For large x, $p\pi_a(x) \leq \frac{x}{\sqrt{L(x)}}$,

where L(X) = exp{ (logx) log(logx)}/ log (logx).

The proof of this theorem is beyond the scope of this paper.

3.4 PSEUDOPRIMES AND TEST OF PRIMALITY

One very important concern in number theory is to establish whether a given positive integer n is a prime or composite. Most of the efficient primality tests known are based on **Fermat's** Little Theorem, which states if p is a prime, then for any positive integer a, such that gcd(a,p) = 1, the congruence relation $a^{p-1} \equiv 1 \pmod{p}$ holds. Thus if for a given positive integer n, there exists a, with $1 \leq a < n$, and gcd(a,n) = 1 such that $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite.

For example, since $2^{90} \not\equiv 1 \pmod{91}$, n = 91 is a composite number. On the other hand $3^{90} \equiv 1 \pmod{91}$, thus the converse of **Fermat's** Little Theory fails to provide a primality test.

Despite the fact that the converse of **Fermat's** Theorem

does not provide a primality test, the "overwhelming majority" of composite integers n can be shown to be composite because they fail to pass **Fermat's** Theorem for some integer a, $1 \leq a < n$. Our objective in the remaining part of this chapter is to clarify the previous sentence.

Theorem 3.9. Let n be an odd composite integer. If for some base a relatively prime to n, $1 \leq a < n$, $a^{n-1} \not\equiv 1 \pmod{n}$, then $b^{n-1} \not\equiv 1 \pmod{n}$ for at least half of the possible bases b, where $1 \leq b < n$.

Proof: Let $\{b_1, b_2, \ldots, b_n\}$ be the set of all possible bases for which n is a pseudoprime with respect to i.e., the set of all integers b_i, where $0 < b_i < n$, $\gcd(b_i, n) = 1$ and for which the congruence relation $b_i^{n-1} \equiv 1 \pmod{n}$ holds. Let b be a fixed base for which n is not a pseudoprime. If n were a pseudoprime to any of the bases bb_i, then by Theorem 3.1, it would be a pseudoprime for the base $b \equiv (bb_i)b_i^{-1} \pmod{n}$ which is not the case (since we have assumed n is not a pseudoprime to the base b). Thus, for the s distinct residues $\{bb_1, bb_2, \ldots bb_s\}$ the integer n fails to satisfy the congruence

$$(bb_i)^{n-1} \equiv 1 \pmod{n}.$$

Hence, there are at least as many bases for which n fails to be pseudoprime as there are many bases for which $b_i^{n-1} \equiv 1 \pmod{n}$ holds. This completes the proof.

Suppose we want to know whether an odd integer n is

prime. We might choose at random a in the range $1 < a < n$. Using the **Euclidean** Algorithm, we find $d = \gcd(a, n)$. If $d > 1$, we know that n is composite and in fact we have found a nontrivial factor $d|n$. If $d = 1$, then we test whether $a^{n-1} \equiv 1 \pmod{n}$ holds. If $a^{n-1} \not\equiv 1 \pmod{n}$, then we know that n is composite. On the other hand if $a^{n-1} \equiv 1 \pmod{n}$, we have some evidence that perhaps n is prime. We then try another a and go through the same process. If for this new chosen a, we obtain $a^{n-1} \not\equiv 1 \pmod{n}$, we know that n is composite and we stop. Thus according to the previous theorem, unless n happen to satisfy the congruence $a^{n-1} \equiv 1 \pmod{n}$ for all positive bases a with $\gcd(a,n) = 1$, we have at least a 50% chance that n will fail to satisfy the $a^{n-1} \equiv 1 \pmod{n}$ for randomly chosen a. Suppose that we try k different a's and find that $a^{n-1} \equiv 1 \pmod{n}$ for all of the k bases. The probability,in each try, the probability that n is composite integer despite passing the k tests is at most $(\frac{1}{2})^k$, unless n happens to be pseudoprime for all bases a, with $1 \leq a < n$. Above we have assumed that trials with different bases are mutually independent. Hence, if k is large, we can be sure with " high probability " that n is a prime (unless n is pseudoprime for all bases).

Let n be a composite positive integer. Using this primality test, if we pick 100 different integers at random between 1 and n and perform the test for each of these 100

bases, the probability that n passes all the tests is less than 10^{-40}, an extremely small number.

Using this primality test does not definitely prove that an integer n that passes all 100 tests is prime, but does give extremely strong, indeed almost overwhelming, evidence that the integer is prime.

This method of testing whether a positive integer is prime is an example of a "probilistic" method. It differs from a deterministic method where such methods will either reveal that an integer n is composite or else determine with 100% certainty that n is a prime.

The probilistic method developed in the previous paragraph fails to work if for a composite integer n the congruence relation $a^{n-1} \equiv 1 \pmod{n}$ holds for all the bases a, with $1 \leq a < n$. The question now, can it ever happen for a composite integer n, $a^{n-1} \equiv 1 \pmod{n}$ for every integer a, with $1 \leq a < n$? Unfortunately the answer is yes, and such numbers exist and they are called **absolute pseudoprimes** or **Carmichael** numbers and they will be discussed in the next chapter.

Example. Let n = 341.

To determine whether n is composite or prime, chose any base a = 2. Since gcd(2,341) = 1, applying **Fermat's** Little Theorem , we see that

$$2^{340} \equiv 1 \pmod{31}.$$

At this stage, we don't know whether n is a prime or composite

number. Now, we try with another base a = 7, again since gcd(7, 341) = 1, applying **Fermat's** Little Theorem, we see that

$$7^{340} \not\equiv 1 \pmod{341}.$$

Hence, 341 is a composite number.

We have seen several examples where an integer n is a pseudoprime to different bases. For example n = 561 is a pseudoprime to the bases 2, 5, and 7. A natural question one may ask is: given a positive composite integer n, how many bases a are there such that n is pseudoprime to the base a? The answer to this question was given by **Monier** in 1980 [19].

Before we give a formula for the number of bases for which a composite integer n is a pseudoprime with respect to the base a, we need the following lemma.

Lemma 3.10. In the congruence equations

$$x^m-1 \equiv 0 \pmod{p^k} \ldots (1)$$

and

$$x^m-1 \equiv 0 \pmod{p} \ldots (2),$$

where p is a prime and k is positive integer, the number of solutions of equations (1) and (2) are equal.

Proof: Let x_0 be a solution of equation (1), then $X_0^m-1 \equiv 1 \pmod{p^k}$ holds. Since p is a divisor of p^k, then $X_0^m-1 \equiv 0 \pmod{p}$ hold, thus x_0 is a solution of equation (2).

Conversely, assume that x_0 is a solution of (2), thus $X_0^m-1 \equiv 0 \pmod{p}$ hold, thus $X_0^m = 1+pt$ for some integer t. Let $y_0 = 1 + p^k t$. We are going to show y_0 is a of solution of equation (1). By the binomial theorem, we have,

$$(1+p^k t)^m-1 = \left[1+\binom{m}{1}p^k t+\binom{m}{2}p^{2k}t^2+\ldots+p^{mk}t^m\right]-1 \equiv 0 \pmod{p^k}.$$

Therefore, $y_0 = 1+p^k t$ is a solution of (2). Thus every solution
of (1) is a solution of (2) and to every solution of (2) there correspond one solution of (1). Hence, the number of solutions of equation (1)and (2) are equal.

Theorem 3.11. If n is a composite number, then the number of bases with $1 \le a \le n - 1$, $\gcd(a,n) = 1$ for which n is a pseudoprime to the base a is given by

$$B(n) = \prod_{p|n} \gcd(n-1,p-1).$$

Proof: The number of such bases a is the number of solutions (mod n) of the congruence equation

$$f(x) = x^{n-1}-1 \equiv 0 \pmod{n} \quad \ldots \quad (1).$$

Let

$n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of n.

For each i consider the equations

$$f(x) = x^{n-1}-1 \equiv 0 \pmod{p_i^{e_i}} \quad . \ . \ . \ (2)$$

and $$f(x) = x^{n-1}-1 \equiv 0 \pmod{p_i} \quad . \ . \ . \ (3).$$

Then by Theorem 1.10, equation (3) has $\delta_i = \gcd(n-1, p_i-1)$ distinct solutions (mod p_i). Moreover, by Lemma 3.10, equation (2) has δ_i distinct solution (mod $p_i^{e_i}$). Finally by the Chinese Remainder Theorem, equation (1) has $\prod_{i=1}^{r} \delta_i$ distinct solutions (mod n), including the two trivial solutions $x_0 = 1$ and $x_0 = -1$ (mod n). Thus the number of solutions x of equation (1), where $1 \leq x \leq n-1$ is $\prod_{i=1}^{r} \gcd(n-1, p_i-1)$. Thus $B(n) = \prod_{p|n} \gcd(n-1, p-1)$. This completes the proof.

Examples: (1). As an illustration of Theorem 3. 11, let us find the number of bases a for which n = 25 is a pseudoprime to the base a.

$$B(25) = \prod_{p|25} \gcd(24, p-1)$$

$$= \gcd(24,4) = 4.$$

Thus there are 4 bases a, these bases are a = 1, a = 7, a = 18, and a = 24. Clearly n = 25 is a pseudoprime to the bases a = 1. Now we are going to show that n = 25 is a pseudoprime to the bases a = 7, a = 18, and a = 24.

$(7)^2 \equiv -1 \pmod{25} \Rightarrow 7^{24} = (7^2)^{12} \equiv 1 \pmod{25}$.

$(18)^2 \equiv -1 \pmod{25} \Rightarrow (18)^{24} \equiv 1 \pmod{25}$.

$(24) \equiv -1 \pmod{25} \Rightarrow (24)^{24} \equiv 1 \pmod{25}$.

So 25 is a pseudoprime to the bases a = 7, 18, and 24.

(2). Let us calculate B(561).

$$B(561) = \prod_{p|561} \gcd(561-1,p)$$

$$= \gcd(561,2)*\gcd(560,10)*\gcd(560,16)$$

$$= 2*10*16$$

$$= 320.$$

As we stated in chapter 2, n = 561 is a pseudoprime to every positive integer a relatively prime to 561. Thus n = 561 is a pseudoprime to $\phi(561)$ bases. But $\phi(561) = 561(1-1/3)(1-1/11)$. $(1- 1/17) = 2*10*16 = 320$.

Corollary. If n is an odd composite number, which is not a power of 3, then n is a pseudoprime for at least two bases a, with $1 < a \leq n-1$, and $\gcd(a,n) = 1$.

Proof: From the proof of Theorem 3.11, it follows that the number of nontrivial bases a for which n is a pseudoprime with

respect to is given by

$$\left[\prod_{i=1}^{r} \gcd(n-1, p_i-1)\right]-2 .$$

Moreover, if n is odd, then both n - 1 and p_i - 1 are even, and hence gcd(n-1, p_i-1) ≥ 2, for every i = 1, 2, . . ., r. Thus if n is not power of 3, then n has at least two distinct prime factors or n is a power of prime > 3. In both cases it follows that $\left[\prod_{i=1}^{r} \gcd(n-1, p_i-1\right]-2 \geq 2$.

Chapter 4

SPECIAL KINDS OF PSEUDOPRIMES

In this chapter we are going to give a brief discussion of some special kinds of pseudoprimes, among them absolute pseudoprimes (or **Carmichael** numbers), **Euler** pseudoprimes, and **strong** pseudoprimes.

4.1 ABSOLUTE PSEUDOPRIMES(OR CARMICHAEL NUMBERS)

Definition 4.1. A composite integer n which satisfies congruence $a^{n-1} \equiv 1 \pmod{n}$ for all positive integers a with gcd(a,n) = 1 is called an **absolute pseudoprime** or **Carmichael number**.

Example. We are going to show n = 561 is a **Carmichael** number. Let us choose an integer b such that gcd(b, 561) = 1. Then gcd(b,3) = gcd(b,11) = gcd(b, 17) = 1. Hence, by **Fermat's** Little Theorem, we have $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$, and $b^{16} \equiv 1 \pmod{17}$. Consequently, $b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$, $b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$, and $b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$. Hence, by Theorem 1.3, $b^{560} \equiv 1 \pmod{561}$ for all b with gcd(b,n) = 1.

In fact n = 561 is the smallest **Carmichael** number.

Theorem 4.1(Carmichael). Let n be an odd composite integer. If n is divisible by a perfect square grater than 1, then n is not a **Carmichael** number.

Proof: Suppose that $p^2|n$. Let g be a generator modulo p^2, i.e. g is an integer whose order(mod p^2) is $\phi(p^2) = p(p-1)$. Let n' be the product of all primes other than p which divide n. By the Chinese Remainder Theorem, there is an integer b satisfying the two congruences: $b \equiv g \pmod{p^2}$ and $b \equiv 1 \pmod{n'}$. Then b, like the generator g, is a generator modulo p^2. The integer b also satisfies gcd(b,n) = 1, since it is not divisible by p or by any prime which divides n'. We claim that n is not pseudoprime to the base b. This is easily seen because if $b^{n-1} \equiv 1 \pmod{n}$ holds, then since $p^2|n$, we automatically have $b^{n-1} \equiv 1 \pmod{p^2}$. But in this case $p(p-1)|(n-1)$, since p(p-1) is the order of b modulo p^2. However, $n-1 \equiv -1 \pmod{p}$, since p|n. This means that n-1 is not divisible by p(p-1). This contradiction proves that there is a base b for which n fails to be a pseudoprime to the base 2.. This completes the proof.

Theorem 4.2. If $n = q_1 q_2 \ldots q_k$, where the q_j's are distinct primes that satisfy $(q_j-1)|(n-1)$ for all j, then n is a **Carmichael** number.

Proof: Let b be a positive integer with gcd(b,n) = 1. Then gcd(b,q_j) = 1 for all j = 1,2, . . ., k, and hence by **Fermat's** Little Theorem, $b^{q_j-1} \equiv 1 \pmod{q_j}$ for all j = 1,2, . . . , k. Since $(q_j - 1) \mid (n-1)$, then for each integer j = 1,2, . . ., k, there are integers t_j with $t_j(q_j-1) = n-1$. Hence, for each j, we know that $b^{n-1} = b^{(q_j-1)t_j} \equiv 1 \pmod{q^j}$. Therefore, by Theorem 1.3, we see that $b^{n-1} \equiv 1 \pmod{n}$, and we conclude that n is a **Carmichael** number. This completes the proof.

Example. Theorem 4.2 shows that 6601 = 7*23*41 is a **Carmichael** number, because 7, 23, and 41 are all prime, 6 = (7-1)|6600, 22 = (23-1)|6600, and 40 = (41-1)|6600.

The converse of Theorem 4.2 is also true. That is, all **Carmichael** numbers are of the form $q_1 q_2 \ldots q_k$, where the q_j's are distinct primes and $(q_j-1) \mid (n-1)$ for all j. Before proving the converse, we need to introduce the concept of universal exponents.

Let n be a positive integer with the canonical prime factorization $n = p_1^{t_1} p_2^{t_2} \ldots p_m^{t_m}$.

If a is an integer relatively prime to n, then **Euler's** Theorem

tells us that $a^{\phi(p^t)} \equiv 1 \pmod{p^t}$, where P^t is one of the prime powers occurring in the factorization of n.

Let

$$U = \text{lcm}[\phi(p_1^{t_1}), \phi(p_2^{t_2}) \ldots, \phi(p_m^{t_m})],$$

since $\phi(p_i^{t_i}) \mid U$ for i = 1,2, . . ., m,

using Theorem 1.3, we see that

$$a^U \equiv 1 \pmod{p_i^{t_i}},$$

and hence it follows that

$$a^U \equiv 1 \pmod{n}.$$

This leads to the following definition.

Definition 4.2. A **universal exponent** of a positive integer n is a positive integer U such that

$$a^U \equiv 1 \pmod{n}$$

for all integers a relatively prime to n.

Definition 4.3. The least universal exponent of a positive integer n is called the **minimal universal exponent** of n, and is denoted by $\lambda(n)$.

A formula for the minimal universal exponent $\lambda(n)$ is given in the following theorem, whose proof can be found in many elementary number theory books, such as [25].

Theorem 4.3. Let n be a positive integer with prime power factorization

$$n = 2^{t_0} p_1^{t_1} p_2^{t_2} \ldots p_m^{t_m}.$$

Then $\lambda(n)$, the minimal universal exponent of n is given by

$$\lambda(n) = \text{lcm}[\lambda(2^{t_0}), \Phi(p_1^{t_1}), \ldots, \phi(p_m^{t_m})].$$

Moreover, there exists an integer a such that $\text{ord}_n(a) = \lambda(n)$, the largest possible order of an integer modulo n.

Finally we prove the converse of Theorem 4.2.

Theorem 4.4. If $n > 2$ is a **Carmichael** number, then $n = q_1 q_2 \ldots q_k$, where the q_j's are distinct primes such that $(q_j - 1) | n-1$ for $j = 1, 2, \ldots, k$.

proof: If n is a **Carmichael** number, then

$$b^{n-1} \equiv 1 \pmod{n},$$

for all possible integers b with $\gcd(b,n) = 1$. Theorem 4.3 tells us that there is an integer a with $\text{ord}_n(a) = \lambda(n)$, where $\lambda(n)$ is the minimal universal exponent, and since $a^{n-1} \equiv 1 \pmod{n}$, Theorem 1.6 tells us that

$$\lambda(n) | (n-1).$$

Now n must be odd, for if n is even, then n-1 would be odd. But $\lambda(n)$ is even (since $n > 2$), contradicting the fact that $\lambda(n) | (n-1)$.

We now show that n must be the product of distinct primes. Suppose n has a prime-power factor p^t with $t \geq 2$. Then

$$\lambda(p^t) = \phi(p^t) = p^{t-1}(p-1) | \lambda(n) = n-1.$$

This implies $p | (n-1)$, which is impossible since $p | n$. Consequently, n must be the product of distinct odd primes,

say

$$n = q_1 q_2 \cdot \cdot \cdot q_k.$$

We conclude the proof by noting that

$$\lambda(q_i) = \phi(q_i) = (q_j-1) \mid \lambda(n) = n-1.$$

Theorem 4.5. A **Carmichael** number must have at least three different odd prime factors.

proof: Let n be a **Carmichael** number. Then n cannot have just one prime factor, since it is composite and is the product of at least two distinct primes. So assume that n = pq, where p and q are odd primes with p > q. Then

$$n-1 = pq-1 = (p-1)q+(q-1) \equiv q-1 \neq 0 \pmod{p-1},$$

which shows that $(p-1) \nmid (n-1)$. Hence, by Theorem 4.4, n cannot be a **Carmichael** number if it has just two different prime factors. This completes the proof.

There are many unanswered questions concerning **Carmichael** numbers. For example, it is not known whether there exist infinitely many **Carmichael** numbers. It has been conjectured that there are infinitely many **Carmichael** numbers, but so far this conjecture has not been settled. In support of this conjecture **Chernick** [5], developed a method of obtaining **Carmichael** numbers with $k \geq 3$ prime factors. First we need to establish the following lemmas.

Lemma 4.6. Let $m \geq 1$ and $M_3(m) = (6m+1)(12m+1)(18m+1)$.

If m is such that all three factors 6m+1, 12m + 1, 18m + 1 are prime then $M_3(m)$ is a **Carmichael** number.

Proof: Expand the expression

$$M_3(m) = (6m + 1)(12m+1)(18m+1)$$
$$= 36m(36m^2+648m+1)+1,$$

hence $M_3(m)-1 = 36m(36m^2+468m+1)$.

Thus $36m \mid M_3(m)-1$, and hence $6m \mid M_3(m)-1$, $12m \mid M_3(m)-1$, and $18m \mid M_3(m)-1$. Therefore, Theorem 4.2 implies $M_3(m)$ is a **Carmichael**number. This completes the proof.

Example. For m = 1, $M_3(1) = 7*13*79 = 1729$ is a **Carmichael** number. For m = 6, $M_3(6) = 37*73*109 = 294409$ is a **Carmichael** number.

Lemma 4.7. Let $C_{n-1} = p_1p_2, \ldots, p_{n-1}$, where the p_i's are distinct primes be a **Carmichael** number, let $q = \text{lcm}[p_1-1, p_2-1, \ldots, p_{n-1}-1]$, and $r = \frac{C_{n-1}-1}{q}$. If $p_n = q\pi + 1$, where π is any divisor of r and p_n is a prime distinct from all the p_i's, i = 1, 2,..., n-1, then $C_n = p_1 p_2 \ldots p_n$ is a **Carmichael** number.

Proof: By Theorem 4.2, it suffices to show that $(p_i-1) \mid (C_n-1)$ for i = 1,2,..., n. Since $C_i-1 = C_{n-1}p_n$, it follows that

$$C_n-1 = C_{n-1}p_n-1 = (qr+1)(q\pi+1)-1$$

$= q(qr\pi+r+\pi)$.

Hence, $q|C_n-1$.

But since $q = lcm[p_i-1, \ldots, p_n-1]$, then

$(p_i-1)|q$ for $i = 1, 2, \ldots, n-1$.

Thus $(p_i-1)|C_n-1$ for $i = 1,2, \ldots, n-1$.

Thus it remains to show that $(p_n-1)|(C_n-1)$.

We have $C_n = C_{n-1}p_n \equiv C_{n-1} \pmod{p_n-1}$ . . . . (1).

Since $\pi|r$ then $r = \pi k$ for some integer k.

Now, $C_{n-1}-1 = qr$, and $p_n-1 = q\pi$, hence $C_{n-1}-1 = q\pi k = (p_n-1)k$.

Thus $C_{n-1} \equiv 1 \pmod{p_n-1}$ . . . (2).

Therefore, (1) and (2) implies

$C_n \equiv 1 \pmod{p^n-1}$, and hence $(p_n-1)|(C_n-1)$. This completes the proof.

Lemma 4.6 and 4.7 provide the basis for a proof by mathematical induction of the following theorem.

Theorem 4.8. Let $k \geq 4$, $m \geq 1$ be integers, and

let $M_k(m) = (6m+1)(12m+1)\prod_{i=1}^{k-2}(9*2^i m+1)$ be a **Carmichael** number. If m is such that all k factors in the right hand side are prime numbers, and $2^{k-4}|m$, then $M_k(m)$ is a **Carmichael** number with k prime factors.

Proof: For $k = 4$, $M_4(m) = (6m+1)(12m+1)(36+1)$. By Lemma 4.6 we

have $M_3(m) = (6m+1)(12m+1)(18m+1)$ is a **Carmichael** number. Now by applying lemma 4.7, $q = \text{lcm}[6m, 12m, 18m] = 36m$, and by taking $\pi = 1$, then $M_4(m)$ is a **Carmichael** number. Now assume that for some $k \geq 4$, $M_k(m) = (6m+1)(12m+1)\prod_{i=1}^{k-2}(9*2^i m+1)$ is a

Carmichael number. Assume also that all the factors in the right hand side are prime numbers and that $2^{k-4} | m$. Consider

$$M_{k+1}(m) = (6m+1)(12m+1)\prod_{i=1}^{k-1}(9*2^i m+1)$$

$$= M_k(m)(9*2^{k-1}m+1)$$

$$= M_k(m)P_{k+1}.$$

Now applying Lemma 4.7, we have

$$q = \text{lcm}[6m, 12m, \ldots, 9*2^{k-2}m] = 9*2^{k-2}*9m = P_k - 1.$$

By the induction hypothesis we have $M_k(m)$ is a **Carmichael** number with k prime factors, where $P_k = 9*2^{k-2}m+1$ is one of its prime factors. Thus by Theorem 4.4, $(P_k-1) | M_k(m-1)$. Let $r = \frac{M_k(m)-1}{P_k-1} = \frac{M_k(m)-1}{q}$. Since $2^{k-4} | m$, then $\pi = 2$ is a divisor of

r. Since $q\pi+1 = 9*2^{k-1}m+1 = p_{k+1}$, Lemma 4.7 implies that M_{k+1} is a **Carmichael** number. This completes the proof.

Example. For $m = 1$, $k = 4$,

$M_k(1) = 7*13*\prod_{i=1}^{2}(9*2^i+1) = 7*13*17*37 = 63973$ is a **Carmichael**

number.

4.2 EULER PSEUDOPRIMES

According to **Euler's** Criterion, if p is an odd prime and b is an integer not divisible by p, then $\left(\frac{a}{b}\right) \equiv a^{(p-1)/2} \pmod{p}$,

where $\left(\frac{a}{b}\right)$ is the **Legendre** symbol. Hence, if we wish to test the positive integer n for primality, we can take an integer b, with gcd(b,n) = 1 and determine whether

$$b^{(n-1)/2} \equiv \left[\frac{a}{n}\right] \pmod{n} \text{ holds,}$$

where the symbol on the right hand side of the congruence is the **Jacobi** symbol. If we find that this congruence fails, then n is composite.

Example. Let n = 341 and b = 2. We calculate that $2^{170} \equiv 1 \pmod{341}$. Since $341 \equiv -3 \pmod{8}$, using Theorem 1.8 from chapter 1, we see that $\left[\frac{2}{341}\right] = -1$. Consequently, $2^{170} \not\equiv \left[\frac{2}{341}\right] \pmod{341}$. This demonstrate that 341 is not a prime.

Thus, we can define a type of pseudoprime based on **Euler's** criterion.

Definition 4.4. An odd composite positive integer n that satisfies the congruence

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \pmod{n},$$

where b is a positive integer, is called an **Euler pseudoprime** to the base b.

Example. Let n = 1105 and b = 2. We calculate that $2^{552} \equiv 1 \pmod{1105}$. Since $1105 \equiv 1 \pmod{8}$. We see that $\left[\frac{2}{1105}\right] = 1$.

Hence, $2^{552} \equiv \left[\frac{2}{1105}\right] \pmod{1105}$. Because 1105 is composite, it is an **Euler** pseudoprime to the base 2.

The following theorem shows that every **Euler** pseudoprime to the base b is a pseudoprime to this base.

Theorem 4.9. If n is an **Euler** pseudoprime to the base b, then n is a pseudoprime to this base.

Proof: If n is an **Euler** pseudoprime to the base b, then

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \pmod{n}.$$

Hence, by squaring both sides of this congruence, we find that

$$(b^{(n-1)/2})^2 \equiv \left[\frac{b}{n}\right]^2.$$

Since $\left[\frac{b}{n}\right] = \pm 1$, We see that $b^{n-1} \equiv 1 \pmod{n}$. This means that n is a pseudoprime to the base b. This completes the proof.

Not every pseudoprime is an **Euler** Pseudoprime to the base 2. For example, the integer 341 is not an **Euler** pseudoprime to the base 2, as we have shown, but is a pseudoprime to this base.

One natural question is: Can an odd composite number be an **Euler** Pseudoprime for every possible a, with $1 < a < n$, where gcd(a,n) = 1? In 1976 **Lehmer** [17] showed the answer to this question to be in the negative.

Theorem 4.10. No odd composite number N is an **Euler** pseudoprime to every base a relatively prime to N.

Proof: Assume the contrary, that is, let N be an odd composite integer such that N is an **Euler** pseudoprime to every base a where $1 \leq a < N$ and gcd(a, N) = 1. Theorem 4.9 implies N is a **Carmichael** number. We have shown in Theorem 4.5 that every **Carmichael** number N is the product of at least three distinct primes. Therefore we can write

$N = p_1 p_2 \ldots, P_t$, where $(p_1 > 2, t \geq 3)$.

Also the congruence relations $a^{n-1} \equiv 1 \pmod{p_i}$, $i = 1,2, \ldots, t$ holds for every a. In particular, if a = q any common

primitive root of all the p_i's, then

$$q^{N-1} \equiv 1 \pmod{p_i}, \quad i = 1,2,\ldots,t.$$

Thus

$$N-1 \equiv 1 \pmod{p_i-1}.$$

Now the primes $p_1, p_2, \ldots, p_t$ can be divided into two types.

Type 1 : Those p for which $\frac{N-1}{2} \equiv 0 \pmod{p-1}$.

Type 2 : Those p for which $\frac{N-1}{2} \equiv \frac{p-1}{2} \pmod{p-1}$.

Thus we have $a^{N-1} \equiv 1 \pmod{p}$ if p is of type 1,

and $a^{(N-1)/2} \equiv \left(\frac{a}{p}\right)$ if p is of type 2.

We now choose a to be quadratic nonresidue of p_1 and a residue for all the other p_i's. First suppose there is a prime of type 1 which we may take to be p_1. Since N is an **Euler** pseudoprime to the base a, then

$$-1 \equiv \left(\frac{a}{N}\right) \equiv a^{\frac{(N-1)}{2}} \equiv 1 \pmod{p_1}.$$

This contradiction shows that all the p's are of type 2. Thus we must have

$$a^{\frac{(N-1)}{2}} \equiv 1 \pmod{p_2}.$$

But, n is an **Euler** psedoprime, implies

$$a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{p_1p_2}, \text{ that is, } a^{\frac{N-1}{2}} \equiv -1 \pmod{p_2}.$$

This contradiction completes the proof.

In 1986, **Kiss, Phong** and **Lieuwens** [13] proved the following result concerning the number of Euler pseudoprimes.

Theorem 4.11. There exists infinitely many **Euler** pseudoprimes to the base b, which are the product of k distinct prime factors.

The proof of this theorem is beyond the scope of this paper.

Finally we close this section with a formula for the number of bases a for which a given odd composite integer n is an **Euler** pseudoprime with respect to a. Let n be an odd composite integer. Let $B_{epsp}(n)$ denote the number of bases a, where $1 < a < n$ and $\gcd(a,n) = 1$ and such that n is an **Euler** pseudoprime to these bases a. In [19] Monier showed that

$$B_{epsp}(n) = \delta(n)\left\{\prod_{p|n} \gcd\left(\frac{n-1}{2}, p-1\right)\right\}-1,$$

where

$$\delta(n) = \begin{cases} 2, & \text{if } v_2(n-1) = \min\limits_{p|n}\{v_2(p-1)\} \\ 1/2, & \text{if there exists a prime p dividing n such that } v_2(p-1) < v_2(n-1). \\ 1, & \text{otherwise.} \end{cases}$$

In the definition of $\delta(n)$ above, $v_p(n)$ denotes the exponent of p in the prime factorization of n and $v_2(n-1)$ is the exponent of 2 in the prime factorization of n-1.

Example. Let us apply this formula to find the number of bases for which n = 2407 = 29*83 is an **Euler** pseudoprime with respect to. First we calculate

$$\prod_{p|n} \gcd\left(\frac{n-1}{2}, p-1\right),$$

$$\prod_{p|2407} \gcd(1203, p-1)$$

$$= \gcd(1203,28)*\gcd(1203,82)$$

$$= 1*1 = 1.$$

Now, we calculate $\delta(n)$.

$$\upsilon_2(n-1) = \upsilon_2(2406) = \upsilon_2(2^1*3*401) = 1$$

$$\min_{p|n} \upsilon_2(p-1) = \min\{\upsilon_2(28), \upsilon_2(82)\}$$

$$= \min\{\upsilon_2(2^2*7), \upsilon_2(2^1*41)\}$$

$$= \min\{2,1\} = 1.$$

Hence $\delta(2407) = 2$. Thus $B_{epsp}(2407) = 2-1 = 1$.

In fact n = 2407 is an **Euler** pseudoprime only to the base a = 2.

4.3 STRONG PSEUDOPRIMES

In this section, we are going to study a special kind of pseudoprimes that are very useful in primality testing. Let p be a prime and b a positive integer relatively prime to p. Assume that $p-1 = 2^s t$, where t is odd and s is a nonnegative integer. We have $a^{p-1} \equiv 1 \pmod{p}$, and since $x^2 \equiv 1 \pmod{p}$

hold if and only if $x = \pm 1 \pmod p$, then $a^{2^j t} \equiv \pm 1 \pmod p$ for every $j = 0,1,2, \ldots, s$. Thus, we can define a type of pseudoprime based on the observation above.

Definition 4.5. Let n be an odd composite integer. Let $n-1 = 2^s t$, where s is a nonnegative integer and t is odd positive integer. Let b be an integer such that $1 < b < n$, and $\gcd(b,n) = 1$, we say that n is a **strong pseudopprime** to the base b if either $b^t \equiv 1 \pmod n$, or there exists j, $0 \le j < s$ such that $b^{2^j t} \equiv -1 \pmod n$.

Theorem 4.12. If n is a strong pseudoprime to the b then n is pseudoprime to the base b.

Proof: If n is a strong pseudoprime, then either $b^t \equiv 1 \pmod n$ or $b^{2^j t} \equiv -1 \pmod n$ for some j with $0 \le j \le s-1$ where $n-1 = 2^s t$ as in the definition. Thus if $b^t \equiv 1 \pmod n$, then $b^{n-1} = (b^t)^{2^s} \equiv 1 \pmod n$. On the other hand if $b^{2^j t} \equiv -1 \pmod n$ for some j, with $0 \le j \le s-1$, then since $b^{n-1} = (b^{2^j t})^{s-j}$, for $j = 0,1,2, \ldots, s$, we have $b^{n-1} \equiv 1 \pmod n$. Thus in either case $b^{n-1} \equiv 1 \pmod n$ and hence n is a pseudoprime to the base b. This completes the proof.

Example. Let $n = 2047$. Then $2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1 \pmod$

2047), so that 2047 is a pseudoprime to the base 2. Since $2^{2046/2} =$

$2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1 \pmod{2047}$. Hence, 2047 is a strong pseudoprime to the base 2.

The converse of Theorem 4.12 is not true. For example, n = 1387 = 19*73 is a pseudoprime to the base 2 but is not strong pseudoprime to the base 2.

Although strong pseudoprimes are exceedingly rare, there are still infinitely many of them. We demonstrate this for the base 2 with the following theorem.

Theorem 4.13. There are infinitely many strong pseudoprime to the base 2.

Proof: We shall show that if n is a pseudoprime to the base 2, then $2^n - 1$ is a strong pseudoprime to the base 2.

Let n be an odd integer which is a pseudoprime to the base 2. Hence, n and $N = 2^n-1$ are composite, and $2^{n-1} \equiv 1 \pmod{n}$. From this congruence, We see that $2^{n-1}-1 = nk$ for some integer k, furthermore, k must be odd. We have

$$N-1 = 2^n - 2 = 2(2^{n-1}-1) = 2^1 nk,$$

this is a factorization of N-1 into an odd integer and a power of 2. We now note that

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \pmod{N},$$

because $2^n = (2^n-1)+1 = N+1 \equiv 1 \pmod{N}$. This implies that N is a strong pseudoprime to the base 2. Since every pseudoprime

$2^n - 1$ yields a strong pseudoprime to the base 2 and since there are infinitely many pseudoprimes to the base 2, we conclude that there are infinitely many strong pseudoprime to the base 2.

Corollary. There exists infinitely many strong pseudoprime to the base 2 with arbitrarily many prime factors.

Proof: By Theorem 2.21, it follows that for every integer $k \geq$ there are infinitely many square free pseudoprimes to the base 2 with exactly k prime factors. By the theorem above, if n is a pseudoprime to the base 2, with k prime factors, then $2^n - 1$ is a strong pseudoprime to the base 2. Moreover, if p is one of the prime factors of n, then by Lemma 2.1, we have $2^p-1 | 2^n-1$. Since the number 2^p-1 with distinct primes p are relatively prime, the number 2^n-1 has at least as many prime factor as n. Thus 2^n-1 is a strong pseudoprime to the base 2 with at least k prime factors.

Theorem 4.14. Every composite Fermat number $F_n = 2^{2^n}+1$ is a strong pseudoprime to the base 2

Proof: Since $F_n-1 = 2^{2^n}$, then

$$2^{F_n-1} = 2^{2^{2^n}} = (2^{2^n})^{2^{2^n-n}} = (F_n-1)^{2^{2^n-n}}.$$

$$(F_n-1)^{2^{2^n-n}} \equiv (-1)^{2^{2^n-n}} = 1 \pmod{F_n}.$$

Now, taking square roots will always give 1's until eventually, after 2^n-n times, a (-1) will appear. Thus F_n is a strong pseudoprime whenever F_n is composite. This completes the proof.

We know that every **Euler** pseudoprime is a pseudoprime. Next we show that every strong pseudoprime is an **Euler** pseudoprime.

Theorem 4.15. If n is a strong pseudoprime to the base b, then n is an **Euler** pseudoprime to this base.

Proof: If n be a strong pseudoprime to the base b. Then if n-1 = 2^st, where t is odd, either $b^t \equiv 1 \pmod{n}$ or $b^{2^r t} \equiv -1 \pmod{n}$, where $0 \le r \le s-1$. Let $n = \prod_{i=1}^{m} p_i^{a_i}$ be the prime-power factorization of n.

First, we consider the case where $b^t \equiv 1 \pmod{n}$. Let p be a prime divisor of n. Since $b^t \equiv 1 \pmod{n}$, we know that $\text{ord}_p(b) \mid t$. Because t is odd, we see that $\text{ord}_p(b)$ is also odd. Hence, $\text{ord}_p(b) \mid (p-1)/2$, since $\text{ord}_p(b)$ is an odd divisor of the even integer $\phi(p-1) = p-1$. Therefore,

$$b^{(p-1)/2} \equiv 1 \pmod{p}.$$

Consequently, by **Euler's** criterion, we have $\left[\frac{b}{p}\right] = 1$. To

compute the **Jaccobi** symbol $\left[\frac{b}{n}\right]$, we note that $\left[\frac{b}{p}\right] = 1$ for all primes p dividing n. Hence,

$$\left[\frac{b}{n}\right] = \left[\frac{b}{\prod_{i=1}^{m} p_i^{a_i}}\right] = \prod_{i=1}^{m}\left[\frac{b}{p_i}\right]^{a_i} = 1.$$

Since $b^t \equiv 1 \pmod n$, we know that $b^{(n-1)/2} = (b^t)^{2^{s-1}} \equiv 1 \pmod n$. Therefore, we have

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \equiv 1 \pmod n.$$

We conclude that n is an **Euler's** pseudoprime to the base b.

Next, we consider the case where

$$b^{2^r t} \equiv -1 \pmod n$$

for some r with $0 \le r \le s-1$. If p is a prime divisor of n, then

$$b^{2^r t} \equiv -1 \pmod p.$$

Squaring both sides of this congruence, we obtain

$$b^{2^{r+1} t} \equiv 1 \pmod p.$$

This implies that $\mathrm{ord}_p(b) \mid 2^{r+1}t$, but that $\mathrm{ord}_p(b) \nmid 2^r t$. Hence,

$$\mathrm{ord}_p(b) = 2^{r+1}c,$$

where c is an odd integer. Since $\mathrm{ord}_p(b) \mid (p-1)$ and $2^{r+1} \mid \mathrm{ord}_p(b)$, it follows that $2^{r+1} \mid p-1)$.

Therefore, we have $p = 2^{r+1}d+1$, where d is an integer. Since

$$b^{(ord_p(b))/2} \equiv -1 \pmod{p}.$$

We have

$$\left[\frac{b}{p}\right] \equiv b^{(p-1)/2} = b^{(ord_p(b)/2)\,(p-1)/ord_p(b))}$$

$$\equiv (-1)^{(p-1)/ord_p(b)} = (-1)^{(p-1)/2^{r+1}c} \pmod{p}.$$

Because c is odd, we know that $(-1)^c = -1$. Hence,

$$\left[\frac{b}{p}\right] = (-1)^{(p-1)/2^{r+1}} = (-1)^d \quad . \quad . \quad . \quad (1).$$

recalling that $d = (p-1)/2^{r+1}$. Since each prime p_i dividing n is of the form $p_i = 2^{r+1}d_i+1$, it follows that

$$n = \prod_{i=1}^{m} p_i^{a_i}$$

$$= \prod_{i=1}^{m} (2^{r+1}d_i+1)^{a_i}$$

$$\equiv \prod_{i=1}^{m} (1+2^{r+1}a_i d_i)$$

$$\equiv 1+2^{r+1}\sum_{i=1}^{m} a_i d_i \pmod{2^{2r+2}}.$$

Therefore,

$$t\ 2^{s-1} = (n-1)/2 \equiv 2^r \sum_{i=1}^{m} a_i d_i \pmod{2^{r+1}}.$$

This congruence implies that

$$t\ 2^{s-1-r} \equiv \sum_{i=1}^{m} a_i d_i \pmod 2, \text{ and}$$

$$b^{(n-1)/2} = (b^{2^r t})^{2^{s-1-r}} \equiv (-1)^{2^{s-1-r}} = (-1)^{\sum_{i=1}^{m} a_i d_i} \pmod n \quad \ldots (2).$$

On the other hand, from (1), we have

$$\left[\frac{b}{n}\right] = \prod_{i=1}^{m} \left[\frac{b}{n}\right]^{a_i} = \prod_{i=1}^{m} ((-1)^{d_i})^{a_i} = \prod_{i=1}^{m} (-1)^{a_j d_j} = (-1)^{\sum_{i=1}^{m} a_i d_i}.$$

Therefore, combining the previous equation with (2), we see that $b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \pmod n$.

Consequently, n is an **Euler** pseudoprime to the base b. This completes the proof.

Corollary. There exist infinitely many **Euler** pseudoprime to the base 2 with arbitrarily many prime factors

Proof: The proof follows directly from the theorem above and the

corollary to Theorem 4.13.

Although every strong pseudopsrime to the base b is an **Euler** pseudoprime to this base b, the converse is not true,

as the following example shows.

Example. We have previously shown that the integer 1105 is an Euler pseudoprime to the base 2. However, 1105 is not a strong pseudoprime to the base 2 since

$$2^{(1105-1)/2} = 2^{552} \equiv 1 \pmod{1105},$$

while

$$2^{(1105-1)/2^2} = 2^{276} \equiv 781 \neq \pm 1 \pmod{1105}.$$

Although an **Euler** pseudoprime to the base b is not always a strong pseudoprime to this base, when certain extra conditions are met, an **Euler** pseudoprime to the base b is, in fact, a strong pseudoprime to this base. The following two theorems give results of this kind.

Theorem 4.16(Malm, 1977). If $n \equiv 3 \pmod 4$ and n is an **Euler Pseudoprime** to the base b, then n is a strong pseudoprime to the base b.

Proof: From the congruence $n \equiv 3 \pmod 4$, we know that $n-1 = 2.t$ where $t = (n-1)/2$ is odd. Since n is **Euler** pseudoprime to the base b, it follows that

$$b^t = b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \pmod{n}.$$

Since $\left[\frac{b}{n}\right] = \pm 1$, we know that either $b^t \equiv 1 \pmod n$ or $b^t \equiv -1 \pmod n$. Hence, one of the congruences in the

definition of a strong pseudoprime to the base b must hold. Consequently, n is a strong pseudoprime to the base b.

Theorem 4.17 (Pomerance, Seltridge & Wagstaff, 1980). If n is a an Euler Pseudoprime to the base b, and $\left[\frac{b}{n}\right] = -1$, then n is a strong pseudoprime to the base b.

Proof: we write $n-1 = 2^s t$, where t is odd and s is a positive integer. Since n is an **Euler** pseudoprime to the base b, we have

$$b^{2^{s-1}t} = b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \pmod{n}.$$

But since

$$\left[\frac{b}{n}\right] = -1,$$

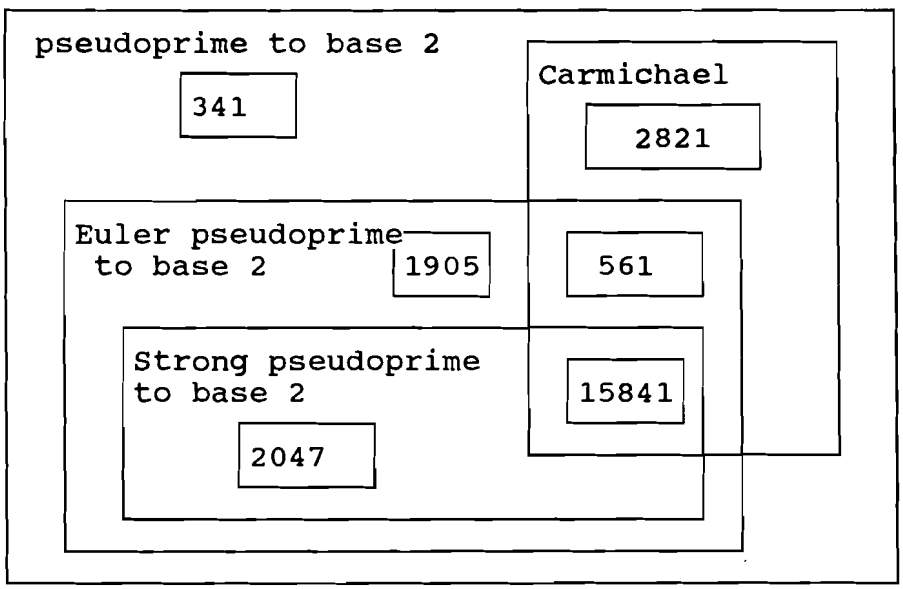
we see that

$$b^{t2^{s-1}} \equiv -1 \pmod{n}.$$

This is one of the congruences in the definition of strong pseudoprime to the base b. Since n is composite, it is a strong pseudoprime to the base b. This completes the proof.

The **venn** diagram below illustrate the relationship between the different kinds of pseudoprime numbers to the base 2 considered in this study together with the least element of

each kind.



In the table below, $\pi P_2(x)$, $E_2(x)$, $\pi S_2(x)$, $\pi C(x)$, $\pi(x)$ denote the number of pseudoprimes, Euler pseudorimes Strong pseudoprimes(base 2), Carmichael numbers, and primes less than or equal to x

x	$\pi P_2(x)$	$\pi E_2(X)$	$\pi S_2(X)$	$\pi C(X)$	$\pi(X)$
10^3	3	1	0	1	168
10^4	22	12	5	7	1,229
10_5	78	36	16	16	9,512
10^6	245	114	46	43	78,498
10^7	750	375	162	105	664,579
10^8	2057	1071	488	255	5,761,456
10^9	5597	2939	1282	646	50,847,534

From this table it is clear that for each given value of x , $\pi C(x) < \pi S_2(x) < \pi E_2(x) < \pi P_2(x)$.

In fact these inequalities are true for any basis as we have seen in Theorem 4.9, Theorem 4.10, Theorem 4.12, and Theorem 4.15.

4.4 PRIMALITY TESTS BASED ON STRONG PSEUDOPRIMES AND EULER PSEUDOPRIMES

In this section we are going to give an out line of two probabilistic primality tests one based on the concept of strong pseudoprimes and the other on **Euler's** pseudoprimes. First, we are going to state a theorem whose proof can be found in [14].

Theorem 4.18. If n is an odd composite integer, then n is a strong pseudoprime to the base a for at most 25% of all the a's where $0 < a < n$.

Rabin's Probabilistic primality Test[23].

Let N be a positive integer that we need to determine whether it is prime or composite.

Step 1.

Choose at random $k > 1$ bases a, with $1 < a < N$, $\gcd(a,N) = 1$.

Step 2.

Test in succession, for each chosen basis a, whether N satisfy the condition in the definition of a strong

pseudoprime in base a; writing $N-1 = 2^s d$ with d odd , $s \geq 0$, and determine whether $a^d \equiv 1 \pmod{n}$ or $a^{2^r d} \equiv -1 \pmod{N}$ for some r, $0 \leq r < s$ hold.

If an a is found for which the above condition does not hold, then declare N to be composite. Otherwise, declare N to be prime.

Remarks. The comments at the beginning of section 4.3 tells us that if the integer N is declared composite by the test, then in fact N is composite. On the other hand if N is declared prime, then according to the previous theorem, the probability that N is a prime,is at least $1-\frac{1}{4^k}$. so, for k = 30, the likely error is at most one in 10^{18} test.

Another useful probabilistic primality test was developed by **Solovay** and **Strassen** in 1977 [32].

The following theorem is the basis for this test, the proof is given in [32].

Theorem 4.19. Let n be an odd composite integer, then the number of bases a, where $0 < a < n$ and $\gcd(a,n) = 1$, for which n is an Euler pseudoprime, is less than $\frac{\phi(n)}{2}$.

Solovay - Strassen probabilistic Primality Test.

Let N be an odd positive integer that we need to determine

whether it is prime or composite.

Step 1. Choose k > 1 numbers a, with 1< a < N, and gcd(a,N) = 1. Usually a is taken not too large, so it is reasonably easly by trial division to confirm that gcd(a,N) = 1.

Step 2.

Test in succession whether N satisfies $\left[\frac{a}{N}\right] \equiv a^{(N-1)/2} \pmod{N}$, where $\left[\frac{a}{N}\right]$ is a **Jacobi** symbol, for the chosen values of a (that is, determine whether N satisfy the condition of an Euler pseudoprime in base a). If an a is found for which the above congruence does not hold , declare that N is composite. Otherwise, declare that N is prime.

Remark. If N is declared composite by the test, then the comments at the beginning of Section 4.2 tells that that is infact the case. On the other hand, if N is declared prime, then according to Theorem 4.19, if the trials with different bases are assumed to be mutually independent (there is no reason or numerical evidence to believe the contrary for the property in the definition of **Euler** pseudoprimes in different bases), then the probability that N is indeed a prime, when declared prime by the test, is at least $1-\frac{1}{2^k}$. For example if k = 30, then the likely error is at most one in billion tests.

Chapter 5

SUMMARY AND CONCLUSION

Our objective in this paper was to study pseudoprimes. In the course of its development, we have discussed pseudoprimes to the base 2, and subsequently generalized to any base a.

In chapter 1, we have provided the readers with a short account of basic concepts from elementary number theory that are needed in later chapters. Here we defined some important terms and stated theorems without proofs.

In chapter 2, we answered questions regarding the number of pseudoprimes, recognition of pseudoprimes, and the distribution of pseueudoprimes. Necessary and sufficient conditions for an integer to be a pseudoprime were established and several sequences generating infinitely many pseudoprimes were given.

In chapter 3, we discussed one of the generalizations of pseudoprimes. We discussed some necessary and sufficient conditions for an integer to be pseudoprime to a given base a. Questions regarding the number of pseudoprimes to a base a, functions that generate pseudoprimes to a base a, and the distribution of pseudoprime to a base a were discussed in this

chapter.

In chapter 4, we discussed some special kinds of pseudoprimes, including **absolute** pseudoprimes(or **Carmichael** numbers), **Euler** pseudoprimes and **strong** pseudoprimes. We concluded the paper with a brief discussion of two probabillistic primality tests, one based on the concept of Euler pseudoprimes and the other on strong pseudoprimes.

In conclusion, we suggest that the results of this paper could be extended in two ways. One way would be the study of other special kinds of pseudoprimes such as Lucas pseudoprimes, Fibonacci pseudoprimes and Lehmer pseudoprimes [24]. A second way would be to investigate the vast literature in primality tests based on different kinds of pseudoprimes.

BIBLOGRAPHY

[1] Bang, A.S. Taltheoretiske Undersogelser, Tidskrift for Math. 4 (1886) 70-80, 130-137.

[2] Beeger, N.G.W.H, On even numbers m dividing 2^m-2, Amer.Math. Monthly 58 (1951) 553-555.

[3] Burton, D.M. Elementary Number Theory. 2nd ed. Dubuque: Wm. C. Brown publishers, 1989.

[4] Carmichael,R.D. On composite numbers p which satisfy the Fermat congruence $a^{p-1} \equiv 1 \pmod{p}$, Amer. Math. Montly 19, (1912) 22-27.

[5] Chernick, J. On Fermat's simple theorem, Bull. Amer. Math. Soc., 45 (1939) 269-274.

[6] Cipolla, M. Sui Numeri composti P, che verificano la congruenza di Fermat $a^{p-1} \equiv 1 \pmod{P}$, Ann.Mat. Pura Appl. 9 (1904) 139-160.

[7] Crocker, R. A theorem on pseudoprimes, Amer.Math.Monthly 69 (1962) p.540.

[8] Dickson, L.E. History of the theory of numbers. Vol.1., New York, Chelsea Publishing Co. 1952.

[9] Erdös, P. On the converse of Fermat's theorem, Amer. Math. Monthly 56 (1949) 623-624.

[10] Erdös, P. On almost primes, Amer. Math. Monthly 57(1950)404-407.

[11] Erdös, P. Problem 4319, Amer. Math. Monthly (1950) P.346.

[12] Jeans, J.H. The converse of Fermat's theorem, Messenger of Mathematics 27 (1897) P.174.

[13] Kiss, P., Phong, B.M & Lieuens. On Lucus psudoprimes which are product of s primes. In Fibonacci Numbers and their Applications (edited by A.N. Philippou, G.E. Bergum & A.F. Horadam), 131-139. Reidel, Dordrecht, 1986.

[14] Koblitz, N. Acourse in Number Theory and Cryptography, New York: Springer-Verlag, 1987.

[15] Lehmer, D.H. On the converse of Fermat's theorem, Amer. Math. Monthly 43 (1936) 346-354.

[16] Lehmer, D.H. On the converse of Fermat's Theorem II, Amer. Math. Monthly 56 (1949) 300-309.

[17] Lehmer, D.H. Strong Carmichael numbers, J. Austral. Math. Soc., A, 21 (1976) 508-510.

[18] Malo, E. Nombre qui, sans être premieres, vérifient exceptionnellement une congruence de Fermat, Intermediare des Math. 10 (1903) p.86.

[19] Monier, L. Evaluation and comparison of two efficient probabilistic primality testing algorithms, Theoret. Comput. Sci.,12, (1980) 1003-1026.

[20] Pomerance, C. Selfridge, J.L. & Wagstaff Jr., S.S., The pseudoprimes to 25.10^9, Math.Comp., 35 (1980) 1003-1026.

[21] Pomerance, C. On the distribution of psuedo-primes, Math. Comp., 37 (1981) 587-593.

[22] Poulet, P. Table de nombres composés vérifieny le théorème de Fermat pour le module 2 jusgu'à 100000000,

Sphinx 8, (1938) 42-52.

[23] Rabin, M.O. Probabilistic algorithm for testing primality, J .Num.Th., 12 (1980) 128-138.

[24] Ribenboim, P. The Book of Prime Number Records, 2nd ed. New York: Springer-Verlag, 1989

[25] Rosen, K.H. Elementary Number Theory. 2nd ed. Reading: Addison - Wesley, 1988.

[26] Rotkiewicz, A. Sur les nombres pseudopremiers de la forme M_pM_q, 20, (1965) 108-109.

[27] Rotkiewicz, A. Less intervalles contentants less nombres pseudoprimes, Rend. Circ. Mat. Palermo 14 (1965), 278-280.

[28] Rotkiewicz, A. On the pseudoprimes of the form ax+b, Proc. Cambridge Philos.Soc. 63 (1967) 389-392.

[29] Rotkiewicz, A. Pseudoprime Numbers and their generalizations. Stud. Assoc. Fac. Sci. Univsad. 1972.

[30] Shanks D. Solved and Unsolved problems in Number Theorey. 2nd ed., New York : Chesla, 1978.

[31] Sierpinski, W. Elementry Theory of Numbers. Vol.30, North Holand: PWN- Polish Scientific Publishers, 1988.

[32] Solovay, R. & Strassen. A fast Monte-Carlo test for primality, SIAM J.Comput., 6 (1977) 84-85.

[33] Steuerwald, R. Über die Kongruenz $2^{n-1} \equiv 1 (\text{mod } n)$ Bayer.Akad.Wiss.Math.Nat.Kl. S-B., (1948) 69-70.

[34] Szymiczek, K. On pseudo-primes which are products o distinct primes, Amer. Math. Monthly 74 (1967) 35-37.

To: All Graduate Students Who Submit a Thesis or Research Problem/Project as Partial Fulfillment of the Requirements for an Advanced Degree

From: Emporia State University

I, M.Mizanur Rahman, 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 non profit nature. No copying which involves financial gain will be allowed without written permission of the author.

M.M.Rahman
Signature of the Author

July 24, 1992
Date

Pseudoprime Numbers
Title of Thesis/Research Project

Doug Cooper
Signature of Graduate Office Staff

July 24, 1992
Date Received

Distribution: Director, William Allen White Library
Graduate School Office
Author